Cisco WAN Switching Command Reference

Release 9.2
November 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-786721=
Text Part Number: 78-6721-05 Rev. A0

Feedback on the Cisco WAN Switching Command Reference

78-6721-05, Rev. A0

Release 9.2

November 2002

Thank you for taking the time to fill out this response card. Your input is important to us and helps us to provide you with better documentation.

If you have comments about this document, please complete this self-addressed response card and mail it to us.

We also encourage you to make copies of this blank response card to complete and send to us whenever you have comments about this document. You can mail copies of this card to:

Cisco Systems, Inc.
Attn: Document
Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

You can also send us your comments by e-mail to bug-doc@cisco.com, or fax your comments to us at (408) 527-8089.

You can also submit comments electronically on the World Wide Web. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

CISCO SYSTEMS

Documentation Response Card

Feedback on the Cisco WAN Switching Command Reference, Release 9.2, Rev. A0, November 2002

Please respond to the following statements by checking a number from 1 to 5:

5 Strongly agree
4 Somewhat agree
3 Neutral
2 Somewhat disagree
1 Strongly disagree

Overall, I am satisfied with this document.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

This document is accurate and free of errors.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

I can find the information I need in this document.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

This document is complete and offers enough relevant information for me to do my job.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

This document is written at the correct level of complexity for the subject matter.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

This document is useful to me in doing my job.

Strongly agree **5** ☐ **4** ☐ **3** ☐ **2** ☐ **1** ☐ Strongly disagree

Would you like us to contact you? Yes ☐ No ☐

Additional Feedback

____

____

____

____

____

____

____

____

Mailing Information

Date ______________________________

Company Name ______________________________

Contact Name ______________________________

Mailing Address ______________________________

____

City	State/Province
Zip/Postal Code	Country
Phone ( )	Extension
Fax ( )	E-mail

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883

CONTENTS

FIGURES

About This Manual

This manual describes the Cisco WAN switch user commands for System Software Release 9.2. These commands configure, monitor, and manage a network consisting of Cisco WAN switches. (For descriptions of the super user commands, refer to the manual titled *Cisco WAN Switch SuperUser Command Reference*.) Each chapter pertains to a particular aspect of using a Cisco WAN switch network. For example, Chapter 4, “Setting Up Trunks” contains the commands that apply to setting up and configuring trunks in the network (except for trunks between an MGX 8220 shelf and a BPX node). Some commands apply to more than one technology. The **addcon** command, for example, appears in many chapters. The locations of each single and multi-application command appear in Appendix A, which contains an alphabetical listing of commands with chapter page numbers.

This section discusses the objectives, audience, organization, and conventions of the *Cisco WAN Switch Command Reference* publication.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, select **Documentation**, and click **Enter the feedback form**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Objectives

This publication provides descriptions for using the Cisco WAN switch user commands in the command line interface.

Audience

The Cisco WAN switch command line interface lets you control the network at the device level. Therefore, this document helps network designers and operators to set up, manage, and troubleshoot networks.

About the Cisco WAN Switch Product Name Change

The Cisco WAN Switch products have new names. Any switch in the BPX switch family (Cisco BPX® 8620 broadband switch) is now called a Cisco BPX® 8650 broadband switch) is now called a Cisco BPX® 8600 series broadband switch. The BPX Service Node switch is now called the Cisco BPX® 8620 broadband switch. The BPX switch as a Tag switch controller is now called the Cisco BPX® 8650 broadband switch. The AXIS shelf is now called the Cisco MGX™ 8220 edge concentrator. Any switch is the IGX switch family (IGX 8, IGX 16, IGX 32 wide-area switches) is now called the Cisco IGX™ 8400 series multiband switch. The IGX 8 switch is now called the Cisco IGX™ 8400 series multiband switch. The IGX 8 switch is now called the Cisco IGX™ 8410 multiband switch. The IGX 16 is now called the Cisco IGX™ 8430 multiband switch. Cisco StrataView Plus® is now called Cisco WAN Manager® (CWM).

Organization

The chapters and appendix in this publication are as follows:

- Preface, "About This Manual," describes this manual and the layout of the command definitions.
- Chapter 1, "IGX and BPX Fundamentals" provides fundamental information on how to communicate with a node.
- Chapter 2, "Basic Commands" describes the commands that support your use of the command line interface (for example, how to clear the screen or add a user).
- Chapter 3, "Setting Up Nodes" describes the commands that let you configure a node.
- Chapter 4, "Setting Up Trunks" describes the commands that let you set up the network trunks, interface shelves, and topology.
- Chapter 5, "Setting Up Lines" describes the commands that let you set up lines to the service ports on the node.
- Chapter 6, "Voice Connections" describes the commands that relate to voice connections
- Chapter 7, "Data Connections" describes the commands that relate to serial data connections.
- Chapter 8, "Frame Relay Connections" describes the commands for Frame Relay connections.
- Chapter 9, "ATM Connections" describes the commands that relate to ATM connections.
- Chapter 10, "Optimizing Traffic Routing and Bandwidth" describes the commands that help fine-tune the use of network resources.
- Chapter 11 "Synchronizing Network Clocks," describes the commands that let you select and monitor clocks for the network.
- Chapter 12, "Managing Jobs" describes the commands for specifying and triggering a job.
- Chapter 13, "Managing the Network" describes the commands that relate to site administration of the Cisco WAN Switching network. Tasks include password and local time specification.
- Chapter 14, "Troubleshooting Commands" describes the commands that let you check alarms or test various links in the network by using loopbacks.
- Chapter 15, "Access Device Commands on a Node" describes the commands that make an access device recognized and configurable on a node. The chapter consists of command descriptions that are unique to access devices (such as the Cisco 3810) and descriptions of commands that are similar for other technologies.

- Chapter 16, "FastPAD Commands" describes the commands used to make a FastPAD recognized and configurable on a node. Some of the command descriptions in this chapter are unique to the FastPAD, however, this chapter also includes descriptions of commands that are applicable to other access devices (such as the Cisco 3810).
- Chapter 17, "VSI Commands" describes the commands used to add a VSI based controller such as the LSC (Label Switch Controller) to the BPX.
- Appendix A, "Command List" contains an alphabetical list of the commands in this manual with the chapter and page number of each.

Each chapter includes an introduction to the function of the commands and a list of the commands in that chapter. Chapters consist primarily of command descriptions. Command descriptions appear in alphabetical order. Several chapters include flow charts to illustrate how commands contribute to a larger task, such as bringing up a circuit line.

Each command description begins with the command name and a functional description. Summaries for the command and its mandatory and optional parameters follow the functional description. The summaries are in table format. The following contains a description for each part of the command summary:

Tables

Normally, the tables contain detailed information on command parameters.

Command Summary

Contains general information about a command. Information includes:

- full name
- syntax (including required parameters and optional parameters, if any)
- related commands
- attributes, such as user privilege required and whether the command can be part of a job
- example usage with screens

The syntax field indicates whether the command requires parameters or optional parameters. If required, the Parameter and Optional Parameter summaries follow the Command summary. When you enter a command at the control terminal, the system usually prompts for individual parameters. Use the Parameter and Optional Parameter summaries to determine which values to enter.

Parameters

Provides all the parameters required to execute the command (included only if noted in the syntax field of the Command Summary table).

Optional Parameters

Provides all the optional parameters that can be used when executing the command (included only if noted in the syntax field of the Command Summary table).

Conventions

This publication uses the following conventions to convey instructions and information.

Command descriptions use these conventions:

- Commands and keywords are in **boldface**.
- Arguments for which you supply values are in *italics*.
- Required command arguments are inside angle brackets (< >).
- Optional command arguments are in square brackets ([ ]).
- Alternative keywords are separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and information the system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([ ]).

Note Means you should *take note*. Notes contain important suggestions or references to materials not contained in the current body of text.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 Kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

IGX and BPX Fundamentals

A workstation, terminal, or a PC can function as a control terminal for an IGX or BPX node through an EIA/TIA-232 link or over an Ethernet TCP/IP LAN. All command input takes place at the terminal, and all displays appear on the terminal screen. Through displays that show status, alarm, or statistics, the terminal constantly provides a view of an individual node, a trunk, a connection, or the entire network.

The control terminal gives you the ability to control the network from any routing node. A remote access command is available for controlling the network from a node other than the node physically connected to the terminal. This command is the Virtual Terminal (**vt**) command. The **vt** command creates a communication channel for the operator to a remote node. After you access a node by using **vt**, you can begin executing commands at the accessed node. Most commands and tasks that you can execute at the local node are also executable at a remote node.

The WAN Manager Network Management Station provides network management capabilities for multi-node networks. WAN Manager also collects and displays statistics. For access, WAN Manager operates in LAN mode or telnet mode. (As of Release 8.0, you can no longer access a node through the serial port.) Refer to the *Cisco WAN Manager Operations manual* for more information.

Powering Up the Control Terminal

After the node receives power and correctly starts up, the terminal screen appears as shown below. If the screen is blank or does not display the initial screen, check all connections to the node, and make sure the terminal and node are receiving power. If the connections are correct, press the Delete key a few times or cycle the terminal power.

```
gamma          TRM   YourID:1        IGX 8420    9.2      Aug. 15 1998  13:47 CST















Enter User ID:
```

The User Command Screen Layout

The screen has three areas. The top line of the screen (status line) displays the node name, current user name, software revision level, date, time and time zone. If the date and time have not been configured on the node, the screen states this.

The middle part of the screen shows the information returned by the executed commands. This could be, for example, configuration or statistical information.

The bottom area of the screen displays prompts for the next command or the current command parameters. As the system receives the parameters you enter, it duplicates them above the command entry line to serve as a record of the entries. The bottom area also shows the command last entered.

All command screens eventually time out. This includes dynamically updated screens such as the display for the **dspbob** command. Furthermore, if sufficient time passes, you are logged out.

Entering a Command

This section describes how to enter a command for those who are unfamiliar with Cisco WAN switch equipment. It also describes the on-line help for the commands.

Each user command can have one or more privilege levels. Entering a particular command is possible for a user at the same or higher privilege of the command. Each definition in this manual shows the privilege or range of privileges for the command. Most commands are not case-sensitive.

When the **Next Command** prompt is at the bottom of the screen, the system is ready for a new command. Some commands do not require parameters. These usually are commands for displaying information. Display commands often have no required parameters but have one or more optional parameters for changing the scope of displayed information. Commands that require parameters usually prompt for each parameter. To abort a command for any reason, press the Delete key. More information for altering command line entries appears in the forthcoming section called "In case of a mistake."

The general syntax is *command* <*parameter*(*s*)> [*optional parameter*(*s*)]. When a command definition displays actual parameters, the required parameters appear within the arrow heads (<>). If the list of command parameters is too long, the command definition's "Syntax" field just shows "parameters," which means the parameters are available only in the parameters table for the definition. For information on the format of system resource numbering, see the section "How network trunks, lines, and channels are numbered."

Users who are not familiar with the system can use the online help feature to become familiar with the categories of commands and get syntax information on a command. Seven categories of commands exist. Figure 1-1 lists the command categories. To enter a command from the menu, do the following:

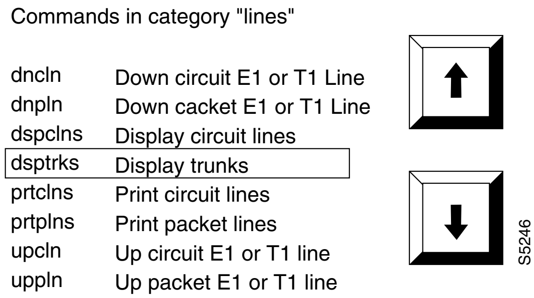
Step 1 At the **Next Command** prompt, either press the Escape key or enter the word **help** or a question mark. A list of command categories appears as in the example below.

```
gamma          TRM   YourID:1        IGX 8420    9.2       Aug. 15 1998 13:47 CST

All commands fall into one (or more) of the following categories:

Control Terminal
Configuration
Lines
Network
Connections
Cards
Alarms and Failures







This Command: ?


Use cursor keys to select category and then hit <RETURN> key:
```

Step 2 Use the up/down arrow keys to select a command category, then press Return. A listing of all the commands in that category appears. (The next example is from the "line" category of commands.)

Step 3 Use the cursor key to select the command you want to enter (**dsptrks** for example), then press the Return key. The selected command appears on the screen, and the system prompts you for any additional parameters needed to complete the command.

Figure 1-1 Entering a Command



A faster way to enter a command, using fewer keystrokes, is to enter the command on the command line, then press the Return key. The system prompts you for any additional parameters required to complete the command. The fastest way to enter a command, using the fewest keystrokes, requires that you know the command along with the necessary parameters. Enter the command name and all of the required parameters in the correct format, then press the Return key.

About Command Categories

The command category menu is listed when you press the Escape key. The commands are organized into seven categories. (These categories are not the categories used to organize this manual.) Table 1-1 lists and describes the command categories.

Table 1-1 Command Categories

Category	Description
Control Terminal	These commands let you configure your password, serial port and printer functions, use the help facility, establish virtual terminal connections, and create and edit jobs.
Configuration network and line timing	These commands configure voice and data channels, and display network configuration.
Lines	These commands activate and deactivate lines and display line status.
Network	These commands add and delete trunks, configure a node name, and display and print network status.
Connections	These commands add, delete, and display circuit (voice and data) and FastPacket data channel connections, configure network routing and connection characteristics (Frame Relay and ATM), and perform connection.
Cards	These commands activate, deactivate, and reset printed circuit cards, and display power supply status.
Alarms and Failures	These commands display, print, and clear alarms, errors, and network history. They also configure alarm thresholds.

Aborting a Command

You can abort any command by pressing the **DELETE** key [on terminals without a DELETE key, you may need to type SHIFT-BACKSPACE or some other key(s) to perform the DELETE function]. The **Next Command:** prompt appears at the bottom of the screen indicating that you can enter another command. The command you aborted appears in low intensity letters on the screen after the **Last Command:** prompt.

About Command Names

Most of the command names follow a descriptive verb and noun format. For example, the **addcon** command adds a connection, the **delcon** command deletes a connection, and the **dspcon** command displays information about a connection. Table 1-2 lists the command-related abbreviations.

Table 1-2 Command-Related Abbreviations

Format	Mnemonic	Descriptor
Verb	add	Add
	bye	Bye
	clr	Clear
	cnf	Configure
	cpy	Copy
	del	Delete
	dn	Down
	dsp	Display
	edit	Edit
	grp	Group
	help	Help
	prt	Print
	red	Redraw
	reset	Reset
	run	Run
	stop	Stop
	switch	Switch
	tst	Test
Noun	adv	Adaptive voice
	ait	AIT
	alm(s)	Alarms
	bob	Breakout box
	bus(es)	Bus(es)
	cd(s)	Card(s)
	ch	Channel
	clk	Clock
	cln(s)	Circuit line(s)

Format	Mnemonic	Descriptor
	cls	Class
	cnf	Configuration
	con(s)	Connection(s)
	congrp	Connection group
	cond	Conditioning
	cos	Class of service (COS)
Nouns (continued)	d	Data
	date	Date
	dfm	DFM
	dial	Dial
	dl	Dial type
	eia	EIA
	errs	Errors
	extlp	External loop
	fp	FastPAD
	fr	Frame Relay
	ftc	FTC
	func	Function
	gn	Gain insertion
	grp(s)	Group(s)
	ict	Interface control template
	ip	IP
	job(s)	Job(s)
	lcn	Logical connection
	ln(s)	Line(s)
	load	Load
	loclp	Local loop
	log	Log
	mc	multicast
	msg	Message
	name	Name
	nw	Network
	ospace	Open space
	parm(s)	Parameter(s)
	port	Port
	pref	Preference
	prt	Printer
	pwr	Power
	rcv	Receiver

Format	Mnemonic	Descriptor
	red	Redundant
	rmtlp	Remote loop
	rts	Routes
	scr	Screen
	seg	Segment
	sig	Signal
Nouns (continued)	slot	Slot
	snmp	SNMP
	src(s)	Source(s)
	st	Status
	stats	Statistics
	stby	Standby
	sys	System
	term	Terminal
	tmzn	Time zone
	tp	Type
	trig	Trigger
	trk(s)	Trunk(s)
	user	User
	utl	Utilization
	xmt	Transmit
	yred	Y-cable redundancy

Command Shortcuts

When you enter a command, it displays next to the **Last Command:** prompt at the bottom of the screen. To copy the command to the new command line, press the **Ctrl** and **A** keys simultaneously. To execute the previous command, you can edit the command line and then press the Return key. You can also enter an exclamation mark (**!**) followed by the first letter or letters of a previous command and press the Return key. For example, to repeat the dspcons command:

Last Command: dspcons

Next Command: **!dsp**

Press the **RETURN** key. You can use the **Display Command History** (**.**) command to display the 12 most recently executed commands:

Step 1 Type **.** (a period) and press Return. A numbered list of commands displays. In the following example, the most recently executed command is numbered 1.

```
12:
11:
10:
 9:
 8:
 7:prtscrn
 6:addcon 12.1 alpha 12.1 v
```

```
5:delcon 12.1
4:cnfport a 1200 n 8 1 x x n
3:cnftime 17 19 34
2:redscrn
1:help
```

Step 2 Type the number of the command you want to re-execute, then press the Return key. The command displays after the **Next Command:** prompt. You can press the Return key to execute the command, or you can edit the command line and then press the Return key. Whenever you end a terminal session by signing off (with the **bye** command), the command list is cleared.

In Case of a Mistake

Before you press Return, you can use control keys to edit a typed command. Table 1-3 lists the control key you can use to edit information on the command line. Not all terminals have the same key characters. If the exact key is not available, determine which key performs the function.

Table 1-3 Keys for Editing the Command Line

Function	Keys	Cursor Movement
Move the cursor	Ctrl-B	Moves the cursor left one word.
	Ctrl-F	Moves the cursor right one word.
	Ctrl-L	Moves the cursor right one character.
	Ctrl-G	Moves the cursor left one character.
	Arrows	Moves the cursor in the direction of the arrow.
Delete	Ctrl-W	Deletes a character.
	CHAR DEL	Deletes a character.
	Ctrl-H	Moves the cursor left one character and deletes that character.
	Ctrl-D	Deletes all characters from the cursor position to the end of the line.
	Ctrl-X	Deletes a line.
	BACKSPACE	Moves the cursor left one character and deletes that character.
Insert	Ctrl-I	Toggles insert mode.
	TAB	Toggles insert mode.
	CHAR INSERT	Toggles insert mode.
	Ctrl-^	Inserts line.
Miscellaneous	*	Leaves the data in this field as it is displayed and go to the next field.
	DELETE	Aborts command.
	Ctrl-M	Carriage return.
	RETURN	Carriage return.
	Ctrl-S	Stops the data flow from the node to the terminal screen.
	Ctrl-Q	Restarts the flow of data from the IGX.
	Ctrl-A	Copies the last command line.

Function	Keys	Cursor Movement
	! (..)	(The exclamation mark followed by the first characters or character of a command, brings that command back to the command line.)

Access Privileges

Access to the commands is password protected. To access the commands, type your **user ID** and **user password** at the log-in prompts. Each user is assigned a privilege level by the System Manager which determines what commands you can use. There are six user privilege levels, ranging from 1 to 6. Level 1 has access to all the commands and level 6 has access to the fewest commands. A given privilege level has access to all levels below it. For example, level 3 has access to levels 3 through 6. The privilege level for each command is part of the command summary. User ID and passwords are case-sensitive.

Commands Supported by Release 9.2

The screens and examples in this manual come network equipped with BPX and IGX nodes with both narrowband (T1 and E1) trunks and broadband (DS-3 and OC-3) ATM trunks. IGX nodes run T3, E3, T1, E1, OC-3 and IMATM services.

Note IPX nodes do not support Release 9.2.

Commands associated with optional software features function only if the option has been purchased and activated for each node in the network. Optional features are activated from the Cisco TAC. The features that fall into this category are:

- Data Frame Multiplexing
- Adaptive Voice
- Frame Relay
- Optimized Bandwidth Management (formerly ForeSight)
- Frame Relay Optimized Bandwidth Management
- Configuration Save/Restore
- Frame Relay Network to Network Interface
- Multiple Virtual Terminals (VTs)
- Configuring an IGX node as an interface shelf
- Network Expansion

Help

The system software provides a help function for commands. The help consists of a list of all commands and a display of command syntax. Entering “help” or “?” with no parameters displays a list of the seven command categories (see the list that follows). Entering “help” and a command name displays the command syntax. Entering “help” and a few letters of a command name lists all commands containing these characters. For example, “help fr” lists all commands containing the letters “fr.” You can then select a particular command from this list for help information.

- Control terminal
- Configuration
- Lines
- Network
- Connections
- Cards
- Alarms and failures

The Online Help feature of WAN Manager provides more detailed command information. Hypertext links allow you to navigate through command category lists, alphabetical indexes, and the command descriptions. Refer to the *Cisco WAN Manager Operations manual* for more information.

The Numbering of Trunks, Lines, and Channels

The information contained in this manual allows you to set up, configure, and maintain traffic on trunks and lines. Table 1-4 lists the format conventions for the names of trunks, lines, and channels.

Table 1-4 Formats of System Resource Names

Trunk, line, or channel	Description
CDP/CVM Circuit Line and NTC/NTM Trunk	The number assigned to a CDP or CVM line (CLN) or an NTC or NTM trunk (TRK) is the slot number of the BC-T1 or BC-E1 back card in the physical slot where the CLN or TRK is connected to the IGX node. In the case of redundant pairs, it is the slot associated with the primary back card.
AIT Trunk	The number assigned to the backslot of the BC-T3 or BC-E3 back card.
BPX Trunk Numbers	The number assigned to a BPX trunk (TRK) is the backslot number and port (1 - 3) of the BNI (**slot.port; example, 2.1**) card to which the T3 trunk cable is attached.
Voice Channel Numbers	A voice channel is specified by “SLOT.CH”. Sets of voice channels are specified by “SLOT.CH-CH”. The notation “SLOT” refers to the back slot number of a circuit line and “CH” refers to a channel (1-24 for T1 or 1-31 for E1). For example, “12.1” indicates channel 1 on circuit line 12, and “12.1-9” indicates channels 1-9 on circuit line 12.
Data Channel Numbers	Data channels are specified by “SLOT.PORT”, where “SLOT” refers to the slot number of a data card, and “PORT” refers to a port on that data card. For example, “9.3” specifies port 3 on the data card in slot 9. The notation “9.1-4” refers to ports 1-4 on that card. The range of port numbers is from 1 to 4 for SDI and DDS data cards. An appended “a”, for example; 11.1-5a, indicates the channels are configured to use the super-rate alternating channel feature.

Trunk, line, or channel	Description
Frame Relay channel numbers (local addressing)	In the local addressing convention, Frame Relay channels are specified by “SLOT.PORT.DLCI”, where “SLOT” refers to the slot number of an FRP, “PORT” refers to a port on the FRP card, and “DLCI” is the local data link connection identifier. The range of port numbers is from 1 to 4. For example, the following **addcon** command at node alpha: addcon 6.1.101 beta 4.1.102 2 The command adds a connection between alpha and beta. The user device at alpha refers to this connection using the local DLCI of 101. The user device at beta refers to this connection using the local DLCI of 102. The DLCIs have local significance only. With local addressing, the same DLCI can be used again, but not for more than one destination from the same port. For example, the following adds another connection from alpha port 6.1: addcon 6.1.100 gamma 6.2.102 2 In this case, a DLCI of 100 is used at alpha. A DLCI of 102 can be used at gamma as well as at beta, because the DLCIs have only local significance.
Frame Relay channel numbers (Global Addressing)	In the global addressing, the format for Frame Relay channel specification is “SLOT.PORT.DLCI.” However, each FRP or FRM port (and associated user device) is identified by a unique DLCI. No two ports in the network can have the same DLCI. For example, alpha port 6.1, gamma port 6.2, and beta port 4.1 could be assigned unique DLCIs of 79, 80, and 81 when adding connections, as in the following example: addcon 6.1.80 gamma 6.2.79 2 (at alpha) addcon 6.1.81 beta 4.1.79 1 (at alpha) addcon 4.1.80 gamma 6.2.81 5 (at beta) The user device at alpha refers to the connection between alpha and gamma, using the DLCI of 80 assigned to gamma. The user device at gamma refers to this connection using the DLCI of 79 assigned to alpha. The user device at alpha refers to the connection between alpha and beta using the DLCI of 81 assigned to beta. The user device at beta refers to this connection using the DLCI of 79 assigned to alpha. The user device at beta refers to the connection between beta and gamma using the DLCI of 80 assigned to gamma. The user device at gamma refers to this connection using the DLCI of 81 assigned to beta. For information on adding Frame Relay connections through a FastPAD, refer to the command descriptions in the online version of the 8.2 *FastPAD User’s Guide*.

Basic Commands

The *user interface* commands let you access an IGX or BPX system through the control terminal. These commands provide help on how to use the commands, display the twelve most recent commands entered into the system, connect to another node, and sign you off. These commands also give you a way to clear, print, or redraw the screen. These commands are all simple to use and have no command parameters except the virtual terminal command (**vt**), in which you must specify the node name, and the help commands, in which you must enter a command character string.

Getting Help

Entering **help** or **?** displays command information. The **help** command gives you access to a general help menu or to information on a specific command. To access the general help menu, enter either **help** or **?**. Either of these commands displays the command category menu on the screen and prompts you to make a selection. Use the arrow keys to move the cursor to the correct category, then press the Return key.

For information on a specific command, enter **help** or **?** followed by a command name. For example, enter the following for information on adding a trunk:

help addtrk

Press Return to display the information. Entering **help** or **?** followed by a character string displays all those commands containing the character string. For example, for a list of all commands that contain the string “fr,” enter the following:

? fr

Signing On

Signing on to the system is a two-step process requiring you to enter both a User ID and a password. The system administrator can provide a User ID and password for the network. Only the system administrator can assign and change User IDs. Once a password is assigned, you can change your own password. For security reasons, users should periodically change their passwords. User ID and passwords are case-sensitive.

When the following prompt appears at the bottom of the initial screen, the system is ready for you to log in:

Enter User ID:

Entering a User ID and password gives access at a particular level of user privilege. (Each command has one or more levels of associated user privilege.) For information on access privileges and passwords, refer to Chapter 13, “Managing the Network”. User IDs can have up to twelve (12) characters. At the prompt, enter the User ID. The system responds with the following prompt:

Enter Password:

When you initially sign on, enter the password. (The password does not appear on the screen.) Upon receiving the correct User ID and password, the log-in is recorded by the event log, and the screen displays the following prompt:

Next Command:

The system is ready to receive commands.

Logging Out

To log out, enter **bye**. When the terminal connection is local, this returns you to the initial screen. To log out completely from a remote (virtual terminal) session, enter **bye** twice.

Clearing and Redrawing the Screen

Use the Clear Terminal Screen (**clrscrn**) to clear the screen. Use the Redraw Terminal Screen (**redscrn**) command to clear and redraw the screen. The **clrscrn** command clears any information displayed in the top portion of the screen. This information could consist of status displays on lines and connections or Help text. To clear the screen, enter **clrscrn**.

The **redscrn** command redraws the screen and updates the status lines. To make sure the status lines have been updated, enter the **redscrn** command. For example, to redraw a screen’s display with the latest statistics before printing the screen, enter **redscrn**.

Printing Screens

The Print Terminal Screen (**prtscrn**) command prints the current screen display. Verify that the node printer is correctly configured before attempting to print a screen. Upon entering the **prtscrn** command, the screen display goes to either a local or remote printer. To print all the information in a screen, enter **prtscrn**.

Accessing Physically Remote Nodes

The Make Virtual Terminal Connection (**vt**) command establishes a virtual terminal connection to a remote node. Once the connection is established, entering and executing commands takes place as if the terminal were the local terminal on the remote node. The **vt** command lets network configuration take place from a central site. The only command that cannot run remotely is the **vt** command itself.

The privilege of user commands available through a **vt** connection is the same as that of the user who logged into a node with **vt**. To establish a virtual terminal connection with a remote node, enter **vt** and the name of the node name. For example, to **vt** to node “alpha,” enter:

vt alpha

The words Virtual Terminal appear on the screen at the lower left corner to indicate that a virtual terminal connection exists. The remote node name appears at the upper left corner of the screen. To terminate the virtual terminal connection and return to your local terminal connection, enter the **bye** command.

The **bye** command has two separate functions:

- If the terminal connection is local, **bye** logs you off the system.
- If the connection is remote (a vt connection), the **bye** command breaks the remote connection and returns the terminal to a local connection.

To log out of the system during a remote (vt) session, enter the **bye** command twice. Note that after a default period of four minutes of inactivity, the vt session automatically ends, and the connection reverts back to being local. The timeout is configurable.

If the multiple **vt** feature has been purchased, multiple users can log into a node with the **vt** command. Cisco personnel must activate this feature.

List of Basic Commands

Table 2-1 lists the commands discussed in the previous sections. Descriptions of these commands make up the rest of this chapter.

Table 2-1 List of Basic Commands

Mnemonic	Description	Page
.	Display command history	2-3
help or **?**	Help	2-5
bye	End user session	2-8
clrscrn	Clear screen	2-10
prtscrn	Print screen	2-11
redscrn	Redraw screen	2-12
vt	Make a virtual terminal connection	2-13

. (a period)

Displays the twelve (12) most recently used commands. To re-use one of these commands, enter the associated number. The command appears on the command entry line, where you can re-enter or re-execute a command. Editing in this case means back-spacing through the command's arguments and typing in a new value or backspacing without typing a new value to restart the command at the cursor position.

Full Name

Display command history

Syntax

. (A period)

Related Commands

None

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

. (A period)

Description

Display the command history.

System Response

```
gamma          TRM   YourID:1        IGX 8420     9.2    Aug. 15 1998 13:47 CST

Command history

12: dspcons
11: vt beta
10: dspcons
9: addcon 6.4 alpha 6.4 (.6
8: addcon 8.1.200 alpha 9.1.300 1
7: upfrport 8.1.200
6: dntrk 14
5: uptrk addjob
4: addjob
3: dspjobs
2: addjob
1: dspjobs


Last Command: .


Next Command:
```

help or ?

Displays a help menu. This command accesses the help routine in the system software. It provides:

- A short description of the command
- An indication of whether the command can be used in a job
- The command syntax

A more extensive, menu-driven, on-line help function exists within the WAN Manager NMS. Consult the *Cisco WAN Manager Operations Guide* for a complete description of the on-line help.

The ways to request help on commands are:

- Entering **`help`** or **`?`** without an argument lists the command categories. Selecting one of these categories (using arrow keys and Return) displays all the commands in that category. You can select commands in this list by using arrow keys then the Return key.
- Entering a command name displays help for that particular command.
- Entering a partial command name lists all commands that contain that character string. For example, **`fr`** indicates all commands (such as **cnffrport**) that contain "fr." You select a command in the list by using arrow keys to scroll to the command then pressing Return.

Full Name

Help command

Syntax

? or **help** [command name | character string]

Related Commands

None

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

help

Description

Display the help menu. (Without an argument, the help command shows the command categories.)

System Response

```
switchnow TN    SuperUser       BPX 15    9.1 Oct. 1 1997  14:14 GMT

All commands fall into one (or more) of the following categories:

Control Terminal
Configuration
Lines
Network
Connections
Cards
Alarms and Failures
Diagnostics
Debug


This Command: help


Use cursor keys to select category and then hit the <RETURN> key:
```

Example 2

help dspbxmsloterrs

Description

Display the syntax and other information for Display BXM Slot Errors (**dspbxmsloterrs**).

System Response

```
switchwhat TN    SuperUser       BPX 15    9.1 Oct. 1 1997  14:16 GMT

dspbxmsloterrs   - Display BXM Slot Errors
Cannot be included in Jobs.
Usage: dspbxmsloterrs [slot]







Last Command: help dspbxmsloterrs


Next Command:
```

Example 3

help fr

Display all commands that contain the string “fr.” (These are the Frame Relay commands.) A list of all commands containing the letters “fr” appears on screen. Scroll to a command then press Return to display the related help screen.

Table 2-2 help – Optional Parameter

Parameter	Description
command	Specifies a command.
string	Specifies a character string as a search argument.

bye

Ends a local or remote terminal connection. With a local terminal connection, the **bye** command logs out the user. If a local terminal is inactive for a (default) period of 20 minutes, the connection is automatically broken. This is the equivalent of entering the **bye** command. With a remote terminal connection (**vt**), the **bye** command returns the terminal to the local node. After a (default) period of four minutes of inactivity, a remote terminal connection is automatically returned to a local connection. This is equivalent to entering the **bye** command.

Full Name

End user session

Syntax

bye

Related Commands

vt

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	No

Example 1

bye

Description

End a current session from a local node. The local connection ends, and the initial sign-on prompt appears on the screen.

System Response

```
gamma          TRM   YourID:1        IGX 8420    9.2   Aug. 15 1998 13:47 CST









Enter User ID:
```

clrscrn

Clears the terminal screen.

Full Name

Clear terminal screen

Syntax

clrscrn

Related Commands

redscrn, prtscrn

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	No

Example 1

clrscrn

Description

Clear the screen.

System Response

```
pubsigx1       TN    SuperUser       IGX 8420    9.2    July 15 1998  22:49 GMT









Last Command: clrscrn


Next Command:
```

prtscrn

Prints the information on the screen at the time the command is entered.

Full Name

Print terminal screen

Syntax

prtscrn

Related Commands

clrscrn, redscrn

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

prtscrn

Description

Send the information on the screen to the printer.

System Response

All information on the terminal screen is printed. If printing is successful, no status message appears. If the printer is unavailable, an appropriate status message appears.

redscrn

Redraws the screen. This command can be useful for communication that involves a modem. If data has become corrupted and caused erroneous characters on the terminal screen, **redscrn** clears them.

Full Name

Redraw the terminal screen

Syntax

redscrn

Related Commands

clrscrn, prtscrn

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	No

Example 1

redscrn

Description

Clear the terminal screen and redraw the valid screen information.

System Response

The current screen reappears without erroneous characters.

vt

Establishes a virtual terminal connection to a remote node. A virtual terminal connection has the following properties:

- On the remote node, any command except the **vt** command can be executed.
- Multiple **vt** sessions is a purchasable option. With it, more than one user can **vt** to a node.
- During a virtual terminal session, jobs can be executed at any time.

During a **vt** session, the remote node name and date flash on the local terminal screen, and "Virtual Terminal" appears in the lower left corner. The **bye** command terminates a virtual terminal session and returns the terminal to local usage. After a default timeout of four minutes of inactivity, a **vt** connection automatically reverts to a local connection. This timeout is the equivalent of using the **bye** command.

Full Name

Make a virtual connection

Syntax

vt <nodename>

Related Commands

bye

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	No

Example 1

vt sw115

Description

Establish a virtual terminal connection to the switch named "sw115."

System Response

```
sw115          VT    SuperUser       BPX 15    9.1       July 15 1997 16:59 PDT










Last Command:


Next Command:

Virtual Terminal      CD
```

Table 2-3 vt – Parameter

Parameter	Description
node name	Specifies the name of the remote node for the virtual terminal connection. If the specified node name is not valid, the returned message states that the "Node is unknown" and prompts for the correct node name. Also, the main area of the screen names the recognized nodes in the network to help determine the correct name.

Setting Up Nodes

This chapter describes the commands that let you set up an IGX or BPX node. (You must set up each node before you build the network.) This chapter also describes how to:

- Configure a node name and time zone.
- Add and remove a network node.
- Add and remove an interface shelf in a tiered network.
- View a node's configuration.
- Specify Y-cable redundancy for cards in the node.
- Start a window session to an external device or specify an interface to an attached terminal.
- Sending Abit Notification on ILMI/LMI Using Configurable Timer

Naming a Node

Before you can add a node to the network, you need to assign a unique node name. All nodes initially have the default name **NODENAME**. The node name consists of one to eight printable characters (beginning with a letter), and cannot contain spaces. If you are naming the node after a city or place that contains more than eight characters, you will have to abbreviate the name to create a valid network node name. The name must be unique across the network. For example, to assign the node the name of **alpha**, enter:

cnfname alpha

To change a node name, do the following:

Step 1 Sign on to (or establish a virtual terminal connection with) the node whose name you want to change.

Step 2 Change the name of the node using the **cnfname** command.

The name of the node you are connected to changes to the new name. This new name will be distributed automatically to other nodes in the network.

Configuring the Time Zone

Each node must have a *time zone*. To set the time zone for the node to Greenwich Mean Time, for example, enter:

cnftmzn GMT

Removing a Trunk from the Network

Since Release 7.0, “packet lines” have been referred to as *trunks*. Use the letters “**trk**” in all commands referring to packet lines. To remove a trunk from the network, do the following.

Step 1 Sign on to (or establish a virtual terminal connection with) the node.

Step 2 Delete all packet (trunk) lines attached to the node using the **deltrk** command. For example, to delete line 5, enter: **deltrk 5**.

Adding an Interface Shelf

An *interface shelf* is a non-routing device that drives ATM cells to and from a BPX or IGX routing hub in a tiered network. (An interface shelf is also sometimes referred to as a *feeder shelf*.) An interface shelf can be either an IGX or MGX 8850 node configured as an interface shelf, or an MGX 8220 interface shelf.

Because tiered network capability is a purchased option, for an IGX node to serve as an interface shelf, personnel in the Technical Assistance Center (TAC) must first configure it for that purpose. Furthermore, you must use the **cnftrk** command to configure an interface shelf to use STI cell headers and BPX Addressing Mode (BAM). Before you can add an MGX 8220 shelf to a tiered network, the shelf must be an available resource in the network. (For instructions on how to bring up an MGX 8220 shelf, see the MGX 8220 documentation.)

To add an interface shelf, use **addshelf**. See Figure 3-7 for an illustration of the command sequence for setting up an interface shelf. To delete a feeder shelf, use **delshelf**. To view conditions on a feeder trunk, use **dspnode**. (Note that **addshelf** and **addtrk** are mutually exclusive commands.

IGX/AF is the designation of an IGX node serving as an interface shelf. Display commands such as **dspnw** and **dspnode** display these designations. The **dspnode** command identifies the hub and feeder nodes and shows the alarm status. The designation for an MGX 8220 shelf serving as an interface shelf is AXIS. The designation for an MGX 8850 serving as an interface shelf is AAL5. The designation for an SES (Service Expansion Shelf) shelf serving as an interface shelf is also AAL5.

The following procedure applies when adding any supported feeder to an IGX routing node. To configure an SES (Service Expansion Shelf) as a feeder to an IGX 8400 routing hub:

- Use **uptrk** to enable the feeder trunk on the port.
- Use **cnftrk** to configure the feeder trunk.
- Use **addshelf** to add the feeder to the database and to enable the LMI signalling channel and the IP relay.
- Use **addcon** to add connections terminating at the UXM/UXM-E feeder endpoints.
- Use **delshelf** to delete the feeder from the database and to disable the LMI signalling channel and the IP relay.

Specifying Card Redundancy

You can set up port redundancy by installing two identical front and back card sets, connecting them with a Y-cable on each paired port, then specifying redundancy with the **addyred** command. Redundancy applies to the entire card and is not port or line-specific. The commands that apply to Y-cable redundancy are:

- **addyred**
- **delyred**
- **dspyred**
- **prtyred**
- **switchyred**

During normal operation, the primary set is "active" and carrying traffic, while the secondary set is in "standby." The primary set configuration is the configuration for both the primary and redundant set. If you reset the primary cards or the primary card set becomes inactive for another reason, the secondary card set becomes active.

IGX card sets can consist of the following:

- HDM front card and SDI back card
- LDM front card and LDI back card
- FRM front card and an FRI back card
- UFM front card and a UFI back card
- FTM front card and an FTI back card
- UVM front card and a BC-UVI-2E1EC or BC-UVI-2T1EC back card
- CVM front card and a BC-T1 or BC-E1 back card
- NTM front card and a BC-E1 or BC-T1 back card
- BTM front card and a BC-E1, AIT-T3, or AIT-E3 back card
- ALM and a BC-UAI back card
- UXM and an MMF, SMF OC-3, T3/E3, T1/E1or IMA back card

BPX card sets may consist of the following:

- BCC front card
- BNI front card and T3, E3, or OC-3 back card
- BXM front card and MMF, SMF, or SMFLR back card
- BME front card and MMF, SMF, or SMFLR back card
- ASI front card and T3, E3, or OC-3/STM-1 back card

The following requirements apply to redundant card sets:

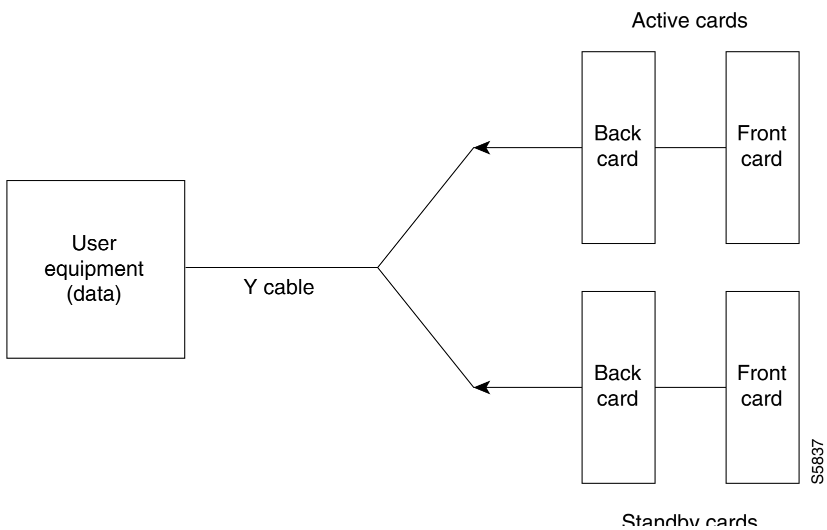
- The primary and secondary card sets must be identical.
- Secondary card sets must not be already active.
- Neither the primary nor secondary card set may already be part of a redundant card set pair.
- If an active card fails, is downed, or removed from the backplane, data automatically goes through the secondary set.

- All service cards on the IGX and BPX nodes support Y-cable redundancy. (The trunk cards also support trunk redundancy. See Chapter 4, “Setting Up Trunks” for a description.)

Figure 3-1 illustrates the typical Y-cable connection of primary and secondary card sets. The single end of a Y-cable (or base of the “Y”) goes to the user equipment. One of the two connectors at the split end goes to the primary back card, and the other connector goes to the secondary back card.

Switching to the standby card occurs only if the secondary card set is in a “Standby” or a “Standby-T” state (but not “Failed”). See the **dspcds** definition for information on these states.

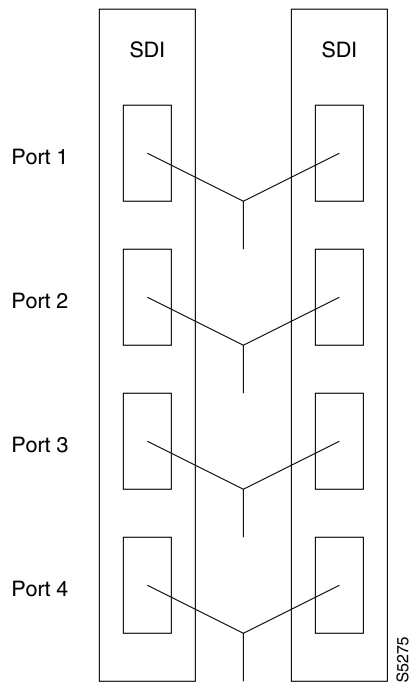
Figure 3-1 Y-Cable Connection



Note Terminating connections is possible at only a primary slot and not at a secondary slot. See the **addcon** description.

On multiport card sets, each primary port is connected by a Y-cable to a secondary (redundant) port. Port 1 of the primary card set must be paired to port 1 of the secondary card set, and so on. Figure 3-2 illustrates the cabling for a multiport card set.

Figure 3-2 Y-Cables on Multiple Ports



If the secondary card set becomes active, the primary card set goes into the standby state. For the primary card set to serve as a backup, it must be a complete set and not have failed status.

You can execute **addyred** even if the primary and secondary slots are empty. If cards reside in the primary and secondary slots, the system checks for card compatibility. Two types of incompatibility can occur: back card and jumper or cable. (On SDI, FRI, and FTI cards, jumpers determine whether a port is configured as DCE or DTE. On LDI cards, either a DCE or DTE adapter cable connects to the LDI port, as applicable).

If incompatibilities exist, the message "Y-Cable Conflict" appears on screen. Specific conflicts are listed in reverse video in the Y-Cable Redundancy screen. See the **dspyred** description for details. Redundancy on V.35 versions of the SDI and FRI cards requires special redundant jumpers. Always use the applicable Y-Cable Redundancy kit for a card.

Card Redundancy for Virtual Trunking

Y-Cable redundancy is supported for both the UXM and BXM trunk cards at the edge of the ATM cloud.

Controlling External Devices

If your system is configured to control an external device*,* such as a multiplexer, you can establish a **window** session to it from the control terminal. While in a **window** session, any characters you type at the control terminal go to the external device for processing. Any characters generated by the external device appear on the control terminal screen.

The Window to External Device (**window**) command establishes a *window* session. You can use this command only if the external device connects to the local node. You can, however, enter the **window** command during a virtual terminal session so that you have a window session with any external device in the network. To start a window session, use the Virtual Terminal (**vt**) command to access the node cabled to the device, then invoke the **window** command. Before starting a window session, you must have configured the port and the port function with **cnfterm** and **cnftermfunc**. In addition, you must know whether the external window device is cabled to a node's Control Terminal (EIA/TIA-232) port or Aux Port (EIA/TIA-232) port. The format for the **window** command is:

window [a | c]

Enter an **a** if the external device is attached to the node's Aux Port or **c** if the device is attached to the node's Control Terminal port. The default for this parameter is Aux Port. To establish a **window** session with an external device attached to a node's Control Terminal port, enter:

window c

The system responds by redrawing the terminal screen. You can now enter commands and send data to the external device as if you were locally connected to its Control Terminal port. While in the **window** session, only commands used to control the external device are recognized. IGX/BPX commands are not recognized. You might notice a slight transfer delay in transmission, due to the IGX/BPX bundling of characters before transmitting them. Transfers are delayed until the transfer buffer is filled, or until the keyboard has been inactive for over 50 milliseconds.

To end a **window** session, enter an escape sequence. Escape sequences are one to eight characters in length and are configured with the Configure Terminal Port Function (**cnftermfunc**) command. For example, if you have specified "signoff" as the escape sequence in the Configure Terminal Port Function, enter the following to end the **window** session:

signoff

The default escape sequence is:

^^ (SHIFT 66)

If this escape sequence does not work and you do not know the configured escape sequence, leave the keyboard idle for four minutes. After four minutes, the system terminates the window session.

Command Sequences for Setting Up Nodes

The sequences in Figure 3-3, Figure 3-4, Figure 3-5, Figure 3-6, and Figure 3-7 show the commands you execute to do the following node-related tasks:

- Set up a node
- View information about the presence of the cards and system power
- Configure an interface for a control terminal that is connected to the node
- Remove a node from a network
- Add an interface shelf

Figure 3-3 Setting Up Nodes

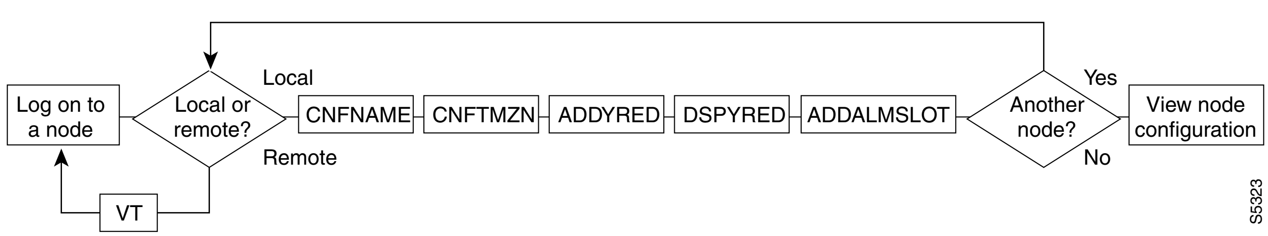


Figure 3-4 Viewing the Node Configuration

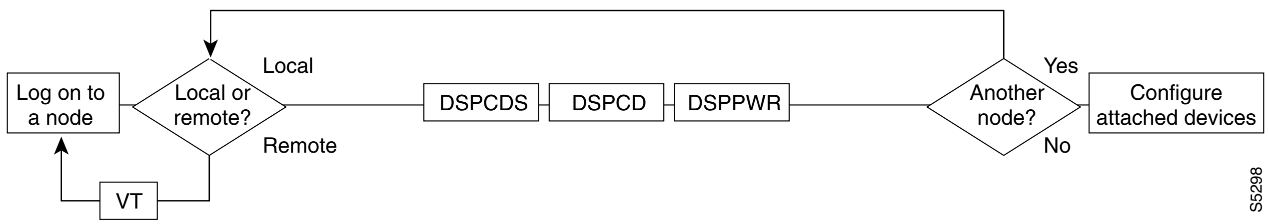


Figure 3-5 Configuring the Node Interface for a Local Control Terminal

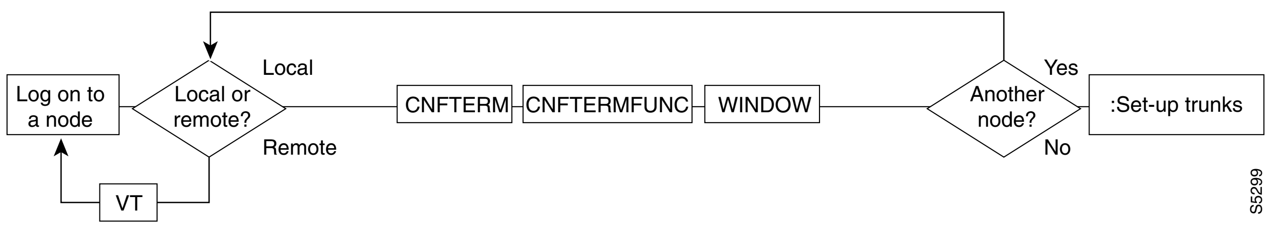


Figure 3-6 Removing a Node From the Network

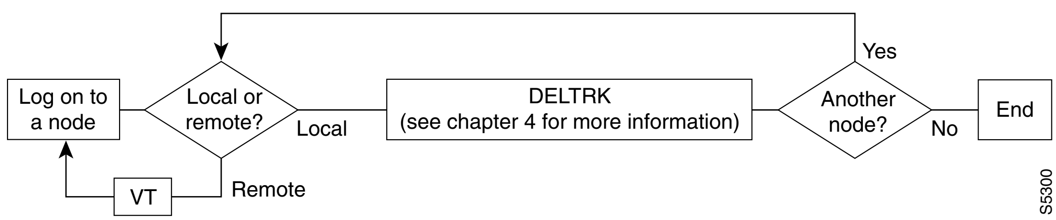
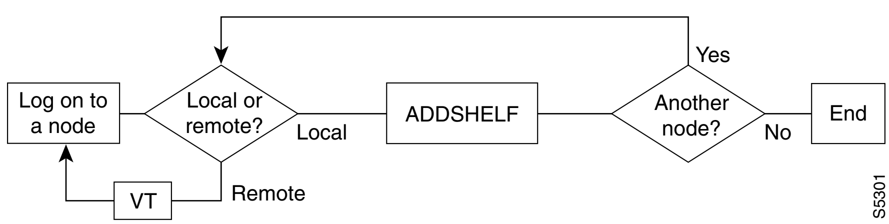


Figure 3-7 Add an Interface Shelf to the Network



Sending Abit Notification on ILMI/LMI Using Configurable Timer

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature provides a mechanism to send Abit = 0 status change over the LMI interface or send ILMI traps over the ILMI interface after the connections are derouted a certain amount of time. You can configure this time period by setting some **cnfnodeparm** parameters. This configurable time approach provides you with the flexibility to synchronize the operation of the primary network and backup utilities, such as dialed backup over the ISDN or PSTN network. This feature is supported on both the BPX and IGX platforms.

Definitions of Terms Related to Abit Notification using Configurable Timer Feature in Release 9.2

These brief definitions are relevant to the Early Abit Notifications on ILMI/LMI Interface using Configurable Timer feature:

CPE
Customer premise equipment.

ILMI
Integrated Local Management Interface provides a means for configuration, status and control information between two ATM entities.

LMI
Logical Management Interface provides a protocol to monitor the status of permanent virtual connections between two communication devices.

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature allows Abit notifications to be sent over the LMI/ILMI interface if a connection cannot be rerouted after a user-specified time. Abit = 0 will not be sent if the connection is rerouted successfully during that time.

Purpose of Early Abit Notification on ILMI/LMI Using Configurable Timer Feature

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature provides the user flexibility to configure the time when the node will start sending out Abit = 0 after a connection becomes derouted. This allows the CPE to take appropriate actions such as initiating the dialed backup process if the deroute process has not finished during a certain period of time.

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature is an enhancement to the Send Abit on Deroute feature provided in Release 9.1.07 for the BPX. To minimize the risk in deploying this feature, and to continue to support the Send Abit on Deroute feature, which was developed in Release 9.1.07 for BPX, the feature has the following guidelines:

1. You can enable this feature by using the **cnfnodeparm** command. You can specify that Abit Notification be sent either on deroute, or a user-configurable time after deroute. This feature can also be turned off. It is recommended that this feature be set the same on all nodes. Otherwise, the Abit behavior can be different on different nodes.
2. If this feature is turned off, switch software behaves the same as in previous releases. Existing functionality continues to function in a mixed release network (releases 8.4, 8.5, or 9.1 IGX or BPX network).
3. The Early Abit Notification on ILMI/LMI Using Configurable Timer feature is provided on both BPX and IGX platforms.
4. If the **cnfnodeparm** Abit Timer Multiplier M parameter is set to 0, then switch software behaves the same way as in Release 9.1.07 (which supported the Send Abit on Deroute feature).

Environment Required to use the Abit Notification Using Configurable Timer Feature

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature is supported on IGX and BPX switch software. No new hardware or firmware is required on line cards or feeder trunk cards.

Configuration of Abit Notification Feature

You can enable the Early Abit Notification on ILMI/LMI Using Configurable Timer feature on both IGX and BPX by using **cnfnodeparm** command parameters Send Abit Early, Abit Timer Multiplier M, and Abit Timer Granularity N.

Compatibility

A Release 9.2 IGX or BPX node using this feature is compatible with Release 8.4 and Release 8.5 nodes or Release 9.1 IGX and BPX nodes so that all existing connection related functions will continue to work. However, the timing in sending out the Abit notifications at both ends of connections may behave differently, depending on how this feature is configured.

Overview of Abit Notification Feature

The time to reroute connections varies depending on different parameters, such as the number of connections to reroute, reroute bundle size, and so on. It is important to notify the CPE if a connection is derouted and fails to transport user data after a specified time interval. However, it is desirable not to send out Abit = 0 and then Abit = 1 when a connection is derouted and rerouted quickly, because such notifications may trigger the CPE backup facilities, which is a costly process and may cause fluctuations in an otherwise stable system. The configurable time interval is a direct solution to these problems.

Function of the Early Abit Notification on ILMI/LMI Using Configurable Timer Feature

The Early Abit Notification on ILMI/LMI Using Configurable Timer feature allows you to specify the time interval after which to start sending out Abit = 0 if a connection fails to reroute and is in the derouted state too long. To avoid having an adverse performance impact on the system, no precise timer is kept for each connection. Instead, all connections derouted during a certain time period go to the same bucket.

This time period is referred to as N, which defines the granularity of the timers, and is specified by the value of the **cnfnodeparm** Abit Timer Granularity N parameter. Another parameter is the time to wait before Abit = 0 is sent out if the connection is in a derouted state. This parameter is called X. A connection that is derouted at a period of time between 0 and N will send out Abit = 0 at a time between X and X + N, if the connection continues to be in a derouted state. In cases where there are many Abit status changes to report to CPE, the last Abit updates may be delayed much longer because Abit updates process about 47 connections per second.

To make a compromise between performance and the granularity of timers, N can be configured to be from 3 to 255 seconds; the bigger the value of N, the better the system performance will be. The other parameter, X, is set to be M*N, where M can be configured to be from 0 to 100. The default value for N is 3sec. Default value for M (Abit Timer Multiplier M parameter) is 0, meaning Abit = 0 is sent out on deroute.

It is recommended that X (value of Abit Timer Multiplier M * the value of the Abit Timer Granularity N) be set such that when a trunk fails, the connections are given sufficient time to reroute successfully, avoiding the need to send out Abit = 0.

The change in the Abit behavior is completely local to the node and is applicable to the master and slave ends of connections when the connections are derouted. When only one of the nodes connected by a connection has this feature turned on, the timing in sending the Abit notification at one end of the connection may be drastically different from the other end. Therefore it is recommended that the Early Abit Notification on ILMI/LMI Using Configurable Timer feature be configured the same on all nodes. Also, because timers on nodes are not in sync, there is a slight time difference (3 seconds maximum) in sending Abit from the two ends of a connection, even if the **cnfnodeparm** parameter settings on the nodes are the same.

Note A pre-Release 9.1.07 node or Release 9.1.07 node with the Send Abit on Deroute feature (**cnfnodeparm** Send Abit immediately parameter) turned off behaves the same way as a Release 9.2 node with the Early Abit Notification on ILMI/LMI Using Configurable Timer feature disabled. A Release 9.1.07 node with the **cnfnodeparm** Send Abit immediately parameter set to yes behaves the same way as a Release 9.2 node with the Send Abit Early parameter set to yes and the Abit Timer Multiplier M set to 0.

If the value of X (value of Abit Timer Multiplier M * value of Abit Timer Granularity N) is set to be smaller than the normal time to reroute connections when a trunk fails, the time it takes to finish rerouting them may take longer. This can happen for line cards and feeder trunks, which have the LMI/ILMI protocol running on those cards, such as BXM on BPX and Frame Relay cards on IGX. Note that it takes time for those cards to process the Abit status information for each connection coming from the controller card.

Caution To follow the general Release 9.2 interoperability guideline, it is not recommended that the Early Abit Notification on ILMI/LMI Using Configurable Timer feature be used when the standby control processor is in a locked state.

There is no impact on control processor switchover or trunk card redundancy switchover because connections are not rerouted.

Using the Early Abit Notification on ILMI/LMI Using Configurable Timer Feature

In releases previous to Release 9.1.07, when connections are derouted, the CPE does not receive Abit notifications. In Release 9.1.07 on BPX, the Send Abit on Deroute feature was developed, which allowed the Abit = 0 to be sent immediately when a connection is derouted. (This was specified by the **cnfnodeparm** parameter Send Abit immediately parameter.) To further enhance the Send Abit on Deroute feature in Release 9.1.07, the Early Abit Notification on ILMI/LMI Using Configurable Timer feature has been implemented in Release 9.2 to allow the network administrator to configure the node as to when Abit = 0 is sent out if a connection is derouted and not rerouted quickly. This feature allows you to specify when Abit notifications will be sent at Frame Relay and ATM ports, and at feeder trunks in a tiered network architecture that supports the ILMI/LMI interface. In a tiered network, the Abit information is used by the feeder nodes such as MGX 8220 (AXIS) which then relays the Abit information to the CPE.

The status update messages are throttled at the rate of one message per second. Each message can be used to specify the conditioning information on a maximum of 47 connections. It may take on the order of minutes for the ILMI/LMI manager to process the Abit status when there is a large number of connections.

Performance of Sending Abit Notification using Configurable Timer Feature

There are two factors in performance: system performance and reroute time. System performance is affected by the value of the time interval. In a network where connections are normally derouted and rerouted quickly before the bucket timer expires, the performance impact is very small. Only when the timer expires, then looping through all LCONs and sending update messages will take up some CPU time which is estimated to be smaller than 1 percent.

Reroute time is not affected if LMI/ILMI is running on the controller card. When the protocol is implemented on the line cards and feeder trunk cards, some additional Abit status communication between them and controller card may delay the reroute process.

Specifically, on the BPX, if the BXM runs LMI/ILMI, the BCC has to send Abit update to the card. These messages will be throttled. When this happens, we estimate the time to reroute all 12K connections increases no more than 5per cent.

For the IGX, enabling the Sending Abit Notification using Configurable Timer feature may impact performance if many connections end at Frame Relay cards. This is due to the restricted format of interface between NPM and Frame Relay cards.

RAS (Reliability, Availability, and Serviceability)

Together with the CPE equipment that has dialed backup capability, this feature increases the availability of the services between the CPEs.

Interoperability with Previous Release of Switch Software

This feature is blocked until all nodes are running Release 9.2. A Release 9.2 node with or without this feature being turned on can interwork with other 8.4 or 8.5 nodes or Release 9.1 nodes with all existing connection management functionality.

Summary of Commands

Table 3-1 shows the command name and starting page for the description of each node command.

Table 3-1 Commands for Setting Up a Node

Mnemonic	Description	Page
addalmslot	Add an alarm slot	3-14
addcdred	Add card redundancy for SONET APS 1+1 across two BXM cards	3-16
addctrlr	Add a PNNI VSI controller to a BPX node through an AAL5 interface shelf	3-16
addshelf	Add a trunk between an IGX or BPX core switch shelf and an interface shelf	3-16
addyred	Add Y-cable redundancy	3-35
cnfasm	Configure ASM card	3-38
cnfdate	Configure date	3-41
cnffunc	Configure system function	3-41
cnfname	Configure node name	3-46
cnfprt	Configure printing functions	3-48
cnfterm	Configure terminal port	3-50
cnftime	Configure time	3-52
cnftmzn	Configure time zone	3-54
delalmslot	Delete alarm slot	3-56
delshelf	Delete a trunk between a IGX/BPX core switch shelf and interface shelf	3-60
delcdred	Delete Y-cable redundancy (disables card redundancy (for SONET Automatic Protection Switching feature)	3-58
delyred	Delete Y-cable redundancy	3-63
dspasm	Display ASM card configuration	3-63
dspcd	Display card	3-65
dspcds	Display cards	3-77
dsplancnf	Display LAN configuration	3-83
dspctrlrs	Display all PNNI VSI controllers on a BPX node	
dsplmistats	Display LMI Statistics	3-85
dspnds	Display nodes	3-87
dspnode	Display summary information about interface shelves	3-89
dsptermcnf	Display terminal configuration	3-96
dsptermfunc	Display terminal port configuration	3-98
dspprtcnf	Display print configuration	3-100
dsppwr	Display power	3-102
dspcdred	Display Y-cable redundancy (displays card redundancy for SONET Automatic Protection Switching)	3-75
dspyred	Display Y-cable redundancy	3-104

Mnemonic	Description	Page
prtcdred	Print card redundancy (prints Y cable redundancy for SONET Automatic Protection Switching)	3-106
prtyred	Print Y-cable redundancy	3-107
upcd	Up card	3-109
window	Window to external device	3-117

addalmslot

Enables the MAJOR and MINOR alarm indicators on an Alarm Relay Card (ARC) or Alarm Relay Module (ARM) front card. It also configures the slot to provide external alarms from the Alarm Relay Interface (ARI) back card. You should use this command at each node equipped to provide external alarm indications to the customer alarm reporting system. The slot specified for the ARC or ARM may be any shelf slot, but is usually the slot farthest to the right.

Upon executing the command, the system places the alarm card set in the active state and displays the current alarm status.

Full Name

Add alarm slot.

Syntax

addalmslot <slot number>

Related Commands

delalmslot, **dspalms**

Attributes

Privilege	1–4
Jobs	NO
Log	Yes
Node	IGX
Lock	Yes

Example 1

`addalmslot` 16

Description

Enable alarm reporting from slot 16 in a node. (The system then displays alarm status.)

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2      Aug. 3 1998 14:27 MST

Alarm summary   (Configured alarm slots: 16)
Connections Failed:       None
Groups Failed:            None
PLN Alarms:               1 Major
CLN Alarms:               None
Cards Failed:             1
Missing Cards:            None
Remote Node Alarms:       1 Major
Remote Domain Alarms:     None




Last Command: addalmslot 16


Next Command:
```

Table 3-2 addalmslot – Parameters

Parameter	Description
slot number	Specifies the slot number of the alarm card set.

addcdred

The **addcdred** is an alias for the **addyred** command (thus has identical functionality) which lets you enable card and line redundancy for the cards on the IGX and BPX. It lets you add card and line redundancy for APS 1+1 across two BXM OC-3 and OC-12 cards. You also use it before enabling APS 1:1 line redundancy. It works similarly to the **addyred** command.

Use the **addcdred** command to specify the slots of the primary and secondary (standby) cards that form the redundant pair.

When configuring APS 1+1 card and line redundancy, you must execute the **addcdred** command before using **addapsln**. Refer to the "APS 1+1 (Card and Line Redundancy)" section on page 4-55" for more information on setting up APS 1+1 card and line redundancy.

Redundant card sets must have the following characteristics:

- The primary and secondary card sets must be identical.
- For APS 1+1 card redundancy only, the primary and secondary card sets must reside in adjacent slots. (This restriction only applies to APS 1+1 Card and Line Redundancy.) APS 1+1 is not supported on a single-card option.
- Secondary card sets must not currently be active.
- Neither the primary nor secondary card set may already be part of a redundant set.
- Redundancy applies to the entire card and not specific trunks or lines.

In both the single and multiport card sets, if the secondary card set becomes active, the primary card set serves as its backup (assuming the primary card set is complete and not failed). You cannot use the **addcdred** command on empty card slots. If one or both of the card slots is empty, and you use the **addcdred** command, the command will fail.

If cards reside in the primary and secondary slots, the system checks for card compatibility. The following types of incompatibility can occur: back card and jumper or cable inconsistencies. Also, the **addcdred** command can fail because of firmware capabilities conflicts. For example, if one of the cards supports virtual trunking, and the other doesn't support virtual trunking, the **addcdred** command might fail. Refer to the *Cisco BPX 8600 Series Installation and Configuration* manual for more information on configuring SONET APS 1+1 card and line redundancy for BXM OC-3 and OC-12 cards.

APS 1+1 Environment (Using Redundant Backcards with Front Card Redundancy)

The same numbered ports on adjacent BXM cards are used. A hardware, firmware, and software upgrade is required. (Firmware that supports APS 1+1 setup, and switch software Release 9.2 is required.)

The APS 1+1 feature requires two BXM front cards, an APS redundant frame assembly, and two redundant type BXM backcards. The two redundant BXM backcards are plugged into the APS redundant frame assembly. (Refer to the SONET APS Configuration chapter in the *Cisco BPX 8600 Series Installation and Configuration* guide for more information on APS hardware configuration.) The types of redundant back card and backplane sets required are:

- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622 (single port, long reach, SMF, FC connector)
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)

- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- BPX-RDNT-SM-622-2 (2 port, medium reach, SMF, FC connector)

  Each of the listed model numbers includes two single backcards and one mini-backplane (providing cross coupling of two backcards).

The single backcards and mini-backplane can be ordered as spares. Their model numbers are:

- BPX-RDNT-BP= (common backplane for all redundant APS backcards)
- BPX-LR-155-8R-BC= (for BPX-RDNT-LR-155-8)
- BPX-LR-622-R-BC= (for BPX-RDNT-LR-622
- BPX-SMF-155-4R-BC= (for BPX-RDNT-SM-155-4)
- BPX-SMF-155-8R-BC= (for BPX-RDNT-SM-155-8)
- BPX-SMF-622-R-BC= (for BPX-RDNT-SM-622)
- BPX-SMF-622-2R-BC= (for BPX-RDNT-SM-622-2)

Note Using only one front card and two backcards is not a valid configuration when adding APS capability, and APS alarm capability is reduced when the standby card is not available. You must configure card redundancy before you can configure APS redundancy.

If incompatibilities exist, the message “Y-Cable Conflict” appears on the screen. Specific conflicts are listed in reverse video on the **dspcdred** display. See the **dspcdred** description for more information.

Note When SONET Automatic Protection Switching (APS) is configured, you will not be able to use the **addyred** or **delyred** commands on a card configured for APS 1:1 architecture. That is, you will not be able to execute the **addyred** command, then configure the APS 1:1 architecture. Similarly, you will not be able to configure APS 1:1, then execute the **addyred** command. You will be blocked from executing these commands at the command line interface.

In this release, to ensure that only cards with the Idle Code Suppression feature enabled on them are allowed to be a Y-redundancy pair, **addcdred** blocks cards that have different idle code suppression capability.

Full Name

Add card redundancy for SONET Automatic Protection Switching (APS) across two OC-3 or OC-12 cards.

Syntax

addcdred <primary slot> <secondary slot>

Related Commands

delcdred, **dspcdred**, **prtcdred, switchcdred**

Attributes

Privilege	1–4
Jobs	No
Log	Yes
Node	BPX
Lock	Yes

Example 1

addcdred 2 3

Description

Add redundant line on port 1 for BXM OC-3 card and APS backcards in slots 2 and 3 of the BPX.

System Response

```
beta           TRM   YourID:1        BPX 8620    9.2    Aug. 15 1997 14:27 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
2    Pri    3   BXM    LM-BXM
3    Sec    2   BXM    LM-BXM










Last Command: addcdred 2 3


Next Command:
```

Table 3-3 addcdred–Parameters

Parameter	Description
primary slot	Specifies the slot number of the primary card set.
secondary slot	Specifies the slot number of the secondary card set.

addctrlr

Adds VSI capabilities to a trunk interface to which a feeder of type AAL5 is attached. The **addctrlr** command is used only to connect a Private Network to Network Interface (PNNI) controller. PNNI is the software residing on the Service Expansion Shelf (SES) hardware

The **addctrlr** command is the second step in the adding of a PNNI controller to a BPX node.

The first step is to run the command **addshelf** with shelf type set to “X” to add a AAL5 feeder.

Then run the **addctrlr** command to set up the VSI control channels from the SES PNNI controller to the VSI slave processes running on the BXM cards to ensure full VSI functionality for the PNNI controller. You execute the **addctrlr** command on an existing AAL5 interface shelf.

Also note that you can add a PNNI controller to a Trunk interface only if the interface already has an active VSI partition corresponding to the partition that is controlled by the PNNI controller. Suppose a PNNI controller controlling the partition “1” were added to an trunk interface 12.1. Then it would be necessary that a VSI partition corresponding to partition “1” be active on the interface 12.1. Otherwise the **addctrlr** command would fail.

When you add VSI controller capabilities onto an AAL5 interface shelf (or feeder), the switch software prompts you for the specifics of the VSI controller:

- controller id of the PNNI controller
- partition id of the VSI partitions controlled by the PNNI controller
- VPI used for the VSI control channels set up by the PNNI controller
- Start VCI value for the VSI control channels set up by the PNNI controller

Note that the **addctrlr** command does not prompt you for the controller name. The controller name is the same as the interface shelf, or feeder, name.

There could be 12 BXM cards on the BPX node and the PNNI controller would control VSI partitions on those BXM cards that support VSI capability. Hence a separate VSI control channel must be set up from the PNNI control to each BXM card that supports VSI. Suppose you specify a VPI value of 0 and start VCI value of 40 for the VSI control channels. Then the control channel corresponding to any BXM card on slot 1 would use VPI, VCI values <0, 40>. The VSI control channels to other slots would use the VPI, VCI values of <0, 40+slot-1>, where “slot” corresponds to the slot number of the BXM card.

The PNNI is the latest networking application controller that can control a BPX node’s resources. PNNI runs on the MGX 8850 and SES platforms. The MGX 8850 connects to the BPX through an already-defined AAL5 interface shelf. The AAL5 interface shelf has Annex G capabilities. The PNNI can be configured as a VSI controller.

You use the **addctrl** and **delctrlr** commands to add and delete an MGX 8220 and MGX 8850 interface shelf configured with VSI controller capabilities. See the **delctrlr** command for information on deleting a PNNI (PNNI) controller from a BPX.

Note ESP 2.x interface shelves can still be configured; however, an ESP 2.x shelf cannot coexist with an AAL5 interface shelf with VSI configured on the same node. The Annex G capabilities of the AAL5 interface shelf are the same as in Release 9.1.

In this release, the **addctrlr** command can be used for controllers that require Annex G capabilities in the controller interface. In this release, the parameters “Control VPI” and “Control VCI start” have been added.

Resource Partitioning

In this release you still use the same commands as in Release 9.1 to configure a VSI controller partition's resources: **cnfrsrc, cnfqbin, dsprsrc,** and **dspqbin**.

The management of resources on the VSI slaves requires that each slave in the node has a communication control VC to each of the controllers attached to the node. When a controller is added to the BCC, the BCC sets up the set of master-slave connections between the new controller port and each of the active slaves in the switch. The connections are set up using a well known vpi.vci. The value of the VPI is 0, and the value of the VCI is (40 + slot -1) where slot is the logical slot number of the slave, for ports, physical trunks, and feeder trunks case. For virtual trunks, the VPI used is the one configured in the command cnftrk and the vci used is (259 + slot -1).

The management of resources on the VSI slaves requires that each slave in the node has a communication control VC to each of the controllers attached to the node. When a controller is added to the BCC, the BCC sets up the set of master-slave connections between the new controller port and each of the active slaves in the switch.

You use **addctrlr** to set up the connections with the VPI/VCI. You enter the value of VPI; and the value of VCI is (value of VCI + slot -1) where slot is the logical slot number of the slave. The default values for these parameters are VPI=0 and VCI=40-53.

For feeder trunk interfaces, the **addctrlr** command will fail. You must delete the connections before proceeding if connections with VPI and VCI in the range exist in the range you specified.

The addition of a controller to a node will fail if there are not enough channels available to set up the control VCs in one or more of the BXM slaves.

The BCC also informs the slaves of the new controller through the VSI configuration CommBus message. The message include a list of controllers attached to the switch and their corresponding controller IDs.

Full Name

Add VSI capabilities to a AAL5 feeder interface.

Syntax

addctrlr < slot.port> <controller id> <partition id> <control_vpi> <start_vci>

Table 3-4 Parameters—addctrlr

Parameter	Description
<slot.port>	Slot and Port numbers corresponding to the feeder trunk
<controller-id>	Controller ID corresponding to the PNNI controller. Values: 1–32
<partition-id>	Partition ID of the VSI partition controlled by the PNNI controller
<control_vpi>	Starting VPI of the VSI control channels used for communication between the VSI master residing on the SES and VSI slaves residing on the BXM cards. There can be a total of 12 such channels one for each slave residing on each BXM card. For a trunk interface with NNI header type: Valid values for this parameter are: 0–4095 For a trunk interface with UNI header type Valid values for this parameter are: 0–255. Default value: 0

Table 3-4 Parameters—addctrlr (Continued)

Parameter	Description
<start_vci>	Starting VCI of the VSI control channels. This vci value is assigned to the first VSI control channel (between the VSI master and the VSI slave residing on the BXM card in slot 1). The last VSI control channel corresponding to communication with the VSI slave on slot 14 will use the vci value of (<start_vci>+14-1). The valid values are: 33 – 65521. Default value: 40

Related Commands

addshelf, delctrlr, dspctrlrs

Attributes

Privilege	1
Jobs	No
Log	Yes
Node	BPX
Lock	Yes

Example 1

addctrlr 10.4 3 2 0 40

Description

Add controller to port 4 on slot 10, partition ID of 2, and controller ID of 3.

System Response

```
night           TN    StrataCom     BPX 8600   9.2.00 Apr. 11 1998 14:31 GMT

                    BPX Controllers Information

 Trunk   Name       Type      Part Id   Ctrl ID   Ctrl IP       State
 10.3    PNNI    VSI       1         1         192.0.0.0     Enabled
 11.1    VSI        VSI       2         2         192.0.0.0     Disabled


Warning partition already in use do you want to add redundant controller

Last Command: addctrlr 10.4 3 2 0 40


Next Command:
```

Description

Adds a controller, such a PNNI controller, to a BPX interface shelf.

System Response

```
night           TN   StrataCom     BPX 8600   9.2.00 Apr. 11 1998 14:31 GMT

                    BPX Controllers Information

 Trunk   Name       Type      Part Id   Ctrl ID   Ctrl IP       State
 10.3    PNNI    VSI       1         1         192.0.0.0     Enabled
 11.1    VSI        VSI       2         2         192.0.0.0     Disabled


Warning partition already in use do you want to add redundant controller

Last Command: addctrlr 10.3 3 1 0 40


Next Command:
```

addshelf

Adds an ATM link between an IGX/BPX core switch shelf and an interface shelf such as an MGX 8220, MGX 8850, IGX shelf, or SES (Service Expansion Shelf) in a tiered network; or an ATM link between a BXM card on a BPX node and a Label Switch Controller (LSC) such as a series 7200 or 7500 router; or an ATM link between a BXM card on a BPX node and an Extended Services Processor. (An MPLS controller, a PNNI controller, or an Extended Services Processor controller is considered an interface shelf from the BPX's perspective.) The routing hub can be either a BPX or an IGX.

The interface shelf can be one of the following:

- An MGX 8220 shelf connected to a BPX node
- An MGX 8850 shelf connected to a BPX node
- A MPLS (Multiprotocol Label Switching) controller connected to a BPX node
- A Private Network to Network Interface (PNNI) Controller connected to a BPX node
- An IGX node connected to an IGX routing node which serves as a hub for the IGX/AF
- An SES (Service Expansion Shelf) connected to an IGX node (supported in Release 9.2.20).

The signaling protocol that applies to the trunk on an interface shelf is Annex G. (Annex G is a bidirectional protocol defined in Recommendation Q.2931, used to monitor the status of connections across a UNI interface. The Annex G protocol is used in this release to pass connection status information between a IGX/BPX core switch shelf and an attached feeder.)

Note Because tiered network capability is a paid option, personnel in the Cisco Technical Assistance Center (TAC) must telnet to the unit and configure it as an interface shelf before you can execute **addshelf**.

Each IGX/AF, MGX 8220, MGX 8850, or SES shelf has one trunk that connects to the BPX or IGX node serving as an access hub. A BPX routing hub can support up to 16 T3 trunks to the interface shelves, which can be IGX/AF, MGX 8220, or MGX 8850 interface shelves. An IGX hub can support up to four trunks to the interface shelves, which can be IGX/AF or SES (Service Expansion Shelf) shelves.

Before it can carry traffic, you must "up" the trunk on an interface shelf (using **uptrk** on both the interface shelf and the IGX/BPX core switch shelf) and "add" it to the network (using **addshelf**). Also, a trunk must be free of major alarms before you can add it with the **addshelf** command.

In this release, the commands **addshelf** and **addctrlr** are used to add a MPLS/PNNI controller to the BPX. The command **addshelf** with option "v" is used to add a VSI shelf. This is used mainly for MPLS controllers. The command **addctrlr** is used to add a controller to a shelf that has LMI capabilities.

In this release, you can use an IGX as a feeder node to connect via a UXM IMA trunk to an IGX or BPX router node using IMATM. You use **addshelf** with the I option at the IGX node to add the feeder trunk connecting it to an IGX feeder node.

Full Name

Add an interface shelf (feeder) or a controller to a routing node or hub.

Syntax

Interface shelf:

addshelf <slot.port> <shelf-type> [vpi] [vci]
addshelf <slot>.<primary link> <shelf type>

Tag switch controller:

addshelf <slot.port> <device-type> <control partition> <control ID>

VSI controller:

addshelf <trunk slot.port> v <ctrlr id> <part id> <control vpi> <control vci start> <redundant ctrlr warning>

Note If you manage a tiered network through the command line interface, you can manage only Frame Relay interworking connections (ATFR) across the network. Three-segment connections for carrying serial data or voice between IGX/AFs is allowed, but you must manage them through Cisco WAN Manager.

Related Commands

delshelf, **dspnode**, **dsptrks**

Attributes

Privilege	1–4
Jobs	Yes
Log	Yes
Node	BPX switch with IGX interface shelves IGX switch with IGX shelves BPX switch with the MGX 8220 interface shelf BPX with the MGX 8850 interface shelf BPX switch for MPLS controller BPX switch for the Extended Services Processor (ESP) IGX switch for the Service Expansion Shelf (SES)
Lock	Yes

Example 1

Interface shelf: **addshelf** 11.1 a 21 200

Label switch controller: **addshelf** 4.1 vsi 1 1

Description

Interface shelf:

Add trunk 11.1 as an MGX 8220 interface shelf. After you add the shelf, the screen displays a confirmation message and the name of the shelf.

MPLS controller:

Add trunk 4.1 as a MPLS Controller interface shelf. After you add the MPLS controller, the screen displays a confirmation message and the name of the shelf:

Description for Interface Shelves

An interface shelf can be one of the following:

- An MGX 8220 connected to a BPX node.
- An MGX 8850 connected to a BPX node.
- An IGX node connected to a BPX node, which serves as a hub for the IGX/AF.
- An IGX node connected to an IGX routing node, which serves as a hub for the IGX/AF.

Table 3-5 Interface Shelf Parameters- addshelf

Parameter	Description
slot.port (trunk)	slot.port Specifies the slot and port number of the trunk.
shelf-type	I, A, P, V, X On a BPX node, shelf type specifies the type of interface shelf when you execute **addshelf**. The choices are I for IGX/AF, A for the MGX 8220, P for EPS (Extended Services Processor, a type of adjunct processor shelf), V for VSI, or X for the MGX 8800. In the case of BNI, only two options are available: I for IGX/AF, A for the MGX 8220. On an IGX node, shelf type specifies the type of interface shelf you can add. The choices are I for IGX/AF or X for AAL5 for an SES (Service Expansion Shelf).
vpi vci	vpi, vci are optional when adding an interface shelf (feeder). (Specifies the vpi and vci (Annex G vpi and vci used). For the MGX 8220 only, the valid range for vpi is 1–1015 and for vci is 1–65535.)
Control VPI Control VCI start	The (VPI.VCI) of the 15 control VCs is (control_VPI.control_VCI_start) to (control_VPI.control_VCI_start+14).The control VC used for slot n (1<= n<=15) is (control_VPI.control_VCI_start + n -1). <control_VPI> should be chosen such that: • if <control_VPI> = 0, <control_VCI_start> can be set to a value > 40. • If any VSI partition exists on the interface, then control_VPI < start_VPI or control_VPI > end_VPI for all partitions on that interface. An error message is displayed if the control VPI falls into the VPI range belonging to a VSI partition. • No AutoRoute connection exists on (VPI.start_VCI to VPI.start_VCI+14). If any AutoRoute connection exists on these VPI/VCI values, you are not allowed to use these VPI/VCI values. • This VPI is “reserved” for control VCs.

Example for Interface Shelves

Add an MGX 8220 at trunk 11.1 After you add the shelf, the screen displays a confirmation message and the name of the shelf. Add the MGX 8220 (may be referred to on screen as AXIS) as follows:

addshelf 11.1 a

The sample display shows a partially executed command prompting you for the interface shelf type:

System Response

```
nmsbpx23       TN    SuperUser       BPX 620    9.2   Apr. 4 1998 13:28 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 1.3     AXIS240   AXIS      OK
 11.2    A242      AXIS      OK





This Command: addshelf 11.1

Enter Interface Shelf Type:  I (IGX/AF), A (AXIS), P (APS), V (VSI), X (AAL5)

Next Command:
```

Example for Adding an MGX 8850 (AAL5) Interface Shelf to a BPX Routing Node

Add an MGX 8850 at trunk 4.1. After you add the MGX 8850 interface shelf, the screen displays a confirmation message and the name of the shelf. Add the MGX 8850 (may be referred to on–screen as AAL5) as follows:

addshelf 4.1 x

The sample display initially shows the output of a **dsptrks** command, then shows how an MGX 8850 was added on trunk 4.1 as an AAL5 type of interface shelf. (AAL5 is the ATM Adaptive Layer 5 protocol, which is an ATM standard interface that is used by the routing node or routing hub to communicate to the MGX 8850 and Service Expansion Shelf feeders.) Adding an MGX 8850 interface shelf or a Service Expansion Shelf is similar to adding an MPLS controller or a PNNI controller.

In releases previous to Release 9.2.10, for BTM E1/T3 feeder interface types, **addshelf** does not prompt you for the “Interface Shelf Type”. In this release, **addshelf** will prompt you for the “Interface Shelf Type”. (This is needed to distinguish which signalling protocol is used.) Because MGX 8220, MGX 8850 and SES use the same LMI signalling protocol, you will be prompted for the “Interface Shelf Type **(A) AAL5**”.

System Response

```
sw288       TN    SuperUser       BPX 8620    9.2.j2   Dec. 10 1998 15:38 PST

TRK      Type    Current Line Alarm Status            Other End
4.1      OC-12    Clear - OK                           -
11.2     T3      Clear - OK                           redhook/14
11.3     T3      Clear - OK                           sw113/16




This Command: addshelf 4.1

Enter Interface Shelf Type:  I (IGX), A (AXIS), P (APS), V (VSI), X (AAL5)

                        BPX Interface Shelf Information

Trunk    Name      Type      Part Id    Ctrl Id    Alarm
 4.1     SIMFDR0   AAL5          -           -      OK




This Command: addshelf 4.1 x

Enter Interface Shelf Type:  A (AXIS), P (APS), V (VSI), X (AAL5)

Shelf has been added
Next Command:
```

Example for Adding a Service Expansion Shelf (SES) to an IGX 8400

Add an SES interface shelf to an IGX 8400 (using a UXM or UXM-E interface). After you add the SES interface shelf, the screen displays a confirmation message and the name of the shelf. Add the SES (may be referred to on–screen as AAL5) as follows:

addshelf 6.1 X

Enter Interface Shelf Type: **X** (AAL5)

Note You can add an SES (Service Expansion Shelf) feeder to an IGX routing node only.

System Response

```
sw288       TN    SuperUser       IGX 8420    9.2.2I   Dec. 10 1998 15:38 PST

TRK      Type     Type          Alarm
9.1      ases1    AAL5        MIN




This Command: addshelf 4.1

Enter Interface Shelf Type:  I (IGX), A (AXIS), P (APS), V (VSI), X (AAL5)

                        IGX Interface Shelf Information

Trunk    Name       Type        Alarm
 9.1     ses_fdr    AAL5      MIN




This Command: addshelf 4.1 x

Enter Interface Shelf Type:  A (AXIS), P (APS), V (VSI), X (AAL5)

Shelf has been added
Next Command:
```

The sample display shows that an SES was added on trunk 9.1 as an AAL5 type of interface shelf. (AAL5 is the ATM Adaptive Layer 5 protocol, which is an ATM standard interface that is used by the routing node or routing hub to communicate with the SES shelves.) Adding an IGX interface shelf is similar to adding an MPLS (Multiprotocol Label Switching) controller as an interface shelf.

The **addshelf** command will prompt for “Interface Shelf Type”. Because the MGX 8220, MGX 8850 and the SES (Service Expansion Shelf) use the same Annex G LMI signalling protocol to communicate with an IGX routing hub, they all use the same interface shelf type of AAL5 (designated by the **addshelf** “X” option).

Types of Interface Shelves Supported in Release 9.2

Previous to Release 9.2, WAN switching software supported the ability to configure an IGX 8400 as an interface shelf to the IGX 8400 hub over a BTM E1 and T3 interface. Also, the MGX 8220 (formerly called “AXIS”) is supported as an interface shelf to the BPX. Release 9.1 introduced the ability for the MGX 8850 to serve as an interface shelf to a BPX routing hub. Release 9.2 introduced the ability for an SES (Service Expansion Shelf) to serve as an interface shelf to an IGX 8400 routing hub.

UXM Feeder Support in Release 9.2

In Release 9.2.20, the following are supported:

- You can attach SES feeders to the routing network through an IGX 8400 routing hub using UXM/UXM-E and PXM trunks using UNI and NNI format. A routing hub can support up to four feeders.
- The LMI/Annex G signalling channel is used to communicate with the SES feeder through the SAR (Segmentation Assembly and Reassembly).
- UXM Feeder support provides voice, Frame Relay, and ATM data connections from feeder node to feeder node for a 2 or 3-segment network.

Not Supported in Release 9.2

An MGX 8220, an ESP (an Extended Services Processor controller, or Adjunct Processor Shelf), or an MGX 8850 can connect as interface shelves to a BPX routing node. An IGX interface shelf can connect to an IGX 8400 routing node over a UXM/UXM-E interface. Similarly, in Release 9.2.10, an SES can connect to an IGX routing hub over a UXM/UXM-E interface. However, you cannot do the following:

- An IGX 8400 interface shelf cannot connect to a BPX hub.
- Two-segment voice and data connections are not allowed on an SES interface shelf.
- An IGX 8400 interface shelf cannot connect to an IGX routing hub over a UXM trunk.
- An MGX 8220 interface shelf cannot connect to an IGX 8400 routing hub.

Signalling Channel Used by MGX 8850 and SES Interface Shelves Connecting to Routing Hubs

Previous to Release 9.2, the IGX 8400 interface shelf communicated with the IGX 8400 routing hub using a BTM E1 interface over the Annex G LMI with STI format. In Release 9.2, the SES interface shelf with a UXM/UXM-E interface communicates with the routing hub over an Annex G LMI interface by using AAL5 format.

Note Annex G is a bidirectional protocol used to monitor the status of connections across a UNI interface. This includes the real-time notification of the addition or deletion of connection segment and the ability to pass the availability (active state) or unavailability (inactive state) of the connections crossing this interface.

An SES feeder uses the Annex G protocol to pass connection status information between itself and an IGX 8400 routing hub. Similarly, an MGX 8850 feeder uses the Annex G signalling channel to pass connection status information between itself and a BPX routing hub.

Previous to Release 9.2, IP relay was supported by encapsulating the IP data in a network message when interfacing with an IGX 8400 interface shelf. In this release, the SES interface shelf communicates with an IGX routing hub through ATM cells. Thus, IP data destined for an IGX 8400 is encapsulated in an AAL5 ATM cell format.

addshelf Error Messages

Some of the possible error messages for the **addshelf** command:

— An MGX 8850 Interface Shelf already exists on this Hub

— Trunk is already added to the Network

— Trunk is in alarm

— An Interface Shelf already exists on this trunk

— Interface Shelf VPI out of range

— Interface Shelf VCI out of range

— No memory available for Interface Shelf allocation

— Communication failure during Shelf modification

— Shelf has been added

— Shelf has been deleted

— Communication breakdown

— Interface Shelf allocation failure

— Interface Shelf already has a network connection

— Interface Shelf name is not unique

— Interface Shelf IP address is not unique

— Interface Shelf modification failure

System Response

```
pswbpx3       TN    SuperUser       BPX 8600    9.1   June 6 1998 13:28 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Part Id    Ctrl Id    Alarm
 4.8     SIMFDR0   AAL5          -           -      OK




This Command: addshelf 4.8 x

Enter Interface Shelf Type:  I (IGX/AF), A (AXIS), P (APS), V (VSI), X (AAL5)

Next Command:
```

Description for Label Switching

For label switching, before it can carry traffic, you need to "up" the link to a tag switch controller (using either **uptrk** or **upport**) at the BPX node. You can then "add" the link to the network (using addshelf). Also, the link must be free of major alarms before you can add it with the **addshelf** command.

Note Once you "up" a port on the BXM in either trunk or port mode by using either the **uptrk** or **upport** commands, respectively, you can only "up" the ports in the same mode.

Table 3-6 Label Switching Parameters- addshelf

Parameter	Description
slot.port	Specifies the BXM slot and port number of the trunk. (You can configure the port for either trunk (network) or port (service) mode.
device-type	vsi, for "virtual switch interface", specifies a virtual interface to an ATM-LSR (Label Switch Router) controller such as a Cisco 7200 or 7500 series router. Note that the "v" option is not applicable when configuring Automatic Routing Management PVCs. You only need to enter the "v" or "vsi" option when configuring VSI options.
control partition	Specifies the control partition. You can typically leave this field blank when you add an MPLS (formerly Tag Switching) controller to a BPX or MGX 8800 node.
control ID	Control IDs must be in the range of 1 to 32, and you must set these identically on the VSI-MPLS Controller and in the **addshelf** command. A control ID of "1" is the default used by the MPLS Controller (formerly Tag Switch Controller).

Example for Multiprotocol Label Switching

Add an LSC (Label Switch Controller) link to a BPX node by entering the **addshelf** command at the desired BXM port as follows:

addshelf 4.1 vsi 1 1

System Response

```
nmsbpx23       TN    SuperUser       BPX 15    9.2   Apr. 4 1998 13:28 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 5.1     j6c       AXIS      MIN
 5.3     j5c       IGX/AF    MIN
 4.1     VSI       VSI       OK






This Command: addshelf 4.1 v 1 1

Next Command:
```

Example for Adding a Redundant VSI Controller

addshelf 11.1 vsi 1 2

Description

Add a redundant (more than one) VSI controller (as an interface shelf to a BPX node), on slot 11 on port 1, with a control partition of 1 and control ID of 2.

System Response

```
night          TN    StrataCom       BPX 8600   9.2.00 Apr. 11 1998 14:31 GMT

                        BPX Interface Shelf Information

Trunk    Name       Type     Part Id   Ctrl Id   Alarm
1.1      sww222     IGX/AF   -         -         UNRCH
10.3     VSI        VSI      1         1         OK





Warning partition already in use do you want to add redundant controller?

Last Command: addshelf 11.1 vsi 1 2
```

Example 4

addshelf 4.1 vsi 1 1

Description

Add a VSI controller to port 4.1, controlling partition 1

Note The second “1” in the addshelf command is a controller ID. Controller IDs must be in the range 1-32, and must be set identically on the TSC and in the addshelf command. A controller id of 1 is the default used by the TSC.

System Response

```
n4             TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:42 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 3.1     j6c       AXIS      MIN
 5.3     j5c       IGX/AF    MIN
 4.1     VSI       VSI       OK









Last Command: addshelf 4.1 vsi 1 1


Next Command:
```

addyred

The **addyred** command performs the same function as the **addcdred** command. It enables card redundancy for cards on the IGX and BPX. Use the **addyred** command to specify the slots of the primary and secondary (standby) cards that form the redundant pair. Refer to the "Specifying Card Redundancy" section at the beginning of this chapter for a list of supported card sets.

Redundant card sets must have the following characteristics:

- The primary and secondary card sets must be identical.
- When configuring APS 1+1, the primary and secondary card sets must be in adjacent slots. (Note that this restriction only applies to the BPX chassis for APS 1+1 redundancy.)
- Secondary card sets must not currently be active.
- Neither the primary nor secondary card set may already be part of a redundant set.
- Redundancy applies to the entire card, and not specific trunks or lines.

If cards reside in the primary and secondary slots, the system checks for card compatibility. Two types of incompatibility can occur: back card and jumper or cable inconsistencies. (On SDI, FRI, and FTI cards, jumpers determine whether a port is configured as DCE or DTE. On LDI cards, either a DCE or DTE adapter cable connects to the LDI port. For descriptions of the jumper positions and cabling, see the *Cisco IGX 8400 Series Installation and Configuration* manual.)

Note that the **addyred** command prevents invalid configurations when you try to configure the SONET APS feature. When SONET Automatic Protection Switching (APS) is configured, you will not be able to use the **addyred** or **delyred** commands on a card configured for APS 1:1 architecture. That is, you will not be able to execute the **addyred** command, then configure the APS 1:1 architecture. Similarly, you will not be able to configure APS 1:1, then execute the **addyred** command. You will be blocked from executing these commands at the command line interface.

If incompatibilities exist, the message "Y-Cable Conflict" appears on the screen. Specific conflicts are listed in reverse video in the **dspyred** display. See the **dspyred** description for more information.

To ensure that only cards with the Idle Code Suppression feature enabled on them are allowed to be a Y-redundancy pair, **addyred** blocks cards that have different idle code suppression capability.

The addyred commands (**addyred, delyred, dspyred, prtyred, switchyred**) will perform feature mismatch checking on both the primary and secondary cards. For information on feature mismatch checking, see "Feature Mismatching" section on page 18-1.

Mismatch Checking Performed by addyred/delyred

During addyred's mismatch checking, the following verifications are done:

- A verification is done to ensure that both the primary and secondary cards support features that are activated. For example, if on the primary card, the APS feature has been configured, and on the secondary card this feature is not available, you will be blocked from using the **addyred** command.
- If the feature is not enabled, and the secondary card does not support similar feature sets, the (internal) logical database is updated to reflect this.
- Following a **delyred** command execution, the logical card's database is updated to reflect the primary card's capabilities.

Full Name

Add Y-cable redundancy.

Syntax

addyred <primary slot> <secondary slot>

Related Commands

delyred, **dspyred**, **prtyred**

Attributes

Privilege	1–4
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

addyred 2 3

Description

Add Y-cable redundancy to the BXM card sets in slots 2 and 3.

System Response

```
beta           TRM   YourID:1        BPX 8620    9.2    Aug. 15 1998 14:27 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
2    Pri    3   BXM    LM-BXM
3    Sec    2   BXM    LM-BXM








Last Command: addyred 2 3


Next Command:
```

Table 3-7 addyred–Parameters

Parameter	Description
primary slot	Specifies the slot number of the primary card set.
secondary slot	Specifies the slot number of the secondary card set.

cnfasm

Lets you set various configurable parameters associated with the BPX Alarm and Status Monitor card in slot 15. Because this card always resides in slot 15, entering the slot number is unnecessary. In Release 9.2, robust alarms are generated for the following alarm conditions:

- Power supply, temperature, fan, and DC voltage level alarms. (Some of these conditions already generate Robust Alarms on the IGX.)
- Connection AIS alarm
- Bus failure
- External clock source failure
- Multiple invalid login attempts on a user port (potential security threat)
- Excessive CPU and memory usage on switch processor card

These alarm conditions above appear in the maintenance log or in the node command line interface commands (dspasm), are not also reported as SNMP trap to the customer NMS. (Such traps are generated by the Cisco WAN Manager RTM proxy upon receiving Robust Alarms from a switch.)

In Release 9.2, robust alarms are generated by the BPX when power and temperature alarm conditions are detected by the ASM card. The ASM card monitors and reports events involving:

- Power supplies
- Cabinet temperature
- Cooling fan speed
- DC voltage level

You configure and control the reporting of these events through the cnfasm command, where you can enable or disable each alarm. For power supply failure/removal events, you can also specify the alarm class (that is, Major vs. Minor).

In Release 9.2, a robust alarm is generated by the IGX platform when a DC voltage out-of-range condition occurs.

A robust alarm is generated by all switch platforms (IGX, BPX) when an Alarm Indicator Signal (AIS) condition is detected on a PVC. The alarm now has an NNI Status field that previously appeared in the Connection NNI Alarm message.

A robust alarm is generated by all switch platforms (IGX, BPX) when a bus failure or failure cleared event occurs. (In releases previous to Release 9.2, such events are currently reported through maintenance log messages.)

A robust alarm is generated by all switch platforms when an external clock source failure or failure cleared event occurs.

A robust alarm is generated by all switch platforms when the number of successive invalid login attempts on a user port exceeds the current threshold setting on the switch. You set the threshold by using the **cnfsysparm** command.)

A robust alarm is generated by all switch platforms when the processor card CPU utilization of the IDLE process falls below a fixed threshold. The purpose of the alarm is to indicate the possible degradation of service caused by processor load reaching an abnormally high level.

Full Name

Configure ASM (Alarm and Status Monitor) card

Syntax

cnfasm

Related Commands

dspasm

Attributes

Privilege	1
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
cnfasm
```

Description

Configure parameters for the ASM card.

System Response

```
D1.jea         TRM   SuperUser       BPX 8600    9.2     Aug. 30 1998 12:25 GMT

[1] Cabinet temp threshold:       50 C  [4] Polling interval (msec):    10000
[2] Power A deviation:             6 V  [5] Fan threshold (RPM):         2000
[3] Power B deviation:             6 V


                    ALM                                         ALM
[6]  ACO button      -                  [14] BPX card slot   -
[7]  History button  -                  [15] PSU A failure   Y
[8]  Cabinet temp    Y                  [16] PSU A removed   Y
[9]  Power A volt    Y                  [17] PSU B failure   Y
[10] Power B volt    Y                  [18] PSU B removed   Y
[11] Fan 1 RPM       Y
[12] Fan 2 RPM       Y
[13] Fan 3 RPM       Y


This Command: cnfasm


Which parameter do you wish to change:
```

cnfdate

Sets the date and time for the entire network. The node broadcasts the specified date and time to every node in the network. The time displayed at each node is consistent with the time zone where the node resides. (See the **cnftmzn** description.) For the first-time configuration of the date and time in a network, **cnfdate** requires all the parameters except for *second*. The default for *second* is 0. If a date and time already exist in the network, the defaults are the existing values at the moment you enter the **cnfdate** command. Note that changes to date and time alter the timestamps on WAN Manager statistics.

Full Name

Configure data and time

Syntax

`cnfdate` <year> <month> <day> <hour> <minute> [second]

Related Commands

cnftime, **cnftmzn**

Attributes

Privilege	1
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`cnfdate` 1997 12 16 13 54 11

Description

Set the time to 1:54:11 in the afternoon, December 16 1997. The system prompts:
"Warning: Changing time of day affects StrataView statistics timestamps

Continue?"
Enter "y" to continue or "n" to abort." Upon a "y" response, the system further prompts with: "Hit RETURN to change clock, DEL to abort."

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Dec. 16 1998 13:54 PST

YourID       1
Sarah        5









Last Command: cnfdate 1997 12 16 13 54 11

Warning: Changing time of day affects StrataView statistics timestamps
Continue?
```

Table 3-8 cnfdate–Parameters

Parameter	Description
year	Specifies the year.
month	Specifies the month. The range is 1–12.
day	Specifies the day. The range depends on the month and can be 1–31.
hour	Specifies the hours. The range is 0–23. For example, enter 6 AM as 6 and 6 PM as 18.
minute	Specifies the minute of the hour. The range is 0–59. The default is 0.

Table 3-9 cnfdate–Optional Parameters

Parameter	Description
second	Specifies the seconds. The range is 0–59. The default is 0.

cnffunc

Enables or disables a specified node function. Each function has an index number. By entering the command, the index parameter, and the letter “e” or “d,” the function is either enabled or disabled.

Upgrading from Release 9.1 to Release 9.2 when IMA Trunks Exist

When IMA trunks exist in a Release 9.1 network, and you are upgrading from Release 9.1 to 9.2, ensure that the following steps have been performed:

- While the network is running Release 9.1, use **cnffunc** command option 15 to disable the **Automatic Card Reset after Burnfw for CBI cards** option. (Note that this option is enabled by default.) This step is required so that you can burn UXM firmware revision on the flash and delay execution with this new firmware revision, then later reset the card by using **resetcd** command. After the UXM at both end of the trunks are burned with the new firmware revision, you can reset the UXM cards at the same time so that the new ATM Forum-Compliant protocol is invoked at both ends at the same time. If this step is not followed, some nodes may not be reachable if this is an IMA trunk, and it is the only trunk connected to that remote node. Note that if an IMA trunk is not used within the 9.1 network, then you do not need to perform this step.
- Upgrade all UXM cards in the Release 9.1 network with UXM firmware model B.

You are now ready to upgrade the switch software from Release 9.1 to 9.2.

Full Name

Configure system functions

Syntax

cnffunc <function_index> <e/d>

Related Commands

none

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`cnffunc` 7 e

Description

Enables automatic card testing after a card failure has been detected.

System Response

```
sw199          TN    StrataCom       IGX 8420    9.2    Apr. 9 1998  18:14 GMT

Index Status    Function

1     Enabled   Automatic CLN/PLN Loopback Test on Local/Remote Alarms
2     Enabled   FDP Loopback button
3     Enabled   User Command Logging
4     Enabled   Automatic Card Reset on Hardware Error
5     Enabled   TXR Model D Download
6     Enabled   Card Error Record Wraparound
7     Disabled  Card Test After Failure
8     Disabled  Download From Remote StrataView
9     Disabled  Logging of conn events in local event log
10    Disabled  Logging of conn events in SV+ event log
11    Disabled  Logging SVC Connection Events
12    Disabled  Force Download From a Specific IP address
13    Disabled  CDP WinkStart Signalling

This Command: cnffunc


Continue? y

Index Status    Function

14    Enabled   Logging of Bus Diagnostic Events in local event log











This Command: cnffunc


Enter index:
```

Table 3-10 cnffunc–Index Parameters

Index	Function	Description	Default
1	Automatic CLN/TRK Loopback Test on Local/Remote Alarms	A remote-end loopback is automatically set up on a failed line or trunk. Used to check the integrity of the back card alarm circuitry.	enabled
2	FDP Loopback button	For an IGX node, enables loopback button on SDP or HDM card faceplate. (Disable it to prevent accidental operation by contact.)	enabled
3	User Command Logging	All commands entered by the user is entered in the system log when enabled. When disabled, system log does not become so large but there is no audit trail of operator commands kept.	enabled

Index	Function	Description	Default
4	Automatic Card Reset on Hardware Error	The controller card (BCC, NPC, or NPM) issues a hardware reset to a card when firmware detects an error during normal operation. This allows the node to return a card to service after a firmware error.	enabled
5	TXR Model D Download	(Not used)	enabled
6	Card Error Record Wraparound	Allows the log entry for each card error to wrap for long entries. When disabled, only first ten failures are logged.	enabled
7	Card Test After Failure	Indicates card function selftests and background test should continue to be executed after a card has been declared as failing these tests.	disabled
8	Download from Remote WAN Manager NMS	Allows a node to download software images from a WAN Manager not directly connected to the node.	disabled
9	Logging of connection events in local event log	All connection event messages are entered in the system log when enabled. When disabled, system log does not become so large but there is no audit trail of connection events kept	disabled
10	Logging of connection events in WAN Manager event log	All connection event messages are entered in the WAN Manager event log when enabled. When disabled, WAN Manager event log does not become so large but there is no audit trail of connection events kept	disabled
11	Force Download From a Specific IP address	Forces the node to only download software images from a WAN Manager with the specified IP address.	disabled
12	Logging of SVC connection events	All SVC connection event messages are entered in the local event log when enabled. When disabled, local event log does not become so large but there is no audit trail of SVC connection events kept	disabled
13	CDP WinkStart Signalling	Toggles WinkStart signaling on the CDP.	disabled
14	Logging of Bus Diagnostic Events in local event log	All Bus Diagnostic event messages are entered in the local event log when enabled. When disabled, local event log does not become so large but there is no audit trail of Bus Diagnostic events kept	enabled
15	Automatic Card Reset after Burnfw for CBI Cards	While the network is running Release 9.1, use the **cnffunc** command option 15 to disable the **Automatic Card Reset after Burnfw for CBI cards** option. (By default, this option is enabled.) You need to perform this step so that you can burn the UXM firmware revision on the flash and delay execution of the new firmware revision until the card is reset with the **resetcd** command. After the UXM at both ends of the trunk are burned with the new firmware revision, you can reset the UXM cards at the same time so that the new ATM Forum Compliant protocol is invoked at both ends of the trunk at the same time. It is important that you perform this step, because a node potentially may be not be reached if this is an IMA trunk, and it is the only trunk connected to that remote node. Also note that if an IMA trunk is not used within the Release 9.1 network, then you do not need to perform this step. Then upgrade all UXM cards in the Release 9.1 network with UXM firmware model B.	Enabled/ Disabled [Default: Enabled]

cnfname

Specifies the name by which a node is known within the network. It may be changed at any time. The new node name is automatically distributed to the other nodes in the network. Node names are case sensitive. For example, an upper-case “A” is not considered to be the same as a lower-case “a”. Duplicate names are not allowed in the same network. Node names may be configured from within a job sequence. If the node name is changed and the corresponding name in the job is not changed, the job will not function properly. In the following situations, the **cnfname** command cannot be executed:

- Another node is attempting to change the network topology by adding or deleting a trunk.
- Another node is notifying all nodes that it has been renamed. Another node is currently adding or deleting a channel connection in the network with the **addcon** or **delcon** commands.
- There is an unreachable node in the network.
- The name chosen is already being used for another node in the network.

Full Name

Configure node name

Syntax

cnfname <nodename>

Related Commands

cnfterm, **cnfprt**, and **window**

Attributes

Privilege	1
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`cnfname` alpha

Description

The name changes to “alpha.” The network topology screen displays indicating the new name. See the **dspnw** description for more information on the network topology screen.

System Response

```
alpha          TRM   YourID:1        IGX 8410     9.2    Aug. 15 1998 12:02 PST


NodeName    Alarm  Packet Line        Packet Line        Packet Line
alpha              10- 7/beta         14- 13/beta
beta        MAJOR  7- 10/alpha        9- 10/gamma        13- 14/alpha
                   15- 15/gamma       20- 11/gamma
gamma       MAJOR  10- 9/beta         11- 20/beta        15- 15/beta










Last Command: cnfname alpha


Next Command:
```

cnfprt

Configures the printing function. To obtain local or remote printing at a node, a printer must connect to the AUX PORT. Also, the configuration must include the correct baud rate and printer type for the port. Use the **cnfterm** and **cnftermfunc** commands to do this.

The **cnfprt** and **cnftermfunc** commands interact. If the auxiliary port on the node is configured for either an External Device Window or the Network Management Log, a "local" printing configuration automatically changes to "no printing." Printing is not possible because the auxiliary port is being used for another purpose.

Establishing a virtual terminal connection with a node does not affect the printing location established for the node that initiates the virtual terminal connection. For example, if node *alpha* is configured so that all alpha information goes to a printer at node *beta* and if alpha establishes a virtual terminal connection with node *gamma*, the results of print commands entered on the *alpha* keyboard still print at *beta*. Furthermore, this occurs regardless of the printing location configured for node *gamma*.

Full Name

Configure printing functions

Syntax

cnfprt <mode> <remote node name>

Related Commands

cnfterm, **dsptermfunc**

Attributes

Privilege	1–6
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
cnfprt
```

Description

Change the configured printing.

System Response

```
alpha          TRM   YourID:1        IGX 8410     9.2    Aug. 15 1998 13:17 PST


Printing Mode

Remote Printing at beta
Local Printing
No Printing









This Command: cnfprt


Select Local (l), Remote (r), or None (n):
```

Table 3-11 cnfprt–Parameters

Parameter	Description
mode	Specifies the printing mode. Enter “L” for local printing, “R” for remote printing, and ‘n’ for no printing.
remote node name	Specifies the remote node whose printer is used for print commands issued by a user who is physically logged on to this node. This option is valid only when remote printing has been selected. A remote node is one within the domain, but not the node where the command is entered.

cnfterm

Configures data transmission parameters for the control and auxiliary ports. The IGX and BPX nodes support two EIA/TIA-232 serial ports on the upper bus expansion card. The top port is called the Control Terminal port. The lower port is called the Auxiliary Port (AUX). Parameters can vary with the equipment connected to the port. The control port may connect to a control terminal, a direct-dial modem, or an external EIA/TIA-232 device. The auxiliary port may connect to either a printer or an external EIA/TIA-232 device. After you have set the data transmission parameters for a port, use the superuser command **cnftermfunc** to specify the equipment attached to the port. The configuration parameters must match the equipment physically attached to the port.

Full Name

Configure terminal port

Syntax

cnfterm <a/c> <baud> <parity> <num_data_bits> <num_stop_bits>

Related Commands

cnfterm, **cnfprt**, **window**

Attributes

Privilege	1–6
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`cnfterm`

Description

Configure an auxiliary control port.

System Response

```
alpha          TRM   YourID:1        IGX 8430     9.2    Aug. 15 1998 11:58 PST


Control port                         Auxiliary port

Baud Rate:          1200             Baud Rate:          9600

Parity:             None             Parity:             None
Number of Data Bits: 8               Number of Data Bits: 8
Number of Stop Bits: 1               Number of Stop Bits: 1
Output flow control: XON/XOFF        Output flow control: XON/XOFF
Input flow control:  XON/XOFF        Input flow control:  XON/XOFF
Use DTR signal:     Yes              DTR signal:         Yes





This Command: cnfterm


Select Control port (c) or Auxiliary port (a):
```

Table 3-12 cnfterrm–Parameters

Parameter	Description
a/c	Specifies the port to be configured, where “a” means auxiliary port, and “c” means control port.
baud rate	Specifies the baud rate. The rates are 1200, 2400, 4800, 9600, and 19200 bps.
parity	Specifies parity checking for character transmission to and from the port. Valid parity choices are “E” for even parity, “O” for odd parity, and “N” for no parity.
data bits	Specifies the number of bits to be sent for each transmitted character and the number of bits to be expected for each received character. A “7” indicates 7 bits for each character. An “8” indicates 8 bits for each character.
stop bits	Specifies the number of stop bits to be sent with each transmitted character and the number of stop bits to be expected with each received character. A “1” indicates one stop bit with each character; a “2” indicates two stop bits with each character.
output flow control	Specifies the output flow control. An “X” specifies XON/XOFF flow control; an “N” specifies no flow control.
input flow control	Specifies input flow control. An “X” specifies XON/XOFF flow control; an “N” specifies no flow control.
cts flow control	Configures cts flow control. An “X” specifies XON/XOFF flow control; an “N” specifies no flow control. This parameter should be turned off if working with modems on a BPX node.
use DTR	Specifies whether the node requires DTR to be asserted to allow or maintain a Login. A “Y” causes the node to require the presence of DTR before allowing a login. A “N” causes the node to ignore DTR.

cnftime

Sets the time for the entire network. The time is broadcast to all nodes in the network. The time displayed at each node is adjusted for the node's time zone. (See the **cnftmzn** command for more information.) This command can only be executed if the date for the network has already been configured using the **cnfdate** command. If hour, minute, or second is not entered, the current value is kept.

Full Name

Configure time

Syntax

`cnftime` <hour> <minute> <second>

Related Commands

cnfdate, **cnftmz**

Attributes

Privilege	1
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`cnftime` 19 31 00

Description

Configure time to 7:31 in the evening. The system displays two warning prompts before it changes the time.

```
pubsigx1       TN    SuperUser       IGX 8430    9.2       Sep. 5 1998  19:31 GMT












This Command: cnftime 19 31 00

Warning: Changing time of day affects StrataView statistics timestamps
Hit RETURN to change clock, DEL to abort
```

Table 3-13 cnftime–Parameters

Parameter	Description
hour	Sets the time for the entire network. The time is broadcast to all nodes in the network. The time displayed at each node is adjusted for the node's time zone. (See the **cnftmzn** command for more information.) This command can only be executed if the date for the network has already been configured using the **cnfdate** command. If hour, minute, or second is not entered, the current value is kept.
min	Specifies the current minute. The range is 0-59.
sec	Specifies the current second. The range is 0-59.

cnftmzn

Configures the time zone for the node. Configuring the time zone for a node ensures that the node's time is correct for the local area regardless of the node at which the network date and time are set. Once configured, the time zone for the node is saved in battery-backed memory. After a power failure, a node's date and time are restored if at least one other node in the network has the current time and date.

Full Name

Configure time zone

Syntax

cnftmzn <timezone | g+/- *hours*>

Related Commands

cnfdate

Attributes

Privilege	1
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example

`cnftmzn` pst

Description

Configures the time zone to Pacific Standard Time.

System Response

```
alpha          TRM   YourID:1        IGX 8420  9.2    Aug. 15 1998 13:19 PST













Last Command: cnftmzn pst


Next Command:
```

Table 3-14 cnftmzn–Parameters

Parameter	Description
time zone	• gmt (or g) Greenwich Mean Time • cst (or c) Central Standard Time • est (or e) Eastern Standard Time • mst (or m) Mountain Standard Time • pst (or p) Pacific Standard Time • yst (or y) Yukon Standard Time • cdt Central Daylight Savings Time • edt Eastern Daylight Savings Time • mdt Mountain Daylight Savings Time • pdt Pacific Daylight Savings Time • ydt Yukon Daylight Savings Time
hours from Greenwich Mean Time (GMT)	Specifies the difference in hours between local time and Greenwich Mean Time. The range is from -12 to +12 hours. Instead of entering the time zone, you can enter the hours from Greenwich Mean Time. For example, instead of entering pdt for Pacific Daylight Time, you could enter g-7, which is Greenwich Mean Time minus 7 hours.

delalmslot

Disables the ARC (IPX) or ARM (IGX) alarm indicators and ARI external alarms. See the **addalmslot** description for more information on ARC/ARM alarm relays and adding alarm slots.

Upon receiving the command, the system places the alarm card set in the standby state and displays the current alarm status.

Full Name

Delete an alarm slot

Syntax

delalm <slot number>

Related Commands

addalmslot, **dspalms**

Attributes

Privilege	1–4
Jobs	No
Log	Yes
Node	IGX
Lock	Yes

Example 1

`delalmslot` 11

Description

Disable the alarm indicators on the ARM card set in slot 11. (The system subsequently displays alarm status.)

System Response

```
pubsigx1       TN    SuperUser       IGX 8430    9.2       July 16 1998 02:09 GMT

Alarm summary   (Configured alarm slots: None)
Connections Failed:       None
Groups Failed:            None
TRK Alarms:               None
Line Alarms:              None
Cards Failed:             None
Missing Cards:            None
Remote Node Alarms:       1 Minor
Remote Domain Alarms:     None

Routing Network Alarms:   None

                                            Cabinet Fan(s) Failed

FastPAD Node Alarms:      None

Last Command: delalmslot 11


Next Command:
```

Table 3-15 delamslot–Parameters

Parameter	Description
slot number	Specifies the slot number of the alarm card set to activate.

delcdred

The **delcdred** command disables card redundancy for the card set in the specified primary slot number. If the secondary card slot is being used as the active slot at the time you use the **delcdred** command, the system attempts to switch back to the primary slot. The substitution takes place only if the primary slot has a complete set of cards and the cards are in a Standby or a Standby-F state (not if they are Failed). See the **dspcds** description for information on card states.

When you issue the **delcdred** command, it always completes. If the primary card is incomplete, control will still be given to the primary card.

Because YRED (Y redundancy) could be considered a misnomer for the SONET APS two-slot case, the following new commands are new in Release 9.2 to support card redundancy:

- addcdred—same functionality as addyred
- dspcdred—same functionality was dspyred
- delcdred—same functionality as delyred
- prtcdred—same functionality as prtyred
- switchcdred—same functionality as switchyred

See the **addcdred** and **dspcdred** commands for more information on card and line redundancy for SONET APS (Automatic Protection Switching) 1+1.

Full Name

Delete redundant card

Syntax

delcdred <primary slot>

Related Commands

addcdred, **dspcdred**, **switchcdred**

Attributes

Privilege	1–4
Jobs	No
Log	Yes
Node	BPX
Lock	Yes

Example

`delcdred` 2

Description

Delete card redundancy for slot 2.

delshelf

Deletes an interface shelf from a tiered network. The identifier for an interface shelf is either the trunk number or the name of the shelf. Normally, you do not execute **delshelf** only at the BPX core switch shelf, but on the IGX/AF itself. The command **delshelf** has the single function of letting you turn off LMI if the trunk is not allowing communication. In contrast to the **deltrk** command, you can execute **delshelf** at any time if no connections terminate at the trunk.

In Release 9.2, when you use **delshelf** to remove an MGX 8850 interface shelf trunk from a BPX routing hub, or an SES interface shelf (or feeder) trunk from an IGX 8400 routing node, the Annex G signalling channel and IP relay programming for the MGX 8850 or SES interface shelf is removed.

Full Name

Delete an interface shelf.

Syntax

delshelf <trunk> | <shelf-name>

Related Commands

addshelf, **dspnode**

Attributes

Privilege	1
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`delshelf` 4.1

Description

Delete shelf trunk 4.1 on a BPX.

System Response

```
nmsbpx23       TN    SuperUser       BPX 8600    9.2  Aug. 16 1998 13:26 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 1.3     AXIS240   AXIS      OK
11.2     A242      AXIS      OK










Last Command: delshelf A241

Shelf has been deleted
Next Command:
```

Table 3-16 delshelf–parameters

Parameter	Description
trunk or shelf name	Specifies the slot and port number of the trunk or the name of the interface shelf.

delyred

This command disables Y redundancy for the card set in the specified primary slot number. If the secondary card slot is being used as the active slot at the time you use the **delyred** command, the system attempts to switch back to the primary slot. The substitution takes place only if the primary slot has a complete set of cards and the cards are in a Standby or a Standby-F state (not if they are Failed). See the **dspcds** description for information on card states. See the **addyred** and **dspyred** commands for more information on Y-cable redundancy.

When you issue the **delyred** command, it always completes. If the primary card is incomplete, control will still be given to the primary card.

Full Name

Delete Y-cable redundancy

Syntax

delyred <primary slot>

Related Commands

addyred, **dspyred**, **prtyred**

Attributes

Privilege	1–4
Jobs	No
Log	Yes
Node	IGX, BPX
Lock	Yes

Example

`delyred` 16

Description

Disable Y-cable redundancy at slot 16.

dspasm

Displays BPX node alarms that, when active, produce an external alarm output (relay closure). These alarms are associated with powering and cooling the node as well as a statistics count. For example, a minor alarm is generated when a fan speed drops below 2000 rpm. Since the single ASM card is always located in slot 15, you do not need to enter a card slot for this command. To configure the ASM alarms, use **cnfasm** (a superuser command)**.**

Full Name

Display ASM card

Syntax

dspasm

Related Commands

cnfasm

Attributes

Privilege	1
Jobs	No
Log	No
Node	BPX
Lock	Yes

Example

`dspasm`

Description

Display the ASM card parameters.

System Response

```
D1.jea         TRM   SuperUser       BPX 8620    9.2    Aug. 30 1998 12:24 GMT

ASM Status:             Active          ASM Alarms
Statistics count:       7               Fan #1 RPM out of range
Statistics timeouts:    0               Fan #2 RPM out of range
Cabinet temperature:    21 C            Fan #3 RPM out of range
Power voltage A/B:      0.0 / 0.0 V

PSU  Ins Type Rev SerNum Failure
 A    N  N/A  N/A   N/A    N/A
 B    N  N/A  N/A   N/A    N/A

FAN    1    2    3
     0000 0000 0000 RPM




Last Command: dspasm


Next Command:
```

dspcd

Displays the status, revision, and serial number of a card. If a back card is present, its type, revision, and serial number appear. The displayed information can vary with different card types.

The **dspcd** screen indicates whether the card supports IMA Compliance. If the card does not support IMA compliance, then the screen will not display any IMA support.

The **dspcd** command displays the SONET APS (Automatic Protection Switching) architecture supported on the card, slot # of redundant back card (if there is a redundant back card), and the reasons for the card's APS mismatch.

In this release, the **dspcd** screen indicates whether the front card supports the Lead State Trap for High/Low Speed Data Modules (HDM/LDM) on IGX.

If SONET APS is configured (which allows switching of SONET lines from the active line to a standby line to provide hardware line redundancy), the **dspcd** command displays the front and back card SONET APS attributes. For the front card, APS attributes are displayed if the front card supports one of the following:

- APS firmware
- APS 1+1 hardware
- APS 1:1 hardware

For the back card, if the back card is a redundant back card, the slot number of the redundant backward is displayed. Also, the reasons for the card's APS mismatch are displayed also.

The **dspcd** command is a single-page display. (Note that the **dsplogcd** command shows all the ports and trunks on a given slot. The second page of the **dsplogcd** command shows each port and interface type corresponding to that *slot.port*.)

In support of feature mismatch checking in Release 9.2, the **dspcd** command provides mismatch information for the specified card.

Full Name

Display card

Syntax

`dspcd` <slot number>

Related Commands

dncd, **dspcds**, **resetcd**, **upcd**

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

`dspcd` 6

Description

The card is the trunk version of the ALM. The “B” next to Revision shows the card set is an ALM/B.

System Response

```
IGX8430          TN    SuperUser       IGX 8430    9.2  Oct. 12 1998 18:44 PST

Detailed Card Display for ALM in slot 6

Status:          Active
Revision:        B0310
Serial Number:   289417
Backplane Installed
Backcard Installed
  Type:          UAI-T3
  Revision:      HN
  Serial Number: 242007



Last Command: dspcd 6


Next Command:
```

Example 2

dspcd 5

Description

Display information on the card in slot 5. The card is a UVM capable of CAS-switching.

```
wx175          TN    SuperUser       IGX 8420    9.2 Sep. 23 1998 22:31 PST

Detailed Card Display for UVM in slot 5

Status:          Standby               (Front Card Supports CAS-switching)
Revision:        B0203
Serial Number:   336878
Integrated Echo Canceller
  Channels:      31
Backplane Installed
Backcard Installed
  Type:          E1-2
  Revision:      AB
  Serial Number: 336728




Last Command: dspcd 5


Next Command:
```

Example 3

dspcd 7

Description

Display information on the card in slot 7. The card is a UXM with an OC-3 back card.

System Response

```
sw224          TN    SuperUser       IGX 8430    9.2    Aug. 27 1998 16:01 GMT
Detailed Card Display for UXM in slot 7
Status:          Standby
Revision:        EXB
Serial Number:   190212
Backplane Installed
Backcard Installed
  Type:          OC-3
  Revision:      AH
  Serial Number: 12345
  Ports:         4
  Line Mode:     SMF



Last Command: dspcd 7


Next Cand:
```

Example 4

dspcd 5

Description

Display information on the card in slot 5. The card is a UXM with an E1 back card.

```
sw224          TN    SuperUser       IGX 16    9.0.n2    Aug. 27 1997 16:07 GMT

Detailed Card Display for UXM in slot 5

Status:          Active                (Front Card Supports SIW)
Revision:        AAB                   (Front Card Supports Cell Forwarding)
Serial Number:   190208                (Front Card with GW installed)
Backplane Installed
Backcard Installed
  Type:          E1-IMA
  Revision:      EW
  Serial Number: 23456
  Ports:         8
  Line Mode:




Last Command: dspcd 5



Next Command:
```

Example 5

dspcd 5

Description

Display information on the card in slot 11. The card is a 2-port BME card with an OC-12 back card.

```
sw60          TN    SuperUser       BPX 15    9.2      Feb. 5 1997  11:37 GMT

          Status:          Active
          Revision:        K0811
          Serial Number:   324027
          Queue Size:      228300
          Support:         8129 Chns
           2 Pts, OC-12

          Backcard Installed
           Type:          LM-BXM
           Revision:      P02
           Serial Number: 240255
           Supports: 2 Pts, OC-12, SMF Md

          Last Command: dspcd 11
```

Example 6

dspcd 5

Description

Display information on the card in slot 11. The card is a 2-port BME card with an OC-12 back card. Note that the second page of dspcd display shows each port and interface type corresponding to that card slot.

```
sw98           TN    SuperUser     BPX 8600    9.2.r3      Feb. 5 1998  11:37 GMT

          Status:          Active
          Revision:        CW07
          Serial Number:   abcdef
          Fab Number:      ----
          Queue Size:      131000
          Support:         FST, 16256 Chns, 4 Ports OC-3


          Backcard Installed
           Type:          LM-BXM
           Revision:      BA
           Serial Number: 686687
           Supports: 4 Pts, OC-3



          Last Command: dspcd 11


sw98           TN    SuperUser       BPX 15    9.2.r3      Feb. 5 1998  11:37 GMT


          Interface Details for BXM-OC-3 in slot 11
          3.1: VSI only Trunk - (256 user chans)
          3.2: Autoroute/VSI Trunk (512 user chans)
          3.3:  ATM Port (UNI/NNI) (2048 user chans)
          3.4:  Virtual Trunks (1..N)



          Last Command: dspcd 11
```

Example 7

`dspcd 5`

Description

Display card for BXM-T3 in slot 5, which shows that VSI version 2 (VSI V2) is supported on the card.

System Response

```
sw58           TN    StrataCom       BPX 8600  9.2.00 June 25 1998 13:40 GMT

Detailed Card Display for BXM-T3 in slot 5
Status:          Standby
Revision:        ED04
Serial Number:   693903
Fab Number:      28-2218-02
Queue Size:      131000
Support:         FST, 8 Pts,T3,VcS, VSI V2
Chnls:16320
PG[1]:1,2,3,4,5,6,7,8,
Backcard Installed
  Type:          LM-BXM
  Revision:      BA
  Serial Number: 692993
  Supports: 12 Pts, T3/E3

Last Command: dspcd 5
```

Example 8

`dspcd 4`

Description

Enter the **dspcd** command on card slot 4 (for example, to check the port group maximum that can be entered for the *maxvsilcn* parameter of the **cnfrsrc** command when configuring VSI resources). In this example, the maximum value for a port group is 7048.

System Response

```
n4            TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:40 PST

Detailed Card Display for BXM-155 in slot 4

Status:          Active
Revision:        CD18
Serial Number:   693313
Fab Number:      28-2158-02
Queue Size:      228300
Support:         FST, 4 Pts,OC-3,Vc
Chnls:16320,PG[1]:7048,PG[2]:7048
PG[1]:1,2,
PG[2]:3,4,

Backcard Installed
  Type:          LM-BXM
  Revision:      BA
  Serial Number: 688284
  Supports: 8 Pts, OC-3, MMF Md

Last Command: dspcd 4

Next Command:
```

Example 9

`dspcd 4`

Description

Enter the **dspcd** command on card slot 4 to show support for Partial Packet Discard (PPD) due to policing on the ingress direction. Only BXM cards with the RCMP (Routing Control Monitoring and Policing) chip support PPD on policing.

System Response

```
bpx04     TN    StrataCom     BPX 8620  9.2.30   Apr. 8 1999 12:00 GMT

Detailed Card Display for BXM-155 in slot 4
Status:          Active
Revision:        DD14                 Backcard Installed
Serial Number:   772850               Type:        LM-BXM
Fab Number:      28-2158-02           Revision:     BB
Queue Size:      228300               Serial Number: 649646
Support: 4 Pts, OC-3, FST, VcShpSupp: 4 Pts,OC-3,SMF,RedSlot:NO
Support: VT, ChStLv 1, VSIlvl 2
Support: APS(FW)
Support: LMIver 1, ILMIver 1
Support: OAMLp, TrfcGen
Support: PPDPolic
#Ch:16320,PG[1]:8160,PG[2]:8160
PG[1]:1,2,
PG[2]:3,4,
#Sched_Ch:16384

Last Command: dspcd 12

Next Command:
```

dspcdred

Displays information for Y-cable pairings. A single slot can be specified, or all pairings are displayed when no slot is specified. Slot numbers appearing in high intensity indicate active card status. Front card, back card, and channel configuration conflicts appear in reverse video. A conflict occurs when the port interfaces are different for corresponding ports in a redundant slot pair. The output display contains the following information:

- First column (Slot) designates the slot of the displayed card.
- Second column (Slot Type) designates its status, Pri (primary) or Sec (secondary).
- Third column (Other Slot) designates the slot number of the associated Y-redundant card.
- Fourth column (Front Card) designates the type of card in the front slot.
- Fifth column (Back Card) designates the type of card in the back slot.

Remaining columns (Channel Configuration) describe the channel configurations when appropriate.

Full Name

Display redundant cards.

Syntax

dspcdred [slot]

Related Commands

addyred, **delyred**, **prtyred**

Attributes

Privilege	1–4
Jobs	No
Log	No
Node	BPX
Lock	No

Example 1

`dspyred`

Description

Display card redundancy for cards in slots 2 and 3.

System Response

```
beta           TRM   YourID:1        BPX 8620    9.2    Aug. 15 1997 14:27 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
2    Pri    3   BXM    LM-BXM
3    Sec    2   BXM    LM-BXM









Last Command: dspcdred 2 3


Next Command:
```

dspcds

Displays the cards in a shelf, front and back, with their type, revision, and status. For front and back card sets, the status field applies to the cards as a set. A letter “T” opposite a card indicates that it is running self-test. A letter “T” opposite a card indicates that it has failed a test. If lines or connections have been configured for a slot, but no suitable card is present, the display will list the missing cards at the top of the screen. If a special backplane is installed or if a card was previously installed, empty slots are identified as “reserved.”

For a two-shelf node, the screen initially displays only the upper shelf with a “Continue?” prompt. Typing “y” to the prompt displays the cards in the lower shelf. The command **dspcds** followed by the letter “L” (for lower shelf) displays card status for just the lower shelf. For an IGX 8410 node, the card information appears in only the left column. The status and update messages are as follows:

- Active — Card in use, no failures detected.
- Active—F — Card in use, failure(s) detected.
- Active—T — Card active, background test in progress.
- Active—F-T — Card active, minor failures detected, background test in progress.
- Standby — Card idle, no failures.
- Standby—F — Card idle, failure(s) detected.
- Standby—T — Card idle, background test in progress.
- Standby—F-T — Card idle, failure(s) detected, background test in progress.
- Failed — Card failed.
- Down — Card downed by user.
- Down—F — Card downed, failure(s) detected.
- Down—T — Card downed, failure(s) detected, background test in progress.
- Mismatch — Mismatch between front card and back card.
- Update * — Configuration RAM being updated from active control card.
- Locked* — Old software version is being maintained in case it is needed.
- Dnlding* — Downloading new system software from the active PCC adjacent node of from WAN Manager.
- Dnldr* — Looking to adjacent nodes or WAN Manager for either software to load or other software needs you have not specifically requested.
- Program — Occurs when new firmware is being burned on the card.

In the preceding messages, an asterisk (*) means an additional status designation for BCC, NPC, or NPM cards. “F” flag in the card status indicates that a non-terminal failure was detected. Cards with an “F” status are activated only when necessary (for example, when no other card of that type is available). Cards with a “Failed” status are never activated.

The “reserved for” logic in Release 9.2 reserves the slot for a BXM if SONET APS (Automatic Protection Switching) has been configured on the slot.

To support the Hitless Rebuild feature in Release 9.2, after a switchover has occurred and the standby updates are about to begin, the dspcds command will show the standby processor card as missing temporarily. This is a result of the delay in performing the full rebuild on the standby processor, which is necessary as part of the hitless rebuild sequence.

Following any processor card switchover, the new standby will rebuild, preserving the critical databases needed for a hitless rebuild. When database updates can start, the standby will rebuild again doing a normal standby rebuild. If there is a failure on the new active card that causes it to switch back before updates can start, the card taking over will do a hitless rebuild. Under most conditions, the second switchover will not be necessary, and a full rebuild will be done on the standby processor. As this process begins, the standby card will briefly appear to be missing.

In support of the Hitless Rebuild feature, there is no change directly to the user command **dspcds.** However, after a switchover has occurred and the standby updates are about to begin, the dspcds command will show the standby processor card as missing temporarily. This is a result of the delay in performing the full rebuild on the standby processor, which is necessary as part of the hitless rebuild sequence.

Following any processor card switchover, the new standby will rebuild preserving the critical databases needed for a hitless rebuild. When database updates can start, the standby will rebuild again doing a normal standby rebuild. If there is a failure on the new active card that causes it to switch back before updates can start, the card taking over will do a hitless rebuild. Under most conditions, the second switchover will not be necessary, and a full rebuild will be done on the standby processor. As this process begins, the standby will briefly appear to be missing.

Full Name

Display cards

Syntax

dspcds [l]

Related Commands

dncd, **dspcd**, **resetcd**, **upcd**

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

dspcds

Description

Display status on all cards.

System Response

```
IGX8430          TN    SuperUser       IGX 8430    9.2       Oct. 12 1998 18:39 PST



   FrontCard  BackCard                          FrontCard  BackCard
   Type  Rev  Type     Rev  Status              Type  Rev  Type     Rev  Status
1  NPM   A0205              Active-T         9  Empty universal backplane
2  Empty reserved for NPM                    10 Empty universal backplane
3  FRM   ESP  FRI-T1   AC   Active           11 ALM   B0305UAI-T3   HN   Active
4  Empty universal backplane                 12 Empty
5  UXM   AA09 E1-IMA   EW   Active           13 FRM   EEV  FRI-T1   AL   Standby
6  ALM   B0310UAI-T3   HN   Active           14 BTM   BFF  BTM-T3   P02  Standby
7  UXM   EX09 OC-3      AH   Standby          15 NTM   FHE  T1       AL   Standby
8  Empty universal backplane                 16 CVM   AFF  T1       AK   Active




Last Command: dspcds


Next Command:
```

Example 2

dspcds l

Description

Display status of cards on the lower shelf of an IPX 32 node (the option “l” means “lower”).

System Response

```
beta           TRM   YourID:1        IPX 8430    9.2    Aug. 15 1998  14:37 MST

Missing Cards: 1 ATM, 1 T3

   Front Card  Back Card    Front Card    Back  Card
   Type  Rev   Type  Rev    Status Type   Rev   Type    Rev   Status
17 PCC   HDB   Standby      25      SDP   BA    RS232   AK    Active-T
18 Empty  26   SDP  BF                          RS232   AK    Standby-F
19 FRP   DFB   FRI-V35 BC   Active-F 27   Empty
20 ATM   HM03  Empty        Failed   28   Empty
21 Empty  29   Empty
22 CDP    AAB  Empty        Unavail  30  Empty
23 Empty  31   Empty
24 Empty reserved for SDP           32  Empty



Last Command: dspcds l


Next Command:
```

Example 3

dspcds

Description

Display status of cards on a BPX 16 node. The 2 port BME card with OC-12 interface is in slot 11.

System Response

```
sw60           TN    SuperUser       BPX 15    9.2      Feb. 5 1997 11:36 GMT
Missing Cards: 1 BCC

   FrontCard  BackCard                         FrontCard  BackCard
   Type   Rev  Type     Rev  Status             Type     Rev  Type      Rev  Status
1  BNI-T3 CCF  T3-3     BE   Active        9  BNI-155   BDK  MMF-2     CM   Standby
2  Empty                                   10 Empty
3  ASI-T3 BJF  T3-2     AA   Standby       11 BME-622   K08  11LM-BXM P02AB Active
4  ASI-E3 BMJ  E3-2     BE   Standby       12 ASI-155   BDK  MMF-2     AB   Standby
5  BNI-E3 CMF  E3-3     EY   Standby       13 Empty
6  Empty                                   14 Empty
7  BCC   BWF   LMBCC    AC   Active        15 ASM   ACA  LMASM    AC   Active
8  Empty reserved for Card

Last Command: dspcds

Next Command:
```

Table 3-17 dspcds–Parameters

Parameter	Description
l	Directs the system to display status of the cards on just the lower shelf of an IGX 32 node.

dspctrlrs

Use the **dspctrlrs** command to display the VSI controllers, such as an PNNI SES controller, on a BPX node. The **dspctrlrs** command lists the controller id, the partition the controller uses, the trunk/interface a controller is attached to, the controller type (always a VSI controller), the interface type (AAL5, VSI (Label Switching), or MGX 8220 (formerly called AXIS) interface shelf, and the name of the controller/entity that the controller exists on (that is, node name, equipment name).

Displays all the VSI controllers on a node, such as a BPX node. Possible VSI controllers added to a node might be a PNNI ESP (Extended Services Processor) controller. (Note that you use addshelf and delshelf to add and delete a VSI controller such as a Label Switch Controller to a BPX node.)

You can also the **dspnode** command to display the VSI controllers on a BPX node.

Full Name

Displays all VSI controllers, for example, such as PNNI SES, on a BPX node.

Syntax

dspctrlrs <slot.port><controller name string><partition_id><controller_id>

Related Commands

addctrlr, cnfctrlr, delctrlr, dspnode

Attributes

Privilege	1
Jobs	Yes
Log	Yes
Node	BPX
Lock	Yes

Example 1

```
dspctrlrs
```

Description

Display VSI controllers on BPX node sw237.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.a3    June 16 1999 05:04 PST

                   BPX 8620 VSI controller information

Ctrl Id  Part Id      Ctrl VC            Trunk  Ctrlr Type   Intfc Type   Name
                   VPI   VCIRange
   1        1       1     20 - 34        4.1   VSI          VSI          VSI
   2        1       0     40 - 54       13.2   VSI          AXIS         SIMFDR0





Last Command: dspctrlrs
```

dsplancnf

Displays the addresses and configuration for the LAN Ethernet. The configuration fields shows the type of network capability and it is ready or unavailable. The **dsplancnf** display contains the following address fields:

Table 3-18 LAN Configuration Address Fields

<IPAdd>	Specifies the Internet address of the node used in the TCP/IP protocol.
<IP subnet mask>	Specifies a 32-bit mask that contains information about the bit lengths of the subnet ID and host ID address fields. The format of this field uses 1s for the subnet ID field and 0s for the host ID address field as defined in the TCP/IP protocol. The default value (in decimal notation) is 255 255 255.0. This mask denotes both subnet ID and host ID fields as 8-bit fields.
<Max. LAN Transmit Unit>	BPX only: typical amount is 1500 bytes.
<TCPServicePort>	Specifies the node's service point used by the transmission control protocol (TCP).
<GatewayIPAddr>	Specifies the Internet gateway address
Type	List of socket types (for example, TCP, UDP, and SNMP) that are open (in READY state) for communication between the node and the LAN. In the system response shown, the TCP socket is no longer used by switch software, indicated by the UNAVAIL state. The TimeHndlr (or Daytime) socket is related to TFTP. It lets an external node retrieve the day and time from the switch. The Tunneling socket is used for communication between a BPX and an INS (Intelligent Network Server).
State	State of communication socket between the node and the LAN. READY indicates that the socket is open for communication between the node and the LAN. UNAVAIL indicates that the socket is not available for communication between the node and the LAN.

Full Name

Display LAN interface configuration

Syntax

dsplancnf

Related Commands

cnflan (a superuser command)

Attributes

Privilege	1–5
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

dsplancnf

Description

Display the LAN configuration for the current node.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2    June 11 1998   13:23 GMT

Active IP Address:                      204.179.31.104
IP Subnet Mask:                         255.255.255.0
IP Service Port:                        5120
Default Gateway IP Address:             None
Maximum LAN Transmit Unit:              1500
Ethernet Address:                       00.C0.43.00.21.F0

Type      State          Type      State
LAN       READY          TUNL      READY
TCP       UNAVAIL
UDP       READY
Telnet    READY
TFTP      READY
TimeHdlr  READY
SNMP      READY

Last Command: dsplancnf


Next Command:
```

dsplmistats

Displays Annex G LMI statistics for the trunk that connects an IGX/AF interface shelf to the BPX core switch shelf. To execute this command from the access shelf itself, you must telnet to the IGX/AF. The **dsplmistats** command can provide information to help you analyze problems that may arise while you set up a tiered network.

Full Name

Display Annex G LMI statistics

Syntax

dsplmistats (parameters depend on the type of node)

Note On an access shelf, the **dsplmistats** command takes no arguments. On an IGX node, **dsplmistats** requires a trunk number. On a BPX node, **dsplmistats** requires the slot and port number.

Related Commands

none

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX/AF, BPX
Lock	No

Example

`dsplmistats`

Description

Display the LMI statistics for the trunk attached to the hub.

System Response

```
batman              SuperUser       IGX/AF    9.2      Nov. 30 1998 18:04 PST

              Annex G  LMI Statistics for slot:1 port:1
VPI.VCI:       0.0                     Lmi enabled         Lmi polling enabled
Invalid Pdu      Rx:           0       Status Polling Timer (T396)    :    10
Invalid Pdu Len  Rx:           0       Status Enquiry Timer (T393)    :    10
Unknown Pdu Type Rx:           0       Max Status Enquiry Retry (N394):     5
Unknown IE Type  Rx:           0       Update Status Timer (T394)     :    10
Bad Transaction  Rx:           0       Max Update Status Retry (N395) :     5
Status           Rx:        1384       Spc Polling Timer              :     3
Status Enq       Tx:        1384       Spc Retry Timer                :     0
Status Enq       Rx:        1384       Spc Retry Counter              :     1
Status           Tx:        1384       Node Status Retry Timer        :     0
Status Ack       Rx:           8       Node Status Retry Counter      :     0
Update Status    Tx:           8       Node Status Polling Timer      :     2
Update Status    Rx:           8
Status Ack       Tx:           8

Last Command: dsplmistats


Next Command:
```

dspnds

Displays the name, type, and alarm status of all nodes within the network of the node executing the command. The remote node alarm is provided. You can use the **vt** command to reach the remote node and obtain the alarm information.

If a node is in alarm, its name is highlighted and the alarm type (major/minor), is displayed. A major alarm will be a flashing word. A junction node is identified with “Yes” printed under the Jct column.

Full Name

Display all nodes

Syntax

dspnds [+n | -p | -d | domain]

Related Commands

dspnw

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

dspnds

Description

Display the alarm status of all nodes within the network.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998  09:42 PST

NodeName Alarm
alpha    MAJOR
beta     MAJOR
gamma    MAJOR









Last Command: dspnds


Next Command:
```

Table 3-19 dspnds–Optional Parameters

Parameter	Description
+n	Specifies the node number. (Assigning a node number requires superuser privilege.)
-p	Specifies that the display include the type of controller card in the node. The types are BCC, NPM, and so on.
-d	Specifies that the display include the type of node for each named node. The type is either “IGX” or “BPX.”

dspnode

Displays a summary of the interface shelves.

The **dspnode** command can isolate the shelf where an alarm has originated. For example, when you execute **dspalms**, the display indicates the number of shelves with alarms but does not identify the shelves. Therefore, execute **dspnode** on the IPX/BPX core switch shelf to determine which interface shelf generated the alarm.

The first example shows a screen display with **dspnode** executed on a BPX node. The second example shows a screen with **dspnode** executed on an IGX/AF. When executed on an IGX/AF, **dspnode** shows the name of the IGX/BPX core switch shelf and the trunk number. Note that to execute a command from an IGX/AF itself, you must either telnet to the shelf or use a control terminal attached to the shelf.

You can also use the **dspnode** command to display the VSI controllers on a BPX node. In this release, you can display the control_VPI and control_VCI_start of the particular controller, as shown in Example 6.

In Example 4, the **dspnode** screen shows loopbacks on feeders to a BPX node. The BPX no longer sends any status updates to the feeder yet it continues to acknowledge any feeder LMI messages received.

If the BPX cannot communicate LMI messages to its feeders, then the LMI status at the feeders must be maintained to keep the connections "active" to their external devices. If the BPX hub is flooded with network messages, then LMI/ILMI communication with its feeders may be interrupted. LMI normally runs a keep-alive between the hub and feeder. If the keep-alive fails, then the other end changes the status of all connections to "failed". If the outage is only due to a network message flood, then it is desirable to override this mechanism to keep the connection status as "active".

Full Name

Display node

Syntax

dspnode

Related Commands

addshelf, **delshelf**, **dsptrks**

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	BPX, IGX, IGX/AF
Lock	Yes

Example 1

dspnode

Description

Display information about the interface shelves (executed on the IGX or BPX core switch shelf).

System Response

```
sw288          TN    SuperUser       BPX 8620    9.2.j2     Dec. 10 1998 15:09 GMT

                        BPX 8620 Interface Shelf Information

Trunk    Name       Type       Part ID    Ctrl ID    Alarm
 1.2     SW93AXIS   AXIS                             UNRCH
 1.3     SW77AXIS   AXIS                             MAJ
 3.1     sw92       TSC                              OK
 5.8     SIMFDR0    AAL5          -          -      OK




Last Command: dspnode


Next Command:
```

Example 2

dspnode

Description

Display information about the interface shelves (feeders) attached to IGX core switch shelf (executed on an IGX 8420). In this case, an SES (Service Expansion Shelf) communicates with the IGX routing hub over the AAL5 protocol.

System Response

```
oo1          TN    SuperUser       IGX 8420    9.2.zR    Dec. 10 1998 07:23 PDT

                        IGX Interface Shelf Information

Trunk    Name      Type      Alarm
 9.1     ases1     AAL5     OK






Last Command: dspnode


Next Command:
```

Example 3

dspnode

Description

Display information about the trunk to a BPX core switch shelf (executed on an BPX 8600).

System Response

```
                         BPX Interface Shelf Information

Trunk   Name    Type      Part Id    Ctrl Id   Alarm
 1.1    sww222  IGX/AF    -          -         UNRCH
10.3    VSI     VSI       1          1         OK
11.1    VSI     VSI       1          2         OK





Last Command: dspnode
```

Example 4

`dspnode`

Description

Displays all interface shelves attached to the node. The resulting screens should show trunk 4.1 as type VSI.

System Response

```
n4             TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:46 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 3.1     j6c       AXIS      MIN
 5.3     j5c       IPX/AF    MIN
 4.1     VSI       VSI       OK
 4.2     VSI       VSI       OK
 4.3     VSI       VSI       OK








Last Command: dspnode

Next Command:
```

Example 5

dspnode

Description

Display information about the loopbacks on feeders to the BPX node.

System Response

```
sazu       TN       StrataCom      BPX 8620    9.2         pr. 18 1998 11:11 GMT

BPX Interface Shelf Information

Trunk    Name      Type      Alarm
10.2     sw157     IPX/AF    MAJ  (L)






Last Command: dspnode

Next Command:
                                                                     Major Alarm
```

Example 6

dspnode

Description

Display information about the BPX 8620 interface shelf with this release enhancement that shows the controller's control_VPI and control_VCI_start.

System Response

```
-----------------------------------------------------------------------
sw237          TN    StrataCom       BPX 8620  9.2.30    June 16 1999 05:06 PST

                  BPX 8620 Interface Shelf Information

Trunk    Name      Type          Part Id   Ctrl Id       CntrlVC        Alarm
                                                      VPI   VCIRange
 4.1     VSI       VSI              1         1        1    20 - 34      OK
13.2     SIMFDR0   AXIS             1         2        0    40 - 54      OK




Last Command: dspnode
```

dsptermcnf

Displays the configuration for the control port and auxiliary port at a node. It includes all the asynchronous communications parameters that are specified by the **cnfterm** command.

Full Name

Display terminal port configurations

Syntax

dsptermcnf

Related Commands

cnfterm, **cnftermfunc** (a superuser command), **dsptermfunc**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

```
dsptermcnf
```

Description

Display the terminal port configuration data.

System Response

```
batman         TN    SuperUser       BPX 8620    9.2       Aug. 26 1997 02:55 PST


Control port                           Auxiliary port

Baud Rate:           9600              Baud Rate:           9600

Parity:              None              Parity:              None
Number of Data Bits: 8                 Number of Data Bits: 8
Number of Stop Bits: 1                 Number of Stop Bits: 1
Output flow control: XON/XOFF          Output flow control: XON/XOFF
Input flow control:  XON/XOFF          Input flow control:  XON/XOFF
CTS flow control:    No                CTS flow control:    Yes
Use DTR signal:      Yes               Use DTR signal:      Yes




Last Command: dsptermcnf


Next Command:
```

dsptermfunc

Displays the port functions configured by the **cnftermfunc** command.

Full Name

Display terminal port functions

Syntax

dsptermfunc

Related Commands

cnfterm, **cnftermfunc**, **dsptermcnf**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

```
dsptermfunc
```

Description

Display the terminal port configuration data. The highlighted or reverse video items are the currently selected options.

System Response

```
swstorm        TN    SuperUser       BPX 8620      9.2      Aug. 23 1997 09:42 PST


Control port                           Auxiliary port

1. VT100/StrataView                    1. Okidata 182 Printer
2. VT100                               2. Okidata 182 Printer with LOG
                                       3. VT100
                                       4. Alarm Message Collector
                                       5. External Device Window
                                       6. Autodial Modem







Last Command: dsptermfunc


Next Command:
```

dspprtcnf

Displays printing configuration for the node. The three printing modes, ‘remote’, ‘local’ and ‘no’ are listed and the currently selected mode is highlighted. If remote printing is selected, the node name where the remote printer is located also appears. If the name of the node is flashing, the node is unreachable.

The **dspprtcnf** command displays the current print configuration for the network where the command is entered.

Remote mode indicates that the log for the node prints on the printer at the listed remote node. Local mode indicates that the log for the node prints on the node’s printer. No printing mode indicates that the log for the node does not print.

Full Name

Display print configuration

Syntax

dspprtcnf

Related Commands

cnfprt

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspprtcnf`

Description

Display the print configuration. The example does not show the highlighted field.

System Response

```
sw83           TN     SuperUser       IGX 8420      9.2       Aug. 22 1997 16:02 PST


Printing Mode

Remote Printing
Local Printing
No Printing










Last Command: dspprtcnf


Next Command:
```

dsppwr

Displays the current status of the power supply monitor, the current power supply configuration (which may consist of from one to four power supplies depending on node requirements), and the current cabinet temperature.

On the right side of the screen is displayed the internal cabinet temperature in degrees Centigrade and Fahrenheit. The temperature is displayed as a thermometer and the exact temperature appears at the top of the thermometer.

Full Name

Display power supply status

Syntax

dsppwr

Related Commands

dspcd, **dspcds**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsppwr`

Description

Display power supply status.

System Response

```
sw81            TN     SuperUser       BPX 8620     9.2       May  21 1997 13:13 PST

         Power Status                                         Cabinet Temperature

ASM Status: Active                                               22        71

Power voltage A/B:      0 / 49 V                              C  60  |  |  140  F
                                                              e      |  |       a
PSU  Ins Type Rev SerNum Failure                              n  50  |--|  122  h
 A    N  N/A  N/A   N/A    N/A                                t      |  |       r
 B    Y  240V  0C 29959   None                                i  40  |  |  104  e
                                                              g      |  |       n
            Fan Status                                        r  30  |  |  86   h
                                                              a      |  |       e
     FAN   1    2    3                                        d  20  |  |  68   i
         3300 3360 3240 RPM                                   e      `--'       t


Last Command: dsppwr


Next Command:
```

dspyred

Displays information for Y-cable pairings. A single slot can be specified, or all pairings are displayed when no slot is specified. Slot numbers appearing in high intensity indicate active card status. Front card, back card, and channel configuration conflicts appear in reverse video. A conflict occurs when the port interfaces are different for corresponding ports in a redundant slot pair. The output display contains the following information:

- First column (Slot) designates the slot of the displayed card.
- Second column (Slot Type) designates its status, Pri (primary) or Sec (secondary).
- Third column (Other Slot) designates the slot number of the associated Y-redundant card.
- Fourth column (Front Card) designates the type of card in the front slot.
- Fifth column (Back Card) designates the type of card in the back slot.

Remaining columns (Channel Configuration) describe the channel configurations when appropriate.

Full Name

Display Y-cable redundancy

Syntax

dspyred [slot]

Related Commands

addyred, **delyred**, **prtyred, switchyred**

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	No	IGX, BPX	No

Example 1

`dspyred`

Description

Display Y-redundancy for all cards.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 14:28 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
25   Pri  26    SDP    RS232   DCE  DCE  DCE  DCE
26   Sec  25    SDP    RS232   DCE  DCE  DCE  DCE







Last Command: dspyred


Next Command:
```

prtcdred

Prints the card redundancy configuration for a BXM card with an OC-3 or OC-3 interface. This command uses the same syntax and prints the same information as the **dspyred** command. See the **dspcdred** command for details on the format of the command output.

Full Name

Print the card redundancy for all cards.

Syntax

prtcdred <start slot>

Related Commands

addcdred, dspcdred, delcdred, prtcdred, switchcdred

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	Yes

Example 1

`prtcdred`

Description

Print card redundancy for all cards (no starting slot entered).

System Response

```
beta           TRM   YourID:1        BPX 8620    9.2    Aug. 15 1997 14:27 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
2    Pri    3   BXM    LM-BXM
3    Sec    2   BXM    LM-BXM








Last Command: prtcdred 2


Next Command:
```

prtyred

Prints the Y-cable redundancy configuration for an SDP, LDP, CDP, FRP, FTC, NTC or AIT card on an IPX node. On an IGX node, the cards are the HDM, LDM, CVM, FRM, FTM, NTM, BTM, ALM/B, UXM, UFM, and UVM. On a BPX node, the applicable cards are the BCC, ASI, and BNI. This command uses the same syntax and prints the same information as the **dspyred** command. See the **dspyred** command for details on the format of the command output.

Full Name

Print the Y-cable redundancy

Syntax

prtyred <start slot>

Related Commands

dspyred, **addyred**, **delyred**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	Yes

Example 1

`prtyred`

Description

Print Y-redundancy for all cards (no starting slot entered).

System Response

```
beta          TRM   YourID:1        IGX 8420     9.2    Aug. 15 1998 14:28 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
25   Pri  26    SDP    RS232   DCE  DCE  DCE  DCE
26   Sec  25    SDP    RS232   DCE  DCE  DCE  DCE









Last Command: prtyred


Next Command:
```

switchcdred

Switches active and redundant cards used for SONET APS (Automatic Protection Switching). The **switchcdred** command is the same as the **switchyred** command, and you can use it on any Y-cable redundancy card pair. You typically only would use the **switchcdred** command when you need to perform diagnostics or maintenance, and you need to remove and service the active card.

Note When implementing two-card APS 1+1, it must be implemented with card redundancy (may also be referred to as "Y-redundancy", because the new card redundancy commands you use to configure APS 1+1 are based on Y-redundancy commands used in releases previous to Release 9.2 APS commands.)

When there is a front card failure, front card downed, or the front card fails a self–test, the card switchover should happen automatically (that is, you should not need to execute the **switchcdred** command for the card switchover to happen.) An automatic switchover typically occurs when the switch software determines that the card is in a worse condition than the redundant pair (that is, a card is in a failed state due to a condition such as self-test, background test, fatal errors.) If a standby card is not available, the **switchcdred** command will not be executed.

Typically, when APS and card redundancy are implemented together, the term Y-redundancy actually refers to card redundancy because there is no Y cable connecting two backcards to one line. With SONET APS card redundancy, there is a primary and a secondary front card/back card pair. The redundant front card must be in Hot Standby state before a switchover can occur. When a front card failure is detected, the switchover should happen automatically (when card redundancy has been implemented). However, for the APS application, the active line is not switched if the line status is good. If the line has Loss of Signal (or other defects), it will be switched to the redundant line. (The line refers to the physical cable attached to the output of the back card.)

For APS 1+1, a front card can switch and become the standby card while its associated back card still has the active lines. The APS line will not switch during a card redundancy switch, unless the APS firmware detects that an APS switch is needed.

Following a **switchcdred**, or active card reset, the BXM card is sent a message from switch software to have it perform an APS switch to align itself with the last user **switchapsln** switch request. If the last user request is "clear", full automatic APS switching is in effect with the working line in the active state by default. When there is no last user request to switch to any particular line (that is, protection line), the working line becomes active.

Note In the APS 1+1 configuration, if the protection line is active and the last user request is "clear", a **switchcdred** will cause the working line to be active if there is no line condition on the working line. When APS 1+1 comes up, it will come up on the working line if the working line is clear. When a **switchcdred** is issued, the active card also comes up on the working line if the working line is clear and there is no user request. **In the case** where the working line is in alarm or there is a user request to switch to the protection line, the card will first come up on the working line. Then the card will detect the alarm or the user request and switch to the protection line.

Other Notes on **switchcdred**

Note In the APS 1+1 configuration, if the last user request was a W->P switch, then **dsplog** will log a W->P switching event when a **switchcdred** command is issued. On issuance of a **switchcdred** command, the newly active card comes up on working line first. Then it responds to a user request to switch from **working** to protection by switching to the protection line and sending an event notification to that effect. The event notification can be seen in the event log by using the **dsplog** command.

Note It may be necessary to perform a **switchcdred** command after performing a service switch with the **switchapsln** command so that the back card that the service switch selects has its associated front card active.

Full Name

Switch active card of a redundant pair of cards.

Syntax

switchcdred

Related Commands

addcdred, delcdred, dspcdred, prtcdred

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	No	BPX	Yes

Example 1

`switchcdred`

Description

Change the active card to be the standby card.

System Response

No display produced.

switchyred

The **switchyred** command is sometimes referred to as *soft y-red switching* (also known as the "graceful switching" feature. It lets you access the y-redundancy switching feature already in the system. Executing the **switchyred** command performs a graceful y-redundancy switch in that no cards need to be reset in the process of switching from the current active card to the current standby card. Thus, all the existing channel programming on both cards remain intact, and is ready to use in the case of a fault condition (where the newly active card is found to be faulty).

The customer typically diagnoses all standby equipment for all duplicated cards. To implement similar preventative maintenance procedures, this command lets you switch active and standby cards, without resetting either card. The customer intends to execute the switch once every two weeks. Should the standby card be found to be faulty, in the current scheme, during re-programming of the reset card, an outage is experienced. To do away with the outage period, the standby card is not to go through a rebuild forced by the resetting of the card. In the case of this feature, neither card is reset, however, programming is continued on both cards. This type of reprogramming will be to make sure all channels are programmed again on the same card. It is transparent to the user, since all the channels were never deleted; they are being reprogrammed as is the custom today in the case of a regular y-redundancy switch.

The **switchyred** command operates on the following BXM cards:

- y-redundancy trunk cards
- BXM y-redundancy port cards
- BXM y-redundancy feeder cards

In addition, you can use the **switchyred** command on ASI cards and BNI cards. In any case where these cards are not supported, you will be blocked from executing the command at the command line interface.   The **switchyred** command initiates the y-redundancy switch. It can also be initiated through a job. The **switchyred** command is available through the same access login as the **addyred** command.

The **switchred** command lets you switch between cards of a y-redundancy pair, avoiding any card resets or failures. The feature is needed to allow the customer fast failure recovery in the cases where the previously standby card is found to be at fault. The feature allows for the previously active card to maintain its configuration and availability, allowing you to switch to it, either through another soft y-redundancy switch request, or through the automated y-red switching (which executes upon card failure).

The graceful switching command (**switchyred**) is applicable to BXM, ASI cards, and BNI cards.

This command requires Release 9.1 software and beyond. The cards in question have to be programmed to be y-redundant. The states of the cards have to be Active (for the Primary card) and Standby (for the Secondary card) OR Standby (for the Primary card) and Active (for the Secondary card).

The purpose of a graceful switch is to switch from the current active card of a y-cable pair, to the current standby card of the pair, without deactivating, resetting, or re-programming either of the cards.

You initiate a graceful switch by issuing a **switchyred** command at the command line interface or through an SNMP script. The input to the command is the primary card's slot number. You can obtain this information through the dspyred command, which lists the Primary card of a yredundancy pair, and the secondary card of the y-red pair. See the example below.

Table 3-20 switchyred Example

Slot	Card Type	Other Slot	Front Card	Back Card
3	Pri	4	BXM	LM-BXM
4	Sec	3	BXM	LM-BXM

In the above example, a y-red has been configured using slots 3 and 4, where slot 3 is identified as the Primary card (Pri) of the pair. Using the example shown in switchyred Exampleswitchyred ExampleTable 3-20, the command line would look as follows:

Next Command: **switchyred 3**

The **switchyred** command displays errors on the screen if the slot used in the command line if the following conditions exist:

- if the card slot is not configured for y-redundancy
- if the state of both cards is not valid

The command line issues a warning and prompts you to continue in case any channel programming is in progress. (Continuing at this stage introduces the risk of encountering continuity problems for a short period of time (until all remaining channels are programmed).

After you issue the command, the switch software starts the process of the graceful switch.

First, turn off the laser of the current active card (by sending it an Ox05 cbus message). In effect, stop running traffic on that card.

Next, activate and start running traffic on the current standby card, forcing it to be the new active card of the pair. This process also starts off the channel re-programming of the cards, and allows for the new standby card to be re-programmed.

All the steps required to complete the graceful y-redundancy switch are in Release 9.2, the main and possible only difference being that neither card is reset.

There are no backward compatibility issues related to the **switchyred** command in Release 9.1.

The switchyred feature introduces the concept of de-activating a card without a failed state being present, or deactivating the card, or the need to reprogram all the channels on the card.

Function

The **switchyred** command kicks off the graceful switch process. After you issue the command, switch software checks for and reports the following error conditions:

- If the input slot number is invalid (the valid ranges for the slot is 1 -6 and 9 - 15).
- If the slot is empty, an error is displayed onto the screen indicating that the slot is empty.
- If the slot is not occupied by a BXM card, an error is displayed on the screen. (In future releases, this check will also be performed for the BNI and ASI card cases).
- If the card in the slot specified is not configured for y-redundancy, an error specifies that the graceful switch command is executed for the y-redundancy feature. If no y-red is configured on the card, graceful switching cannot be performed.

If the y-redundancy pair (specified through the primary slot) contains cards in the incorrect state, a message is displayed onto the screen indicated the incorrect state of the cards. (valid states for the cards are:

- the primary card is in active state and the secondary is in standby state.
- the primary card is in standby state, and the secondary card is in active state. No other state combination is valid.

You are prompted to continue if the following is true:

— the switch software determines that channel programming is in progress for either of the cards in the y-redundancy pair.

To choose to continue in this state implies that channels (connections) in the process of being programmed might not exist on the standby card after the graceful switching has completed, that is, the programming must be completed on both cards.

A message displays listing the cards being switched from, and the card being switched to, just before the graceful switching process begins.

After the switching process has been kicked off, the switch software does the following:

- Turns off the laser on the active card (stopping traffic).
- Puts the current active card into the standby state.
- Activates the current standby card to be the Active one of the pair.

Event Logging

Event logging does not distinguish between a y-redundancy switch due to a failure (beyond logging the indication of the failure), and a y-redundancy switch due to the execution of the **switchyred** command.

Full Name

Switch Y-redundant cards.

Syntax

switchcdred

Related Commands

addyred, delyred, dspyred, prtyred, switchyred

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	No	BPX	Yes

Example 1

`switchcdred`

Description

Change the active card to standby card.

System Response

No display produced.

upcd

Activates a card you have downed with the **dncd** command. (If a slot contains a complete card set, both the front and back card are upped. After a card set is upped, it is available as a node resource. When you activate a card, it comes up in either the *standby* or *active* state. The initial state depends on whether the network is ready to use the card immediately.

Full Name

Up card

Syntax

upcd <slot>

Related Commands

dncd, **dspcds**

Attributes

Privilege	1–
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

upcd 10

Description

Activate the card in slot 10. After you activate the NTC in slot 10, its status is "Standby."

System Response

```
pubsipx1       VT    SuperUser       IPX 16    9.1 Oct. 30 1997 21:15 GMT


   FrontCard  BackCard                         FrontCard  BackCard
   Type  Rev  Type     Rev  Status             Type  Rev  Type     Rev  Status
1  NPC   ABC                Standby      9  Empty
2  NPC   ABC                Active       10 NTC   ESC  E1       P06  Standby-F
3  SDP   CBC  V35      AF   Standby      11 Empty
4  Empty                                 12 Empty
5  FRP   DFR  FRI-V35  AA   Active       13 CDP   ABE  T1       P06  Standby-T
6  LDP   CC03 232-4    AC   Standby      14 Empty
7  Empty universal backplane             15 NTC   EC02 Empty         Unavail
8  AIT   BBF  AIT-T3   AD   Active       16 Empty


Last Command: upcd 10


Next Command:
```

Table 3-21 upcd–Parameters

Parameter	Description
slot	Specifies the card slot number of the card

window

Provides an interface to an external device. To establish a session with an external device, first use the **cnftermfunc** command to designate the auxiliary port to serve as the external device window. To begin the session, enter the **window** command and specify the port. The control terminal screen subsequently clears, after which characters entered at the control terminal go to the external device and vice versa.

Because the IGX and BPX nodes “bundle” characters together before transmitting them, a slight transfer delay occurs. Transfers are delayed until the transfer buffer is filled or the keyboard is inactive for over 50 milliseconds. To end the session, enter the escape sequence designated with the **cnftermfunc** command. The default for the escape sequence is ^^ (SHIFT 66).

The **window** command can be executed over a virtual terminal connection. This makes it possible to control external devices from a single point in the network. Devices such as Channel Service Units (CSUs), routers, channel banks and other devices with RS-232 console ports can be accessed remotely with this feature.

Full Name

Window to external device

Syntax

window <a/c>

Related Commands

cnfterm, **cnftermfunc**

Attributes

Privilege	1–4
Jobs	No
Log	No
Node	IGX, BPX
Lock	Yes

Example 1

`window` a

Description

Connect to a local router attached to the auxiliary port. The following dialogue shows the prompts and example responses.

System Response

```
Protocol [ip]:

Target IP address:  192.9.202.1

Repeat count [5]:
Datagram size [100]:

Timeout in seconds [2]:


Extended commands [n]::

Type escape sequence to abort. ^^

Sending 5, 100-byte ICMP Echoes to 192.9.202.1, timeout is 2 seconds:

.......


Success rate is 100 percent

left #
```

Table 3-22 window–Parameters

Parameter	Description
a	Specifies a window into external equipment attached to the node's auxiliary port. This is the default connection.
c	Specifies a window into external equipment attached to the node's control port.

Setting Up Trunks

This chapter describes the commands you use to set up and configure trunks. The contents in this chapter are as follows:

- Introduction
- A table showing the supported combinations of nodes, card sets, and line types
- Descriptions of trunk-related procedures:
  - Setting up a trunk
  - Setting up a virtual trunk
  - Configuring resources on a physical or virtual trunk
  - Reconfiguring a trunk
  - Removing a trunk
  - Displaying or printing a trunk configuration
  - Specifying trunk or line redundancy
  - Using subrate trunk interface control templates
- A list of commands in this chapter with beginning page number
- Descriptions of the trunk commands

Introduction

After you have configured the *nodes*, you must activate the *trunks*. Trunks are intra-node communication links in a network. A trunk can connect any combination of IGX or BPX nodes. Trunk characteristics are:

- Physical line type: T1 (including fractional), E1 (including fractional), Subrate, E3, T3, or OC-3 (STM1), OC-3/AIM with UXM, OC-12 with BXM
- Communication technology: Asynchronous Transfer Mode (ATM) or FastPackets.

Table 4-1 shows the communication technology for each node type, card combination, and line type.

Table 4-1 Supported Card Types in Release 9.2

Node Type	Front Card	Back Card	Line Types	Technology
IGX	NTM	BC-T1	T1, T1 Fractional	FastPacket
IGX	NTM	BC-E1	E1, E1 Fractional	FastPacket
IGX	NTM	BC-SR	Subrate	FastPacket
IGX	NTM	BC-Y1	Y1	FastPacket
IGX	UXM	BC-UAI-2OC3-SMF, BC-UAI-2STM-1-SMF BC-UAI-4OC3-SMF, BC-UAI-4STM-1-SMF BC-UAI-4OC3-MMF BC-UAI-4STM-1-MMF BC-UAI-4T1-IMA DB15, BC-UAI-4E1-IMA DB15, BC-UAI-4E1-IMA BNC BC-UAI-8T1-IMA DB15, BC-UAI-8E1-IMA DB15, BC-UAI-8E1-IMA BNC BC-UAI-3T3 BC-UAI-6T3 BC-UAI-3E3 BC-UAI-6E3	OC-3 (STS) OC-3 (STM1) OC-3 (STS) OC-3 (STM1) OC-3 (STS) OC-3 (STM1) T1 E1 E1 T1 E1 E1 T3 T3 E3 E3	ATM
IGX	UXM	BC-6T3, BC-6E3 BC-3T3, BC-3E3 BC-UAI-3T3 BC-UAI-6T3 BC-UAI-3E3 BC-UAI-6E3	T3, E3 T3, E3 T3 T3 E3 E3	ATM
IGX	ALM/B	BC-BTM-HP-T3 BC-BTM-HP-E3	T3, E3	ATM
IGX	BTM	AIT-T3, AIT-E3, AIT-E2, AIT-HSSI, BTI-E1	T3, E3, E2, E1, HSSI	ATM
BPX	BNI	LM-3T3, LM-3E3	T3, E3	ATM
BPX	BNI-155, BNI-155E	2OC3-SMF or 2OC3-MMF	OC-3 (STS)	ATM
BPX	BXM-155-8	MMF-155-8 SMF-155-8 SMFLR-155-8	OC-3 (STS)	ATM
BPX	BXM-155-4	MMF-155-4 SMF-155-4 SMFLR-155-4	OC-3 (STS)	ATM
BPX	BXM-622-2	SMF-622-2 SMFLR-622-2	OC-12 (STM4)	ATM

Setting Up a Trunk

Before executing the commands in this section, you must have finished setting up the nodes, as described in Chapter 3, “Setting Up Nodes.” Also, the front and back cards that support the proposed line type and communication technology must reside in the slot intended for the trunk.

In this release, the Ports and Trunks feature, which is supported on the BPX and IGX, allows you to configure port, routing trunk and feeder trunk interfaces simultaneously on a slot containing a BXM or UXM card. For example, you can up port 1 on a BXM slot as a trunk interface while also upping port 2 as a line interface. For BXM and UXM cards, you do not need to upgrade the firmware.

Note You cannot use a virtual trunk as an interface shelf (feeder) trunk; similarly, you cannot configure an interface shelf trunk to act as a virtual trunk. Similarly, you cannot terminate interface shelf (feeder) connections on a virtual trunk.

Table 4-2 Interface Types Supported on the Same Card

Interface Type	BXM	UXM
Physical trunks	supported	supported
Virtual trunk	supported	supported
Interface shelf (feeder) trunks	supported	Not supported
Ports (UNI)	supported	supported

1 Use the **uptrk** command to activate the trunk.

Use the uptrk command to activate the port so that it can start to generate framing. It also determines whether the trunk is a physical-only trunk or a virtual trunk. The third digit you specify in the **uptrk** command (represented by *slot.port.vtrk*) indicates that the trunk is virtual. See the *Cisco BPX Series 8600 Reference* for more information on virtual trunking.

Use **uptrk** at each end of the trunk. When the trunk is upped at only one end, the node detects the trunk as being in an alarm state (see **dsptrks**). Upping the trunk at both ends clears the alarm.

2 Use the **cnftrk** command to override the trunk’s default values. You must use **cnftrk** for virtual trunks, but it is an optional command for physical trunks. For virtual trunks, you must change the VPI to a non-0 value before executing **addtrk**.

If you use **cnftrk**, you must make the same changes at both ends of the trunk. To display existing trunk parameters, use the **dsptrkcnf** command. The configurable parameters are listed for each card type in Table 4-1. (The possible parameters are PKT for FastPackets, ATM cells, BNI if the trunk is a BNI card, or All.) Not all of these parameters apply to the BPX node.

After you configure the trunk, and add the trunk (**addtrk**), you can re-specify certain parameters. For example, a period of trunk use may give you enough information to indicate that you should change parameters to optimize how the trunk is used. Refer to the “Removing a Trunk” section on page 4-49 for details.

3 Use **addtrk** to add the trunk. Adding the trunk makes the trunk a usable resource, so you can add connections (**addcon**) to carry traffic. You only need to add one end of the trunk.

To add an interface shelf to a routing node in a tiered network, use the **addshelf** command.

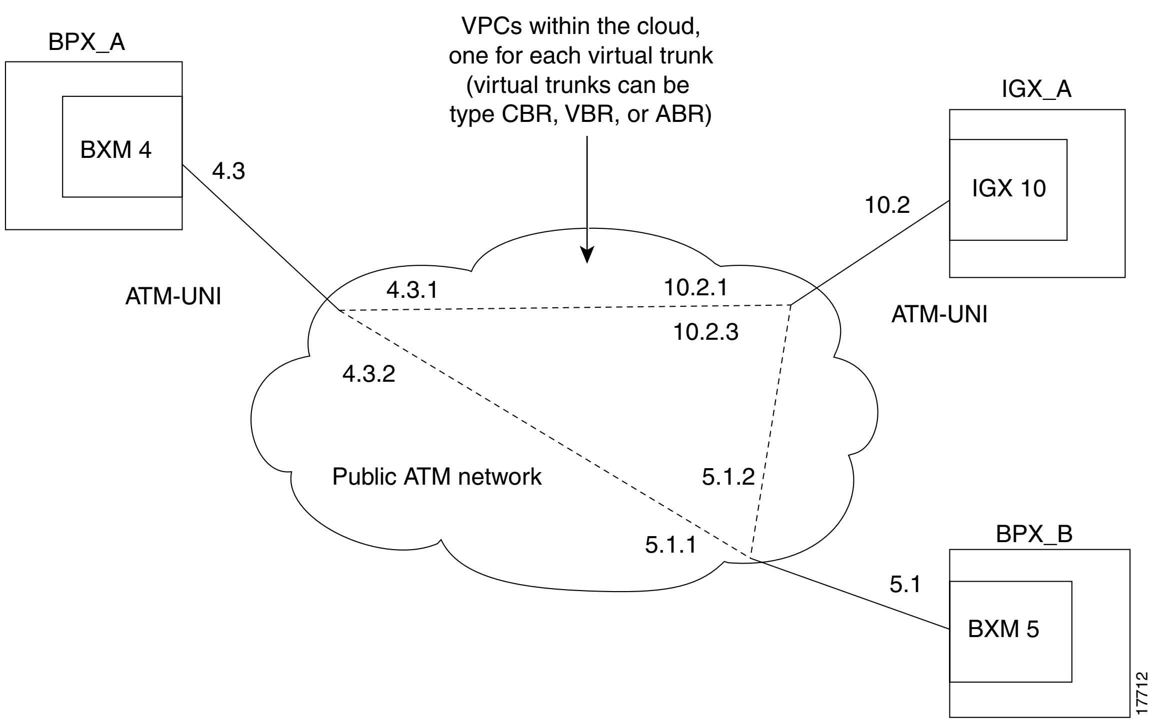
Overview of Virtual Trunking

The purpose of virtual trunks is to provide customers with a cost-effective way to use Cisco equipment while connecting to a public ATM network. This hybrid network of private trunks and public networks is expected to be a common configuration as customers begin to implement ATM in their networks and public carriers begin to offer ATM service. This hybrid network configuration provided by virtual trunking allows private virtual trunks to use the mesh capabilities of the public network in interconnecting the subnets of the private network.

You establish connectivity through a public ATM cloud by allocating virtual trunks between the nodes on the edge of the cloud. With only a single trunk port attached to a single ATM port in the cloud, a node uses the virtual trunks to connect to multiple destination nodes on the other side of the cloud. From the perspective of a Cisco node, a virtual trunk is equivalent to a VPC provided by the ATM cloud network, which provides connectivity through the cloud.

A virtual trunk is simply “a trunk defined over a public ATM service.” The trunk really does not exist as a physical line in the network. You use an additional level of reference, called a *virtual trunk number*, to differentiate the virtual trunks found within a physical port. The ATM equipment in the cloud must support Virtual Path switching and moving incoming cells based on the VPI in the cell header. Within the cloud, one virtual trunk is equivalent to one VPC. Because the VPC is switched with just the VPI value, the 16 VCI bits (from the ATM cell format) of the ATM cell header are passed transparently through to the other end. The VCI bits within the header are passed transparently through the entire cloud (Figure 4-1). The virtual path ID (VPI) is provided by the ATM cloud administrator (for example, service provider).

Figure 4-1 Typical ATM Hybrid Network using Virtual Trunks



This release introduces support of the UXM trunk card as a physical interface to the public ATM cloud on the IGX. BXM trunk card support is introduced as a physical interface to the cloud on the BPX. The trunk connection at the cloud’s access point can be an ATM UNI or ATM NNI interface.

Virtual trunking is supported on the IGX and BPX platforms. With the BPX switch, virtual networks can be set up with either the BNI card or BXM card.   The virtual trunks originate and terminate on Buxom to Buxom, or BXMs to UXMs (IGX switch), or BNIs to BNIs, but not BNIs to BXMs or UXMs.

Each Cisco sub-network is connected through the public ATM network with virtual trunks. The trunk interface at the Cisco nodes is either a BNI, BXM, or UXM trunk card. The BXM card's physical trunk interface to the ATM cloud is a standard ATM UNI or NNI interface at the cloud's access point. The administrator of the ATM cloud (for example, service provider) specifies whether the interface is UNI or NNI, and also provides the VPI to be used by a virtual trunk across the cloud. Specifying an NNI cell interface provides 4 more bits of VPI addressing space.

Virtual trunking is a purchased feature, so Cisco Customer Service must enable it on each node where you intend to use virtual trunking. Virtual trunking is supported on the ASI, BNI and BXM cards in the BPX, and on the UXM card in the IGX. Note that firmware levels on ASI, BXM, and UXM cards must be current. For more information on virtual trunking, see the chapter on BXM virtual trunks in the *Cisco BPX Series Installation and Configuration* and *Cisco BPX 8600 Series Reference*.

Compatibility between Cards in Virtual Trunks

Virtual trunking is supported on the BPX and IGX. However, because the BXM and UXM cards both use the standard UNI and NNI cell header formats across the virtual trunks (instead of the Strata-UNI cell format used on BNI virtual trunks), BNI virtual trunks are not compatible with BXM/UXM virtual trunks.

To use virtual trunking on a BXM or a UXM card, Release 9.2 software is required, and Release 9.2 BXM and UXM firmware. No hardware upgrade is required. The new firmware is backward compatible. Also, nodes running Release 9.2 software can interoperate with nodes running 9.1 or 8.5, but you cannot add UXM and BXM virtual trunks into a network of mixed software releases. This is because the networking messages are different among the software releases, specifically the virtual trunk number and the cell format on virtual trunks.

You configure the BXM and UXM cards similarly as in releases previous to Release 9.2; that is, you use similar card, line, port and connection commands for configuration.

Virtual Trunking Support on BPX and IGX in Release 9.2

Each BPX node can have a combined maximum of 64 logical (physical and virtual) trunks per node. Each IGX node can have a combined maximum of 32 logical (physical and virtual) trunks per node.

A BNI-T3 or E3 line can support up to 32 virtual trunks on one or both physical ports. A BNI-OC-3 line can support up to 11 virtual trunks.

A BXM card can support up to 31 virtual trunks. A UXM card can support up to 15 virtual trunks. Note that, like regular trunks, virtual trunks can carry high-priority traffic.

Channel Capacities. In Release 9.2, networking channels will be pre-allocated only for AutoRoute trunks. In releases previous to Release 9.2, for UXM and BXM cards, networking channels are pre-allocated when the first trunk is upped; that is, 270 channels are allocated for each trunk on that card. For example, if the card had four trunks enabled on it, trunk 1 would have channels 0 through 270 allocated, trunk 2 would have channels 271 through 540; trunk 3 would have channels 541 through 810, and trunk 4 would have channels 811 through 960 allocated.

Network channels are no longer pre-allocated. Networking channels will be allocated for each trunk when the trunk is upped. For each trunk that is upped, 270 channels will be dynamically allocated for networking.

For legacy UXM/BXM cards, approximately 270 networking channels are allocated for each virtual trunk. For example, UXM cards will allocate 4320 channels if all 16 virtual trunks are upped on a single card. BXM cards will allocate 8640 channels if all 32 virtual trunks are upped. See Table 4-3 for networking channel capacities for virtual trunks.

Table 4-3 Networking Channel Capacities for Virtual Trunks

#VT	# Networking Channels for Legacy Cards	# Networking Channels for Enhanced Cards
1 VTs	270 chans	270 chans
2 VT s	540 chans	270 chans
3 VTs	810 chans	270 chans
16 VTs	4320 chans	270 chans
32 VTs	8640 chans	270 chans

This implies that UXM legacy cards upping all 15 virtual trunks would consume 4320 gateway channels for networking, leaving none for user traffic. For this reason, you will need to limit the number of virtual trunks that you up on a legacy UXM card. You can use the **cnfport** command to control the number of trunks upped on a UXM card.

Introduction to Ports and Trunks and Virtual Trunking

The fundamental architecture of the virtual trunking feature in this release is similar to that of the BNI virtual trunk implementation in previous switch software releases. The standard UNI/NNI cell headers are used across the virtual trunks, and two-stage queueing as defined by the VI interface.

This section discusses some features that interact with virtual trunking, including:

- trunks and ports on the same card
- VSI resource partitioning
- virtual ports

You up and configure virtual trunks with the existing commands. The commands have additional parameters for virtual trunk specific items. You up a trunk with **uptrk** <*slot.port.vtrk*>. You configure the trunk VPI (VPI range 1-4095) and other parameters on the trunk with **cnftrk, cnftrkparm,** and **cnfrsrc** commands.

Below lists the permutation of virtual trunks that you can interface through the public ATM cloud.

Table 4-4 Permutation of Virtual Trunks that can be Connected through a Public Cloud

	BNIs (T3/E3/OC-3)	BXM (T3/E3/OC-3/OC-12)	UXMs (T3/E3/OC-3)	UXM-AIM
BNIs (T3/E3/OC-3)	yes	no	no	no
BXMs (T3/E3/OC-3/OC-12)	no	yes	yes	yes

Table 4-4 Permutation of Virtual Trunks that can be Connected through a Public Cloud

	BNIs (T3/E3/OC-3)	BXM (T3/E3/OC-3/OC-12)	UXMs (T3/E3/OC-3)	UXM-AIM
UXMs (T3/E3/OC-3)	no	yes	yes	yes
UXM-AIM	no	yes	yes	yes

The Ports and Trunks feature lets you configure multiple trunk lines and circuit lines on a single BXM or UXM card simultaneously. In releases previous to Release 9.2, when you upped a single port as a trunk (by using the **uptrk** command), all the remaining ports on that card are treated as trunks. Similarly, when you up a single port as a circuit line (by using the **upln** command), all the remaining ports on the card are treated as circuit-line ports.

The Ports and Trunks feature is supported on the BXM and UXM cards for the BPX and IGX platforms. A port, routing trunk and feeder trunk interface can be supported on a given slot containing a BXM or UXM card type simultaneously. For example, a user of a BXM slot can have port 1 upped as a trunk interface while having port 2 upped as a line interface.

For example a BXM card can have:

- port 1 upped as a physical trunk;
- port 2 upped as a feeder trunk;
- port 3 upped with multiple virtual trunks;
- port 4 upped as a UNI interface

Table 4-5 lists the interface types that can be supported on a single card.

Table 4-5 Interface Types that can be Supported on a Single Card

	ASIs (T3/E3/OC-3)	BNIs (T3/E3/OC-3)	BXM (T3/E3/OC-3/OC-12)	UXMs (T3/E3/OC-3)	UXM-AIM
MGX 8850 Feeder	no	yes	yes (except OC-12)	no	no
IGX Feeder	no	yes	no	no	no
Physical Trunks	no	yes	yes	yes	yes
Virtual Trunks	no	yes	yes	yes	yes
UNI port	yes	no	yes	yes	yes
Virtual UNI	no	no	no	no	no

Virtual Trunking Configuration

You use the existing trunk commands to manage trunks (for example, **uptrk**, **cnftrk**, and **addtrk**). The syntax to identify a logical trunk has an optional virtual trunk identifier, which you append to the slot and port information.

The ATM cloud must be configured to support virtual trunking. For an ATM cloud containing Cisco equipment (for example, BPX nodes are in the public ATM cloud), the access points are ASI or BXM ports. (These access points serve as physical interfaces to the cloud.) If the ATM cloud has access points of ASI or BXM ports, and the cloud attaches to either BXM or UXM virtual trunks, the ASI or BXM port should be configured (with **cnfport**) so that the HCF field (sometimes called the Shift/No shift option is set correctly. The **cnfport** "shift" option specifies that a one-byte shift on the HCF field of the cell header will occur.

For an ATM cloud containing IGXs, the access points are UXM ports. Similarly, you must configure the ports to handle the virtual trunk cells from Cisco nodes. This entails setting the physical port parameters such that they match the trunk to which they are attached. In addition, if the access point in the BPX cloud is a BNI port, you must to configure the port to not shift (*Shift n*) the VCI in the cell header.

Note For a non-BPX and non-IGX cloud, due to ILMI signalling support, you no longer need to configure the ATM ports to block signalling traffic to the Cisco nodes.

Virtual Trunk Example

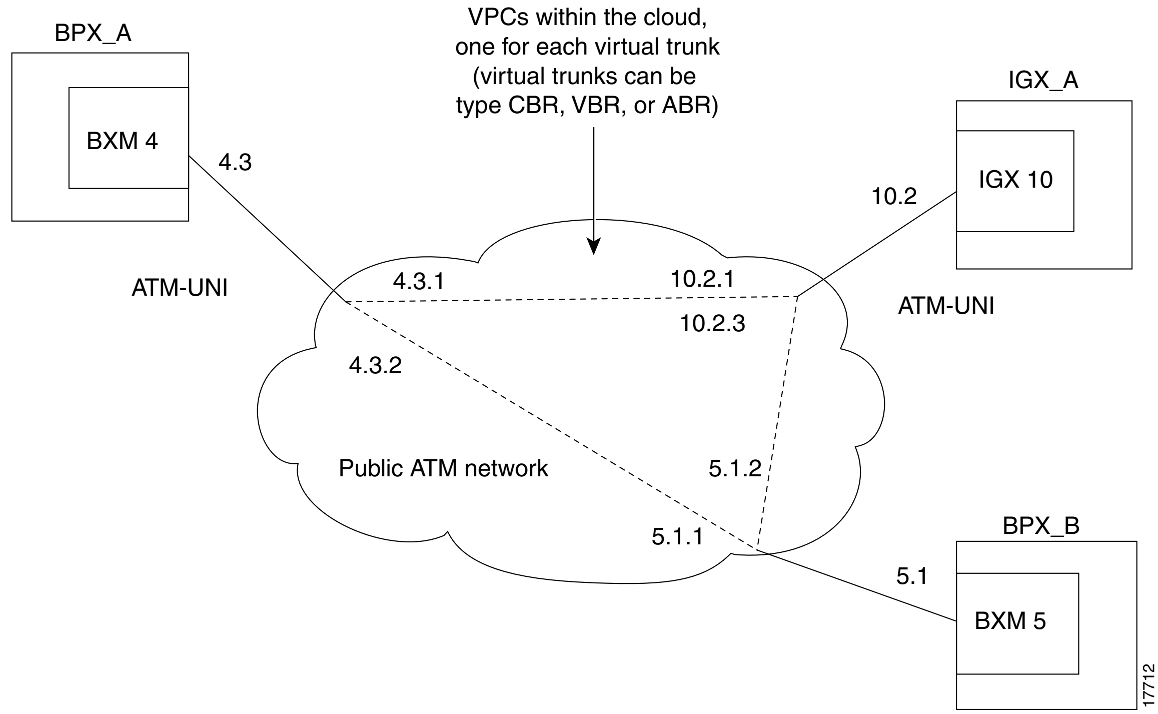
An example of a number of virtual trunks configured across a public ATM Network is shown in Figure 4-2. There are three virtual trunks shown across the network, each with its own unique VPC.

The three virtual trunks shown in the network are:

- between BPX_A 4.3.1 and IGX 10.2.1
- between BPX_A 4.3.2 and BPX_B 5.1.1
- between BPX_B 5.1.2 and IGX_A 10.2.3.

Each VPC defines a virtual trunk which you can configure for support of CBR, VBR, or ABR traffic.

Figure 4-2 Virtual Trunks across a Public ATM Network



Connection Management

Virtual trunking allows a BPX and IGX node to provide trunks that are compatible with the standard 3.0/3.1 ATM UNI cell format interface of a public ATM network. Unlike previous trunk implementations, the ATM cells are not in a proprietary STI (StrataCom Trunk Interface) format, permitting StrataCom (STRM) trunks to connect through a public ATM network.

The cell addressing method for connections routed through a virtual trunk handles multiple type of traffic flowing through an ATM cloud. The header format of cells may match the ATM-UNI or ATM-NNI format since the port interface to the ATM cloud is a physical interface configured as either a UNI or NNI interface, as specified by the administrator of the ATM cloud.

Congestion management (resource management) cells are passed transparently through the network. Cisco features such as Advanced CoS Management and Optimized Bandwidth Management may not be supported within the public network, but the information is carried through the network. Leased lines may also exist to connect the Cisco sub-networks outside of the ATM network.

Cell Header Formats

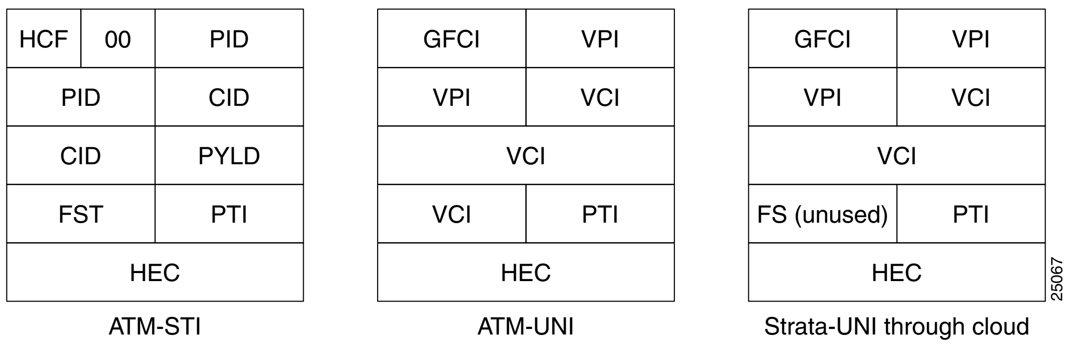
Before cells enter the cloud on a virtual trunk, the cell header is translated to a user configured VPI value for the trunk, and a software configured VCI value which is unique for the cell.

As cells are received from the cloud by the BPX or IGX in the Cisco networks at the other end of the cloud, these VPI/VCIs are mapped back to the appropriate VPI/VCI addresses by the Cisco nodes for forwarding to the next destination.

The VPI value across the virtual trunk is identical for all cells on a single virtual trunk. The VCI value in these cells determines the final destinations of the cells. On BNI cards, for virtual trunking, a modified ATM UNI cell format (Strata-UNI) stores the Optimized Bandwidth Management information, as applicable, in the header of a Strata-UNI cell format. A virtual trunk with a BNI at one end must terminate on a BNI at the other end. (BNI trunks are incompatible with BXM or UXM trunks.)

Figure 4-3 shows three different cell header types: ATM-STI, ATM-UNI, and Strata-UNI through a cloud. The ATM-NNI header (which is not shown in the figure) differs in format from the ATM-UNI only in that there is no GFCI field, and those four bits are added to the VPI bits to give a 12-bit VPI.

Figure 4-3 ATM Virtual Trunk Header Types



The ATM-STI header is used with BNI trunks between BPX nodes within a Cisco switch subnetwork. The ATM-UNI is the standard ATM Forum UNI supported by the BXM card along with standard NNI. Virtual trunks terminating on BXMs or UXMs use the standard ATM-UNI or ATM-NNI header as specified by the cloud administrator (for example, service provider). Virtual trunks terminating on BNIs use the Strata-UNI header.

Because the BNI cards use a Strata-UNI format across a virtual trunk, BNI virtual trunks are not compatible with BXM/UXM virtual trunks which use either the standard UNI or NNI cell header formats. Therefore, BXM to BXM, UXM to UXM, and BXM to UXM virtual trunks are supported while BNI to BXM or BNI to UXM virtual trunks are not supported.

Bit Shifting for Virtual Trunks

The ATM-STI header uses four of the VCI bit spaces for additional control information. Only two of the bits are used for HCF. When the cell is to be transferred across a public network, a shift of these bit spaces is performed to restore them to their normal location so they can be used across a network expecting a standard ATM cell header.

This bit shifting is shown in Table 4-6. A BNI in the Cisco subnetwork can interface to an ASI or BXM (port configured for port mode) in the cloud. The ASI or BXM in the cloud is configured for no shift in this case.

A BXM in the Cisco subnetwork can interface to an ASI UNI port, BXM UNI port, or other UNI port in the cloud. The BXM in the cloud is configured for bit shifting as shown in Table 4-6.

In this case, the BXM or ASI in the cloud is configured for bit shifting as shown in Table 4-6.

Table 4-6 Bit Shifting for Virtual Trunking

Subnetwork	FW Rev	Shift		Cloud	FW Rev	Shift
BXM	--	??	>	BXM (port mode)		Yes
BNI	--		>	ASI		No
BNI	--		>	BXM (port mode)		No

Setting up a BNI Virtual Trunk through an ATM Cloud

The following example provides a general procedure on how to set up a virtual trunk through an ATM cloud using Cisco equipment (that is, a BPX or IGX cloud).

Step 1 Obtain a VPC from the ATM cloud provider.

Step 2 Set up cables by doing the following: in the cloud network, physically connect an ASI port to each BNI port that is likely to carry virtual trunks.

Step 3 For each ASI port connected to a BNI virtual trunk port, use the following configuration sequence:

upln *slot.port*

upport *slot.port*

cnfport *slot.port*, and set the *shift* parameter to “N” for *no shift*.

The *Shift/No shift* parameter specifies whether or not the VCI bits in the cell header should be shifted based on the HCF field of the cell header on cells arriving from the backplane. It is how Cisco networks convert STI cells to standards based cell formats, and similarly how standards-based cell formats are converted back to STI cells.

Step 4 Execute **addcon**. In the cloud network, add a virtual path ASI connection for each end of the virtual trunk that is to be routed through the cloud. An example of the syntax for this is:

addcon joker 5.1.1.* swstorm 6.2.10.*

where 5.1 and 6.2 are ASI ports that are hooked up and configured for virtual trunking. DACS connections are acceptable.

Note that the third number is the VPI, which must correspond to the virtual trunk VPI configured with **cnftrk** in step 4. For BNI virtual trunks, the usable range of VPIs is 1 to 255 (for T3/E3 trunks). For BNI OC-3 virtual trunks, the usable range of VPIs is 1-63.

The VPI configured for a virtual trunk must match the VPI of the VPC in the public ATM cloud. Every cell transmitted to the virtual trunk has this VPI value. Valid VPC VPIs depend on the port type as shown in Table 4-7.

Table 4-7 VPI Ranges

Port Type	Valid VPI Range
BXM/UXM (UNI)	1-255
BXM/UXM (NNI)	1-4095
BNI T3/E3	1-255
BNI OC-3	1-63

The CBR/VBR parameter must also correspond to the virtual trunk type of the virtual trunk. For T3, set PCR to 96000 and CDTV to 24000 for the connection so that the ASI does not drop cells. Cisco recommends these values based on testing.

Step 5 Configure BNI trunks. Use **uptrk** to enable the virtual trunk on the port. Take this step if the ATM cloud provider has assigned the VPC. On BNIs that connect to the cloud's ASI ports, configure the virtual trunks, as follows:

uptrk *slot.port.vtrk*

If the cloud is already configured, the alarm on the virtual trunk should clear.

cnftrk *slot.port.vtrk*

When you use **cnftrk** to configure the virtual trunk, make sure the virtual trunk type and VPI correspond to the existing ASI Virtual Path connections (that is, make sure that the virtual trunk matches the cloud's VPC configuration, uses the correct cell format (UNI or NNI), and that HCF-based shifting is *off* (which you configure using **cnfport** on the ASI port).

Step 6 Use **addtrk** to add the virtual trunk to the network topology.

addtrk *slot.port.vtrk*

The parameters *slot.port.vtrk* on a BNI card can have the following values:

- Slot can be 1–6, 9–14.
- Port is the physical port number, which can be 1–3 for T3/E3 or 1–2 for OC-3/STM1.
- Vtrk is the virtual trunk number, which (for BNIs) can be 1–32 for T3/E3 or 1–11 for OC-3/STM1. Note that the two ends of a virtual trunk can have different port interfaces. For example, a virtual trunk supported by a UXM-OC-3 on one end can be supported by a BXM-T3 at the other end. However, both ends of the trunk must have the same trunk bandwidth, connection channels, cell format, and traffic classes. The **addtrk** command verifies this when you add the trunk.

Setting up a BXM or UXM Virtual Trunk through an ATM Cloud

The following example describes how to set up a virtual trunk through a BPX or IGX cloud:

Step 1 Obtain a VPC from the ATM cloud provider.

Step 2 Set up cables by doing the following: in the cloud network, physically connect an ASI port (or a BXM port) to each BXM port that is likely to carry virtual trunks.

Step 3 For each ASI port connected to a BXM virtual trunk port, use the following configuration sequence:

upln *slot.port*

upport *slot.port*

cnfport *slot.port*, and set the *Shift* parameter to "H" for *shift*.

The *Shift/No shift* parameter specifies whether or not the VCI bits in the cell header should be shifted based on the HCF field of the cell header on cells arriving from the backplane. It is how Cisco networks convert STI cells to standards based cell formats, and similarly how standards-based cell formats are converted back to STI cells. See Table 4-8 for some general guidelines on how to set the Shift parameter when using virtual trunking through a cloud of non-Cisco equipment versus Cisco equipment using BXMs.)

Note If the network has BNI cards, or if the VPC can route over BNIs, set the **cnfport** *Shift* parameter to "H". This causes the cell, when transported over a public network, to shift these bit spaces to restore them to their normal location that they can be used across a network expecting a standard ATM cell header. If, however, the route through the cloud traverses all BXMs, for example, then configure the **cnfport** command to *No shift* (on the port's entry point into the cloud).

For UXM cards, you cannot configure the *Shift* parameter—the Shift setting is always *N*, or *Shift off*.

Table 4-8 General Guidelines on setting cnfport Shift on/Shift off parameter for Virtual Trunking

	Non-Cisco Cloud	Cisco BXM Cloud
BNI Virtual Trunks	Shift off	Shift off
BXM/UXM Virtual Trunks	Shift off	Shift on

Step 4 Execute **addcon**. In the cloud network, add a virtual path ASI connection for each end of the virtual trunk that is to be routed through the cloud. An example of the syntax for this is:

addcon joker 5.1.1.* swstorm 6.2.10.*

where 5.1 and 6.2 are ASI ports that are hooked up and configured for virtual trunking. DACS connections are acceptable.

Note that the third number is the VPI, which must correspond to the virtual trunk VPI configured with **cnftrk** in step 4. For UXM/BXM UNI virtual trunks, the usable range of VPIs is 1 to 255. For UXM/BXM NNI virtual trunks, the usable range of VPIs is 1-4095.

The CBR/VBR parameter must also correspond to the virtual trunk type of the virtual trunk. For T3, set PCR to 96000 and CDTV to 24000 for the connection so that the ASI does not drop cells. Cisco recommends these values based on testing.

Step 5 Configure BXM trunks. Use **uptrk** to enable the virtual trunk on the port. Take this step if the ATM cloud provider has assigned the VPC. On BXMs that connect to the cloud's ASI ports, configure the virtual trunks, as follows:

uptrk *slot.port.vtrk*

If the cloud is already configured, the alarm on the virtual trunk should clear.

cnftrk *slot.port.vtrk*

When you use **cnftrk** to configure the virtual trunk, make sure the virtual trunk type and VPI correspond to the existing ASI Virtual Path connections (that is, make sure that the virtual trunk matches the cloud's VPC configuration, uses the correct cell format (UNI or NNI), and that HCF-based shifting is *Shift on*.)

Note Ports on UXM cards that connect to a cloud must always be set to *Shift off*. Connections between a port set to Shift on and a port set to Shift off are not guaranteed.

Step 6 Optionally, use **cnfrsrc** to configure the number of connection IDs (conids) and the bandwidth available on the trunk. (Refer to the **cnfrsrc** command in this chapter.)

Step 7 Use **addtrk** to add the virtual trunk to the network topology.

addtrk *slot.port.vtrk*

The parameters *slot.port.vtrk* on a BXM card can have the following values:

- Slot can be 1–6, 9–14.
- Port is the physical port number, which can be 1–3 for T3/E3 or 1–2 for OC-3/STM1.
- Vtrk is the virtual trunk number, which (for BXMs) can be 1–31 for T3/E3.

Note BXM cards support up to 31 virtual trunks, while UXM cards support up to 15 virtual trunks.)

Note The two ends of a virtual trunk can have different port interfaces. For example, a virtual trunk supported by a UXM-OC-3 on one end can be supported by a BXM-T3 at the other end. However, both ends of the trunk must have the same trunk bandwidth, connection channels, cell format, and traffic classes. The **addtrk** command verifies this when you add the trunk.

Routing with Virtual Trunks

Virtual trunks appear in the routing topology map as available trunks for routing. The existing physical trunk characteristics, such as bandwidth and satellite/terrestrial type, apply to virtual trunks. The routing algorithm must take into account additional criteria when virtual trunks are in the routing topology:

- Virtual Trunk Existence - Routing has special restrictions and conid assignments for a virtual trunk. For example, VPC's may not be routed over a virtual trunk.
- Traffic Classes - The unique characteristics of CBR, VBR, and ABR traffic are maintained through the cloud as long as the correct type of virtual trunk is used. You configure the traffic classes allowed per virtual trunk with **cnftrk**. The routing algorithm excludes virtual trunks whose traffic class is not compatible with the candidate connection to be routed.
- Connection Identifier (Conid) Capacity - Each virtual trunk has a configurable number of connection channels reserved from the card. The routing algorithm checks for adequate channel availability on a virtual trunk before selecting the trunk for a route.

Virtual Trunk Bandwidth

The total bandwidth of all the virtual trunks in one port cannot exceed the maximum bandwidth of the port. The trunk loading (load units) is maintained per virtual trunk, but the cumulative loading of all virtual trunks on a port is restricted by the transmit and receive rates for the port.

Virtual Trunk Connection Channels

The total number of connection channels of all the virtual trunks in one port cannot exceed the maximum number of connection channels of the card. The number of channels available is maintained per virtual trunk.

Cell Transmit Address Translation

All cells transmitted to a virtual trunk have a translated cell address. This address consists of a VPI chosen by the user and a VCI (ConId) chosen internally by the software. The trunk firmware is configured by the software to perform this translation.

Cell Receive Address Lookup

The user-chosen VPI is the same for all cells on a virtual trunk. At the receiving end, multiple virtual trunks can send cells to one port. The port must be able to determine the correct channel for each of these cells. The VPI is unique on each trunk for all the cells, but the VCI may be the same across the trunks. Each port type has a different way of handling the incoming cell addresses. This applies to both the BXM and UXM cards.

Selection of Connection Identifier

For connections, the associated LCNs are selected from a pool of LCNs for the entire card. Each virtual trunk can use the full range of acceptable conid values. The range consists of all the 16-bit values (1-65535) excluding the node numbers and blind addresses. A port uses the VPI to differentiate connections that have the same conid.

You can change the number of channels per virtual trunk after the trunk has been added to the network. Decreasing the number of channels on an added virtual trunk will cause connection reroutes, but increasing the number of channels on an added virtual trunk will NOT cause connection reroutes.

Routing VPCs over Virtual Trunks

A VPC is not allowed to be routed over a virtual trunk. The routing algorithm excludes all virtual trunks from the routing topology. The reason for this restriction is due to how the virtual trunk is defined within the ATM cloud.

The cloud uses a VPC to represent the virtual trunk. Routing an external VPC across a virtual trunk would consist of routing one VPC over another VPC. This use of VPCs is contrary to its standard definition. A VPC should contain multiple VCCs, not another VPC. In order to avoid any non-standard configuration or use of the ATM cloud, VPCs cannot be routed over a virtual trunk through the cloud.

Configuration Requirements

The primary commands you use to configure virtual trunks are **cnftrk, cnfrsrc,** and **cnftrkparm**.

Note A virtual trunk cannot be used as a feeder trunk. Feeder connections cannot be terminated on a virtual trunk.

Configuration with **cnftrk**

cnftrk: the main parameters are transmit trunk rate, trunk VPI, Virtual Trunk Type, Connection Channels, and Valid Traffic Classes.

The VPI you configure for a virtual trunk must match the VPI of the VPC in the public ATM cloud. Every cell transmitted to the virtual trunk has this VPI value. Valid VPC VPIs depend on the port type as shown in Table 4-9.

Table 4-9 VPI Ranges

Port Type	Valid VPI Range
BXM/UXM (UNI)	1-255
BXM/UXM (NNI)	1-4095
BNI T3/E3	1-255
BNI OC-3	1-63

Configuration with **cnfrsrc**

You use **cnfrsrc** to configure conids (lcns) and bandwidth. The conid capacity indicates the number of connection channels on the trunk port that are usable by the virtual trunk.

This number cannot be greater than the total number of connection channels on the card. The maximum number of channels is additionally limited by the number of VCI bits in the UNI cell header. For a virtual trunk, the number is divided by the maximum number of virtual trunks on the port to determine the default. You configure this value with the **cnfsrc** command on the BPX. Table 4-10 lists the number of connection ids for virtual trunks on various cards.

Table 4-10 Maximum Connection IDs (LCNs)

Port Type	Maximum Conids	Default
BXM/UXM	1-(number of channels on the card)	256
BNI T3/E3	1-1771	256
BNI OC-3	1-15867 (3837 max/vtrk	256

Configuration with cnftrkparm

cnftrkparm: BXM and UXM virtual trunks have all the configuration parameters for queues as physical trunks.

The integrated alarm thresholds for major alarms and the gateway efficiency factor is the same for all virtual trunks on the port. Note that BNI VTs are supported by a single queue and do not support configuration of all the Advanced CoS Management queues on a single virtual trunk.

VPC Configuration with the ATM Cloud

For the virtual trunk to successfully move data through an ATM cloud, the cloud must provide some form of connectivity between the trunk endpoints. The ATM equipment in the cloud must support virtual path switching and move incoming cells based on the VPI in the cell header.

A virtual path connection (VPC) is configured in the cloud to join two endpoints. The VPC can support either CBR, VBR, or ABR traffic. A unique VP ID per VPC is used to moved data from one endpoint to the other. The BPX nodes at the edge of the cloud send in cells that match the VPC's VPI value. As a result the cells are switched from one end to the other of the ATM public cloud.

Within the ATM cloud, one virtual trunk is equivalent to one VPC. Because the VPC is switched with just the VPI value, the 16 VCI bits (from the ATM cell format) of the ATM cell header are passed transparently through to the other end.

If the public ATM cloud consists of BPX nodes using BXM cards, the access points within the cloud are BXM ports. If the cloud consists of IGX nodes, the access points within the cloud are UXM ports.

If the link to the public cloud from the private network is using BNI cards, then access points within the cloud are ASI ports. The BNI card uses an STI header. The ASI port cards within the cloud should be configured to not shift the VCI when forming the STI header. The command cnfport allows you to configure the Shift parameter to *Shift off* on the port.

For more guidelines and information on configuring virtual trunks and setting the cnfport HCF shift parameter, refer to the "More Guidelines on VPC Configuration within the ATM Cloud" section on page 4-41.

Virtual Trunk Interfaces

The two ends of a virtual trunk can have different types of port interfaces. For example, a virtual trunk may contain a T3 port at one end of the ATM cloud and an OC-3 port at the other end. However, both ends of the trunk must have the same bandwidth, connection channels, cell format, and traffic classes. This requirement is automatically checked when a trunk is added.

Virtual Trunk Traffic Classes

All types of traffic from a private network using Cisco nodes are supported through a public ATM cloud. The CBR, VBR, and ABR configured virtual trunks within the cloud should be configured to carry the correct type of traffic.

- CBR Trunk: ATM CBR traffic, voice/data/video streaming, and so on.
- VBR Trunk:ATM VBR traffic, Frame Relay traffic, and so on.
- ABR Trunk:ATM ABR traffic, Optimized Bandwidth Management traffic, and so on.

A CBR configured trunk is best suited to carrying delay sensitive traffic such as voice/data, streaming video, and ATM CBR traffic, and so on.

A nrt-VBR configured trunk is best suited to carrying Frame Relay and nrt-VBR traffic, and so on.

An ABR configured trunk is best suited to carrying Optimized Bandwidth Management and ABR traffic, and so on.

Two-stage queueing at the egress of virtual trunks to the ATM cloud allows shaping of traffic before it enters the cloud. However, the traffic is still routed on a single VPC and may be affected by the traffic class of the VPC selected.

A user can configure any number of virtual trunks up to the maximum number of virtual trunks per slot (card) and the maximum number of logical trunks per node. These trunks can be any of the three trunk types: CBR, VBR, or ABR.

A user can configure any number of virtual trunks between two ports up to the maximum number of virtual trunks per slot and the maximum number of logical trunks per node. These trunks can be any of the three trunk types.

Virtual Trunk Cell Addressing

Cells transmitted to a virtual trunk use the standard UNI or NNI cell format.

The trunk card at the edge of the cloud ensures that cells destined for a cloud VPC have the correct VPI/VCI. The VPI is an 12-bit value ranging from 1-4095. The VCI is a 16-bit value ranging from 1-65535.

BXM/UXM Two Stage Queueing

The UXM and BXM share the same queueing architecture. The egress cells are queued in two stages. First they are queued per Virtual Interface (VI), each of which supports a virtual trunk. Within each VI, the traffic is queued as per its normal OptiClass traffic type. In other words, voice, Time-Stamped, Non Time-stamped, High Priority, BDATA, BDATB, CBR, VBR, and ABR traffic is queued separately. The overall queue depth of the VI is the sum of all the queue depths for all the available queues. The user does not directly configure the VI.

The user command **cnftrkparm** is used to configure the queues within the virtual trunk.

Virtual Trunking Configuration

Connectivity is established through the public ATM cloud by allocating virtual trunks between the nodes on the edge of the cloud. With only a single trunk port attached to a single ATM port in the cloud, a node uses the virtual trunks to connect to multiple destination nodes across the network thereby providing full or partial meshing as required.

From the perspective of the Cisco node, a virtual trunk is equivalent to a VPC provided by an ATM cloud where the VPC provides the connectivity through the cloud.

Virtual Trunk Example

The following is a typical example of adding one virtual trunk across an ATM network. On one side of the cloud is a BPX with a BXM trunk card in slot 4. On the other side of the cloud is an IGX with a UXM trunk card in slot 10. A virtual trunk is added between port 3 on the BXM and port 2 on the UXM (see Figure 4-4).

Perform the following: .

Step 1	Initial Setup		Contact Customer Service to enable virtual trunking on the nodes in your network.
Step 2	In the public ATM cloud		Obtain the VPCs for the virtual trunks for the service provider. These are the VPCs that are configured within the ATM cloud by the service provider to support the virtual trunks.
Step 3	At BPX_A	uptrk 4.3.1 uptrk 4.3.2	Up virtual trunks 4.3.1 and 4.3.2 on BXM port 4.3

Step 4	At BPX_A	cnftrk 4.3.1 ... cnftrk 4.3.2 ...	Configure the virtual trunks to match the cloud's VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, and so on.
Step 5	At BPX_A	cnfrsrc 4.3.1 ... cnfrsrc 4.3.2 ...	Configure the number of conids, bandwidth, and so on., available for the virtual trunks.
Step 6	At BPX_B	uptrk 5.1.1 uptrk 5.1.2	Up virtual trunks 5.1.1 and 5.1.2 on BXM port 5.1
Step 7	At BPX_B	cnftrk 5.1.1 ... cnftrk 5.1.2 ...	Configure the virtual trunks to match the cloud's VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, and so on.
Step 8	At BPX_B	cnfrsrc 5.1.1 ... cnfrsrc 5.1.2 ...	Configure the number of conids, bandwidth, and so on., available for the virtual trunks.
Step 9	At IGX_A	uptrk 10.2.1 uptrk 10.2.3	Up virtual trunks 10.2.1 and 10.2.3 on IGX trunk port 10.2
Step 10	At IGX_A	cnftrk 10.2.1 ... cnftrk 10.2.3 ...	Configure the virtual trunks to match the cloud's VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, and so on.
Step 11	At IGX_A	cnfrsrc 10.2.1 ... cnfrsrc 10.2.3 ...	Configure the number of conids, bandwidth, and so on., available for the virtual trunk.
Step 12	At BPX_A	addtrk 4.3.1 IGX_A 10.2.1 addtrk 4.3.2 BPX_B 5.1.1	Add the virtual trunks between three nodes. Using addtrk 10.2.1 ... at IGX_A and addtrk 5.1.1 ... at BPX_B would also add the virtual trunks.
Step 13	At BPX_B	addtrk 5.1.2 IGX_A 10.2.3	Add the virtual trunks between the two nodes. Using addtrk 10.2.3 ... at IGX_A would also add the virtual trunks.

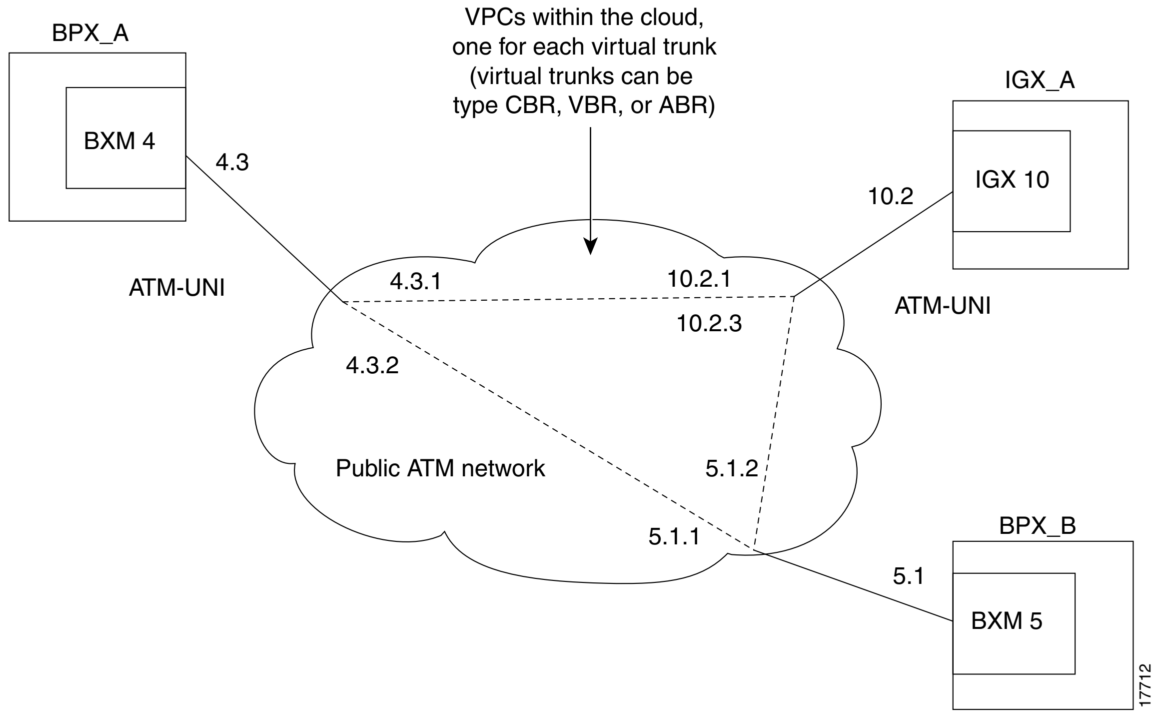
The VPI values chosen using **cnftrk** must match those used by the cloud VPC. In addition, both ends of the virtual trunk must match with respect to: Transmit Rate, VPC type, traffic classes supported, and the number of connection channels supported. The **addtrk** command checks for matching values before allowing the trunk to be added to the network topology.

The network topology as seen from a **dsptrks** command at BPX_A would be:

BPX_A 4.3.1-10.2.1/IGX_A

BPX_A 4.3.2-5.1.1/BPX_B

Figure 4-4 Addition of Virtual Trunks across a Public ATM Network



Trunk and Line Redundancy

Trunk redundancy can refer to one of two features:

- SONET Automatic Protection Switching (APS)
- Y-redundancy

APS Redundancy

APS line redundancy is supported. APS line redundancy is only available on BXM SONET trunks and is compatible with virtual trunks. The trunk port supporting virtual trunks may have APS line redundancy configured in the same way it would be configured for a physical trunk. The commands **addapsln**, **delapsln**, **switchapsln**, and **cnfapsln** are all supported on virtual trunk ports. The syntax for these commands still accept trunk port parameters as *slot.port*.

Y-Redundancy

The original trunk redundancy feature is an IGX only feature and is not supported for virtual trunks. The commands **addtrkred**, **deltrkred**, and **dsptrkred** are rejected for virtual trunks.

Networking

Virtual Trunk Configuration

The characteristics of a virtual trunk used by connection routing are maintained throughout the network. This information - virtual trunk existence, traffic classes and connection channels - is sent to every node to allow the routing algorithm to use the trunk correctly. Routing only uses those virtual trunks which can support the traffic type of the connection.

ILMI (Integrated Local Management Interface)

For ATM clouds that do not have Cisco equipment (such as BPX or IGX nodes), previous to release 9.2, you had to configure the ATM ports to block signalling traffic to the Cisco nodes. In this release, you no longer need to configure the ATM ports to block signalling traffic due to ILMI (Integrated Layer Management Interface) signalling support.

Blind Addressing

Each virtual trunk is assigned a blind address. In general terms the blind address is used by a node to communicate to the node at the other end of a trunk. Specifically, the blind address is used for sending messages across a virtual trunk when a trunk is added, and for sending messages for the Trunk Communication Failure testing.

VPC Failure Within the ATM Cloud

Any VPC failure within the ATM cloud generates a virtual trunk failure in the Cisco network. This trunk failure allows applications (for example, connection routing) to avoid the problem trunk.

Upon receiving notification of a VPC failure, the trunk is placed into the "Communication Failure" state and the appropriate trunk alarms are generated. The trunk returns to the "Clear" state after the VPC clears and the trunk communication failure test passes.

Trunk Alarms

Logical Trunk Alarms

Statistical alarming is provided on cell drops from each of the Advanced CoS Management (formerly called OptiClass) queues. These alarms are maintained separately for virtual trunks on the same port.

Physical Trunk Alarms

A virtual trunk also has trunk port alarms which are shared with all the other virtual trunks on the port. These alarms are cleared and set together for all the virtual trunks sharing the same port.

Physical and Logical Trunk Alarm Summary

A listing of physical and logical trunk alarms is provide in Table 4-11.

Table 4-11 Physical and Logical Trunk Alarms

	Physical							
Alarm Type	**T1**	**E1**	**T3**	**E3**	**SONET**	**Logical**	**Statistical**	**Integrated**
LOS	X	X	X	X	X		X	X
OOF	X	X	X	X	X		X	X
AIS	X	X	X	X	X		X	X
YEL	X	X	X	X	X			X
PLCP OOF			X					X
LOC				X	X			X
LOP					X			X
PATH AIS					X			X
PATH YEL					X			X
PATH TRC					X			X
SEC TRC					X			X
ROOF	X	X						X
FER	X	X						X
AIS16	X	X					X	X
IMA	X	X						X
NTS Cells Dropped						X	X	
TS Cells Dropped						X	X	
Voice Cells Dropped						X	X	
Bdata Cells Dropped						X	X	
BdatB Cells Dropped						X	X	
HP Cells Dropped						X	X	
CBR Cells dropped						X	X	
VBR Cells dropped						X	X	
ABR Cells dropped						X	X	

Event Logging

All trunk log events will display the virtual trunk number. The examples in Table 4-12 and Table 4-13 show the log messaging for activating and adding a virtual trunk 1.2.1.

Table 4-12 IGX Log Messaging for Activating and Adding VTs

Class	Description
Info	NodeB at other end of TRK 1.2.1
Clear	TRK 1.2 OK
Major	TRK 1.2 Loss of Sig (RED)
Clear	TRK 1.2.1 Activated

Table 4-13 BPX Log Messaging for Activating and Adding VTs

Class	Description
Info	NodeB at other end of TRK 1.2.1
Clear	TRK 1.2.1 OK
Major	TRK 1.2.1 Loss of Sig (RED)
Clear	TRK 1.2.1 Activated

Error messages

Added error messages for virtual trunks are listed in Table 4-14.

Table 4-14 Virtual Trunk Error Messages

Message	- Description
"Port does not support virtual trunking"	Port is not configured for virtual trunks
"Port configured for virtual trunking"	Port is not configured for a physical trunk
"Invalid virtual trunk number"	Virtual trunk number is invalid
"Maximum trunks per node has been reached"	Trunk limit per node has been reached
"Invalid virtual trunk VPI"	Virtual trunk VPI is invalid
"Invalid virtual trunk traffic class"	Virtual trunk traffic class is invalid
"Invalid virtual trunk VPC type"	Virtual trunk VPC type is invalid
"Invalid virtual trunk conid capacity"	Virtual trunk conid capacity is invalid
"Mismatched virtual trunk configuration"	Ends of virtual trunk have different configuration
"Maximum trunks for card has been reached"	The trunk card is out of VIs

Virtual Trunking Commands

The following command descriptions are summaries specific to virtual trunk usage on the BPX, using the BXM cards. For information about the BPX, refer to the BPX 8600 Series documents. For information about the UXM, refer to the IGX 8400 Series documents. Also, refer to the Cisco WAN Manager documents for application information using a graphical user interface for implementing command functions.

- Three main commands are used for configuring virtual trunks. These are **cnftrk**, cnftrkparm, and **cnfrsrc**, which configure all port and trunk attributes of a trunk. When a physical port attribute change is made, the user is notified that all trunks on the port are affected.
- Virtual trunks support APS redundancy on BXM OC-3 and OC-12 ports. The commands **addapsln**, **delapsln**, **switchapsln**, and **cnfapsln** are the main commands. For more information, refer to the section on APS Redundancy in this manual. The prior Y-redundancy is not supported by virtual trunks, nor the related commands addtrkred, deltrkred, and dsptrkred.

Note Since a virtual trunk is defined within a trunk port, its physical characteristics are derived form the port. All the virtual trunks within a port have the same port attributes.

If a physical trunk is specified on a physical port which supports multiple virtual trunks, the command is applied to all virtual trunks on the physical port. **If a virtual trunk is specified for a command that configures information related to the physical port, then the physical port information is configured for all virtual trunks.**

With Release 9.2, the BPX statistics organization is modified to separate logical and physical trunk statistics. This is also the method used on the UXM card on the IGX 8400 series switches.

Virtual Trunks Commands Common to BXM and UXM

The following commands are available on both the IGX and the BPX and have the same results. Refer to the IGX 8xxx Series documentation for information the IGX and UXM.

The entries in Table 4-15 that are marked with a [*} are configured on a logical trunk basis, but automatically affect all trunks on the port when a physical option is changed. For example, if the line framing is changed on a virtual trunk, all virtual trunks on the port are automatically updated to have the modified framing.

Table 4-15 Virtual Trunk Commands Common to BXM and UXM (IGX)

Command	Description
addtrk	adds a trunk to the network
ckrtrkerrs	clears the trunk errors for a logical trunk
clrtrkstats	clears the summary trunk statistics for a logical trunk
clrphyslnerrs	clears trunk errors for a physical line
cnflnalm	configures the statistical alarm thresholds for trunks and ports (affects all trunks on node)
cnftrk	configures a logical trunk [*]
cnftrkparm	configures the trunk parameters of a logical trunk [*]
cnftrkstats	configures the interval statistics collection for a logical trunk
cnfphyslnstats	configures the interval statistics for a physical line

Table 4-15 Virtual Trunk Commands Common to BXM and UXM (IGX) (Continued)

Command	Description
deltrk	deletes a trunk from the network
dntrk	downs a trunk
dsplogtrk	displays the logical trunk information
dspphyslnstatcnf	displays the statistics configuration for a physical line
dspphyslnstathist	displays the statistics collection result for a physical line
dsptrkcnf	displays the trunk configuration
dsptrkcons	displays the number of connections routed over a trunk
dsptrkerrs	displays the trunk errors for a logical trunk
dsptrks	displays the upped/added trunks
dsptrkstatcnf	displays the configured statistics collection for a trunk
dsptrkstathist	displays the statistics collection results for a trunk
dsptrkstats	displays the summary trunk statistics for a trunk
dsptrkutl	displays the utilization/traffic for a logical trunk
prtphyslnerrs	print the trunk errors for a physical line
prttrkerrs	prints the trunk errors for a logical trunk
prttrks	prints the active logical trunks
uptrk	ups a trunk

Virtual Trunk UXM Commands

The commands listed in Table 4-16 are IGX specific, or behave differently than their BPX counterparts. Refer to the IGX 8400 Series documentation for further information about UXM virtual trunk commands.

Table 4-16 Virtual Trunk UXM Commands

Command	Description
clrtrkalm	clears the statistical alarms for a logical trunk (affects logical trunk alarms only)
clrphyslnalm	clears statistical alarms for a physical trunk (IGX only)
dspphysln	displays physical line status (IGX only)
clrtrkstats	clear trunk stats (IGX only)

Virtual Trunk BXM/BNI commands

The commands listed in Table 4-17 are BPX-specific.

Table 4-17 Virtual Trunk Commands BXM/BNI

Command	Description
clrtrkalm	Clears the statistical alarms for a logical trunk [*]. (Clears logical and physical trunk alarms)

Table 4-17 Virtual Trunk Commands BXM/BNI

Command	Description
cnfrsrc	Configure cell rate and number of conids (BXM only)

Permutations of Virtual Trunks you can Configure through the ATM Cloud

Table 4-18 lists the permutations of virtual trunks that you can set up to pass through the ATM cloud. For example, you can set up a virtual trunk between a BXM card with a T3, E3, OC-3, or OC-12 interface and a UXM card with a T3, E3, or OC-3 interface.

Table 4-18 Permutations of Virtual Trunks that can be Configured through ATM Cloud

	BNI Card (T3/E3/OC-3)	BXM Cards (T3/E3/OC-3/ OC-12)	UXM Cards (T3/E3/OC-3)	UXM-AIM Card
BNI (T3/E3/OC-3)	yes	no	no	no
BXM (T3/E3/OC-3/OC-12)	no	yes	yes	yes
UXMs (T3/E3/OC-3)	no	yes	yes	yes
UXM-AIM	no	yes	yes	yes

Ports and Trunks Feature in Release 9.2

The Ports and Trunks feature lets you configure multiple trunk lines and circuit lines on a single BXM or UXM card simultaneously. In previous releases, when a single port is upped as a trunk (by using **uptrk** command), all the remaining ports on that card are treated as trunks. Similarly, in releases previous to Release 9.2, when a single port is upped as a circuit line (by using the **upln** command), all the remaining ports on the card are treated as circuit-line ports.

The way virtual trunk numbers are displayed is new for IGX trunks. IMA trunk ports are referenced by the first physical line of the trunk port after **uptrk** has been executed. For example, you can execute *uptrk 1.5-8.9*, then you can up a second trunk on the same trunk port with *uptrk 1.5.11*.

In support of the Ports and Trunks feature, a single BXM card can support physical trunks, virtual trunks, feeder trunks and UNI interfaces simultaneously; a UXM card can support physical trunks, virtual trunks and UNI interfaces simultaneously. For example, a BXM card can have:

- port 1 upped as a physical trunk
- port 2 upped as a feeder trunk
- port 3 upped with multiple virtual trunks
- port 4 upped as a UNI interface

Below lists the interface types that can be supported on a single card:

Table 4-19 Interface Types that can be Supported on Single Card

	ASIs (T3/E3/OC-3)	BNIs (T3/E3/OC-3)	BXM (T3/E3/OC-3/OC-12)	UXMs (T3/E3/OC-3)	UXM-AIM
SES Feeder	no	yes	yes (except OC-12)	no	no
IPX Feeder[1]	no	yes	no	no	no
Physical Trunks	no	yes	yes	yes	yes
Virtual Trunks	no	yes	yes	yes	yes
UNI Port	yes	no	yes	yes	yes
Virtual UNIs	no	no	no	no	no

1 Note that an IPX node running Release 9.1, 8.5, and 8.4 can interoperate with nodes running Release 9.2; however, an IPX node cannot support Release 9.2 switch software.

Virtual Trunking Features Supported in Release 9.2

These virtual trunking features are supported in Release 9.2:

- Cell format for BXM/UXM virtual trunks. Standard UNI and NNI cell headers are used, as opposed to the Strata-UNI format used on BNI virtual trunks. This implies that BNI virtual trunks are not compatible with BXM or UXM virtual trunks. A VPI range of 1-4095 is supported.
- Cell Queueing. A virtual trunk is supported by a Virtual Interface (VI) on the BXM and UXM cards. Each virtual interface is a collection of traffic based queues. Thirty-one (31) multiclass virtual trunks are supported per BXM and 15 per UXM (all types) using virtual interfaces. You can define virtual trunks on a port by port basis.
- Support for current trunk statistics
- Traffic shaping on physical and virtual trunks is supported. This feature operates in a similar manner as UNI traffic shaping. (See the **cnfport** command in the "cnfport" section on page 9-47 for information on configuring traffic shaping.)
- Support current trunk and line configuration and debug options.
- Support ILMI (Integrated Local Management Interface) between a virtual trunk and a foreign switch. Integrated Local Management Interface is a bidirectional protocol for exchanging configuration, status, and control information between two ATM Interface Management Entities (IMEs).
- BXM virtual trunks can work over another BPX network acting as the ATM cloud. Testcon (**tstcon** command), test delay, and Optimized Bandwidth Management must operate over virtual trunks in this configuration.
- Virtual trunks are accessible to VSI controllers. You cannot partition the virtual trunk. The trunk is entirely owned by either a VSI controller or Automatic Routing Management (formerly called AutoRoute).
- F4/F5 OAM flows supported are as follows:
  - AIS/RDI OAM Flows:

    F5 (VCC) flows are supported for end to end connections through a virtual trunk.

    F4 (VPC) VPC is not supported through virtual trunks

F4 flows are not supported between the ATM cloud network and virtual trunk

— OAM (test delay) Loopback:

F5 (VCC) flows are supported for end to end connections through a virtual trunk

F4 (VPC)VPC is not supported through virtual trunks

Impact of Other Features on Virtual Trunking in Release 9.2

LMI/ILMI on the BXM Firmware. ILMI monitoring on virtual trunks is supported for the new card types. LMI and ILMI were implemented in the BCC switch software previous to Release 9.2. Because switch software must process multiple LMI/ILMI requests from all the configured ports in the BPX node, this is a severe drain on the available processor bandwidth on the BCC. For this reason, the LMI/ILMI functionality has moved from the switch software in Release 9.1 to the BXM card firmware in Release 9.2.

Hitless Rebuild feature. The hitless trunk re-configuration feature introduces new flexibility in the options that you can configure on active trunks. This will affect some of the new and existing virtual trunk options.

BXM & UXM Card Interface Capacities

BXM and BXM Enhanced cards can support up to a maximum of 31 interfaces per card. The UXM and UXM Enhanced cards can support up to a maximum of 15 interfaces per card.

For each interface upped on a card's physical trunk, feeder trunk, virtual trunk, or UNI interface, a single virtual interface is used. This implies that on BXM cards any combination of 31 interfaces can be supported, and for UXM any combination of 15 interfaces can be supported. See Table 4-20 for information on BXM and UXM interface capacities.

Table 4-20 BXM and UXM Interface Capacities

	BXM (T3/E3/OC-3/OC-12)	UXM (T3/E3/OC-3/AIM)	BXM (T3/E3/OC-3/OC-12)	BXM (T3/E3/OC-3/OC-12)
SES Feeder	4 feeder ports	N/A	4 feeder ports	0 feeder ports
IGX Feeder	N/A	N/A	no	no
Physical Trunks	4 physical trunks	1 physical trunks	4 physical trunks	0 physical trunks
Virtual Trunks	10 Virtual Trunks on 1 port	5 Virtual Trunks on 1 port	0 Virtual Trunks	10 Virtual Trunks on 1 port
UNI port	3 UNI ports	1 UNI ports	4 UNI ports	0 UNI ports
Total VIs used	21 VIs	7 VIs	12 VIs	10 VIs
Total Ports used	12 ports	4 ports	12 ports	1 port

Channel Capacities

For legacy UXM/BXM cards, approximately 270 networking channels are required for each virtual trunk. For example, UXM cards allocate 4320 channels if all 16 virtual trunks are upped on a single card. BXM cards allocate 8640 channels if all 32 virtual trunks are upped. Table 4-21 lists channel capacities for BXM and UXM cards.

Table 4-21 Channel Capacities for BXM and UXM Cards

Number of Virtual Trunks	# Networking Channels for Legacy (non-Enhanced) Cards	Number of Networking channels for Enhanced Cards
1 virtual trunk	270 chans	270 chans
2 virtual trunks	540 chans	270 chans
3 virtual trunks	810 chans	270 chans
16 virtual trunks	4320 chans	270 chans
32 virtual trunks	8640 chans	270 chans

This implies that for UXM legacy cards, upping all 15 virtual trunks would consume 4320 gateway channels for networking, leaving none for user traffic. For this reason, the number of virtual trunks upped on a legacy UXM card is limited. Use the **cnftrkport** command to control the number of trunks upped on a UXM card.

Errors and Alarm Handling

Errors and alarms function the same as in releases previous to Release 9.2. The Trunks and Ports feature continues to support:

- slot errors and alarming
- trunk/line errors and alarming
- statistical line alarms
- integrated line alarms
- connection conditioning

Physical Interface Specifications and Applicable Standards

For virtual trunking, the trunk cell format will be either standard UNI or NNI.

The current ATM and physical layer standards are the same as in Release 9.1.

Commands you use to Configure Virtual Trunking

The following commands let you configure virtual trunking on a BXM on a BPX, and a UXM on an IGX node:

- **uptrk** slot.port[.vtrk]
- **dntrk** slot.port[.vtrk]
- **addtrk** slot.port[.vtrk]
- **deltrk** slot.port[.vtrk]
- **dsptrkstats** slot.port[.vtrk]
- **dsptrkerrs** slot.port[.vtrk]
- **dsplog** entries display the virtual trunk (*vtrk*) number
- **cnftrk** slot.port[.vtrk]

- **cnftrkparm** slot.port[.vtrk]

Commands to Configure Trunks and Ports on Same Card

Following are the commands you use to configure trunks, lines, ports, and connections on BXM and UXM cards:

- Card Commands: **upcd, dncd**
- Circuit Line Commands: **upln, dnln, cnfln, cnfrsrc**
- Trunk Commands: **uptrk, dntrk, cnftrk, cnfrsrc, cnftrkparm**
- Port Commands: **upport, dnport, cnfport, cnfportq**
- Connection Commands: **addcon, delcon, cnfcon**

Reliability, Availability, and Serviceability (RAS) Feature Support

- Availability. Networking channels are allocated dynamically. This can provide more user channels. Card redundancy/hot standby is supported for RAS features.
- Serviceability. The Ports and Trunks feature lets you configure both service provider and trunk interfaces from the same card.

Version Interoperability

Virtual trunking is not supported in a mixed network (that is, of mixed releases 8.4, 8.5, 9.1, and 9.2). You must upgrade nodes to Release 9.2 to use virtual trunking.

You can use the Ports and Trunks feature in a network of mixed releases.

To support virtual trunk networking channels and VSI on virtual trunks, you must upgrade to new firmware. Refer to 9.2 release notes for system requirements.

Virtual Trunking Features Supported on BXM and UXM Cards

The BXM and UXM cards come with several combinations of number of virtual interfaces, number of ports, and number of channels. Refer Table 4-22.

Table 4-22 VIs, Ports, and Channels Supported on BXM and UXM Cards

	Number of VIs	Max LCNs	Default LCNs
BXM	31	32000	16320
UXM	15	8000	8000

- The maximum number of virtual trunks per card equals the number of virtual interfaces.
- The maximum number of logical (physical and virtual) trunks per node allowed are:
  - 64 logical (physical and virtual) trunks per BPX node
  - 32 logical (physical and virtual) trunks per IGX node

- The total connection channels (LCNs) per card are shared by all the trunks (physical and virtual) on the card. The number of channels used by all the virtual trunks on a port cannot exceed the total number of LCNs on the card. The number of LCNs on a given trunk is further limited by the port group to which it belongs.
- The number of port groups limits the number of LCNs that you can use on a port. For example, consider an 8-port BXM card with two (2) port groups and a total of 16320 channels. Each port group can access a pool of 8160 channels. Each port can only access the channels in its port group, so each port is limited to a maximum of 8160 channels. Refer to the description of the BXM card and firmware in the *BPX 8600 Series Reference* and *BPX 8600 Series Configuration* guides for a more detailed description of port groups.
- The total bandwidth per port is shared by all the virtual trunks on the port. The sum of bandwidth of all the virtual trunks on a port cannot exceed the bandwidth of the port. Following are several maximum supported bandwidth per physical line type:
    - T3 (PLCP mode) 96000 cells/second
    - T3 (HEC /Direct mapping mode) 104000 cells/second
    - E3 80000 cells/second
    - OC-3 353208 cells/second
    - OC-12 1412830 cells/second
    - IMA (No. of physical lines)* (T1 or E1) cells/second
- Queue depth per port is shared by all the logical (physical and virtual) trunks on the card. The queues are dynamic, which allows oversubscription of the available queue space. This means that the sum of all the configured queue depths can be larger than the available queue space on the card.
- The two ends of a virtual trunk can have different port interfaces. For example, a virtual trunk supported by a UXM-OC-3 on one end can be supported by a BXM-T3 at the other end.
- BNI virtual trunks are incompatible with UXM and BXM virtual trunks. UXM and BXM virtual trunks are compatible with each other. The incompatibility arises from the cell header formats used by the different cards.
- On the BXM and UXM, virtual trunks support ATM-UNI or ATM-NNI cell format. This is in contrast to physical trunks on these cards, which only support NNI. For a virtual trunk to be added, both ends must use the same cell format.
- Virtual trunking is a chargeable feature. Cisco Customer Service must enable this feature per node by using the **cnfswfunc** command. The **cnfswfunc** command has a privilege level of Service and higher.
- Advanced CoS Management (FairShare and Advanced CoS Management combined) is supported for virtual trunking on the BXM and UXM virtual trunks. Multiple traffic classes are queued and serviced separately.
- APS Line redundancy is supported for virtual trunks.
- Cisco VPCs (Virtual Path Connections) cannot be routed over virtual trunks.
- You cannot configure a virtual trunk as a feeder trunk.
- Following are the VPI limitations for virtual trunks:
    - 1–255 for UXM/BXM UNI virtual trunks
    - 1–4095 for UXM/BXM NNI virtual trunks

- ILMI signalling has been moved to the BXM firmware. The current implementation is in switch software, and is used on physical ports that support virtual trunks. BNI virtual trunks continue to use the current scheme (that is, ILMI signalling is performed by the switch software), but for BXM cards, ILMI signalling will be performed by the BXM firmware. UXM virtual trunks use the same scheme as the BNI, in other words, the protocol will be run by switch software.
- The ATM-UNI supported on the Cisco trunk and ATM cloud is Version 3.0 or later.

Virtual Trunking Features

The BXM and UXM cards come with several combinations of number of virtual interfaces, number of ports, and number of channels. See Table 4-23.

Table 4-23 Virtual Interfaces and LCNs Allowed Per Card

	Number of VIs	Max LCNs	Default LCNs
BXM	31	65535	16320
UXM	15	8000	8000

- The maximum number of virtual trunks per card equals the number of virtual interfaces.
- Maximum number of logical (physical and virtual) trunks per node.
  - — 64 logical trunks per BPX node
  - — 32 logical trunks per IGX node
- Total connection channels per card are shared by all the trunks (physical and virtual) on the card. The number of channels used by all the virtual trunks on a port cannot exceed the total number of channels on the card. The number of channels on a given trunk is further limited by the port group to which it belongs.
- The number of port groups limits the number of channels which may be used on a port. For example, consider an 8 port BXM card with 2 port groups and a total of 16320 channels. Each port group may access a pool of 8160 channels. Each port may only access the channels in its port group, so each port is limited to a maximum of 8160 channels. Refer to the BXM firmware/hardware specification for a more detailed description of port groups.
- Total bandwidth per port is shared by all the virtual trunks on the port. The sum of bandwidth of all the virtual trunks on a port cannot exceed the bandwidth of the port.
  - — T3(PLCP mode 96000 cells/second
  - — T3(HEC /Direct mapping mode104000 cells/second
  - — E3 80000 cells/second
  - — OC-3 353208 cells/second
  - — OC-12 1412830 cells/second
  - — IMA (No. of physlns)* (T1 or E1) cells/second
- Queue depth per port is shared by all the logical (physical and virtual trunks on the card). The queues are dynamic, which allows oversubscription of the available queue space. The sum of all the configured queue depths may be larger than the available queue space on the card.
- The two ends of a virtual trunk can have different port interfaces. For example, a virtual trunk supported by a UXM-OC-3 on one end may be supported by a BXM-T3 at the other end.

- BNI virtual trunks are incompatible with UXM and BXM virtual trunks. UXM and BXM virtual trunks are compatible with each other. The incompatibly arises from the cell formats used by the different cards.
- On the BXM and UXM, virtual trunks support ATM-UNI or ATM-NNI. This is in contrast to physical trunks on these cards, which only support NNI. For a virtual trunk to be added, both ends must use the same cell format.
- Virtual trunking is a chargeable feature, which is enabled with the **cnfswfunc** command on a per-node basis. Because this command has a privilege level of Service and higher, it must be enabled by the Cisco Technical Assistance Center.
- Advanced CoS Management is supported for virtual trunking on the BXM and UXM virtual trunks. Multiple traffic classes are queued and serviced separately.
- Cisco VPCs (Virtual Path Connections) cannot be routed over virtual trunks.
- Virtual trunks cannot be used as feeder trunks.
- APS Line redundancy is supported for virtual trunks.
- VPI limitations on virtual trunks:
  - 1–255 for UXM/BXM UNI virtual trunks
  - 1–4095 for UXM/BXM NNI virtual trunks
- ILMI signalling is moved to the BXM firmware. The current implementation is in switch software, and is used on physical ports which support virtual trunks. In 9.2, BNI virtual trunks will continue to use the current scheme, but the BXM cards will use the firmware implementation. UXM VTs use the same scheme as the BNI, in other words, the protocol will be run by switch software.
- The ATM-UNI supported on the Cisco trunk and ATM cloud is Version 3.0 or later.

Virtual Trunking Limitations

The following lists some items not supported in Release 9.2, or limitations in Release 9.2, related to virtual trunking:

- Pass-through connections
- VSI VPC partitioning
- Multiple virtual trunks per virtual interface
- Support of virtual UNIs
- The maximum number of virtual trunks supported on a UXM is 15.
- The maximum number of virtual trunks supported on a BXM is 31.
- The Peak Interval Timer for port statistics has been increased from 10 seconds to 1 minute.
- Reporting of BXM/UXM virtual interface statistics for RX CLP0 and CLP1 discards only counts user-based traffic. That is, networking traffic is not included in these counts.
- You need to upgrade BXM firmware to support virtual trunking. If virtual trunking is not required, you do not need to upgrade firmware.
- To support this release, you will need to upgrade the UXM firmware.
- F4/F5 OAM flows are NOT supported between the BXM/UXM virtual trunk and the cloud's VPC connection.

Compatibility

The BXM and UXM virtual trunking feature requires Release 9.2 switch software, and new BXM and UXM firmware. The new firmware revisions are backward compatible and support the current physical trunking. The Release 9.2 software is also compatible with the current (Release 9.1) BXM firmware. Release 9.2 software is *not* compatible with Release 9.1 UXM firmware. A UXM firmware upgrade is required for networks running Release 9.2.

Node by node upgrades in Release 9.2 allows interoperability between 9.2 software and 9.1 or 8.5 software. In a network of hybrid releases, you cannot add UXM and BXM virtual trunks. The restriction is enforced because of changes to networking messages, which involve the virtual trunk number and the cell format on virtual trunks.

Virtual Trunking

The virtual trunking feature lets you define multiple trunks within a single trunk port interface. In previous releases, trunking has been associated with the physical existence of a trunk card and port. The virtual trunking capability already exists for the BPX BNI trunk card. In Release 9.2, the virtual trunking capability is now supported on the BXM and UXM trunk cards.

Virtual trunking allows you to define an additional level of trunking within the port resources. This "many-to-one" virtual trunk to port relationship produces a "fanout" trunk capability.

Each Cisco sub-network is connected through the public ATM network with virtual trunks. The trunk interface at the Cisco nodes is either a BNI, BXM or UXM trunk card. Congestion management (RM) cells are passed transparently through the network. Cisco features such as Advanced COS Management (formerly called FairShare Advanced CoS Management) and Optimized Bandwidth Management (formerly called Optimized Bandwidth Management) may not be supported within the public network, but the information is carried through the network. Leased lines may also exist to connect the Cisco sub-networks outside of the ATM network.

How Virtual Trunking Interacts with Virtual Interfaces

The BXM and UXM trunks are the first to use more than one virtual interface per physical port. Each virtual interface aggregates a group of traffic-type based queues. On a physical trunk, only one virtual interface is used. On a physical port supporting multiple virtual trunks, a virtual interface is used to support each virtual trunk. The virtual interfaces are scaled and managed in the same way queues are, regarding their bandwidth, maximum depth, and drop thresholds. This is sometimes referred to as *two-stage queueing* for these virtual trunks.

Virtual Trunking Function Changes

Resource management, networking and connection management are the largest areas affected by this project. A virtual trunk requires special handling, even though it behaves very similarly to a physical trunk. Cells routed on a virtual trunk require special address management as they enter and exit the cloud.

Some functional areas of virtual trunking have changed in Release 9.2:

Resource Management —To ease managing virtual trunks, the software now handles physical and virtual trunk configuration similarly. Virtual trunk configuration of a port level characteristic affects all the virtual trunks on the port. The port characteristics of a trunk consist of the configuration associated with the trunk port. The logical trunk characteristics of a trunk consist of those items not tied directly to the port.

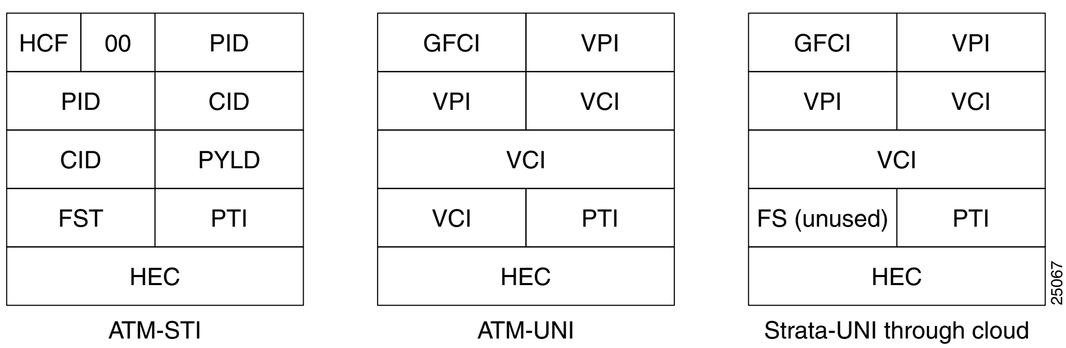
The logical trunks in a node are either virtual or physical trunks. The current trunk commands to up/down, configure, or add/delete a trunk apply to all logical trunks. Trunk statistics are kept for logical trunks.

The logical trunk configuration is stored in the existing logical trunk database. This change allows the number of trunks supported per switch to grow independently of the number of slots and ports per switch.

The way you manage logical trunks is different in Release 9.2. In general, managing virtual interfaces is hidden from the user. Internally, the depth and the bandwidth of the virtual interface are configured based on the aggregate queue depth and bandwidth of all the queues within the virtual interface.

Connection Management—The cell addressing scheme for connections routed through a virtual trunk handles multiple types of traffic flowing through an ATM cloud. The header format of cells may match the ATM-UNI or ATM-NNI format since the port interface to the cloud is a UNI or NNI port. On BNIs, the cell format is modified to store the Optimized Bandwidth Management information in the header. The incompatible cell headers makes BNI to BXM or UXM virtual trunks technically difficult. The solution of adopting the Strata-UNI cell format for all of our virtual trunks has a few distinct disadvantages, including: limiting the number of connections which can be routed, inability to guarantee Optimized Bandwidth Management over the trunks, and propagation of a non-standard cell format. Because of all these issues, BNI to BXM or UXM virtual trunks are not supported.

Figure 4-5 ATM Header Types



Before cells enter the cloud on a virtual trunk, the cell header is translated to a user-configured VPI value for the trunk, and a software configured VCI value which is unique for the cell. As cells are received at the other end of the cloud, this VPI/VCI is mapped back to a correct cell header by the Cisco equipment. The VPI value is identical for all cells on a single virtual trunk, so the VCI contains the unique information needed to determine the final destination of the cell.

NNI virtual trunks have four additional VPI bits in place of the GFC bits in the UNI header. Otherwise, this cell format is the same as the ATM-UNI format.

Connection routing uses existing trunk characteristics in the route selection algorithm. Both virtual and physical trunks appear as logical trunks in the routing topology. Supported traffic classes may be configured on virtual or physical trunks. VPC connections can *not* be routed over virtual trunks.

The trunks and ports feature modifies the way channel allocation is done. Virtual trunk channel allocation will be included in the design from the Trunks and Ports project.

Networking —Virtual trunks appear in the network topology just like physical trunks. Network communication (blind messaging and node-to-node communication) through these trunks is modified to support the cell addressing scheme through the cloud. Information about virtual trunks is stored in each node's Node Information Block (NIB) database.

User Interface —The parsing and display of virtual trunk numbers is new for IGX trunks. IMA trunk ports are referenced by the first physical line of the trunk port after uptrk has been done. For example, a user may *uptrk 1.5-8.9*. A second trunk on the same trunk port may be upped with *uptrk 1.5.11*.

External Interfaces —A virtual trunk description consists of a virtual trunk number appended to a physical port description. The user interface and event logging of trunks support this extra number. The current Cisco WAN Manager messages handle virtual trunks, but require modification to support virtual trunks consisting of multiple physical lines (IMA VTs). IMA VTs are only a concern on the IGX. The BPX uses the same modified interface as the IGX.

Common Control—The trunk configuration database is modified to include the mapping between logical trunks and VI numbers and vice versa. These new database fields are supported in the standby updates and BRAM recovery.

SNMP—The configurable trunk options for *ATM trunk header type(NNI/UNI)* and *Traffic Shaping* are introduced by this project. The corresponding MIB tables are updated for these values.

Establishing a Virtual Trunk Through an ATM Cloud

You establish connectivity through an ATM cloud by allocating virtual trunks between the nodes on the edge of the cloud. With only a single trunk port attached to a single ATM port in the cloud, a node uses the virtual trunks to connect to multiple destination nodes on the other side of the cloud.

A virtual trunk from the Cisco perspective is equivalent to a VPC provided by an ATM cloud. The VPC provides the connectivity through the cloud. To correctly set up a virtual trunk, the following steps are required.

Step 1 Secure a VPC from the ATM cloud provider.

Step 2 Use **uptrk** to enable the virtual trunk on the port.

Step 3 Use **cnftrk** to configure the virtual trunk to match the cloud's VPC configuration.

Step 4 Use **cnftrk** to configure the trunk to use the correct cell format (UNI or NNI). UNI is the default.

Step 5 Use **cnfport** to configure the trunk to use no HCF based shifting (BXM only).

Step 6 **cnfrsrc** can optionally be used to configure the number of conids and the bandwidth available on the trunk.

Step 7 Use **addtrk** to add the virtual trunk to the network topology.

Managing Virtual Trunk Numbers

A simple description of a virtual trunk is a "trunk defined over a public ATM service." The trunk does not exist as a physical line in the network. You must use an additional level of reference, called a **virtual trunk number**, to differentiate the virtual trunks found within a port.

For the BXM, you can define a maximum of **31** virtual trunks within one port. Valid virtual trunk numbers are 1-31 per port. The number of virtual trunks available is limited by the number of virtual interfaces available on the card. Each logical trunk (physical or virtual) consumes one virtual interface.

The same restrictions apply to the UXM. The maximum virtual trunks on the UXM is **15**.

The following user syntax describes a virtual trunk:

— UXM/BXM: slot.port.vtrunk

— slot = slot number (1-32)

port = port number (1-16)
vtrunk = virtual trunk number (1-31) (1-15 on UXM)

Virtual Trunk Commands

You use the current set of trunk commands to manage virtual trunks. These commands apply to a virtual trunk when you specify a virtual trunk number. Otherwise, the commands apply to a physical trunk. If you specify a physical trunk on a physical port that supports multiple virtual trunks, the command is applied to all virtual trunks on that physical port. **If you specify a virtual trunk for a command that configures information related to the physical port, then the physical port information is configured for all virtual trunks.**

The user interface for UXMs is different from BXMs in Release 9.2 because physical line information, including physical line statistics and alarms, is maintained separately from logical trunk statistics and alarms on UXMs. The BPX statistics organization has changed in Release 9.2 to separate logical and physical trunk statistics, so the BPX user interface *for statistics only* matches the UXM. This change affects the BXM and the BNI.

Virtual Trunk Commands Common to BXM and UXM Cards

The following commands are available on both the IGX and the BPX and have the same results. The entries marked with [*] are configured on a logical trunk basis, but automatically affect all trunks on the port when you change a physical option. For example, if the line framing is changed on a virtual trunk, all virtual trunks on the port are automatically updated to have the modified line framing.

The physical line commands for statistics exist on the IGX and as of Release 9.2, exist on the BPX. These are listed in italics below.

- **addtrk**—Adds a trunk to the network
- **clrtrkerrs**—Clears the trunk errors for a logical trunk
- **clrtrkstats**—Clears the summary trunk statistics for a logical trunk
- **clrphyslnerrs**—Clears trunk errors for a physical line (IGX only)
- **cnflnalm**—Configures the statistical alarm thresholds for trunks and ports (affects all trunks on node)
- **cnftrk**—Configures a logical trunk[*]
- **cnftrkparm**—Configures the trunk parameters of a logical trunk[*]
- **cnftrkstats**—Configures the interval statistics collection for a logical trunk
- **cnfphyslnstats**—Configures the interval statistics collection for a physical line
- **deltrk**—Deletes a trunk from the network
- **dntrk**—Downs a trunk
- **dsplogtrk**—Displays the logical trunk information
- **dspphyslnstatcnf**—Displays the statistics configuration for a physical line (IGX only)

- **dspphyslnstathist—**Displays the statistics collection result for a physical line (IGX only)
- **dsptrkcnf—**Displays the trunk configuration
- **dsptrkcons—**Displays the number of connections routed over a trunk
- **dsptrkerrs—**Displays the trunk errors for a logical trunk
- **dsptrks**—Displays the upped/added trunks
- **dsptrkstatcnf**—Displays the configured statistics collection for a trunk
- **dsptrkstathist**—Displays the statistics collection results for a trunk
- **dsptrkstats—**Displays the summary trunk statistics for a trunk
- **dsptrkutl—**Displays the utilization/traffic for a logical trunk
- **prtphyslnerrs—**Prints the trunk errors for a physical line (IGX only)
- **prttrkerrs—**Prints the trunk errors for a logical trunk
- **prttrks—**Prints the active logical trunks
- **uptrk**—Ups a trunk

UXM Commands

The following commands are IGX-specific, or behave differently than their BPX counterparts.

clrtrkalm—Clears the statistical alarms for a logical trunk **(affects logical trunk alarms only)**

clrphyslnalm—Clears statistical alarms for a physical line (IGX only)

dspphysln—Displays physical line statusclrtrkstats (IGX only)

cnftrkalm—Configures whether or not alarms on a trunk cause system alarms (IGX only)

BXM/BNI commands

The following commands are BPX specific.

- **clrtrkalm—**Clears the statistical alarms for a logical trunk[*] **(clears logical and physical trunk alarms)**
- **cnfrsrc—**Configure cell rate and number of conids (BXM only)

Virtual Trunk Configuration

Because a virtual trunk is defined within a trunk port, its physical characteristics are derived from the port. All the virtual trunks within a port have the same port attributes.

You configure all port and trunk attributes of a trunk with **cnftrk**, **cnftrkparm** or **cnfrsrc.** When a physical port attribute change is made, you are notified that all the trunks on the port are affected.

cnftrk command Parameters

Below are the trunk options you can configure with **cnftrk**. You can specify all physical options on virtual trunks. If you change a physical option on a virtual trunk, the change is propagated to all virtual trunks on the trunk port.

X in indicates the parameter is configurable.
X* in the virtual trunk columns indicates that the parameter is a physical parameter, and changing the value for one virtual trunk on the port automatically causes all virtual trunks on the port to be updated with the same value. See Table 4-24

Table 4-24 Trunk Options you can Configure with cnftrk Command

	BXM		UXM	
Descriptions	**Physical**	**Virtual**	**Physical**	**Virtual**
Transmit Trunk Rate	X	X	X	X
Receive Trunk Rate	X	X	X	X
Pass Sync	X	X*	X	X*
Loop Clock	X	X*	X	X*
Statistical Reserve	X	X	X	X
Header Type	X	X*	X	X*
Trunk VPI		X	X	X
Routing Cost	X	X	X	X
Virtual Trunk Type		X		X
Idle Code	X	X*	X	X*
Restrict PCC traffic	X	X	X	X
Link Type	X	X*	X	X*
Line Framing	X	X*	X	X*
Line Coding			X	X*
Line Cable type			X	X*
Line cable length	X	X*	X	X*
HCS Masking	X	X*	X	X*
Payload Scramble	X	X*	X	X*
Connection Channels	X	X	X	X
Gateway Channels			X	X
Valid Traffic classes	X	X	X	X
Frame Scramble	X	X*	X	X*
Deroute Delay Time	X	X	X	X
VC (Traffic) Shaping	X	X	X	X
Protocol by the Card	X		X	

Transmit Trunk Rate - This parameter indicates the trunk load for a BXM. You configure this value by using **cnfrsrc** on BXMs.

Virtual Trunk Type - The VPC type indicates the configuration of the VPC provided by the ATM cloud. Valid VPC types are CBR, VBR, and ABR.

Traffic classes—The traffic classes parameter indicates the types of traffic a trunk can support. By default, a trunk supports all traffic classes, that is, any type of traffic can be routed on any type of VPC. However, to prevent unpredictable results, a more appropriate configuration would be to configure traffic classes best supported by the VPC type:

VPC Type	Recommended Traffic Classes
CBR	All Traffic classes
VBR	ATM VBR, Bdata, Bdatb (Optimized Bandwidth Management), ABR
ABR	ATM ABR, Bdatb (Optimized Bandwidth Management)

High priority traffic can be routed over any of the VPC types.

Protocol by the Card— If set to "yes," specifies that LMI is running on the (BXM/UXM) card instead of processor card. If set to "no," LMI is running on the processor card.

VPC VPI—The VPI configured for a virtual trunk matches the VPI for the VPC in the cloud. Every cell transmitted to this trunk has this VPI value. Valid VPC VPIs depend on the port type.

Port Type	Valid VPI Range
BXM/UXM (UNI)	1-255
BXM/UXM (NNI)	1-4095
BNI T3/E3	1-255
BNI OC-3	1-63

Conid Capacity—The conid capacity indicates the number of connection channels on the trunk port that can be used by the virtual trunk. This number cannot be greater than the total number of connection channels on the card. The maximum number of channels is additionally limited by the number of VCI bits in the UNI cell header. For a virtual trunk, this number is divided by the maximum number of virtual trunks on the port to get the default. You configure this value by using **cnfrsrc** on BPXs.

Port Type	Max Conids
BXM/UXM	1-(#channels on card)
BNI T3/E3	1-1771
BNI OC-3	1-15867 (3837 max/VTRK)

Header Type—You can change the cell header from NNI (virtual trunk) to UNI (physical trunk). UNI is the default for virtual trunks, but it may be necessary to configure this parameter to NNI to match the header type of the VPC provided by the cloud. This is a new configurable parameter for physical and virtual trunks.

VC Traffic Shaping—You can change the traffic shaping over the trunk. Different algorithm run by firmware/hardware.

cnfrsrc command

Use the **cnfrsrc** command to configure resource partitions. The resources that you can currently configure are:

- number of conids
- trunk bandwidth

cnftrkparm command

BXM and UXM virtual trunks have all the configuration parameters for queues that physical trunks have. The integrated alarm thresholds for major alarms and the gateway efficiency factor is the same for all virtual trunks on the port.

Note BNI virtual trunks are supported by a single queue and do not support configuration of all the Advanced CoS Management queues on a single virtual trunk.

VPC Configuration within the ATM Cloud

For the virtual trunk to successfully move data through an ATM cloud, the cloud must provide some form of connectivity between the trunk endpoints. The ATM equipment in the cloud must support virtual path switching and move incoming cells based on the VPI in the cell header.

A virtual path connection (VPC) is configured in the cloud to join two endpoints. The VPC can support either CBR, VBR, or ABR traffic. A unique VP ID per VPC is used to moved data from one endpoint to the other. The BPX nodes at the edge of the cloud send in cells which match the VPC's VPI value. As a result the cells are switched from one end to the other of the ATM public cloud.

Within the ATM cloud one virtual trunk is equivalent to one VPC. Since the VPC is switched with just the VPI value, the 16 VCI bits (from the ATM cell format) of the ATM cell header are passed transparently through to the other end.

If the public ATM cloud consists of BPX nodes using BXM cards, the access points within the cloud are BXM or ASI ports. (Both BXM and ASI ports can be configured to not shift the VCI (that is, to set the cnfport command HCF Shift parameter to off). If the cloud consists of IGX nodes, the access points within the cloud are UXM ports.

If the link to the public cloud from the private network is using BNI cards, then access points within the cloud are ASI ports. The BNI card uses an STI header. The ASI port cards within the cloud are configured to not shift the VCI when forming the STI header. The command **cnfport** allows the user to configure no shifting on the port.

More Guidelines on VPC Configuration within the ATM Cloud

If you have a cloud with all Cisco equipment using all BPX-BXM cards, or any public ATM cloud that can fully pass 16 bits in the ATM cell header (thus uses a standard ATM cell header), then there is no need to set the Shift on/Shift off parameter with cnfport.

In a simple example of virtual trunking, say you have BXM and UXM virtual trunks feeding into a public ATM cloud. The cloud has equipment that uses a standard ATM cell header. If the cloud is using equipment that can cleanly pass a 16-bit ATM cell header (a standard ATM cell header), you would need to configure the **cnfport** parameter to *No Shift* on both ports at either end of the cloud. In other words, you must configure the port In this case, because the cloud uses standard NNI and UNI cell headers, the cell will pass transparently to the other end of the cloud without any problem.

Note You would configure the Shift parameter to *Shift off* in the case where you have an ASI or BXM port entering into the cloud. For best results, the Shift parameter should be set on both ends of the cloud, at the port's entry point to the cloud.

Because BNI cards were deployed before the ATM cell header became an ATM Forum standard, the BNI cards still use a non-standard ATM cell header. So if within a public cloud there is Cisco equipment with BNIs, these non-standard cell headers use 12-bit VCIs. To work with this situation, if BXM/UXM virtual trunks are being connected, the port can be configured for *Shift on*. If BNI virtual trunks are being connected, the ports should be *Shift off*. If the virtual trunk ports are configured this way, as the cells traverse the network through BNI cards, connection continuity can be preserved. Similarly, if BXM cards are used within a cloud, then the VCI bits are preserved when a VPC connection is routing through the cloud.

Note If a network outside of a public ATM cloud has Cisco equipment using BNIs, for a VPC connection to be routed over the BNIs, the **cnfport** Shift parameter must be configured to Shift off on all ports entering into the cloud. As long as the **cnfport** Shift parameter is set to Shift off on all ports connecting into the cloud, then all 16 bits of the VCI will be preserved, thus connection continuity can be preserved.

Consider the case where non-Cisco equipment is used within the public cloud, and a standard ATM cell header is supported. Also consider another example where the cloud has Cisco equipment with BXMs. Another case might be where the cloud has some Cisco equipment, and has some BNI cards in use. In this latter case (cloud has Cisco equipment, including BNIs), ports interfacing with this cloud must have the **cnfport** parameter set to *Shift on.* These examples are discussed in the following sections.

BXM and UXM Virtual Trunks Connecting through Cloud with non-Cisco Equipment (Standard Cell Header)

Consider an example where the cloud consists of all equipment that supports a standard ATM cell header (16-bit VCI). For example, there are three virtual trunks connecting through the cloud—from two BPX-BXM nodes and one IGX-UXM node. Consider that these virtual trunks are connecting to each other through a cloud with non-Cisco equipment. If the cloud has non-Cisco equipment, then Shift/No Shift cannot be configured.

Note Note that UXM cards cannot be configured for Shift off or Shift on. They always have Shift set to off.

BXM and UXM Virtual Trunks Connecting through Cloud with Cisco Equipment

Consider the example where the cloud consists of some Cisco MSSBU switches such as BPXs or IGXs. In the case where a virtual trunk is routing cells over only BXM routing trunks, all 16 bits of the ATM cell header can be passed cleanly because BXMs have the capability to handle a standard ATM cell header. However, if there are BNIs in the cloud network, some bits of the VCI could be lost. (For an explanation of why this occurs, refer to the "More Guidelines on VPC Configuration within the ATM Cloud" section on page 4-41.) There is no guarantee that connections can be made. If there are only BXM trunks in the cloud, then set the **cnfport** Shift parameter to *Shift off* on all BXM or ASI ports that connect to the cloud. However, if there are some BNIs within the cloud that connections may be routed over, then set the **cnfport** Shift parameter to *Shift on* for all ports that connect to the cloud.

Consider another example where you have a BXM routing trunk and a UXM routing trunk connecting through a public cloud. In this situation, all the trunk cards can support the standard ATM cell header, thus all 16 bits of the VCI can be passed through the cloud. In this case, each port interfacing to the cloud should have its **cnfport** parameter set to Shift off.

Virtual Trunk Port Interfaces

The two ends of a virtual trunk can have different types of port interfaces. For example, a virtual trunk can contain a T3 port at one end of the ATM cloud and an OC-3 port at the other end. However, both ends of the trunk must have the same trunk bandwidth, connection channels, cell format, and traffic classes. Switch software confirms this when a trunk is added.

Virtual Trunk Traffic Classes

All types of Cisco traffic are supported through an ATM cloud. Every trunk is defaulted to carry every type of traffic. The CBR, VBR, and ABR virtual trunks within the cloud should be configured to carry the correct type of traffic. The CBR trunk is suited to carry all types of traffic. The VBR trunk is best suited to carry IPX Frame Relay and BPX VBR traffic, as well as Optimized Bandwidth Management and ABR traffic. The ABR trunk is best suited to carry Optimized Bandwidth Management and ABR traffic. You can change the types of traffic each trunk carries. However, to avoid unpredictable results, it is best to stick to the recommended traffic types for a given VPC type.

Two-stage queueing at the egress of virtual trunks allows shaping of traffic before it enters the cloud. However, the traffic is still routed on a single VPC and may be affected by the traffic class of the VPC selected.

You can configure any number of virtual trunks between two ports up to the maximum number of virtual trunks per slot, and the maximum number of logical trunks per node. These trunks can be any of the three trunk types.

Virtual Trunk Cell Addressing

Cells transmitted to a virtual trunk use the standard UNI or NNI cell format. The examples below assume an NNI cell format.

The trunk card at the edge of the cloud ensures that cells destined for a cloud VPC have the correct VPI/VCI. The VPI is an 12-bit value ranging from 1–4095. The VCI is a 16-bit value ranging from 1–65535.

Virtual Trunking Feature must be Enabled by Cisco Technical Assistance Center

The virtual trunking feature is a chargeable feature, which means that it must be enabled on a per node basis with the **cnfswfunc** command by Cisco TAC personnel. Virtual trunking must be enabled on a node before you can up a virtual trunk on a port in the node.

Virtual Trunking Examples

Adding a Single Virtual Trunk Across an ATM Cloud Network

The following example describes a typical scenario of adding one virtual trunk across an ATM network. On one side of the cloud is a BPX with a BXM trunk card in slot 4. On the other side of the cloud is an IGX with a UXM trunk card in slot 10. The example shows a virtual trunk being added between port 3 on the BXM and port 2 of the UXM:

Note The VPC within the ATM cloud must be configured before adding the trunk.

Step 1	at BPX_A node	uptrk 4.3.1	Up virtual trunk #1 on BXM trunk port 4.3
Step 2	at BPX_A node	cnftrk 4.3.1	Configure VPI,VPC type, traffic classes, number of channels, and header type
Step 3	IGX_A	uptrk 10.2.1	Up virtual trunk #1 on UXM trunk port 10
Step 4	IGX_A	cnftrk 10.2.1	Configure VPI,VPC type, traffic classes, number of channels, and header type.

Step 5 BPX_A addtrk 4.3.1 Add the virtual trunk between the two nodes.

Executing the command
addtrk 10.2.1
at IGX_A would have the same effect. That is, you can add the virtual trunk at either endpoint.)

The VPI values you chose when using **cnftrk** must match those used by the cloud VPC. In addition, the following parameters must match on both ends of the virtual trunk:

- Transmit Rate
- VPC type
- Traffic classes supported
- Number of connection channels supported.

The **addtrk** command checks for matching values before allowing the trunk to be added to the network topology.

BXM/UXM Two Stage Queueing

The UXM and BXM share the same queueing architecture. The egress cells are queued in two stages. First they are queued per Virtual Interface (VI), each of which supports a virtual trunk. Within each VI, the traffic is queued as per its normal Advanced CoS Management traffic type. In other words, voice, Time-Stamped, Non-Time-stamped, High Priority, BDATA, BDATB, CBR, VBR, and ABR traffic is queued separately. The overall queue depth of the VI is the sum of all the queue depths for all the available queues. The user does not directly configure the VI.

Use the **cnftrkparm** command to configure the queues within the virtual trunk.

Virtual Trunks cannot be Configured as Feeder Trunks

A virtual trunk cannot be used as a feeder trunk. Feeder connections cannot be terminated on a virtual trunk. If you try to add a virtual trunk as a feeder trunk, or try to terminate a feeder connection on a virtual trunk, you will be prevented from doing so at the command line interface.

Networking

Virtual Trunk Configuration

The new characteristics of a virtual trunk used by connection routing are maintained throughout the network. This information—virtual trunk existence, traffic classes and connection channels—is sent to every node to allow the routing algorithm to use the trunk correctly. Routing only uses those virtual trunks that can support the traffic type of the connection.

VPC Failure Within the ATM Cloud

Any VPC failure within the ATM cloud generates a virtual trunk failure in the Cisco network. This trunk failure allows applications (for example, connection routing) to avoid the problem trunk. The current method of testing trunk integrity by using the Trunk Communication Failure test across a logical trunk can be used to detect a VPC failure. The method can be used for all physical and virtual trunks.

The CommFail test is augmented by using the ILMI protocol to monitor the VPIs of the virtual trunk within the cloud. The protocol is used to query the status of the VPC within the cloud.

Upon receiving notification of a VPC failure, the trunk is placed into the “Communication Failure” state and the appropriate trunk alarms are generated. The trunk returns to the “Clear” state after the VPC repairs and the trunk communication failure test passes.

User Interfaces

User Syntax

All trunk commands that allow a trunk description accept a virtual trunk number. You add physical trunks in the same way as in releases previous to 9.2. For virtual trunks, the virtual trunk number is added to the end of the trunk description.

UXM/BXM: slot.port--- slot.port.vtrunk

Event Logging

All trunk log events display the virtual trunk number. These messages were implemented on the BPX platform previous to Release 9.2, but are new on the IGX in Release 9.2. The following example shows the log messaging for activating and adding virtual trunk 1.2.1.

(IGX)

Class	Description
Info	NodeB at other end of TRK 1.2.1
Clear	TRK 1.2 OK
Major	TRK 1.2 Loss of Sig (RED)
Clear	TRK 1.2.1 Activated

(BPX)

Class	Description
Info	NodeB at other end of TRK 1.2.1
Clear	TRK 1.2.1 OK
Major	TRK 1.2.1 Loss of Sig (RED)
Clear	TRK 1.2.1 Activated

Error messages

In Release 9.2, there are new error messages to manage the virtual trunks, some of which are listed below:

- “Port does not support virtual trunking” - Port is not configured for virtual trunks
- “Port configured for virtual trunking” - Port is not configured for a physical trunk
- “Invalid virtual trunk number” - Virtual trunk number is invalid
- “Maximum trunks per node has been reached”- Trunk limit per node has been reached
- “Invalid virtual trunk VPI” - Virtual trunk VPI is invalid
- “Invalid virtual trunk traffic class” - Virtual trunk traffic class is invalid

- "Invalid virtual trunk VPC type" - Virtual trunk VPC type is invalid
- "Invalid virtual trunk conid capacity" - Virtual trunk conid capacity is invalid
- "Mismatched virtual trunk configuration" - Ends of virtual trunk have different configuration
- "Maximum trunks for card has been reached" - The trunk card is out of VIs

Cisco WAN Manager

In Release 9.1, the Cisco WAN Manager user interface displays virtual trunks on IGXs. The trunk description passed to Cisco WAN Manager contains the new virtual trunk number. The topology display on Cisco WAN Manager shows the <slot>.<port>.<vtrunk>. Both the topology and robust messages used to maintain network status and displays are modified. This is new for IGX nodes only in this release.

Virtual trunk parameters can be configured or queried through an SNMP manager. This capability already exists on the BPX, but is new to the IGX in Release 9.2.

Virtual trunk information is passed to Cisco WAN Manager using the existing mechanism for physical trunks—no virtual trunk number is sent.

The interface to Cisco WAN Manager has an improved scheme for multiplexed virtual trunks. The messages that communicate trunk and physical line information to Cisco WAN Manager include a *primary physical line number*, which is used to "glue" the physical lines and the logical trunks. For example, suppose the trunks 5.2-4.9 and 5.2.11 are upped on a UXM/IMA card set. Switch software internally assigns each physical line (5.2, 5.3 and 5.4) a unique physical line number. In this example, assume our physical lines are numbered 8, 9, and 10, respectively. The primary physical line number is the unique identifier for the first physical line of the aggregated trunk port—in this case 8. The Physical line messages for 5.2, 5.3, and 5.4 include the primary physical line 8. The messages for 5.2.9 and 5.2.11 also include the primary physical line 8. Cisco WAN Manager uses this identifier to associate physical lines to an aggregate multiplexed pipe (trunk port), and to associate trunks with a trunk port.

The Compliant IMA (Inverse Multiplexing over ATM) feature requires a bitmap of physical lines to be added to the messages. The bitmap is required because the physical lines forming the trunk port may be non-consecutive. Previously, the first port and the number of physical lines were included. Note that the information provided by the physical line bitmap and the primary physical line number is in some ways redundant. The bitmap enhances the primary physical line scheme by giving instant information about all physical lines associated with a logical trunk.

Trunk Redundancy

Trunk redundancy can refer to one of two features:

- SONET Automatic Protection Switching (APS)
- Y-redundancy

APS Redundancy

APS line redundancy is supported. APS line redundancy is only supported on BXM SONET trunks and is compatible with virtual trunks. The trunk port supporting virtual trunks may have APS line redundancy configured in the same way it would be configured for a physical trunk. The commands **addapsln, delapsln, switchaplsln,** and **cnfapsln** are all supported on virtual trunk ports. These commands accept a trunk port parameter as <slot>.<port>. Refer to the "APS 1:1 (Line Redundancy)" section on page 4-60 for more information on SONET Automatic Protection Switching support.

Note that you cannot configure virtual trunks as interface shelf (feeder) trunks; similarly, you cannot configure interface shelf (feeder) trunks as virtual trunks.

Reconfiguring a Trunk

This section describes how to change trunk parameters after you have added the trunk. After you have added a trunk, you can reconfigure some parameters without first deleting the trunk (with **deltrk**). This means that you can reconfigure the following list of trunk and line parameters when the port is in use (active). The **cnftrk** display highlights all configurable parameters, and dims parameters that are not configurable. The parameters that you can change *without* first deleting the trunk are:

- Restrict Control Card traffic (“PCC restrict”)
- Pass sync
- Loop clock
- Statistical reserve
- Bursty data peak speed
- Bursty data peak average frame
- Idle Code (reconfigurable for trunk and line)
- User traffic
- Maximum PVC Channels
- Trunk Partitions SVC/PVC
- DS0 Map (IGX only, as of Release 9.2)
- Cable type/length
- Virtual trunk type
- Link type
- HCS Masking
- Payload Scrambling
- Frame Scrambling
- Gateway Channels
- Retained Links
- IMA link auto disabled
- IMA window size
- IMA max transition counts
- IMA link reenable time
- Traffic classes
- Recv Impedance
- Gateway Efficiency
- Cost of Trunk
- Deroute Delay Time
- Line T1 signalling (Line reconfiguration allowed)
- Line caching (Line reconfiguration allowed)
- Line CAS Switching (Line)

- Line Cnf slot.line (Line)
- Line Cnfg (Line)
- Line pct fast modem (Line)
- Trunk Receive Rate—On IGX, configurable after a trunk has been added.
- Trunk Transmit Rate—On BPX platforms, configurable after a trunk has been added.

Before making changes to any other trunk parameters, you must first delete the trunk (**deltrk**).

To display the current trunk parameters, use **dsptrkcnf**. If you can make all the needed parameter changes without deleting the trunk, execute **cnftrk**. Use **cnftrk** at both ends of the trunk.

To change parameters that require you to first delete the trunk, do the following:

Step 1 Delete the trunk by executing **deltrk** at one end of the trunk.

Step 2 Execute **cnftrk** at both ends of the trunk to reconfigure parameters.

Step 3 Execute **addtrk** at only one end of the trunk to add the trunk.

Switch software triggers a reroute of connections only if a change to a parameter results in too few resources to support the current load of connections.

If you attempt to change one of these parameters, the other endpoint will be updated by switch software. It is not necessary to change both endpoints' parameters.

Before Release 9.2, changes made to the following three parameters caused a reroute on the trunk. For example, any increase to Statistical reserve would cause a reroute of all connections on the trunk. In this release, any changes you make to the following parameters will cause reroutes to PVCs on the trunk only if resources are no longer available to support the current connection load:

- Statistical reserve
- Trunk Partitions SVC/PVC
- Maximum PVC Channels

Note Note that MPLS (Tag switching) partitions will not be affected by trunk/line reconfiguration, as tag switching partitions cannot be increased beyond the available number of resources.

For a trunk between a node running Release 9.2 and node running an earlier release (such as 9.1 or 8.5), you will be prompted that you can change a parameter only if both ends allow such a change.

Removing a Trunk

To remove a trunk:

Step 1 Use the **deltrk** command to delete the trunk. If both nodes are reachable, perform this command at one end of the trunk only. Otherwise, you must perform this command at both ends. **Q**Connections using the deleted trunk that cannot be rerouted are automatically deleted.

Step 2 Use the **dntrk** command to down the trunk. Execute **dntrk** at both ends of the trunk.

Displaying or Printing Trunk Configurations

You can display the network trunk configuration on the screen or print it on the printer in a one-step process by using any one of the following commands.

- **dsptrks—**Displays the current trunk configuration and alarm status at a node.
- **prttrks—**Prints the current trunk configuration and alarm status at a node.
- **dspnw**—Displays all trunks for each node in a domain.
- **prtnw**—Prints all trunks for each node in a domain.

Setting Up ATM Trunk and Line Redundancy

Trunk redundancy can refer to one of two features:

- the original ATM trunk redundancy feature supported on the IPX/IGX platform previous to Release 9.2
- *APS line redundancy*, supported in Release 9.2

APS line redundancy is only available on BXM SONET trunks and is compatible with virtual trunks. In other words, you can configure APS line redundancy on a trunk port that supports virtual trunks in the same way you configure a physical trunk. The commands **addapsln, delapsln, switchapsln,** and **cnfaplsln** are all supported on virtual trunk ports. (These APS line redundancy commands are described in this chapter.)

The original ATM trunk redundancy feature is an IPX/IGX feature only and is not supported for virtual trunks. The **addtrkred, deltrkred,** and **dsptrkred** will be rejected for virtual trunks.

ATM trunk redundancy is the T3 and E3 trunk redundancy supported by the AIT, ALM/B, and BTM cards. Redundancy can exist between either an AIT card and BNI (BPX) card, an ALM/B and BNI card, or a BTM and a BNI card. Trunk redundancy cannot exist between IPX and IGX nodes. Also, virtual trunking and trunk redundancy are incompatible. Trunk redundancy uses the standard trunk cables rather than a Y-cable. (For all service card sets other than trunk cards, you manage redundancy by using the Y-cable redundancy commands **addyred**, **delyred**, **prtyred**, and **dspyred**).

Trunk redundancy depends on the applicable commands, the trunk card in the adjacent slot, and the standard trunk cable. You can execute trunk redundancy commands only on the IGX node. The BPX node does not require information regarding this feature. Use the following commands to manage the original trunk redundancy feature (which was supported in previous releases and is still supported in this release) on IGX platforms:

- **addtrkred—**Sets up redundancy for a pair of AIT, BTM, or ALM/B cards.
- **deltrkred**—Deletes redundancy for a current redundant pair.
- **dsptrkred**—Displays all redundant ATM trunk pairs.

Trunk Redundancy

Trunk redundancy can refer to one of two features: *APS line redundancy* or the original ATM trunk redundancy feature supported in releases previous to Release 9.2 on the IGX/IPX platforms. APS line redundancy is only available on BXM SONET trunks and is compatible with virtual trunks. In other words, you can configure the trunk port supporting virtual trunks with APS line redundancy the same way you would configure a physical trunk. There are new APS line redundancy commands—**addapsln**, **delapsln**, **switchapsln**, and **cnfapsln—**which you can use on virtual trunk ports. The syntax for these commands is unchanged from Release 9.1: that is, they accept a trunk port parameter as *slot.port*. Refer to the "Overview of SONET Automatic Protection Switching (APS)" section on page 4-51, and to the **addapsln**, **delapsln**, **cnfapsln**, and **cnfcdaps** commands in this chapter for information on how to configure the APS line redundancy feature.

The original trunk redundancy feature is an IGX only feature and is not supported for virtual trunks. The commands **addtrkred**, **deltrkred**, and **dsptrkred** are rejected for virtual trunks.

Overview of SONET Automatic Protection Switching (APS)

This section provides a description of the SONET Automatic Protection System (APS) feature, which provides card and line redundancy for BXM OC-3 and OC-12 cards. SONET APS is a standard that describes the switching of SONET lines from the active line to a standby line to provide hardware line redundancy. The SONET APS feature provides a standards-based solution to line redundancy. In moving away from Y-cable redundancy (Y redundancy), the line can be eliminated as a single point of failure. Refer to Table 4-44 for descriptions of APS 1+1 (card and line redundancy), APS 1:1 (line redundancy), and APS 1+1 Annex B card and line redundancy protocols.

This section contains information on the following:

- Overview of Automatic Protection Switching (APS)
- APS Command Summary
- Introduction
- Operation Criteria
- APS 1+1 (Card and Line Redundancy)
- APS 1:1 (Line Redundancy)
- APS 1+1 Annex B (Card and Line Redundancy)—GR783
- Test Loops
- Notes on APS Messages
- APS Alarms
- APS K1 Command Precedence
- Troubleshooting Notes

Refer to the descriptions of the following commands for more information about configuring SONET Automatic Protection Switching:

- **addapsln**
- **delapsln**
- **cnfapsln**
- **cnfcdaps**
- **dspapsln**
- **dsplog**
- **dspalms**
- **switchapsln**

Note The **addapsln** and **delapsln** command line displays are similar; the **dsplog** and **dspalms** command line displays are identical.

Introduction to SONET APS for BXM Cards

Automatic Protection Switching provides a standards based line-redundancy for BXM OC-3 and OC-12 cards. With Release 9.2, the BXM OC-3 and BXM OC-12 cards support the SONET APS 1+1 for card and line redundancy and APS 1:1 standards for line redundancy which is provided by switching from the working line to the protection line. The working line is normally the active line, and the protection line is normally the standby line.

The APS 1+1 and APS 1:1 protocols that are supported by the BXM are listed in Table 4-25 and shown in Figure 4-6. APS 1+1 Annex B has the same general layout as shown in Figure 4-6, except that the active line is called the primary, and the standby line is referred to as the secondary line.

Table 4-25 BXM SONET APS

APS 1+1	The APS 1+1 redundancy provides card and line redundancy, using the same numbered ports on adjacent BXM back cards.
APS 1:1	The APS 1:1 redundancy provides line redundancy, using adjacent lines on the same BXM back card.
APS 1+1 Annex B	The APS 1+1 Annex B redundancy provides 1+1 card and line redundancy, which can be configured only for bi-directional and non-revertive protection switching. For Annex B, the active line is called the "primary section", and the standby line is termed the "secondary section". Manual switching (switchapsln) is not allowed in APS 1+1 Annex B implementation. It is recommended that you not use the Manual switch option (**switchapsln** option) in an Annex B configuration when the BPX is connected to a switch from another vendor.

Figure 4-6 APS 1+1 Redundancy

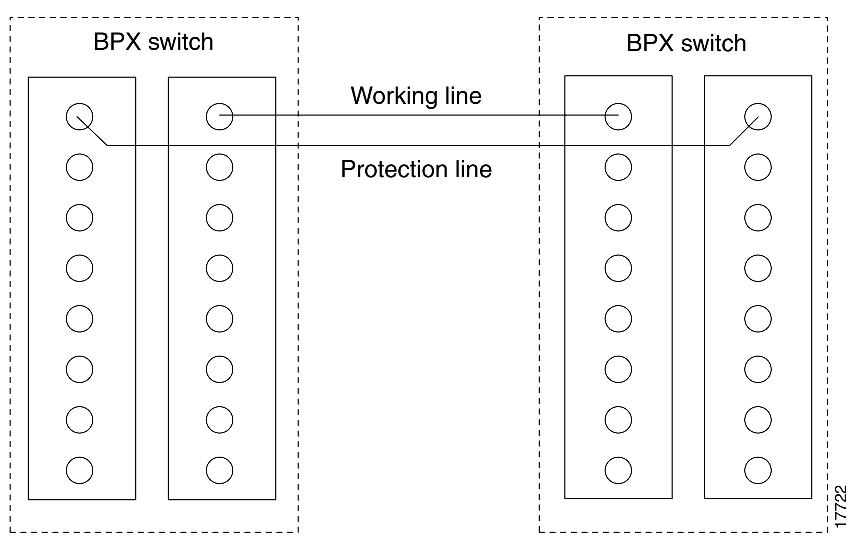
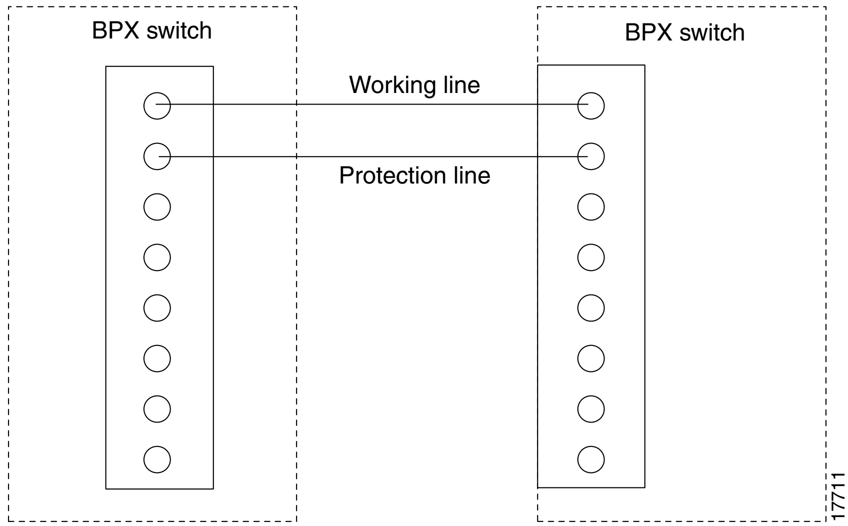


Figure 4-7 APS 1:1 Redundancy



Automatic Operation

SONET Automatic Protection Switching lets you configure a pair of SONET lines for line redundancy so that the interface hardware automatically switches from a working line to the protection line within a specified period after an active line failure.

Note For Annex B, the Working line is referred to as "Work1" (or "Working section 1"), and the Protection line is referred to "Work2" (or "Working section 2").

Upon detection of a signal fail condition (that is, LOS, LOF, Line AIS, or Bit Error Rate in excess of a configured limit) or a signal degradation condition (that is, BER exceeding a configured limit), the hardware switches from the working line to the protection line. This case assumes that the working line was the active line and the protection line was not in alarm.

If the "Revertive" option is enabled, (by using the **cnfapsln** command), the hardware switches back to the working line from the protection line after a configured time period called "Wait to Restore" (**cnfapsln** command) has elapsed. The working line must be in a clear state for this to occur. The "Revertive" option is the default for APS 1:1, but not for APS 1+1.

Coordination between the interfaces on the two ends of the lines is provided through an in-band protocol.

Manual Operation

You can use the **switchapsln** command to control switching manually. The last user switch request per line pair is saved by switch software so that you can configure APS correctly in the event of a node rebuild.

Operation Criteria

APS cards provide both front and back card LED displays providing line and card status active and standby status.

APS Front Card Displays

The front card LED functions are listed in Table 4-26.

Table 4-26 BXM Front Card LED Display

LED	Description
Card LED, Green	Active
Card LED, Yellow	Inactive
Port LED, Green	Line is active
Port LED, Yellow	Line is standby

APS 1+1 LED Displays

The back cards used for APS 1+1 with front card redundancy have an LED which indicates whether the back card can be pulled out for service replacement.

For example, all the lines on the card except one may be working properly and therefore the card needs to be replaced. The back card LED functions are listed in Table 4-27.

Note In the APS 1+1 configuration, when the primary card is active and the protection line is active, LEDs on both back cards are green. The LED of the secondary is green because that back card is carrying traffic. The LED of the primary back card is green, because that is in the physical path of the front card in receiving traffic from the protection line. When the back card LED is green do not pull out the back card, because it will disrupt traffic. When the LED is yellow it is OK to pull out the back card, but it should be put back as soon as possible, because the card will needed in the event of a switchover.

Table 4-27 BXM Back Card for APS 1+1 LED Display

LED	Description
Green	The card has at least one active line and may not be removed without affecting service.
Yellow	The card has no active lines and my be removed.
Red	Not used and not applicable.

APS 1+1 (Card and Line Redundancy)

The APS 1+1 feature requires two BXM front cards, an APS redundant frame assembly, and two redundant type BXM back cards. The two redundant BXM back cards are plugged into the APS redundant frame assembly (refer to the APS Configuration chapter in the *BPX 8600 Series Installation and Configuration* guide. The types of available back cards are:

The types of redundant back card and backplane sets required are:

- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622 (single port, long reach, SMF, FC connector)
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- BPX-RDNT-SM-622-2 (2 port, medium reach, SMF, FC connector)

  Each of the listed model numbers includes two single back cards and one mini-backplane (providing cross coupling of two back cards).

The single back cards and mini-backplane can be ordered as spares. Their model numbers are:

- BPX-RDNT-BP= (common backplane for all redundant APS back cards)
- BPX-LR-155-8R-BC= (for BPX-RDNT-LR-155-8)
- BPX-LR-622-R-BC= (for BPX-RDNT-LR-622
- BPX-SMF-155-4R-BC= (for BPX-RDNT-SM-155-4)
- BPX-SMF-155-8R-BC= (for BPX-RDNT-SM-155-8)
- BPX-SMF-622-R-BC= (for BPX-RDNT-SM-622)
- BPX-SMF-622-2R-BC= (for BPX-RDNT-SM-622-2)

APS 1+1 (Card and Line Redundancy)

The APS 1+1 feature requires two BXM front cards, an APS daughter backplane, and two redundant type BXM back cards (**dspcd** command). The two redundant BXM back cards must be plugged into the APS daughter backplane.

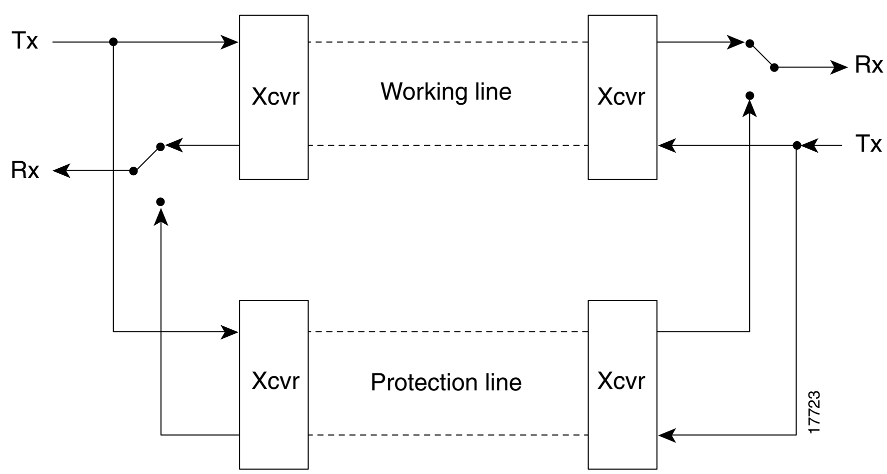
Traffic protected by APS 1+1 redundancy is carried on the working line and the protection line simultaneously (see Figure 4-8). Bridging is implemented such that the same payloads are transmitted identically over the working line as the protection line.

Note For Annex B, the Working line is referred to as "Working section 1," and the Protection line is referred to as "Working section 1." On the **dspapsln** screen, for Annex B, they are shown as "Work1" and "Work2" (under the Work/Prot column designations for Annex A).

The receiver terminating the APS 1+1 has to select cells from either the working or protection line and be able to forward one consistent traffic stream. Because both working and protection line transport identical information, the receiving ends can switch from one to the other without needing to coordinate with the transmit end.

Note APS 1+1 is not supported on one card.

Figure 4-8 SONET APS 1+1 Detail



To set up APS, use the **addapsln** command.

- The **addapsln** command defines which line is working and which is protection.
- Before you can execute the **addapsln** command for a line pair, the protection line must be in standby state.
- If the **addapsln** command is executed, the working line is always initially selected.

When no port on a BXM is configured for APS, each back card of the pair can be used independently by independent front cards. The switch software disallows configuration of APS is independent usage is detected. There must be no active lines on the card that is selected to be the secondary card.

With previous card cages, because of the positioning of mechanical stiffeners, you can only insert the APS card pairs in certain slots. These are slots 2 through 5 and 10 through 13. The mechanical stiffeners are located at slots 1 and 2, 5 and 6, 9 and 10, and 13 and 14. An APS 1+1 card pair must reside in adjacent slots (2,3 or 4,5, and so on.)

With current cordages, the previously-mentioned limitation is removed, and the BXM cards configured for APS 1+1 can be located anywhere, except BCC cards slots 7 and 8, and ASM card slot 15.

An APS 1+1 redundant card pair must be in adjacent slots (2,3 or 4,5 and so on.).

Redundancy Criteria for APS 1+1

You implement the APS 1+1 redundancy by first setting up Y-redundancy, then adding APS.

When you implement card redundancy, the two BXM front cards must reside in the same two adjacent slots as the APS back cards, which you need to insert into the APS two- slot daughter board.

Front and back cards must always match (port type, port count, number of channels support) and be in adjacent slots for APS to be enabled and function. That is, there should be no "mismatch" condition when **addcdred** is executed. Also, when the **addapsln** command is executed, cards will be checked to verify that they are adjacent.

You must connect the working lines on the back card to the same slot as the primary front card, and connect the protection lines to the same slot as the secondary front card.

The switching of the front cards is controlled by switch software under the Y-redundancy protocol. The switch software performs switching between the two cards in the event of a front card failure, front card downed, front card failing self-test, and so on.

You can add APS at any time after Y-redundancy is configured, as long as the protection line is in the standby state. You can add APS even if lines and trunks are upped and the card is passing traffic.

Note Typically, when APS and card redundancy are implemented together, the term YRED really means card redundancy, as in this case there is no Y-cabling involved. An exception exists when the BXM is attached to an MGX8220 (interface shelf, also called "feeder") or other device that does not support APS. In that case, you can use Y-cables or straight cables with APS.

When APS is configured on a card pair, capability checking is performed to ensure that both cards match and support APS.

For APS 1+1 redundancy, the same numbered ports on adjacent BXM back cards are used. The maximum number of connections supported does not change, as the complete connection capability of the cards is available.

Note Using only one front card and two back cards is not a valid configuration when adding APS capability, and the APS alarm capability is reduced when the standby card is not available.

Application Notes for APS 1+1

Using switchcdred/switchyred command

Note Entering **switchcdred** or **switchyred** executes the same command. The newer name is **switchcdred** which replaces **switchyred**, but you can still use **switchyred** for those familiar with that command.

You can use the **switchcdred (**switchyred**)** command to switch between an active and standby front card in an APS 1+1 configuration. For example, you might want to do this to test the standby front card.

Following a **switchcdred (**switchyred**)**, or active card reset, the BXM card is sent a message from switch software to have it perform an APS switch to align itself with the last user **switchapsln** switch request. If the last user request is "clear", full automatic APS switching is in effect with the working line in the active state by default. When there is no last user switch request to switch any particular line **(that is, protection line)**, the working line becomes active.

Note In the APS 1+1 configuration, if the protection line is active and the last user request is "clear", a **switchcdred** will cause the working line to be active if there is no line condition on the working line. When APS 1+1 comes up, it will come up on the working line if the working line is clear. When a **switchcdred** is issued, the active card also comes up on the working line if the working line is clear and there is no user request. **In the case** where the working line is in alarm or there is a user request to switch to the protection line (**switchapsln**), the card will first come up on the working line. Then the card will detect the alarm or the user request and switch to the protection line.

Other Notes related to APS 1+1 Configurations

Note In the APS 1+1 configuration, if the last user request was a W->P switch, then **dsplog** will log a W->P switching event when a **switchcdred** is issued. On a **switchcdred**, the newly active card comes up on the working line first. Then it responds to a user request to switch from the **working** to protection line by switching to the protection line and sending an event notification to that effect. **You can view the event notification s in the event log by using the dsplog command.**

Note It may be necessary to perform a **switchcdred (switchyred)** command after performing a service switch with the **switchapsln** command so that the back card that the service switch selects has its associated front card active.

Some **switchapsln** Notes

With APS 1+1, when repetitive **switchapsln** commands are issued, up to two in a row can be executed sequentially, when alternating between options 3 and 4 (forced switch), or 5 and 6 (manual switch), but no more. Attempts to execute a third **switchapsnln** will not succeed, and the following error message is displayed:

```
"Cannot request manual W->P when manual P->W switch in progress"
```

If users want to perform repetitive switchapsln commands, they need to issue a clear switch between each W-P, P-W pair of commands, for example:

```
switchapsln 2.1 1
```

Configuration Procedure, APS 1+1

The following is an example of configuring APS 1+1 redundancy:

Note You should use slots 2 and 3 because slots and 1 and 2 cannot be used due to mechanical dividers.

Step 1 Verify that the appropriate front and back cards are installed along with the APS two-card daughterboard.

Step 2 Ensure that lines are connected, for example, on port 1 of BXM card in slot 2 and port 1 of BXM card in slot 3.

Step 3 Execute the following commands and verify chan half=no, and standard=GR-253 (default).

cnfcdaps 2.1 N 1

cnfcdaps 3.1 N 1

Step 4 Execute the following command; for example, for a redundant line on port 1 for BXM OC-3 cards and APS back cards in slots 2 and 3 of the BPX:

addcdred 2 3

Step 5 **addapsln 2.1 3.1 1** { addapsln<slot.port> <slot.port> <1|2|3|..>

Note The last entry, “1”, in the **addapsln** command specifies the type of APS, in this example, APS 1+1.

Step 6 **cnfapsln 1.1**

Step 7 **upln** 2.1 {or uptrk, as applicable

Note Lines 1.1 and 2.1 are considered the same line and are referred to as line 1.1 in this case. There is no need to configure line 2.1 as an APS line (by using **cnfapsln 2.1.)** The **cnfapsln 1.1** command performs this step of the procedure.

Also, the CLI does not allow you to configure the protection line (in this case, line 2.1).

APS 1:1 (Line Redundancy)

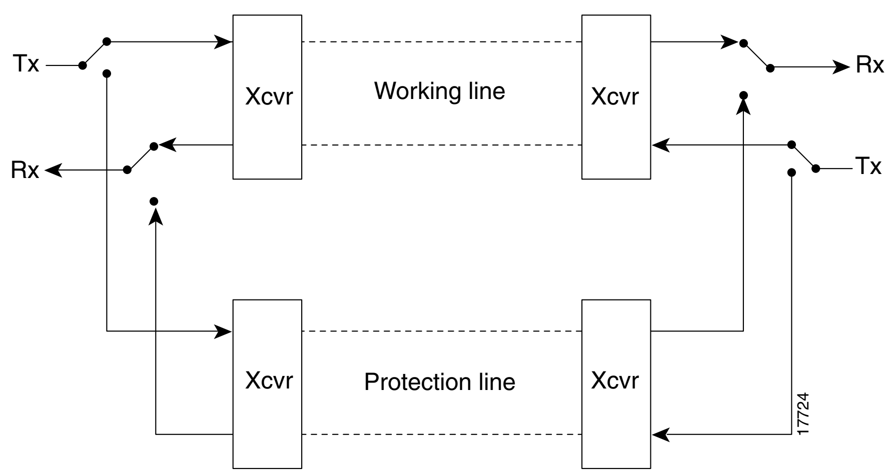
The APS 1:1 feature provides port and line redundancy for a single BXM front card and associated OC-3 or OC-12 back card.

There is no new hardware required to support APS 1:1. A single front card with a standard back card is used.

Two adjacent lines on the same card are used. The maximum number of connections supported by a non-enhanced BXM is reduced by half for APS 1:1 operation. Using enhanced BXM cards, the number of available connections is not decreased. See Figure 4-9 for an illustration of SONET APS 1:1.

Similarly to APS 1+1, SONET Linear APS 1:1 requires that for every working line, there must exist a redundant protection line. However, unlike the 1+1 case, traffic protected by the redundancy must be carried on the protection line **only** when a failure occurs on the working line. In the case of no failure, the protection line can transport idle traffic, 'same' traffic as working line, or extra traffic. Because the protection line is not guaranteed to carry real traffic until the transmit end is informed of the failure and switch, this requires coordination between the equipment at both ends, thus is more complicated.

Figure 4-9 SONET APS 1:1 Detail



Note APS 1:1 operating in APS 1+1 is not supported in Release 9.1, if the far end LTE (Line Terminating Equipment) indicates that it is 1+1 LTE.

Note APS 1+1 on one card is not supported in Release 9.2. Refer to the Cisco WAN Switching software release notes for Release 9.2 for up-to-date feature support.

To set up APS, use the **addapsln** command. (See the **addapsln** command in this chapter.)

- You can only add APS 1:1 to lines in standby state (lines that are not upped).
- Before using the **addapsln** command, the switch software will not attempt to use or monitor the protection line; only the working line is used.

- If the **addsapsln** command is used with a working line in place, the working line is always initially selected.

General Criteria

APS 1:1 cannot be configured on cards already configured for YREd. They cannot be configured concurrently. Use APS 1+1 instead.

APS 1:1 configuration requires that the user add the APS configuration to a line before upping the line.

APS 1:1 configuration requires that the user down a line before deleting the APS configuration on the line.

APS 1:1 can only be configured for bi-directional operation and revertive switching.

Configuration Criteria

The redundant lines must be adjacent. In addition, the lines that you can pair are:

— 1 and 2

— 3 and 4

— 5 and 6

— 7 and 8

Either of the two lines can be designated as working line and the other as the protection line.

The switching of the working and protection lines is controlled by the BXM hardware and firmware APS protocol.

The BXM hardware and firmware performs switching between the protection and working lines in the event of a line or port failure.

You can add APS at any time as long as the working line and protection line are in the standby state. You can only up lines and trunks after you have first added APS 1:1.

Configuration Procedure, APS 1:1

The following is an example of configuring APS 1:1 redundancy:

Note Before configuring for APS 1:1 redundancy, all card connections must be deleted using the **delcon** command.

Step 1 Ensure that lines are connected, for example, on ports 1 and 2 of a BXM in slot 3.

Note The last entry, “2”, in the **addapsln** command specifies the type of APS, in this example, APS 1:1.

Step 2 Execute **cnfcdaps** and verify chan half=yes (not default), and standard=GR-253 (default).

cnfcdaps 3.1 Y 1

Step 3 **addapsln** 3.1 3.2 2 {addapsln<slot.port> <slot.port> <1|2|3|4|5>

Step 4 **upln** 3.1 {or uptrk, as applicable

Note The CLI does not allow you to configure the protection line (in this case, line 3.2).

APS 1+1 Annex B (Card and Line Redundancy)

The APS 1+1 Annex B Card and Line Redundancy feature is similar to the APS 1+1 feature, with the main difference being that APS 1+1 Annex B redundancy can only be configured for bi-directional operation and non-revertive switching on a line.

General Criteria

APS 1+1 Annex B can only be configured for bi-directional operation and non-revertive switching on a line.

Note In non-revertive switching, to avoid data loss, a line is not automatically switched back to active after a failure is corrected.

Configuration Procedure, APS 1+1 Annex B

Following is an example of configuring APS 1+1 redundancy:

Step 1 Verify that the appropriate front and back cards are installed along with the APS two-card daughterboard.

Step 2 Ensure that lines are connected, for example, port 1 on BXM in slot 1 and port 1 on BXM in slot 2.

Step 3 Execute the following commands and verify chan half=no, and standard=GR-253 (default).

cnfcdaps 1.1 N 1

cnfcdaps 2.1 N 1

Step 4 Execute the following command, for example, for redundant line on port 1 for BXM OC-3 cards and APS back cards in slots 2 and 2 of the BPX:

addcdred 1 2

Step 5 **addapsln** 1.1 2.1 3 { addapsln<slot.port> <slot.port> <1|2|3|..>

Note The last entry, "(3)", in the **addapsln** command specifies the type of APS, in this example, APS 1+1, Annex B.

Step 6 **cnfapsln** 1.1

Step 7 **upln** 1.1 {or uptrk, as applicable

Test Loops

The test commands **addlnloclp** and **addlnrmtlp** are service-affecting even when APS is configured. In all APS configurations, if the working line is looped, both lines will be looped and traffic will be disrupted.

Notes on APS Messages

When adding an APS 1+1 line or trunk using **addapsln**, if the working slot's paired redundant slot is not a legal protection slot, or if firmware cannot determine what the paired slot is, an invalid slot pairing exists and one of the following two messages will be displayed:

"Protection card specified by user does not match HW."

"Working card specified by user does not match HW."

You can display the redundant card information with the **dspcd** command under the "Backyard Installed" heading. For example, if a redundant pair is configured with a primary slot of 2 and a secondary slot of 3, the **dspcd** 2 command should display "RedSlot: 3", and the **dspcd** 3 command should display "RedSlot: 2". The following example is of **dspcd** 2:

```
swwye     TN       silves        BPX8620      9.2.20       Aug. 9 1999

Detailed Card Display for BXM-155 in slot 2

Status:          Active
Revision:        DDA                  Backcard Installed
Serial Number    652774                 Type:          LM-BXM
Fab Number       28-2158-02             Revision       EW
Queue Size       228300                 Serial Number 1..1...
Support: 4 Pts, OC-3, FST, VcShp        Supp: 4 Pts, OC-3, SMF, RedSlot:3
Support: VT, ChStLv 2, VSIlvl 2
Support: APS (FW, HW1+1)
Support: OAMLp, TrfcGen
#Ch: 8128, PG[1] :8123
#Sched_Ch:16284

Last Command: dspcd 2
```

APS Alarms

The APS alarms are listed in Table 4-28. The listing includes the class or state of the alarm: *minor, major, info,* or *clear*. (Classes of "Info" type are APS events—events do not display when you use the **dspapsln** command, but they do display when you use the **dsplog** command.) Use the **cnfcdaps** and **cnfapsln** commands to modify the APS parameters. To change from APS 1+1 to APS 1:1 and vice-versa, use the **delapsln** and **addapsln** commands.

Note APS events are internal to the switch software and are not displayed when you use the **dspapsln** command; however, you can view APS events by using the **dsplog** command. APS events are listed with a class type of "Info" in Table 4-28.

Note For Annex B, the Working and Protection lines are referred to as “Working section 1” and “Working section 2”. To read alarms, **dsplog** information and other information related to Annex B configuration, refer to the “Work1” and “Work2” columns shown on the **dspapsln** screens.

Statistical Alarms

Statistical alarms are not cleared when a YRED switch occurs. You can clear these statistics as appropriate.

Separate line statistics are not kept for the redundant line, and no counter statistics are kept for APS alarms.

Note On the active line/trunk, alarms (for example, LOS and LOF) and statistics (for example, error counters) are supported. On the standby line/trunk, alarms are supported but not statistics.

Summary statistics are not supported on a standby line/trunk.

APS Alarms and Logs

Switch software provides a new set of APS alarms and events from the working APS line. Both the APS working and protection line alarms are propagated from the BXM firmware to software through the working line’s CommBus interface for the one card solution, and to the active card for the two-card solution (may not be the same slot number as the working line).

Software issues “Info” events whenever an APS line pair is added, deleted, switched or reconfigured by the user. The APS alarms and events are listed and described in Table 4-28.

The APS alarms are sent to the Cisco WAN Manager in the APS robust alarm message.

APS alarms are displayed when you execute the **dsplog** command.

Table 4-28 APS Alarms

Class	Name	Description
Minor	APS Standard Mismatch	In a 2 card APS 1+1 configuration, one card is programmed for GR-253 and the other card is programmed for ITUT.
Minor	APS Card Missing	Indicates that either a BXM front card or back card supporting this APS line is detected as missing by a BXM.
Clear	APS OK	APS line is up with no alarms.
Clear	APS Deactivated	APS line is down.
Minor	APS Lines looped	APS line is looped.
Minor	APS Remote Signal Failure	A remote signal failure indicates that there is a problem with the far end signalling information in the K1K2 bytes.
Minor	APS Channel Mismatch	Can only happen in bidirectional mode and indicates that there is a problem with the underlying APS channel protocol. The receive K2 channel number does not equal the transmit K1 channel number.

Table 4-28 APS Alarms (Continued)

Class	Name	Description
Minor	APS Protection Switch Byte Failure	Protection Switch Byte failure or PSB. In bidirectional mode indicates that there is an invalid K1 byte. The receive K1 request does not match the reverse request and is less than the transmit K1 request. In all modes a PSB alarm indicates that K1/K2 protocol is not stable.
Minor	APS Far End Protection Failure	Far end protection failure indicates that the far end's protection line is failing. When there is Signal Failure on the protection channel, the remote end sees Far End Protection Fail.
Minor	APS Architecture Mismatch	Architecture mismatch means that the APS configuration on one end of the line does not match the APS configuration at the other side of the line. Specifically GR-253 at one end and ITUT at the other or 1+1 at one end and 1:1 at the other.
Info	APS Init/Clear/Revert	A BXM APS event indicating that the BXM APS has been initialize or a clear switch has occurred or a revert switch has occurred.
Info	Cannot perform a Clear/Revert switch	A BXM APS event indicating that the BXM APS was unable to perform a clear or revertive switch.
Info	APS Manual switch	A BXM APS event indicating that the BXM APS has performed a user requested manual switch.
Info	Cannot perform a Manual switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested manual switch.
Info	APS Signal Degrade LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal degrade condition. An automatically initiated switch due to a "soft failure" condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Info	Cannot perform a Signal Degrade LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal degrade condition.
Info	APS Signal Degrade HiPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a high priority signal degrade condition. An automatically initiated switch due to a "soft failure" condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Info	Cannot perform a Signal Degrade HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal degrade condition.
Info	APS Signal Failure LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a Signal Failure LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal failure condition.

Table 4-28 APS Alarms (Continued)

Class	Name	Description
Info	APS Signal Failure HiPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a high priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a Signal Failure HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal failure condition.
Info	APS Forced switch	A BXM APS event indicating that the BXM APS has performed a user requested forced switch.
Info	Cannot perform a Forced switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested forced switch.
Info	APS Lockout switch	A BXM APS event indicating that the BXM APS has performed a user requested switch which prevents switching from working line to protection line from taking place.
Info	Cannot perform a Lockout switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested lockout of protection switch.
Info	WTR switch	A BXM APS event indicating that the BXM APS performed a switch due to a Wait to Restore timeout. A state request switch due to the a revertive switch back to the working line because the wait-to-restore timer has expired.
Info	Cannot perform a WTR switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a WTR condition.
Info	Exercise switch	Not supported.
Info	Cannot perform a Exercise switch	Not supported.
Info	Reverse switch	A BXM APS event indicating that the BXM APS performed a switch due to a reverse request. A state request switch due to the other end of an APS bi-directional line performing an APS switch.
Info	Cannot perform a Reverse switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a reverse switch request.
Info	No Revert switch	A BXM APS event indicating that the BXM APS performed a switch due to a Do not Revert. A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
Info	Cannot perform a No Revert switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a Do not Revert switch request.
Minor	Standby Line Section Trace	APS standby line alarm.
Minor	Standby Line Path Trace	APS standby line alarm.
Minor	Standby Line path yellow alarm	APS standby line alarm.
Minor	Standby Line path AIS	APS standby line alarm.
Minor	Standby Line loss of pointer	APS standby line alarm.

Table 4-28 APS Alarms (Continued)

Class	Name	Description
Minor	Standby Line loss of cell	APS standby line alarm.
Minor	Standby Line plcp yellow alarm	APS standby line alarm.
Minor	Standby Line plcp out of frame alarm	APS standby line alarm.
Minor	Standby Line yellow alarm	APS standby line alarm.
Minor	Standby Line alarm indication signal (AIS)	APS standby line alarm.
Minor	Standby Line out of frame alarm (LOF)	APS standby line alarm.
Minor	Standby Line loss of signal alarm (LOS)	APS standby line alarm.

Architecture Mismatch

Architecture mismatch means that one side supports 1+1 and the other end of the line is configured for 1:1, or the directional or revertive parameter does not match. Firmware cannot bring the two ends into compliance on the fly; the user must correct the configuration error.

APS K1 Command Precedence

The possible conditions that can cause or prevent a switch are listed in Table 4-29. The list is arranged starting from highest precedence and ending with lowest precedence.

Table 4-29 K1 Switching Conditions

APS K1 Command Precedence
Lock out of Protection—An external user requested switch which prevents switch from working line to protection line from taking place. Lock out specified APS pair from being switched to protection line. If protection line is already active, switch is made back to the working line. Prevents specified APS pair from being switched to protection line. If protection line is already active, switch is made back to the working line.
Forced Switch—An external user requested switch which forces a switch from the working line to protection line, or vice-versa even if there is an alarm on the destination line. See Table 4-73 on page 4-184, options 3 and 4, for more information.
Signal Fail—An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Signal Degrade—An automatically initiated switch due to a “soft failure” condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Manual Switch—An external user requested switch which requests a switch from working line to protection line or vice-versa but only if there is no alarm on the destination line. Manual switch (Protection to working line)—Will not switch if other line is in alarm. Manual switching does not exist for Annex B.

Table 4-29 K1 Switching Conditions (Continued)

APS K1 Command Precedence
Wait To Restore—A state request switch due to the revertive switch back to the working line because the wait-to-restore timer has expired. Revertive switch Wait-to-restore timer expired, reverted back to working line.
Reverse Request—A state request switch due to the other end of an APS bi-directional line performing an APS switch.
Do not Revert—A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
No Request—A state request due to the external user request being cleared (such as a forced switch) while using revertive switching.

APS Command Summary

A number of commands have been added and modified to support APS. These are listed in Table 4-30, and defined in more detail in the following pages. This is a list of the APS switch events that the BXM can return to switch software. They can be switched successfully or failed (that is, the switch cannot be done).

Table 4-30 APS Commands

Command	Description
New Commands in Release 9.2 to Manage APS	
cnfcdaps slot	sets APS options on the card
addapsln slot1.port1 slot2.port2 protocol	adds APS
delapsln slot.port	deletes APS
dspapsln	displays status of APS line pairs
switchapsln slot.port	controls the APS user switching interface
cnfapsln slot.port	configures the APS parameters on a line a
New Commands for Card Redundancy for APS 1+1	
addcdred	adds redundancy across two cards (operates like **addyred** command)
dpscdred	displays redundant cards (operates like **dspyred** command)
delcdred	deletes redundancy configuration for cards (operates like **delyred** command)
prtcdred	prints active and redundant cards (operates like **prtyred** command)
switchcdred	switches active and redundant cards (operates like **switchyred** command)
Commands Modified for use with APS	
cnfbkcd	modified to APS options
dspalms	added row for "APS Alarms" which lists Minor and Major APS alarms
dspcd	displays front and back card APS attributes. For the front card, displays that card supports APS 1+1 and APS 1:1. For the back card, displays if back card is a redundant back card, and if so, the slot number of the redundant back card. Also, displays APS mismatch conditions
dspsv3	modified to display APS alarms pending
dsplog	displays APS alarms
addyred	modified to prevent invalid configurations when combined with APS
delyred	modified to prevent invalid configurations when combined with APS

Troubleshooting Notes

Introduction

Automatic Protection Switching (APS) is the ability to configure a pair of SONET lines for line redundancy so that hardware automatically switches from a Working line to a Protection line when the Working line fails, and vice versa. Each redundant line pair consists of a Working Line and a Protection Line. The concept of Working and Protection Lines is similar to the concept of Primary and Secondary Y Redundant cards. That is, the Working line is the logical line which the user refers to.

Left undisturbed, hardware performs line switching automatically. Upon detection of a Signal Fail condition (LOS, LOF, Line AIS or Bit Error Rate exceeding a configured limit) or a Signal Degrade condition (BER exceeding a configured limit), hardware switches from the Working Line to the Protection Line (assuming the Working line was the Active line and the Protection line is not in alarm). If the Revertive option is Enabled, hardware switches back to the Working line automatically after a configured time period called Wait to Restore has elapsed (assuming the Working line is now OK). Coordination between the two ends of the line is accomplished using the in-band protocol.

During setup, the commands **addapsln**, **cnfcdaps**, and **cnfapsln** are used to create the line-redundant pair. Also, appropriate front cards, back cards, and a special RDNT-BP daughter backplane are required for APS 1+1 configurations.

During operation, signal failure or signal degradation can cause APS "switchovers". A switchover is when the line that was active gives up control to its partner line. This partner line now becomes the "active" line, while the original active line becomes the "standby" line.

For APS line redundancy, the following problems can occur:

- "APS Configuration Problems" section on page 4-71
  - "Not Able to Correctly Set Up APS 1+1 Line Redundancy Configuration" section on page 4-71
  - "Unable to set up APS 1:1 line redundancy configuration" section on page 4-71
  - "Operator information about APS architectures" section on page 4-72
- "Operational Problems" section on page 4-73
  - "What the various APS switches mean" section on page 4-73
  - "Unable to perform APS external switch after forced or manual APS switch" section on page 4-73
  - "APS manual switch to a line does not occur right away" section on page 4-74
  - "Switch occurs after lockout issued" section on page 4-74
  - "APS switch made to a line in alarm" section on page 4-75
  - "APS Switch occurs even though APS Forced switch is in effect" section on page 4-76
  - "APS switch occurs at the same time as a yred switch" section on page 4-75
  - "APS switch occurs after issuing an APS clear switch" section on page 4-76
  - "APS Switch occurs even though APS Forced switch is in effect" section on page 4-76
  - "APS line is failing to switch" section on page 4-76
  - "Large cell loss when performing a front card switchover" section on page 4-77

APS Configuration Problems

The following sections describe possible APS configuration problems.

Not Able to Correctly Set Up APS 1+1 Line Redundancy Configuration

Description

The **addapsln** user interface command fails to execute correctly for APS 1+1 line addition.

Initial Investigation

The **addapsln** command is used to setup the APS line redundancy configuration. For APS 1+1 configurations, BPX software supporting APS and BXM firmware supporting APS must be used. Also the following hardware requirements must be met:

- BXM-Enhanced OC-3 or OC-12 front cards. BXM -155-4 or BXM-155-8 front card of revision C or higher. BXM-622-2 or BXM-622-1 of revision E or higher.
- RDNT-BP daughter backplane - special APS redundancy backplane
- BXM OC-3 or OC-12 APS back cards (they have two connectors on the back instead of one and require the daughter backplane in order to fit into the BPX backframe.
- Card redundancy (**addcdred or addyred**) must be set up on the card pair prior to **addapsln**, see section on Y-cable issues. APS does not use the special Y-cable, it uses straight cables on both ports to the remote port. The redundant card must be in adjacent slots.
- Using a back card frame containing internal card cage stiffeners requires that only slots 2-5 and 10-13 be used for APS 1+1 configurations. This is due to the stiffeners preventing the daughter backplane from fitting into the back card frame.
- A newer back card frame removes the slot restriction of having to put daughter backplane and APS back cards in slots 2-5 and 10-13.

Workaround

None.

Unable to set up APS 1:1 line redundancy configuration

Description

The **addapsln** user interface command fails to execute correctly for APS 1:1 line addition.

Initial Investigation

For APS 1:1 configuration, two adjacent lines on the same card are used. No special hardware is required however the maximum connections supported must be reduced by half using the **cnfcdaps** command. FW and SW support of APS is required.

Workaround

APS 1:1 can be run on non APS enhanced BXM card by halving the number of channels the card can support (**cnfcdaps**). No special back cards are needed for APS 1:1.

Detailed Debugging

For APS 1:1 configuration the APS line must be configured (**addapsln**) before a line (**upln**) or trunk (**uptrk**) can be upped. Conversely, the line or trunk must be downed before the APS line can be deleted (**delapsln**). Use **dspapsln** to verify that the APS line has been added.

Operator information about APS architectures

Description

The **cnfapsln** user interface command fails to allow the user to configure any combination of APS architectures.

Initial Investigation

The APS configuration can be changed using the **cnfapsln** command, however not all combinations are allowed. Here is a table of combinations allowed and disallowed.

Table 4-31 Possible APS System Architectures

	APS 1:1		APS 1+1, 1+1 ignore K1		APS 1+1 Annex B	
Mode	**Revertive**	**Non-revertive**	**Revertive**	**Non-revertive**	**Revertive**	**Non-revertive**
Bi-directional	Default	Not Valid	Valid option	Valid option	Not Valid	Default
Uni-directional	Not Valid	Not Valid	Valid option	Default	Not Valid	Not Valid

Once the APS configuration 1+1, 1:1, 1+1 Annex B, or 1+1 ignore K1 is chosen by the **addapsln**, it cannot be changed except by deleting the APS line (**delapsln**) and re-adding the APS line with the new configuration (**addapsln**).

Work Arounds

None.

Operational Problems

The following sections describe possible APS operational problems.

What the various APS switches mean

Description

There are ten reasons an APS switch may occur. You can view these reasons by using the **dsplog** command. When the BXM switches an APS line it returns an event message to switch software with the reason why it switched and which line is active.

Initial Investigation

The following list shows the possible conditions that may cause/prevent a switch. The list is arranged starting from highest precedence and ending with lowest precedence.

1. Lock out of Protection—An external user requested switch that prevents switching from working line to protection line from taking place.
2. Forced Switch—An external user requested switch that forces a switch from working line to protection line or vice-versa even if there is an alarm on the destination line.
3. Signal Fail—An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
4. Signal Degrade—An automatically initiated switch due to a "soft failure" condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
5. Manual Switch—An external user requested switch which requests a switch from working line to protection line or vice-versa but only if there is no alarm on the destination line.
6. Wait To Restore—A state request switch due to the a revertive switch back to the working line because the wait-to-restore timer has expired.
7. Exercise—Not supported
8. Reverse Request—A state request switch due to the other end of an APS bi-directional line performing an APS switch.
9. Do not Revert—A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
10. No Request—A state request due to the external user request being cleared (such as a forced switch) while using revertive switching.

Unable to perform APS external switch after forced or manual APS switch

Description

The user performs a forced switch from the working line to the protection line (**switchapsln** Ln1 Ln2 3) and then another forced switch back to working line (**switchapsln** Ln1 Ln2 4). After this the user again tries to perform a forced switch to the protection line but sees nothing happen.

Investigation

Once a forced switch is made from the working line to the protection line and back again, a clear switch (**switchapsln** Ln1 Ln2 1) must be issued in order to perform another forced switch. This applies to APS manual and lockout switching also.

With APS 1+1, when repetitive **switchapsln** commands are issued, up to two in a row can be executed sequentially, when alternating between options 3 and 4 (forced switch), or 5 and 6 (manual switch), but no more. Attempts to execute a third **switchapsnln** will not succeed, and the following error message is displayed:

```
"Cannot request manual W->P when manual P->W switch in progress"
```

If users desire to perform repetitive **switchapls** commands, they need to issue a clear switch between each W-P, P-W pair of commands, for example:

```
switchapsln 2.1 1
```

APS manual switch to a line does not occur right away

Description

The user has issued a manual switch either to working or protection line. The switch did not occur because the destination line was in alarm. When the alarm is cleared on that line the switch does occur.

Explanation

The BXM firmware remembers the “last user switch request” (also called external request) and tries to switch to that line when it becomes available.

Switch occurs after lockout issued

Description

With protection line active, the user issues an APS switch lockout and a switch occurs back to the working line.

Investigation

This is normal operation. When the protection line is active and an APS switch lockout is issued, a switch to the working line will happen. The lockout function locks the working line as active. Only an external (user request) APS clear switch (**switchapsln** Ln1 Ln2 1) will disable the lockout.

APS switch made to a line in alarm

Description

The user performs a forced switch to a line with a line alarm. The switch is successful making an alarmed line active with possible loss of traffic.

Investigation

It is normal operation for a forced switch to cause a switch to a line even though it may be faulty. This allows the user to “force” a switch to standby line even if it is in alarm. A traffic outage may occur. During a manual switch request, the BXM firmware decides whether the switch should occur and the switch may not occur if there is an alarm on the standby line. An APS clear switch will allow automatic switching to resume following a forced switch.

Reverse switch

Description

User performs a forced or manual switch on local end of APS line in bidirectional mode but other end indicates a reverse switch was performed.

Investigation

This is normal operation. A reverse switch in bidirectional mode occurs on the far end of the APS line when the local end of the APS line performs a switch for any reason.

APS switch occurs at the same time as a yred switch

Description

Two related scenarios could cause this to occur.

1. A forced or manual switch is in effect. In **dspapsln**, the Last User Switch Request is forced or manual w->p or p->w. If a **switchcdred/switchyred** is performed (could be caused by card failure or physically removing card also) the front card switches and an APS switch occurs.
2. A clear switch is in effect. In **dspapsln**, the Last User Switch Request is clear. If a **switchyred** is performed (could be caused by card failure or physically removing card also) the front card switches and an APS switch occurs.

Explanation

Following a **switchcdred/switchyred**, or active card reset the BXM card will be instructed to perform an APS switch to align itself with the Last User Switch Request (**switchapsln**).When a yred (**switchcdred**) switch takes place on a BXM card pair being used for APS 1+1, the card being switched is sent configuration messages including the last user switch request. The BXM card will initially become active in an APS “clear” switch mode following a **switchcdred** or reset. This means that the APS switching is on automatic. However if the Last User Switch Request is a manual or forced switch, the software sends this request to the BXM, and the BXM will switch to this line if it is not already active. This switch is done to comply with the users last APS switch request.

In the second case, if the last user request is “clear”, full automatic APS switching is in effect with the working line being active by default. When there is no last user switch request (**switchapsln** to protection, for example) to switch to any particular line, the working line will become active.

APS switch occurs after issuing an APS clear switch

Description

User issues an APS clear switch (**switchapsln** Ln1 Ln2 1) command while protection line is active and a switch occurs to the working line.

Explanation

This is normal operation. An APS clear switch request causes the APS switching mechanism in the BXM to initialize. This will cause a switch back to the working line if the working line is in better shape than the protection line. If the protection line is not faulty, no switch will occur.

APS Switch occurs even though APS Forced switch is in effect

Description

A forced switch to protection line is performed. LOS on protection line causes a switch back to working line even though a forced switch is in progress

Explanation

Signal Fail on Protection line has higher priority than Forced switch. Whenever the protection line is in failure, there will be a switch to working line, even if the working line is failed or there is a forced W->P in effect.

APS line is failing to switch

Description

The user issues an APS forced or manual switch request but no switch occurs.

Investigation

This could be due to a forced, manual, or lockout switch being in progress and a clear switch is required (**switchapsln** Ln1 Ln2 1). Need to issue an APS clear switch (**switchapsln**) to exit forced, manual, or lockout switch state.

If running the ITUT APS standard protocol which does not report an Architecture Mismatch APS alarm the problem could be that one end of the line is bi-directional and the other is uni-directional.

Check that configuration is the same on both ends, specifically uni/bidirectional mode, 1:1/1+1 configuration.

A manual switch will not occur if the standby line is in alarm.

Large cell loss when performing a front card switchover

Description

A line that is configured for APS 1+1 line redundancy has its active front card switched either due to card failure, **switchyred** (**switchcdred**), or resetting the card. A loss of cells is observed.

Investigation

Cell loss at card switchover is not due to faulty APS. It is a a result of the card redundant switch (YRED switch) and there will be up to 250ms worth of traffic disruption during BXM front card switchovers.

APS service switch description

Description

What is an APS service switch? Does it work on APS 1:1 configurations?

Investigation

An APS service switch is only applicable to APS 1+1 configuration. It allows the user to switch all the APS lines on a card with a single **switchapsln** command with an "s" option at the end of the command. All APS lines on this card pair will be switched and made active on a single back card allowing the other back card to be removed for service.

Note Be sure that the associated front card is active for the back card that is to remain in the rack. You may have to perform a **switchcdred** so that the back card that the service switch switches to has its associated front card active. A service switch is not required in order to remove a BXM front card with APS 1+1 lines on it. The card redundancy will handle the switch to the other card without affecting the lines.

APS line does not seem to switch and active line is in alarm

Description of problem

A major line alarm is indicated on the active line yet it remains active due to no APS switch to the redundant line.

Initial Investigation

1 Verify that the configuration is correct (**dspapsln**, **cnfapsln**). See above configuration problems.

2 Use **dspapsln** to check the APS line's status. The **dspapsln** display shows the active and standby line's alarm status. It also shows if there are any APS alarms. If the active line alarm status shows OK but the standby line alarm status shows an alarm then a switch will not occur due to the standby line alarm. Troubleshoot the standby line problem. If the standby line alarm status shows OK but the active line alarm status shows an alarm then a switch should have occurred and there is a more obscure problem. If there is an APS alarm shown under Current APS alarms then this could be the problem, see above section on APS Alarms. If APS 1+1 is configured, use **dspcds** to check the status of the protection line's card. If there is a problem with this card a switch may not occur.

3 Verify the sequence of events by using **dsplog** and tracing the entries which contain information about this line or APS on this line. If a switch was attempted and succeeded due to a Loss of Signal, the message "APS SignalFail switch from LN 1 to LN 2" should be logged. If the switch failed there will be a message such as "Cannot do APS SigFail switch from LN 1 to LN 2".

Work Around

Perform a clear switch on each end of the APS line (**switchapsln 2.1 1**). This may get both ends in sync and clear up the problem.

A forced switch from working to protection may be performed (example: **switchapsln 2.1 3**). **WARNING:** If the protection line is in LOS and we force a switch to it, traffic will be lost.

If the line is an APS 1+1 line, then the front cards are redundant and the user may try a **switchcdred** (**switchyred**) to induce APS switching. This should normally have no affect on APS switching. APS switching and card redundancy switching are independent.

The BXM card may be reset in combination with an APS clear switch either before of after the reset at both ends of the APS line. Perform an APS clear switch on both on both ends of the line. Reset the BXM cards (**resetcd h**).

BXM back card LED green and yellow indications

Description

Prior to an APS switch the active card LED is green and the standby card LED is yellow. After the APS switch, both LEDs are green.

Explanation

The BXM back card LED is meant to show whether the card is currently being used by at this time. Green means that this card is in use. Yellow means that the card is not in use and could be removed for service. If the standby line's card's LED is green it means that part of this card is being used at this time. This could happen due to the APS 1+1 cross over circuit where the working line's front card is active but the protection line itself is active. The working line's back card is being used to shunt traffic to the protection line's back card.

BXM Port LED states

Scenario

For an APS 1+1 or APS 1:1 line pair, the port LEDs are the same color on working and protection line.

Explanation

To switch software, the APS line pair is a single logical line. Although required to send BXM messages to both lines, these messages will be the same message. Thus switch software cannot send different LED states to the BXM for the same APS line. The BXM firmware makes the protection line LED state the same as the working line LED state.

Alarms

What do APS Alarms Represent

The following sections describe APS alarm types.

Description

An APS alarm occurs in **dspalms** and **dspapsln**.

Initial Investigation

APS alarms can be of two types. There are APS specific alarms and there are line alarms reported by the standby line. The standby line alarm will be displayed in the **dspapsln** screen under “Standby Line Alarm Status”. If there are no other APS specific alarms, the standby line alarms will also show under “Current APS Alarm Status”. The meaning of the standby line alarms are the same as the meaning of the active line alarms which are reported in the 0x55 Line Alarms command and are discussed in other documentation. The APS specific alarms consist of seven alarms in addition to APS OK, and APS Deactivated, and Line Looped.

Some of the APS alarms reflect problems with the underlying APS channel protocol, the K1/K2 bytes. The K1 byte carries the request for a switch action on a specific channel to the remote end of the line. The K2 byte indicates the status of the bridge in the APS switch and also carries mode information.

- **Remote Signal FAIL**—A remote signal failure indicates that there is a problem with the far end signalling information in the K1K2 bytes. There is a problem with the protection line’s physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback and so on.).
- **Channel Mismatch**—Can only happen in bidirectional mode and indicates that there is a problem with the underlying APS channel protocol. The receive K2 channel number does not equal the transmit K1 channel number. There is a problem with the protection line’s physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback and so on.).

- **Prot Sw Byt FAIL**—Protection Switch Byte failure or PSB. In bidirectional mode indicates that there is an invalid K1 byte. The receive K1 request does not match the reverse request and is less than the transmit K1 request. In all modes a PSB alarm indicates that K1/K2 protocol is not stable. There is a problem with the protection line's physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback and so on.). This alarm will be seen if the local end of an APS working line or trunk is connected directly to the remote end's protection line or trunk.
- **APS Card Missing**—This alarm is seen in APS 1+1 configurations when BXM firmware determines that any BXM front or back card is missing. Check **dspcds** or look in the **dsplog** to see which card associated with the APS line is missing.
- **FarEnd Prot FAIL**—Far end protection failure indicates that the far end's protection line is failing. When there is Signal Failure on the protection channel, the remote end sees Far End Protection Fail. There is a problem with the protection line's physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback, and so on).If the other end shows the "Architect Mismatch" APS alarm then the APS standards could be different at each end. Use **cnfcdaps** or **cnfapsln** to check for this.
- **Architect Mismatch**—Architecture mismatch indicates that one end of the APS line is configured for APS 1+1 and the other end is configured for APS 1:1 which will not work. If the line is configured for GR-253 standard operation an architecture mismatch can also mean that one end is bi-directional and the other end is uni-directional (ITUT will not report this). Verify that the APS architecture is configured the same on either end of the APS lines using the **cnfapsln** command. This alarm will also be seen if the local end of an APS working line or trunk is connected directly to the remote end's protection line or trunk. In this case one end of the line usually will have a "Prot Sw Byt FAIL" alarm present. If the other end shows the "FarEnd Prot FAIL" APS alarm then the APS standards could be different at each end. Use **cnfcdaps** or **cnfapsln** to check for this.
- **Standard Mismatch**—Indicates that on the local end of an APS 1+1 configuration that one card is running the ITUT standard and the redundant card is running the GR-253 standard. Use the **cnfcdaps** command to check and change the standard.
- **Usr Line Loop**—The line is looped. Use the **dellnlp** command to clear the loop. Both working and protection lines are looped when an APS line is looped.
- **APS Standby Line Alarms** are also shown as APS alarms unless there is a higher priority APS alarm (those above) masking the standby line alarm. The APS standby alarms are the integrated line alarms reported by the standby line in the BXM Line Alarms message (0x55). If one of these alarms is shown, there is a problem with the standby line. Troubleshoot the line using standard line fault isolation procedures.
  - Rmt Sec Trc Fail
  - Rmt Path Trc Fai
  - Path Yellow
  - Path AIS
  - Loss of Pointer
  - Loss of Cell
  - Remote Framing
  - Frame Sync Alarm
  - Remote (YEL)
  - AIS (BLU)

- — Loss of Frm (RED)
- — Loss of Sig (RED)

Using Subrate Trunk Interface Control Templates

Subrate trunks use an Interface Control Template that specifies the configuration of an output control lead. The template defines which output lead is to be configured and whether the lead is asserted, inhibited, or follows a specified input source. You can configure a template for a subrate trunk individually or copy a template of another subrate trunk.

You manage subrate trunk interface control templates by using the following commands:

- **cnftrkict**—Configures an interface control template for a subrate trunk.
- **cpytrkict**—Copies the template from one subrate trunk and applies it to another trunk.
- **dsptrkict**—Displays the interface control template for a specified line.
- **prttrkict**—Prints the interface control template for a specified line.

Summary of Commands

Table 4-32 shows the full name and starting page for the description of each trunk command.

Table 4-32 List of Trunk Commands

Mnemonic	Description	Page
addapsln	Add SONET APS line redundancy to a BXM OC-3 or OC-12 card	4-84
addtrk	Add trunk	4-86
addtrkred	Add trunk redundancy	4-89
cnfapsln	Configure APS parameters on a working line of APS redundant pair	4-91
cnfcdaps	Configure various APS line parameters	4-96
cnfrsrc	Configure resources	4-100
cnftrk	Configure trunk	4-105
cnftrkalm	Configure trunk alarm	4-125
cnftrkict	Configure trunk interface control template	4-130
delapsln	Delete SONET APS line from a BXM OC-3 or OC-12 card	4-134
deltrk	Delete trunk	4-136
deltrkred	Delete trunk redundancy	4-138
dntrk	Down trunk	4-140
dspapsln	Display currently configured APS lines and their status	4-134
dspnw	Display network	4-145
dspphyslns	Display lines in an IMA trunk	4-147
dspphyslnstathist	Display statistics gathered for lines in an IMA trunk	4-150
dsptrkbob	Display trunk breakout box	4-152
dsptrkcnf	Display trunk configuration	4-154
dsptrkict	Display trunk interface control template	4-161
dsptrkred	Display trunk redundancy	4-163
dsptrks	Display trunks	4-165
dsptrkstats	Display trunk statistics	4-173
prtnw	Print network	4-182
prttrkict	Print trunk interface control template	4-184
prttrks	Print trunks	4-185
printapsln	Print the APS line redundancy switching interface	4-181
switchapsln	Control the APS line redundancy switching interface	4-186
uptrk	Up trunk	4-189

addapsln/delapsln

The **addapsln** and **delapsln** command lets you add SONET APS (Automatic Protection Switching) for BXM OC-3 or OC-12 lines.

SONET APS is a standard that describes the switching of SONET lines from the active line to a standby line to provide hardware line redundancy. The SONET APS feature only applies to BXM OC-3 and OC-12 cards in this release.

You must specify the desired APS protocol when adding a new APS line pair. The **delapsln** command deletes APS for the lines.

For background information on how SONET APS for BXM cards works, refer to the "Overview of SONET Automatic Protection Switching (APS)" section on page 4-51.

When the **addapsln** command executes, the switch software does the following:

- Verifies that the slot.port arguments support APS
- Verifies that the appropriate back card is installed
- Verifies that the protection port is not already active
- If card redundancy is already configured for the two-slot case (APS 1+1), verifies that the primary card is the same type as the working line card.

Before the **addapsln** command has been executed, there is no working or protection line. The **addapsln** command defines which line is the working line and which line is the protection line. (For APS 1+1 Annex B, the active line is called the "primary section", and the standby line is called the "secondary section", which provides protection for the primary section.)

Feature Mismatching to Verify APS (Automatic Protection Switching) Support

In this release, the **addapsln** command, in addition to other configuration commands, will perform mismatch verification on the BXM and UXM cards. For example, the **addapsln** command will verify whether the cards both have APS support configured. Refer to the "Feature Mismatching" section on page 18-1 for more information about Feature Mismatching in Release 9.2; also refer to Table 18-1 on page 18-2 for more information about upgrading firmware when single active card and Y-cable are in use.

Whenever you activate a feature by configuring the feature with CLI commands, switch software performs a verification to ensure that the hardware and firmware support the feature. For example, if you are attempting to add APS on a specific line (by using **addapsln**), and the BXM card does not support this feature, a warning message is displayed and the addition is not completed.

The Feature Mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Full Name

Add a SONET APS (Automatic Protection Switching) line

Syntax

addapsln <slot.port1> < slot.port2> <protocol>

You must enter the slot.port pair and the protocol option. If you do not enter the protocol option, a menu listing the options is displayed.

Table 4-33 addapsln Parameters

Parameter	Description
slot.port1	The desired working line number
slot.port2	The desired protection line number
protocol	1: 1+1 2: 1:1 3: 1+1 Annex B 4: 1+1, ignore K1K2 bytes

Related Commands

delapsln, cnfapsln, cnfcdaps, dspapsln, dsplog, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	BPX	Yes

Example 1

`addspln 2.1 3.1 1`

Description

Add an APS redundant pair, with Working line on slot2, port 1; Protection line on slot 3, port 1; with "1" specifying APS 1+1 protocol.

System Description

```
alexa       TRM    genre        BPX 8620          9.2        Sep. 9 1998          16:08 PDT

                                Actv        Current Line         Current APS          Last User
Work/Protect     Protocol       Line        Alarm Stat           Alarm StatCard       Switch Req
2.1 3.1          1+1            WORK        OK                   APS OK               Clear

Command: addapsln 2.1 3.1 1
```

addtrk

Adds a trunk between nodes. You must add a trunk to the network before it can carry traffic. You only need to execute **addtrk** at one of the nodes terminating the trunk. Before you add a trunk to the network, you must have activated (or "upped") the trunk at both ends by using **uptrk**.

A trunk must be free of major alarms before you can add it. If you use **addtrk** to join two networks that were previously separate, the local node verifies that all node names and node numbers in both networks are unique before it adds the trunk.

You cannot add a trunk while any of the following conditions are true:

- Another node is attempting to change the network topology by adding or deleting a trunk.
- Another node is notifying all nodes that it has been renamed.
- Another node is currently adding or deleting a connection in the network with the **addcon** or **delcon** command.
- An unreachable node exists in the network.
- Connections are rerouting.
- The node names or the node numbers across the two networks are not unique. Use the command and optional parameter **dspnds +n** to see the node numbers.

When using the **addtrk** command, exercise caution when adding a new node to a network or one network to another network. With these particular operations, the user IDs and passwords may be replaced by those in the other network. Consult Customer Service before performing these operations.

Adding a Virtual Trunk

You can add a trunk as a physical trunk or a virtual trunk. A virtual trunk is a way to connect Cisco nodes through a public ATM cloud. For this release, you can define virtual trunks on BNI, BXM and UXM cards. Note that even though nodes running Release 9.2 can interoperate with 9.1 or 8.5 nodes, if you are running a network with mixed releases, you cannot add UXM and BXM virtual trunks because the networking messages are incompatible due to the virtual trunk number and different cell format on virtual trunks. (BNI cards use STI cell format, and BXM and UXM cards use NNI cell format.)

To designate a trunk as a virtual trunk, you use a virtual trunk number, which is used to differentiate the virtual trunks within a physical port. (Refer to the *BPX 8600 Series Reference* for more information on virtual trunking.)

For the BXM card, you can define a maximum of 32 virtual trunks within one port. Valid virtual trunk numbers are 1-31 per port. The number of virtual trunks available is limited by the number of VI (virtual interfaces) available on the card. Each logical trunk (physical or virtual) consumes on VI.

For the UXM card, you can define a maximum of 16 virtual trunks within one port. Valid virtual trunk numbers are 1–15.

The addtrk command will be blocked for virtual trunks configured for VSI.

Full Name

Add trunk to the network

Syntax

addtrk <slot.port>[.vtrk]

Related Commands

deltrk, dsptrks, uptrk

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

addtrk 7

Description

Add trunk between node beta slot 7 and node alpha slot 10.

System Response

```
beta           TRM   YourID:1        IPX 8430    9.2    Aug. 3 1998 15:04 MST

PLN Type      Current Line Alarm Status               Other End
7    E1/32     Clear - Line OK                          alpha.10
9    T1/24     Clear - Line OK                          gamma.10
13   T1/24     Clear - Line OK                          alpha.14
15   T1/24     Clear - Line OK                          gamma.15
20   T3/3      Major - AIT Missing                      -









Last Command: addtrk 7


Next Command:
```

Table 4-34 addtrk–Parameters

Parameter	Description
slot.port	Specifies the slot and port number of the trunk to add.

Table 4-35 addtrk–Optional Parameters

Parameter	Description
vtrk	Specifies the virtual trunk number. Virtual trunking is supported on a BNI or BXM card on a BPX node, or a UXM card on an IGX node. The maximum number of virtual trunks per physical port you can add on a BNI card is 32. The maximum on a T3 or E3 line is 32. The maximum on an OC-3/STM1 line is 11. The maximum number of virtual trunks per port you can add on a BXM card is 32 virtual trunks The maximum number of virtual trunks per port you can add on a UXM card is 16.

addtrkred

Configures trunk redundancy on an ATM trunk. The **addtrkred** command specifies a backup trunk to the primary trunk. Applicable line types are T3 and E3. The redundancy scheme requires two sets of ATM trunk cards and two standard T3 or E3 cables (not Y-cables). Note the following characteristics of trunk redundancy:

- Applicable card sets are the AIT, BTM, and ALM/B connected to a BNI card set on a BPX node. (Trunk redundancy between an AIT, BTM, and ALM/B is not allowed.)
- Execute **addtrkred** on an IPX or IGX but not on the BPX side.
- Primary and backup card sets must be in adjacent slots.
- After a primary trunk failure clears, the traffic automatically returns to the primary card set.
- Trunk redundancy is not compatible with virtual trunking.

Full Name

Add trunk redundancy

Syntax

addtrkred <primary trunk> <secondary trunk>

Related Commands

deltrkred, dsptrkred

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	IGX	Yes

Example 1

```
addtrkred 4 5
```

Description

Add bandwidth redundancy for the primary ATM trunk in slot 4 with backup from the ATM trunk in slot 5.

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 3 1998   15:15 MST

ATM Line   Backup ATM Line
   4           5












Last Command: addtrkred 4 5


Next Command:
```

Table 4-36 addtrkred–Parameters

Parameter	Description
primary trunk	Specifies the slot number of the primary trunk card set.
secondary trunk	Specifies the slot number of the secondary trunk card set as backup.

cnfapsln

SONET APS Line Redundancy in this release implements industry standards. Switching is performed by hardware with better performance than the ATM Trunk Redundancy feature introduced in release 8.4. (The ATM trunk redundancy feature is supported on the IGX platform only.) Both features are supported in this release: the IGX platform supports ATM trunk redundancy; the BPX supports SONET APS line redundancy. APS line redundancy provides a standards-based solution to line redundancy.

The **cnfapsln** command lets you configure various APS line parameters. Below is a list of the configurable APS parameters:

- **Signal Fail Bit Error Rate (SFBER)**—Signal Fail Bit Error Rate threshold which will cause an APS switch.
- **Signal Detect Bit Error Rate (SDBER)**—Signal Detect Bit Error Rate threshold for line degradation (which will cause an APS switch).
- **Revertive/Non Revertive—**Revert to working line after WTR interval expires. You must enter the number 0 or 1. This only applies to automatic switches. Revertive switching does not take place as a result of user-initiated switching.
- **Wait to Restore (WTR)**—Wait to restore interval. After a switch from a working to a protection line, this is the interval in minutes to wait before attempting to switch back to the working line. This is not applicable if the revertive mode option is set to N (non-revertive).
- **Direction (Uni-directional/Bi-directional)**—Direction of switching. Uni-directional is switching in only one direction. With Bi-directional, after one side switches, the other end will switch also.

Note For the Annex A protocol, you cannot set both the Bi-directional and Non-revertive options—they are invalid combinations. For the Annex B protocol option, the default is Bi-directional and Non-revertive.

Table 4-37 lists configurable APS parameters, descriptions, and possible ranges and options.

Table 4-37 Configurable APS Parameters

Parameter	Description	Range/Options
slot.port	Slot and port of the line you want to configure	–
SFBER (Signal Fail Bit Error Rate)	Signal Fail Bit Error Rate threshold at which point an APS switch occurs	Default is 3 range is 3–12
SDBER (Signal Detect Bit Error Rate)	Signal Detect Bit Error Rate for line degradation	Default 5 range is 5–12
Revertive mode	Revert to Working line after Wait to Restore interval expires. You must enter the number 0 or 1. This only applies to automatic switches. Revertive switching does not take place as a result of user-initiated switching. For Annex A, the default is non-revertive. For Annex B, the default is non-revertive. For Annex B, you are not allowed to change to uni-directional or revertive mode.	Default = 1 range is 0–1 0 = revertive 1 = non-revertive
WTR (Wait to Restore)	Wait to restore interval. After a switch from a Working to a Protection line, this is the interval in minutes to wait before attempting to switch back to the Working line. This is not applicable if the Revertive Mode option is set to N (Non-revertive)	Default is 5, range is 1–12 minutes
Direction	Direction of switching. Unidirectional is switching in only one direction. With Bidirectional, after one side switches, then the other side also switches. For Annex A, the default is unidirectional. For Annex B, default is bidirectional. For Annex B, you are not allowed to change to unidirectional or revertive mode.	Default is 0 (unidirectional) Range is 0–1, where 0 is unidirectional and 1 is bidirectional.

Full Name

Configure various SONET APS line parameters

Syntax

cnfapsln <*slot.port*> <*SFBER*> < *SDBER*> <*Revertive_mode*> <*WTR*> <*Direction*>

where:

slot.port	slot.port of working line of APS pair to be configured
SFBER	Signal Fail Bit Error Rate for line degradation You must enter a number between 3 and 12. Default is 3.
SDBER	Signal Detect Bit Error Rate for line degradation. You must enter a number between 5 and 12. Default is 5.
Revertive/Non	Revert to working line after WTR interval. You must enter 0 (revertive) or 1 (non-revertive).
WTR	Wait to Restore timer [1–12 minutes] You must enter a number between 1 and 12.

Direction	Direction of switching. Uni-directional is switching in only one direction. With bidirectional, after one side switches, then the other side also switches. You must enter 0 for Unidirectional, 1 for Bidirectional. (For Annex B, you are not allowed to change to Uni-directional or revertive mode.)

Related Commands

addapsln, delapsln, cnfapsln, cnfcdaps, dspapsln, dsplog, dspalms, switchapsln

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	BPX	Yes

Example 1

`cnfapsln 1.1`

Description

Configures various APS line parameters (described in Table 4-37).

System Response

```
alexa       TRM    genre         BPX 8620          9.2         Sep. 9 1998
16:15 PDT

APS Configuration parameters for Working, Protection lines 1.1, 1.2

APS Protocol:                                          1+1

Signal Fail BER threshold (10 to the -n):              3
Signal Detect BER threshold (10 to the -n):            5
Revertive Switching:                                   Yes
Wait to Restore Timer:                                 5 minutes
Uni/Bi Directional Switching:                          Unidirectional

Command: cnfapsln 1.1
```

Example 2

cnfapsln 1.1

Description

Configures various APS line parameters (described in Table 4-37).

System Response

```
colossus       TN    StrataCom       BPX 8600    9.2    Sep. 9 1998 16:08 PDT

APS Configuration parameters for Working, Protection lines 1.1, 1.2

APS Protocol:                                  1+1

Signal Fail BER threshold (10 to the -n):     3
Signal Detect BER threshold (10 to the -n):   5
Revertive Switching:                           Yes
Wait to Restore Timer:                         5 minutes
Uni/Bi Directional Switching:                  Unidirectional

Command: cnfapsln 1.1
```

Example 3

`cnfapsln 6.3`

Description

Configures various APS line parameters (described in Table 4-37) for APS 1:1 line redundancy

System Response

```
colossus       TN    StrataCom       BPX 8600    9.2    Sep. 9 1998 16:08 PDT

APS Configuration parameters for Working, Protection lines 6.3, 6.4

APS Protocol:                                  1+1

Channels Halved for APS operation:             Yes
APS Standard for Card:                         GR-253

Signal Fail BER Threshold (10 to the -n):      3
Signal Detect BER Threshold (10 to the -n):    5
Uni/Bi Directional Switching:                  Bidirectional
Revertive Switching:                           Yes
Wait to Restore Timer:                         5 minute(s)


Command: cnfapsln 6.3
```

cnfcdaps

Use the **cnfcdaps** command to set the APS 1:1 "channels halved" option and the APS standard option on the card. When you execute the command, the switch software performs the following syntax checking:

- verifies that the slot is a BXM OC-3 or OC-12 card
- verifies that the BXM card version supports APS
- verifies that the card does not already have **cnfcdaps** enabled
- issues a warning if any trunks or lines are upped on the card, and if so, issues a warning and prompts you to continue with the **cnfcdaps** command.
- issues a warning if you attempt to change the APS standard to GR-253 while an Annex B–configured trunk/line is on the card.

Caution The **cnfcdaps** command is a service-level command, which is not accessible to privilege levels 1 through 6, or to SuperUser level users. You must have service-level privileges to access this command. As improper use of this command could cause card mismatch, thus affecting traffic, use it with caution.

Note You must have Service level privileges to use the **cnfcdaps** command.

Executing the **cnfcdaps** command will automatically perform a **resetcd** (reset card).

Configuring the APS Standard Option (GR-253—Annex A or ITUT–Annex B)

Following are some things to be aware of when configuring either Annex A (GR-253) or Annex B (ITUT) options:

- You use the same commands to configure the Annex A (GR–253) protocol as you do to configure the Annex B protocol (ITUT).
- If you are configuring the Annex B (ITUT) protocol, there is no difference in the way the APS commands work from the way they work when configuring the Annex A option.
- You cannot configure Annex B in uni–directional mode. (Annex B is bi-directional only.) Also, you cannot configure Annex B in revertive mode. (Annex B is non-revertive.)
- If you specify the ITUT protocol by using the **cnfcdaps 0** option, the Annex B protocol will be configured and used as the APS standard. Annex B always uses APS 1+1, bi–directional, and non–revertive.
- When configuring APS with **cnfapsln**, you may be prevented from making some changes (if you have specified the ITUT (Annex B) option by using the **cnfcdaps** command.
- You cannot use the Annex B protocol while in GR-253 (Annex A) mode.

GR-253 (Annex A) Configuration. When you configure GR-253 (Annex A) with the **cnfcdaps 1** option (the default), the working and protection lines are identified as "Work/Prot".

When Annex A (GR–253) is configured with the **cnfcdaps 1** option (GR-253 is the default), either the working line or the protection line can be active. If the working line has an alarm activated on it, APS switches back to the protection line, thus making the protection line the "active" line. If there is an alarm on that line, and the alarm has been cleared on the working line, it reverts the working line back to the active line. The protection line serves as a backup line to the "active" line, or "working" line.

ITUT (Annex B) Configuration. When Annex B is configured as the APS standard (with the **cnfcdaps 0** option), the lines are identified as "Work1/Work2". (These are shown on the **dspapsln** screen as "Work1" and "Work2".) The "Work1" line corresponds to the working line used in Annex A (GR–253), and the "Work2" line corresponds to the protection line used in GR-253 (Annex A). (Work1 and Work2 lines are also sometimes referred to as "primary" and "secondary" lines, and as "working section 1" and "working section 2".) The GR-253 (Annex A) terminology (that is, "working" and "protection" lines) refers to lines on all other screen displays (except for **dspapsln** screen) for ITUT (Annex B) lines.

If the Work1 line has an alarm activated on it, APS switches to Work2. While the alarm is still on the Work1 line, and APS has already switched, the "Work1" line is still the primary line, and "Work2" is still considered the secondary line. If the alarm clears on "Work1", no switch occurs. Instead, the "Work2" line becomes the primary line, and the "Work1" line becomes the secondary line.

Note When using the Annex B protocol (ITUT) (which you configure with the **cnfcdaps 0** option), some configuration changes may not be allowed that would be allowed when using Annex A (GR-253) protocol.

You cannot use Annex B protocol standard when in GR-253 mode. Annex B can be configured by specifying the ITUT option of **cnfcdaps 0**.

APS Environment Setup

This section provides a brief functional description of APS support for the BPX platform. The following configurations of APS are supported in this release:

- APS 1:1, front and back card, using existing hardware

  To use the APS 1:1 feature, no new hardware is required. A single front card with a regular single back card will support APS 1:1. Two adjacent lines on the same card are used. A firmware upgrade that supports APS 1:1, Release 9.2 switch software, and Cisco WAN Manager Release 9.2 is required.

  For APS 1:1 using existing hardware, you must use the **cnfcdaps** command to reduce the maximum number of connections on the BXM card, which will in turn decrease the number of channels on the card by half. If lines or trunks are upped already on this card, a warning will be issued and the request denied, because changing the number of channels on the fly will cause a card mismatch condition.

- APS 1:1, using new hardware

  Two adjacent lines on the same card are used. (You do not need to use the **cnfcdaps** command to change the number of maximum connections on the card.) A BXM-Enhanced card, a BXM-E daughter card, BXM firmware revision that supports APS in Release 9.2 (refer to 9.2 release notes), Release 9.2 BPX system software, and Cisco WAN Manager 9.2 software.

- APS 1+1, two front and back cards, new hardware, combined with front card redundancy

You should first use the **dspcd** command to check if the BXM card supports the APS option.

Installing SONET APS is service-affecting. For APS 1:1 using existing hardware, you can use the **cnfcdaps** command only when all lines and trunks have been downed. For the other options (for example, APS 1:1 with front and back card and new hardware; APS 1+1 with two front and back cards, new hardware, combined with front card redundancy), logical lines, trunks and connections can remain intact, but you must install new firmware and hardware.

For the two-card option, you must install a special dual slot backplane. In addition, when existing BXMs are replaced with BXM APS hardware, the new card must match or exceed the old card's number of channels to avoid a Mismatch condition. Refer to the "Overview of SONET Automatic Protection Switching (APS)" section on page 4-51 for more information.

Executing the **cnfcdaps** command will automatically perform a **resetcd** (reset card).

Full Name

Configure BXM OC-3 or OC-12 card with SONET APS line redundancy options

Syntax

```
cnfcdaps <slot> <Y/N> < 0/1>
```

where:

slot Desired APS slot number

N/Y Disable/enable the channels halved option on the card (Default is disabled, or *N*.)

0/1 0 = ITUT (Annex B), 1= GR–253 (Default is 1—GR–253, or Annex A)

Table 4-38 cnfcdaps Parameters

Parameter	Description
slot	Specifies the desired BXM APS slot number.
Y/N	Disable/enable the channels option on the card.
10/1	0 = ITUT, 1 = GR253

Related Commands

addapsln, delapsln, cnfapsln, cnfcdaps, dspapsln, dsplog, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	BPX	Yes

System Response

```
sw117          TN    StrataCom       BPX 8620 9.2.q3    Mar. 24 1999 21:54 GMT

APS Card Configuration parameters for card 2

Channels Halved for APS operation:               Yes
APS Standard for Card:                           GR-253







This Command: cnfcdaps 2 n


Enter channels halved option (Y or N);

Enter APS protocol standard to be used on card (0=ITUT, 1=GR-253):

                                                                     MAJOR ALARM
```

cnfrsrc

Use the **cnfrsrc** command to partition resources for Automatic Routing Management PVCs, VSI-Multiprotocol Label Switching (MPLS), or PNNI SVCs. To configure SVCs, an Extended Services Processor shelf must be configured in the BPX node. (If you want to configure resources for a VSI-MPLS controller or PNNI SVCs, refer to the "cnfrsrc" section on page 17-62 for more information specific to configuring VSI options.)

This command was introduced in Release 9.1 to support physical trunks. It has been extended to support virtual trunks. After VSI has been enabled, the virtual trunk becomes a "dedicated" VSI virtual trunk. Note that if the trunk has already been added or if the VPI value has not been configured, you will not be able to configure the VPI value. (Switch software will block you from doing so.)

Note Note that VSI-MPLS is not supported in Release 9.2; VSI will be supported in a post-9.2 release. If you upgrade to Release 9.2, the VSI commands will not be blocked at the CLI level, but they will not function.

In this release, you can configure a virtual trunk to be dedicated to VSI or to Automatic Routing Management. You cannot configure a virtual trunk for both VSI and Automatic Routing Management.

You configure all port and trunk attributes with **cnftrk**, **cnftrkparm**, or **cnfrsrc**. Note that when you change a physical port attribute, you will be notified that all the logical (physical and virtual) trunks on the port are affected.

Note Note that when using **cnfrsrc** to configure partition resources for Automatic Routing Management PVCs, and you are prompted whether you want to configure VSI options, enter "n" for No. You will not be prompted to enter any VSI options.

Configurable resources (using **cnfrsrc**) are:

- Template number— relevant only when configuring VSI options
- Maximum PVC LCNs
- Maximum PVC Bandwidth
- Configure Partition (Y/N)—Enter "n" for No to configure Automatic Routing Management PVCs. Enter "y" for yes to configure VSI options (in post-9.2 release).
- Partition ID
- Enable Partition (Enable/Disable)
- Minimum VSI LCNs
- Maximum VSI LCNs
- Start VSI VPI - **Warning message will tell you to use the cnftrk command**
- End VSI VPI - **Warning message will tell you that the end vsi vpi is equal to the start vsi vpi for virtual trunks**
- Minimum VSI Bandwidth
- Maximum VSI Bandwidth

The resources that you can currently configure are the number of connection IDs (conids) and the trunk bandwidth. In this release, you use the **cnfrsrc** command to configure the cell rate and number of connections on a BXM card only. (You cannot use the **cnfrsrc** command on the IGX.)

Configuration with **cnfrsrc**

cnfrsrc is used to configure conids (lcns) and bandwidth. The conid capacity indicates the number of connection channels on the trunk port which are usable by the virtual trunk.

This number cannot be greater than the total number of connection channels on the card. The maximum number of channels is additionally limited by the number of VCI bits in the UNI cell header. For a virtual trunk, the number is divided by the maximum number of virtual trunks on the port to determine the default. This value is configured by the **cnfsrc** command on the BPX. Table 4-39 lists the number of connection ids for virtual trunks on various cards.

Table 4-39 Maximum Connection IDs (LCNs)

Port Type	Maximum Conids	Default
BXM/UXM	1-(number of channels on the card)	256
BNI T3/E3	1-1771	256
BNI OC-3	1-15867 (3837 max/vtrk	256

Full Name

Configure partition resources

Syntax

cnfrsrc <slot>.<port> <maxpvclcns> <maxpvcbw> <partition> <e/d> <minvsilcns> <maxvsilcns> <vsistartvpi> <vsiendvpi><vsiminbw> <vsimaxbw>

Related Commands

dsprsrc

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX (BXM cards only)	No

Example 1

```
cnfrsrc 11.2 256 96000 y 1 e 0 0 1 1 0 0
```

Description

Configure resource partitions on card slot 11, port 2, to use Automatic Routing Management PVCs.

System Response

```
sw98             TN    SuperUser       BPX 8600    9.2.0r      Apr. 4 1998 16:40 PST

Port/Trunk : 11.2
Maximum PVC LCNS:            256     Maximum PVC Bandwidth:96000
Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1
Partition State :            Enabled
Minimum VSI LCNS:            0
Maximum VSI LCNS:            0
Start VSI VPI:               1
End VSI VPI :                1
Minimum VSI Bandwidth :      0       Maximum VSI Bandwidth :        0

Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000

Next Command:
```

Table 4-40 cnfrsrc—Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Maximum PVC LCNs	The maximum number of LCNs allocated for Automatic Routing Management PVCs for this port. The range is 1 to 256. 256 is the default. For trunks, there are additional LCNs allocated for Automatic Routing Management that are not configurable. You can use the **dspcd** <slot> command to display the maximum number of LCNs you can configure using the **cnfrsrc** command for the given port. For trunks, "configurable LCNs" represent the LCNs remaining after the BCC has subtracted the "networking LCNs" needed. A trunk has 270 networking LCNs, or channels. For a port card, a larger number is shown, as compared with a trunk card. This is because a trunk uses 270 networking LCNs, as compared with a port card, which uses no networking LCNs. Setting this field to "0" would disable Automatic Routing Management PVCs on the specified port. Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management PVC connections on a BXM card. Also, if these parameters do not have values greater than 0, you will be unable to change the connection channel amount when you configure the BXM trunk using **cnftrk**.
Maximum PVC Bandwidth	Specifies the maximum bandwidth of the port allocated for Automatic Routing Management use. The range is 0 to 352207. 0 is the default. You can configure the Maximum PVC Bandwidth value for ports, but not for trunks. Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management PVCs on the BXM card.

Table 4-40 cnfrsrc—Parameters

Parameter	Description
Configure Partition	Answer yes or no to begin configuring resources for the partition. If you enter “n” for No, you will not be prompted to configure any VSI options. If you are configuring Automatic Routing Management PVCs, enter “n” for No. If you want to configure VSI options, enter “y” for yes, and you will be prompted to enter the rest of the **cnfrsrc** parameters, which are related to configuring VSI (such as a VSI MPLS controller or a PNNI controller). Refer to the “cnfrsrc” section on page 17-62 for more information about VSI-related options.
Partition ID	Specifies the ID number of the partition. 1 is the default. Always use 1 in Release 9.1 and Release 9.2.10. (The range of 0 to 255.)
Enable Partition	Answer yes or no to enable your configured partition.
Minimum VSI LCNs	The minimum number of LCNs guaranteed for this partition. The range is 1 to 256. 0 is the default. The VSI controller guarantees at least this many connection endpoints in the partition, provided there are sufficient free LCNs in the common pool to satisfy the request at the time the partition is added. When a new partition is added or the value is increased, it may be that existing connections have depleted the common pool so that there are not enough free LCNs to satisfy the request. The BXM gives priority to the request when LCNs are freed. The net effect is that the partition may not receive all the guaranteed LCNs (min LCNs) until other LCNs are returned to the common pool. You can increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. To avoid this deficit condition, which could occur with maximum LCN usage by a partition or partitions, it is recommended that all partitions be configured ahead of time before adding connections. Also, it is recommended that all partitions be configured before adding a VSI controller using the **addshelf** command.
Maximum VSI LCNs	The total number of LCNs the partition is allowed for setting up connections. The min LCNs is included in this calculation. If max LCNs equals min LCNs, then the max LCNs are guaranteed for this partition. Otherwise, (max - min) LCNs are allocated from the common pool on a FIFO basis. If the common pool is exhausted, new connection setup requests will be rejected for the partition, even though the maximum LCNs has not been reached. You may increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. Different types of BXM cards support different maximum values. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum value. Note that you must specify a value greater than 0 for the Maximum VSI LCNs, Maximum PVC Channels, and Maximum PVC Bandwidth parameters. Otherwise, you will not be able to add any connections on a BXM card.

Table 4-40 cnfrsrc—Parameters

Parameter	Description
Start VSI VPI	By default the TSC (for example, the 7200 or 7500 series router) will use either a starting VSI VPI of 1 or 2 for tag switching, whichever is available. If both are available, a starting VSI VPI of 1 is used. The VPI range should be 2-15 on a BPX 8620 VSI. The VSI range for tag switching on the BPX 8620 is configured as a VSI partition, usually VSI partition number 1. VSI VPI 1 is reserved for Automatic Routing Management PVCs. (This restriction applies only to trunks, not to ports. For a port, you can use any VPI value.) For a port UNI, the VPI range is 1 to 255. For a port NNI, the range is 1 to 4095. For trunks that do not have Automatic Routing Management configured, the VPI ranges are the same as for ports. The VSI partition for tag switching should start at VPI 2. If VPI 2 is not to be used, you can use the tag switching VPI interface configuration on the TSC to override the defaults. For trunks with Automatic Routing Management configured, the range is 2 to 4095. Always set to 2 for trunks.
End VSI VPI	Two VPIs are sufficient for Release 9.1, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 2-15. The range is the <*Start VSI VPI* > value to 4095.
Minimum VSI Bandwidth	The minimum port bandwidth that can be used by this partition in cells/second. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.
Maximum VSI Bandwidth	The maximum port bandwidth that can be used by this partition. This value is used for VSI Qbin bandwidth scaling. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.

cnftrk

Configures trunk parameters. A trunk has a default configuration after you activate (or "up") the trunk with the **uptrk** command. Beyond this default configuration, **cnftrk** lets you configure trunk parameters. Typically, you use **uptrk** to first up the trunk, then use **cnftrk** to configure trunk parameters, then use **addtrk** to add it to the network. You must execute **cnftrk** at both ends of a trunk. (You also use **cnftrk** to configure an interface shelf.)

The section "cnftrk–Parameters" in this description shows required **cnftrk** parameters. The section entitled "cnftrk–Optional Parameters" shows virtual trunk parameters. You can reconfigure some parameters after adding a trunk with **addtrk**. See the "Reconfiguring a Trunk" section on page 4-48."

In the display for **cnftrk**, the current value for each parameter appears on screen. At the command line prompt for each parameter, the current or default value appears in parentheses and stays the same if you press Return without entering anything. Configurable parameters depend on the trunk type. For example, an NTM card and a BNI support different parameters. If a displayed parameter is not available for the current interface, its name displays at half-intensity, and the value field contains dashes. (Note that Clock Rate is a required parameter for only HSSI. The Clock Rate range is 4 Mbps–50.84 Mbps. The actual clock limits depend on the front card.)

Note If you specify **cnftrk** in a job, prompts appear for line format and line options when you create or edit the job with **addjob** or **editjob**, respectively.

As of Release 9.1, you can configure cost-based routing from either end of the trunk. You can change the cost before or after the trunk has been added to the network. You can also change the cost after connections have been routed over the trunk. Any cost change is updated network-wide. Every node in the network stores the cost of every trunk in the network.

In this release, the **cnftrk** command configures a logical trunk (physical or virtual), so when you change a physical parameter, all trunks on the port (both physical and virtual) are affected. For example, if you change the line framing on a virtual trunk, all virtual trunks on the port are automatically updated to have the modified line framing.

You can use **cnftrk** to configure the Transmit Trunk Rate for all BPX cards, except for the BXM card. For BXM cards, you must use the **cnfrsrc** command to configure the Transmit Trunk Rate (trunk load). For IGX cards, you can configure the Transmit Trunk Rate after a trunk has been added.

You can use the **cnftrk** command to assign a VPI value. You will not be able to configure the VPI value if the virtual trunk is already configured for VSI. Also note that if the VSI feature is enabled, and you execute **cnftrk** to decrease the transmit rate, you must confirm whether the qbin configuration is set up correctly by using the **cnfqbin** command to change the value. The reason for this is that when the transmit rate is decreased, the qbin depth will be automatically recalculated.

In this release, **cnftrk** supports the rt-VBR and nrt-VBR traffic classes (instead of just the VBR traffic class). Similarly, the virtual trunk type can be rt-VBR or nrt-VBR.

You can configure the ILMI protocol running on a trunk interface to run on the BCC instead of the BXM.

Subrate and Fractional Trunks

For FastPacket trunks, which the NTC and NTM front cards support, you can configure the Subrate interface and Subrate data rate fields only if the back card is a BC–SR. The interface types for a subrate trunk are V.11, X.21, V.35, and EIA/TIA-449. Set the data rate to match the subrate facility within the range 64 Kbps–1.920 Mbps.

The DS-0 map is used to define fractional E1 and T1 trunks. It consists of a repeating set of specifications in the form <x[-y[a]]>, where "x" and the optional "y" are DS-0 numbers 0–23, and the optional "a" indicates *alternating*. The value of "y" must be greater than the value of "x." The values of both "x" and "y" cannot be less than 0 or greater than the maximum number of DS-0s for the line type. In the DS-0 map for unframed E1, use 0–31. For framed E1, use 1–31. For 30 DS-0 E1, use 1–15, 17–31.

Receive and Transmit Rates on Physical Trunks

The parameters RCV Trunk Rate and Transmit Trunk Rate apply to physical ATM trunks on an IGX node. On a BPX node, only Transmit Trunk Rate is available. These parameters let you configure lower rates than the maximum line rate for the trunk type. If you adjust a rate, you need to do this at both ends of the trunk. For example, if RCV Trunk Rate on an IGX is 40,000 packets per second (pps), Transmit Trunk Rate on the far end must be 20,000 cells per second (cps). The typical relationship between pps and cps is two FastPackets for each cell.

For ATM trunks terminating on a BTM (IGX), make sure the receive rate is below the maximum of the T3 or E3 line rate. For these cards, the rate should be no more than 40,000 packets per second. Increments for RCV Trunk Rate and Transmit Trunk Rate can be as small as 1 cell or packet per second. (Note that the node may round up or round down the value you enter.)

The default value for Transmit Trunk Rate is the maximum rate for the back card type. You can reduce this rate to any number of cells per second that is less than or equal to the physical port rate. If E3 or T2 is selected, the bandwidth is reduced from the T3 rate.

Note You can configure the Transmit Trunk Rate parameter, which indicates the trunk load, by using the **cnfrsrc** command on BXM cards. On both IGX and BPX nodes, the trunk load displays in cps (cells per second), and the value is displayed in brackets on the first line of the **cnftrk** display.

On the **cnftrk** screen, the Transmit Rate and Transmit Load are always displayed in cps (cells per second). (The Transmit Load displays in brackets above the Transmit Rate field, for example, TRK 13.1.1 Config T3 [2867 cps].) Because switch software performs an internal conversion from DS0s to cells for the receive rate, this receive rate dictates the transmit load at the other end of the trunk, and vice versa. Because the Transmit Load (in cps) may not fit into the full DS0, the resulting number that appears in the Transmit Load field (for example, [2867 cps], could be truncated. For example, if you were to change the Transmit Rate on a routing trunk from 96000 to 104268, **cnftrk** will prompt you to enter a Transmit Rate of 0-104268, and will accept 104268, but it may assign a value of 104150 instead of 104268. The Transmit Load would be the same, for example, 104150 cps, regardless of whether the user configured the Transmit Rate as 104268 or 104269 or 104270.

The following shows how the transmit rate is calculated internally by switch software:

1 DS0 = 64000 bits/sec
or
DS0 = 8 bits x 8000 samples/sec = 64000 bits/sec

1 cell long unit = 424 bits/sec
therefore:
Number of cells per second (cps) = ds0 * 8000 / 53 bytes per ATM cell

Following is some further explanation of how the Transmit Trunk Rate is calculated internally by switch software:

For any user-provided Transmit Trunk Rate value in T1 cells per second (cps).

Rcv Trunk Rate = T1 x 53 /8000 (in DS0)

(This is the actual value used for everything and dictates the Transmit Trunk Load value at the other end of the trunk.)

The conversion occurs again at the other end:

T2 = R1 * 8000 / 53 (in cps)

The Transmit Load number displayed in brackets is the same, that is, 104150 cells per second, whether the user has given the Transmit Rate as 104268 or 104269 or 104270.

Receive and Transmit Rates on Virtual Trunks

The implementation of XMT Trunk Rate on a virtual trunk differs from the implementation on a physical trunk. On a physical trunk, XMT Trunk Rate limits the rate at which the back card physically generates cells. For a virtual trunk, XMT Trunk Rate does not limit the rate at which the back card generates cells: the line rate stays at the maximum for the line type. However, XMT Trunk Rate is the maximum transmission rate allowed on a virtual trunk.

The provider of the virtual trunk service assigns the value for XMT Trunk Rate. You must have this provider-assigned value for XMT Trunk Rate and enter it when you use **cnftrk**.

The total bandwidth of all the virtual trunks in one port cannot exceed the maximum bandwidth of the port. The trunk loading (load units) is maintained per virtual trunk., but the cumulative loading of all virtual trunks on a port is restricted by the transmit and receive rates for the port.

Physical and Virtual Trunk Configuration

Physical and virtual trunk configuration is similar. When you configure a port-level characteristic of a virtual trunk, all the virtual trunks on the port are modified with that characteristic. When the port characteristics of a trunk are modified, all characteristics related to that trunk port are updated.

Virtual trunks appear in the routing topology map as available trunks for routing. The existing physical trunk characteristics, such as bandwidth and satellite/terrestrial type, apply to virtual trunks. The routing algorithm must take into account special restrictions and conid assignments for a virtual trunk. For example, VPCs cannot be routed over a virtual trunk. Also, each virtual trunk has a configurable number of connection channels reserved from the card. The routing algorithm checks for adequate channel availability on a virtual trunk before selecting the trunk for the route.

The connection channel management scheme for the UXM and BXM cards is the same as in the previous release. The conids are selected on a per logical trunk basis. The associated LCNs are selected from a pool of LCNs for the entire card. Each virtual trunk can use the full range of acceptable conid values. The range consists of all the 16-bit values (1-65535), excluding the node numbers and blind addresses. A port uses the VPI to differentiate connections that have the same conid.

The number of channels per virtual trunk can be changed after the trunk has been added to the network. Decreasing the number of channels on an added virtual trunk causes connection reroutes where increasing the number of channels on an added virtual trunk will not cause connection reroutes.

Configuring an IMA Compliant Trunk

The **cnftrk** command has a parameter that lets you add or delete physical lines of an existing IMA group (IMA Group member parameter). You will be prompted to enter the physical lines using the same format as described in the "Configuring IMA Physical Lines" section on page 4-189. When you add or delete a physical link, the following are enforced:

- You cannot delete primary links.
- The total number of physical links in the group must be greater than or equal to the number of retained links. You will be prompted to decrease the number of retained links, if necessary.
- The bandwidth of the deleted physical link will be subtracted from the trunk's Trunk Transmit Rate only. The trunk's Trunk Receive Rate is unaffected. If the Trunk Receive Rate needs to be dropped down, you will be prompted to do this first in a separate operation. You will be warned that connection reroutes may occur.

Note that the above functional characteristics only apply to the UXM Firmware Model M, which supports the ATM Forum IMA Compliant protocol. If a card has UXM Firmware Model A, which supports the Cisco Proprietary protocol, the IMA trunk functions as it did in Release 9.1. For example, you will not be able to add or delete physical links of an existing IMA group.

Primary Link—In an IMA group, you must select one of the physical links to be a primary link. This primary link number is used to refer to this IMA group or trunk. You can use **cnftrk** to add additional links to the group or delete existing links.

When deleting existing links from an IMA group, you cannot delete the primary link. You must first deactivate the trunk using **deltrk**, then use **dntrk** to remove the primary link.

Refer to 9.2 release notes for up-to-date feature support and system requirements.

Specifying a Set of Physical Lines (Comprising an IMA Group)

In Release 9.1, it was a requirement that the IMA group had to consist of consecutive physical lines. In this release, you can define an IMA trunk consisting of non-consecutive physical lines. In addition, you can change the group member by deleting a physical line from an existing IMA trunk.

Use the following syntax to specify an IMA group on a UXM trunk:

- **uptrk** *slot.group_member.vtrk*

  where:

  slot is the slot number

  group_member is a set of physical lines composing an IMA group. You can specify the member in an expression consisting of the primary link followed by a , or – and additional physical links.

  vtrk is the optional virtual trunk number. If at least one virtual trunk already exists on this port, the you only have to specify the primary link as the group_member.

  For example, 9.1–4 defines trunk 9.1 to consist of four physical links, that is, 1, 2, 3 and 4, where physical link 1 is the primary link. (This example is compatible with Release 9.1.)

For example, 9.1–3,5 defines trunk 9.1 to consist of four physical links, that is, 1, 2, 3 and 5 where physical link 1 is the primary link.

For example, 9.5–7,2–3 defines trunk 9.5 to consist of five physical links, that is, 2, 3, 5, 6 and 7 where physical link 5 is the primary link.

9.8,2,4,6 defines trunk 9.8 to consist of all even number of physical links where physical link 8 is the primary link.

Physical and Virtual Trunk Parameters You Can Configure with cnftrk

Table 4-41 below shows the trunk parameters that you can configure with cnftrk. You can specify all physical options on virtual trunks. If you change a physical option on a virtual trunk, the change is propagated to all virtual trunks on the trunk port. An X indicates that the parameter is configurable. An X* in the Virtual column indicates that the parameter is a physical parameter, and changing the value for one virtual trunk on the port will automatically cause all virtual trunks on the port to be updated with the same value.

Table 4-41 cnftrk Parameters that are Configurable on Physical and Virtual Trunks

	BXM		UXM	
Descriptions	**Physical**	**Virtual**	**Physical**	**Virtual**
Transmit Trunk Rate (configurable using **cnfrsrc**)	X	X	X	X
Receive Trunk Rate	X	X	X	X
Pass Sync	X	X*	X	X*
Loop Clock	X	X*	X	X*
Statistical Reserve	X	X	X	X
Header Type NNI	X	X*	X	X*
Trunk VPI		X	X	X
Routing Cost	X	X	X	X
Virtual Trunk Type		X		X
Idle Code	X	X*	X	X*
Restrict PCC traffic	X	X	X	X
Link Type	X	X*	X	X*
Line Framing	X	X*	X	X*
Line Coding			X	X*
Line Cable type			X	X*
Line cable length	X	X*	X	X*
HCS Masking	X	X*	X	X*
Payload Scramble	X	X*	X	X*
Connection Channels	X	X	X	X
Gateway Channels			X	X
Valid Traffic classes	X	X	X	X
Frame Scramble	X	X*	X	X*
Deroute Delay Time	X	X	X	X

Table 4-41 cnftrk Parameters that are Configurable on Physical and Virtual Trunks

	BXM		UXM	
Descriptions	**Physical**	**Virtual**	**Physical**	**Virtual**
VC (Traffic) Shaping	X	X	X	X
Protocol by the Card	X	X	X	X
IMA Differential Delay			X	X
IMA Clock Mode			X	X
IMA Group member			X	X
Retained links			X	X

Virtual Trunk Traffic Classes

All types of Cisco traffic are supported through an ATM cloud. Every trunk is defaulted to carry every type of traffic. The CBR, VBR (rt-VBR and nrt-VBR), and ABR virtual trunks within the cloud should be configured to carry the correct type of traffic. The CBR trunk is suited to carry all types of traffic. The VBR trunk is best suited to carry IGX Frame Relay and BPX VBR traffic, as well as Optimized Bandwidth Management (formerly called ForeSight) and ABR traffic. The ABR trunk is best suited to carry Optimized Bandwidth Management and ABR traffic. You can change the type of traffic each trunk carries. However, to avoid unpredictable results, it is best to stick to the recommended traffic types for a given VPC type.

Two-stage queueing at the egress of virtual trunks allows shaping of traffic before it enters the cloud. However, the traffic is still routed on a single VPC and may be affected by the traffic class of the VPC selected.

You can configure any number of virtual trunks between two ports up the maximum number of virtual trunks per slot and the maximum number of logical trunks per node. These trunks can be any number of three trunk types.

The unique characteristics of CBR, VBR (rt-VBR and nrt-VBR), and ABR traffic are maintained through the cloud as long as the correct type of virtual trunk is used. The traffic classes allowed per virtual trunk are configured with cnftrk. The routing algorithm excludes virtual trunks whose traffic class is not compatible with the candidate connection to be routed.

Adding a Single Virtual Trunk

The following example describes a typical scenario of adding one virtual trunk across an ATM network. One one side of the cloud is a BPX with a BXM trunk in slot 4. On the other side of the cloud is an IGX with a UXM trunk card in slot 10. A virtual trunk is added between port 3 on the BXM and port 2 of the UXM.

Note You must configure a VPC within the cloud first.

1. On BPX_A, up virtual trunk #1 on BXM trunk port 4.3.1.

   uptrk 4.3.1

2. On BPX_A, configure the VPI, VPC type, traffic classes, number of connection channels, and header type.

   cnftrk 4.3.1

3 On IGX_A, up the virtual trunk #1 on the UXM trunk port 10.

uptrk 10.2.1

4 On IGX_A, configure the VPI, VPC type, traffic classes, number of connection channels, and header type.

cnftrk 10.2.1

5 On BPX_A, add a virtual trunk between the two nodes. (Executing addtrk 10.2.1 at IGX_A would also add a virtual trunk between the two nodes.)

addtrk 4.3.1

The VPI values you chose during **cnftrk** must match those used by the cloud VPC. Also, both ends of the virtual trunk must match on Transmit Rate, VPC type, traffic classes supported, and number of connection channels supported. The **addtrk** command checks for matching values before allowing the trunk to be added to the network topology.

The network topology from BPX_A's perspective after you add the trunk be:

BPX_A 4.3.1-10.2.1/IGX_A

Adding a Single Virtual Trunk on Top of IMA Ports for IGX

The following example describes a typical scenario of adding one virtual trunk across an ATM network. One one side of the cloud is a BPX with a BXM trunk in slot 4. On the other side of the cloud is an IGX with a UXM trunk card in slot 10. A virtual trunk is added between port 3 on the BXM and port 2 of the UXM. This example shows how virtual trunk is added on top of IMA ports on the IGX platform.

Once you up a virtual trunk, and the IMA port has been allocated during the **uptrk** command, then you up additional virtual trunks using ONLY the primary IMA port, for example, 10.2.2, 10.2.3, and so on.

Note You must configure a VPC within the cloud first.

---

1 On BPX_A, up virtual trunk #1 on BXM trunk port 4.3.1.

uptrk 4.3.1

2 On BPX_A, configure the VPI, VPC type, traffic classes, number of connection channels, and header type.

cnftrk 4.3.1

3 On IGX_A, up the virtual trunk #1 on the UXM trunk port 10.

uptrk 10.2.1

4 On IGX_A, configure the VPI, VPC type, traffic classes, number of connection channels, and header type.

cnftrk 10.2.1

5 On BPX_A, add a virtual trunk between the two nodes. (Executing addtrk 10.2.1 at IGX_A would also add a virtual trunk between the two nodes.)

addtrk 4.3.1

This release supports virtual trunking on both the BPX and IGX. IMA trunk ports are referenced by the first physical line of the trunk port after **uptrk** has been executed. For example, you can *uptrk 1.5–8.9*. You can then up a second trunk (which, in this case, is a virtual trunk on slot.port 1.5) on the same trunk port using *uptrk 1.5.11*.

Full Name

Configure trunk

Syntax

cnftrk <*slot.port*>[*.vtrk*] <options for E1 | T1 | E3 | T3 | OC-3 | OC-12 | E2 | HSSI | SR >

Related Commands

addtrk, dsptrkcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

`cnftrk 11`

Description

Configure trunk 11. The trunk in slot 11 is an ATM T3 trunk on an ALM/B. (If you want to verify the card is the trunk version of the ALM, use either **dspcd** or **dspcds** and check the front card “Rev.” The Rev column contains a B for the first character for an ALM/B.)

System Response

```
IGX8420          TN    SuperUser       IGX 8420    9.2   Sep. 5 1998 16:38 PST

PLN 11 Config         T3/576 [192000pps]    ALM slot: 11
Clock Rate:           --                    Idle code:            7F hex
Transmit Trunk Rate: 96000 cps             Restrict PCC traffic: No
Rcv Trunk Rate:       192000 pps            Link type:            Terrestrial
Subrate interface:    --                    Line framing:         --
Subrate data rate:    --                         coding:          --
Line DS-0 map:        --                         CRC:             --
Pass sync:            Yes                        recv impedance: --
Loop clock:           No                         cable type:
Statistical Reserve: 992   pps                        length:    0-225 ft.
Header Type:          STI                   HCS Masking:          Yes
Gateway Type:         BAM                   Payload Scramble:     No
VPI Address:          0                     End supp BData:       Yes
VCI Address:          0                     End supp FST:         Yes
                                            Deroute delay time: 0 seconds


Last Command: cnftrk 11


Next Command:
```

Example 2

cnftrk 1.1

Description

Configure trunk 1.1. This trunk is an ATM T3 trunk on a BPX node.

System Response

```
batman         TN    SuperUser       BPX 8620    9.1       Date/Time Not Set

TRK 1.1 Config        T3    [96000 cps]   BNI-T3 slot: 1
                                           Restrict CC traffic:   No
Transmit Rate:         96000               Link type:             Terrestrial
Subrate interface:     --                  Line framing:          --
Subrate data rate:     --                      coding:            --
Line DS-0 map:         --                      CRC:               --
Pass sync:             Yes                     recv impedance:    --
Loop clock:            No                      cable type:
Statistical Reserve:   992   cps                     length:      0-225 ft.
Idle code:             7F hex              HCS Masking:           Yes
Connection Channels:   1771                Payload Scramble:      No
Valid Traffic Classes:                     Frame Scramble:        --
 V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR   Cell Header Type:      --
                                           Virtual Trunk Type:    --
SVC Channels:          0                    Virtual Trunk VPI:     --
SVC Bandwidth:         0     cps            Virtual Trunk Service: --

This Command: cnftrk 1.1


Transmit Rate [T2=14490, E3=80000, T3=96000, OC-3 = 353208](96000):
```

Example 3

cnftrk 13.1.1

Description

Configure trunk 13.1.1 (a virtual trunk on an ATM T3).

System Response

```
sw97           TN    SuperUser       BPX 8620    9.2       July 30 1998 11:45 GMT

TRK 13.1.1 Config T3        [2867 cps]   BNI-T3 slot: 13
                                           Restrict CC traffic:   No
Transmit Rate:         3000                Link type:             Terrestrial
Subrate interface:     --                  Line framing:          --
Subrate data rate:     --                       coding:           --
Line DS-0 map:         --                       CRC:              --
Pass sync:             No                       recv impedance:   --
Loop clock:            No                       cable type:
Statistical Reserve:   992   cps                      length:     0-225 ft.
Idle code:             7F hex              HCS Masking:           Yes
Connection Channels:   55                  Payload Scramble:      No
Valid Traffic Classes:                     Frame Scramble:        --
   V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR Virtual Trunk Type:    CBR
                                           Virtual Trunk VPI:     0
                                           Virtual Trunk Service: 4

Last Command: cnftrk 13.1.1 3000 N N 992 7F 55 V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR N
TERRESTRIAL 0 Y N CBR 0

Next Command:
```

Example 4

cnftrk 6.3

Description

Configure trunk 6.3 (an OC-3 trunk on a UXM).

System Response

```
sw228          TN    SuperUser       IGX 8420    9.2.0r    Aug. 27 1998 17:42 PST

TRK 6.3 Config       OC-3     [353056cps] UXM slot: 6
Transmit Trunk Rate: 353207 cps          Frame Scramble:       Yes
Rcv Trunk Rate:       353207 cps          Cell Framing:         STS-3C
Pass sync:            Yes
Loop clock:           No
Statistical Reserve: 1000   cps
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
Routing cost:         10
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels: 256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR

Last Command: cnftrk 6.3


Next Command:
```

Example 5

cnftrk 8.1

Description

Configure trunk 8.1 (a T3 trunk on a UXM).

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1997 17:42 PST

TRK 8.1 Config       T3      [96000cps] UXM slot: 8
Transmit Trunk Rate: 96000 cps
Rcv Trunk Rate:       96000 cps           Line Framing:         PLCP
Pass sync:            Yes                 Cable Length          0-255 ft.
Loop clock:           No
Statistical Reserve: 1000   cps
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
Routing cost:         10
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels: 256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR

Last Command: cnftrk 8.1


Next Command:
```

Example 6

`cnftrk 10.1`

Description

Configure trunk 10.1 (an E3 trunk on a UXM).

System Response

```
sw228          TN    SuperUser       IGX 8420    9.2    Aug. 27 1998 17:42 PST

TRK 10.1 Config       E3      [80000cps] UXM slot: 10
Transmit Trunk Rate: 80000 cps
Rcv Trunk Rate:       80000 cps           Line Framing:         HEC
Pass sync:            Yes                 Cable Length          0-255 ft.
Loop clock:           No
Statistical Reserve: 1000   cps
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
Routing cost:         10
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels: 256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR

Last Command: cnftrk 10.1


Next Command:
```

Example 7

`cnftrk 5.2`

Description

Configure an IMA trunk 5.2 (an E1 trunk on a UXM) which consists of non-consecutive physical lines 1, 3, 5, and 7.

System Response

```
sw224          TN    SuperUser       IGX 8420    9.2    Aug. 27 1998   17:50 GMT

TRK 5.2-8 Config     E1/203 [30641 cps] UXM slot: 5
Line DS-0 map:        1-15,17-31
Retained links:       7
IMA Group member:     1,3,5,7             Valid Traffic Classes:
Transmit Trunk Rate: 30641 cps             V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR
Rcv Trunk Rate:       28075 cps          IMA Protocol Option: Disabled
Pass sync:            Yes                 IMA Max. Diff. Dly:   200 msec
Loop clock:           No                  IMA Clock Mode:       CTC
Statistical Reserve: 600    cps          Deroute delay time:   0 seconds
Idle code:            54 hex
Restrict PCC traffic: No
Link type:            Terrestrial
Routing cost:         10
Line coding:          HDB3
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels: 256
Gateway Channels:     256

This Command: cnftrk 5.2
```

Note The ATM Forum–compliant ATM Inverse Multiplexing standard does not support the IMA link auto disable option. Previous to Release 9.2, the IMA link auto disable parameter displayed for IMA links, but it does not display in Release 9.2.

The IMA group member and IMA Differential delay parameters are configurable. The IMA Clock Mode parameter is fixed at CTC and is not configurable.

Also, note that you can configure IMA trunk parameters on virtual trunks that are on top of IMA ports.

Example 8

cnftrk 10.1

Description

Configure trunk 10.1 (a T1 trunk on a UXM).

System Response

```
sb-reef        TN    SuperUser       IGX 8420    9.2    Aug. 27 1998   17:46 PDT

TRK 10.1-5 Config     T1/115 [17358 cps] UXM slot: 10
IMA group member      1,3,5,7
Transmit Trunk Rate: 17358 cps          Connection Channels: 256
Rcv Trunk Rate:       17358 cps          Gateway Channels:     256
Pass sync:            Yes                 Valid Traffic Classes:
Loop clock:           No                     V,TS,NTS,FR,FST,CBR,rt-VBR,nrt-VBR,ABR
Statistical Reserve: 600    cps          Retained links:       5
Idle code:            7F hex              IMA Protocol Option: Disabled
Restrict PCC traffic: No                  IMA Max. Diff. Dly:   200 msec.
Link type:            Terrestrial         IMA Clock Mode:       CTC
Line framing:         ESF
Line coding:          B8ZS
Line cable type:      ABAM
Line cable length:    0-131 ft.
HCS Masking:          Yes
Payload Scramble:     No

Last Command: cnftrk 10.1
```

Note The ATM Forum–compliant ATM Inverse Multiplexing standard does not support the IMA link auto disable option. Previous to Release 9.2, the IMA link auto disable parameter displayed for IMA links, but it does not display in this release.

If the IMA link auto disable option is disabled, the Window size, Max transition counts, and Link reenable time parameters will not display. In this release, because the ATM Forum-compliant ATM Inverse Multiplexing standard does not support the IMA link auto disable option, these parameters do not display.

Refer to Table 4-42 and Table 4-43 for a list of cnftrk parameters, and cnftrk optional parameters.

Table 4-42 cnftrk—Parameters

Trunk Option	Type	Description	Possible Entries	Default
slot.port	All	The number of the trunk to configure.	Any valid slot and port. For cards with one port, use slot.	N/A
Trunk Identification (display only—not configurable)	All	Displays trunk number, trunk type and bandwidth supplied; and the card type and slot number of the unit supporting the trunk.	T3, E3, T1, E1, E2, fractional T1, fractional E1 subrate, ATM, NTC, NTM, OC-3, STM1, OC-12, STM4.	none
Clock Rate	ATM	This clock rate is for only HSSI.	4 Mbps–50.84Mbps	
Transmit Trunk Rate (display only—not configurable)	ATM	This indicates the trunk load, and is configurable by using **cnfrsrc** command for BXM cards (BPX platform). This parameter appears on the **cnftrk** screen for display purposes only. On IGX, Transmit Trunk Rate is configurable after a trunk has been added. **Note** The trunk load, which displays in brackets at the end of the first line on the **cnftrk** display, may vary from the Transmit Trunk Rate value. This is due to the way that cells are converted to DS0s, and vice versa, and the way the Rcv Trunk Rate determines the Transmit load at the other end of the trunk. The Transmit Trunk Rate in cells per second (cps) may not fit in the full DS0 thus the resulting value may be truncated. The result is that the values displayed in Trunk load field and Transmit Trunk Rate fields may display different values.		
Rcv TRK Rate	ATM	CELLBUS or MUXBUS bandwidth in packets per second (pps) to allocate to a BTM, ALM/B. On a BPX, Rcv TRK Rate is not used. On IGX, Rcv Trunk Rate is configurable after a trunk has been added.	ALM/B T3: 1K–192K pps BTM (IGX): 0–80K pps BTM-E1: 0–10538 pps for CGW, unframed E1 or 0–10208 pps for CGW, for framed E1	1000 pps
Subrate interface	PKT	Subrate physical interface type	X.21 | V.35	X.21
Subrate data rate	PKT	Subrate data rate in Kbps. Allows you to specify, in Kpbs, the clock rate for the selected subrate interface. Acceptable values are any multiple of 64 Kpbs up to a maximum of 1920 Kbps.	64 Kbps, 128 Kbps, 256 Kbps, 384 Kbps, 1.024Mbps, 1.536 Mbps, and 1.920Mbps	1920 Kbps
DS0 map	PKT	Specifies the DS0s to use for a fractional T1 or E1 bundle. Optional “a” = “use alternating channels” (for example, 20–30a means 20, 22, 24, and so on.)	x - y[a]	0-31 (E1) 0-23 (T1)

Table 4-42 cnftrk—Parameters (Continued)

Trunk Option	Type	Description	Possible Entries	Default
Pass sync	All	Enables the trunk to pass a clock for network synchronization.	Yes | No	Yes for standard, no for virtual trunks
Loop Clock	All	Loop receive clock back to transmit.	Yes | No	No
Statistical Reserve	All	This trunk bandwidth is reserved for non-standard traffic, such as internode controller messages or user traffic diverted because of a failure.	0–10666	600 for FastPackets 1000 for ATM cells (992 cells on BNI)
Header Type	ATM	Selects the ATM cell header type: UNI, NNI, or STI. UNI is the default for virtual trunks but you may need to configure this parameter to NNI to match the header type of the VPC provided by the ATM cloud. In this release, this parameter is configurable for physical and virtual trunks. See the *Cisco WAN Switching System Overview* for a description.	UNI | NNI | STI .	STI
Gateway Type	ATM	Defines the type of addressing mode for this trunk. See *Cisco WAN Switching System Overview* for a description.	BPX-BPX (BAM) Cloud (CAM) Simple (SAM)	BAM
VPI Address	ATM	Virtual path address in ATM cell. The VPI configured for a virtual trunk must match the VPI for the VPC in the cloud. Valid VPC VPIs depend on the port type. Must be non-0 for a virtual trunk.	BXM/UXM (UNI)—1-255 BXM/UXM (NNI)—1-4095 BNI T3/E3—1-255 BNI OC-3 —1-63	0
VCI Address	ATM	Virtual circuit address in ATM cell.	0–65,535	0
Idle code	All	HEX code either in the payload space of an ATM *idle cell* or on an *idle FastPacket trunk* (idle *packets* do not exist)	0–FF (hex)	54 (E1) 7F (T1, ATM)
SVC Channels	ATM	The number of channels reserved for SVCs.	T3: 0–1771 E3: 0–1771 OC-3: 0–16199	0
SVC Bandwidth	ATM	The bandwidth reserved for SVCs.	T3: 96000 cps E3: 80000 cps OC-3: 353208 cps	0
Restrict CC traffic (requires superuser privilege)	All	Restrict node controller messages from a trunk. Restricting CC traffic can cause serious problems. Contact the TAC through Cisco Customer Engineering before you change it.	Y | N	No

Table 4-42 cnftrk—Parameters (Continued)

Trunk Option	Type	Description	Possible Entries	Default
Link type	All	Terrestrial or Satellite link.Link Type applies to configuring a route so it can “avoid satellite.”	T | S	T
Routing Cost	ATM	The administrative cost of a trunk for when cost-based routing is configured.	1–50	10 (upon trunk activatio n)
Line framing	PKT	T1 line framing	D4 | ESF	D4
Line coding	PKT	E1 line coding T1 line coding	HDB3 | AMI ZCS | B8ZS | AMI	HDB3 ZCS
Line CRC	PKT	E1 CRC-4	Yes | No	No
Recv impedance	PKT	E1 receive impedance	1 = 75W unbalanced 2 = 75W balanced 3 = 120W balanced	1
Cable type and cable length	PKT ATM	Length and type of cable used for trunk. Designates the software configurable line build-out to match the cable length from the IGX node to the DSX cross-connect. For BPX, the choices are 0–225 feet and over 225 feet. Cable type is not selectable for BPX. Not applicable to MMF or SMF	1 = 0–220' MAT 2 = 220–440' MAT 3 = 440–655' MAT 4 = 0 -133' ABAM 5 = 133–266' ABAM 6 = 266–399' ABAM 7 = 399–533' ABAM 8 = 533–655' ABAM 0= 0–225 1= greater than 255	4 0
HCS Masking	ATM	Mask the ATM cell header checksum to disable error checking. HCS Masking applies to E3, OC-3, and OC-12 only.	Yes | No	Yes
Payload Scramble	ATM BNI	Scramble the cell payload.	Yes | No	Yes for BNI-E3 No for all others
End supp BData	PKT ATM	Indicates whether the far end of a trunk supports bursty, Frame Relay data.	Yes | No	No
End supp FST	PKT ATM	Indicates whether the far end of the trunk supports Optimized Bandwidth Management for Frame Relay.	Yes | No	No
Gateway Efficiency	ATM	How many packets to stuff into an ATM cell. Does not apply to BNI.	1 | 2 | 3	2

Table 4-42 cnftrk—Parameters (Continued)

Trunk Option	Type	Description	Possible Entries	Default
IMA Differential Delay		The possible value ranges between 0 to 200 milliseconds. Differential delay of 200 msec is the default. Because all physical links share the same line configuration, any changes made to this parameter and IMA Clock Mode parameter will be applied to all physical links of the specified IMA group. This parameter is configurable on virtual trunks that are on top of IMA ports.	0-200 msec	0-200 msec
IMA Clock Mode		Two clock mode options are available: Common Transmit Clock Source (CTC mode), and Independent Transmit Clock Source (ITC mode). CTC mode is the default. This parameter is configurable on virtual trunks that are on top of IMA ports.		CTC mode
IMA Group member		Lets you add or delete physical lines of an existing IMA group. You are prompted to enter the physical lines using the following format, for example: IMA Group member: 1,3,5,7 or IMA Group member: where 1,3,5,7 are physical lines that comprise the IMA group. You can configure this parameter on virtual trunks that are on top of IMA ports. *IMA Group member* is a set of physical lines comprising an IMA group. You can specify the group member as an expression consisting of the primary link followed by a "," (comma), or a hyphen (-), and additional physical links. You then use the following syntax to up a trunk when you specify an IMA group on a UXM trunk: **uptrk** slot.group_member.vtrk	primary link (slot.port	No default
Retained links		Total number of physical links in the group must be greater than or equal to the number of retained links.		
IMA Protocol Option		Lets you enable/disable the IMA Protocol on trunks that have only *one* physical line.	Enabled/Disabled	Default: IMA protocol disabled on these types of trunks

Table 4-42 cnftrk—Parameters (Continued)

Trunk Option	Type	Description	Possible Entries	Default
Deroute Delay Time	All	Indicates how long in seconds the network will wait before rerouting connections on a failed trunk. This helps when statistical errors are occurring or when a trunk momentarily moves into a failure state then returns to normal operation. This feature is relevant when rerouting the connections is more of a disruption than the errors caused by the intermittent trunk. Causes each node not to recognize the trunk as failed until this timer expires at the nodes used by the trunk. This indirectly affects the time that Abit notifications are sent out because the connection deroute is also delayed. Regarding the Abit Notifications feature in Release 9.1.07, this parameter specifies the maximum number of connections that can be derouted at the same time when the connection management (CM) state machine runs.	0-600	0

Table 4-43 cnftrk—Optional Parameters

Virtual Trunk Parameter	Type	Description	Possible Entries	Default
Connection Channels	BNI	The maximum number of connection channels per trunk. All virtual trunks on the port share this total. The number of connections added to the port cannot exceed the number of connection channels configured for the port. Number of connection channels, or LCNs, on the trunk port that are usable by the virtual trunk. This number cannot be greater than the total number of connection channels on the card. The maximum number of channels is additionally limited by the number of VCI bits in the UNI cell header. For a virtual trunk, divide this number by the maximum number of virtual trunks on the port to get the default.	BNI-T3/E3: max 1771 BNI-OC-3: max 15867 (3837 maximum/virtual trunk) BXM/UXM: 1–*number of channels allowable on card*)	BNI-T3/E3: 1771 BNI-OC-3: 15867 For Virtual Trunks: BNI-T3/E3: 55 BNI-OC-3: 1442

Table 4-43 cnftrk—Optional Parameters (Continued)

Virtual Trunk Parameter	Type	Description	Possible Entries	Default
Valid Traffic Classes	BNI, BXM	The valid types of traffic for a virtual trunk. The recommended traffic classes for each virtual trunk type: On a CBR trunk: ATM CBR, NTS, TS, voice. All traffic classes are recommended on a CBR trunk. On a VBR trunk: ATM VBR, bursty data A, bursty data, bursty data B (Optimized Bandwidth Management), ABR On an ABR trunk: ATM ABR and bursty data B (Optimized Bandwidth Management).	V—voice TS—timestamped NTS—non-timestamped FR—Frame Relay FST—Optimized Bandwidth Management (formerly Foresight) CBR—constant bit rate VBR—variable bit rate ABR—available bit rate	
Virtual Trunk Type	BNI	This choice usually comes from the carrier that provides the ATM cloud. This is the VPC type provided by the ATM cloud.	CBR, VBR, ABR	CBR
Virtual Trunk VPI	BNI	Virtual trunks must be configured to have a greater-than-0 VPI before connections are added by **addcon**. This value usually comes from the carrier that provides the ATM cloud. VPI configured for a virtual trunk matches VPI for VPC in the ATM cloud. Every cell transmitted to this trunk has this VPI value. Valid VPC VPIs depend on the port type.	1–255 for BXM/UXM (UNI) 1–4095 for BXM/UXM (NNI) 1–255 for BNI T3/E3 1–63 for BNI OC-3 (STM1)	

cnftrkalm

Use cnftrkalm to configure whether or not alarms on a trunk cause system alarms and reporting (on IGX only). When a trunk is upped and added to the network, alarm reporting is enabled, but **cnftrkalm** lets you disable alarms on upped trunks. Disabling alarms can be useful when a trunk is connected to a node but not yet in service or when a trunk has occasional bursts of errors but still functions.

A virtual trunk also has trunk port alarms that are shared with all the other virtual trunks on the port. These alarms are cleared and set together for all the virtual trunks sharing the same port.

Statistical alarming is provided on cell drops from each of the Advanced CoS Management queues. These alarms are maintained separately for virtual trunks on the same port.

On an IGX node, enabled alarms cause an output from the ARC or ARM card or an indication to Cisco WAN Manager.

Table 4-44 below shows a table of physical and logical trunk alarms, with the alarm type, the physical interface type, and whether the alarm is a logical, statistical, or integrated alarm.

Table 4-44 Physical and Logical Trunk Alarms Supported on IGX and BPX

	Physical							
Alarm Type	**T1**	**E1**	**T3**	**E3**	**SONET**	**Logical**	**Statistical**	**Integrated**
LOS	X	X	X	X	X		X	X
OOF	X	X	X	X	X		X	X
AIS	X	X	X	X	X		X	X
YEL	X	X	X	X	X			X
PLCP OOF			X					X
LOC				X	X			X
LOP					X			X
PATH AIS					X			X
PATH YEL					X			X
PATH TRC					X			X
SEC TRC					X			X
ROOF	X	X						X
FER	X	X						X
AIS16	X	X					X	X
IMA	X	X						X
NTS Cells Dropped						X	X	
TS Cells Dropped						X	X	
Voice Cells Dropped						X	X	
Bdata Cells Dropped						X	X	
BdatB Cells Dropped						X	X	

Table 4-44 Physical and Logical Trunk Alarms Supported on IGX and BPX (Continued)

	Physical							
Alarm Type	T1	E1	T3	E3	SONET	Logical	Statistical	Integrated
HP Cells Dropped						X	X	
CBR Cells dropped						X	X	
VBR Cells dropped						X	X	
ABR Cells dropped						X	X	

Trunk Alarms

Logical trunk alarms, physical trunk alarms, and IMA physical line alarms are briefly described below.

Logical Trunk Alarms

Statistical alarming is provided on cell drops from each of the Advanced CoS Management queues. These alarms are maintained separately for virtual trunks on the same port.

Physical Trunk Alarms

A virtual trunk also has trunk port alarms which are shared with all the other virtual trunks on the port. These alarms are cleared and set together for all the virtual trunks sharing the same port.

IMA Physical Line Alarms

IMA physical line alarms are a special case. Each IMA trunk port has a configurable number of retained links. If the number of non-alarmed lines is less than the number of retained links, the logical trunks on the IMA trunk port are placed into major alarm.

For example, suppose there are IMA virtual trunks 4.5-8.2 and 4.5-8.7. Further, the number of retained links on 4.5-8 has been configured to 2. If 4.5 and 4.6 go into LOS, physical line alarms are generated for these 2 physical lines. The logical trunks 4.5-8.2 and 4.5-8.7 do not go into alarm because the two retained links are still healthy. In this situation, the bandwidth on the logical trunks is adjusted downwards to prevent cell drops, and the connections on those trunks are re-routed. If a third line goes into alarm, the logical trunks are then failed. See Table 4-45 for a list of physical and trunk alarms that are supported on IMA lines.

Table 4-45 Physical and Logical Alarms Supported on IMA Physical Lines

	Physical							
Alarm Type	T1	E1	T3	E3	SONET	Logical	Statistical	Integrated
LOS	X	X	X	X	X		X	X
OOF	X	X	X	X	X		X	X
AIS	X	X	X	X	X		X	X
YEL	X	X	X	X	X			X

Table 4-45 Physical and Logical Alarms Supported on IMA Physical Lines

	Physical							
Alarm Type	T1	E1	T3	E3	SONET	Logical	Statistical	Integrated
PLCP OOF			X					X
LOC				X	X			X
LOP					X			X
PATH AIS					X			X
PATH YEL					X			X
PATH TRC					X			X
SEC TRC					X			X
ROOF	X	X						X
FER	X	X						X
AIS16	X	X					X	X
IMA	X	X						X
NTS Cells Dropped						X	X	
TS Cells Dropped						X	X	
Voice Cells Dropped						X	X	
Bdata Cells Dropped						X	X	
BdatB Cells Dropped						X	X	
HP Cells Dropped						X	X	
CBR Cells dropped						X	X	
VBR Cells dropped						X	X	
ABR Cells dropped						X	X	

Full Name

Configure trunk alarms

Syntax

cnftrkalm <slot.port>[.vtrk] <e | d>

Related Commands

dspalms, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

`cnftrkalm 7 d`

Description

Disable trunk alarms on trunk 7.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 3 1998 15:21 MST

PLN Type      Current Line Alarm Status               Other End
7    E1/32     Clear - Line OK                          alpha.10
9    T1/24     Clear - Line OK                          gamma.10
13   T1/24     Clear - Line OK                          alpha.14
15   T1/24     Clear - Line OK                          gamma.15
20   T3/3      Major - AIT Missing                        -









Last Command: cnftrkalm 7 d


Next Command:
```

Table 4-46 cnftrkalm—Parameters

Parameter	Description
slot.port	Specifies the trunk number.
e	Enables the alarm.
d	Disables the alarm.

Table 4-47 cnftrkalm—Optional Parameters

Parameter	Description
vtrk	Specifies the virtual trunk number.

cnftrkict

Configures the output lines of an interface control template for a subrate trunk. Table 4-48 shows the configurable signals.

Table 4-48 Configurable Signals in an Interface Control Template

Interface Type	Output Signal	Inputs
X.21	C, I	
V.35	RTS, DTR	CTS, DSR
MIL-188	IS, LL, RL, RS, SF, SS, TR	DM, CS

Full Name

Configure trunk interface control template

Syntax

cnftrkict <line> <output> <source>

Related Commands

dsptrkict, prttrkict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnftrkict 9 c on
```

Description

Configure output lead “c” as “on” in the interface control template for subrate trunk 9.

System Response

```
beta           TRM   YourID:1        IPX 8430    9.2    Aug. 3 1998 15:15 MST


Packet Line:    9
Interface:      X.21           DTE

                Interface Control Template for Trunk Line

Lead             Output Value   Lead     O Output Value
                C /DTR         ON








Last Command: cnftrkict 9 c on


Next Command:
```

Table 4-49 cnftrkict–Parameters cpytrkict

Parameter	Description
line	Specifies the trunk for the interface control template.
output	Specifies the output lead to be configured. Configurable output leads vary depending on the type of data interface used (X.21or V.35).
source	Specifies how the specified output lead is to be configured. The options are as follows: • On, which means the output lead is asserted. • Off, which means the output lead is inhibited. • l (lower case L) Output follows a local input lead. • Input, which specifies the name of the local input lead that the output lead follows. Input leads vary according to the type of data interface supported (X.21 or V.35).

Copies the interface control template of one trunk to another trunk. Once copied, the control information can be edited with the **cnftrkict** command. See the **cnftrkict** description for more information on configuring the trunk interface control templates.

Full Name

Copy trunk interface control template

Syntax

cpytrkict <source_trunk> <destination_trunk>

Related Commands

cnftrkict, dsptrkict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

cpytrkict 9 11

Description

Copy the interface control template for trunk 9 to trunk 11.

System Response

```
beta           TRM   YourID:1        IPX 8430    9.2    Aug. 3 1998 15:15 MST


Packet Line:      9
Interface:        X.21   DTE

Interface Control Template for Trunk Line

Lead Output Value Lead   Output Value
                    C/DTR ON








Last Command: cpytrkict 9 11


Enter destination line number:
```

Table 4-50 cpytrkict–Parameters

Parameter	Description
source trunk	Specifies the trunk number of the interface control template information to be copied.
destination trunk	Specifies the trunk number to which the interface control template information is copied.

delapsln

The **delapsln** command deletes SONET Automatic Protection Switching (APS) for the lines. You must enter the working slot.port pair. When you execute the **delapsln** command, the **dspapsln** display appears, showing you that the line you deleted is gone. (The **delapsln** display will be empty, or show only the remaining APS lines.)

SONET APS is a standard that describes the switching of SONET lines from the active line to a standby line to provide hardware line redundancy. The SONET APS feature only applies to BXM OC-3 and OC-12 cards in this release.

For background information on how SONET APS for BXM cards works, refer to "Overview of SONET Automatic Protection Switching (APS)" section on page 4-51.

When you execute the **delapsln** command, the switch software does the following:

- verifies that the slot.port arguments support APS

Full Name

Delete a SONET APS (Automatic Protection Switching) line

Syntax

delapsln <slot.port1> < slot.port2> <protocol>

where:

slot.port1 Desired working line number.

Table 4-51 delapsln Parameters

Parameter	Description
slot.port1	The desired working line number

Related Commands

addapsln, cnfapsln, cnfcdaps, dspapsln, dsplog, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	BPX	Yes

Example 1

```
delapsln 2.1
```

Description

Deletes a SONET APS line from a BXM OC-3 or OC-12 card.

System Response

```
sw117       TRM    genre         BPX 8620           9.2.c1         June 1 1999          16:25 PDT

Work/Protect      Actv   Active Line         Standby Line    Current APS      Last User
(Work 1/Work 2)  Line   Alarm Status        Alarm Status    Alarm Status     Switch Req




Command: delapsln 2.2
```

deltrk

Deletes a trunk. Because deleting a trunk removes the communication path between two nodes, using **deltrk** may split a network into two separate networks. If executing **deltrk** splits the network, then the connections that are using the deleted trunk are also deleted.

If both nodes on the trunk are reachable, you only need to execute **deltrk** on one node. If you delete a trunk on a node while the node at the other end is unreachable, the unreachable node does not detect that the trunk to the other node has been deleted, so be sure to delete the trunk at both nodes in this case.

After you delete a trunk, it still carries framing signals but no traffic. Also, the trunk can generate alarms for counting. To remove a trunk completely, use **dntrk** after executing the **deltrk** command**.**

In the following situations, the node does not allow **deltrk** to execute:

- Another node is attempting to change the network topology by adding or deleting a trunk.
- Another node is notifying all other nodes that it has a new node name.
- Another node is adding or deleting a channel connection in the network with the **addcon** or **delcon** command.

In Release 9.1.07, when the Abit Notifications on LMI/ILMI Interface feature is enabled (using **cnfnodeparm**), after deleting the trunk, the master node will deroute all the connections on the trunk. The slave end will receive the A7 (CMUP_DEROUTE) message before the reroute message from the master node. For information on the Abit Notifications feature, see the "Summary of Commands" section on page 4-83.

Regarding the Abit Notifications feature, each pass in the Connection Management routing state machine involves two activities: deroute and then followed by routing connections. However, connections can be derouted without going through the reroute state machine (for example, deltrk). There are several ways to kick off the routing state machine resulting in slightly different deroute and reroute behavior. See the **deltrk**, **dncd**, and **cnfcmparm** (SuperUser) commands.

Full Name

Delete trunk from a network

Syntax

deltrk <slot.port>[.vtrk]

Related Commands

addtrk, dntrk, dspnw, dsptrks, uptrk

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

```
deltrk 7
```

Description

Delete trunk 7 from the network.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:02 MST

PLN Type      Current Line Alarm Status               Other End
7    E1/32     Clear - Line OK                          -
9    T1/24     Clear - Line OK                          gamma.10
13   T1/24     Clear - Line OK                          alpha.14
15   T1/24     Clear - Line OK                          gamma.15
20   T3/3      AIT   - AIT Missing                      -









Last Command: deltrk 7


Next Command:
```

Table 4-52 deltrk–Parameters

Parameter	Description
slot.port	Specifies the physical trunk number.

Table 4-53 deltrk–Optional Parameters

Parameter	Description
vtrk	Specifies the virtual trunk portion of the trunk identifier.

deltrkred

Removes redundancy from a UXM, ALM/B, BTM, or AIT trunk. After you execute **deltrkrd**, you can remove the backup card without causing an alarm.

The trunk redundancy feature (not the Automatic Protection Switching redundancy feature) is supported on the IPX and IGX platforms. (This is different from the Automatic Protection Switching redundancy feature, supported in this release. APS is only supported on BXM SONET trunks, and can be used with virtual trunks. That is, the trunk port supporting virtual trunks can have APS line redundancy configured in the same way it would be configured for a physical trunk. The APS commands **addapsln**, **delapsln**, **switchapsln**, and **cnfaplsn** are all supported on virtual trunk ports.)

Note that the trunk redundancy feature is not supported for virtual trunks. The **addtrkred, deltrkred,** and **dsptrkred** commands will be rejected for virtual trunks.

Note that Y-cable redundancy is supported for both the UXM and BXM trunk cards at the edge of the ATM cloud.

Full Name

Delete ATM trunk redundancy

Syntax

deltrkred <backup ATM trunk number>

Related Commands

addtrkred, dsptrkred

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	IGX	Yes

Example 1

```
deltrkred 5
```

Description

Remove ATM trunk redundancy for the card set in slot 5.

System Response

```
beta          TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:15 MST

ATM Line    Backup ATM Line

5           8











Last Command: deltrkred 5


Next Command:
```

Table 4-54 deltrkred–Parameters

Parameter	Description
Backup trunk number	Specifies of the ATM card set assigned as the backup.

dntrk

Downs a trunk, after which it no longer carries framing or statistics. Before you can down a trunk with **dntrk**, you must remove it must from the network with **deltrk** (or **delshelf** in a tiered network).

Full Name

Down trunk

Syntax

dntrk <slot.port>[.vtrk]

Note No space exists between the port number and the "." for the virtual trunk specification.

Related Commands

addtrk, deltrk, uptrk, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

```
dntrk 9
```

Description

Deactivate trunk 9.

System Response

```
beta           TRM   YourID:1        IPX 8430    9.2    Aug. 3 1998 10:53 MST

From Type      Current Line Alarm Status              Other End
13   T1/24     Clear - Line OK                        alpha.14
15   T1/24     Clear - Line OK                        gamma.15
20   T3/3      Major - AIT Missing                    -










Last Command: dntrk 9


Next Command:
```

Table 4-55 dntrk–Parameters

Parameter	Description
slot.port	Specifies the physical trunk.

Table 4-56 dntrk–Optional Parameters

Parameter	Description
vtrk	Specifies a virtual trunk number (applies to BNI only). T3/E3 range is 1–32. OC-3 range is 1–11.

dspapsln

The **dspapsln** command displays the currently configured APS lines and their status.

Full Name

Display currently configured APS lines and their status

Syntax

dspapsln

Related Commands

addapsln, delapsln, cnfapsln, cnfapsln, dspapsln, dsplog, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	No	BPX	No

Example 1

dspapsln

Description

Display all the currently configured APS lines and their status.

System Response

```
alexa       TRM    genre         BPX 8600          9.2       May 11 1999    16:25 PDT

                Actv Active Line    Standby Line      Current APS         Last User
Work/Protect    Line Alarm Status   Alarm Status      Alarm Status        Switch Req

2.1 3.1        PROT OK             OK                Loss of Sig(RED)    Clear
5.1 5.2        WORK OK             LOS               LOS                 Lockout
6.3 6.4        NONE Deactivated    APS Deactivated
10.1 11.1      PROT OK             OK                Standard Mismatch   Clear

Command: dspapsln
```

Example 2

dspapsln

System Description

Display currently configured APS lines and their status.

System Response

```
sw117       TRM    genre       BPX 8620         9.2.c1       June 1 1999      16:25 PDT

Work/Protect     Actv   Active Line         Standby Line    Current APS      Last User
(Work 1/Work 2)  Line   Alarm Status        Alarm Status    Alarm Status     Switch Req
2.2    3.2       WORK   Loss of Sig (RED)   Remote (YEL)    Remote (YEL)     Clear




Command: dspapsln
```

dsplog

The **dsplog** command lets you display APS (Automatic Protection Switching) alarms. The **dsplog** command's display is similar to the **dspalms** command.

You can display APS alarms with the **dsplog** command, which are propagated to the Cisco WAN Manager. Also, the **dspalms** command includes a row for APS alarms. Refer to the "APS Alarms" section on page 4-63 for more information about APS alarms. Also, APS alarms and events are listed in Table 14-47 on page 14-93. (Possible classes, or types, of alarms are: *Major, Minor, Clear,* and *Info*. *Info* indicates they are APS events. Note that events display with the **dsplog** command, but are not displayed by the **dspapsln** command.

For example, in this release, the **dsplog** command displays the SES interface shelf (feeder) when the shelf is added or removed (using **addshelf** and **delshelf**) from an IGX 8400 routing hub.

Also refer to the "dsplog" section on page 14-92.

Syntax

dsplog

Related Commands

dspalms

System Response

```
alexa       TRM    genre         BPX 8620        9.2      Sep. 9 1998       16:35 PDT


Alarm summary   (Configured alarm slots: None)
Connections Failed:                                        None
TRK Alarms:                                                None
Line Alarms:                                               None
Cards Failed:                                              None
Slots Alarmed:                                             1 Major
Missing Cards:                                             1
Remote Node Alarms:                                        1 Minor
Remote Domain Alarms:                                      None
APS Alarms:                                                 1 Major, 1 Minor

Interface Shelf Alarms:                                    None
ASM Alarms:                                                None




Last Command: dsplog
```

dspnw

Displays the network topology in tabular form. Alarms appear in a column, and added trunks (by **addtrk**) appear to the right to the node name. Each trunk entry shows the local back card slot number and the node name and back card slot number on the other end of the line. Note the following conventions:

- ~ indicates that the trunk is a satellite line.
- Flashing entry indicates a failed line.
- Blinking node name indicates a node executing downloader software.

If the network has more nodes and trunk connections than are currently on the screen, a “Continue?” prompt appears. Press the Return key to display other parameters, or enter “n” to exit the command.

Full Name

Display network

Syntax

dspnw [+b | -b] [+z | -z]

Related Commands

dspnds, prtnw

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspnw`

Description

Display the network topology in tabular form.

System Response

```
sw91           TN    SuperUser       IGX 8410     9.2   Nov. 13 1998 16:06 GMT


NodeName    Alarm            Trunk                    Trunk
sw92        UNRCH
   8-7/sw91
sw200       UNRCH
   14-14/sw201               15-15/sw201              16-16/sw201
sw201       UNRCH
   14-14/sw200               15-15/sw200              16-16/sw200
   12.1-4.5/sw26
sw12        MAJOR
   3.1.2-4.7/sw26            3.1.3-6.3/sw91
sw91        MAJOR
   7-8/sw92                  6.3-3.1.3/sw12           6.4-3.1.4/sw68
sw68        Minor
   3.1.4-6.4/sw91

This Command: dspnw


Continue?
```

The display shows a network containing the nodes sw92, sw200, sw201, sw12, sw91, and sw68. The word “Major” to the right of “sw12” and “sw91” (see Alarm column) indicates the existence of alarm conditions such as loss of signal.

On node “sw92”, trunk 8 connects to trunk 7 on node “sw91”. Similarly, on node “sw200”, trunk 14 connects to trunk 14 on node “sw201”. If the two trunk numbers are separated by a tilde (~) in place of a dash (-), this indicates a satellite. The following illustrates a map of this network.

Table 4-57 dspnw–Optional I Parameters

Parameter	Description
+b	Display only the lines that support bursty data.
-b	Display only the lines that do not support bursty data.
+z	Display only the lines that use ZCS encoding.
-z	Display only the lines that do not use ZCS encoding.

dspphyslns

Displays a summary of line alarm status for the ATM port specified. These include the cell count in the transmit and receive directions, and error counts associated with the port. The display indicates the date and time that the statistics were cleared and the statistics collection time since they were last cleared. Cells transmitted indicates the amount of data transmitted out the port to the user device. Cells received indicates the amount of data received from the user device at the port. Corrupted statistics result from channel/port loopbacks or port tests. A yes in this field indicates that such a loopback or port test has occurred since the statistics were last cleared.

Note that IMA physical line alarms are maintained differently from other types of logical (physical and virtual) trunks. Each IMA trunk has a configurable number of retained links. If the number of non-alarmed lines is less than the number of retained links, the logical (physical and virtual) trunks on the IMA trunk are placed into major alarm. For example, if a line has IMA virtual trunks 4.5–8.2 and 4.5–8.7, the number of retained links on 4.5–8 has been configured to 2. If 4.5 and 4.6 go into LOS (loss of signal), physical line alarms are generated for these two physical lines. The logical trunks 4.5–8.7 do not go into alarm because the two retained links are still healthy. In this situation, the bandwidth on the logical trunks is adjusted downward to prevent cell drops, and the connections on those trunks are re-routed. If a third line goes into alarm, the logical trunks are then failed.

Full Name

Display the status of the UXM trunk and its physical line (or lines if IMA).

Syntax

dspphyslns [slot]

Related Commands

dspphyslnstathist

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspphyslns`

Description

Display the physical line of all the UXM cards on the node.

System Response

```
sw228          TN    SuperUser       IGX 8420    9.2      Aug. 27 1998 17:52 PST

PHYSLN   Type   Current Line Alarm Status                  TRK
 6.2     OC-3    Major - Loss of Sig (RED)                   6.2
 6.3     OC-3    Clear - OK                                  6.3
11.3     E1/30 Clear - OK                                  11.3
11.4     E1/30 Major - Loss of Sig (RED)                   11.4-6
11.5     E1/30 Major - Loss of Sig (RED)                   11.4-6
11.6     E1/30 Major - Loss of Sig (RED)                   11.4-6










Last Command: dspphyslns
```

Example 2

dspphyslns 11

Description

Display the physical lines of the UXM card in slot 11.

System Response

```
sw228          TN    SuperUser       IGX 8420    9.2    Aug. 27 1998 17:53 PST

PHYSLN   Type   Current Line Alarm Status                  TRK
11.1     T1/24 Clear - OK                                  11.1x4
11.3     T1/24 Clear - OK                                  11.1x4
11.5     T1/24 Clear - OK)                                 11.1x4
11.7     T1/24 Clear - OK                                  11.1x4










Last Command: dspphyslns 11
```

Table 4-58 dsphyslns–Optional Parameters

Parameter	Description
slot	Specifies the slot number.

dspphyslnstathist

Displays a summary of physical statistics for the specified individual line within an IMA trunk. These include the cell count in the transmit and receive directions, and error counts associated with the port. The display indicates the date and time that the statistics were cleared and the statistics collection time since they were last cleared. Cells transmitted indicates the amount of data transmitted out the port to the user device. Cells received indicates the amount of data received from the user device at the port. Corrupted statistics result from channel/port loopbacks or port tests. A yes in this field indicates that such loopback or port test have occurred since the statistics were last cleared.

On both the BPX and the IGX, physical line statistics display only on the **dspphyslnstats**, **dspphyslnstathist**, and **dspphyslnerrs** screens. These commands accept only physical line numbers (that is, *slot.port*).

In this release, the **dspphyslnstathist** command displays the following additional physical line statistics. A summary and description of these statistics follows. See Table 4-59.

Table 4-59 IMA Physical Line Statistics

Statistics
IMA Violations
Near End Severely Errored Seconds (SES-IMA)
Far End Severely Errored Seconds (SES-IMA-FE)
Near End Unavailable Seconds (UAS-IMA)
Far End Unavailable Seconds (UAS-IMA-FE)
Near End Tx Unusable Seconds (Tx-UUS-IMA)
Near End Rx Unusable Seconds (Rx-UUS-IMA)
Far End Tx Unusable Seconds (Rx-UUS-IMA-FE)
Far End Rx Unusable Seconds (Rx-UUS-IMA-FE)
Near End Tx No. of Failures (Tx-FC)
Near End Rx No. of Failured (Rx-FC)

Full Name

Display individual physical line statistics

Syntax

dsphyslnstathist

Related Commands

dspphyslns, dspportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX (UXM)	No

Example 1

dspphyslnstathist 4.1

Description

Display the statistics for line on the IMA trunk on port 4.1.

System Response

```
ca19           VT    SuperUser       BPX 8620    9.2    Aug. 23 1998 18:55 GMT

Port Statistics for 4.1         Cleared: Aug. 23 1997 18:19
Port Speed: 96000 cps   Collection Time: 0 day(s) 00:00:00      Corrupted: NO

              Cells           CLP         (EFCI)
Rx Port:    1274609       1032194              0
Tx Port:    1274607       1032192              0
                                                    CellBuf Ofl:         0
Unknown Addr:               0
Last Unknown Addr:
Tx Payload Err Cnt:         0
Tx Hdr Err discard:         0
Nonzero GFC Count:          0



This Command: dspphyslnstathist 4.1


Hit DEL key to quit:
```

Table 4-60 dspphyslnstathist–Parameters

Parameter	Description
slot.port	Specifies the ATM card set and port number.

Table 4-61 dspphyslnstathist–Optional Parameters

Parameter	Description
interval	Specifies the refresh interval time for data. It can be specified between 1 and 60 seconds. The default interval is 1 seconds.

dsptrkbob

Displays the state of all inputs from subrate line equipment to an IPX or IGX node and the state of all outputs from the node to the subrate line equipment. Display updates can occur at an optional, user-specified interval. Otherwise, the display remains on-screen until Delete is pressed or the display times out. The default interval for updating the display is every 5 seconds. If a trunk is disabled, its number appears in dim, reverse video. See **cnftrkict** for configuration details.

Full Name

Display trunk breakout box

Syntax

dsptrkbob <line> [interval]

Related Commands

cnftrkict, dsptrkict

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	Yes

Example 1

```
dsptrkbob 9
```

Description

Display the breakout for subrate trunk 9.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Sep. 15 1998 15:15 MST


Packet Line:9
Interfaces:   X.21    DTE

Inputs from Line Equipment               Outputs to Line Equipment
Lead     Pin    State   Lead   Pin    State     Lead   Pin   State     Lead  Pin  State
RxD     4/11   Idle    TxD    2/9    Active
I/DSR   5/12   On                               C/DTR  3/10  On
S/RxC    6/13   Active




Last Command: dsptrkbob 9


Hit DEL key to quit:
```

Table 4-62 dsptrkbob–Parameters

Parameter	Description
trunk	Specifies the subrate trunk.

Table 4-63 dsptrkbob–Optional Parameters

Parameter	Description
interval	The number of seconds between updates of the breakout box display. The range is 1–60.

dsptrkcnf

Displays trunk configuration. The parameter values that **dsptrkcnf** displays have been set with **cnftrk** or are default values.

As of Release 9.1, **dsptrkcnf** displays the cost of a trunk if cost-based routing is configured. You configure the administrative cost of a trunk with **cnftrk**.

Full Name

Display trunk configuration

Syntax

dsptrkcnf <slot.port>[.vtrk]

Related Commands

cnftrk

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsptrkcnf 6.8`

Description

Display the configuration for trunk 6.8

System Response

```
sw203          TN    StrataCom       BPX 8620    9.2    Sep. 25 1998 07:35 GMT

TRK  6.8 Config    OC-3       [353207cps]   BXM slot:     6
Transmit Rate:         353208              Line framing:          STS-3C
Subrate data rate:     --                       coding:           --
Line DS-0 map:         --                       CRC:              --
Statistical Reserve:   1000    cps              recv impedance:   --
Idle code:             7F hex                   cable type:       --
Max Channels/Port:     256                            length:     --
Connection Channels:   256                 Pass sync:             Yes
Traffic:   V,TS,NTS,FR,FST,CBR,VBR,ABR     Loop clock:            No
SVC Vpi Min:           0                   HCS Masking:           Yes
SVC Channels:          0                   Payload Scramble:      Yes
SVC Bandwidth:         0      cps          Frame Scramble:        Yes
Restrict CC traffic:   No                  Cell Header Type:      --
Link type:             Terrestrial         Virtual Trunk Type:    --
Routing Cost:          10                  Virtual Trunk VPI:     --
Deroute delay time:    0 seconds

Last Command: dsptrkcnf 6.8


Next Command:
```

Example 2

dsptrkcnf 6

Description

Display the configuration for trunk 6. Trunk 6 is an AIT trunk on an IPX node.

System Response

```
sw91           TN    SuperUser       IGX 8410     9.2       Sep.  22 1998 16:09 GMT

PLN 6 Configuration   T3/3    [1000  pps]   AIT slot: 6
Clock Rate:           --                    Idle code:            7F hex
Transmit Trunk Rate:  96000 cps             Restrict PCC traffic: No
Rcv Trunk Rate:       1000 pps              Link type:            Terrestrial
Subrate interface:    --                    Line framing:         --
Subrate data rate:    --                         coding:          --
Line DS-0 map:        --                         CRC:             --
Pass sync:            Yes                        recv impedance:  --
Loop clock:           No    pps                  cable type:
Statistical Reserve:  992                              length:    0-225 ft.
Header Type:          STI                   HCS Masking:          Yes
Gateway Type:         BAM                   Payload Scramble:     No
VPI Address:          0                     End supp BData:       Yes
VCI Address:          0                     End supp FST:         Yes
Routing Cost:         0

Last Command: dsptrkcnf 6


Next Command:
```

Example 3

dsptrkcnf 11

Description

Display the configuration for the E3 trunk in slot 11 (an ALM/B trunk).

System Response

```
IGX16          TN    SuperUser       IGX 16    9.1 Sep. 23 1997 02:08 GMT

PLN 11 Config         E3/480 [160000pps]    ALM slot: 11
Clock Rate:           --                    Idle code:            7F hex
Transmit Trunk Rate:  80000 cps             Restrict PCC traffic: No
Rcv Trunk Rate:       160000 pps            Link type:            Terrestrial
Subrate interface:    --                    Line framing:         --
Subrate data rate:    --                         coding:          --
Line DS-0 map:        --                         CRC:             --
Pass sync:            Yes                        recv impedance:  --
Loop clock:           No                         cable type:
Statistical Reserve:  992   pps                        length:    0-225 ft.
Header Type:          STI                   HCS Masking:          Yes
Gateway Type:         BAM                   Payload Scramble:     No
VPI Address:          0                     End supp BData:       Yes
VCI Address:          0                     End supp FST:         Yes
Routing Cost:          10

Last Command: dsptrkcnf 11


Next Command:
```

Example 4

dsptrkcnf 13.3.1

Description

Display the configuration for virtual trunk 13.3.1. The trunk is on a BNI-T3 card set in a BPX node.

System Response

```
sw97           TN    SuperUser       BPX 8620    9.2       June 22 1998 07:34 GMT

TRK 13.3.1 Config T3        [2867 cps]   BNI-T3 slot: 13
                                           Restrict CC traffic:   No
Transmit Rate:         3000                Link type:             Terrestrial
Subrate interface:     --                  Line framing:          --
Subrate data rate:     --                       coding:           --
Line DS-0 map:         --                       CRC:              --
Pass sync:             No                       recv impedance:   --
Loop clock:            No                       cable type:
Statistical Reserve:   992   cps                      length:     0-225 ft.
Idle code:             7F hex              HCS Masking:           Yes
Connection Channels:   55                  Payload Scramble:      No
Valid Traffic Classes:                     Frame Scramble:        --
         V,TS,NTS,FR,FST,CBR,VBR,ABR       Virtual Trunk Type:    CBR
                                           Virtual Trunk VPI:     1
                                           Virtual Trunk Service: 3

Last Command: dsptrkcnf 13.3.1
```

Example 5

dsptrkcnf 4.1

Description

Display the configuration for BXM 4.1 trunk.

System Response

```
b2             TRM   StrataCom       BPX 8620 9.2.3N    Dec. 14 1999 04:43
GMT

TRK 4.1 Config     E3      [80000 cps]    BXM slot:     4
Transmit Rate:         80000               VPC Conns disabled:    No
Protocol By The Card:  No <=====??              Line framing:          --
VC Shaping:            No                       coding:           --
Hdr Type NNI:          Yes                      recv impedance:   --
Statistical Reserve:   1000    cps              cable type:       --
Idle code:             7F hex                         length:     0-225ft.
Connection Channels:   256                 Pass sync:             No
Traffic:V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR    Loop clock:            No
SVC Vpi Min:           0                   HCS Masking:           Yes
SVC Channels:          0                   Payload Scramble:      Yes
SVC Bandwidth:         0      cps          Frame Scramble:        --
Restrict CC traffic:   No                  Virtual Trunk Type:    --
Link type:             Terrestrial         Virtual Trunk VPI:     --
Routing Cost:          10                  Deroute delay time:    0
```

Example 5

dsptrkcnf 6.3

Description

Display the configuration for trunk 6.3. The trunk is on a UXM-OC-3 card set in an IGX node.

System Response

```
sw228          TN    SuperUser       IGX 8420    9.2    Aug. 27 1998 17:42 PST

TRK 6.3 Config       OC-3     [353056cps] UXM slot: 6
Transmit Trunk Rate: 353207 cps          Frame Scramble:       Yes
Rcv Trunk Rate:       353207 cps          Cell Framing:         STS-3C
Pass sync:            Yes
Loop clock:           No
Statistical Reserve:  1000   cps
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels:  256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,VBR,ABR
Routing Cost:         10                  Deroute delay time:    0 seconds

Last Command: dsptrkcnf 6.3


Next Command:
```

Example 6

`dsptrkcnf 5.2`

Description

Display the configuration for trunk 5.2. The trunk is on a UXM-E1 card set in an IGX node.

System Response

```
sw224          TN    SuperUser       IGX 8420    9.2    Aug. 27 1998 17:50 GMT

TRK 5.2-8 Config     E1/203 [30641 cps] UXM slot: 5
Line DS-0 map:        1-15,17-31          Valid Traffic Classes:
Transmit Trunk Rate: 30641 cps                   V,TS,NTS,FR,FST,CBR,VBR,ABR
Rcv Trunk Rate:       28075  cps          Retained links:       7
Pass sync:            Yes                 IMA link auto disable:Disable
Loop clock:           No
Statistical Reserve:  600    cps
Idle code:            54 hex
Restrict PCC traffic: No
Link type:            Terrestrial
Line coding:          HDB3
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels:  256
Gateway Channels:     256
Routing Cost:          10                  Deroute delay time:    0 seconds

This Command: dsptrkcnf 5.2
```

Example 7

dsptrkcnf 10.1

Description

Display the configuration for trunk 10.1. The trunk is on a UXM-T1 card set in an IGX node.

System Response

```
sb-reef        TN    SuperUser       IGX 8420    9.2    Aug. 27 1998 17:46 PDT

TRK 10.1-5 Config     T1/115  [17358 cps] UXM slot: 10
Transmit Trunk Rate:  17358  cps          Connection Channels:  256
Rcv Trunk Rate:       17358  cps          Gateway Channels:     256
Pass sync:            Yes                 Valid Traffic Classes:
Loop clock:           No                           V,TS,NTS,FR,FST,CBR,VBR,ABR
Statistical Reserve:  600    cps          Retained links:       5
Idle code:            7F hex              IMA link auto disable:Enable
Restrict PCC traffic: No                    Window size:        30  (x10 secs)
Link type:            Terrestrial           Max transition cnts:10
Line framing:         ESF                   Link reenable time: 6   (x10 mins)
Line coding:          B8ZS
Line cable type:      ABAM
Line cable length:    0-131 ft.
HCS Masking:          Yes
Payload Scramble:     No
Routing Cost:         10                  Deroute delay time:    0 seconds

Last Command: dsptrkcnf 10.1
```

Table 4-64 dsptrkcnf–Parameters

Parameter	Description
slot.port	Specifies the physical slot and port number of the trunk.

Table 4-65 dsptrkcnf–Optional Parameters

Parameter	Description
vtrk	Specifies the virtual trunk number. The maximum value on a node is 32. The maximum on a T3 or E3 line is 32. The maximum for user traffic on an OC-3/STM1 trunk is 11. (See also the “Overview of Virtual Trunking” section on page 4-4” of this chapter.)

dsptrkict

Displays interface control information for the subrate trunks. The displayed information includes:

- Specified line.
- Associated leads and their status (that is, on or off)
- Whether output follows a local input.
- Name of the local or remote input lead that the output lead follows.

To see a list of configurable outputs, and information on how to configure an output, see the **cnftrkict** command. Disabled trunks have their trunk number displayed in dim, reverse video on the screen.

Full Name

Display trunk interface control templates

Syntax

dsptrkict <line>

Related Commands

cnftrkict, prttrkict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX	No

Example 1

```
dsptrkict 9
```

Description

Display subrate for the trunk 9 interface control template.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2 Aug. 15 1998 15:15 MST


Trunk:      9
Interface: X.21   DTE

Interface Control Template for Trunk Line

Lead    Output Value    Lead     Output Value
C/DTR   ON








Last Command: dsptrkict 9


Next Command:
```

dsptrkred

Displays the backup and primary cards for a trunk.

Full Name

Display ATM trunk redundancy

Syntax

dsptrkred [trunk]

Related Commands

addtrkred, deltrkred

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	No	IGX, BPX	No

Example 1

`dsptrkred`

Description

Display all ATM trunks with redundancy.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:15 MST

ATM Line Backup ATM Line
4         5
7          8










Last Command: dsptrkred


Next Command:
```

Table 4-66 dsptrkred–Optional Parameters

Parameter	Description
ATM trunk number	Specifies the slot number of the primary or backup ATM card set to display. Without this optional entry, the screen displays all primary and backup ATM trunks.

dsptrks

Displays basic trunk information for all trunks on a node. This command applies to both physical only and virtual trunks. The displayed information consists of:

- Trunk number, including the virtual trunk number, if applicable
- Line type (E1, T3, or OC-3, for example)
- Alarm status

In addition, for trunks that have been added to the network with the **addtrk** command, the information includes the node name and trunk number at the other end. Trunks that have a "–" in the Other End column have been upped with **uptrk** but not yet added on both ends with **addtrk**. For disabled trunks, the trunk numbers appear in reverse video on the screen.

For UXM trunks with ATM Forum IMA compliant trunks, a trunk is displayed in **dsptrks** as:

<slot>.<primary_port>x<num ports>

For example, an IMA trunk would display in the TRK column in the **dsptrks** screen as the following:

5.1x4

In this case, 5.1x4 indicates an ATM Forum compliant IMA trunk 5.4 which consists of four physical lines. To see all physical lines belonging to this IMA trunk, you can enter the **dspphyslns** command.

In Release 9.2.20, **dsptrks** displays all interface shelves attached to a BPX or an IGX routing hub that use the AAL5 protocol.

Note that in this release, for IMA trunks, you can configure non-consecutive physical lines. In Release 9.1, an IMA trunk required that consecutive physical lines be configured on the same card. In this release, non-consecutive physical lines are supported.

For VSI "dedicated" virtual trunks, **dsptrks** will indicate this.

Full Name

Display trunks

Syntax

dsptrks

Related Commands

addtrk, deltrk, dntrk, uptrk

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsptrks`

Description

Display information on the trunk configuration and alarm status for the trunks at a node. The trunk numbers with three places represent virtual trunks.

System Response

```
sw288          TN    SuperUser       BPX 8620    9.2    Dec. 10 1998 15:39 GMT

TRK     Type      Current Line Alarm Status          Other End
 4.1    OC-12      Clear - OK                          SIMFDR(AAL5)
11.2    T3        Clear - OK                         redhook/14
11.3    T3        Clear - OK                         sw113/16




Last Command: dsptrks


Next Command:
```

Example 2

`dsptrks`

Description

Display information on the trunk configuration and alarm status for the trunks at a node. The trunk numbers with three places (*slot.port.vrtk*) represent virtual trunks; for example—trunk 13, port 3, virtual trunk 12. Also, on trunk 4, slot 8, is a simulated interface shelf "SIMFDR0", with interface shelf type of AAL5.

System Response

```
sw288           TN    SuperUser       BPX 8620    9.2    Dec. 10 1998 23:03 GMT

TRK        Type   Current Line Alarm Status                  Other End
 2.1       T3      Clear - OK                                pswbpx1/1.2
 4.8       T3      Clear - OK                                SIMFDR0 (AAL5)
 13.3.12   OC-3     Clear - OK                                rita/4.2.10




Last Command: dsptrks


Next Command:
```

Example 3

`dsptrks`

Description

Display information on the trunk configuration and alarm status for the trunks at a node. The trunk numbers with three places (*slot.port.vrtk*) represent virtual trunks. An ATM Forum-compliant trunk is configured on slot 11, which has a primary port of 1 and 4 physical lines.

System Response

```
sw53           TN    SuperUser       BPX 8620    9.2    Sep. 24 1998 23:03 GMT

TRK      Type       Current Line Alarm Status               Other End
 2.1     T3         Clear - OK                              pswbpx1/1.2
 4.8     T3         Clear - OK                              SIMFDR0 (AAL5)
 11.1x4  T1/92      Clear - OK                              a1c/3.5x4
 15.1    OC-3        Clear - OK                              alc/3.5x4




Last Command: dsptrks


Next Command:
```

Example 4

dsptrks

Description

Display information on the trunk configuration and alarm status for the trunks at an IGX node showing IMA compliant links on slot 11.

System Response

```
oo1          TN    SuperUser       IGX 8430    9.2.zR    Dec. 10 1998 23:03 GMT

TRK      Type     Current Line Alarm Status                 Other End
 6.1     OC-3      Clear - OK                                oo1p(AAL5)
 8.5     T3       Clear - OK                                n4b/4.5
 8.6     E3/530   Clear - OK                                alc/15
 10      T3/240   Clear - OK                                alc/3.5x4
 11.1x4  T1/92    Clear - OK                                alc/3.5x4
 15.1    OC-3      Clear - OK                                n1a/11.3
 15.2    OC-3      Clear - OK                                n2b/5.3



Last Command: dsptrks


Next Command:
```

Example 5

dsptrks

Description

Display information on the feeders attached to an IGX 8400 routing hub. (The SES feeder uses the AAL5 protocol to communicate with the routing network.) Feeder names appear in the Other End field on the dsptrks screen on an IGX routing hub.

System Response

```
oo1           TN    SuperUser       IGX 8430    9.2.zR    Dec. 10 1998 23:03 GMT

TRK      Type     Current Line Alarm Status                  Other End
13       E1       Clear - OK                                 igx1/12
14.1     OC-3      Clear - OK                                 ases1 (AAL5)



Last Command: dsptrks


Next Command:
```

Example 6

dsptrks

Description

Display trunks including virtual trunks. A VSI trunk is on trunk 2.1.1; dsptrks indicates this with “VSI trunk”.

System Response

```
TRK     Type   Current Line Alarm Status        Other End
 1.1    E3      Clear - OK                      sw58/1.1
 1.2    E3      Clear - OK                      sw183(AXIS)
 2.1.1 OC-3     Clear - OK                      VSI trunk
```

Example 7

dsptrks

Description

The dsptrks screen shows VSI trunks 4.1, 4.2 and 4.3, with the “Other End” of 4.1 reading “VSI (VSI)”. A typical dsptrks screen example showing some VSI trunks configured follows:

System Response

```
n4            TN    SuperUser       BPX 15    9.2      Apr. 4 1998 16:45 PST

TRK     Type     Current Line Alarm Status              Other End
 2.1    OC-3      Clear - OK                             j4a/2.1
 3.1    E3       Clear - OK                             j6c(AXIS)
 5.1    E3       Clear - OK                             j6a/5.2
 5.2    E3       Clear - OK                             j3b/3
 5.3    E3       Clear - OK                             j5c(IPX/AF)
 6.1    T3       Clear - OK                             j4a/4.1
 6.2    T3       Clear - OK                             j3b/4
 4.1    OC-3      Clear - OK                             VSI(VSI)
 4.2    OC-3      Clear - OK                             VSI(VSI)
 4.3    OC-3      Clear - OK                             VSI(VSI)


Last Command: dsptrks
```

dsptrkstats

Displays the trunk port status, ATM cell loss counts, cell payload errors, and cell header errors for the specified trunk. Table 4-67 lists the other statistics. If you include the optional *clear* parameter, executing **dsptrkstats** clears the statistics.

Logical trunk statistics refer to counts on trunks that are visible as routing entities. This includes physical and virtual trunks (all logical trunks). Logical trunk statistics are displayed on the **dsptrkstats, dsptrkstathist,** and screens. These commands only accept logical trunk numbers and display only logical trunk statistics. Virtual interface (VI) statistics and queue statistics are both subsets of the logical trunk statistics.

Table 4-67 Additional Statistics in the dsptrkstats Display

Statistics	Description
Cells dropped due to BFrame parity err.	A parity error was detected in one or more of the P bits in the BFrame header or in the BIP-16 parity check for the header causing the cell to be dropped.
Cell header mismatch error count.	A count of cells received by a BNI in this slot.port with an incorrect header address for that card.
First mismatch cell header VPI/VCI.	This displays the VPI/VCI address of the first header mismatch to be received by the card in this slot.port.
BFrame cell data payload error.	A separate BIP-16 parity check is used for the payload data. This number represents the number of errors detected by this parity check. This does not necessarily cause a cell to be dropped.
BFrame cell loss due to admin access.	Internal to the BNI card is an administrative processor. This statistic is a count of the cells that were lost in an internal administrative shuffle.

Trunk Statistics

Statistics are collected on trunks at several different levels.

- **Physical line** statistics apply to each physical port. In the case of IMA trunks, the physical line statistics are tallied separately for each T1 port.

  On both the BPX and the IGX, physical line stats are displayed on the **dspphyslnstats**, dspphyslnstathist, and **dspphyslnerrs** screens. These commands only accept physical line numbers (that is, slot.port). These commands are new to the BPX in this release.

- **Logical trunk** statistics refer to counts on trunks that are visible to users as routing entities. This includes physical trunks and virtual trunks.

  Logical trunk stats are displayed on the **dsptrkstats**, **dsptrkstahist**, and **dsptrkerrs** screens. These commands only accept logical trunk numbers and display only logical trunk statistics.

- **VI statistics** are a subset of the logical trunk statistics.
- **Queue statistics** are a subset of the logical trunk statistics.
- **Channel statistics** are not polled by software on trunks. However, they are available if the debug command **dspchstats** is used.

A listing of trunk statistics including statistics type, card type, and line type, as applicable, is provided in Table 4-68.

Table 4-68 Trunk Statistics

Statistic	Stat Type	Card Type	Line Type
Total Cells Received	Logical	UXM/BXM	All
Total Cells Transmitted	Logical	UXM/BXM	All
LOS transitions	Physical	UXM/BXM	All
LOF transitions	Physical	UXM/BXM	All
Line AIS transitions	Physical	UXM/BXM	T3/E3/Sonet
Line RDI (Yellow) transitions	Physical	UXM/BXM	T3/E3/Sonet
Uncorrectable HCS errors	Physical	UXM	T3/E3/Sonet
Correctable HCS errors	Physical	UXM	T3/E3/Sonet
HCS errors	Physical	BXM	T3/E3/Sonet
Line Code Violations, ES, and SES	Physical	BXM	T3/E3
Line Parity (P-bit]) errors, ES, and SES	Physical	BXM	T3
Path Parity (C-bit) errors, ES, and SES	Physical	BXM	T3
Far End Block Errors	Physical	BXM	T3
Framing Errors and SES	Physical	BXM	T3/E3
Unavailable Seconds	Physical	BXM	T3/E3
PLCP LOF and SES	Physical	BXM	T3
PLCP YEL	Physical	BXM	T3
PLCP BIP-8, ES, SES	Physical	BXM	T3
PLCP FEBE, ES, SES	Physical	BXM	T3
PLCP FOE, ES, SES	Physical	BXM	T3
PLCP UAS	Physical	BXM	T3
LOC errors	Physical	UXM/BXM	E3/Sonet
LOP errors	Physical	UXM/BXM	Sonet
Path AIS errors	Physical	UXM/BXM	Sonet
Path RDI errors	Physical	UXM/BXM	Sonet
Section BIP-8 counts, ES, and SES	Physical	UXM/BXM	Sonet
Line BIP-24 counts, ES, and SES	Physical	UXM/BXM	Sonet
Line FEBE counts, ES, and SES	Physical	UXM/BXM	Sonet
Section SEFS	Physical	UXM/BXM	Sonet
Line UAS and FarEnd UAS	Physical	UXM/BXM	Sonet
Clock Loss Transitions	Physical	UXM	T1/E1
Frame Loss Transitions	Physical	UXM	T1/E1
Multiframe Loss	Physical	UXM	T1/E1
CRC errors	Physical	UXM	T1/E1

Table 4-68 Trunk Statistics (Continued)

Statistic	Stat Type	Card Type	Line Type
BPV	Physical	UXM	T1
Frame bit errors	Physical	UXM	E1
Unknown VPI/VCI count	Physical	UXM/BXM	All
Errored LPC cell count	Physical	UXM	All
Non-zero GFC cell count	Physical	UXM/BXM	
Max Differential Delay	Physical	UXM	T1/E1
Uncorrectable HEC errors	Physical	UXM	All
Cell Hunt count	Physical	UXM	T1/E1
Bandwidth Changed count	Physical	UXM	T1/E1
Receive CLP=0 cell count	Logical	UXM/BXM	All
Receive CLP=1 cell count	Logical	UXM/BXM	All
Receive CLP=0 cell discard	Logical	UXM/BXM	All
Receive CLP=1 cell discard	Logical	UXM/BXM	All
Transmit CLP=0 cell count	Logical	UXM/BXM	All
Transmit CLP=1 cell count	Logical	UXM/BXM	All
Receive OAM cell count	Logical	UXM/BXM	All
Transmit OAM cell count	Logical	UXM/BXM	All
Receive RM cell count	Logical	UXM/BXM	All
Transmit RM cell count	Logical	UXM/BXM	All
For Each Traffic Type: (V,TS,NTS,ABR,rt-VBR, nrt-VBR,CBR, BdatB, BdatA,HP)			
Cells served	Logical	UXM/BXM	All
Maximum Qbin depth	Logical	UXM/BXM	All
Cells discarded count	Logical	UXM/BXM	All

Full Name

Display trunks statistics

Syntax

dsptrkstats <slot.port> [clear]

Related Commands

cnftrkstats, dsptrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX, IGX (UXM)	Yes

Example 1

`dsptrkstats 1.1`

Description

Display cell statistics for ATM trunk 1.1.

System Response

```
sw53           TN    SuperUser       BPX 8620    9.2       Sep. 24 1998 23:07 GMT

Trunk  1.1      Status: Clear - OK                      Cleared: 04/24/96 17:31:16
Type                                    Count
Cells dropped due to BFrame parity err     0
Cell header mismatch error count           0
BFrame cell data payload error             0
BFrame cell loss due to disabled chan      0
BFrame cell count(TX)                  8316        non-hipri cells -    52
BFrame cell count(RX)                  12452

First mismatch cell masked VPI/VCI         0
First mismatch cell full VPI/VCI           0



Last Command: dsptrkstats 1.1


Next Command:
```

Example 2

`dsptrkstats 11.1`

Description

Display cell statistics for ATM trunk 11.1 on a UXM card.

System Response

```
sw199          TN    SuperUser       IGX 8620    9.2   Aug. 27 1998 19:26 PDT

Trunk 11.1-2 Status: Clear - OK                                    Snapshot
Collection Time: 0 day(s) 00:49:40                     Clrd:  08/27/97 18:36:05
Type                                     Count
QBIN: NTS Cells Tx to line                   0
QBIN: Tx NTS Cells Received                  0
QBIN: Tx NTS Cells Discarded                 0
QBIN: Hi-Pri Cells Tx to line             2561
QBIN: Tx Hi-Pri Cells Received            2561
QBIN: Tx Hi-Pri Cells Discarded              0
QBIN: rt-VBR Cells Tx to line                0
QBIN: Tx rt-VBR Cells Received               0
QBIN: Tx rt-VBR Cells Discarded              0
QBIN: TimeStamped Cells Tx to ln             0
QBIN: Tx TS Cells Received                   0
QBIN: Tx TS Cells Discarded                  0
QBIN: BData A Cells Tx to line               0
QBIN: Tx BData A Cells Received              0
QBIN: Tx BData A Cells Discarded             0
QBIN: BData B Cells Tx to line               0
QBIN: Tx BData B Cells Received              0
QBIN: Tx BData B Cells Discarded             0
QBIN: Tx CBR Cells Served                    0
QBIN: Tx CBR Cells Received                  0
QBIN: Tx CBR Cells Discarded                 0
QBIN: Tx nrt-VBR Cells Served                0
QBIN: Tx nrt-VBR Cells Received              0
QBIN: Tx nrt-VBR Cells Discarded             0
QBIN: Tx ABR Cells Served                    0
QBIN: Tx ABR Cells Received                  0
QBIN: Tx ABR Cells Discarded                 0
VI: Cells received                         655
VI: Cells transmitted                      653
VI: Cells received w/CLP=1                   0
VI: Cells transmitted w/CLP=1                0
VI: Cells received w/CLP=0                 655
VI: Cells transmitted w/CLP=0              653
VI: Cells discarded w/CLP=1                  0
VI: Cells discarded w/CLP=0                  0
VI: OAM cells received                       0
VI: OAM cells transmitted                    0
VI: RM cells received                        0
VI: RM cells transmitted                     0
CGW: Packets Rx From Network                 0
CGW: Cells Tx to Line                        0
CGW: NIW Frms Relayed to Line                0
CGW: SIW Frms Relayed to Line                0
CGW: Aborted Frames Tx to Line               0
CGW: Dscd Pkts                               0
CGW: 0-Length Frms Rx from Network           0
CGW: Bd CRC16 Frms Rx from Network           0
CGW: Bd Length Frms Rx from Network          0
CGW: OAM RTD Cells Tx                        0
CGW: Packets Tx to Network                   0
CGW: Cells Rx from Line                      0
CGW: NIW Frms Relayed from Line              0
CGW: SIW Frms Relayed from Line              0
CGW: Aborted Frms Rx From Line               0
CGW: Dscd Cells                              0
CGW: 0-Lngth Frms Rx from Line               0
CGW: Bd CRC32 Frms Rx from Line              0
```

```
CGW: Bd Lngth Frms Rx from Line              0
CGW: OAM RTD Cells Rx                        0
CGW: OAM Invalid OAM Cells Rx                0
CF: Egress Packet Sequence Errs              0
CF: Egress Bad HEC from cellbus              0
CF: Egress Packets from cellbus              0
CF: Egress Cells Tx to Line                  0
CF: Ingress Packets to cellbus               0
CF: Ingress Cells from Line                  0
IE: Egress Packets to Extract Buf            0
IE: Egress Cells injected                    0
IE: Egress Packets Extract Buf full          0
IE: Ingress Cells to Extract Buf             0
IE: Ingress Packets injected                 0
IE: Ingress Cells Extract Buf full           0

Last Command: dsptrkstats 11.1


Next Command:
```

Table 4-69 dsptrkstats–Parameters

Parameter	Description
slot.port	Specifies the physical part of the logical trunk number.

Table 4-70 dsptrkstats–Optional Parameters

Parameter	Description
clear	Directs the system to clear the statistics counters.

Table 4-71 lists some trunk statistics provided in this release, along with the statistic type, card type, and line type for each statistic.

Table 4-71 Trunk Statistics Supported in Release 9.2

Statistic	Stat Type	Card Type	Line Type
Total Cells Received	Physical	UXM/BXM	All
Total Cells Transmitted	Logical	UXM/BXM	All
LOS transitions	Physical	UXM/BXM	All
LOF transitions	Physical	UXM/BXM	All
Line AIS transitions	Physical	UXM/BXM	T3/E3/SONET
Line RDI (Yellow) transitions	Physical	UXM/BXM	T3/E3/SONET
Uncorrectable HCS errors	Physical	UXM	T3/E3/SONET
Correctable HCS errors	Physical	UXM	T3/E3/SONET
HCS errors	Physical	BXM	T3/E3/SONET
Line Code Violations, ES, and SES	Physical	BXM	T3/E3
Line Parity (P-bit]) errors, ES, and SES	Physical	BXM	T3

Table 4-71 Trunk Statistics Supported in Release 9.2 (Continued)

Statistic	Stat Type	Card Type	Line Type
Path Parity (C-bit) errors, ES, and SES	Physical	BXM	T3
Far End Block Errors	Physical	BXM	T3
Framing Errors and SES	Physical	BXM	T3/E3
Unavailable Seconds	Physical	BXM	T3/E3
PLCP LOF and SES	Physical	BXM	T3
PLCP YEL	Physical	BXM	T3
PLCP BIP-8, ES, SES	Physical	BXM	T3
PLCP FEBE, ES, SES	Physical	BXM	T3
PLCP FOE, ES, SES	Physical	BXM	T3
PLCP UAS	Physical	BXM	T3
LOC errors	Physical	UXM/BXM	E3/SONET
LOP errors	Physical	UXM/BXM	SONET
Path AIS errors	Physical	UXM/BXM	SONET
Path RDI errors	Physical	UXM/BXM	SONET
Section BIP-8 counts, ES, and SES	Physical	UXM/BXM	SONET
Line BIP-24 counts, ES, and SES	Physical	UXM/BXM	SONET
Line FEBE counts, ES, and SES	Physical	UXM/BXM	SONET
Section SEFS	Physical	UXM/BXM	SONET
Line UAS and FarEnd UAS	Physical	UXM/BXM	SONET
Clock Loss Transitions	Physical	UXM	T1/E1
Frame Loss Transitions	Physical	UXM	T1/E1
Multiframe Loss	Physical	UXM	T1/E1
CRC errors	Physical	UXM	T1/E1
BPV	Physical	UXM	T1
Frame bit errors	Physical	UXM	E1
Unknown VPI/VCI count	Physical	UXM/BXM	All
Errored LPC cell count	Physical	UXM	All
Non-zero GFC cell count	Physical	UXM/BXM	
Max Differential Delay	Physical	UXM	T1/E1
Uncorrectable HEC errors	Physical	UXM	All
Cell Hunt count	Physical	UXM	T1/E1
Bandwidth Changed count	Physical	UXM	T1/E1
Receive CLP=0 cell count	Logical	UXM/BXM	All
Receive CLP=1 cell count	Logical	UXM/BXM	All
Receive CLP=0 cell discard	Logical	UXM/BXM	All
Receive CLP=1 cell discard	Logical	UXM/BXM	All
Transmit CLP=0 cell count	Logical	UXM/BXM	All

Table 4-71 Trunk Statistics Supported in Release 9.2 (Continued)

Statistic	Stat Type	Card Type	Line Type
Transmit CLP=1 cell count	Logical	UXM/BXM	All
Receive OAM cell count	Logical	UXM/BXM	All
Transmit OAM cell count	Logical	UXM/BXM	All
Receive RM cell count	Logical	UXM/BXM	All
Transmit RM cell count	Logical	UXM/BXM	All
For Each Traffic Type: (V, TS, NTS, ABR, VBR, CBR, BdatB, BdatA, HP)			
Cells served	Logical	UXM/BXM	All
Maximum Qbin depth	Logical	UXM/BXM	All
Cells discarded count	Logical	UXM/BXM	All

prtapsln

The **prtapsln** command prints the **dspapsln** screen, that is, the currently configured APS lines and their status.

Full Name

Prints **dspapsln** screen (currently configured APS lines and their status)

Syntax

printapsln

Related Commands

addapsln, delapsln, cnfapsln, cnfcdaps, dspapsln, dsplog, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	No	BPX	No

Example

`prtapsln`

System Response

No display produced.

prtnw

Prints the network topology table. Alarms print in a column, and added trunks (by **addtrk**) appear to the right to the node name. Each trunk entry shows the local back card slot number and the node name and back card slot number on the other end of the line. Note the following conventions:

- ~ indicates the trunk is a satellite line.
- Flashing entry indicates a failed line.
- Blinking node indicates a node is executing downloader software.

Parameters set Zero Coded Suppression (ZCS) display characteristics. ZCS writes a 1 over the least significant bit of any byte that contains 0s. The purpose is to ensure a minimum occurrence of 1s so that the receiving node can extract timing information. The **prtnw** command uses the same syntax and prints the same information as the **dspnw** command.

Full Name

Print network

Syntax

prtnw [+b | -b] [+z | -z]

Related Commands

dspnw

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

`prtnw`

Description

Print the network topology.

System Response

(No screen display appears—just a printout.)

Table 4-72 prtnw–Parameters

Parameter	Description
+b	Display only the lines that support bursty data.
-b	Display only the lines that do no support bursty data.
+z	Display only the lines that use ZCS encoding.

Parameter	Description
-z	Display only the lines that do not use ZCS encoding.

prttrkict

Prints the interface control template of a subrate trunk. For a list of configurable outputs and configuration steps, see the **cnftrkict** description. The printed information includes:

- Specified line.
- Associated leads and their status
- Whether output follows a local input
- Name of the local or remote input lead that the output lead follows

Full Name

Print trunk interface control template

Syntax

prttrkict <*line*>

Related Commands

dsptrkict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	IGX	Yes

Example 1

`prttrkict`

Description

Print network topology.

System Response

No screen display—just a printout.

Table 4-73 prttrkict–Parameters

Parameter	Description
line	Specifies the trunk interface control template.

prttrks

Prints the trunk configuration for the node. This command uses the same syntax and prints the same information as the **dsptrks** command. Configuration information for trunks includes the trunk number and the type of line (T3, E3, and so on). For trunks that have been added to the network with the **addtrk** command, the configuration information also includes the node name and trunk number at the other end of the line.

Note the following printout characteristics:

- Those trunks that show a "–" in the "Other End" column, have been *upped* with the **uptrk** command but not yet *added* with the **addtrk** command.
- The Other End column shows the node name and slot number of the other end of the trunk.
- Names of disabled trunk appear as light text in the printout.

Full Name

Print trunks

Syntax

prttrks

Related Commands

dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

`prttrks`

Description

Print trunk configuration for the node.

System Response

No screen display appears—just a printout.

switchapsln

The **switchapsln** command lets you control the APS switching interface. You use the **switchapsln** command, along with other APS commands such as **addapsln**, **delapsln**, **dspapsln**, **switchapsln**, and **cnfapsln** to configure and control a SONET APS (Automatic Protection Switching) line for a BXM OC-3 or OC-12 card. SONET APS is a standard that describes the switching of SONET lines from the active line to a standby line to provide hardware line redundancy.

Several options are available that determine the type of switch operation:

- *Clear*—clear user switch request. This option clears the last user switch request and sets the switching state machine to fully automatic hardware control.
- *Forced Switch (Working to Protection* or *Protection to Working)*—the forced switch forces hardware to switch to the standby line even if it is in alarm.
- *Manual Switch (Working to Protection* or *Protection to Working)*—the manual switch is lower priority than a forced switch and will only cause a switch if certain conditions are met.

Note It is recommended that you not use the *Manual Switch* option with Annex B configured when the BPX is connected to a third-party vendor's switch.

- *Lockout*—prevents switching from the working line to the protection line from taking place. A lockout request is cleared by a subsequent Clear request.
- *Service*—the service switch for the two-slot solution only. This request causes all lines to be forcibly switched to one back card so that the other card of the pair can be removed for service.

Be sure that the associated front card is active for the back card that is to remain in the rack. You may have to perform a **switchcdred** so that the back card to which the service switch switches has its associated front card active.

Note When Annex B is configured, **switchapsln** options will not be blocked at the command line interface.

Full Name

Controls APS switching interface.

Syntax

switchapsln <slot.port> <switchoption> [S]

Related Commands

cnfcdaps, addapsln, delapsln, dspapsln, switchapsln, cnfapsln

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	BPX	Yes

Example 1

switchapsln 2.1 1 S

Description

Controls the APS switching interface to configure and control SONET APS line switching from an active line to a standby line. Upon executing **switchapsln**, the **dspapsln** screen appears.

System Response

```
alexa       TRM    genre        BPX 8600        9.2       Sep. 9 1998      16:25 PDT

                           Active   Current Line   Current APS      last User
Work/Protect   Protocol    Line     Alarm Status   Alarm Status     Switch Request

2.1 3.1        1+1         PROT     OK             APS OK           Forced W->P

Command: switchapsln 2.1 3
```

Table 4-74 switchapsln Parameters

Parameter	Description	
slot.port	The working APS line to be switched	
	Switch Options	
	1. Clear	*Clear* clears the last user request, returns state back to working line, resets to all defaults, and sets BXM to fully automatic line control.
	2. Lockout	*Lockout of Protection*—Prevents specified APS pair from being switched to protection line. If protection line is already active, switch is made back to the working line. (For Annex B, the Working line is termed the “primary line”, and the Protection line is termed the “secondary line”.)
	3. Forced switch (working to protection line)	*Forced Working to Protection line switch*—If working line is active, switch is made to protection line unless the protection line is locked out or in the SF condition or Forced Switch is already in effect. Forces hardware to switch to the protection line even if it is in alarm.
	4. Forced switch (protection to working line)	*Forced Protection to Working line switch*—If Protection is active, switch is made to Working unless a request of equal or higher priority is in effect. P-->W switch applies only in the 1+1 architecture. If protection line is active, switch is made to working line unless a request of equal or higher priority is in effect.

Table 4-74 switchapsln Parameters (Continued)

Parameter	Description	
	5. Manual switch (working to protection line)	*Manual switch (Working to protection line)*—Switch from working to protection line unless a request of equal or higher priority is in effect. Will not switch if other line is in alarm. **Note** Not applicable to APS 1+1, Annex B.
	6. Manual switch (Protection to working line)	*Manual switch (Protection to Working line)* **Note** Not applicable to APS 1+1, Annex B.
S	If you enter S as an additional parameter, a service switch is performed for all ports on the card such that all lines are forcibly switched to one back card so that the other back card of the pair can be removed for service. Be sure that the associated front card is active for the back card that is to remain in the rack. You may have to perform a switchcdred command so that the back card that the service switch changes to has its associated front card active.	

uptrk

Activates (or "ups") a trunk and, if you include the optional *vtrk* parameter for applicable cards, activates the trunk as a virtual trunk. You also use uptrk to enable a feeder trunk on a port.

After you have upped the trunk but not yet added it, the trunk carries line signalling but does not yet carry live traffic. Before you add the trunk with **addtrk**, the node can monitor the trunk for reliability. Once a trunk has shown reliability and is ready to go into service, add the trunk to the network. If you need to take an active trunk out of service, use **dntrk**. The **dntrk** command causes the node to reroute any existing traffic if sufficient bandwidth is available.

The Ports and Trunks feature lets you configure multiple trunk lines and circuit lines on a single BXM or UXM card simultaneously. In previous releases, when a single port is upped as a trunk (by using the uptrk command), all the remaining ports on that card are treated as a trunk. Similarly, when you up a single port as a circuit line (by using the **upln** command), all the remaining ports on the card are treated as circuit line ports. This feature allows the BXM and UXM trunks to be trunk line cards as well as circuit line cards, and to allow trunks and circuit lines to coexist on these cards.

For example, assuming that a four-port BXM card is plugged into slot 11, you could do the following:

1. uptrk 11.1
2. upln 11.2
3. upln 11.3
4. uptrk 11.4

That is, you could up a trunk at port 1 on slot 11, up a line at port 2 of slot 11, up a line at port 3 of card slot 11, and also up a trunk at port 4 of card slot 11.

You can now mix physical and virtual trunk specifications. For example, after you up a trunk as a standard trunk, you can then add it as a virtual trunk when you execute **addtrunk**. Furthermore, if you want to change trunk types between standard and virtual, you must first down the trunk with **dntrk,** then up it as the new trunk type.

You cannot up a trunk if the required card is not available. Furthermore, if a trunk is executing self-test, a "card in test" message may appear on-screen. If this message appears, re-enter **uptrk**.

If, after upping a BXM trunk, you get a message telling you to use **cnfrsrc** to configure PVCs, make sure that when configuring resource partitions with **cnfrsrc**, you specify values greater than 0 for the Maximum PVC Channels, Maximum PVC Bandwidth, and Maximum VSI LCNs. Otherwise, you will be unable to create any PVCs on a BXM card. Also, you will not be able to change the Connection Channels amount with **cnftrk** if you do not first use **cnfrsrc** to configure PVCs.

In this release, to support the Multilevel Channels Statistics feature, you will be prompted when you attempt to up the line with upln or up the trunk with uptrk, warning you to initialize the channel statistics level before activating the card. This warning only applies when upping the first trunk or first line on the card:

```
"Channel Statistic Level must be initialized prior to card activation"
```

Configuring IMA Physical Lines

Release 9.1 supported a Cisco proprietary IMA (Inverse Multiplexing ATM) protocol on UXM trunks which was able to interoperate only with Cisco products, for example, MGX-8220 IMATM. Release 9.2 supports the ATM Forum compliant IMA protocol, which allows UXM trunks to interoperate with other vendor equipment. IMA provides inverse multiplexing of ATM cells across multiple physical lines. The ATM Forum compliant IMA protocol is supported only on UXM trunks.

The IMA protocol feature requires you to upgrade the UXM firmware to Model B. When you load Model B firmware onto a UXM card, all IMA trunks invoked on that card automatically perform ATM Forum compliant IMA protocol. You do not need to use any switch software commands to enable the IMA protocol. Note that switch software Release 9.2 is not set up to work with UXM Release 9.1 firmware, so it is advised that you *not* downgrade to Model A firmware, as the software will not work. (The UXM firmware code space is not large enough to hold both versions of the protocol in a single firmware image.)

Note also that the ATM Forum compliant IMA feature is not compatible with the Cisco proprietary IMA protocol supported in Release 9.1 (which uses UXM firmware Model A). Both ends of the UXM IMA trunk requires UXM firmware Model B. If the UXM trunk is connected to another device, that device must support the ATM Forum compliant IMA protocol.

Note Refer to 9.2 release notes for up-to-date feature support and system requirements.

Note that this release supports a subset of the ATM Forum compliant IMA protocol. These functions supported in Release 9.2:

- You can add and delete physical links while the IMA group is active.
- You can up an IMA group with a minimum number of retained links.
- New configurable link (**cnftrk**) parameters:
  - IMA Max. Differential Delay
  - IMA Protocol Option
  - IMA Clock Mode (this parameter is fixed and not configurable)
- Additional IMA group and individual physical link state and statistics can be collected.
- Allows non-consecutive physical links on the same card to be in the same IMA group. This is specific to the UXM card and is not specified as part of the ATM Forum compliant IMA standard.

Release 9.2 supports virtual trunking on both the BPX and IGX. IMA trunk ports are referenced by the first physical line of the trunk port after **uptrk** has been executed. For example, you can *uptrk 1.5–8.9*. You can then up a second trunk (which, in this case, is a virtual trunk on slot.port 1.5) on the same trunk port using *uptrk 1.5.11*.

This release supports using a UXM IMA trunk to connect an IGX feeder node to a routing node, either an IGX or a BPX using IMATM. UXM IMA provides redundancy in case one of the physical lines on an IMA trunk should fail. This reduces the chance of a single point of failure when a single feeder trunk is out of service. Also, you may configure the services on a feeder node rather than on a router node; this indirectly allows the network to scale better with respect to the limit of 223 network nodes.

Specifying an IMA Group Member

In Release 9.1, it was a requirement that the IMA group had to consist of consecutive physical lines. In this release, you can define an IMA trunk consisting of non-consecutive physical lines. In addition, you can change the group member by deleting a physical line from an existing IMA trunk.

Use the following syntax to specify an IMA group on a UXM trunk:

- **uptrk** *slot.group_member.vtrk*

  where:

slot is the slot number

group_member is a set of physical lines composing an IMA group. You can specify the member in an expression consisting of the primary link followed by a , or – and additional physical links.

vtrk is the optional virtual trunk number. If at least one virtual trunk already exists on this port, the you only have to specify the primary link as the group_member. In the case of adding a UXM IMA feeder trunk from an IGX routing node to an IGX feeder node, you will not know whether the trunk is a regular trunk or feeder trunk. There is no virtual trunk for the feeder.

For example, 9.1–4 defines trunk 9.1 to consist of four physical links, that is, 1, 2, 3 and 4, where physical link 1 is the primary link. (This example is compatible with Release 9.1.)

For example, 9.1–3,5 defines trunk 9.1 to consist of four physical links, that is, 1, 2, 3 and 5 where physical link 1 is the primary link.

For example, 9.5–7,2–3 defines trunk 9.5 to consist of five physical links, that is, 2, 3, 5, 6 and 7 where physical link 5 is the primary link.

Similarly, 9.8,2,4,6 defines trunk 9.8 to consist of all even number of physical links where physical link 8 is the primary link.

cnftrk is used to specify the primary link on the IMA trunk.

Primary Link—In an IMA group, you must select one of the physical links to be a primary link. This primary link number is used to refer to this IMA group or trunk. You can use **cnftrk** to add additional links to the group or delete existing links. When deleting existing links from an IMA group, you cannot delete the primary link. You must deactivate the trunk using **deltrk** followed by **dntrk** to remove the primary link. The **cnftrk** will be blocked after the trunk has been added as a feeder trunk.

Feature Mismatching on Virtual Trunks

The **uptrk** command, in addition to other configuration commands, will perform mismatch verification on the BXM and UXM cards. For example, the uptrk command will verify whether the card has virtual trunk support. Refer to the "Feature Mismatching" section on page 18-1 for more information on Feature Mismatching in Release 9.2.

The Feature Mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Full Name

Up trunk

Syntax

uptrk <slot.port>[.vtrk]

uptrk <slot.group_member.[<vtrk]> for IMA

uptrk <slot>.<group-member(s)>

Related Commands

addtrk, dntrk, cnfrsrc

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

`uptrk 21`

Description

Activate (up) trunk 21—a single-port card, in this case, so only the slot is necessary.

Example 2

`uptrk 6.1.1`

Description

Activate (up) trunk 6.1.1—in this case, a virtual trunk, as indicated by the third digit.

Example 3

`uptrk 4.1`

`uptrk 4.2`

`uptrk 4.3`

Description

On the BXM in slot 4, bring up the ports 4.1, 4.2, and 4.3.

Note The previous example enables ports 4.1, 4.2, and 4.3 in trunk mode with the uptrk command, they could also all be upped in port mode using the upport command. This is because label switching and the VSI make no distinction between a "port" and a "trunk".

System Response

```
n4           TN    SuperUser       BPX 15    9.2      Apr. 4 1998 16:39 PST

TRK     Type     Current Line Alarm Status              Other End
 2.1    OC-3      Clear - OK                             j4a/2.1
 3.1    E3       Clear - OK                             j6c(AXIS)
 5.1    E3       Clear - OK                             j6a/5.2
 5.2    E3       Clear - OK                             j3b/3
 5.3    E3       Clear - OK                             j5c(IPX/AF)
 6.1    T3       Clear - OK                             j4a/4.1
 6.2    T3       Clear - OK                             j3b/4
 4.1    OC-3      Clear - OK                             VSI(VSI)


Last Command: uptrk 4.1


Next Command:
```

Table 4-75 uptrk—Parameters

Parameter	Description
slot.port	Specifies the slot and port of the trunk to activate. If the card has only one port, the *port* parameter is not necessary. An NTM card, for example, has one port.
slot.group_member	Specifies the slot and a set of physical lines composing an IMA group on an IMA trunk to activate. You can specify the group_member in an expression consisting of the primary link followed by a , or – and additional physical links. (When specifying an IMA group, you must select one of the physical links to be a *primary link*. This primary link number is used to refer to this IMA group or trunk. You can use **cntrk** to add additional links to the group of delete existing links. When deleting existing links from an IMA group, you cannot delete the primary link. You must deactivate the trunk using **deltrk**, followed by **dntrk** to remove the primary link.

Table 4-76 uptrk—Optional Parameters

Parameter	Description
vtrk	Specifies the virtual trunk number. The maximum on a node is 32. The maximum on a T3 or E3 line is 32. The maximum for user traffic on an OC-3/STM1 trunk is 11 (so more than one OC-3/STM1 may be necessary). See also the “Event Logging” section on page 4-22 of this chapter. When specifying an IMA group, if at least one virtual trunk already exists on this port, then you only have to specify the primary link as the group_member.

Setting Up Lines

A circuit line is the physical line that carries data, voice, Frame Relay, or ATM traffic between an IGX or BPX node and customer premises equipment (CPE). Each piece of customer premises equipment is attached to a node through a circuit line. After a *card* has been “upped” with the **upcd** command, a *circuit line* on that card can be “upped” and configured.

This chapter:

- Describes input circuit line formats
- Summarizes circuit line card combinations
- Explains how to set up lines
- Describes each command

Note “Line” commands are the same as “circuit line” commands. However, the **cnfcln** command is no longer used; use **cnfln** instead. The switch software prompts for the parameters appropriate for the card type it detects.

The following table shows the permissible card combinations for CPE-to-IGX lines.

Table 5-1 Input Line Formats

Type	Country	Electrical Signal Format	Ones Density Enforcement	Multiplexing
J1	Japan	Coded Mark Inversion (CMI)		31 channels @ 64kbps each
E1	Others	Alternate Mark Inversion (AMI)	High density bipolar 3 (HDB3)	31 channels @ 64kbps each 1 E1 line on CDP/CVM, FRP/FRM 8 E1 lines on UFM
T1	USA Canada ASIA	Alternate Mark Inversion (AMI)	Bipolar Zero Substitution (B8ZS)	24 channels @ 64kbps each 1 T1 line on CDP/CVM, FRP/FRM 8 T1 lines on UFM
E3	Europe and others	Physical Layer Convergence Protocol per AT&T publication; ITU I-361 with HEC for E3	HDB3	ITU-T G.804, G.832
T3	USA Canada	Physical Layer Convergence Protocol per AT&T publication TA-TSY-00772 and 000773 for T3	B3ZS+	M13 mode

Table 5-2 Line Card Combinations

Service	Node Type	Front Card	Back Card
ATM	IGX	UXM	BC-UAI BC-UAI BC-UAI-1T1 BC-UAI-1E1 BC-UAI-1OC3
ATM	IGX	ALM/A	BC-UAI-1T3 BC-UAI-1E3
Frame Relay	IGX	UFM-4C, UFM-8C	UFI-8T1-DB15, UFI-8E1-DB15, UFI-8E1-BNC
Frame Relay	IGX	FRP-6, FRP-31/FRM-6, FRM-31	FRI-T1, FRI-E1
Frame Relay	IGX	UFM-C	UFI-8T1-DB15 UFI-8E1-DB15 or UFI-8E1-BNC
High Speed Data	IGX	SDP/HDM	SDI/RS-232 SDI/RS-422
High Speed Data	IGX	SDP/HDM	SDI/RS-232 SDI/RS-422
Voice	IGX	UVM	BC-UVI-2T1EC BC-UVI-2E1EC BC-UVI-2J1EC

Table 5-2 Line Card Combinations (Continued)

Service	Node Type	Front Card	Back Card
Voice	IGX	CDP/CVM	BC-T1 BC-E1 BC-J1

Setting Up a Circuit Line

Frame relay, data, and voice connections require an active line. Use the commands in the following steps to establish a line. The card must be in either the active or standby state before you enter these commands.

Step 1 Use **upln** to activate a circuit line in a slot that contains the appropriate circuit line card set.

Step 2 Use **cnfln** to configure the circuit line.

The **upln** and **cnfln** commands establish the general parameters for the line but do not establish specific Frame Relay, data, or voice parameters. Refer to applicable chapters for details on a particular service. For example, "Data Connections" describes specific commands for data connections, and "Frame Relay Connections" describes specific commands for Frame Relay connections.

Other Circuit Line Commands

The following describes related commands.

- **dnln**—downs a line. A downed line is inactive, so no signals or statistics are generated. You must remove all connections on a line (**delcon** or **delcongrp**) before you down the line with **dnln**.
- **dsplncnf**—displays the configuration of a specified circuit line.
- **dsplns**—displays the circuit line configuration and alarm status for the node.
- **prtlns**—prints the circuit line configuration and circuit line alarm status for the node.

Flow Diagrams for Line Setup

Figure 5-1, Figure 5-2, Figure 5-3, Figure 5-4, and Figure 5-5 show the command sequence for setting up lines for voice, serial data, Frame Relay, ATM, and FastPADs, respectively. A yes/no decision branch for "Other Side?" and the **vt** command in the sequence indicates command sequences on local and far nodes. "Multiplex" refers to channelized streams.

Figure 5-1 Setting Up Voice Lines

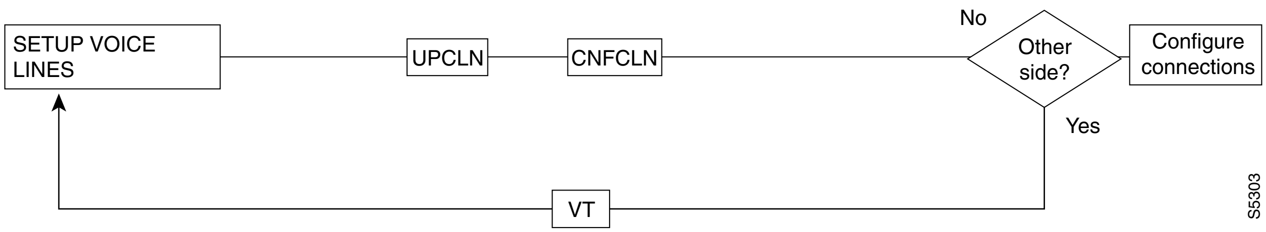


Figure 5-2 Setting Up Data Lines

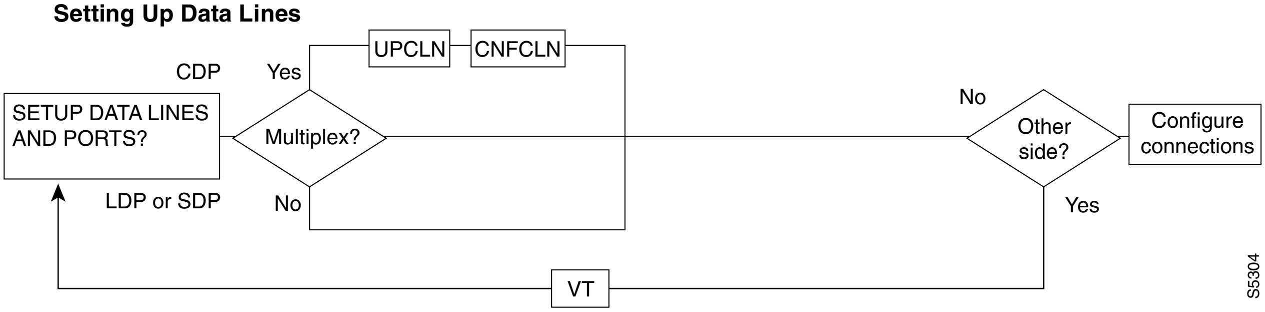


Figure 5-3 Setting Up Frame Relay Lines

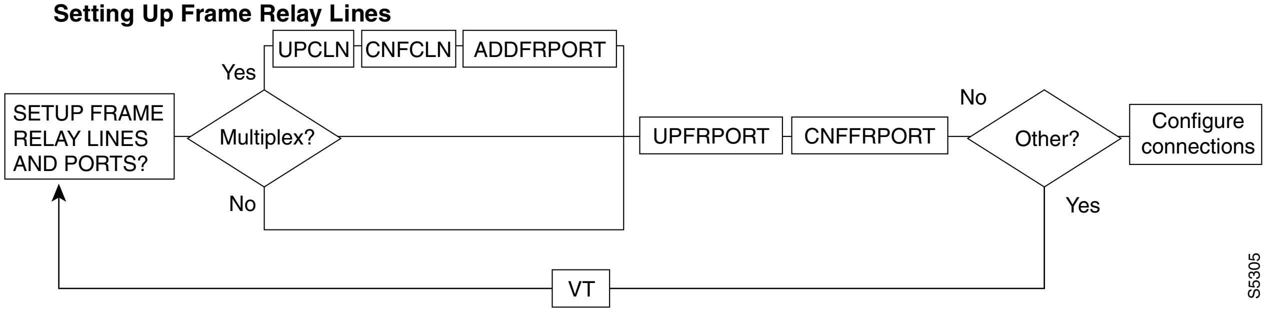
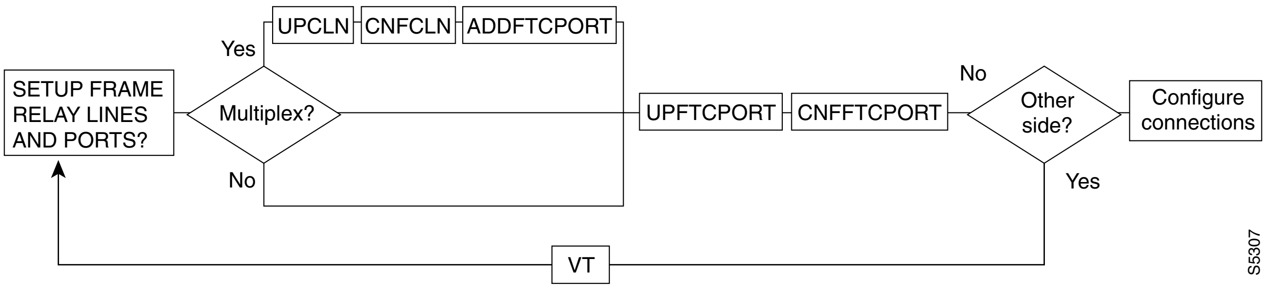


Figure 5-4 Setting Up ATM Lines

Figure 5-5 Setting Up FastPAD Lines



List of Commands

Table 5-3 shows the full command name and starting page for each line command description.

Table 5-3 Line Commands

Mnemonic	Description	Page
cnfcassw	Configure CAS switching	5-6
cnfln	Configure line (same as cnfcln)	5-8
cnfrsrc	Configure resources	5-15
dnln	Down line (same as dncln)	5-20
dsplncnf	Display line configuration (same as dspclncnf)	5-22
dsplns	Display lines (same as dspclns)	5-27
dsptsmap	Display time slot map	5-29
prtlns	Print circuit lines (same as prtclns)	5-31
upln	Up line (same as upcln)	5-32

cnfcassw

Configures a UVM to convert channel associated signaling (CAS) and dual-tone multi-frequency (DTMF) tones to common channel signaling (CCS) call control messages. This conversion is necessary for voice networks in which a Voice Network Switch (VNS) uses SVCs to route calls from a CAS-based PBX through a WAN. Model B or later firmware on the UVM is necessary.

Before you can execute **cnfcassw**, note the following:

- The line to which you apply **cnfcassw** must be up.
- If any connections exist on the line, you cannot change the **cnfcassw** parameters. However, you can execute the command to see the current parameters in the **cnfcassw** display.
- You cannot configure a line for both CAS-switching and pass-through.
- With CAS-switching on a UVM that has Y-cable redundancy, the call state of each connection is lost in the event of a switch-over.

Full Name

configure CAS switching

Syntax

cnfcassw <line> <mode> <CCS type> <CAS type> <conn type> <country code> <interdigit timeout> <tone level> <DTMF duration> <idle pattern> <*parameters 6–18*>

Note For the initial implementation of CAS switching, you should specify only port 1 for the *line* parameter (where *line* has the format *slot.port*) and select "PBX-end" for *mode*.

Related Commands

dspln, dsplncnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	Yes	IGX	Yes

Example 1

```
cnfcassw 5.1
```

Description

Configure port 1 of the UVM in slot 5 to support CAS switching.

System Response

```
sw175          TN    SuperUser       IGX 8420    9.2 Sep. 17 1998 06:11 PST

Line 5.1 CAS Switching Parameters
=> CASSW mode     [OFF]                   Parm 11       [00] (H)
   CCS Type       [ 1] (D)                Parm 12       [00] (H)
   CAS Type       [ 1] (D)                Parm 13       [00] (H)
   Conn Type      [a32   ]                Parm 14       [00] (H)
   Country code   [00] (H)                Parm 15       [00] (H)
   Interdigit TO  [05] (H)                Parm 16       [00] (H)
   Tone level     [00] (H)                Parm 17       [00] (H)
   DTMF duration  [0C] (H)                Parm 18       [00] (H)
   Idle pattern   [54] (H)
   Parm 6         [00] (H)
   Parm 7         [00] (H)
   Parm 8         [00] (H)
   Parm 9         [00] (H)
   Parm 10        [00] (H)

This Command: cnfcassw 5.1

Enter mode: Pbx/Server/Off (o):
```

Table 5-4 cnfcassw—Parameters

Parameter	Description	Default
line	Specifies the line in the format *slot.port*. The line must be up before you can execute *cnfcassw*.	
mode	Possible entries are "p" for PBX-end, "s" for server-end, or "o" for off. The applications are as follows: • PBX-end applies to a UVM connected to a PBX. Specify PBX-end mode if you plan to add the signaling channel (using **addcon**) at the UVM connected to the PBX (rather than the CVM or UVM connected to the VNS). • Server-end applies to a UVM connected to the VNS. Specify Server if you plan to add the signaling channel (using **addcon**) at the UVM connected to the VNS (rather than the PBX). • Off means the UVM is not in CAS-switching mode.	off
CCS type	The range of entries 1–4. A 1 selects Q.SIG.	1
CAS type	The range is 1–32. A 1 specifies AB signaling for 2-wire E&M line.	1
connection type	Specifies the type of voice connection. Valid entries are a32 and a24.	a32
country code	The range is 0–0xFF. A 0, for example is the U.S.	0
interdigit timeout	The range is 0–0xFF, where each hexadecimal value you enter is a multiplier of 50 millisecond increments.	05, which results in 250 ms.
tone level	Specifies the dB level of the DTMF below 0 dBm. The range is 0–0xFF.	00 for 0 dB
DTMF duration	Specifies the DTMF on/off duration. The range is 0–0xFF, and the value you enter is multiplied by 5 millisecond increments.	0C, which results in 60 ms on then 60 ms off.
idle pattern	Specifies the data pattern for the data channel. The range is 0–0xFF.	7F for T1, 54 for E1 line
parms 6–19	Parameters 6-18 are reserved for future use.	00

cnfln

Configures a line to be compatible with the device to which it connects. The **cnfln** command applies to voice, data, Frame Relay, and ATM lines. See Table 5-1 for a list of the front and matching back cards. Because of the variety of line types and characteristics, the parameters section of this description has three tables to describe the parameters. The system automatically presents the correct options on the command line for each line type. If a parameter is not applicable to a card type, the system displays the parameter in half-tone or the value field of that parameter with dashed lines. Table 5-4 describes the parameters for voice, data, and Frame Relay parameters. Table 5-5 describes the parameters for the ATM Line Module (ALM/A). Table 5-6 describes the parameters for the ASI line card (BPX node). Table 5-7 describes the ATM parameters for the UXM card (IGX node).

For an ALM/A, the **cnfln** command lets you configure the receive rate and header type and enable payload scrambling. For more details on the features and configurable parameters of the ALM/A, refer to the *Cisco IGX 8400 Series Reference* and the *Cisco IGX 8400 Series Installation* manuals. Note that, although the **cnfln** display shows the transmit rate, you cannot configure it because the ALM/A transmit rate is always the maximum line rate.

Note The **cnfln** command is the same as **cnfcln**.

Full Name

Configure line

Syntax

cnfln <line> <*parameters*>

Related Commands

dspln, dsplncnf, dsptsmap

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX, BPX	Yes

Example 1

```
cnfln 14
```

Description

Configure voice line 14.

System Response

```
alpha          TRM   YourID:1        IGX 8420      9.2    Aug. 23 1998 09:55 PST

CLN 14 Configuration   T1/24               CDP slot: 13
Loop clock:            --

Line framing:          --
     coding:           --
     CRC:              --
     recv impedance:   --
     E1 signalling:    --
     encoding:         --
     T1 signalling:    --
     cable type:       --
     length:           --
     56KBS Bit Pos:    --
     pct fast modem:   --

Last Command: cnfcln 14


Next Command:
```

Example 2

cnfcln 7 n 2

Description

Configure a Frame Relay T1 line for the following options: no loop clock and a receive impedance of 75 ohms.

System Response

```
alpha          TRM   YourID:1        IPX 16    9.2    Aug. 23 1997 09:55 PST

CLN 14 Configuration   T1/24 FRPslot: 13
Loop clock:            --

Line framing: ESF
     coding:          ZCS
     CRC:              --
     recv impedance:   --
     E1 signalling:    --
     encoding:         --
     T1 signalling:    --
     cable type:       ABAM
     length:          0-133 ft.
     56KBS Bit Pos:    --
     pct fast modem:   --


Last Command: cnfcln 7 n 2


Next Command:
```

Example 3

cnfln 4.2 7F 0 N

Description

Configure ASI port 4.2 with an idle code 7F and without payload scrambling.

System Response

```
ca19           VT    SuperUser       BPX 8620    9.2    Aug. 23 1998 19:11 GMT

LN   4.2 Configuration T3    [96000 cps]   ASI-T3 slot:4
Loop clock:           --                  Idle code:             7F hex

Line framing:         --
     coding:          --
     CRC:             --
     recv impedance:  --
     E1 signalling:   --
     encoding:        --                       cable type:
     T1 signalling:   --                       length:           0-450 ft.
                                          HCS Masking:           Yes
                                          Payload Scramble:      No
     56KBS Bit Pos:   --
     pct fast modem:  --


Last Command: cnfln 4.2 7F 0 N


Next Command:
```

Example 4

cnfln 12

Description

Configure the ALM/A in slot 12.

System Response

```
reach          TN    SuperUser       IGX 8420    9.2   July 22 1998 12:39 PDT

LN  12 Config        T3/3    [452   cps]    ALM slot: 12
Transmit Line Rate:  96000 cps
Receive Line Rate:   452 cps
Header Type:         VCC
Payload Scramble Yes











Last Command: cnfln 12 452 vcc y


Next Command:
```

Example 5

cnfln 10.1 N D4 ZCS AB 4 20 _

Description

Configure line 1 on the UVM in slot 10 with no loop clock, D4 framing, Zero Code Suppression coding, AB T1 signalling, and 20% expected channel utilization by a high speed modem.

System Response

```
sw176          TN    SuperUser       IGX 8420    9.2     Sep. 15 1998 13:37 PST

LN  10.1 Config      T1/24                UVM slot: 10
Loop clock:          No

Line framing:        D4                        cnfg:            External
     coding:         ZCS                           slot.line:  --
     CRC:            --                        CAS-switching: PBX-end
     recv impedance: --                        SVC-Caching  : On
  E1/J1 signalling:  --
     encoding:       u-law
     T1 signalling:  AB
     cable type:     ABAM
     length:         0-133 ft.
     56KBS Bit Pos:  msb
     pct fast modem: 20


This Command: cnfln 10.1 N D4 ZCS AB 4 20 _

Turn on SVC-Caching (Y):
```

This release has added a prompt to configure a UVM line for SVC Caching. It is also supported on CVM lines on the IPX. The SVC Caching feature speeds up call setup for most VNS controlled calls by avoiding some of the call setup/tear-down operations when a call originates or terminates.

Refer to the *VNS Installation and Configuration Manual* for more information on SVC Caching.

Table 5-5 cnfln—Voice, Frame Relay, or Data Parameters

Parameter	Description	Default
slot or slot.line	Specifies the line. If the back card has one line connector and cable, enter the slot number. If the card has more than one physical line, include a line number. If the card is a UVM, however, enter just the slot number.	
loop clock	Enables the transmit and receive control leads to use the same clock. Format for the parameter is Y or N	N
line framing	Configures T1 line framing to be D4 or ESF. Note that UFM-C series is ESF only.	D4 (ESF on UFM/FRM)
line coding	Configures T1 and E1 coding: T1:ZCS B8ZS AMI E1:HDB3 ZCS	ZCS B8ZS for FRM HDB3
line CRC on	Enables CRC-4 detection for E1 lines. Use either Y or N	N

Table 5-5 cnfln—Voice, Frame Relay, or Data Parameters (Continued)

Parameter	Description	Default
E1 recv impedance	Parameter Impedance Description 1 75 ohm unbalanced 2 75 ohm balanced 3 20 ohm balanced 4 0–133 ft ABAM cable 5 133–266 ft ABAM cable 6 266–399 ft ABAM cable 7 399–533 ft ABAM cable	1
signaling	E1:Common channel signaling (CCS) or ABCD signaling bits with channel associated signaling (CAS) T1:ABCD or ABAB (with ESF line framing) or AB (with D4 line framing); CCS is available in time slot 24 if applicable PBXs need it.	CAS AB
encoding	A-law µ-law	depends on the back card
cable type/length	ParameterVoice CircuitsFrame Relay Circuits 10-220 ft. MAT cableCSU Network Interface 2220-440 ft MAT cable0–133 ft ABAM cable 3440-655 ft MAT cable133–266 ft ABAM cable 40-133 ft ABAM cable266–399 ft ABAM cable 5133-266 ft ABAM cable399–533 ft ABAM cable 6266-399 ft ABAM cable533–655 ft ABAM cable 7399-533 ftnot used 8533-655 ftnot used	4
56kbs bit stuffing	most significant byte (msb) least significant byte (lsb)	msb
pct fast modem	Expected ADPCM fast connections (range 0-100). High speed modems preclude the use of ADPCM. Consequently, channel load requirements increase over that required for a voice channel. The pct fast modem parameters specify the expected channel utilization (%) by a high speed modem.	20

Table 5-6 cnfln—ATM (ALM/A) Parameters

Parameter	Description
line	Identifies the line. The line is the slot number of the ALM/A.
receive rate	Specifies the receive rate for the line. The range for a T3 line is 150 cells per second (cps) through 96000 cps. For an E3 line, the range is 150 cps–96000 cps.
header type	The header type is either VCC or VPC. The default is VCC. Refer to the IGX-related documentation for an explanation of the header type on the ALM/A.
payload scramble	Enables or disables payload scramble. The default is No.

Table 5-7 cnfln—ATM (ASI) Parameters

Parameter	Description			
line number	Specifies the ASI line to configure			
line options	Specifies the ATM line options:			
	Parameter	**Description**	**Options**	**Default**
	Loop clock	Enable loop clocking	Yes/No	No
	Idle Code	Hex data placed in unused payload of cells.	0 - FF (hex)	7F
	Cable Type/Length	Length and type of cable used for trunk.	1 = 0 - 225 2 = >225	1
	HCS Masking	Masking of cell header checksum to disable error checking.	Yes | No	Yes
	Payload Scramble	Whether or not to scramble (randomize) the cell payload data. Note: for E3, this must always be set to Yes.	Yes | No	No

Table 5-8 cnfln—ATM (UXM) Parameters

Parameter	Description			
slot.line	Specifies which line on which slot to configure			
line options	Specifies the ATM line options:			
	Parameter	**Description**	**Options**	**Default**
	Loop clock	Enable loop clocking	Yes/No	No
	Idle Code	Hex data placed in unused payload of cells.	0 - FF (hex)	7F
	HCS Masking	Masking of cell header checksum to disable error checking.	Yes | No	Yes
	Payload Scramble	Whether or not to scramble (randomize) the cell payload data. Note: for E3, this must always be set to Yes.	Yes | No	Yes
	Frame Scramble	Whether or not to scramble (randomize) the frame data. Note: for E3, this must always be set to Yes.	Yes | No	No
	Cell Framing	Choose the cell framing format. Select either STS-3C (SONET) or STM-1 (SDH).	STS-3C | STM-1 PLCP HEC	STS-3C for OC-3 PLCP for T3 HEC for E3

cnfrsrc

Use the **cnfrsrc** command to partition resources (ports and trunks) for Automatic Routing Management PVCs, VSI-MPLS (Multiprotocol Label Switching), or PNNI SVCs. To configure SVCs, an Extended Services Processor shelf must be configured in the BPX node. (If you want to configure resources for a VSI-MPLS controller or PNNI SVCs, refer to **cnfrsrc** in the "VSI Commands" chapter for more information specific to configuring VSI options.)

Note Note that VSI-MPLS is supported in this release. Up to two controllers of the same type can be attached to a node and assigned the same partition to provide controller redundancy on that partition. A different set of controllers can be attached to the node and be assigned a different partition to provide controller redundancy on this second partition.

You can configure a virtual trunk to be dedicated to VSI or to Automatic Routing Management. You cannot configure a virtual trunk for both VSI and Automatic Routing Management.

This command was introduced in Release 9.1 to support physical trunks. It has been extended to support virtual trunks. After VSI has been enabled, the virtual trunk becomes a "dedicated" VSI virtual trunk. Note that if the trunk has already been added or if the VPI value has not been configured, you will not be able to configure the VPI value. (Switch software will block you from doing so.)

Configurable resources (using **cnfrsrc**) are:

- Template number—only relevant when configuring VSI options
- Maximum PVC LCNs
- Maximum PVC Bandwidth
- Configure Partition (Y/N)—Enter "n" for No to configure Automatic Routing Management PVCs. Enter "y" for yes to configure VSI options.
- Partition ID
- Enable Partition (Enable/Disable)
- Minimum VSI LCNs
- Maximum VSI LCNs
- Start VSI VPI - **Warning message will tell you to use the cnftrk command**
- End VSI VPI - **Warning message will tell you that the end vsi vpi is equal to the start vsi vpi for virtual trunks**
- Minimum VSI Bandwidth
- Maximum VSI Bandwidth

The resources that you can currently configure are the number of connection IDs (conids) and the trunk bandwidth. You use the **cnfrsrc** command to configure the cell rate and number of connections on a BXM card only. (You cannot use the **cnfrsrc** command on the IGX.)

You configure all port and trunk attributes with **cnftrk**, **cnftrkparm**, or **cnfrsrc**. Note that when you change a physical port attribute, you will be notified that all the logical (physical and virtual) trunks on the port are affected.

Note Note that when using **cnfrsrc** to configure partition resources for Automatic Routing Management PVCs, and you are prompted whether you want to configure VSI options, enter "n" for No. You will not be prompted to enter any VSI options.

Full Name

Configure resource

Syntax

cnfrsrc <slot>.<port> <maxpvclcns> <maxpvcbw> <partition> <e/d> <minvsilcns> <maxvsilcns> <vsistartvpi> <vsiendvpi><vsiminbw> <vsimaxbw>

Related Commands

dsprsrc

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX (BXM cards only	No

Example 1

```
cnfrsrc 11.2 256 96000 y 1 e 0 0 1 1 0 0
```

Description

Configure resource partitions on card slot 11, port 2, to use Automatic Routing Management PVCs.

System Response

```
sw98              TN    SuperUser       BPX 8600    9.2.0r      Apr. 4 1998  16:40 PST

Port/Trunk : 11.2
Maximum PVC LCNS:             256     Maximum PVC Bandwidth:96000
Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1
Partition State :             Enabled
Minimum VSI LCNS:             0
Maximum VSI LCNS:             0
Start VSI VPI:                1
End VSI VPI :                 1
Minimum VSI Bandwidth :       0       Maximum VSI Bandwidth :        0

Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000

Next Command:
```

Table 5-9 cnfrsrc—Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Maximum PVC LCNs	The maximum number of LCNs allocated for Automatic Routing Management PVCs for this port. The range is 1 to 256. 256 is the default. For trunks, there are additional LCNs allocated for Automatic Routing Management that are not configurable. You can use the **dspcd** <slot> command to display the maximum number of LCNs you can configure using the **cnfrsrc** command for the given port. For trunks, “configurable LCNs” represent the LCNs remaining after the BCC has subtracted the “networking LCNs” needed. A trunk has 270 networking LCNs, or channels. For a port card, a larger number is shown, as compared with a trunk card. This is because a trunk uses 270 networking LCNs, as compared with a port card, which uses no networking LCNs. Setting this field to “0” would disable Automatic Routing Management PVCs on the specified port. Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management PVC connections on a BXM card. Also, if these parameters do not have values greater than 0, you will be unable to change the connection channel amount when you configure the BXM trunk using **cnftrk**.
Maximum PVC Bandwidth	Specifies the maximum bandwidth of the port allocated for Automatic Routing Management use. The range is 0 to 352207. 0 is the default. You can configure the Maximum PVC Bandwidth value for ports, but not for trunks. Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management PVCs on the BXM card.
Configure Partition	Answer yes or no to begin configuring resources for the partition. If you enter “n” for No, you will not be prompted to configure any VSI options. If you are configuring Automatic Routing Management PVCs, enter “n” for No. If you want to configure VSI options, enter “y” for yes, and you will be prompted to enter the rest of the **cnfrsrc** parameters, which are related to configuring VSI (such as a VSI MPLS controller or a PNNI controller). Refer to the **cnfrsrc** command in “VSI Commands” chapter for more information on VSI-related options.
Partition ID	Specifies the ID number of the partition. 1 is the default. Always use 1 in Release 9.1. In this release, you can use 2. (The range of 0 to 255.)
Enable Partition	Answer yes or no to enable your configured partition.

Table 5-9 cnfrsrc—Parameters (Continued)

Parameter	Description
Minimum VSI LCNs	The minimum number of LCNs guaranteed for this partition. The range is 1 to 256. 0 is the default. The VSI controller guarantees at least this many connection endpoints in the partition, provided there are sufficient free LCNs in the common pool to satisfy the request at the time the partition is added. When a new partition is added or the value is increased, it may be that existing connections have depleted the common pool so that there are not enough free LCNs to satisfy the request. The BXM gives priority to the request when LCNs are freed. The net effect is that the partition may not receive all the guaranteed LCNs (min LCNs) until other LCNs are returned to the common pool. You can increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. To avoid this deficit condition, which could occur with maximum LCN usage by a partition or partitions, it is recommended that all partitions be configured ahead of time before adding connections. Also, it is recommended that all partitions be configured before adding a VSI controller using the **addshelf** command.
Maximum VSI LCNs	The total number of LCNs the partition is allowed for setting up connections. The min LCNs is included in this calculation. If max LCNs equals min LCNs, then the max LCNs are guaranteed for this partition. Otherwise, (max - min) LCNs are allocated from the common pool on a FIFO basis. If the common pool is exhausted, new connection setup requests will be rejected for the partition, even though the maximum LCNs has not been reached. You may increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. Different types of BXM cards support different maximum values. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum value. Note that you must specify a value greater than 0 for the Maximum VSI LCNs, Maximum PVC Channels, and Maximum PVC Bandwidth parameters. Otherwise, you will not be able to add any connections on a BXM card.
Start VSI VPI	By default the TSC (for example, the 7200 or 7500 series router) will use either a starting VSI VPI of 1 or 2 for tag switching, whichever is available. If both are available, a starting VSI VPI of 1 is used. The VPI range should be 2-15 on a BPX 8620 VSI. The VSI range for tag switching on the BPX 8620 is configured as a VSI partition, usually VSI partition number 1. VSI VPI 1 is reserved for Automatic Routing Management PVCs. (This restriction applies only to trunks, not to ports. For a port, you can use any VPI value.) For a port UNI, the VPI range is 1 to 255. For a port NNI, the range is 1 to 4095. For trunks that do not have Automatic Routing Management configured, the VPI ranges are the same as for ports. The VSI partition for tag switching should start at VPI 2. If VPI 2 is not to be used, you can use the tag switching VPI interface configuration on the TSC to override the defaults. For trunks with Automatic Routing Management configured, the range is 2 to 4095. Always set to 2 for trunks.

Table 5-9 cnfrsrc—Parameters (Continued)

Parameter	Description
End VSI VPI	Two VPIs are sufficient for Release 9.1, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 2-15. The range is the <*Start VSI VPI* > value to 4095.
Minimum VSI Bandwidth	The minimum port bandwidth that can be used by this partition in cells/second. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.
Maximum VSI Bandwidth	The maximum port bandwidth that can be used by this partition. This value is used for VSI Qbin bandwidth scaling. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.

dnln

Deactivates (“downs”) a line. After **dnln** executes, the line no longer generates framing, and no statistics are gathered. Before you deactivate a line, use **delcon** to remove all connections on the line and use **dnport** to deactivate the port associated with the line.

Note The **dnln** command is the same as the **dncln** command.

Full Name

Down line

Syntax

dnln <line number>

Related Commands

upcln, dsplns, dsptsmap

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX, BPX	Yes

Example 1

```
dnln 12
```

Description

Deactivate line 12.

Table 5-10 dnln–Parameters

Parameter	Description
line number	Specifies the line. If the back card has one line, enter the slot number. If the card has more than one line, include a line number.

Example 2

```
dnln 3.12
```

Description 2

Deactivate line 12 on slot 3.

Table 5-11 dnln—Parameters for UXM

Parameter	Description
slot.line number	Specifies the slot and line to down on the UXM.

dsplncnf

Displays the configuration of a line. Table 5-11 shows all possible parameters in the display. The fields that actually contain data depend on the type of line.

Table 5-12 Possible Line Configuration Parameters

Screen Item	Description	Options
LN configuration	Line type and the number of channels.	T1 E1
Loop clock	Specifies whether the receive clock is looped back to the transmit clock.	Y N
Line framing	Identifies the type of line framing used by the circuit line.	DS4 for T1 ESF for T1 PLCP for T3/E3 HEC for T3/E3 STS-SC for OC-3 STM-1 for OC-3
Line coding	Identifies the line coding used by the circuit line.	E1:HDB3, AMI T1:ZCS, B8ZS, AMI
CRC	Specifies the CRC checking on E1 lines	Y N
recv impedance	Nominal impedance for the receive line.	75 ohms balanced or unbalanced 120 ohms balanced
E1 signaling	Identifies the signaling type used for E1.	CCS or ABCD with CAS
encoding	Specifies the voice encoding scheme	µlaw Alaw
T1 signaling	Identifies the signaling type used for T1	ABCD or ABAB (with ESF line framing) or AB (with D4 line framing); CCS is available in timeslot 24 if applicable PBXs need it.
56 kbps Bit Pos:	Position in word for bit stuffing on 56 kbs data channels.	MSB or LSB
Pct fast modem		
Cable type	Specifies the T1 or E1 cable type (used for equalization)	MAT ABAM
Cable length	Specifies the T1 or E1 cable length in feet to the CSU or digital cross-connect.	0–220220–440440–655 0–133133–262262–393 393–524524–655 T3/E3 = 0-255 ft.|greater than 255 ft.
Cnfg	Applies to the UVM: cnfg shows the mode of an individual UVM port. The *slot.line* identifies the line.	External, Passing, Blocked, or Inserting See the UVM documentation in the *Cisco IGX 8400 Series Reference* for a description of these modes.
Transmit Line Rate	Applies to ATM line cards: the display shows the transmit line rate (the direction is away from the node).	The value is always the maximum for the line and is in cells per second (cps): 96000 cps for T3, 80000 cps for E3, or 353208 cps for OC-3.

Table 5-12 Possible Line Configuration Parameters (Continued)

Screen Item	Description	Options
Receive Line Rate	Applies to ATM line cards: the display shows the user-configured receive line rate (the direction is towards the node).	The value is in cells per second (cps). The range is 150–9600 cps for T3, 150–80000 cps for E3, or 353208 cps for OC-3.
Header Type	Applies to ATM cards: the display shows the user-specified header type.	The header type is VCC or VPC.
Payload Scramble	Applies to ATM cards: the display shows whether payload scramble is on.	The display shows "Yes" or "No."

Full Name

Display line configuration

Syntax

dsplncnf <line number>

Related Commands

cnfln (obsolete name: **cnfcln**)

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX, BPX	o

Example 1

```
dsplncnf 5.1
```

Description

Displays configuration for line 1 of the UVM in slot 5. The "cnfg" field shows "External," so all DS0s terminate on line 1. Also, CAS switching is off, and SVC caching is on.

System Response

```
sw175          TN    SuperUser       IGX 8420    9.2 Sep. 17 1998 23:28 PST

LN   5.1 Config      E1/30                  UVM slot: 5
Loop clock:          No

Line framing:        On                              cnfg:            External
     coding:         HDB3                                slot.line:  --
     CRC:            No                              CAS-Switching:   Off
     recv impedance: 75 ohm + gnd                    SVC-Caching  :   On

  E1/J1 signalling:  CAS
     encoding:       A-LAW
     T1 signalling:  --
     cable type:     --
     length:         --
     56KBS Bit Pos:  msb
     pct fast modem: 20

Last Command: dspclncnf 5.1

Next Command:
```

Example 2

dsplncnf 13

Description

Display the configuration of the line card in slot 13. The card in slot 13 is an ALM/A.

System Response

```
sw142          TN    SuperUser       IGX 16    9.1 July 31 1997 12:01 PDT

LN  13 Config        T3/1    [150   cps]    ALM slot: 13
Transmit Line Rate:  96000 cps
Receive Line Rate:   150 cps
Header Type:         VCC
Payload Scramble:    No









Last Command: dsplncnf 13


Next Command:
```

Example 3

dsplncnf 12.1

Description

Display the line configuration for 12.1. The card is slot 12 is an ASI in a BPX node.

System Response

```
ca20          LAN   SuperUser       BPX 8620    9.2   Aug. 23 1998 10:35 PST

LN  12.1 Configuration T3    [96000 cps]   ASI-T3 slot:12
Loop clock:            --                  Idle code:             7F hex

Line framing:          --
     coding:           --
     CRC:              --
     recv impedance:   --
     E1 signalling:    --
     encoding:         --                       cable type:
     T1 signalling:    --                       length:           0-450 ft.
                                           HCS Masking:           Yes
                                           Payload Scramble:      No
     56KBS Bit Pos:    --
     pct fast modem:   --


Last Command: dsplncnf 12.1


Next Command:
```

Example 4

`dsplncnf 7.1`

Description

Displays configuration for line 1 of the UXM OC-3 card set in slot 7.

System Response

```
sw224          TN    SuperUser       IGX 16    9.0.n2    Aug. 27 1997 16:09 GMT

LN   7.1 Config       OC-3                 UXM slot: 7
Loop clock:           No
Idle code:            7F hex
HCS Masking:          Yes
Payload Scramble:     Yes
Frame Scramble:       Yes
Cell Framing:         STS-3C









Last Command: dsplncnf 7.1
```

Table 5-13 dsplncnf—Parameters

Parameter	Description
line number	Identifies the line in the format *slot* or *slot.line*. If the back card has one line connector and cable, enter the slot number. If the card has more than one physical line, such as a UXM, enter a slot and line number. In the case of a UVM, however, enter just the slot number.

dsplns

Displays basic configuration and status information for all the lines on the node. The information includes the line number, the type of line, and the line alarm status. The line type shows whether the line is J1, T3, E3, T1, E1, or OC-3 and shows the number of configured DS0s. *Line* alarm *status* categories include:

- Clear—Line OK
- Loss of Signal
- Out of Frame
- Minor—Bad clock source
- Alarm Information Signal
- Remote Out of Frame
- Remote Out of Packet Frame
- Loss of Multiframe

Full Name

display lines

Note The **dspclns** command is the same as the **dsplns** command.

Syntax

dspclns

Related Commands

dncln, dsptrks, upcln

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX, BPX	No

Example

`dsplns`

Description

Display circuit lines on the node.

System Response

```
sw109          VT    SuperUser       IGX 8420    9.2 Aug. 20 1998 18:40 PST

Line Type      Current Line Alarm Status
 3   T1/24     Clear - OK
 5.1 E1/30     Clear - OK
 5.2 E1/30     Clear - OK
 5.3 E1/30     Clear - OK
 5.7 E1/30     Clear - OK
 5.8 E1/30     Clear - OK
 7.1 T1/24     Clear - OK
11   E1/30     Clear - OK







Last Command: dsplns


Next Command:
```

dsptsmap

Use the **dsptsmap** command to display the channel to time slot mapping usage information on a UVM card on an IGX node or a CDP/CVM card on an IPX node. The **dsptsmap** command is for use with the SVC caching feature which speeds up call setup for most VNS controlled calls. The SVC caching feature avoids some of the call setup/tear-down operations associated with **addcon** and **delcon** as a call originates or terminates. The SVC caching feature reduces the connect time for many switch calls over a busy network.

To use the **dsptsmap** command, the line must have SVC caching enabled on it. You can find out if a channel is disabled by using the **dsptsmap** command.

The **cnfln** command is used to configure the SVC caching parameter setting.

The **dspcons** command is used to view disabled connections provided the SVC has not been deleted.

The **dsplncnf** command will show the value (On/Off) of the SVC caching mode feature.

Refer to the *VNS Installation and Configuration Manual* for more information on SVC caching.

Full Name

Display the channel to time slot mapping usage for a UVM on an IGX node.

Note The **dspclns** command is the same as the **dsplns** command.

Syntax

dsptsmap <line_number>[update_interval]

Related Commands

cnfuiparm, cnfln, cnfupcln, dncln, dsptrks, dspln, dsplncnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX	No

Example

dsptsmap 7.2

Description

Display channel to time slot mapping for a specified line.

Table 5-14 dsptsmap—Parameters

Parameter	Description
line_number	*slot.line* for UVM or line for CVM/CDP

Table 5-14 dsptsmap—Parameters (Continued)

Parameter	Description
interval_number	Interval in seconds between screen updates. The default value is controlled by “Screen Update Time” in the **cnfuiparm** command.

Example

dsptsmap 9 1

Description

Enabled channels are shown on the screen underlined and in reverse video. Disabled (cached) channels are shown with the channel number underlined and in reverse video, while the time slot is shown in normal video. Channels that have no connection are shown in normal video for both channel number and time slot.

For example:

— Channel 1 does not have a connection.

— Channel 2 is an enabled connection carrying traffic.

— Channel 3 is a disabled connection.

Specify the *line_number* parameter in *slot.line* format for UVM, and *line* format for CDP/CVM.

Use the optional *update_interval* parameter to control how often the screen gets updated. If you do not enter any value through the CLI, the value of the “Screen Update Time” parameter set using in the **cnfuiparm** command is used.

System Response

```
sw176        TRM   StrataCom       IGX 16    9.1.0     Sep. 5 1997 11:00 PST

Line 7.2 Channel to Timeslot Map

Chan  TS       Chan  TS       Chan  TS       Chan  TS
--------       --------       --------       --------
 1     1        9    14       17    17
 2     2       10    12       18     5
 3    22       11    18       19    19
 4     5       12    10       20    20
 5    11       13    13       21    21
 6     6       14     9       22     3
 7     7       15    15       23    23
 8     8       16     9       24    24


This Command: dsptsmap 7.2

Hit DEL key to quit:
```

prtlns

Prints the current line configuration and line alarm status for a node. This command uses the same syntax, and prints the same information as is displayed using the **dsplns** command. See the **dspclns** command for syntax and output information.

Full Name

print line configuration

Syntax

prtlns

Related Commands

dsplns

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example

`prtlns`

Description

This command uses the same syntax and prints the same information as is displayed using the **dsplns** command. See the **dsplns** command for syntax and output information.

upln

Activates (ups) a line. Use the **upln** command to make the line available for configuring and to start statistics gathering.

You must activate ports at both ends of the line by executing the **upport** command before running **upln**. You must execute **upln** at both ends of the line. Executing **upln** at only one end of the line eventually causes an alarm. Once both ends of the line are active, you can add connections with the **addcon** command or optionally configure the line's signal characteristics for the data you intend for the line. See **cnfln** for information on defining the line characteristics.

A line consists of a cable for transmitting data and the interface circuitry for the line. The cable can be a coaxial wire, fiber optic, or a twisted pair. See Table 5-1 for information on card combinations.

The Ports and Trunks feature lets you configure multiple trunk lines and circuit line cards on a single BXM or UXM card simultaneously. In previous releases, when a single port is upped as a trunk (by using the **uptrk** command), all the remaining ports on that card are treated as a trunk. Similarly, when you upped a single port as a circuit line (by using the **upln** command), all the remaining ports on the card are treated as circuit line ports.

The Ports and Trunks feature lets you configure multiple trunk lines and circuit lines on a single BXM or UXM card simultaneously. In previous releases, when a single port is upped as a trunk (by using the **uptrk** command), all the remaining ports on that card are treated as a trunk. Similarly, when you up a single port as a circuit line (by using the **upln** command), all the remaining ports on the card are treated as circuit line ports. This feature allows the BXM and UXM trunks to be trunk line cards as well as circuit line cards, and to allow trunks and circuit lines to coexist on these cards.

For example, assuming that a four-port BXM card is plugged into slot 11, you could do the following:

1. **uptrk** 11.1
2. **upln** 11.2
3. **upln** 11.3
4. **uptrk** 11.4

That is, you could up a trunk at port 1 on slot 11, up a line at port 2 of slot 11, up a line at port 3 of card slot 11, and also up a trunk at port 4 of card slot 11.

In Release 9.2, the BXM or UXM card can be a trunk card and a line (port) card at the same time. For example, a BXM slot can up port 1 as a trunk interface while upping port 2 as a line interface.

Multi-Level Channels Statistics Feature Support in Release 9.2

To support the Multi-Level Channels Statistics feature, you will be prompted when you attempt to up the line with **upln** or up the trunk with **uptrk**, warning you that you must initialize the channel statistics level before the card will be activated. This warning applies only when upping the first trunk or first line on the card.

```
Channel Statistic Level must be initialized prior to card activation
```

Note If, after upping a BXM line, you get a message telling you to use **cnfrsrc** to configure PVCs, make sure that when configuring resource partitions with **cnfrsrc**, you specify values greater than 0 for the Maximum PVC Channels, Maximum PVC Bandwidth, and Maximum VSI LCNs. Otherwise, you will be unable to create any AutoRoute PVCs on a BXM card. You also will not be able to change the Connection Channels amount with **cnftrk** if these parameters' values are not set to values greater than 0.

Note The **upln** command is the same as **upcln**.

Full Name
Up line

Syntax
upln <line number>

Related Commands
cnfcln, dsplns, dspln, dncln

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX, BPX	Yes

Example 1
`upln 4.2`

Description
Activate line 4.2. After this command executes, the system displays the status of the line using the same information as **dsplns** displays.

System Response

```
ca19           VT    SuperUser       BPX 8620    9.2    Aug. 23 1998 19:08 GMT

Line Type      Current Line Alarm Status
 4.1 T3        Clear - OK
 4.2 T3        Clear - OK










Last Command: upln 4.2


Next Command:
```

Table 5-15 upln—Parameters

Parameter	Description
line number	Identifies the line number in the form *slot* for a single-line card or *slot.port* for a card with more than one line.

Example 2

upln 3.2

Description 2: Upping a Line on a UXM

Activate line 2 on slot 3. After this command executes, the system displays the status of the line using the same information as **dsplns** displays.

Table 5-16 upln–Parameters for UXM

Parameter	Description
slot.line number	Specifies the slot and line to up on the UXM. There can be no more than sixty four (64) lines per node. The upln command will be rejected if all sixty four lines have already been upped.

Voice Connections

The voice commands apply to setting up and configuring, and statistical reporting for voice connections (including FAX). In addition to the command descriptions, this chapter describes how to add a voice connection, configure card redundancy, and optimize the use of voice activity detection (VAD). A list of the commands that let you modify most characteristics of voice and data connections also appears at the front of the chapter. Use this list as a guideline for building voice service.

Voice connections exist as ports on circuit lines that are supported by a Channelized Voice Module (CVM) or Universal Voice Module (UVM) in an IGX node. The back card for the CDP or CVM is either a BC-T1, BC-E1, or BC-J1. For the UVM, the back card is either a BC-UVI-2T1EC, a BC-UVI-2J1EC, or BC-UVI-2E1EC.

Setting Up a Voice Connection

The following steps describe how to set up a voice connection.

Step 1 Configure the voice channel at each end of the connection. The associated commands are:

- **upln** Use **upln** to activate the line.
- **cnfcassw** If the UVM must convert CAS/DTMF to CCS signaling for a Voice Network Switch (VNS), use **cnfcassw** to configure the UVM for CAS switching. For CAS switching, the minimum UVM firmware level is B. Note that CAS switching is incompatible with passthrough. Before you use **addcon** to add signaling channels (to *slot.port*.24 or *slot.port*.16 for T1 or E1, respectively), specify “PBX-end” mode with **cnfcassw**.
- **cnflnpass** For a UVM intended to carry voice traffic with low delay code-excited linear predictive coding (LDCELP) or conjugative algebraic code-excited linear predictive coding (CACELP) per G.729, use **cnflnpass** to configure the UVM lines for the *passthrough* feature. Refer to the *Cisco IGX Reference* for a description of passthrough. Before you can execute **cnflnpass**, you must activate (**upln**) and configure (**cnfln**) the lines. Note that passthrough is incompatible with CAS-switching.
- **cnfchadv** Configures the channel for adaptive voice (ADV). This command enables or disables adaptive voice compression for one or more voice channels. The feature must be configured at both ends of the channel.
- **cnfchdl** Configures a channel’s dial-type. The options are inband, pulse, and user-configured.
- **cnfchec** Configure the echo canceller for the channel. The command enables or disables the echo canceller for a range of voice channel, sets the echo return loss to high or low and enables/disables the tone disabler, convergence, and non-linear processing.
- **cnfchgn** Configures the amount of gain inserted in a voice channel.
- **cnfcond** Configures a conditioning template for the channel.
- **cnfrcvsig** Configures receive signaling for the channel.
- **cnfxmtsig** Configures transmit signaling for the channel.
- **cnfvchtp** Configures a voice interface type for the channel.
- **cnfchutl** Configures channel utilization (see “Optimizing Traffic Routing and Bandwidth” chapter).
- **addyred** Enables voice channel redundancy.
- **dsplncnf** Use **dsplncnf** to make sure you have correctly configured the line.

Step 2 Add the connections with the **addcon** command. You must complete the appropriate steps at each end by using the commands in the preceding list before you add connections.

Configuring Voice Channel Redundancy

You can configure voice cards for redundancy by installing two identical card sets in adjacent slots and connecting them to the CPE through a Y-cable. Configure redundancy by using **addyred**. Note that a switch to a standby UVM that has active CAS-switching causes the loss of all call states.

Using VAD and Configuring Voice Channel Utilization

The bandwidth savings you gain by using VAD are less than optimal if you do not set the utilization of the voice channels to a reasonable value. To configure the utilization, use the **cnfchutl** command.

Summary of Commands

Table 6-1 shows the command name and starting page for the description of each command.

Table 6-1 Voice Connection Commands

Command	Full Name	Page
addcon	Add connection	6-4
cnfchadv	Configure channel adaptive voice	6-8
cnfchdl	Configure channel dial type	6-10
cnfchec	Configure channel echo canceller	6-13
cnfchfax	Configure fax modem detection for channels (UVM)	6-16
cnfchgn	Configure channel gain insertion	6-18
cnfcond	Configure conditioning template	6-20
cnfdch	Configure data connection to have idle code suppression enabled/disabled	6-22
cnflnpass	Configure line pass	6-22
cnfrcvsig	Configure receive signaling	6-24
cnfvchtp	Configure voice channel interface type	6-26
cnfxmtsig	Configure transmit signaling	6-30
delcon	Delete connection	6-32
dspchcnf	Display channel configuration	6-34
dspchdlcnf	Display channel dial type configuration	6-36
dspchec	Display channel echo canceller	6-38
dspcon	Display connection	6-40
dspcond	Display conditioning template	6-42
dspcons	Display connections	6-44
dspconst	Display connection state	6-48
dspsigqual	Display signal qualifiers	6-50
dspsvcst	Display voice SVC statistics	6-54
prtchcnf	Print channel configuration	6-55
prtchdlcnf	Print dial type configuration	6-56
prtcons	Print connections	6-57

addcon

Establishes the channel connections between nodes in the network. You can add voice connections to any slot that has a CDP, UVM, or CVM. Before you add a connection, determine its compression type.

If you plan for a port on a UVM to carry more than 16 channels with LDCELP or the G.729 version of CACELP, you must have a second, connected UVM and configure the resultant pair of UVMs for passthrough operation. If you attempt to add more than 16 LDCELP or G.729 channels, the system reports any excess connections as being failed connections after **addcon** execution finishes. Furthermore, if you execute **dspcon**, the status display for the excess connections shows "ConnRJ" (connection rejected). Refer to the **cnflnpass** description in this chapter and the UVM description in the *Cisco IGX Reference* for a description of passthrough.

After you have established passthrough for a pair of UVM card sets, the system does not allow duplication of channel numbers when you add connections. For example, if you add 7.1.1-16, the node does not allow you to add 8.1.1-8 if you have linked the UVMs by using **cnflnpass**. Instead, you would add 8.1.17-24.

A UVM with Model B or higher firmware supports CAS switching. Before you can add connections in a network with CAS switching, you must configure the UVM for this feature with the **cnfcassw** command. Note that, for CAS switching, you use **addcon** to add the signaling channels at the near and far end in the format *slot.port*.24 on a T1 line and *slot.port*.16 on an E1 line. Also, the connection *type* for these signaling channels is "t." If you specify D-channel compression, the connection type is "td." See the description of **cnfcassw** in the "Setting Up Lines" chapter or, for a more detailed description, the manual titled *Cisco VNS (Voice Network Switching) Installation and Operation*.

When adding a range of channels, you do not have to specify the full channel set at the near-end. You may specify only the first channel in the set. For example, to connect channels 13.1-10 at alpha to channels 12.5-14 at beta, you could enter "**addcon** 13.1-10 beta 12.5." In this example, channel 13.1 is connected to channel 12.5, and channel 13.2 is connected to channel 12.6, and so on.

Connections are added with a default *class of service* (COS). The value of COS is the number of seconds that the node waits before it reroutes the connection after a failure. The COS applies to various types of connections other than voice and therefore is described elsewhere (see the **cnfcos** description in the "Optimizing Traffic Routing and Bandwidth" chapter.)

Table 6-2 describes what you enter for the *type* parameter for each rate and compression variable.

Table 6-2 Types of CDP and CVM Operation

Rate	VAD	No VAD	Comment
64 Kbps	v	p	
32 Kbps	c32	a32	
32 Kbps for FAX	c32d	a32d	Specifies 32 Kbps specially optimized for FAX. c32d incorporates Voice Activity Detection (VAD).
24 Kbps ADPCM	c24	a24	
16 Kbps no ZCS	c16z	a16z	For non-ZCS only.
16 Kbps	c16	a16	ZCS is permissible. c16 and a16 use non-standard compression algorithms.

Table 6-3 Types of UVM Operation

Rate	VAD	No VAD	Comment
64 Kbps	v	p, t	Pass-through does not accept t-type connections.
32 Kbps	c32	a32	
24 Kbps ADPCM	c24	a24	
16 Kbps no ZCS	l16V	l16	For non-ZCS only.
8 Kbps	g729r8v g729ar8v	g7298 g729ar8	The UVM supports two forms of CACELP. Both versions can support VAD (or no VAD). The "a" indicates G.729A. The other version is G.729.

Table 6-4 Types of UVM Connections

p	A p-connection carries 64 Kbps PCM voice and supports A-law or µ-law encoding and conversion, gain adjustment, and signaling.
t	A t-connection carries 64 Kbps clear channel data traffic.
td	A td-connection carries compressed, 16-Kbps signaling between an IGX node and VNS unit.
v	A v-connection is the same as "p" (above) but with VAD.
a32 a24	Specifies ADPCM only. You can specify 32-Kbps or 24-Kbps.
c32 c24	Specifies both ADPCM and VAD. You can specify 32-Kbps or 24-Kbps.
l16	LDCELP compression of voice to 16 Kbps.
l16v	LDCELP compression of voice to 16 Kbps with VAD.
g729r8	CACELP voice compression at 8 Kbps according to G.729. This type also supports automatic FAX and modem upgrade.
g729r8v	CACELP voice compression at 8 Kbps with VAD according to G.729.
g729ar8	CACELP voice compression at 8 Kbps according to G.729A.
g729ar8v	CACELP voice compression at 8 Kbps with VAD according to G.729A.

The difference between a PCM (p) connection and a transparent (t) or transparent D-compression (td) connection is that the D4 frame signaling bits are identified and processed as signaling information with PCM connections. PCM connections permit gain adjustment to be applied to the connection. Transparent connections treat all bits, including signaling bits, as data bits and disables any gain adjustment conversion that you may have specified.

The *number* in the type field indicates the ADPCM rates in Kbps. The "z" suffix indicates that 00 code level is used. Type a16 or c16 uses only 01, 10, and 11 binary codes to avoid long strings of zeros. Type a16z and c16z connections use the 00 code and are automatically configured to avoid ZCS lines (*Z).

Full Name

Add connection

Syntax

addcon <local channel> <remote node> <remote channel> <type> [avoid]

Related Commands

delcon, dncon, dspcon, dspcons, cnfcos

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
1–2	Yes	Yes	IGX	Yes

Example 1

`addcon 7.2 beta 8.2 v`

Description

Add a “v” type voice connection. This command connects channel 7.2 on node alpha to channel 8.2 on node beta. A prompt appears asking you to confirm the proposed connections.

Connection type is “v,” “class of service” (COS) is “2,” compression is VAD, and ownership is local. For an explanation of COS, see the **cnfcos** description in the “Optimizing Traffic Routing and Bandwidth” chapter. Because you are entering the **addcon** command at node alpha, the node alpha is the owner of the connection.

System Response

```
alpha          TRM   YourID:1        IPX 16    9.1    Aug. 16 1997 09:37 PST

 Local      Remote      Remote                                Route
 Channel    NodeName    Channel    State  Type    Compression Avoid COS
 7.2        beta        8.2        Ok     v       VAD         L     2








Last Command: addcon 7.2 beta 8.2 v


Next Command:
```

Table 6-5 addcon—Parameters

Parameter	Description
local channel	Specifies the local channel or set of channels to add. Right-angle brackets indicate a range of channels. Channel specification on a UVM has one more parameter than the specification on a CDP or CVM, as follows: For a CDP or CVM, the format for channel specification is *slot.chan*[–*chan*]. For a UVM, the format for channel specification is *slot.line.chan*[–*chan*]. Refer to the *Cisco IGX Reference* for a description of the UVM's lines. Note that, if you are using CAS switching with Model B firmware, *line* must be "1."
node	Specifies the name of the node at the other end of the connection. For a DAX connection (where channels on a node are connected to channels on the same node), use the local node name.
remote channel	Specifies the remote channel or set of channels to connect. Brackets indicate that a range of channels can be specified. Channel specification on a UVM has one more parameter than the specification on a CDP or CVM. For a CDP or CVM, the format for channel specification is *slot.chan*[–*chan*]. For UVM, the format for channel specification is *slot.line.chan*[–*chan*]. Access devices such as the Cisco 3800 use the following format for the remote channel specification: <*slot.port*> <*access_device_connection_ID*> where *slot* is the slot number of the FTC or FTM card, *port* is the port number, and *access_device_connection_ID* is in the range 1–252.
type	Specifies the voice connection type. Refer to Table 6-1 or Table 6-2 for voice connection types and compression. For connections to an access device such as the Cisco 3810, *type* can be one of the following: 24-Kbps or 32-Kbps ADPCM, LDCELP, or CACELP.

Table 6-6 addcon—Optional Parameters

Parameter	Description
avoid	Specifies the type of trunk for the connection to avoid. The default is no avoidance. The choices are: *savoid satellite trunks. *tavoid terrestrial trunks. *zavoid trunks using zero code suppression techniques that modify any bit position to prevent long strings of zeros.

cnfchadv

Enables the adaptive voice (ADV) feature for individual channels. ADV must also be enabled at each node that terminates the connection. The channel-specific **cnfchadv** has no effect at nodes that do not support ADV enabled.

If the ADV feature is enabled for a channel with a “c” or “v” connections, VAD is automatically disabled on that channel when trunk bandwidth is available and enabled when trunk bandwidth is needed. If the Adaptive Voice feature is not enabled for a channel with a “c” or “v” connections, VAD is always turned on for that channel. In order for a voice (“c” or “v”) connection to use ADV, both ends must have ADV enabled with the **cnfchadv** command.

Full Name

Configure channel adaptive voice

Syntax

cnfchadv <channel(s)> <y/n>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfchadv 14.1 e
```

Description

Enable Adaptive Voice for channel 14.1.

System Response

```
alpha          TRM   YourID:1        IPX 8420    9.2    Aug. 16 1998 09:43 PST

           %    Adaptive  Gain (dB)   Dial                            OnHk      Cond
Channels  Util  Voice      In  Out     Type   Interface Type    A  B  C  D  Crit.
14.1-24    40   Enabled     0    -    Inband  Unconfig          ?  ?  -  -    a









Last Command: cnfchadv 14.1 e


Next Command:
```

Table 6-7 cnfchadv–Parameters

Parameter	Description
channel	Specifies the channel or range of channels over which you specify Adaptive Voice.
e	Enables ADV (default).
d	Disables ADV.

cnfchdl

Configures the dial type for a channel or set of channels. The dial type may be inband, pulse, or user-configured. The user-configured option allows non-default timing values to be used. The parameters associated with the **cnfchdl** command are timing constants used to ensure that signaling pulses are not distorted in time by transmission through the network.

- Dial type determines the signaling message timing for a connection. Dial type is ignored for DS0 data connections.
- When you add an inband or pulse dial type to a channel, the channel configuration screen appears, showing the designated dial types for each channel.
- When you add a user-configured dial type, a more detailed screen appears, showing the dial type as well as the signaling delay, minimum wink, interdigit times, and playout delay.

If you select inband, the node assumes that the A and B bits are not used for loop-disconnect dialing. Therefore, any change in signaling bit status goes in a packet to the far end of the connection.

If you select pulse, the transmitting node waits (normally 72 ms) after an A or B bit transition for another transition to arrive. If a transition arrives, the new transition goes into the same signaling packet that is sent to the far end of the connection. This step increases the delay of the signaling transition across the network but decreases the amount of trunk bandwidth used for signaling.

If the default timings are not correct for the network, you must configure the options. The dialing type should be set correctly. If a connection-designated pulse is used for inband signaling, a greater than necessary delay across the network results. If a connection-designated inband is used for pulse signaling, the relative timing of signaling transitions may be lost and so distort the pulses.

Full Name

Configure dial type for channels

Syntax

cnfchdl <channel(s)> <dial_type> [<sig_delay> <min_wink> <int_dig_time>
<playout delay>]

Related Commands

dspchcnf, dspchdlcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX,	Yes

Example 1

```
cnfchdl 14.1 p
```

Description

Configure the dial type of channel 14.1 to pulse.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2   Aug. 16 1998 09:46 PST

           %    Adaptive  Gain (dB)   Dial                          OnHk      Cond
Channels  Util  Voice     In  Out      Type   Interface Type    A  B  C  D  Crit.
14.1       40   Enabled    0    -     Pulse   Unconfig          ?  ?  -  -    a
14.2-24    40   Enabled    0    -     Inband  Unconfig          ?  ?  -  -    a






Last Command: cnfchdl 14.1 p


Next Command:
```

Table 6-8 cnfchdl—Parameters

Parameter	Description
channel	Specifies the channel or range of channels over which to configure dial type.
dial type	Specifies the dial type to assign. The three possible dial types are: iinband ppulse uuser-configured Inband is the default dial type. If you designate "**u**" for a user-configured dial type, you are prompted, as applicable, from among the following: sig delay, min wink, interdigit time, and playout delay.

Table 6-9 cnfchdl—Optional Parameters

Parameter	Description
signaling delay	Specifies the signaling delay for the user-configured dial type. The range is 12–96 ms. Your entry is rounded to the closest multiple of 1.5 ms.
minimum wink	Specifies the minimum wink to assign to the user-configured dial type. The range is 3–765 ms. Your entry is rounded down to the nearest multiple of 3 ms. This parameter does not apply to CDP, UVM, or CVM channels.
interdigit time	Specifies the interdigit time for the user-configured dial type. The range is 3–765 ms. Your entry is rounded down to the nearest multiple of 3 ms. This parameter does not apply to CDP, UVM, or CVM channels.
playout delay	Specifies the signaling delay assign to the user-configured dial type. The range is 12–96 ms. Your entry is rounded to the closest multiple of 1.5 ms.

cnfchec

Configures the echo canceller and other channel parameters associated with a voice channel. (You cannot configure CAS and data channels using **cnfchec**). The CDP/CVM and UVM have slightly different parameters. Unavailable parameters appear on the screen as a dashed line, so no prompts for these unavailable options appear.

Full Name

Configure channel echo canceller

Syntax

For CDP/CVM:

cnfchec <chan> <ec> <erl> <td> <convergence> <nlp>

For UVM:

cnfchec <chan> <ec> <td> <nlp> <bkgd_filter>

Related Commands

dspchec

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	No	IGX	Yes

Example 1

```
cnfchec 7.1 e h e e e
```

Description

Enable and configure the Echo Canceller in channel 7.1 with high echo loss tone disabled, convergence enabled, and non-linear processing enabled. In this example, the card is either a CDP or CVM because the channel is specified with *slot.channel* rather than *slot.line.channel*.

System Response

```
pubsigx1       TN    cisco      IGX 8420 9.2   July 27 1998 06:06 PDT

          Echo     Echo Return    Tone      Conver-  Non-Linear Voice
Channels  Cancel   Loss (.1 dBs)  Disabler gence    Processing Tmplt
7.1       Enabled  High  60       Enabled   Enabled  Enabled    USA
7.2-31    Disabled High  60       Enabled   Enabled  Enabled    USA








Last Command: cnfchec 7.1 e h e e e


Next Command:
```

Example 2

cnfchec 13.1.1 e

Description

Enable the echo canceller in channel 13.1.1. In this example, the card is a UVM because the channel is specified with *slot.line.channel*. Note the available parameters differ slightly from a CDP/CVM.

System Response

```
sw176          TN    Cisco      IGX 8420    9.1 Aug. 4 1997 13:29 PST

           Echo     Echo Return  Tone     Conver-  Non-Linear Voice Bkgrnd
Channels   Cancel   Loss(.1 dBs) Disabler gence    Processing Tmplt Filter
13.1.1-24  Disabled       -      Enabled      -    Enabled     -    Enabled
13.2.1-24  Disabled       -      Enabled      -    Enabled     -    Enabled








This Command: cnfchec 13.1.1


Enable or Disable Echo Cancel (e/d)? [d]:
```

Table 6-10 cnfchec—Parameters

Parameter	Description
channel	Specifies the channel or range of channels. For a CDP or CVM, “channel” has the format *slot.channel(s)*. For a UVM, “channel” has the format *slot.line.channels(s)*.
echo canceller	Enable or disable the echo canceller. An “e” enables. A “d” disables.
echo return loss	Sets the echo return loss as high/low). An “h” specifies high. An “l” specifies low.
tone disabler	Enables or disables the tone disabler. An “e” enables. A “d” disables.
convergence	Enables or disables convergence. An “e” enables. A “d” disables. Except for test purposes, the normal state for convergence is enabled.
non-linear processing	Enables or disables non-linear processing. An “e” enables. A “d” disables.
bkgd_filter	Enables or disables the background filter.

cnfchfax

Configures a channel on a UVM for either *FAX detection* or *FAX relay*. If you enable FAX detection, the UVM suspends voice compression when it detects a FAX or modem tone on the channel. For the duration of the FAX, transmission takes place at 64 Kbps.

FAX relay is a mechanism for compression the FAX transmission rate across a network to 9.6 Kbps.

To view the current configuration, use the **dspchcnf** command.

Full Name

Configure FAX modem detection for channels

Syntax

cnfchfax <slot.line> <channel(s)> <e/d>

Related Command

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfchfax 7.1.1
```

Description

Configure channels 1-24 on line 1 of the UVM in slot 7 to have FAX modem detection.

System Response

```
sw109          VT    Cisco      IGX 8420    9.2   Aug. 20 1998 19:10 PST

           %   Adaptive          Gain (dB)  Dial   Interface       OnHk    Cond
Channels Util Voice      Fax    In Out    Type   Type         A  B  C  D Crit
7.1.1-24   40  Enabled  Disabled  0    0   Inband  2W E&M       0  X  -  -  a
7.2.1-24   40  Enabled  Disabled  0    0   Inband  Unconfig     ?  ?  -  -  a









Last Command: cnfchfax 7.1.1


Next Command:
```

Table 6-11 cnfchfax—Parameters

Parameter	Description
slot.line	Specifies the line of the UVM.
channel(s)	Specifies the DS0 or range of DS0s.
e/d	Enable or disable FAX detection.

cnfchgn

Configures the amount of gain inserted by the IGX node for a given circuit line channel or range of channels. Gain can be configured between +6 dB and -8 dB. The input gain is inserted at the receive side of a voice card and is therefore applied before the signal is packetized by the card. The output gain is inserted at the transmit side of a voice card and is applied after the signal has been depacketized by the card. Gain is meaningless for channel that carry data.

Full Name

Configure gain insertion for channels

Syntax

cnfchgn <channel(s)> <input_gain> <output_gain>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfchgn 14.1 -4 2
```

Description

Configure input gain of –4 db and an output gain of +2 dB for channel 1 of circuit line 1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 09:52 PST

           %    Adaptive  Gain (dB)   Dial                          OnHk      Cond
Channels  Util  Voice     In  Out      Type   Interface Type    A  B  C  D  Crit.
14.1       40   Enabled   -4    -2 User    Unconfig ?  ?  -  -    a
14.2-24    40   Enabled    0    -2 Inband  Unconfig ?  ?  -  -    a











Last Command: cnfchgn 14.1 -4 2


Next Command:
```

Table 6-12 cnfchgn–Parameters

Parameter	Description
channel	Specifies the channel or range of channels.
input_gain	Specifies the gain, in decibels, to assign to the channel. The range is –8 dB–+6 dB.
output_gain	Specifies the gain, in decibels, to assign to the channel. The range is –8 dB –+6 dB.

cnfcond

Creates a conditioning template that specifies the bit patterns to be transmitted for each of the T1 and E1 timeslots and their A, B, C, and D signaling bits while the channel is in the failed state. Its purpose is to prevent the signaling bits from returning to the idle (on-hook) bit pattern during a channel failure and to force a known bit pattern (usually busy). If a connection fails and the template has been specified as the conditioning template for the failed connection, the data parameter in the template is transmitted in the channels timeslot, and the A, B, C, and D bits are processed according to the specified parameters.

A two-character sequence in the id parameter field identifies the template. The ‘Data Pattern’ field displays the pattern transmitted in the channels timeslot. The ‘signaling Pattern’ field displays the pattern transmitted in the channel’s A, B, C, and D signaling bit positions. Each of the A, B, C, and D signaling bits are specified independently and may be held high or low or toggled to the on-hook condition for a short time then off-hook (the name of this latter action is a *wink*). You can control the timing of the bit-toggling by specifying the duration of winks in increments of 50 ms.

A typical failure response is for the node to:

1. Transmit idle characters in the channel’s timeslot
2. Signal off-hook for a period of 2 seconds
3. Return permanently to the on-hook condition.

Full Name

Configure conditioning template

Syntax

cnfcond <id> <data> <A bit> <B bit> <C bit> <D bit>

Related Commands

cnfvchtp, dspchcnf, dspcond

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfcond lm 01010100 0(40)/1 1 1 1
```

Description

Configure the conditioning template.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 09:59 PST

Conditioning criterion lm:

  Data Pattern
  01010100 - E1/T1



  Signalling Pattern
  A            0(40)/1
  B            1
  C            1
  D            1



Last Command: cnfcond lm 01010100 0(40)/1 1 1 1


Next Command:
```

Table 6-13 cnfcond—Parameters

Parameter	Description
id	Specifies the identifier of conditioning template. The identifier may be any two character combination of lowercase letters (a–z) and numeric digits (0–9).
data	Specifies an eight-bit binary string to use instead of the voice in the event the channel fails.
A bit B bit C bit D bit	Specifies the signaling sequence to be transmitted for these bits in the event of a channel failure. You can independently set each of these parameters. Each element in the sequence is expressed as a 1 or 0 (to indicate the logic state of the line) followed by a number in parenthesis to indicate the duration that the state remains on the channel. The duration number is expressed in 50 ms intervals. If you do not enter a duration value, the state remains the same indefinitely. For example, if <B> is set to 1(40); upon a channel failure, the B bit remains in the 1 state for 2 seconds (40 x 50 ms=2 seconds). For another example, <C> set to 0 would cause the C bit to be held permanently at 0 during a failed channel condition because no duration value is present. Note that you can specify a sequence of states by entering several states separated by slash symbols. The maximum number of states in a sequence is 5. For example, you could set <A> to 1(40)/0(20)/1 to vary the duration of the 0 and 1 states.

cnflnpass

Configures a pair of ports so that unprocessed channels go from a *primary* UVM to a *secondary* UVM. The **cnflnpass** command primarily applies to channels that use LDCELP or G.729 CACELP (although passthrough is possible on any type of connection except t-type or td-type). For a description of *passthrough*, refer to the UVM description in the *Cisco IGX Reference*.

To return ports to the non-passing configuration, execute **cnflnpass** with a 0 as the second argument.

Full Name

Configure line passthrough

Syntax

To configure passthrough, enter:

cnflnpass <primary line> <secondary line>

To remove passthrough from the primary and secondary lines, enter:

cnflnpass <primary line> 0

Related Commands

dsplncnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX	Yes

Example 1

```
cnflnpass 13.1 12.1
```

Description

Configure line 13.1 to pass any unsupported channels to line 12.1.

System Response

Upon successful execution of the command, the screen displays the slot and line of the passing channel on the right. The screen also shows other characteristics of the line.

```
sw176          TN          IGX 8420    9.2   Aug. 26 1998 00:18 GMT

LN  13.1 Config      E1/30                 UVM slot: 13
Loop clock:          No

Line framing:        On                         cnfg:            Passing
     coding:         HDB3                           slot.line:   12.1
     CRC:            No
     recv impedance: 75 ohm + gnd
  E1/J1 signalling:  CAS
     encoding:       A-LAW
     T1 signalling:  --
     cable type:     --
     length:         --
     56KBS Bit Pos: msb
     pct fast modem: 20


Last Command: cnflnpass 13.1 12.1


Next Command:
```

Note that, when you remove passthrough by entering a 0 for the secondary line, the screen also still line characteristics but with dashed lines in the column for the secondary (or passing) line.

Table 6-14 cnflnpass—Parameters

Parameter	Description
primary line	Specifies the channels that the primary card supports. The format is *slot.port*.
secondary line	Specifies the channels that the secondary card supports. The format is *slot.port*.

cnfrcvsig

Configures the receive signaling bits for a voice channel. Channel signaling bit options are t (transparent), 0, 1, or I (invert). If signaling is set to "not used" (-) by **cnfchtp**, the following condition is maintained: A=1, B=1, C=0, D=1.

Full Name

Configure receive signaling

Syntax

cnfrcvsig <channel(s)> <[A/]Conv> <[B/]Conv> <[C/]Conv> <[D/]Conv>

Related Commands

cnfxmtsig, dspsigqual

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfrcvsig   8.1 A/T  B/0 C/I D/I
```

Description

Configure channel 8.1 signaling to transparent for the A bit, inhibited for the B bit, inverted for the C and D bits.

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:36 MST

                                Signalling Qualifiers
From 8.1    TXAbit TXBbit TXCbit TXDbit RXAbit RXBbit RXCbit RXDbit
8.1         T       T       T       T       T      0      I      I
8.2-31      T       T       T       T       T      T      T      T









Last Command: cnfrcvsig 8.1 A/T B/0 C/I D/I


Next Command:
```

Table 6-15 cnfrcvsig—Parameters

Parameter	Description
channel	Specifies the channel or range of channels to receive signaling.

Table 6-16 cnfrcvsig—Optional Parameters

Parameter	Description
A/	Specifies the conversion applied to the A bit. <Conv> can be one of: 1:bit is asserted. 0:bit is inhibited. T:bit is passed transparently. I:bit is inverted.
B/	Specifies the conversion applied to the B bit.
C/	Specifies the conversion applied to the C bit.
D/	Specifies the conversion applies to the D bit.

cnfvchtp

Configures an interface signaling type for a voice channel. Most standard signaling types are maintained by the node, but a custom template may be built by the user. If you enter the **cnfvchtp** command without a specific interface number, the system will present you with a list of valid interface types and their associated onhook and conditioning information.

To assign an interface type (and its associated onhook and conditioning information) to the channel or set of channels, enter the number of the desired interface type. As mentioned previously, type “1” requires user configuration. Interface type is ignored for “d” type connections.

Full Name

Configure interface type for voice channels

Syntax

cnfvchtp <channel(s)> <type> [<A> <B> <C> <D> <cond_code>]

Related Commands

cnfchgn, cnfchdl, dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfvchtp 7.1.1
```

Description

Configure the interface type for channel 7.1.1-24.

System Response

```
sw109          VT    cisco      IGX 8420    9.2 Aug. 20 1998   18:54 PST

CDP Models All                              None               All
UVM Models All                              None               All
           Sample Delay Bkgnd              Echo Suppression   V.25    Xmit
From 7.1.1 VAD  Non-VAD  Noise  HPF  Float   Function    Loss   Detect  Delay
7.1.1-24   A8   01       67     ON   ON      ON          ON     64K     5
7.2.1-24   A8   01       67     ON   ON      ON          ON     64K     5







This Command: cnfvchparm 7.1.1


Sample delay for VAD connections:
```

Example 2

cnfvchtp 15.5-8 1 X X - - b

Description

Configure a user configurable interface type for channel 15.1 to 15.8. The channel configuration screen shows that channels 5-8 of circuit line 15 now has a user-configured interface type with an Abit on-hook value of "X", a B-bit on-hook value of "X", an C-bit on-hook value of not used, D-bit on-hook value of not used, and conditioning template b.

Table 6-17 cnfvchtp—Parameters

Parameter	Description
channel	Specifies the channel or range of channels for the interface type configuration. For a CVM or CDP, the format is *slot.channel*[-*channel*]. For a UVM, the format for channel is *slot.line.channel*[-*channel*].

Table 6-17 cnfvchtp—Parameters (Continued)

Parameter	Description
interface type	Specifies the number of the interface type to assign to the channel or range of channels. These types are listed below. The Onhook column has A bits on the left and B bits on the right. The conditioning column has different types of conditioning specified. If you designate interface type number 1 to indicate a user-configured interface type, the system prompts for: onhook A, onhook B, onhook C (if applicable), onhook D (if applicable), conditioning A, conditioning B, conditioning C (if applicable), conditioning D (if applicable), and conditioning template information.

Interface Number	Interface Type	Onhook	Conditioning
1	User Config		
2	Unconfig	? ? - -	a
3	No Sig	? ? ? ?	a
4	Force Sig	? ? - -	a
5	2W E&M	0 X - -	a
6	4W E&M	0 X - -	a
7	FXO	11 - -	b
8	FXS G/S	01 - -	c
9	FXS L/S	0 X - -	d
10	DPO	0 X - -	a
11	DPT	0 X - -	a
12	RPO	0 X - -	a
13	RPT	0 X - -	a
14	SDPO	0 X - -	a
15	DX	0 X - -	a
16	ETO	? ? - -	e
17	PLAR	? ? - -	d
18	PLR	0 X - -	a
19	RD	? ? - -	a
20	R1 (SOCOTEL)	0 - - -	e
21	SSDC5A	1 1 0 1	f
22	R2 (backward)	1 1 - -	e
23	R2 (forward)	1 0 - -	d

When the IPX or IGX receives A, B, C, and D bits corresponding to the onhook values, that channel is known to be onhook. If the A, B, C, and D bits do not correspond to the onhook values, that channel is known be offhook

Parameter	Description
onhook A	Abit value for the onhook state of a channel or set of channels.
onhook B	B-bit value for the on-hook state of a channel or set of channels.
onhook C	C-bit value for the on-hook state of a channel or set of channels.

Table 6-17 cnfvchtp—Parameters (Continued)

Parameter	Description
onhook D	D-bit value for the on-hook state of a channel or set of channels. Possible values are: 1high 0low Xdon't care ?don't know -not used
conditioning template	One of many predefined or user-defined conditioning templates in the range of 00000000 to 11111111. (See **dspcond** and **cnfcond** commands). Each interface type, except for option 1, has a predetermined conditioning template associated with it. These represent the A, B, C, D bit values as well as the substitute PCM voice sample sent to the attached equipment in case the voice connection fails for any reason.

cnfxmtsig

Allows the node to pass A, B, C, and D channel signaling bits through unchanged, or to invert, or hold them at a given value for a CDP or CVM line. It affects signaling bits in the transmit direction (to the PBX or channel bank) in an E1 system. The command configures the transmit signaling. Channel signaling bit options are T (transparent), 0, 1, or I (invert). If signaling is set to “not used” (-) by **cnfchtp**, the following is maintained: A=1, B=1, C=0, D=1.

Full Name

Configure transmit signaling

Syntax

cnfxmtsig <channel(s)> <[A/]Conv> <[B/]Conv> <[C/]Conv> <[D/]Conv>

Related Commands

cnfrcvsig, dspsigqual

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfxmtsig 8.1 a/I b/0 c/1 d/t
```

Description

Configure the transmit signaling for channel 8.1 to inverted for the A bit, inhibited for the B bit, asserted for the C bit and transparent for the D bit.

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:38 MST

                                Signalling Qualifiers
From 8.1     TXAbit  TXBbit  TXCbit  TXDbit  RXAbit RXBbit RXCbit RXDbit
8.1          1       0       1       T       T      0      I      I
8.2-31       T       T       T       T       T      T      T      T









Last Command: cnfxmtsig 8.1 a/I b/O c/1 d/t


Next Command:
```

Table 6-18 cnfxmtsig—Parameters

Parameter	Description
channel	Specifies the channel or range of channels to receive signaling.

Table 6-19 cnfxmtsig—Optional Parameters

Parameter	Description
A/	Specifies the conversion applied to the A bit. <Conv> can be one of: 1:bit is asserted. 0:bit is inhibited. T:bit is passed transparently. I:bit is inverted.
B/	Specifies the conversion applied to the B bit.
C/	Specifies the conversion applied to the C bit.
D/	Specifies the conversion applies to the D bit.

delcon

Removes one or more voice connections from a network. You can delete connections at either end of the connection.

Do not delete a connection when the node at the other end of the connection is unreachable. The unreachable node does not recognize the deletion.

Also, you must not delete a connection to an unreachable node then connect that deleted channel to another node.

Full Name

Delete connection

Syntax

delcon <channel(s)>

Related Commands

addcon, dspcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
delcon 14.1
```

Description

Delete connection 14.1. The proposed deletions are highlighted, a prompt requests confirmation of the deletion. Enter a “y” to delete the highlighted connections or an “n” to keep the highlighted connections. The example shows the screen after deletion of 14.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 09:35 PST

 Local      Remote      Remote                                           Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 5.1        beta        25.1       Ok     256                  7/8          0  L
 9.1.100    gamma       8.1.200    Ok     fr                                0  L
 9.2.400    beta        19.2.302   Ok     fr                                0  L











Last Command: delcon 14.1


Next Command:
```

Table 6-20 delcon—Parameters

Parameter	Description
channel(s)	Specifies a channel or range of channels to delete.
	The format for channel on a CDP or CVM is *slot.channel*
	The format for channel on a UVM is *slot.line.channel.*
	For a range of channels, separate the first and last channel with a dash (-).

dspchcnf

Displays configuration details for voice, data, or Frame Relay channels. When you specify a voice channel with **dspchcnf**, the display shows:

- Percent of channel utilization
- Adaptive voice enable status
- Fax enable status
- Gain in both directions (in decibels)
- Dial Type
- Interface type (such as 2w E&M)
- Onhook and conditioning specifications

For the contents of the display when you apply **dspchcnf** to a serial data channel or Frame Relay channel, refer to the chapters in this manual that describe those traffic types.

Full Name

Display channel configuration

Syntax

dspchcnf <start_channel>

Related Commands

cnfchadv, cnfchdfm, cnfchdl, cnfcheia, cnfchgn, cnfchtp, cnfchutl

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	o

Example 1

```
dpchcnf 7.1.1
```

Description

Display the channel configuration of line 7.1.1-24. The card in slot 7 is a UVM.

System Response

```
sw109          VT    cisco      IGX 8420    9.2 Sept. 20 1998 18:59 PST

           %   Adaptive          Gain (dB)  Dial   Interface       OnHk    Cond
Channels Util Voice      Fax    In Out    Type   Type          A  B  C  D Crit
7.1.1-24   40  Enabled  Disabled  0    0   Inband  2W E&M        0  X  -  -  a
7.2.1-24   40  Enabled  Disabled  0    0   Inband  Unconfig      ?  ?  -  -  a







Last Command: dspchcnf 7.1.1


Next Command:
```

Example 2

dspchcnf 9.1.3-8

Description

Display configuration values for all channels on Frame Relay port 9.1 (which also shows if a data channel is configured for idle code suppression).

```
sw176          TRM   StrataCom       IGX 16    9.2.a2    Apr. 3 1998 17:32 PST

            Maximum EIA     %      DFM Pattern     DFM    Idle Code   PreAge
From 9.1.3  Update Rate   Util     Length        Status     Suppr      (usec)
9.1.3-8        -           -         -           -        Enabled         0



Last Command: dspchcnf 9.1.3
```

Table 6-21 dspchcnf–Parameters

Parameter	Description
start channel	Specifies the channel to begin the display.
	The format for a CDP or CVM is *slot.channel*.
	The format for a UVM is *slot.line.channel*.
	The format for an IMA-compliant line is *slot.line.start_channel—end_channel*.

dspchdlcnf

Displays dial type configurations for all channels on a circuit line as follows:

Table 6-22 Information in dspchdlcnf Display

Channel Type	Dial Type	Description
All	Dial Type	Inband, pulse, or user-configured.
User-configured	signaling delay	The signaling delay on a channel. The range is 12 ms–96 ms.
	minimum wink	The minimum wink on the channel. The range is 3 ms–765 ms. (Minimum wink does not apply to a CDP or CVM channel.)
	interdigit time	The interdigit times on a channel. The range is 3 ms–765 ms. (Interdigit time does not apply to a CDP or CVM channel.)
	playout delay	The playout delay on a channel. The range is 12 ms–96 ms.

Full Name

Display channel dial type configurations

Syntax

dspchdlcnf <start_channel>

Related Commands

cnfchdl

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspchdlcnf 14.1`

Description

Display the dial type configuration for all channels beginning with 14.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 09:45 PST


Channels Type   Sig Delay   Min Wink  IntDigit Time  Playout Delay
14.1-24   Inband      12        141           300           -











Last Command: dspchdlcnf 14.1


Next Command:
```

Table 6-23 dspchdlcnf—Parameters

Parameter	Description
start channel	Specifies the channel at which the display begins. For a CDP or CVM, the format is *slot.channel*. For a UVM, the format is *slot.line.channel*.

dspchec

Displays the integrated echo canceller (IEC) parameters for one or more voice channel(s). The **dspchec** command does not apply to CAS or data channels. The specified channels must be on a CDP, CVM, or UVM. Table 6-24 lists the displayed parameters and possible values.

Table 6-24 Information in the dspchec Display

Category	Possible Value
Echo cancellation	Enabled or Disabled
Echo Return Loss (.1 dBs)	High/low (loss is in units are 0.1 dBs)
Tone Disabler	Enabled or Disabled
Convergence	Enabled or Disabled
Nonlinear Processing	Enabled or Disabled
Voice Template	USA, other

Full Name

Display channel echo canceller configuration

Syntax

dspchec <channel(s)>

Related Commands

cnfchec

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspchec 7.1
```

Description

Display the echo canceller configuration for channel 7.1.

System Response

```
pubsipx1       TN    cisco      IGX 8420    9.2    July 27 1998   06:10 PDT

          Echo     Echo Return    Tone      Conver-  Non-Linear Voice
Channels  Cancel   Loss (.1 dBs)  Disabler  gence    Processing Tmplt
7.1       Enabled  High  60       Enabled   Enabled  Enabled    USA
7.2-31    Disabled High  60       Enabled   Enabled  Enabled    USA










Last Command: dspchec 7.1


Next Command:
```

Table 6-25 dspchec—Parameters

Parameter	Description
channels	Specifies the channel or channels to display. For a CVM or CDP, the format is *slot.channel(s)*. For a UVM, the format is *slot.line.channel(s)*.

dspcon

Displays connection information for a specified channel. The information displayed includes:

- The channel numbers for both the local and remote ends of the connection.
- The node names at both ends of the connection.
- The routing restriction.
- The class of service (COS) of the connection (see **cnfcos** description for details).
- The connection route listing the end nodes and any intermediate nodes.
- The preferred route for the connection (if configured).
- If cost-based routing cost-based routing is configured, displays maximum and current costs for a connection route.
- The status of the cards associated with the connection.
- Any Y-cable conflicts.
- The type of the compression, if applicable (VAD, ADPCM, LDCELP, CACELP for voice; repetitive pattern suppression (RPS) applies to data connections).

The status that may be displayed includes:

ok	Connection good
failed	Connection failed

Full Name

Display connection

Syntax

dspcon <channel>

Related Commands

addcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX	No

Example 1

```
dspcon 6.1
```

Description

Display connection information for 6.1.

System Response

```
sw196         VT    cisco      IGX 8420    9.2    Oct. 19 1998   13:35 PDT

Conn:  6.1              sw83        7.13               c16
                                                               Status: OK


Owner: LOCAL  Restriction: NONE  COS: 2 Compression: ADPCM


Path:   sw196     14-- 6.1sw86     1.1--  11sw83
Pref:   sw196     14-- 6.1sw86     1.1-- 11sw83



sw196     Line  6: OK           ONHK  sw83      Line  7: OK



Last Command: dspcon 6.1


Next Command:
```

Table 6-26 dspcon—Parameters

Parameter	Description
channel	Specifies the channel for the connection details display.The command displays connection information for one channel at a time. The format for *channel* on a CDP or CVM is *slot.channel*. The format for a channel on a UVM is *slot.line.channel*.

dspcond

Displays the signaling bit patterns from the specified template. Refer to the description of the **cnfcond** command for the purpose of the conditioning template.

Full Name

Display conditioning criteria

Syntax

dspcond <identifier>

Related Commands

cnfchtp, cnfcond

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspcond   a
```

Description

Display the conditioning template identified as “a.”

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998   09:56 PST

Conditioning criterion a:

  Data Pattern
  01010100 - E1
  01111111 - T1


  Signalling Pattern
  A            0(40)/1
  B            1
  C            1
  D            1




Last Command: dspcond a


Next Command:
```

Table 6-27 dspcond—Parameters

Parameter	Description
identifier	Specifies the identifier of the template.

dspcons

Displays a summary of the connections on an IGX node. Table 6-27 shows the fields displayed in the **dspcons** screens.

The **dspcons** screen in Example 3 shows whether the Idle Code Suppression feature is enabled or disabled. The Idle Code Suppression feature provides a way to stop fast packet generation on an Nx64 super-rate PVC connection when the connected PBX has terminated a video call. Traffic on the data network will therefore be reduced. Bursty data will be able to use this unused bandwidth.

On the **dspcons** screen, data connections show the word “ICS” under the “Compress” field if the connection has idle code suppression enabled or not.   This feature is supported only on IGX platforms in Release 9.2. It is supported only on the UVM and CDP/CVM cards. The UVM model E and CVM/CDP model B revision E firmware are required to use the Idle Code Suppression feature in Release 9.2.

Table 6-28 Information in the dspcons Display

Fields	Description
Local Channel	The connection’s channel at this node.
Remote Node Name	The name of the node at the other end of the connection.
Remote Channel	The connection’s channel at the remote node.
State	The state of the connection(s) as follows: • OKRouted • DownDowned • OK DownedWaiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command. • FailedUnrouted, but trying
Type	The type of connection (v = voice, d = data, fr = Frame Relay, atfr = ATM to Frame Relay interworking, atfst = ATM to Frame Relay interworking with ForeSight, -fail = failed connections; data rate in kbps for data)
Compression	The type of compression applied to the connection. The types of voice compression appear earlier in the chapter. The compression that applies to data connections is the purchased option called repetitive pattern suppression (RPS).
COS	The Class Of Service.
Loopback	A connection with a local loopback is indicated by a right parenthesis symbol between the “Local Channel” and “Remote NodeName” columns. A Frame Relay connection with a port loopback is indicated by a right bracket symbol between the “Local Channel” and “Remote NodeName” columns. A connection with a remote loopback is indicated by a right parenthesis symbol before the channel number in the “Remote Channel” column.
Local/Remote Abit	Abit status on the local and remote nodes if -abit option selected. Note that -abit is incompatible with -v, -d, and +d.

Full Name

Display connections

Syntax

dspcons [start_channel] [nodename] [state] [type]
[-g | +d | -v | -d | -f | -abit | -fabit | -atfr | -siw | -fail | -down]]

Related Commands

addcon, cnfchadv, chfchdfm

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspcons

Description

Display a summary of all connections.

System Response

```
pubsipx1       TN    cisco      IPX 16    9.1    July 24 1997 23:04 PDT

 Local          Remote      Remote
 Channel        NodeName    Channel         State Type      Compress Code COS
 5.1.100        pubsipx3    5.1.200         Ok     fr                       0











Last Command: dspcons


Next Command:
```

Example 2

dspcons -abit

Description

Display connections and abit status.

System Response

```
sw53           VT    cisco      BPX 8420    9.2    July 25 1998 11:52 GMT

 Local           Remote      Remote                          Local     Remote
 Channel         NodeName    Channel          State           Abit     Abit
 4.1.2.1         sw53        4.3.2.1          Ok          OK        OK
 4.1.2.2         sw53        4.3.2.2          Ok          OK        OK
 4.1.2.3         sw53        4.3.2.3          Ok          OK        OK
 4.1.2.4         sw53        4.3.2.4          Ok          OK        OK
 4.1.2.5         sw53        4.3.2.5          Ok          OK        OK
 4.1.2.6         sw53        4.3.2.6          Ok          OK        OK
 4.1.2.7         sw53        4.3.2.7          Ok          OK        OK
 4.1.2.8         sw53        4.3.2.8          Ok          OK        OK
 4.1.2.9         sw53        4.3.2.9          Ok          OK        OK
 4.1.2.10        sw53        4.3.2.10         Ok          OK        OK
 4.1.2.11        sw53        4.3.2.11         Ok          OK        OK
 4.1.2.12        sw53        4.3.2.12         Ok          OK        OK

This Command: dspcons -abit


Continue?
```

Example 3

dspcons

Description

Display connections (shows if ICS is enabled on a channel)

System Response

```
sw176          TRM   StrataCom       IGX 8420    9.2.a2    Apr. 3 1998 17:36 PST

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
 9.1.2-3        sw176       9.1.2-3         Ok     2x64                7/8
 9.1.4          sw176       9.1.4           Ok     1x64      ICS       7/8
 9.1.6          sw176       9.1.6           Ok     g729r8    LDCELP
 9.1.7          sw176       9.1.7           Ok     1x64                7/8
 9.1.9          sw176       9.1.9           Ok     c32       VAD/ADPCM
 9.1.10-13      sw176       9.1.10-13       Ok     4x64      ICS       7/8


 d

Last Command: dspcons
```

Table 6-29 dspcons–Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. The start channel on a CDP or CVM is specified as *slot.channel*.The start channel on a UVM is *slot.line.channel*.
node name	Specifies that only connections to this remote node from the local note be displayed. If no "nodename" is designated, connections from the local node to all other nodes are displayed.
connection type	Specifies that only connections of a certain type be displayed. If you do not add at least one argument to specify a particular connection type, all connections appear. When you enter the connection type on the command line, precede it with a hyphen (-). In some cases, you can add more than one connection type (with a space between), but not all compound arguments are compatible, so you may not always see the expected combination of types. The connection types are: -v displays only voice connections. -d displays only data connections. -f displays only Frame Relay connections. -abit shows Abit (nni) status. -fabit shows connections with failed Abit (nni) status. -fail shows only failed connections -siw shows service interworking connections. -atfr shows only network interworking connections.
+d	Causes the display to show the user-configured descriptor for the connection instead of the compression and ownership fields.

dspconst

Displays the status of the circuit line(s) and continues to display the status until you press the Delete key. While the display is on the screen, the status is automatically updated. The update frequency is one second for each circuit line being displayed. (For example, if only one line is displayed, the update frequency is once per second, if three circuit lines are displayed, the update frequency is once per three seconds). Table 6-29 shows the connection type. **cnfchtp** must be correctly configured.

Table 6-30 Types of Connection Status

Symbol	Description
+	offhook
-	onhook
m	slow modem
M	fast modem
F	FAX
blank	channel not connected

Full Name

Display connection state for line connections

Syntax

dspconst [circuit line]

Related Commands

cnfchtp

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspconst
```

Description

Display the condition state for the voice channels on the node.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 09:55 PST

Connection status display

+ offhook, - onhook, m slow modem, M fast modem, F FAX
                      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
CLN   1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

14    +








This Command: dspconst


Hit DEL key to quit:
```

Table 6-31 dspconst—Optional Parameters

Parameter	Description
circuit line	Specifies the number of the line for the channel state display. If you do not specify a line, all upped circuit lines (up to a maximum of eight at once) are displayed.

dsprtcache

This command displays the cache of all cost-based routing connections. The optional *index* parameter lets you specify a cache entry index. The optional *c* parameter clears the cache. The information displayed includes:

Full Name

Display cost-based route cache

Syntax

dsprtcache [index] [c]

[index] specifies the cache entry index

[c] specifies to clear the entire cache or a single entry

Related Commands

dspcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, PX	No

Example 1

```
dsprtcache
```

Description

Display route cache contents, and let you monitor and manually clear the cache.

System Response

```
pissaro    TN       StrataCom   BPX 8620   9.2  Jun. 18 1998 11:11 GMT
Route Cache (Summary)
Index  Use    Cost  Delay  Restrict  Load  VPC   Hops  Remote Node
0      Yes    1     Yes    No        None  VBR   No    2      lautrec
1      Yes    6     Yes    No        *s    BDB   No    3   vangogh
2      Yes    9     Yes    No        None  BDA   No    3     matisse
3      Yes    3     Yes    No        *t    BDB   No    3     rousseau
4      Yes    1     Yes    No        None  CBR   No3     seurat<- current
5      No     0     No     No        None  ---   No0     ---
6      No     0     No     No        None ---    No0    ---
7      No     0     No     No        None---No0    ---
8      No     0     No     No None---No0     ---
9      No     0     No     No None---No0     ---
10     No     0     No     No None---No0     ---
11     No     0     No     No None---No0     ---

Last Command: dsprtcache

Next Command:
```

Table 6-32 dsprtcache–Parameters

Parameter	Description
index	Specifies a particular route entry within the cache. When used with the c parameter, the route is either displayed or cleared from the cache.
c	Clears the cache, or if you also enter the index parameter, clears the route cache specified by the index number.

dspsigqual

Displays the configuration for the A, B, C, and D bit signaling qualifiers for all channels. The only parameter is the starting channel. You set the values for these signaling bits with the **cnfrcvsig** and **cnfxmtsig** commands. Note that these signaling bit states are different from the states during circuit alarm (signaling conditioning).

During normal operation of the voice circuit, the A, B, C, and D signaling bits may be held at a fixed value (0 or 1), inverted (I), or passed through transparently (T). For the direction of the signals, the transmit direction is towards the PBX or channel bank. Receive is from the external equipment.

Full Name

Display signaling qualifiers

Syntax

dspsigqual <start channel>

Related Commands

cnfxmtsig, cnfrcvsig

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspsigqual 8.1
```

Description

Display the channel signaling bit qualifiers for channel 8.1.

System Response

```
beta           TRM   YourID:1        IPX 8420    9.2    Aug. 23 1998 11:39 MST

                                Signalling Qualifiers
From 8.1    TXAbit  TXBbit  TXCbit  TXDbit  RXAbit RXBbit RXCbit RXDbit
8.1         1       0       1       T       T      0      I      I
8.2-31      T       T       T       T       T      T      T      T










Last Command: dspsigqual 8.1


Next Command:
```

Table 6-33 dspsigqual—Parameters

Parameter	Description
start channel	Specifies the starting channel. On a CDP or CVM, the format is *slot.channel*. On a UVM, the format is *slot.line.channel*.

dspsvcst

Displays the voice SVC statistics.

Full Name

Display voice SVC statistics

Syntax

dspsvcst

Related Commands

None

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspsvcst

Description

Display the voice SVC statistics for the current node.

System Response

```
sw91           TN    cisco      IGX 8410     9.2       Aug. 29 1998 14:11 GMT


Number of Active SVC             :         0
Number of SVC Requests           :         0
Number of Failed Requests        :         0
Last Reason for request failure  :         0
Number of Completed SVC Routes   :         0
Number of Failed SVC Routes      :         0
Number of Deleted SVC(s)         :         0
Number of Failed SVC             :         0
Max Secs To Perform SVC Route       :      0.000
Avg Secs To Perform SVC Route       :      0.000





Last Command: dspsvcst


Next Command:
```

prtchcnf

Prints the configuration details for voice channels or data channels. This command uses the same syntax, and prints the same information as is displayed using the **dspchcnf** command. See the **dspchcnf** command for syntax and output information.

Full Name

Print channel configurations

Syntax

prtchcnf [start_channel]

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IP IGX	Yes

Example 1

`prtchcnf 14.1`

Description

Print the configuration values of circuit line 14.1.

System Response

None available because this command produces hardcopy.

Table 6-34 prtchcnf–Parameters

Parameter	Description
start channel	Specifies the starting channel for the print output. On a CDP or CVM, the format is *slot.channel*. On a UVM, the format is *slot.line.channel*.

prtchdlcnf

Prints the dial type configurations for channels on a circuit line.

Full Name

Print dial type configuration for channels

Syntax

prtchdlcnf <start_channel>

Related Commands

cnfchdl, dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

`prtchcnf 14.1`

Description

Print the dial type configuration for all channels beginning with 14.1.

System Response

None available as this command produces hardcopy.

Table 6-35 prtchdlcnf–Parameters

Parameter	Description
start channel	Specifies the starting channel for the print output. On a CDP or CVM, the format is *slot.channel*. On a UVM, the format is *slot.line.channel*.

prtcons

Prints a summary of connections terminated at the IGX node.

Full Name

Print connections

Syntax

prtcons [start_channel] [nodename] [type]

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

`prtcons`

Description

Print a summary of all connections.

System Response

None available as this command produces hardcopy.

Table 6-36 prtcons–Optional Parameters

Parameter	Description
start channel	Specifies the starting channel. On a CDP or CVM, the format is *slot.channel*. On a UVM, the format is *slot.line.channel*.
node name	Specifies that only connections to this remote node from the local note be displayed. If no "nodename" is designated, connections from the local node to all other nodes are displayed.

Parameter	Description
connection type	Specifies that only connections of the specified type appear. If you do not include a connection-type argument, all connections appear. Connection types require a hyphen (-). Valid connection type entries are: -v Displays only voice connections. -d Display only data connections. -f Displays Frame Relay connections. -nni Displays Frame Relay network to network connections for failed connections only.

Data Connections

Data commands apply to setting up, configuring, and statistical reporting on data connections. For descriptions of the data commands on a FastPAD, refer to the *FastPAD User's Guide*. Examples of the tasks described in the chapter are:

- Setting up a circuit line and a data connection
- Configuring data channel redundancy
- Using interface control templates
- Enabling DFM and data channel utilization
- Enabling Embedded EIA operation
- Setting up DDS trunks
- Configuring idle code suppression on a per-connection basis

The nodes and card sets to which the commands in this chapter apply are:

- On an IGX node, the card sets are the
  - — HDM/SDI,
  - — LDM/LDI
  - — CVM/BC-T1, BC-E1, or BC-J1
  - — UVM/UVI-2T1, UVI-2E1, or UVI-2J1

Setting Up a Data Connection

To set up a data connection:

Step 1 If necessary, configure the data channel at each end of the connection. Default configuration parameters exist, so using the following commands are optional. The designation of a data channel has the format *slot.port*. For example, 6.3 is port 3 on the card in slot 6. The items that need configuring depend on the type of data connection. The configuration commands and their associated parameters are as follows.

- cnfdclk — Specifies the clocking for the data channel
- cnfcldir — Sets the control leads for bidirectional pins 11 and 23 on an EIA/TIA-232 data channel. The default is *input*
- tstport — Use sixth lead feature to provide test port loopback

- addyred — Enables optional card redundancy. This step requires extra hardware.
- cnfict — Configures an interface control template that determines output lead behavior for data channels. Output leads can be either configured as steady state (on or off) or programmed to follow an input lead. Five types of templates exist for channels in active, conditioned, looped, near, and far states.
- cpyict — Copies interface control template information from one channel to another. This step is optional.

Step 2 Add the connection with the **addcon** command. The above configuration must have been completed at each end before the connection can be added.

Configuring Data Channel Redundancy

You can configure redundant data channels by installing two identical card sets in adjacent slots and connecting the cards to the customer's line through a Y-cable. Applicable commands are:

- Use the **addyred** command to establish the redundant connection between the two card sets.
- Use the **delyred** command to remove redundancy from a redundant pair.
- Use the **dspyred** command to display Y-cable configurations.
- Use the **prtyred** command to print Y-cable configurations.

Using an Interface Control Template

Data channels have an associated default interface control template for each of the active (normal), conditioned, looped, near and far states. The templates define how the control leads at the data interface are to be configured (asserted, inhibited, follow a local source or follow a remote source). The interface control template can be changed by using the **cnfict** command. Each template and each control lead must be configured individually. The **cpyict** (copy interface control panel) can be used to apply (copy) the settings of a template for one data channel to those of a template for another data channel.

Enabling DFM and Data Channel Utilization

DFM (Data Frame Multiplexing) is a feature on the IGX nodes in which repetitive data patterns (such as IDLE codes) are suppressed at the source and regenerated at the remote node. This feature has the effect of approximately doubling the bandwidth of the data channel.

Note DFM operates on connections with maximum rate of 128 Kbps.

The command for changing the DFM enable-status for individual data channels is **cnfchdfm**. Before you execute this command, make sure the DFM feature has been activated on each applicable node by Customer Service. You can check the DFM configuration for a channel by using the **dspchcnf** command. When the DFM feature is first activated at a node, it has the following default values:

- Percent of channel utilization is 100%
- Pattern length is 8 bits

- DFM status is enabled.

Enabling Embedded EIA Operation on the LDP or LDM

The EIA feature encodes the status of the CTS or RTS lead as the eighth bit in each data byte. The byte subsequently is processed in accordance with the DFM algorithm, which remains unchanged.

Any DCE and DTE combination at each end is valid. A typical configuration might have the LDP at one end of a connection as DCE (normal clocking) and an LDM at the other end as DTE (looped clocking). RTS is transmitted in encoded form from the remote end to the local end, and CTS is transmitted in the other direction. Other EIA leads use the non-interleaved format.

The EIA feature is allowed for all legal baud rates 19.2 kbps and below and is activated by typing encoding type 7/8E followed by an *Z when adding a connection using the **addcon** command. Different channels on the same card may be set up with or without the feature, but all ports on the card must be configured at or below 19.2 kbps for EIA to be active. Note that you do not have to enter *Z after 7/8E on the command line because the system automatically enters it.

Setting Up DDS Trunks

DDS Trunks normally operate at 56 Kbps. The IGX nodes can provide a direct interface to a DDS line and provide limited distance access to Data Service Units (DSUs) by using the DDS format over private lines. The LDI4/DDS back card and LDP (Model B) or LDM front card support DDS. Each LDI/DDS supports four DDS trunks in DSU or OCU modes.

- Use the **cnfdchtp** command to configure the DDS port. Specify OCU or DSU for the port type.
- Add the connection using the **addcon** command. When prompted for the rate, enter 2.4 Kbps, 4.8 Kbps, 9.6 Kbps, 19.2 Kbps, or 56 Kbps.

Configuring a Channel to Use Idle Code Suppression

In Release 9.2, the UVM and CVM cards on the IGX support Idle Code Suppression (ICS) for video calls. You can configure the idle code suppression (ICS) feature on an Nx64 super-rate PVC connection (which uses multiple channels) to stop fast packet generation when the connected PBX has terminated a video call. No video traffic will be generated when a video call has terminated. Use the **chfdch** and **dspchcnf** commands to enable or disable idle code suppression for the UVM and CDP/CVM cards, and to display the configuration for the cards. All back card types supported by UVM/CVM/CDP support the idle code suppression feature.

Note The UXM/CVM firmware needs to be upgraded for this feature. The CVM model B revision E and above support this feature. The UVMs Model E and above supports this feature. The **dspcd** screen displays “Front card supports idle code suppression.”

The UVM/CVM card firmware detects the idle (on-hook) state of a video call, which uses an nx64K data connection, and suppresses packet transmission during this idle connection. The UVM or CVM at the far end of the connection plays out the idle code during this time. You use the switch software **cnfdch** and **dspchcnf** commands to enable/disable and display this feature on a per connection basis. The primary benefit of the ICS feature is the trunk bandwidth savings during the on-hook state of an nx64 connection. This extra bandwidth can be used by other connections.

Summary of Commands

Table 7-1 shows the full command name and starting page of each description:

Table 7-1 Data Connection Commands

Mnemonic	Description	Page
addcon	Add connection	7-5
cnfchdfm	Configure Data Frame Multiplexing (DFM)	7-17
cnfcheia	Configure EIA	7-19
cnfcldir	Configure control lead direction	7-21
cnfdchtp	Configure data channel interface type	7-23
cnfdch	Configure data connection to have ICS (Idle Code Suppression)	7-23
cnfdclk	Configure data clock	7-32
cnfict	Configure interface control template	7-36
cpyict	Copy interface control template	7-41
delcon	Delete connection	7-43
dspchcnf	Display channel configuration	7-45
dspcon	Display connection	7-47
dspcons	Display connections	7-49
dspict	Display interface control template	7-55
prtchcnf	Print channel configuration	7-57
prtcons	Print connections	7-58
prtict	Print interface control template	7-60

addcon

Establishes data channel connections between nodes in a network. After you add a connection using the **addcon** command, the node automatically routes the connection. The node where you execute **addcon** is the "owner" of the added connections. The concept of ownership is important because you must enter information about automatic rerouting and preferred routing at the node that owns the connection. See the **cnfpref** and **cnfcos** commands for more information on automatic rerouting. Before the node adds the connection, the proposed connection appears on the screen with a prompt for you to confirm the addition.

When applied to data connections, the **addcon** command adds a synchronous data connection to the network. You can add synchronous data connections to any node slot equipped with either an LDM or HDM in an IGX node. Before you add a connection, determine the desired data rate. To find the data rates that individual cards support, refer to the card descriptions in the *Cisco IGX 8400 Series Reference* manual or the *Cisco IGX Reference* manual.

When connecting sets of data channels, you do not have to specify the full channel set for the local end of the connection. You have to designate only the first channel in the range. For example, to add connects 27.1-4 at local node alpha to channels 9.1-4 at beta, you can enter "addcon 27.1-4 beta 9.1". If Y-cable redundancy has been specified, you can add data connections at only primary card slots (not at the secondary card slots). See the **addyred** description for more information. Standard Data Rates tables follow, listing data rates. The following notations appear with some data rates:

- * Must be used with 8/8 or 8/8I coding.
- /n Specifies a partially filled packet type: the /n allows partial packets to be sent and so avoid the delay incurred by waiting to build a full packet
- f Entered after the data rate, an *f* specifies "fast EIA" (interleaved EIA) for the connection.
- t Indicates "transparent" (CDP or CVM subrate DS0A): if you include the t-option, the IGX node does not check for supervisory or control information.

Table 7-2 Data Connection Load Table with Normal EIA and No DFM

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
1.2	43	28	38	32
1.8	65	28	57	32
2.4	35	70	30	80
3.2	46	70	40	80
3.6	52	70	45	80
4.8	35	140	30	160
6.4	46	140	40	160
7.2	52	140	45	160
8	58	140	50	160
9.6	69	140	60	160
12	86	140	75	160
12.8	92	140	80	160
14.4	103	140	90	160
16	115	140	100	160
16.8	120	140	105	160
19.2	138	140	120	160
24	172	140	150	160
28.8	206	140	180	160
32	229	140	200	160
38.4	275	140	240	160
48	343	140	300	160
56	381	147	334	160
57.6	392	147	360	160
54	436	147	381	168
72	490	147	429	168
76.8	523	147	458	168
84	572	147	500	168
96	654	147	572	168
112	762	147	667	168
115.2	784	147	686	168
128	871	147	762	168
144	980	147	858	168
168	1143	147	1000	168
192	1307	147	1143	168
224	1524	147	1334	168
230.4	1568	147	1372	168

Table 7-2 Data Connection Load Table with Normal EIA and No DFM (Continued)

256	1742	147	1524	168
288	1960	147	1715	168
336	2286	147	2000	168
384	2613	147	2286	168
448	3048	147	2667	168
512	3483	147	3048	168
672	4572	147	4000	168
768	5225	147	4572	168
772	5252	147	4596	168
896	6096	147	5334	168
1024	6966	147	6096	168
1152	7837	147	6858	168
1344			8000	168

Unshaded connections generate timestamped data packets. Shaded connections generate non-timestamped data packets.

Table 7-3 Data Connection Load Table with Interleaved EIA

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
1.2f	35	35	30	40
1.8f	52	35	45	40
2.4f	35	70	30	80
3.2f	46	70	40	80
3.6f	52	70	45	80
4.8f	69	70	60	80
6.4f	92	70	80	80
7.2f	103	70	90	80
8f	115	70	100	80
9.6f	138	70	120	80
12f	172	70	150	80
12.8f	183	70	160	80
14.4f	206	70	180	80
16f	229	70	200	80
16.8f	240	70	210	80
19.2f	275	70	240	80
24f	343	70	300	80
28.8f	412	70	360	80
32f	458	70	400	80
38.4f	549	70	480	80
48f	686	70	600	80
56f	800	70	700	80
57.6f	823	70	720	80
54f	915	70	800	80
72f	1029	70	900	80
76.8f	1098	70	960	80
84f	1200	70	1050	80
96f	1372	70	1200	80
112f	1600	70	1400	80
115.2f	1646	70	1440	80
128f	1829	70	1600	80
144f	2058	70	1800	80
168f	2400	70	2100	80
192f	2743	70	2400	80
224f	3200	70	2800	80
230.4f	3292	70	2880	80

Table 7-3 Data Connection Load Table with Interleaved EIA (Continued)

256f	3658	70	3200	80
288f	4115	70	3600	80
336f	4800	70	4200	80
384f	5486	70	4800	80
448f	6400	70	5600	80
512f	7315	70	6400	80

Connections above the line generate timestamped data packets. Shaded connections generate non-timestamped data packets. DFM is not available on interleaved EIA connections.

Table 7-4 Data Connection Load Table with Partially Filled Packets and No DFM

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
2.4/4	86	28	75	32
3.2/4	115	28	100	32
3.6/4	129	28	113	32
4.8/10	69	70	60	80
4.8/4	172	28	150	32
6.4/10	92	70	80	80
6.4/4	229	28	200	32
7.2/10	103	70	90	80
7.2/4	258	28	225	32
8/10	115	70	100	80
9.6/10	138	70	120	80
12/10	172	70	150	80
12.8/10	183	70	160	80
14.4/10	206	70	180	80

All of the above connections generate timestamped data packets.

Table 7-5 Data Connection Load Table with Normal EIA and DFM

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
1.2	58	21	24	3
1.8	86	21	24	3
2.4	39	63	72	9
3.2	51	63	72	9
3.6	58	63	72	9
4.8	37	133	152	19
6.4	49	133	152	19
7.2	55	133	152	19
8	61	133	152	19
9.6	73	133	152	19
12	91	133	152	19
12.8	97	133	152	19
14.4	109	133	152	19
16	121	133	152	19
16.8	127	133	152	19
19.2	145	133	152	19
24	181	133	152	19
28.8	217	133	152	19
32	241	133	152	19
38.4	289	133	152	19
48	361	133	152	19
56	422	133	152	19
57.6	434	133	152	19
64	482	133	152	19
72	542	133	152	19
76.8	578	133	152	19
84	632	133	152	19
96	722	133	152	19
112	843	133	152	19
115.2	867	133	152	19
128	963	133	152	19

All of the above connections generate timestamped data packets.

Table 7-6 Data Connection Load Table with Partially Filled Packets and DFM

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
2.4/4	115	21	100	24
3.2/4	153	21	134	24
3.6/4	172	21	150	24
4.8/10	77	63	67	72
4.8/4	229	21	200	24
6.4/10	102	63	89	72
6.4/4	305	21	267	24
7.2/10	115	63	100	72
7.2/4	343	21	300	24
8/10	127	63	112	72
9.6/10	153	63	134	72
12/10	191	63	167	72
12.8/10	204	63	178	72
14.4/10	229	63	200	72
All of the above connections generate timestamped data packets.				

Table 7-7 Data Connection Load Table with Partially Filled Packets and Interleaved EIA

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
1.2f/2	86	14	75	16
1.8f/2	129	14	113	16
2.4f/5	69	35	60	40
2.4f/2	172	14	150	16
3.2f/5	92	35	80	40
3.2f/2	229	14	200	16
3.6f/5	103	35	90	40
3.6f/2	258	14	225	16
4.8f/5	138	35	120	40
6.4f/5	183	35	160	40
7.2f/5	206	35	180	40

All of the above connections generate timestamped data packets. DFM is not available on interleaved EIA connections.

Table 7-8 Sub-Rate Data Connection Load Table (HDM to HDM)

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	Bits/Pkt	Pkt/Sec	Bits/Pkt
2.4t			35	80
4.8t			35	160
9.6t			70	160
56t			381	168
t			381	168

All sub-rate data connections use 8/8 coding. Unshaded connections generate timestamped data packets. Shaded connections generate non-timestamped data packets. DFM is not available on sub-rate connections. Interleaved EIA is not available on sub-rate connections.

Table 7-9 Sub-Rate Data Connection Load Table (HDM to HDM)

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	**Bits/Pkt**	**Pkt/Sec**	**Bits/Pkt**
2.4/4t			88	32
4.8/10t			70	80
4.8/4t			175	32
9.6/10t			140	80

All sub-rate data connections use 8/8 coding. All of the above connections generate timestamped data packets. DFM is not available on sub-rate connections. Interleaved EIA is not available on sub-rate connections.

Table 7-10 Super-Rate Data Connection Load Table (LDM to HDM)

Bit Rate (kbps)	7/8 Coding		8/8 Coding	
	Pkt/Sec	**Bits/Pkt**	**Pkt/Sec**	**Bits/Pkt**
1x56	381	147	334	168
2x56	762	147	667	168
3x56	1143	147	1000	168
4x56	1524	147	1334	168
5x56	1905	147	1667	168
6x56	2286	147	2000	168
7x56	2667	147	2334	168
8x56	3048	147	2667	168
1x64	436	147	381	168
2x64	871	147	871	168
3x64	1307	147	1307	168
4x64	1742	147	1143	168
5x64	2177	147	1524	168
6x64	2613	147	1905	168
7x64	3048	147	2286	168
8x64	2483	147	2667	168

All of the above connections generate non-timestamped data packets. DFM is not available on interleaved EIA connections.

In "fast EIA" signalling mode, an interleaved byte of EIA signalling information is associated with every byte of data in a packet. This format is appropriate for applications where EIA lead transitions must closely synchronize with user data. Fast EIA can apply to data rates up to 512 Kbps.

When FastPackets are built using the 7/8 coding format, each octet in the FastPacket payload consists of seven user data bits followed by a "1." This "bit-stuffing" allows these FastPackets to be safely carried on trunks which enforce ones density requirements by ensuring that each octet contain at least one "1" (such as IGX trunks configured for ZCS or AMI encoding). The user data may have any format and may contain any pattern, including all “0”s. The single “1” inserted in the final bit position of each octet ensures that no more than seven consecutive “0”s occur in a FastPacket. The 7/8 coding format is the safest mode to use when the data protocol is unknown and certain trunks in the network use ZCS or AMI.

When FastPackets are built using the 8/8 coding format, each octet in the FastPacket payload consists of eight user data bits. The 8/8 coding format is more efficient than the 7/8 format. However, the ones density requirement on trunks must be met by one of the following:

- Ensuring that the end-user equipment data protocol can never send more than seven consecutive “0”s.
- Ensuring that the connection can never be carried on a trunk which uses ZCS ones density enforcement.

The vast majority of trunks today use intelligent ones density enforcement schemes, such as B8ZS, HDB3, B3ZS, or CMI. All such trunks can safely carry 8/8 data connections with no risk of data corruption. Data connections can be configured to NOT use ZCS trunks by specifying the optional “*Z” routing restriction.

When FastPackets are built using the 8/8I coding format, each octet in the FastPacket payload consists of eight inverted user data bits, i.e., each “0” is changed to a “1” and each “1” is changed to a “0.” The bits are re-inverted at the far end of the connection. For such connections, the ones density requirement on trunks must be met by one of the following:

- Ensuring that the end-user equipment data protocol can never send more than seven consecutive “1”s.
- Ensuring that connection can never be carried on a trunk which uses ZCS ones density enforcement.

As with the 8/8 coding format, 8/8I connections can be safely carried on the vast majority of trunks today. However, the 8/8I format is primarily intended to provide the efficiency of 8/8 coding for any data which is HDLC or SDLC-based. HDLC/SDLC can never send more than six consecutive “1”s, which, when inverted, automatically meets the ones density requirements of every possible trunk format.

If the data protocol requires an acknowledgment and is delay-sensitive avoid routing the connection over a satellite line (*s for avoid). If 8/8 or 8/8I coding is the selected format, avoid trunks with zero code suppression (*z for avoid) because the zero code suppression could corrupt the last bit in the byte.

Full Name

Add a connection

Syntax

addcon <local channel> <remote node> <remote channel> <type> <coding> [avoid]

Related Commands

delcon, dncon, dspcon, dspcons, upcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	IGX	Yes

Example 1

`addcon 6.1 pubsigx2 11.1 56`

Description

Add a low speed data connection of 56 Kbps at 6.1. The connections are highlighted on the screen. A prompt appears asking you to confirm these connections. Respond "y" for yes to add the connection. The connections screen then appears showing that data channel 11.1 on node pubsigx2 is connected to channel 6.1 on node pubsigx1. The "56" under the "type" category indicates that the data rate for the channel is 56 Kbps.

System Response

```
pubsigx1       TN    SuperUser       IGX 8420    9.2    July 25 1998  06:23 PDT

 From           Remote      Remote
 6.1            NodeName    Channel         State  Type       Compress  Code COS
 6.1            pubsigx2    11.1            Ok     56                   7/8  0













Last Command: addcon 6.1 pubsigx2 11.1 56


Next Command:
```

Example 2

`addcon 5.1 beta 6.1-4 4x64`

Description (CDP super-rate connection)

Add a 256 Kbps (4x64) connection from an SDP at node "alpha" to the CDP at node "beta." Data rates come from the Standard Data Rate Connections in the preceding pages. The elements on the command line consist of the following:

addcon *slot.port remote nodename slot.start channel at far-end channel rate*

Example 3

addcon 5.4-7 beta 6.1-4 4x64

Description (CDP to CDP or CVM to CVM)

Add a 256 Kbps (4x64) data connection from a CDP (or CVM) at node “alpha” to the CDP (or CVM) at node “beta.” The syntax for this example requires that the start and end channel are entered for both ends of the connection and that the *data rate* is specified to be the same at both ends. The channel *numbers* can be different on each end if they are contiguous.

addcon	slot.start channel	-end channel	remote nodename
	slot.start channel	-end channel	rate

Table 7-11 addcon–Parameters

Parameter	Description
local channel	Specifies the local channel or set of channels in the format slot.port [–port]. (The brackets indicate you can specify a range of channels.)
remote node	Specifies the name of the node at the other end of the connection. For a DACS-type connection (where a channel on a node connects to a channel on the same node), use the local node name for *remote node*.
remote channel	Specifies the remote channel or set of channels in the format slot.port [–port]. (The brackets indicate you can specify a range of channels.)
type	Specifies the data connection bit rate, EIA control lead mode, and in some cases, the number of data bytes in a data packet. Refer to the Standard Data Connection rates for allowable bit rates.
coding	Specifies the data coding format for data transmissions. Valid formats are: 7/8 7 bits of user data plus a "1" inserted in the final bit position of each data byte in a data packet. This is the default coding. 7/8e Used with LDP or LDM application. 8/8 8 bits of user data for each data byte in a data packet. 8/8I 8 bits of user data for each data byte in a packet. The data is inverted

Table 7-12 addcon–Optional Parameters

Parameter	Description
avoid	Specifies the type of trunk for the connection to avoid. The default is no avoidance. The choices are: *s avoid satellite trunks. *t avoid terrestrial trunks. *z avoid trunks using zero code suppression techniques that modify any bit position to prevent long strings of 0s.

cnfchdfm

Enables or disables Data Frame Multiplexing (DFM) for individual channels and sets the DFM parameters for the channels. The default state when the DFM feature is activated on a card is enabled. Because DFM is a purchased option, the Cisco Technical Assistance Center (TAC) must activate on the applicable nodes before you use the **cnfchdfm** command. The cards that support the use of the LDM and HDM on the IGX node.

The DFM feature must be both *installed* and *enabled*. The DFM feature must be installed through software control at each node terminating the connection. If DFM is not installed for a pertinent node in the network, the **cnfchdfm** command has no effect at that node. Furthermore, you must use **cnfchdfm** at both ends of the connection to enable DFM.

Full Name

Configure channel DFM

Syntax

cnfchdfm <channel(s)> <7 | 8 | 16> [e | d]

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfchdfm 5.1 8
```

Description

Set the DFM pattern length to 8 bits for data channel 5.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 16:21 PST

     Maximum EIA      %     DFM Pattern          DFM
Channels     Update Rate      Util      Length          Status
5.1     15     100     8                                Enabled
5.2-4    2     100     8                                Enabled









Last Command: cnfchdfm 5.1 8


Next Command:
```

Table 7-13 cnfchdfm–Parameters

Parameter	Description
channel	Specifies the channel or range of channels.
7/8/16	Specifies the pattern length in bits for the DFM algorithm. The default is 8 bits

Table 7-14 cnfchdfm–Optional Parameters

Parameter	Description
e/d	Enables or disables DFM. The default is "e." Note that DFM works at rates no higher than 128 Kbps.

cnfcheia

Sets the sampling rate for the updating EIA control leads. You can set this rate from 0 (no sampling) to 20 updates per second and defaults to 2 seconds. This rate governs the polling interval and packet generation rate for the EIA leads associated with the channel.

At 20 updates/second, the control leads are polled for changes every 50 msec. Therefore, changes occurring more rapidly than that may not be detected. If there is no change in EIA lead status, no packet is sent. A minimum of one update per second is sent if the maximum update rate chosen is from 1 to 20. If the connection is configured in such a way that an implied isochronous clock is detected, the update rate is always 20 per second in the same direction as that of the clock signal. For 1.544 Mbps data connections, this defaults to 0. This does not affect EIA sampling rates of “fast EIA” or “embedded” EIA leads.

Full Name

Configure EIA update rate for channels

Syntax

cnfcheia <channel(s)> <update_rate>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfcheia 5.1 15
```

Description

Set the EIA update rate to 15 sec. for data channel 5.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 16:20 PST

             Maximum EIA     %     DFM Pattern     DFM
Channels      Update Rate     Util     Length     Status
5.1                    15     100     8          Enabled









Last Command: cnfcheia 5.1 15


Next Command:
```

Table 7-15 cnfcheia–Parameters

Parameter	Description
channel	Specifies the channel or range of channels to over which to configure the EIA update rate.
update rate	Specifies the maximum EIA update rate in updates per second.

cnfcldir

Sets the control lead direction for pins 11 and 23 on the EIA/TIA-232 data channels of an SDP or HDM card set. This allows the control leads to carry “backward” channels. Pins 11 and 23 on an EIA/TIA-232 interface are bi-directional. The signals on these pins can have various names, such as SI, SF, CH, CI, and QM. To display control lead information about pins 11 and 23, use the **dspbob** command. Use the **cnfict** command to configure the behavior of all output leads.

Full Name

Configure control lead direction

Syntax

cnfcldir <channel> <lead> <direction>

Related Commands

cnfict, dspbob, dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfcldir 3.1 11 input
```

Description

Configure lead number 11 of channel 3.1 to be an input. The screen example shows the display after the system has accepted the input as valid.

System Response

```
pubsigx1       TN    SuperUser       IGX 8420    9.2      Aug. 14 1998 00:30 GMT

Port:           3.1
Interface:      V35   DCE
Clocking:       Normal

      Inputs from User Equipment               Outputs to User Equipment
 Lead  Pin          Lead  Pin           Lead  Pin          Lead  Pin
 RTS   C                                CTS   D
 DTR   H                                DSR   E
 TxD   P/S                              DCD   F
 TT    U/W                              RI    J
                                        TM    K
                                        RxD   R/T
                                        RxC   V/X
                                        TxC   Y/a


Last Command: cnfcldir 3.1 11 input


Next Command:
```

Table 7-16 cnfcldir–Parameters

Parameter	Description
channel	Specifies the EIA/TIA-232 data channel whose control lead direction to configure.
pin number	Specifies the pin number of the control lead. The valid pin numbers are 11 and 23.
direction	Specifies the direction of the control lead signal. Valid control lead directions are: Input: The control lead acts as an input to the IGX node. This is the default. Output: The control lead acts as an output from the IGX node.

cnfdch

The **cnfdch** command lets you configure a super-rate data connection that has idle code suppression (ICS) enabled or disabled, before you add a connection. The ICS information in the **cnfdch** screen is identical to that of **dspchcnf**.

The idle code suppression feature provides a way to stop fast packet generation on an Nx64 super-rate PVC connection when the connected PBX has terminated a video call and there are no video calls in progress. Traffic on the data network is therefore reduced. Bursty data can then use this un-used bandwidth.

The idle code suppression feature enables the UVM and CVM to detect the on-hook condition of video conferencing calls. During the on-hook phase, FastPacket generation ceases, resulting in more trunk bandwidth becoming available. All connections that use ForeSight can use this bandwidth, resulting in higher information rate.

The **cnfdch** command is blocked if one or more specified channels is carrying a voice connection (including t-type).

If some of the specified channels do not yet have any connection attached, those channels will be initialized to a data type channel.

The **cnfdch** command prompts you to enable or disable idle code suppression with the following prompt:

```
Enable or Disable Idle Code Suppression (e/d)?[d]:
```

The **cnfdch** command is a level 2 access command, which lets you configure a super-rate data connection that has idle code suppression (ICS) enabled or disabled.

The **cnfdchl** command lets you configure a channel before you add a connection. The configuration remains the same when connections are removed and added again. This configuration will be removed when the associated line is deactivated.

The Idle Code Suppression feature supported in Release 9.2 provides a way to stop fast packet generation on an Nx64 super-rate PVC connection when the connected PBX has terminated a video call. No video traffic will be generated when a video call has terminated.

Because there are multiple channels involved in an Nx64 data connection, the idle code suppression configuration of the first channel in the Nx64 channel will be used for the entire connection bandwidth.

The **cnfdch** command is available for level 2 users and above; that is, you must have at least privilege level 2 or above to use this command. Use the **cnfdch** command to configure a channel before you add a connection. The configuration will stay the same even if connections are removed and added again.

Because there are multiple channels involved in an Nx64 data connection, the idle code suppression configuration of the first channel in the Nx64 bundle will be used for the entire connection.

Configuration must be done for each endpoint of a connection. When the state of an ICS connection changes, no network message is sent to the other end. You can choose to configure the other end if ICS is supported on the other end also. To maximize the benefit of the idle code suppression feature, you should enable ICS on both endpoints of the connection.

To interwork with HDM/LDM/SDP/LDP cards, idle code suppression on UVM/CVM/CDP channel will be turned off for any super-rate connection that also terminates on HDM/LDM/SDP/LDP.

All super-rate data connections will have their ICS state set to “disabled” state unless they have been specifically configured with the **cnfdch** command to be enabled, or through Cisco WAN Manager (or another SNMP manager application).

How Idle Code Suppression Works

When a video call terminates, the PBX generates the appropriate line idle code (for example, 0x7f for mu-law). Per ITU H.221 video coding scheme, no byte will be repeated on one DS0 for more than 80 times. In the case of BONDING protocol, the maximum is 256 (32 msec). The firmware can distinguish a video call and an idle channel carrying idle code. Idle code suppression is not programmable. Any byte that repeats for more than 32 msec in all DS0s in a super-rate connection will be suppressed.

Switch software determines idle code suppression capability on a card based on firmware model and revision number (for example, it considers that the CVM card supports idle code suppression starting with model B revision E firmware).

The idle code suppression feature for the UVM and CVM cards on the IGX detects the idle (on-hook) state of a video call, which uses an nx64k data connection, and suppresses packet transmission during this idle condition. The UVM or CVM at the far end plays out the idle code during this time. You disable or enable and display the status of idle code suppression on a per-connection basis through the switch software CLI **cnfdch** and **dspchcnf** commands.

The UVM and CVM card firmware identifies an on-hook or idle condition by detecting repetition of idle codes. These codes can be present in the regular video traffic also (that is, in H.221 or BONDING frames). The code must repeat a certain number of times before it can be concluded that the call is on-hook. It is not necessary to look for specific idle codes. Any byte-code repeating beyond the threshold (about 32 ms) indicates idle channels. The firmware monitors byte repetition on each nx64 connection for which this feature is enabled. On detecting repetition beyond the specified threshold, FastPacket generation for such a connection would cease. This results in the remote side of the connection to under-run. In this condition, it would transmit the previously transmitted byte on each DS0 for the connection. The UVM/CVM continues to monitor DS0s for the connection to detect a change in data received. Any change would indicate an off-hook condition, after which FastPacket transmission would resume.

The idle code suppression feature consists of IGX switch software Release 9.2, and requires UVM model E firmware and CVM/CDP model B revision E firmware. The new UVM/CVM/CDP firmware ensures that idle code suppression can interoperate with UVM/CVM/CDP cards that do not have idle code suppression capability. Such a configuration means that fast packet generation stops in one direction while the other end continues to generate fast packets. This behaves exactly the same as enabling idle code suppression on one side but not on the other side.

All back card types supported by UVM/CVM/CDP support idle code suppression.

Configuring Idle Code Suppression

The standard configuration involves UVM/CVM/CDP cards on both ends of the video connections. An Nx64 super-rate PVC is set up between the two cards. Each video codec is connected through a PBX which is attached to the UVM/CVM/CDP cards.

The idle code suppression feature is available on IGX. When idle code suppression is disabled on a connection (the default), switch software behaves the same as in releases previous to Release 9.2.

UVM/CVM/CDP cards that support idle code suppression can interwork with HDM/LDM/SDP/LDP cards. If the UVM/CVM/CDP channels are configured with idle code suppression enabled, the actual channel will not have idle code suppression enabled if the other end of the connection is not a UVM/CVM/CDP (that is, HDM/LDM/SDP/LDP).

All connection limitations that exist in Release 9.1 remain the same. A t-type connection is not supported. On a VNS controlled network, t-type SVCs are used for video calls. VNS does not support Nx64 super-rate connections.

The idle code suppression feature provides a way to stop fast packet generation on an Nx64 super-rate PVC connection when the connected PBX has terminated a video call. No video traffic will be generated when a video call has terminated. Current UVM/CVM/CDP implementation restricts N to between 1 and 8. This feature is intended to work with video codecs that implement H.221 or BONDING protocol only.

The basic idea is that when a video call terminates, the PBX will generate the appropriate line idle code (for example, 0x7f for mu-law). Per the ITU H.221 video coding scheme, no byte will be repeated on one DS0 for more than 80 times. In the case of BONDING protocol, the maximum is 256 (32 msec). The firmware can distinguish a video call and an idle channel carrying idle code. It is important to understand that the idle code is not programmable. It is a more general approach where any byte that repeats for more than 32 msec in all DS0s in a super-rate connection will be suppressed.

Switch software's job is mainly one of providing interfaces for configuring of channels by enabling/disabling idle code suppression for super-rate data connections. In turn, switch software informs the UVM/CVM/CDP card if idle code suppression should be used on each of the super-rate connections.

No new hardware is needed. All back card types supported by UVM/CVM/CDP support the idle code suppression feature.

Interface with Cisco WAN Manager and other Network Management Systems

The SNMP agent interface on the IGX provides the following operations: Get/Set of MIB information of the desired state of idle code suppression (enabled/disabled).

If a request fails, a General Error is returned to Cisco WAN Manager. An error string is logged in the switch software error table. Cisco WAN Manager can then optionally obtain the error string from switch software. Examples of error messages are "Card in slot does not support Idle Code Suppression" and "E1 CAS and Voice Channels - Not Configured".

Inserting/Removing Cards (Idle Code Suppression Mismatch)

Given an active non-Y-redundant UVM/CVM/CDP card without ICS support, upgrades to a card with ICS are allowed. However, you cannot downgrade a card with ICS capability to a card that does not support ICS (see Table 7-17).

Given a pair of cards in a Y-redundancy configuration, whether any of them is active or not, they must have the same ICS capability (see Table 7-18).

Table 7-17 Active Line that is Not in Y-Redundant Pair

ICS Support		
Old Card	**New Card**	**Comment**
NO	NO	OK - same card
NO	YES	OK
YES	NO	mismatch
YES	YES	OK - same card

Table 7-18 Card is Configured for Y-Redundancy

ICS Support		
Old Card	New Card	Comment
NO	NO	OK
NO	YES	OK but ICS is not available until both cards support ICS
YES	NO	Mismatch if both cards support ICS before
YES	YES	OK

Y-Redundancy

To ensure that cards with the same ICS capability be allowed to be a Y-redundancy pair, **addyred** blocks cards that have different idle code suppression capability.

ICS Support		
Primary Card	Secondary Card	Comment
NO	NO	OK
NO	YES	addyred blocked
YES	NO	addyred blocked
YES	YES	OK

Upgrading and Downgrading the Idle Code Suppression Feature

Given an active non-Y-redundant UVM/CVM/CDP card without idle code suppression support, an upgrade to a card with ICS support is allowed. Downgrading a card with ICS capability to a card without ICS capability is not allowed.

Upgrading the ICS feature to a Y-redundancy pair that does not support the ICS feature is not allowed. The Y-redundancy pair must be deleted first to upgrade the feature. After both cards complete the ICS upgrade, the cards can be added as a Y-redundancy pair.

Table 7-19 Active Line that is Not in Y-Redundant Pair

ICS Support		
Old Card	New Card	Comment
NO	NO	OK - same card
NO	YES	mismatch
YES	NO	mismatch
YES	YES	OK - same card

Table 7-20 Card is Configured for Y-Redundancy

ICS Support		
Old Card	**New Card**	**Comment**
NO	NO	OK
NO	YES	OK but ICS is not available until both cards support ICS
YES	NO	Mismatch if both cards support ICS before
YES	YES	OK

Limitations with Idle Code Suppression

T-type connections are not supported. On a VNS controlled network, t-type SVCs are used for video calls. VNS does not support Nx64 super-rate connections.

This feature is intended to work with video codecs that implement H.222 or BONDING protocol only.

Full Name

Configures a voice connection to have idle code suppression enabled/disabled.

Syntax

cnfdch *<channel><ch_ics_state>*

Related Commands

dspchcnf, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
2–6	Yes	No	IGX	No

Example 1

```
cnfdch 9.1.3–5
```

Description

Display configuration values for channels 9.1.3 through 9.1.5.

```
sw176          TRM   StrataCom       IGX 8420    9.2.0r    Apr. 3 1998 17:28 PST

            Maximum EIA     %      DFM Pattern     DFM    Idle Code   PreAge
From 9.1.3  Update Rate    Util      Length       Status    Suppr      (usec)
9.1.3-5         -           -         -            -       Disabled        0



This Command: cnfdch 9.1.3-5
```

Table 7-21 cnfdch – Parameters

Parameter	Description
channel	*slot.line.channel* for UVM or *line.channel* for CVM/CDP. A channel range is allowed.
ch_ics_state	Channel idle code suppression state: d for disabled; e for enabled.

Full Name

Configures a voice connection to have idle code suppression enabled/disabled.

Syntax

cnfdch <*channel*><*ch_ics_state*>

Related Commands

cnfdch 9.1.3–5

cnfdchtp

Configures a CDP, CVM, or LDP or LDM DDS port interface type to OCU or DSU. When configuring DDS operations, this command returns an error if executed on a slot with an EIA/TIA-232 back card. It forces a back card slot from EIA/TIA-232 mode to DDS mode if a back card is not installed and there are no connections. Any Y-cable association is deleted in this case. The clocking tracks the DDS port interface type. OCU type interfaces are configured as “looped”, and DSU type interfaces are configured as “normal”. The default interface is “DSU”.

When configuring CDP, CVM, LDP, or LDM operation, this command configures DCE types as “normal” clocking and DTE types as “looped” clocking. The default type is DCE. For T1 lines, DS0A on T1 unassigned signalling is configurable. When a connection is not present, voice channels are converted to data channels.

Full Name

Configure data channel interface type

Syntax

cnfdchtp <channel> <interface type> [unassigned signaling]

Related Commands

none

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfdchtp 31.1 oc
```

Description

Configure DDS channel 31.1 as OCU.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:30 MST

Data Channel:      31.1
Interface:         DDS-4   OCU Config
Clocking:          Looped

            Interface Control Template for Connection while ACTIVE

 Lead Output Value   Lead     Output Value
 DSR   ON             CTS      ON
 DCD   ON






Last Command: cnfdchtp 31.1 oc


Next Command:
```

Example 2

cnfdchtp 22.1 dce

Description

Configure channel 22.1 as DCE with T1 unassigned signalling.

System Response

```
beta           TRM   YourID:1        IGX 32    9.2    Aug. 15 1998 17:30 MST

Data Channel: 22.1
Interface:MissingDDS0A DCE Configuration
Clocking:Normal

            Interface Control Template for Connection while ACTIVE

 LeadOutput ValueLeadOutput Value
 DSRONCTSON
 DCDON






Last Command: cnfdchtp 22.1 dce t


Next Command:
```

Table 7-22 cnfdchtp–Parameters

Parameter	Description
channel	Specifies the channel to configure in the format <slot>. <port>.
interface type	Specifies the interface type to configure. An LDP or LDM DDS port can be configured as DSU or OCU (enter ‘ds’ or ‘oc’). A CDP or CVM port can be configured as DCE or DTE (enter ‘dce’ or ‘dte’).

Table 7-23 cnfdchtp–Optional Parameters

Parameter	Description
channel	Specifies the channel to configure in the format slot. port
unassigned signalling	Specifies an optional parameter for T1 lines to indicate DS0A or T1 unassigned signalling. Enter ‘d’ for DS0A or ‘t’ for T1.

cnfdclk

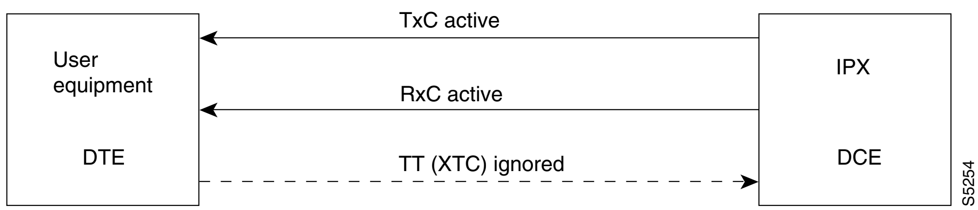
Configures the clocking for a data channel. In general, the clock configuration may be normal, split, or looped for an SDP or HDM (fewer options for an LDP or LDM). The clock configuration of each channel of a connection determines how the clock will be propagated through the network, and how external equipment should be synchronized.

If clocking is not set correctly, there may be no synchronization, and the connection will operate in a plesiochronous mode. Each data port can be configured independently to act as either DCE or DTE by adjusting the jumper (SDI card) or changing the adapter cable (LDI card) on the data interface card. The effect of the clocking type designated depends on whether each data port is configured as DTE or DCE. The following data clocking configurations are possible with the **cnfdclk** command:

DCE-Configured Data Port: Normal Clocking

When the data port is configured as DCE, selecting a clocking type of "n" (for normal) results in clocking as illustrated below. The IGX node, acting as DCE, provides both the transmit and receive data clocks to the user equipment.

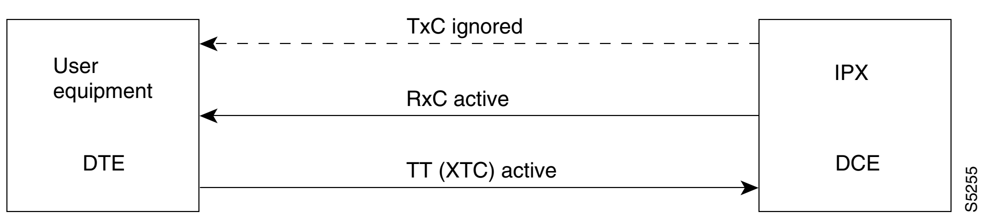
Figure 7-1 Normal Clocking on a DCE



DCE-Configured Data Port: Split Clocking

When the data port is configured as DCE, selecting a clocking type of "s" (for split) results in clocking as illustrated below. In "split" clocking, TT may be generated independently of RxC. The maximum data rate for split clocking is 112 kbps.

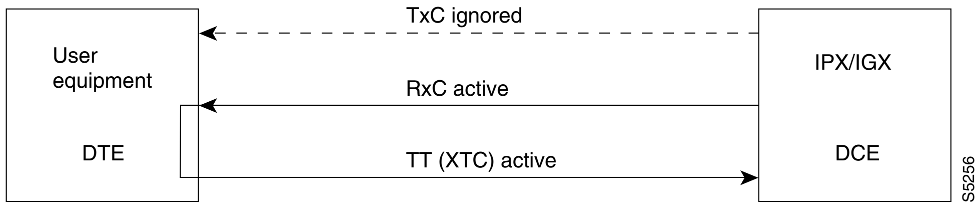
Figure 7-2 Split Clocking on a DCE



DCE-Configured Data Port: Looped Clocking

When the data port is configured as DCE, selecting a clocking type of "l" (for looped) results in clocking as illustrated below. The "Terminal Timing" signal, called TT or XTC, is simply RxC looped back from the user equipment. In this configuration, it is important that the two clocks (RxC and TT) be frequency locked. This clocking configuration is supported for all data rates.

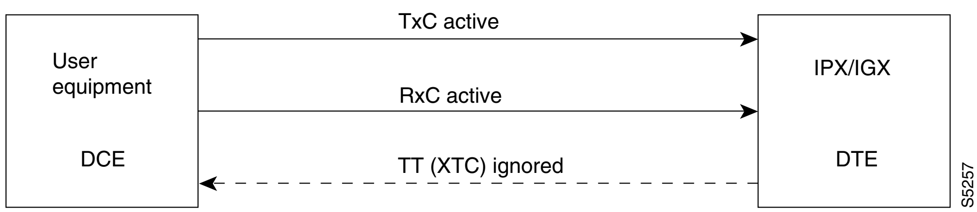
Figure 7-3 Looped Clocking on a DCE



DTE-Configured Data Port: Normal Clocking

When the data port is configured as DTE, selecting a clocking type of "n" (for normal) results in clocking as illustrated below. The IGX, acting as DTE, receives both the transmit and receive data clocks from the user equipment. When the user equipment is not referenced to the network clock, the maximum data rate for this configuration is 112 kbps. The two clocks must be frequency-locked for proper operation.

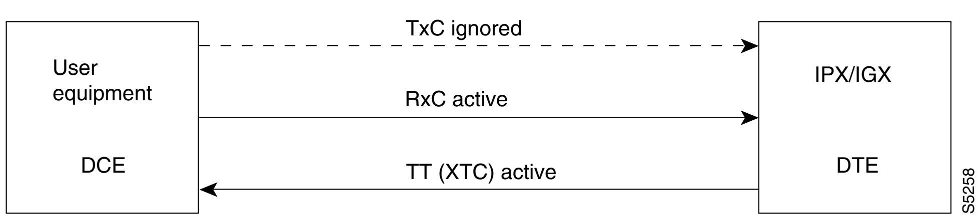
Figure 7-4 Normal Clocking on a DTE



DTE-Configured Data Port: Split Clocking

When the data port is configured as DTE, selecting a clocking type of "s" (for split) results in the clocking as illustrated below. When the user equipment is not referenced to the network clock, the maximum data rate for this configuration is 112 kbps. The two clocks must be frequency-locked for proper operation.

Figure 7-5 Split Clocking on a DTE

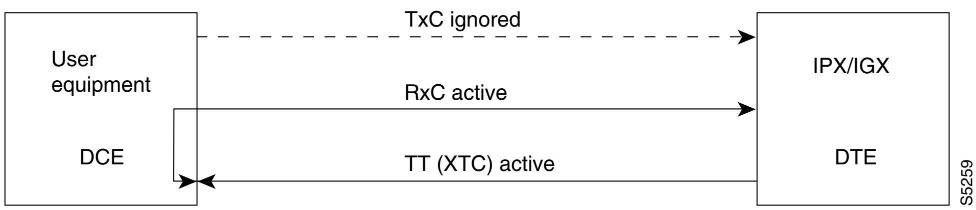


DTE Configured Data Port: Looped Clocking

If you specify clocking type of "l" (looped) when the data port is in DTE mode, the result is the clocking arrangement shown in Figure 7-6. The RxC clock signal is the TT(XTC) signal looped back to the IGX node by the user equipment. The network supports this clocking configuration for all data rates. The restrictions to the data clocking schemes are:

- Except for special cases, isochronous clocking is limited to data rates of 112 Kbps or less. For higher data rates, all clocks must be frequency-locked to the network.
- For any port there must be only one isochronous clock in a direction. Any situation where user equipment provides two clock signals that are not locked is subject to slippage.
- Slippage may also occur in any situation where there are opposing user clocks for a single direction of data.

Figure 7-6 Looped Clocking on a DTE



Full Name

Configure data channel clocking type

Syntax

cnfdclk <channel> <normal/split/looped>

Related Commands

none

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfdclk 5.1 n
```

Description

Configure the clocking for channel 5.1 to normal.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:41 PST

Data Channel:      5.1
Interface:         V35   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead      Output Value   Lead       Output Value
 RI(J)     OFF            DSR (E)    ON
 CTS(D)    ON             TN (K)     OFF
 DCD(F)    ON





Last Command: cnfdclk 5.1 n


Next Command:
```

Table 7-24 cnfdclk–Parameters

Parameter	Description
channel	Specifies the channel to configure in the format <slot>. <port>.
normal/split/looped	Specifies the clocking type to assign to the channel. Valid clocking types are: • n for Normal • s for Split • l for Looped

cnfict

Sets the interface control template signals. The signals that can be set using **cnfict** depend on the type of back card used and whether the hardware is configured for DCE or DTE. On an IGX node, the applicable front cards are the LDM, HDM, FRM, CVM (for data), and FTM (for data). Each data channel has a default interface control template for its active, conditioned, and looped near and far states. The **cnfict** command is used to change a control template. Each interface control lead in each template is individually configured.

When Y-cable redundancy is in effect, the control template configuration for the data channels terminating at the primary slot is also applied to the data channels of the secondary slot. Any configuration information for the secondary slot is ignored. Table 7-25 shows the configurable leads and the equivalence between EIA/TIA-232C, EIA/TIA-232D, EIA/TIA-449, V.35, and X.21 interfaces. The leads are configurable for each type of data interface supported by the IGX node. The entries under the "IGX Name" column indicate the abbreviations to use when specifying input or output leads on the command line. A node treats leads impartially for non-interleaved connections. Any signal received on an EIA pin at one end may be transmitted to any pin at the other end, up to the maximum of 12 EIA leads on any interface type. For interleaved EIA connections, refer to the "Fast EIA" column. The column shows which leads are carried in the interleaved bytes of the data packets. All remaining leads are carried in standard control lead packets.

Table 7-25 Configurable Lead Names and Functions

Configurable Leads								
Source	**IGX Name**	**EIA/TIA-232C**	**EIA/TIA-232D**	**EIA/TIA-449**	**V.35**	**X.21**	**Fast EIA**	**Function**
DTE	RTS	CA	CA	RS	C		F4	Request to Send
DCE	CTS	CB	CB	CS	D		F4	Clear to Send
DCE	DSR	CC	CC	DM	E		F3	Data Set Ready
DCE	DCD	CF	CF	RR	F		F7	Data Carrier Detect (RLSD)
DCE	QM	QM	QM					Equalizer Mode
DTE	pin 11	11	11					Sometimes used for Data
DCE	SDCD	SCF	SCF					Secondary Data Carrier Detect
DCE	SCTS	SCB	SCB					Secondary Clear to Send
DTE	STxD	SBA	SBA				F5	Secondary Transmit Data
DTE	NS			NS			F7	New Sync
DCE	SRxD	SBB	SBB				F5	Secondary Receive Data
DCE	DCR	DCR						Divided Receiver Clock
DTE	RL		RL	RL			F6	Remote Loopback
DTE	SRTS	SCA	SCA					Secondary Request to Send
DTE	DTR	CD	CD	TR	H		F3	Data Terminal Ready
DCE	SQ	CG	CG	SQ				Signal Quality Detect
DCE	RI	CE	CE	IC	J**			Ring Indicator
DTE	SF	CH	CH	SF				Signal Rate Select (to DCE)
DCE	SI	CI	CI	SI				Signaling Rate Select. (to DTE)
DTE	BSY	BSY		IS			F1	Busy (In Service)
DCE	SB		TST	SB			F1	Test Indicator

Configurable Leads

Source	IGX Name	EIA/TIA-232C	EIA/TIA-232D	EIA/TIA-449	V.35	X.21	Fast EIA	Function
DTE	LL			LL			F2	Local Loopback
DCE	TM			TM	K[1]		F6	Test Mode
DTE	SS			SS				Select Standby
DTE	C					C		Control
DCE	I					I		Indicator

1 Applicable to SDP cards only.

Note that pins 11 and 23 on an EIA/TIA-232 port are bi-directional, and their default direction is input. See the **cnfcldir** command for information on changing the direction of these pins. The **cpyict** command can be used to copy an interface control template from one data channel to another. You can then edit it by using the **cnfict** command. The **dspbob** command displays the state of leads at specified intervals.

Full Name

Configure interface control templates

Syntax

cnfict <port> <template> <output> <source>

Related Commands

addextlp, dspict, tstport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfict 31.1 c SB on
```

Description

Configure the conditioned interface control template for channel 31.1 to SB on (DDS).

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 17:30 MST

Data Channel:      31.1
Interface:         DDS-4   OCU Config
Clocking:          Looped

            Interface Control Template for Connection while CONDITIONED

Lead     Output Value     Lead     Output Value
SB       ON               RI       OFF
DSR      OFF              CTS      ON
DCD      OFF





Last Command: cnfict 31.1 c   sb on


Next Command:
```

Example 2

cnfict 25.1 a CTS on

Description

Configure the active interface control template for channel 25.1 to CTS on (EIA/TIA-232).

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:36 MST

Data Channel:      25.1
Interface:         EIA/TIA-232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                 Lead    Output Value
 RI      OFF                           DSR     ON
 CTS     ON                            SRxD    ON
 DCR     OFF                           DCD     ON
 SCTS    ON                            SDCD    ON
 SQ      ON



Last Command: cnfict 25.1 a cts on


Next Command:
```

Example 3

`cnfict 5.1 active CTS on`

Description

Configure the active interface control template for channel 5.1 to CTS on (V.35).

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:29 PST

Data Channel:      5.1
Interface:         V35   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                     Lead     Output Value
 RI  (J) OFF                               DSR (E) ON
 CTS (D) ON                                TM  (K) OFF
 DCD (F) ON





Last Command: cnfict 5.1 a cts on


Next Command:
```

Table 7-26 cnfict—Parameters

Parameter	Description		
port	Specifies the data channel or Frame Relay port whose interface control template is to be configured. Entered as <slot.port>. On an IGX node, the applicable cards are the LDM, HDM, FRM, CVM, and FTM.		
template	Specifies which interface control template to configure for the channel and has the format <a/c/l/n/f>. Valid entries are listed below: The only valid template for a Frame Relay port, X.21 or V.35, is the ACTIVE template. Also, all the output leads have steady state values and do not follow local or remote inputs		
	Entry	**Template**	**Description**
	a	Active	The active control template is in effect while the data channel is active (normal operation) i.e. when the connection is routed and not failed.
	c	Conditioned	The conditioned control template is in effect when conditioning is applied to the data channel. The conditioned template is used when the network detects that it cannot maintain the connection because of card failures or lack of bandwidth (The connection is failed.)

Table 7-26 cnfict—Parameters (Continued)

Parameter	Description		
	l	Looped	The looped template is in effect when the data channel is being looped back in either direction. The looped template is used when **addloclp** or **addrmtlp** has been used to loop the connection within the network.
	n	Near loopback	The near template is in effect when running a **tstport n** command or an **addextlp n** command on a port. The port is configured such that the external near modem is placed in a loopback.
	f	Far loopback	The far template is in effect when running a **tstport f** command or an **addextlp f** command on a port. The port is configured such that the external far-end modem is placed in a loopback.
output	Specifies the output lead. Refer to the Configurable Lead information in the command description for abbreviations. Configurable output leads vary with the type of data interface (EIA/TIA-232, V.35, X.21, or EIA/TIA -449).		
source	Specifies how the lead is to be configured and has the format <on | off |local | remote> <input> [delay]. Valid source choices follow:		
	Source Options		
	on	The output lead is asserted.	
	off	The output lead is inhibited.	
	l	(for local) indicates that the output follows a local lead.	
	r	(for remote) indicates that the output follows a remote lead.	
	input	Specifies the name of the local or remote input lead that the output lead follows.	
	delay	Specifies the time in milliseconds that separates the "off" to "on" lead transitions. Delay is valid *only* when the output lead is CTS and the input lead is local RTS. "On" to "Off" lead transitions are not subject to this delay.	

cpyict

Copies all control template information associated with a given channel: the active template information, the conditioned template information, and the looped template information for near and far ends. Once copied, the control template information may be edited with the **cnfict** command. See the **cnfict** command for more information on interface control templates.

On an IGX node, the applicable front cards are the LDM, HDM, FRM, CVM (for data), and FTM (for data).

Full Name

Copy interface control templates

Syntax

cpyict <source_port> <destination_port>

Related Commands

cnfict, dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cpyict 25.1 25.2
```

Description

Copy the interface control template for data channel 25.1 to channel 25.2.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2   Aug. 15 1998 17:40 MST

Data Channel:        25.2
Interface:           EIA/TIA 232   DCE
Clocking:            Normal

            Interface Control Template for Connection while ACTIVE

 Lead     Output Value                    Lead   Output Value
 RI       OFF                           DSR      ON
 CTS      ON                            SRxD     ON
 DCR      OFF                           DCD      ON
 SCTS     ON                            SDCD     ON
 SQ       ON




Last Command: cpyict 25.1 25.2


Next Command:
```

Table 7-27 cpyict—Parameters

Parameter	Description
source channel	Specifies the data channel or Frame Relay port whose interface control template information to copy.
designating channel	Specifies the data channel or Frame Relay port that will receive the copied control template information.

delcon

Removes connections from the network. After entry of the channel or range of channels to delete, a prompt requests confirmation of the selection. Connections can be deleted from the node at either end of the connection. Do not delete a connection when the node at the other end of the connection is unreachable. The unreachable node does not recognize the deletion. It is especially important not to delete a connection to an unreachable node and then connect that channel to another node.

Full Name

Delete connections

Syntax

delcon <channel(s)>

Related Commands

addcon, dspcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
delcon 3.1
```

Description

Delete connection 3.1.

System Response

```
pubsigx1       TN    SuperUser       IGX 8410    9.2       Aug. 14 1998  00:53 GMT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
 3.1            pubsigx1    3.2             Ok     64                  7/8
 3.2            pubsigx1    3.1             Ok     64                  7/8
 5.1.101        pubsigx1    5.1.102         Ok     fr
 5.1.102        pubsigx1    5.1.101         Ok     fr
 5.1.111        pubsigx1    9.1.1           Ok     atfr
 5.1.203        pubsigx1    5.1.204         Ok     fst
 5.1.204        pubsigx1    5.1.203         Ok     fst
 5.1.222        pubsigx1    8.5.2           Ok     atfst
 5.1.223        pubsigx1    8.5.3           Ok     atfst
 8.5.1          pubsigx1    5.1.111         Ok     atfr
 8.5.2          pubsigx1    5.1.222         Ok     atfst
 8.5.3          pubsigx1    5.1.223         Ok     atfst
 13.1           pubsigx1    13.2            Failed p

This Command: delcon 3.1


Delete these connections (y/n)?
```

Table 7-28 delcon—Parameters

Parameter	Description
channel	Specifies the data channel or channels to delete. The format is *slot.port*.

dspchcnf

Displays configuration details for data channels. This command provides information for voice, Frame Relay, ATM, and data channels. For data connections on the specified card and starting with the specified channel, the **dspchcnf** command displays the following information:

- Maximum EIA update rate
- Percentage of channel utilization
- DFM pattern length
- DFM status.(enabled or disabled)
- Idle code suppression (enabled or disabled)
- PreAge (in microseconds)

The data cards that support this command are the HDM, LDM, UVM, and CVM/CVP cards on the IGX node.

Full Name

Display channel configurations

Syntax

dspchcnf <start_channel>

Related Commands

cnfdch, cnfchadv, cnfchdfm, cnfchdl, cnfcheia, cnfchgn, cnfchtp, cnfchutl, cnffrcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspchcnf 3.1`

Description

Display the configuration values for data channels starting at 3.1.

System Response

```
pubsigx1       TN    SuperUser       IGX 8410    9.2 Jan. 9 1998 00:04 GMT

            Maximum EIA     %      DFM Pattern     DFM
Channels    Update Rate    Util      Length       Status
3.1-4             2        100         8         Enabled











Last Command: dspchcnf 3.1


Next Command:
```

Example 2

dspchcnf 9.1.3

Description

Display the configuration values for data channels starting at channel 9.1.3.

System Response

```
sw176          TRM    StrataCom       IGX 8420    9.2.a2    Apr. 3 1998  17:32 PST

            Maximum EIA     %      DFM Pattern     DFM    Idle Code   PreAge
From 9.1.3  Update Rate    Util      Length       Status    Suppr      (usec)
9.1.3-8        -            -          -          -        Enabled         0





Last Command: dspchcnf 9.1.3
```

Table 7-29 dspchcnf–Parameters

Parameter	Description
start channel	Specifies the starting channel using the format *slot.port*

dspcon

Displays connection information for a specified channel. The information displayed includes:

- The channel numbers for both the local and remote ends of the connection.
- The node names at both ends of the connection.
- The routing restriction.
- The class of service (COS) of the connection. For an explanation of COS, see the chapter "Optimizing Traffic Routing and Bandwidth".
- The connection route listing the end nodes and any intermediate nodes.
- The preferred route for the connection (if configured).
- If cost-based AutoRoute is configured, displays maximum and current costs for a connection route.
- The status of the cards associated with the connection.
- Any Y-cable conflicts.
- The compression status (VAD on or off, ADPCM on or off, DFM on or off, Frame Relay compression on or off).
- The connection descriptor (if configured).

The status that may be displayed includes:

OK	Connection OK
FAILED	Connection failed

Full Name

Display connection

Syntax

dspcon <channel>

Related Commands

cnfchec, cnfrtcost

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspcon  13.1
```

Description

Display information for data channel 13.1. This connection is FAILED and "off hook."

System Response

```
pubsigx1       TN    SuperUser       IGX 8420    9.2       Aug. 14 1998 00:20 GMT

Conn:  13.1              pubsigx1    13.2               p
Desc: bogus                                                     Status:Failed




Path:   Route information not applicable for local connections




pubsigx1  Line 13: Failed        OFFHK pubsigx1  Line 13: Failed        OFFHK



Last Command: dspcon 13.1


Next Command:
```

Table 7-30 dspcon–Parameters

Parameter	Description
channel	Specifies the channel. The command displays connection information for one channel at a time. The format for channel specification is *slot.channel*.

dspcons

Displays a summary of the connections on an IGX node. Status that you can display includes:

OK	Connection OK
FAILED	Connection failed

Table 7-30 describes the fields in the **dspcons** screens.

Table 7-31 Fields in the dspcons Display

Fields	Description
Local Channel	The connection's channel at this node.
Remote Node Name	The name of the node at the other end of the connection.
Remote Channel	The connection's channel at the remote node.
State	The state of the connection(s) as follows: OKRouted DownDowned OK DownedWaiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command. FailedUnrouted, but trying
Type	The type of connection (v = voice, d = data, fr = Frame Relay, atfr = ATM to Frame Relay interworking, atfst = ATM to Frame Relay interworking with ForeSight, -fail = failed connections; data rate in kbps for data)
Route Avoid	The type of lines to avoid when routing (satellite lines, terrestrial lines, lines with zero code suppression).
Compression	The type of compression applied to the connection (PCM, PCM and VAD, ADPCM, VAD and ADPCM for voice connections), (DFM or ICS for data connections).
COS	Class Of Service.
Loopback	A connection with a local loopback is indicated by a right parenthesis symbol between the "Local Channel" and "Remote NodeName" columns. A Frame Relay connection with a port loopback is indicated by a right bracket symbol between the "Local Channel" and "Remote NodeName" columns. A connection with a remote loopback is indicated by a right parenthesis symbol before the channel number in the "Remote Channel" column.

Full Name

Display connections

Syntax

dspcons [start_channel] [nodename] [connection type]

Related Commands

addcon, cnfchadv, chfchdfm

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspcons

Description

Display a summary of all connections.

System Response

```
alpha  TRM     YourID:1   IGX 8410  Rev:9.2     Aug. 16 1998 09:42 PST

 Local      Remote      Remote                                      Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 5.1        beta       25.1      Ok      256     7/8   0     L
 9.1        gamma      8.1       Ok      v             0     L
 9.2        beta       19.2      Ok      v             0     L
14.1        gamma      15.1      Ok      v       VAD   2     L










Last Command: dspcons


Next Command:
```

Example 2

dspcons

Description

Display the connection with descriptors.

System Response

```
pubsigx1       TN    SuperUser       IGX 8410    9.2    July 25 1998 06:40 PDT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Descriptor
 5.1.100        pubsigx3    5.1.200         Ok     fr
 6.1            pubsigx2    11.1            Ok     56







Last Command: dspcons +d


Next Command:
```

Example 5

dspcons

Description

Display a summary of all connections.

System Response

```
sw176          TRM   StrataCom       IGX 16    9.2.a2    Apr. 3 1998  17:36 PST

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
 9.1.2-3        sw176       9.1.2-3         Ok     2x64                7/8
 9.1.4          sw176       9.1.4           Ok     1x64      ICS       7/8
 9.1.6          sw176       9.1.6           Ok     g729r8    LDCELP
 9.1.7          sw176       9.1.7           Ok     1x64                7/8
 9.1.9          sw176       9.1.9           Ok     c32       VAD/ADPCM
 9.1.10-13      sw176       9.1.10-13       Ok     4x64      ICS       7/8
```

Table 7-32 dspcons–Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. The start channel is specified as follows: slot.channel | slot.port.dlci | slot.vpi.vci
node name	Specifies that only connections to this remote node from the local node be displayed. If no “nodename” is designated, connections from the local node to all other nodes are displayed.

Parameter	Description	
connection type	Specifies that only connections of this type be displayed. If no "connection type" is designated, all connections appear. When you enter the connection type on the command line, precede it with a hyphen (-). Valid connection types to display are:	
	-v	Displays only voice connections.
	-d	Display only data connections.
	-f	Displays Frame Relay connections.
	-abit	Shows A-bit (nni) status.
	-fabit	Shows connections with failed A-bit (nni) status.
	-fail	Shows only failed connections.

dsprtcache

This command displays the cache of all cost-based routing connections. The optional *index* parameter lets you specify a cache entry index. The optional *c* parameter clears the cache.

Full Name

Display cost-based route cache

Syntax

dsprtcache [index] [c]

[index] specifies the cache entry index

[c] specifies to clear the entire cache or a single entry

Related Commands

dspcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsprtcache`

Description

Display route cache contents, and let you monitor and manually clear the cache.

System Response

```
pissaro     TN      StrataCom          BPX 15      9.1     Jun. 18 1997 11:11 GMT
Route Cache (Summary)
Index   Use   Cost    Delay    Restrict   Load     VPC      Hops       RemoteNode
0       Yes    1       Yes     No         None      VBR      No      2     lautrec
1       Yes    6       Yes     No         *s        BDB      No      3     vangogh
2       Yes    9       Yes     No         None      BDA      No      3     matisse
3       Yes    3       Yes     No         *t        BDB      No      3     rousseau
4       Yes     1       Yes     No         None      CBR      No      3     seurat  <-
current
5       No     0       No      No         None      ---      No      0     ---
6       No     0       No      No         None      ---      No      0     ---
7       No     0       No      No         None      ---      No      0     ---
8       No     0       No      No         None      ---      No      0     ---
9       No     0       No      No         None      ---      No      0     ---
10      No     0       No      No         None      ---      No      0     ---
11      No     0       No      No         None      ---      No      0     ---

Last Command: dsprtcache

Next Command:
```

Table 7-33 dsprtcache—Parameters

Parameter	Description
index	Specifies a particular route entry within the cache. When used with the c parameter, the route is either displayed or cleared from the cache.
c	Clears the cache, or if you also enter the index parameter, clears the route cache specified by the index number.

dspict

Displays interface control template information for data channels and Frame Relay ports. Displayed information includes:

- The specified channel.
- The type of template: a, c, l, n, or f.
- The associated output leads and their status:

  ON.
  OFF.
  Following a local input.
  Following a remote input.

For Frame Relay ports, the entire port configuration screen is displayed (see **dspfrport** command). The input being followed, where applicable, is specified. Any RTS to CTS delay is also shown.

Full Name

Display interface control template

Syntax

dspict <port> <template>

Related Commands

cnfict, cpyict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX	No

Example 1

`dspict 25.1`

Description

Display the active interface control template for 25.1.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:33 MST

Data Channel:      25.1
Interface:         EIA/TIA 232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                  Lead    Output Value
 RI      OFF                            DSR     ON
 CTS     ON                             SRxD    ON
 DCR     OFF                            DCD     ON
 SCTS    ON                             SDCD    ON
 SQ      ON



Last Command: dspict 25.1


Next Command:
```

Table 7-34 dspict—Parameters

Parameter	Description
channel	Specifies the channel. The format of the channel specification is *slot.port*.
template	Specifies which control template to display for the channel. There are three templates available for data channels and one available (a only) for Frame Relay ports. You also specify which end of the circuit. **a** Active control template (normal operation). The only choice for a Frame Relay port. **c** Conditioned control template (when connection fails). **l** Looped control template (with local or remote loopback). **n** Near. **f** Far.

prtchcnf

Prints the configuration details for voice channels or data channels. This command uses the same syntax, and prints the same information as the **dspchcnf** command. See the **dspchcnf** description for syntax and output information.

Full Name

Print channel configurations

Syntax

prtchcnf <start_channel>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

`prtchcnf 14.1`

Description

Print the configuration values of circuit line 14.1.

System Response

None available as this command produces hardcopy.

Table 7-35 prtchcnf–Parameters

Parameter	Description
start channel	Specifies the channel at which the printout begins. The format is *slot.channel*.

prtcons

Prints a summary of connections terminated at the IGX node.

Full Name

Print connections

Syntax

prtcons [start_channel] [nodename] [type]

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

`prtcons`

Description

Print a summary of all connections.

System Response

None available as this command produces hardcopy.

Table 7-36 prtcons—Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. The start channel is specified as follows: slot.channel
node name	Specifies that only connections to this remote node from the local note be displayed. If no *nodename* is designated, connections from the local node to all other nodes are displayed.

Table 7-36 prtcons—Optional Parameters (Continued)

Parameter	Description
connection type	Specifies that only connections of this type be displayed. If no *connection type* is designated, all connections display. When you enter the connection type on the command line, it must be preceded with a hyphen (-). Valid connection types to display are: -v Displays only voice connections. -d Display only data connections. -f Displays Frame Relay connections. -nni Displays Frame Relay network to network connections for failed connections only. -fail Displays only failed connections.

prtict

Prints the configuration details for voice channels or data channels. This command uses the same syntax, and prints the same information as is displayed using the **dspchcnf** command. See the **dspchcnf** command for syntax and output information.

Full Name

Print interface control template

Syntax

prtict <port> <template>

Related Commands

cnfict, cpyict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	IGX	Yes

Example 1

`prtict 25.1`

Description

Print the active interface control template for 25.1.

System Response

None as this command produces hardcopy.

Table 7-37 prtict—Parameters

Parameter	Description
channel	Specifies the channel containing the data card. The start channel has the format *slot.port*.
template	Specifies which control template to display for the channel. Three templates are available for data channels. One template (option “a”) is available for Frame Relay ports. You can also specify the near or far end of the connection. **a** Active control template (normal operation). This choice is the only option for a Frame Relay port. **c** Conditioned control template (when connection fails). **l** Looped control template (with local or remote loopback). **n** Near. **f** Far.

Frame Relay Connections

The Frame Relay commands let you add, configure, delete, and specify statistical reporting for Frame Relay connections. In addition to describing the commands, this chapter tells you how to:

- Set up a Frame Relay connection
- Use Frame Relay classes
- Use interface control templates
- Configure channel utilization
- Set channel priorities
- Display statistics

The Frame Relay commands in this chapter operate on an FRM or UFM card set in an IGX node. For the Frame Relay commands that operate on an FRSM in an MGX 8220 shelf, refer to the *Cisco MGX 8220 Command Reference*. For the Frame Relay commands that operate on the FastPADs and supporting service cards, refer to the FastPAD manuals.

For a greater number of low-speed connections, the Port Concentrator Shelf (PCS) is available. The PCS is an external device that requires an FRM-2/FRI-2 card set in an IGX node. The system recognizes an FRM-2 or FRC-2 and accepts commands for the PCS.

Note A connection is the same as a PVC (permanent virtual circuit).

Physical and Logical Frame Relay Ports

This section describes the command-related issues for physical and logical Frame Relay ports.

In the IPX and IGX nodes, the Frame Relay-only cards are the FRP, FRM and UFM card sets. (The FTM supports Frame Relay, voice, and serial data but is not described in this manual.) In the FRP and FRM, both physical and logical ports can exist. The UFM has *logical* ports and *physical* lines.

Physical and Logical Ports on an FRM

In the FRP and FRM card sets, a *logical* port is a convention that applies to a T1 or E1 back card. In contrast, the ports on an X.21 or V.35 back card are physical. The reason that T1 and E1 ports on an FRP or FRM card set are logical is that these ports use one, bidirectional connector. To support the range of possible PVCs, the traffic passes through a demultiplexer on a T1 or E1 FRI. Therefore, although only one connector exists on the card, the Frame Relay commands accept port numbers 1–24 (T1) or 1–31 (E1). When a Frame Relay command takes the parameter *slot.port*, the port in this case is logical, and the node tracks it accordingly.

Note Keep in mind the distinction between a logical *port* and a logical *channel*: a logical channel is one or more DS0s.

Logical Ports and Physical Lines on a UFM

On the UFI back cards, the presence of multiple physical lines adds a parameter to the connection identifier. When you identify a UFM-C channel, use the format *slot.port line.DS0_range*. Due to the architecture of the software, *port* is a logical specification, and *line* is a physical specification. The range of logical ports is 1–250. The number of physical lines (hardware connectors) on the UFI-8T1 and UFI-8E1 is 8 (regardless of whether the front card is a UFM-4C or UFM-8C). The range of DS0s is 1–24 for T1 and 1–31 for E1.

For interfaces attached to a UFM-U front card, the range of ports is 1–12 for the UFI-12V.35 or UFI-12X.21 and 1–4 for the UFI-4HSSI.

Setting Up a Frame Relay Connection

Frame relay connections can exist between the following cards:

- FRP, FRM, or UFM to any FRP, FRM or UFM.
- UFM to an ASI in a BPX or an ALM/A in an IGX: These paths use service interworking (SIW) to terminate a connection that is Frame Relay at one end and ATM at the other end.
- FRP, FRM, or UFM and an FRSM (in an MGX 8220 shelf): this path uses network interworking (NIW) to carry Frame Relay data encapsulated in ATM cells between an IPX or IGX node and an FRSM.
- FRP, FRM, or UFM to a FastPAD port.

An IPX or IGX node provides a Permanent Virtual Circuit (PVC) Frame Relay Service for interconnecting user devices (routers, bridges, and packet switches). The PVCs are internally created on the node and rely on FastPacket switching. The user device connects to the Frame Relay back card in the node. The back card provides the adaptation layer function to convert between the Frame Relay format and the FastPacket format.

In addition to the interface cards just listed, Frame Relay connections require a trunk card. Trunk cards can be an NTC or AIT in an IPX node or an NTM, BTM, or ALM/B in an IGX node. Because Frame Relay is a purchased option, Cisco must enable it on each applicable WAN Switching node.

A variety of external user devices can operate with an IGX node. The configuration on these devices must be appropriate for the type of interface on the back card.

The following command sequence brings up a Frame Relay port and adds a Frame Relay connection.

Step 1 Activate a Frame Relay port with the **upfrport** command.

Step 2 Use **cnffrport** to specify the Frame Relay parameters for the Frame Relay service.

An optional command may be applicable to a Port Concentrator Shelf (PCS): you can use **cnffrcport** to configure the concentrated link between the PCS and Frame Relay cards.

Step 3 Use the **dspcls** command to view the existing Frame Relay classes. Decide on a class if a suitable class exists, otherwise create a suitable class using the **cnffrcls** command. Use the class number in the **addcon** command.

Step 4 Use the **vt** command to access the node at the remote end of the proposed Frame Relay connection, then use the **upfrport** and **cnffrport** commands as in steps 1 and 2.

Step 5 Use the **addcon** command on the local node to add the Frame Relay connection.

Using Frame Relay Classes

For each Frame Relay connection you add, you must specify a *Frame Relay class*. A Frame Relay class is a set of parameters that specify the bandwidth and congestion-prevention characteristics for a connection. Cisco provides ten (10) predefined classes, but you can modify any of the 10 Frame Relay classes with **cnffrcls**. To see the parameters in all connection classes, execute **dspfrcls**. A Frame Relay class is relevant only at the time you add a connection with **addcon**. Once the connection exists, the system uses the parameters but does not keep track of the class number.

Apart from using the **cnffrcls** command, you can change one or more Frame Relay parameters with the **addcon** command. When you add a Frame Relay connection with **addcon**, a prompt appears requesting a Frame Relay class. At this prompt you can do one of the following:

- Enter the number of a pre-defined class. The range is 1–10.
- Enter the number of a class modified with the **cnffrcls** command. The range is 1–10.
- Override one or more parameters in a connection class by typing the class number—*without pressing the Return key*—then continue the line by typing either a new value or an asterisk (*) for each parameter. Separate each item with a space and no comma.

If you are overriding class parameters, but want to keep the existing value of the parameter, use the asterisk to cause the connection to use the existing value of the parameter in that class. Most parameters are bi-directional and have the format *parameter/parameter*. If you want to keep a value for both directions, enter a single *. If you want to change a value for only one direction, enter the parameter in the form */*new_parameter* or *new_parameter*/*. When you type individual parameters, you need to enter characters only up to the last changed item. Before the last item, you must enter new values or * as a placeholder.

The parameters in the list that follows make up a Frame Relay class. Collectively, the name of these parameters is *frp_bw*. For most parameters, you can specify the value for each direction of the connection, so most parameter names appear in the format *parameter/parameter*. ForeSight (FST) is the exception because ForeSight automatically applies to both directions.

- **MIR/MIR** is defined as fr_MIR_Tx /fr_MIR_Rx, where fr_MIR is the minimum information rate for the connection. The range for MIR is 2.4 Kbps–2048 Kbps.
- **CIR/CIR** is defined as fr_CIR_Tx and fr_CIR_Rx, where fr_CIR is defined as the committed information rate guaranteed to the user.

  The full range of values for Frame Relay cards is 0–2048 Kbps. Note that a CIR of 0 is not a standard setting. The standard range is 2.4 Kbps–2048 Kbps. CIR = 0 is a valid parameter only if the connection terminates at both ends on either a UFM, FRM or FRP. Before you can specify CIR = 0 with either **addcon** or **cnffrcls**, you must enable IDE-to-DE mapping with the **cnffrport** command. If you do not first enable IDE-to-DE mapping, the range for CIR is 2.4 Kbps–2048 Kbps. Additionally, the CIR = 0 specification is necessary at only one end of the connection.

  The Port Concentrator Shelf does not support CIR = 0. On the FRP-2 and FRM-2 cards sets, the range for CIR is 2.4 Kbps–2048 Kbps.
- **VC_Q/VC_Q** is defined as fr_vc_q_Tx/fr_vc_q_Rx, where fr_vc_q Tx is the transmit VC maximum queue depth. Specify the VC_Q in bytes within the range 1–65535.

  OR

  Bc/Bc is defined as fr_Bc_Tx /fr_Bc_Rx. If you have selected Frame Relay Forum standard parameters (through the **cnfsysparm** command), the Committed Burst (Bc) parameter is used instead of vc_q. Bc is defined as the amount of data the network can accept over a variable time interval Tc for committed delivery on a specific PVC. Specify Bc in bytes in the range 1–65535. Bc has meaning for only FST connections. The relationship between Bc and VC_Q is:

  Bc = VC_Q / ((1 – (CIR/port speed))
- **PIR/PIR** is defined as fr_PIR_Tx /fr_PIR_Rx, where fr_PIR_Tx is the peak transmit rate for the PVC. The PIR range is 2.4–2048 Kbps. You can also specify the value 0 to cause PIR to default to the port speed. Thus, you can modify PIR, leave it the same, or set it to the port speed.

  OR

  Be/Be is defined as fr_Be_Tx /fr_Be_Rx. If you have selected Frame Relay Forum standard parameters (through the **cnfsysparm** command), the PVC uses Excess Burst (Be) instead of PIR. Be is the *amount* of transmit/receive data above the number of bytes set by Bc if enough extra bandwidth is available. Specify Be in bytes within the range 1–65535. Delivery of Be-data is not guaranteed. Be has meaning to only ForeSight. The relationship between Be and PIR is:

  Be = Bc * ((PIR/CIR) – 1)
- **Cmax/Cmax** is defined as fr_cmax_Tx /fr_cmax_Rx, where Cmax is the maximum credits the connection can accrue. **Cmax** has the range 1–255 packets per second (pps).
- **ECNQ_thresh/ECNQ_thresh** are the transmit and receive threshold settings for the explicit congestion notification control queues. The range for ECNQ_thresh is 1–65535 bytes.
- **QIR/QIR** is defined as fr_QIR_Tx /fr_QIR_Rx where fr_QIR is the quiescent information rate for the connection, which is the initial transmit rate after a period of inactivity on the channel. If you do not specify the quiescent receive rate fr_QIR_Rx, the system sets it to the transmit value. The values are specified in Kbps and must be in the range MIR–PIR. In addition, you can specify the value 0 to default to the MIR. QIR has meaning for only ForeSight connections.
- **FST** enables or disables ForeSight for a connection. Valid entries are “y” (use ForeSight) or “n” (do not use ForeSight). If the ForeSight status changes, the network reroutes the connection.
- **%utl/%utl** are the percentage transmit and receive utilization settings for the Frame Relay class. This value is specified as a percentage in the range 0%–100%.

Using Interface Control Templates

X.21 ports use a *fixed*, *active* control template. In contrast, although V.35 and V.28 ports use an active control template, you can set the signals that are active to on or off. These ports cannot use *looped*, *conditioned*, *near*, or *far*.

Configuring Channel Utilization

You can use the **cnfchutl** command to enter the expected channel utilization of a Frame Relay circuit into the system. This command helps the system allocate the proper bandwidth to the circuit.

Setting Channel Priorities

A Frame Relay connection has either low or high priority. The default is low priority. You can use **cnfchpri** to assign a high priority to a circuit or to re-assign a high priority circuit to low priority.

Displaying Statistics

Nodes collect statistics for Frame Relay traffic, channel use, and Explicit Congestion Notification. Use **dspchstats** to display these statistics. Use **clrchstats** to clear the statistics and start collecting new statistics. To display Frame Relay use and error statistics, use **dspportstats**.

Summary of Commands

This table lists the full name and starting page of the description for each Frame Relay command.

addcon

Adds a Frame Relay connection to the network. After you add a connection, the system automatically routes the connection. The node on which you execute **addcon** is the *owner* of the connection. The concept of ownership is important because you must specify automatic rerouting and preferred routing information at the node that owns the connection. See the **cnfpref** and **cnfcos** descriptions for information on automatic rerouting. Before it actually adds the connection, the system displays the parameters you have specified and prompts you to confirm them.

Note For cards with Y-cable redundancy specified, you can add connections to only primary cards.

Each Frame Relay connection (and associated user device) has a local identification in the form of a unique DLCI. The total range for DLCIs is 1–1023. Typically, DLCIs 16–1007 are available for local and remote channels. According to ANSI standards, DLCIs 1–15 and 1008–1022 are reserved. DLCI 1023 is reserved for LMI signaling.

Only a UFM could come close to using all DLCIs. The maximum number of connections on a UFM is 1000. The maximum number of Frame Relay connections on an FRC or FRM is 252.

If a user device can automatically determine the network configuration by using the LMI, you do not need to specify the DLCIs in the network to the device. If a device cannot interrogate the network to determine the DLCIs in the network, you must specify the network DLCIs to the user device.

As the following sections describe, you can generally differentiate Frame Relay connections as *normal*, *bundled*, *grouped*, and *frame forwarding*. In particular, a Frame Relay connection can also terminate at a Frame Relay endpoint or an ATM endpoint if the endpoints have firmware to support this arrangement. A connection that terminates at Frame Relay and ATM endpoints uses service interworking (SIW).

Service Interworking

Frame relay connections that terminate at ATM endpoints require service interworking (SIW) support. At the Frame Relay end, service interworking is one of the optional parameters. The line cards on which you can add service interworking connections are the UFM on an IGX node, ASI on a BPX node, and FRSM in an MGX 8220 shelf. The Frame Relay endpoint has an identifier in the format *slot.port.DLCI*. For SIW connections, the ATM endpoint identifier has the format *slot.port.vpi.VCI*.

Note You cannot group or bundle SIW connections with non-SIW connections.

Normal Connections

A *normal* connection is a single PVC. A Frame Relay PVC can terminate at either a Frame Relay endpoint or an ATM endpoint.

Bundled Connections

Connection bundling creates a full mesh of connections between two groups of Frame Relay ports by executing **addcon** command only once. When you add a bundle between two groups of ports, you create a connection between each port of one group of ports and each port of the other group of ports. Each group of Frame Relay ports can include up to four ports. Consequently, the maximum number of connections in a bundle is 16 (resulting from a full mesh of connections between two groups of four ports each). Note that a Port Concentrator Shelf does not support bundling. Characteristics of connection bundling are:

- The number of ports used at each end of the bundle does not have to be the same.
- All of the ports used in a group must be on the same card.
- Only the FRP Model D and the FRM Model D support connection bundles. The UFM does not support connection bundling.
- All of the ports used for a bundle must be contiguous. For example, a bundle on a card may not consist of only ports 1, 3, and 4.
- The syntax for specifying a group of ports for a connection bundle is *slot.port[xport]*.

When you create a connection bundle with **addcon**, you do not explicitly specify the required DLCI at each endpoint of each connection. Instead, the DLCIs are automatically assigned using global addressing with the Port IDs, which have been previously assigned to the ports. Consequently, you must first assign a Port ID (other than 0) to every port to which you plan to assign a connection bundle. Use **cnffrport** to assign a Port ID or **dspport** to see an existing Port ID.

For example, the command

addcon 6.1x3 alpha 7.2x3 1

defines a single connection bundle between a local group of 3 ports (ports 1, 2, and 3 on card 6) and a remote group of 2 ports (ports 2 and 3 on card 7). The resulting connection bundle consists of the following six connections:

local node slot 6.port 1 to node alpha slot 7.port 2

local node slot 6.port 1 to node alpha slot 7.port 3

local node slot 6.port 2 to node alpha slot 7.port 2

local node slot 6.port 2 to node alpha slot 7.port 3

local node slot 6.port 3 to node alpha slot 7.port 2

local node slot 6.port 3 to node alpha slot 7.port 3

Each connection in the bundle is assigned the parameters of the same Frame Relay class (class 1, in the example above). Notice that no DLCIs were specified for the six connections. The DLCIs are automatically assigned using the Port IDs of the ports.

As an example, assume that the following Port IDs had been previously assigned for the five ports.

port 6.1	Port ID = 22
port 6.1	Port ID = 534
port 6.3	Port ID = 487
port 7.2	Port ID = 92
port 7.3	Port ID = 796

As a result of the **addcon** command, the six connections that you create are automatically assigned DLCIs using global addressing as follows.

6.1.*92* – 7.2.*22*

6.1.*796* – 7.3.*22*

6.2.*92* – 7.2.*534*

6.2.*796* – 7.3.*534*

6.3.*92* – 7.2.*487*

6.3.*796* – 7.3.*487*

The **dspcons** display shows the entire bundle as a single item. Therefore, you cannot see the automatically assigned DLCIs on the **dspcons** screen. (The automatically assigned DLCIs in the preceding list appear in italics.) To see the DLCIs, use **dspcon**, as in the following example:

dspcon 6.1x3 alpha 7.2x3

The preceding shows one screen for the whole bundle then an additional screen for each connection in the bundle. The assigned DLCIs appear in these individual connection display screens.

Frame Forwarding Connections

A non-Frame Relay data connection (such as HDLC or SDLC) that is routed through Frame Relay cards can bypass a router or take advantage of DFM at higher data rates. The format *slot.port.** identifies a frame forwarding connection. An example is:

addcon 11.2.* alpha 12.3.* 2

The “*” indicates to the node that a DLCI is meaningless.

Maximum Connections Per Port With Signaling Protocols

For any Frame Relay card set that has a maximum frame length of 4510 bytes, the use and type of signaling protocol you may have (optionally) specified with the **cnffrport** command results in a limit on the possible number of connections per physical or logical port. The maximum number of connections per port for each protocol is as follows:

- For Annex A: 899
- For Annex D: 899
- For StrataLMI: 562

The **addcon** command does not prevent you from adding more than the maximum number connections on a port. If the number of connections is exceeded, the particular LMI does not work on the port, the full status messages that result are discarded, and LMI timeouts occur on the port. A port failure results and subsequently leads to a-bit failures in segments of the connection path.

Full Name

Add connection

Syntax

addcon <local_channel> <remote_node> <remote_channel> [con_type] <frame_relay_class | [individual parameters]> [route_avoid]

Note If you request help for **addcon** at the command line prompt, the Help line shows *type* as a parameter. However, when you are *using* **addcon** for a Frame Relay connection, the *type* shown in the help display is actually the *Frame Relay class* shown on the preceding syntax line and described in the preceding section titled "Using Frame Relay Classes,"As stated in "Using Frame Relay Classes," you can optionally override any or all of the bandwidth parameters and ForeSight enable in the Frame Relay class by typing the parameters that appear as *frp_bw* and *avoid* in the Help display. See the forthcoming "Optional Parameters" table.

Note also that you do not enter the *coding* parameter shown on the Help line.

Related Commands

delcon, dncon, dspcon, dspcons, upcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, (and BPX for service internetworking	Yes

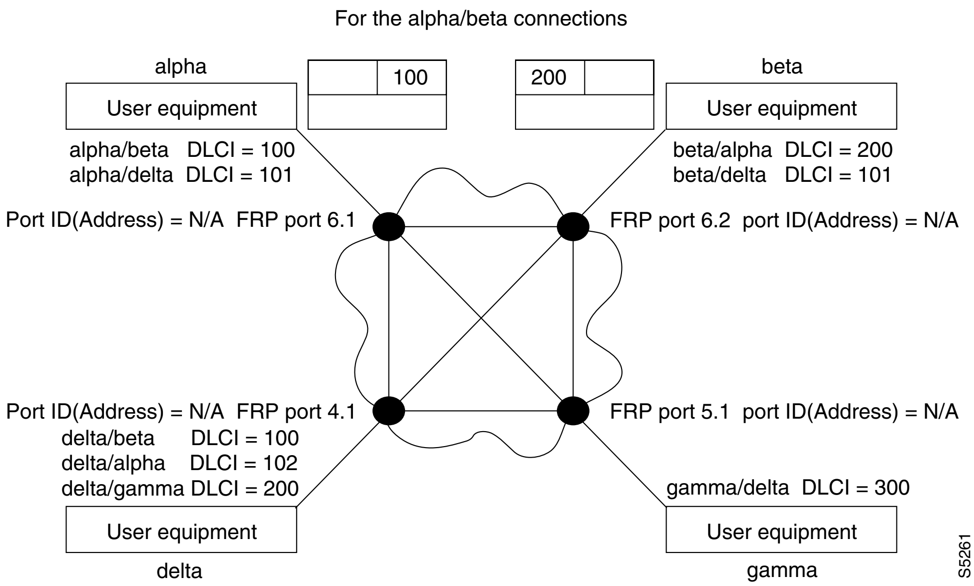
Example 1 (local addressing)

```
addcon 6.1.100 beta 6.2.200 3
addcon 6.1 101 delta 4.1.102 2
addcon 4.1.100 beta 6.2.101 4
addcon 4.1.200 gamma 5.1.300 1
```

Description

Execute the preceding commands at node Alpha to configure the following network shown in Figure 8-1.

Figure 8-1 Local Addressing Example



Example 2a

```
addcon 9.1.200 gamma 8.1.300 1
```

Description

Add a connection between the user-device at alpha port 9.1 and the user-device at gamma port 8.1. The user-device at alpha refers to the connection using local DLCI 200. The user-device at gamma refers to this connection using local DLCI 300. The DLCIs have only local significance, so a DLCI must apply to only one connection.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:12 PST

Local      Remote     Remote                                           Route
Channel    NodeName   Channel    State   Type Compression   Code   Avoid    COS   O
 5.1       beta       25.1       Ok      256                 7/8             0     L
 9.1.100   gamma      8.1.200    Ok      fr                 0                      L
 9.1.200   gamma      8.1.300    Ok      fr                 0                      L
 9.2.400   beta       19.2.302   Ok      fr                 0                      L
 14.1      gamma      15.1       Ok      v                  0                      L









Last Command: addcon 9.1.200 gamma 8.1.300 1

Next Command:
```

Example 2b

addcon 9.1.100 beta 6.2.300 2

Description

Add another connection at local port 9.1. A DLCI of 100 is used at the local node. A DLCI of 300 can be used at both beta gamma because the DLCIs have only local significance.

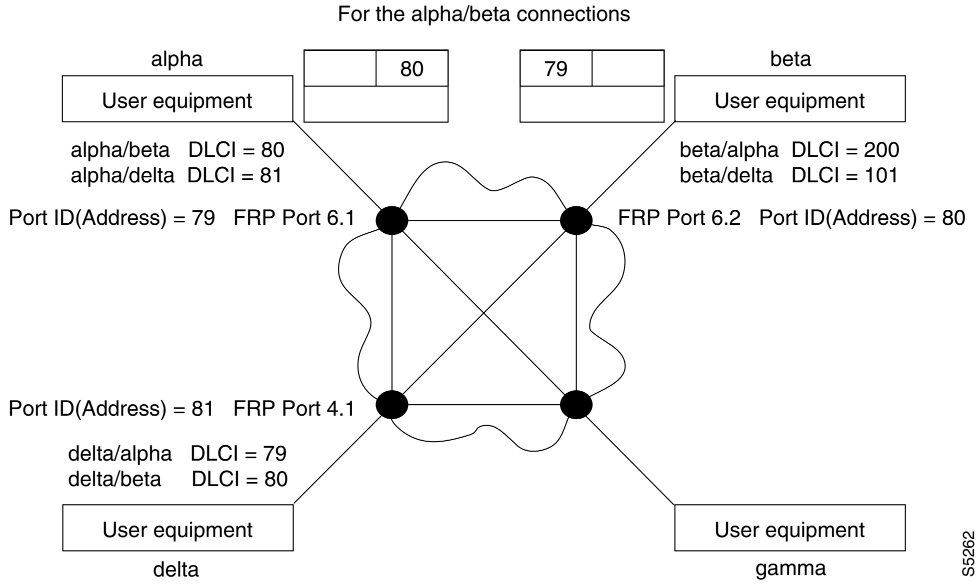
Example 3 (global addressing)

addcon 6.1.80 beta 9.2.79 2
addcon 6.1.81 gamma 4.1.79 1
addcon 4.1.80 beta 6.2.81 5

Description

The network to configure in this example is as in Figure 8-2.

Figure 8-2 Global Addressing Example



Example 4 (bundle connections)

`addcon 8.1x3 alpha 19.2x4 1`

Description

Add a bundle of connections between Frame Relay ports 8.1-3 on node gamma and 19.2-4 on node alpha. For this bundle, the network routes traffic between gamma port 8.2 and alpha port 19.2.

System Response

```
pubsigx3       VT    SuperUser       IGX 8410     9.2 Aug. 3 1998 19:41 GMT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
     8.1x3      alpha      19.2x4     Ok      fr







This Command: addcon 8.1x3 alpha 19.2x4 1


Add these connections (y/n)?
```

Example 5 (frame forwarding)

addcon 8.2.* alpha 19.2.* 1

Description

Add a frame forwarding connection between the local node's port 8.2 and 19.2 on node alpha.

System Response

```
Locals       Remote      Remote                                        Route
Channel      NodeName    Channel   State    Type   Compression Code   Avoid COS   O
6.1          beta        25.2       Ok      256                7/8            0     R
8.1.200      alpha       9.1.100    Ok      fr                                0     R
8.2.300      beta        19.1.101   Ok      fr                                0     R
15.1         alpha       14.1       Ok      v                                 0     R







This Command: addcon 8.2.* alpha 19.2.* 1


Add these connections (y/n)?
```

Example 6 (modifying bandwidth)

addcon 8.3.101 beta 19.3.201 7 * * * * 30/30 * * Y 80/80

Description

Parameters specified by Frame Relay class 7 for this connection are modified by substituting 30 for Cmax in both directions, enabling ForeSight, and reducing percent utilization from 100% to 80%.

System Response

```
gamma          TRM   YourID:1        IGX 8410    9.2   Aug. 23 1998 12:10 CST

 Local      Remote      Remote                                      Route
 Channel    NodeName    Channel    State  Type   Compression  Code Avoid COS O
 6.1        beta        25.2        Ok     256                 7/8         0  R
 8.1.200    alpha       9.1.100     Ok     fr                              0  R
 8.2.300    beta        19.1.101    Ok     fr                              0  R
 15.1       alpha       14.1        Ok     v                               0  R




Last Command: dspcons


Next Command: addcon 8.3.101 beta 19.3.201 7 * * * * 30/30 * * Y 80/80
```

Table 8-1 addcon—Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>local channel</td><td>Specifies the local channel to connect in the format:

slot.port.DLCI | x port | .*

On an FRP or FRM, the range for port is 1–24 or 1–31. On a UFM-C, the range for port is 1–250. (For connections on a UFM-C, line is not necessary because of the port-to-line mapping through addfrport). For a UFM-U, the range for port is 1–12 for V.35 or X.21 and 1–4 for HSSI. The range for DLCI is 16–1007.</td></tr>
<tr><td>node</td><td>Specifies the name of the remote node at the other end of the connection.</td></tr>
<tr><td>remote channel</td><td>Specifies the connection at the far end. For Frame Relay termination points, use:

<i>slot.port.DLCI | x port | .*</i>

If the far end is an ATM termination (as in interworking), use:

<i>slot.port.vpi.vci</i>

where <i>vpi</i> has a range of 0–255, and <i>vci</i> has a range of 1–4095. One exception to these ranges is the ALM/A, which has a vci range of 0–255. Another exception is an interface shelf (which uses Annex G signaling) in a tiered network, as follows:

• For an MGX 8220 shelf, the VPI range is 1–1015, and the VCI range is 1–65535.

• For an MGX 8850 shelf, when adding a connection with a UNI interface to a BPX routing node, the VPI range is 1–4095. The VCI range is 1–65535.

For an MGX 8850 shelf, when adding a connection with a NNI interface to a BPX routing node, the VPI range is 1–4095. The VCI range is 1–65535.

• For an IPX/AF or IGX/AF shelf, the range for both VPI and VCI is 1-255.

Access devices such as the Cisco 3800 use the following format for the remote channel specification: <<i>slot.port</i>> <<i>access_device_connection_ID</i>>

where <i>slot</i> is the slot number of the FTC or FTM card, <i>port</i> is the port number, and <i>access_device_connection_ID</i> is in the range 1–252.</td></tr>
<tr><td>Frame Relay class</td><td>Specifies a Frame Relay class. Entering a Frame Relay class is a shortcut for specifying bandwidth parameters. You must enter a Frame Relay class, but then you can modify any of the bandwidth parameters specified by the class. To do so, do not press Return after you type the class number but continue typing either a value for the parameter or a * to keep the current value. The system does not display the parameters, but the description of the frp_bw parameters in the”Optional Parameters” table that follows shows the order and ranges of the parameters you can specify. For more details on the parameters and the Frame Relay classes, refer to “Using Frame Relay Classes” earlier in this chapter.</td></tr>
</table>

Table 8-2 addcon—Optional Parameters

Parameter	Description
con_type	Specifies the type of ATM-to-Frame Relay service interworking. (If the connection is Frame Relay-to-Frame Relay, the network selects any necessary interworking.) The possible *con_type* entries are *atft* and *atfx*. To specify service interworking in transparent mode, type "atft." To specify service interworking in translation mode, type "atfx." In translation mode, a standard set of encapsulation protocols are translated. If system software does not recognize an encapsulation protocol for an atfx connection, it generates one of two Frame Relay endpoint statistics: rcvFramesDscdUnknownProtocol or xmtFramesDscdUnknownProtocol.
frp_bw	Optionally specifies individual bandwidth parameters. The parameter name "frp_bw" is the label for the bandwidth parameters described here. The slash (/) between the repeated parameter name shows that you can specify a value for each direction. (FST is the exception.) Two parameters can be either the (default) Cisco versions or the Frame Relay Forum standard parameters. To switch between Cisco and Frame Relay Forum, use the **cnfsysparm** command. Note that all parameters you select with **cnfsysparm** are network-wide and not confined to the current connection addition. The switchable parameters are as follows: Cisco ParametersStandard Parameters PIR (peak information rate)Be (excess burst) VC_Q (VC queue depth)Bc (committed burst) When you are using the Cisco parameter set, the names and order of specification are as follows: MIR/MIR, CIR/CIR, VC_Q/VC_Q, PIR/PIR, Cmax/Cmax ECNQ_thresh/ECNQ_thresh, QIR/QIR, FST, %utl/%utl When you are using the parameters with the two Frame Relay Forum versions, the names and order of specification are as follows: MIR/MIR, CIR/CIR, Bc/Bc, Be/Be, Cmax/Cmax, ECNQ_thresh/ECNQ_thresh, QIR/QIR, FST, %utl/%utl For the definition of each parameter and important information on setting CIR=0, refer to the section titled "Using Frame Relay Classes" earlier in this chapter.
avoid	Specifies the type of trunk or route to avoid for the connection. The default is no avoidance. To specify an *avoid* value, type it after the Frame Relay class or — if you override the Frame Relay class — after the frp_bw values. Be sure to include the asterisk (*). The *avoid* parameters are: ***s** Avoid satellite trunks. ***t** Avoid terrestrial trunks. ***z** Avoid trunks using zero-code suppression techniques that modify any bit position to prevent long strings of zeros.

addfrport

Activates a logical Frame Relay port on a channelized FRP, FRM, or UFM card set. Only T1 or E1 lines carry channelized Frame Relay traffic, so the **addfrport** command does not apply to a Port Concentrator Shelf or front cards with a V.35, X.21, or HSSI interface.

The **addfrport** command adds a logical Frame Relay port by using the slot number of the FRM and the DS0/timeslots that make up the logical port. On a UFM, the logical ports span the whole range of physical lines: you associate the logical ports to the lines as needed, then include the DS0s as the last field of the argument. Table 8-2 lists the error and warning messages for **addfrport**.

Table 8-3 Frame Relay Port Error and Warning Messages

Messages	Reason for Message
"Slot is out of range"	Line number not correct for T1/E1. You cannot add slots 0-31, that is, you cannot have a port at E1 speed. The maximum you can get is 31 slots (1984) using CCS (Common Channel Signalling) since slot 0 is used for FAS, etc.
"Line must first be upped"	Line is down.
"invalid channel range"	Channel is out of the range 1–24 or 1–31 (16 is a reserved channel for E1).
"Channel is busy"	Channel is already assigned to a logical port.
“You cannot use signaling channel 16" (E1)	CAS channel 16 included in logical port (E1). CCS permits the use of channel 16 but not in all countries.
"Invalid rate"	Entered rate is not 56 Kbps or 64 Kbps.
"This rate is available for single channel only"	Entered rate is 56 Kbps, but multiple channels specified.

Full Name

Add Frame Relay port T1/E1

Syntax

For FRP or FRM card sets: **addfrport** <slot.port> [DS0 channel] [56 | 64]

For UFM-C card sets: **addfrport** <slot.port> <line.DS0_channel>

Related Commands

upln (upcln is the obsolete name), **delfrport, cnffrcport, cnffrport, dspfrport**

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

`addfrport 21.9 -15`

Description

Add a single Frame Relay port that occupies DS0s (timeslots) in the range 9–15. For a T1 line, this channel rate is 7 x 64 Kbps = 448 Kbps, as the screen example shows. The card is an FRP.

System Response

```
gamma          TRM   YourID:1        IGX 8410    9.2    Aug. 15 1998 17:28 CST

Port configuration for FRP 21

From   Chan   Speed    Interface   State
1      9-15    448      FRI           T1    INACTIVE










Last Command: addfrport 21.9-15


Next Command:
```

Table 8-4 addfrport–Parameters

Parameter	Description
slot.port (FRP or FRM series) slot.port line.DS0 channel (for UFM-C series)	Specifies the FRI T1 or E1 line number and the logical port number. For a UFM-U, specifies the physical slot and port. For an example of a T1 or E1: 8.12 is physical slot 8 and timeslot (or *channel*) 12. For the UFM card sets, this parameter specifies the slot and logical port, the physical line (the connector), and one or more contiguous DS0s. The range of logical ports is 1–250. The range of lines is 1–4 for the UFM-4C and 1–8 for the UFM-8C. Note the space between the port and line.

Table 8-5 addfrport—Optional Parameters

Parameter	Description
– chan	Specifies that multiple DS0/timeslots should form one logical port. A "–" separates the starting and ending DS0s/timeslots). Timeslots must be contiguous. An example is **addfrport** 8.1–5. The system uses the lowest DS0/timeslot number as the logical port number and shows this in related displays.
rate	Specifies the rate of a single, logical port. By default, a single logical port (or channel) is 64Kbps. A single DS0 (timeslot) may be 56 Kbps or 64 Kbps. If you do not enter a rate, the default is 64 Kbps.

cnfdch

The **cnfdch** command lets you configure a super-rate data connection has idle code suppression (ICS) enabled or disabled. All super-rate data connections will have the Idle Code Suppression (ICS) state set to “disabled” unless it has been specifically configured with the new **cnfdch** command or through SNMP. The **cnfdch** screen is identical to that of **dspchcnf**.

The Idle Code Suppression feature supported in this release provides a way to stop fast packet generation on an Nx64 super-rate PVC connection when the connected PBX has terminated a video call. No video traffic will be generated when a video call has terminated.

Configuration is done for each of channel of an endpoint. Upon changes in the state of Idle Code Suppression of a connection, no network message will be sent to the other end. You can choose to configure the other end if ICS is supported there also. To maximize the benefit of this feature, you should enable ICS on both sides of a connection.

The **cnfdch** command prompts you to enable or disable idle code suppression with the following prompt:

```
Enable or Disable Idle Code Suppression (e/d)?[d]:
```

The **cnfdch** command is available for level 2 users and above; that is, you must have at least privilege level 2 or above to use this command. Use it to configure a channel before you add a connection. If some of the specified channels do not yet have any connection attached, those channels will be initialized to a data type channel.

The configuration will stay the same even if connections are removed and added again.

The **cnfdch** command will be blocked at the CLI if one or more of the specified channels is carrying a voice connection (including t-type).

The switch software provides an interface to configure channels to enable or disable idle code suppression for super-rate data connections, In turn, the switch software tells the UVM/CVM/CDP card if idle code suppression should be used on each of the super-rate connections.

Because there are multiple channels involved in an Nx64 data connection, the idle code suppression configuration of the first channel in the Nx64 channel will be used for the entire connection. The configuration of the other channels in the bundle will be ignored in channel programming or on the **dspcons** screen.

To inter-work with HDM/LDM/SDP/LDP cards, idle code suppression on a UVM/CVM/CDP channel will be turned off for any super-rate connection that also terminates on HDM/LDM/SDP/LDP.

Full Name

Configures data connection to have ICS enabled/disabled.

Related Commands

prtchcnf

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
2–6	No	No	IGX	No

Example 1

dspchcnf 31.1.8

Description

Display configuration values for channel 9.1.3–5

System Response

```
sw176          TRM   StrataCom       IGX 16    9.2.a2    Apr. 3 1998 17:28 PST

            Maximum EIA     %      DFM Pattern     DFM    Idle Code   PreAge
From 9.1.3  Update Rate   Util       Length       Status    Suppr      (usec)
9.1.3-5        -           -          -            -       Disabled       0


This Command: cnfdch 9.1.3-5
```

Syntax

dspchcnf [parameters]

Table 8-6 cnfdch – Parameters

Parameter	Description
channel(s)	*slot.line.chan* for UVM or *line.chan* for CVM/CDP. You can enter a range of channels.
ch_ics_state	Channel idle code suppression state: d for disabled; e for enabled.

clrfrcportstats

Clears port statistics for FRM-2 or FRP-2 physical ports connected to a Port Concentrator Shelf. To see the statistics that you clear with **clrfrcportstats**, execute **dspfrcportstats**. The controller card collects statistics from the FRM-2 or FRP-2 once per minute. Because **clrfrcportstats** clears statistics on the controller card, it may not clear statistics generated within the last minute.

Full Name

Clear FRC/FRM port statistics

Syntax

clrfrcportstats <slot.port | *>

Related Commands

dspfrcportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	No

Table 8-7 clrfrcportstats—Parameters

Parameter	Description
slot,port | *	Slot and port of the physical port. The range for *port* is 1–4. An asterisk (*) specifies all FRC-2/FRM-2 physical ports.

cnfchpri

Sets the channel priority for a Frame Relay connection. The Channel Priority feature permits some Frame Relay connections to receive a higher priority within a port queue than other Frame Relay traffic on a per-connection basis. The default priority is low. You can configure Frame Relay LMI ports to communicate the priority to a router. You must change the priority on both ends of a connection.

Note Note that data of high priority (hi-pri) connections is sent to the CPE (customer premises equipment) ahead of data from low priority (low-pri) connections. Note that this parameter has nothing to do with how the connection is routed through the network, but affects only how data is sent to the CPE.

Full Name

Configure Frame Relay channel priority

Syntax

cnfchpri <connection> <priority>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfchpri 9.1.100 h
```

Description

Configure a high priority for Frame Relay connection 9.1.100.

System Response

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 15 1998 16:00 PST

Conn: 9.1.100    gamma       8.1.200     fr
   MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR    FST
 9.6/9.6   9.6/9.6      5/5       256/256    10/10  65535/65535  9.6/9.6   n
% Util: 100/100
Owner: LOCAL  Restriction: NONE  COS: 0                    Status: OK
Group: NONE  Priority: H  TestRTD: 0 msec

Path:     alpha   14--13beta    15--15gamma
Pref:     Not Configured


alpha 9.1.100                                  gamma 8.1.200
FRP:   OK                                      FRP:   OK
FRI:   OK                                      FRI:   OK


Last Command: cnfchpri 9.1.100 h


Next Command:
```

Table 8-8 cnfchpri—Parameters

Parameter	Description
channels	Specifies the channel or range of channels. The format is *slot.port.DLCI*.
h | l	The priority: h = high; l = low.

cnffrcls

Configures a system-wide Frame Relay connection class. Refer to the “Using Frame Relay Classes” section at the beginning of this chapter for a definition of a Frame Relay class. The following are characteristics of this command:

- You should configure network-wide classes only when all nodes are reachable.
- Beware of conflicting values with existing, joined networks.
- Changing a class does not affect any existing connections. An altered Frame Relay class affects only connections that are added using the changed class.

Full Name

Configure Frame Relay class

Syntax

cnffrcls <class_num> [<BW params>] [<description>]

Related Commands

addcon, dspfrcls

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnffrcls 1 *
```

Description

Configure Frame Relay class #1 to operate with ForeSight. The list of * parameters leaves those parameters unchanged, and “y” enables ForeSight. Because the utilization and description parameters have not been entered, any existing values for these parameters remain in effect.

System Response

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 15 1998 16:05 PST

                        Frame Relay Connection Classes

 #    MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR   FST
.6/9.6   9.6/9.6  65535/65535    128/128  10/10  65535/65535  9.6/9.6  y
   % Util: 100/100 Description: "Default 9.6"
 2 19.2/19.2 19.2/19.2 65535/65535     */*      10/10  65535/65535 19.2/19.2 n
   % Util: 100/100 Description: "Default 19.2"
 3   16/16     16/16   65535/65535     */*      10/10  65535/65535   16/16   n
   % Util: 100/100 Description: "Default 16"
 4   32/32     32/32   65535/65535     */*      10/10  65535/65535   32/32   n
   % Util: 100/100 Description: "Default 32"
 5   56/56     56/56   65535/65535     */*      10/10  65535/65535   56/56   n
   % Util: 100/100 Description: "Default 56"



Last Command: cnffrcls 1 * * * * * * * y


Continue (y): y
```

System Response (continued)

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 15 1998 16:03 PST

                        Frame Relay Connection Classes

 #    MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR   FST
 6   64/64     64/64   65535/65535     */*      10/10  65535/65535   64/64   n
   % Util: 100/100 Description: "Default 64"
 7  128/128   128/128  65535/65535     */*      10/10  65535/65535  128/128  n
   % Util: 100/100 Description: "Default 128"
 8  192/192   192/192  65535/65535     */*      10/10  65535/65535  192/192  n
   % Util: 100/100 Description: "Default 192"
 9  256/256   256/256  65535/65535     */*      10/10  65535/65535  256/256  n
   % Util: 100/100 Description: "Default 256"
10  512/512   512/512  65535/65535     */*      10/10  65535/65535  512/512  n
   % Util: 100/100 Description: "Default 512"



Last Command: cnffrcls 1 * * * * * * * y


Next Command:
```

Table 8-9 cnffrcls—Optional Parameters

Parameter	Description
frp_bw	Optionally specifies individual bandwidth parameters. The parameter name "frp_bw" is the label for the bandwidth parameters described here. The slash (/) between the repeated parameter name shows that you can specify a value for each direction. (FST is the exception.)Two parameters can be either the (default) Cisco versions or the Frame Relay Forum standard parameters. To switch between Cisco and Frame Relay Forum, use the **cnfsysparm** command. Note that all parameters you select with **cnfsysparm** are network-wide and not confined to the current connection addition. The switchable parameters are as follows: Cisco ParametersStandard Parameters PIR (peak information rate)Be (excess burst) VC_Q (VC queue depth)Bc (committed burst) When you are using the Cisco parameter set, the names and order of specification are as follows: MIR/MIR, CIR/CIR, VC_Q/VC_Q, PIR/PIR, Cmax/Cmax ECNQ_thresh/ECNQ_thresh, QIR/QIR, FST, %utl/%utl When you are using the parameters with the two Frame Relay Forum versions, the names and order of specification are as follows: MIR/MIR, CIR/CIR, Bc/Bc, Be/Be, Cmax/Cmax, ECNQ_thresh/ECNQ_thresh, QIR/QIR, FST, %utl/%utl For the definition of each parameter and important information on setting CIR=0, refer to the section titled "Using Frame Relay Classes" earlier in this chapter.
description	Any text string up to 25 characters terminated by a <RET>. This is used to provide the user with a descriptive identifier for the class.

cnffrcon

Configures bandwidth parameters or enables ForeSight for an individual Frame Relay connection. Because you normally specify bandwidth parameters through the Frame Relay class or by the option of overriding bandwidth parameters through specific arguments for **addcon**, using **cnffrcon** tends to be used for instances where you need to customize a single connection's bandwidth parameters.

Be sure the MIR you specify is appropriate. If the MIR is too high, bandwidth is wasted. If it is too low, the connection may drop data. The statistics reports are the best source of information to help you determine the appropriate MIR.

The PIR usually is set to the port speed. You can specify a lower PIR if other constraints on the data generation rate exist. Be sure the PIR you specify is appropriate. If it is too low, frames are dropped. If it is too high, bandwidth may be wasted unless the network has ForeSight.

You should change the Cmax, VC Q, and ECN Q values by only knowledgeable users and when tuning data is available to support the determination of appropriate values. These values affect system buffering resources, so any change from the defaults requires caution. Refer to the *Cisco WAN Switching System Overview* for more details on connection parameters.

If the connection type has ForeSight (FST = y), the result of the last test round trip delay command (Test RTD) is displayed. Note that this is not the current RTD but the result of the last, user-specified test. High or low connection priority is displayed for both standard Frame Relay connections and ForeSight connections.

The node checks the bandwidth parameters to promote efficient use of network bandwidth. The following messages reflect the checks on bandwidth usage.

Error	Min cannot exceed peak.
Warning	Min exceeds this port's speed.
Warning	Sum of mins exceeds port's speed.
Warning	Peak exceeds this port's speed.

Warning messages are informational and do not indicate that the command is failing to execute. Error messages indicate the command is not executing.

When you specify the frp_bw parameters, enter all changes (or unchanged values indicated by an asterisk) on the line. You must specify either a change or a place-holder (*) up to at least the last changed value (after which place-holders are unnecessary). Decide on any changes before starting this command. The parameters section of this command description lists frp_bw parameters. The section "Using Frame Relay Classes" at the beginning of this chapter describes the parameters.

Full Name

Configure Frame Relay Connection

Syntax

cnffrcon <channel> [bandwidth_parameters]

Related Commands

addcon, dspcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

`cnffrcon 8.1.200`

Description

Configure Frame Relay connection 8.1.200.

System Response

```
gamma          TRM   YourID:1        IGX 8410    9.2    Aug. 15 1998 17:28 CST

Conn:  8.1.200    alpha       9.1.100     fr
   MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR    FST
 9.6/9.6   9.6/9.6      5/5       256/256    10/10  65535/65535  9.6/9.6   n
% Util: 100/100
Owner: REMOTE  Restriction: NONE  COS: 0                    Status: OK
Group: NONE  Priority: L  TestRTD: 0 msec

Path:     gamma   15--15beta    13--14alpha
Pref:     Not Configured


gamma 8.1.200                                    alpha 9.1.100
FRP:   OK                                        FRP:   OK
FRI:   OK                                        FRI:   OK


Last Command: cnffrcon 8.1.200


Next Command:
```

Table 8-10 cnffrcon—Parameters

Parameter	Description
channel	Specifies the channel to configure connection parameters. The command configures connection information for one channel at a time. You cannot specify a set of channels. The channel has the following format: slot.port.DLCI

Table 8-11 cnffrcon—Optional Parameters

Parameter	Description
bandwidth_para-meters	Specifies the bandwidth parameters in the following format: MIR/MIR, CIR/CIR, VC_Q/VC_Q, PIR/PIR, Cmax/Cmax ECNQ_thresh/ECNQ_thresh, QIR/QIR, FST, %utl/%utl See “Using Frame Relay Classes” in this chapter for information on the bandwidth parameters. A slash indicates you can specify a value for each direction. FST is either ForeSight enable (y) or disable (n). A “*” is a place-holder for a parameter you do not change.

cnffrcport

Configures the port speed and percent of utilization on the concentrated link of a Port Concentrator Shelf (PCS). This is not a standard command. Primarily, you would use **cnffrcport** to adjust the rate on the concentrated link due to some unusual system configuration.

Because this command applies to the FRC interface (the concentrated link) rather than the user port for the CPE, the port number and the range of speeds is the same as that of the FRP or FRM card. Thus, the port numbers are 1–4 with rates varying from 56 Kbps through 2 Mbps. During port configuration, a prompt for each parameter appears. To keep the current value of the parameter, press the Return key without typing anything.

Full Name

Configure Frame Relay port

Syntax

cnffrcport <slot.port> <percent utilization>

Related Commands

upfrport, dnfrport, dspfrport, dspcd

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnffrcport  6.1 512 88
```

Description

Reconfigure PCS port 6.1 to have a speed of 512 Kbps and a concentrated link utilization of 88%. (Note that executing **dspcd** for this slot would show a port count of 44, which indicates that the card set supports a PCS. The Configured Clock of 512 Kbps by itself does not indicate a PCS because a standard FRP-2 or FRM-2 also supports this rate.

System Response

```
minnow         TN    SuperUser       IGX 8410     9.2       Aug. 30 1998 10:16 PST

Physical Port: 6.1            [INACTIVE]
Interface:  FRI-X21 DCE                       Configured Clock:   512 Kbps
Clocking:   Normal                            Measured Rx Clock:    0 Kbps
                                       Min Flags / Frames           1
Port ID                      1022
Port Queue Depth            65535      OAM Pkt Threshold            3 pkts
ECN Queue Threshold         65535      T391 Link Intg Timer        10 sec
DE Threshold                  100 %    N391 Full Status Poll        6 cyl
Signalling Protocol          None      EFCI Mapping Enabled        No
Asynchronous Status            No      CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer       15      IDE to DE Mapping          Yes
N392 Error Threshold            3      Interface Control Template
N393 Monitored Events Count     4         Lead      I
Communicate Priority           No         State   ON
Upper/Lower RNR Thresh  75%/ 25%       Concentrated Link Util    88%

Last Command: cnffrcport 6.1 512 88


Next Command:
```

Table 8-12 cnffrcport—Parameters

Parameter	Description
slot.port	Specifies the card slot and port number. Because the port number is that of the concentrated link rather than the user port number, the range is 1–4 (not 1–44).
speed	Specifies the port clock speed for a 2.0 Mbps FRP-2 or FRM-2. The display shows the *configured* speed as Configured Clock and the *actual* speed as Measured Rx Clock. The available speeds are: 1 port (selected speeds, 56–2048 Kbps) 2 ports (selected speeds, 56–1024 Kbps) 3 ports (selected speeds, 56–672 Kbps) 4 ports (selected speeds, 56–512 Kbps)
utilization	Specifies the percent of utilization of the concentrated link.

cnffrport

Configures the parameters of a Frame Relay port. The **cnffrport** command applies to the UFM/UFI, FRP/FRI, FRM/FRI, and FRM-2/FRP-2. (Note that a less commonly used command also exists for the concentrated link between the PCS and FRM-2 or FRP-2: **cnffrcport**.)

During port configuration, a prompt for each parameter appears. To keep the current value of the parameter, press the Return key without typing any characters. When a parameter is not configurable for an application, the parameter appears shaded or with dashed lines. You can mix the data rate for each of the ports if the total for all ports does not exceed the maximum composite data rate that the card set supports. Table 8-12 shows the supported data rates for individual T1 and E1 lines.

Table 8-13 T1 and E1 Data Rates

Data Rates at 56 Kbps Increments				Data Rates at 64 Kbps Increments			
56	112	168	224	64	128	192	256
280	336	392	448	320	384	448	512
504	560	616	672	576	640	704	768
728	784	840	896	832	896	960	1024
952	1008	1064	1120	1088	1152	1216	1280
1176	1232	1288	1344	1344	1408	1472	1536
1400	1456	1512	1568	1600	1664	1728	1792
1624	1680	1736	1792	1856	1920	1984	2048

Table 8-13 shows the available data rates on a single, PCS user-port. For the FRP-2 and FRM-2 cards, the maximum composite data rate over the 44 logical, user-ports is 1.792 Mbps.

Table 8-14 PCS Data Rates

Data Rates in Kbps							
9.6	14.4	16	19.2	32	38.4	48	56
64	112	128	168	192	224	256	280
320	336	384					

For a PCS, some additional rules for assigning data rates to the 44 ports apply:

- No single user-port should have a speed greater than 384 Kbps.
- The total for each group of 11 ports should not exceed 448Kbps. The software allows higher rates, but the system may drop data if user-equipment passes data above the aggregate total of 448 Kbps.
- The port numbers for the 11-port groups are 1–11, 12–22, 23–33, and 34–44.

Signaling Protocol Timers

This section introduces the implementation of two signaling timers and related parameters you can specify through the **cnffrport** command.

Periodically, devices use *signaling* to request the status of other, connected devices or networks. The signaling can be a simple confirmation of the other device's existence or more detailed information, such as the DLCIs, bandwidth, and state of all PVCs. The signaling described here occurs between:

- The user-equipment and a Frame Relay port across the user-to-network interface (UNI)
- Frame relay ports in the network across the network-to-network interface (NNI)

Periodically, Frame Relay ports within the network transmit a Status Enquiry and wait for a Status response. These exchanges occur across the UNI and the NNI. At the UNI, the user-equipment periodically sends a series of Status Enquiries and awaits a Status response for each enquiry. At the NNI of any network, a Frame Relay port can generate Status Enquiries and, at alternate times, receive Status Enquiries. In this way, the signaling between networks mirror each other. (Figure 8-3 shows the three possible exchanges.) The timers for Status Enquiry and Status response and other, related parameters are the:

- *Link integrity timer*—the time period between each Status Enquiry that either the user-equipment or a Frame Relay port in the network generates
- *Polling verification timer*—a time period in which a Frame Relay port waits for a Status response to a Status Enquiry that the port generated
- *Error threshold*—the number of missing or erroneous events that triggers a Port Communication Failure
- *Monitored events count*—the number of events in a polling cycle
- *Full status polling cycle*—a polling cycle in which the port that has sent the Status Enquiry waits for detailed status information

In the preceding list, an *event* is either a Status Enquiry or a Status response. The meaning of the event depends on whether the link integrity timer or the polling verification timer is waiting for the event. The link integrity timer waits for *Status responses*. The polling verification timer waits for *Status Enquiries*.

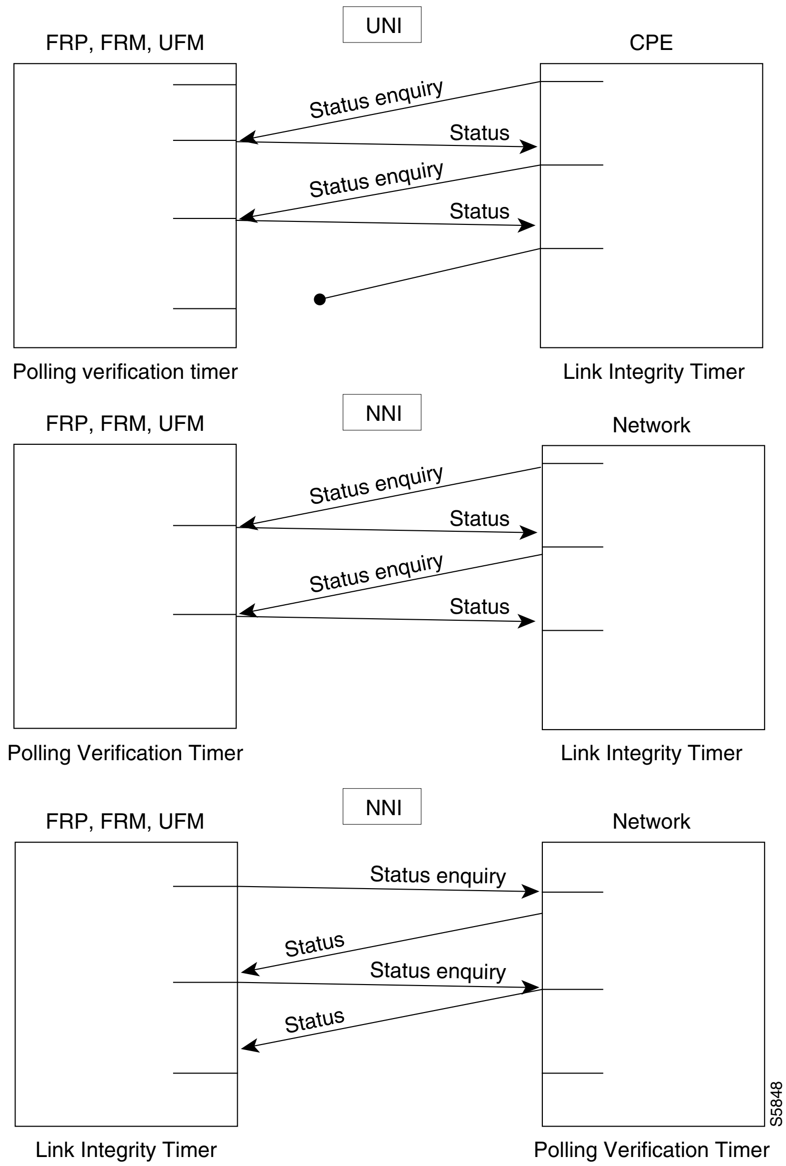
Most Status Enquiries contain only a sequence number. After sending these simple Status Enquiries, the polling device checks for the sequence number. Periodically, a *full status polling cycle* takes place, in which the polling device waits for all applicable information, such as the status of all connections that cross the NNI. For signaling across the UNI, the Frame Relay Forum has recommended a full status polling cycle at every sixth polling cycle. The Frame Relay Forum has not recommended a frequency for the NNI. The **cnffrport** command lets you select a frequency in the range of once every 1–10 polling cycles.

The Frame Relay port or user-device counts a user-specified number of errors out of a user-specified number of attempts before it signals a Port Communication Failure. These parameters are the *error threshold* and the *monitored events count*, respectively. The defaults for these parameters are 3 and 4, respectively. To use the defaults in an example: if 3 out of 4 events are either missing or erroneous within the specified time period, the port signals a Port Communication Failure (a minor alarm).

An event has a user-specified amount of time to arrive. The allowed time period for the arrival of a valid event is the number of seconds you assign to a timer. If an enquiry or response is missing or bad within the timer value, the event is failed. Again, using all default values in an example: if the polling verification timer is 15 seconds and no Status Enquiry arrives within that time, the port records a missing Status Enquiry. If no Status Enquiry arrives during the next two 15-second periods, the port signals a Port Communication Failure. In the UNI example in the figure, the third Status Enquiry does not arrive. Note that each time a Status Enquiry arrives, the polling verification timer restarts counting at 0 seconds rather than waiting until the specified number of seconds has elapsed.

Whether the port is on a UNI or NNI, the polling verification timer setting must be longer than the link integrity timer. (Refer to the forthcoming **cnffrport** parameters table for values.) You cannot set the link integrity timer for the user-equipment with **cnffrport**. Usually, the link integrity timer on user-equipment is 10 seconds, which you can verify by executing **dspportstats** and counting the number of seconds between statistical updates. On the NNI, you can set both timers (they use either Annex A or Annex D).

Figure 8-3 Signaling Protocol Timing



The 1 Mbps FRI

The data rates available with the 1 Mbps FRI are:

Table 8-15 Data Rates for the 1-Mbps FRI

Port Data Rates in *Kbps* for 1Mbps FRI			
1024	512	256	128
896	448	224	112
768	384	192	64
672	336	168	56

The rules for assigning data rates to the four ports when using the 1 Mbps FRI are:

- If you assign a data rate of 672 Kbps or higher on any port, you cannot use any other port.
- If you assign a data rate of between 384 Kbps and 512 Kbps to any port, you can specify a second port with an available data rate of 512 Kbps or less.
- If you assign a data rate of 336 Kbps to any port, you can specify two other ports for any available data rates of 336 Kbps or less.
- If the data rate of any port does not exceed 256 Kbps, you can specify all four ports with any available data rates of 256 Kbps or less.

Full Name

Configure Frame Relay port

Syntax (T1/E1 ports on UFM-C)

cnffrport <slot.port> <line.DS0_range> <port queue depth> <ecn queue threshold> <de threshold> <signaling protocol> [*protocol parameters*]

Syntax (Unchannelized ports on UFM-U)

cnffrport <slot.port> <port type> <port queue depth> <ecn queue threshold> <de threshold> <signaling protocol> [*protocol parameters*]

Syntax (T1/E1 ports on FRM or FRP)

cnffrport<slot.port> <port queue depth> <ecn queue threshold> <de threshold> <signaling protocol> [*protocol parameters*]

Syntax (All other ports—for an FRM or FRP)

cnffrport <slot.port> <speed> <port queue depth> <clocking> <de_threshold> <min-flags-bet-frames> <ECN q_threshold> <port ID> <signaling protocol y/n> [*protocol parameters*]

Related Commands

addfrport, upfrport, dnfrport, dspfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnffrport 3.1 48000 48000 100 n N Y 1
```

Description

Change Frame Relay port 3.1 to have queue depths of 48000. The interface in this example is a T1.

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2       Sep. 10 1997 16:25 GMT

Port:       3.1               [ACTIVE  ]
Interface:  FRI-T1                           Configured Clock:    64 Kbps
Clocking:   None                             Measured Rx Clock: None
                                      Min Flags / Frames           1
Port ID                       -       Channel Range                1
Port Queue Depth          48000       OAM Pkt Threshold            3 pkts
ECN Queue Threshold       48000       T391 Link Intg Timer        10 sec
DE Threshold                100 %     N391 Full Status Poll        6 cyl
Signalling Protocol        None       EFCI Mapping Enabled        No
Asynchronous Status          No       CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer     15       IDE to DE Mapping          Yes
N392 Error Threshold          3       Channel Speed               64
N393 Monitored Events Count    4
Communicate Priority         No
Upper/Lower RNR Thresh  75%/ 25%

Last Command: cnffrport 3.1 48000 48000 100 n N Y 1


Next Command:
```

Example 2

cnffrport 5.1 256 n 12000 10000 100 a N N 15 3 4 3 y y 100 Y 1

Description

Change queue depths for port 8.1. An explanation of the screen appears after the screen example.

System Response

```
padma       VT    SuperUser       IGX 8410     9.2       Sep. 10 1998  16:39 GMT

Port:       5.1               [ACTIVE  ]
Interface:  FRI-V35 DCE                           Configured Clock:   256 Kbps
Clocking:   Normal                                Measured Rx Clock:  256 Kbps
                                       Min Flags / Frames           1
Port ID                        0
Port Queue Depth           12000       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        10000       T391 Link Intg Timer        10 sec
DE Threshold                 100 %     N391 Full Status Poll        6 cyl
Signalling Protocol  Annex A UNI       EFCI Mapping Enabled       Yes
Asynchronous Status           No       CLLM Enabled/Tx Timer  Yes/100 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead    CTS    DSR    DCD
Communicate Priority          No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: cnffrport 5.1 256 NORMAL 0 12000 10000 100 a N N 15 3 4 3 y y 100
Y 1

Next Command:
```

The screen in Example 2 shows the following:

• Port Speed (configured, measured)	256 Kbps 256 Kbps	The screen displays both the configured clock speed and the measured clock speed—256 Kbps for both in this case.
• Clocking (type)	Normal	Of the two clocking types, the interface uses normal clocking.
• Port ID	0	The optional Port ID has not been specified.
• Port Queue Depth	12000	Depth of port queue is set at 12000 bytes.
• ECN Queue Depth	10000	Port queue must reach 10000 bytes before FECN and BECN bits are set.
• DE Threshold	100	Port buffer must be 100% full before DE frames are dropped.
• Signaling Protocol	Annex A	The selected protocol for the UNI.
• Asynchronous Status	N	No asynchronous messages to user-device; wait for polling from user-device.
• Polling Verify Timer	15	15 seconds heartbeat period.
• Error Threshold	3	3 failures trigger port communication failure.
• Monitored Events Count	4	4 events are monitored.
• Communicate Priority	N	Do not communicate port priority to user-device.
• Upper RNR Threshold	75	75% of buffer capacity triggers receiver not ready condition.
• Lower RNR Threshold	25	25% of buffer capacity clears a receiver not ready condition.
• Minimum Flags/Frame	1	One flag exists for each FR data frame.

Example 3

cnffrport 13.1

Description

Configure the parameters for the newly upped V.35 port at 13.1. In this case, the only change is the port type: the interface becomes a DTE in this example.

```
sw180          TN    SuperUser       IGX 16    9.2 July 30 1997 00:09 GMT
Port:       13.1              [ACTIVE  ]
Interface:  V35     DCE                      Configured Clock:    256 Kbps
Clocking:   Normal                           Measured Rx Clock:     0 Kbps

Port ID                       0       Min Flags / Frames           1
Port Queue Depth          65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold       65535       T391 Link Intg Timer        10 sec
DE Threshold                100 %     N391 Full Status Poll        6 cyl
Signalling Protocol        None       EFCI Mapping Enabled        No
Asynchronous Status          No       CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer     15       IDE to DE Mapping          Yes
N392 Error Threshold          3       Interface Control Template
N393 Monitored Events Count   4          Lead    CTS    DSR    DCD
Communicate Priority         No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: cnffrport 13.1 DTE 256 NORMAL 0 65535 65535 100 n N N Y

Next Command:
```

Note The following table describes both mandatory and optional parameters because some parameters are mandatory for T1/E1 lines and optional for other line types.

Table 8-16 cnffrport—Parameters

Parameter	Description
slot.port	Specifies the logical port on the FRP, FRM, or UFM-U in the format *slot.port*. For a T1/E1 line on an FRM or FRP, port is a logical number. For a UFM-C, the range for port is 1–250. (See the description of *slot.port line* in the *Cisco IGX 8400 Series Reference* manual.) For a Port Concentrator Shelf, *port* is to the logical port in the range 1–44.
port type (for a UFM-U) For *port type* on a PCS, see next box.	Specifies whether a port on a UFM-U is DCE or DTE. The prompt appears if the system detects a UFM-U. The default is DCE. For an FRM or FRP, “port Type” is display-only because jumper blocks on the back cards set the mode. When you use **cnffrport** in a job, the “Enter mode (line or port)” prompt follows *slot.port*. Note that this *mode* is the interface type of the Frame Relay port rather than the mode of the UFM-U. Valid entries are HSSI, V35, X21, PORT (PORT is generically “unchannelized”), or LINE (LINE indicates T1 or E1). If the front card is a UFM-U, a subsequent prompt asks you to specify DCE or DTE.
port type (for a PCS) (For port type on a UFM-U, see preceding box.)	*Port type* for a PCS tells switch software whether the port is V.35, V.11 or V.28. *Port type* for a PCS does not actually configure the port: to configure the port, you must install the appropriate card in the PCS. See the *port type* description for the UFM-U for information on **cnffrport** in a job.

Table 8-16 cnffrport—Parameters (Continued)

Parameter	Description
interface type	Specifies an interface type for a Port Concentrator Shelf (PCS). This parameter appears if switch software detects a PCS. It applies to the user interface display only and not the PCS itself because system software does not detect the interface type within the PCS. To change the user-interface type, you must change a card in the PCS.
slot.port line	Specifies the UFM-C slot, port, and line number, where *port* can be 1–250, and *line* can be 1–8. Note that the maximum number of T1/E1 lines per node is 32. This maximum could be, for example, spread over 4 UFM-8C card sets that utilize all 8 lines on each back card.
speed	Specifies a port clock speed in Kbps for a 2.0 Mbps UFM, FRP, or FRM. The *configured* speed appears under the Configured Clock heading. The *actual* clock rate appears under the Measured Rx Clock heading. Note that this option does not apply to T1/E1 lines because these line types use 64 or 56 Kbps timeslots. The range of speeds according to the number of active ports is as follows: • 1 port (selected speeds, 56–2048 Kbps) • 2 ports (selected speeds, 56–1024 Kbps) • 3 ports (selected speeds, 56–672 Kbps) • 4 ports (selected speeds, 56–512 Kbps) Refer to the table at the beginning of this command description for the available clock rates for all port combinations.
clocking	Specifies the port's clock type for HSSI, V.35, and X.21 lines. *Clocking* does not apply to T1, E1, or Port Concentrator lines. The clock is either *normal* or *looped*. Four combinations of clocking are available for the V.35 ports. Two combinations of clocking are available for HSSI and X.21. Note that the clock and data direction in DCE mode is the opposite of the direction for DTE mode. The possibilities are: • FRP, FRM, or UFM-U port is DCE with normal clocking (HSSI, V.35, X.21). • FRP, FRM, or UFM-U port is DCE with looped clocking (V.35 only). • FRP, FRM, or UFM-U port is DTE with normal clocking (HSSI, V.35, X.21). • FRP, FRM, or UFM-U port is DTE with looped clocking (V.35 only). For a description of looped and normal clocking, refer to the *Cisco IGX 8400 Series Reference* manual*,* or the *Cisco WAN Switching System Overview.*
port ID	Specifies the DLCI associated with the port (0–1024) {0}. A node uses this number when you add bundled connections. Otherwise, port ID can be used as a network destination number in global addressing. The *port ID* does not apply to T1, E1, or PCS ports.
port queue depth	Specifies the maximum bytes in the transmission queue at the UFM, FRP, or FRM port. The range is 0–65535 bytes. The default is 65535 bytes.
ecn queue threshold	Specifies the threshold at which the system begins to generate explicit congestion notification (BECN and FECN bits) for the port. The range is 0–65535 bytes. The default is 65535 bytes.
de threshold	Specifies the port queue depth above which the system discards frames with a set Discard Eligibility (DE) bit. The range is 0–100%. The default is 100%. A threshold of 100% disables DE for the port because a queue cannot contain more than 100% of its capacity.

Table 8-16 cnffrport—Parameters (Continued)

Parameter	Description
signaling protocol	Specifies the LMI operation mode. The first time you execute **cnffrport** on a port, the command line interface displays the following options for this parameter: "none, Strata LMI, a (for Annex A), and d (for Annex D)." If you enter "a" or "d," the subsequent prompt asks if the interface is NNI. For the *initial* port specification and *subsequent* port specifications for a particular port, you can also use a single digit from the LMI definition list that follows. The total industry standard range is 0–255, but Cisco WAN Switching nodes recognize only the following (the default is internally recognized as LMI=2): LMI = 0 LMI is disabled at this port. LMI = 1 Cisco LMI and the asynchronous update process is enabled at this port. Greenwich Mean Time is also enabled. LMI = 2 LMI is disabled at this port. LMI = 3 Cisco LMI is enabled at this port, but asynchronous update process is disabled. LMI = 4 The port configuration is UNI using CCITT Q.933 Annex A parameters. LMI = 5 The port configuration is UNI using ANSI T1.617 Annex D parameters. LMI = 6 The port configuration is NNI using CCITT Q.933 Annex A parameters. LMI = 7 The port configuration is NNI using ANSI T1.617 Annex D parameters. For any Frame Relay card set that has a maximum frame length of 4510 bytes, the use and type of a signaling protocol results in a limit on the possible number of connections per port (the port here is either physical or logical). The maximum number of connections per port for each protocol is as follows: For Annex A: 899 For Annex D: 899 For StrataLMI: 562 Neither **addcon** nor **cnffrport** prevents you from adding more than the maximum number of connections on a port. (You might, for example, use **cnffrport** to specify an LMI when too many connections for that particular LMI already exist.) If the number of connections is exceeded for a particular LMI, the LMI does not work on the port, the full status messages that result are discarded, and LMI timeouts occur on the port. A port failure results and also subsequently leads to a-bit failures in other segments of the connection path.
asynchronous status	Specifies whether the node should send unsolicited LMI update messages when they appear or wait for the user-device to poll. Enter y (yes) or n (no).
polling verify timer	Specifies a Link Integrity Verification Timer heartbeat (keep-alive) period. The range is 5–30. The default is 15. Set the timer to 5 secs. more than the setting in the user equipment.
error threshold	Specifies the number of failures in the monitored events that cause the "keep alive" process to report an alarm. The theoretical range is 0–255. The valid range is 1–10. A threshold of 0 reverts to 1. A threshold greater than 10 reverts to 10.
monitored events count	Specifies the number of monitored events for the "keep alive" process. It has a theoretical range of 0–255 and a valid range of 1–10. A port communication-fail condition is cleared after this number of successful polling cycles. A value of 0 reverts to 1, and a value more than 10 reverts to 10.
communicate priority	Specifies whether the system should communicate the SNA priority of the connections to the user-device on the port. Enter y (yes) or n (no). (SNA priority is either H or L.)

Table 8-16 cnffrport—Parameters (Continued)

Parameter	Description
upper/lower RNR threshold	Specifies the *receiver not ready* (RNR) thresholds. The upper threshold is the number of receiver not ready indications from the user equipment before an alarm is generated for this port. The lower RNR threshold is the number of indications from the user equipment before an alarm is cleared. The range is 1–255. The default for the upper RNR threshold is 75. The default for the lower RNR threshold is 25.
Enable EFCI to BECN mapping	Directs the system to map the ForeSight congestion bit (which is set in the FastPackets by a trunk card) to the FECN and BECN bits on the affected PVC.
ForeSight over port	Specifies whether the system should use CLLM over the port.
min. flags/frame	Specifies the minimum number of flags between frames when the direction of transmission is from the node to the user-equipment. Any value greater than 0 is valid on the UFM, FRP or FRM. The default is 1. On a Port Concentrator Shelf, the range is 1–16.
OAM FastPacket threshold	Specifies how many OAM FastPackets must arrive from a remote NNI port before the local port generates “Abit = 0” in the signaling protocol message to the locally attached device. The range for this parameter is 0–15 packets. The default is 3 packets. A 0 disables this function. The *OAM FastPacket threshold* setting applies to UNI and NNI ports. The following two paragraphs provide a more detailed explanation of the Abit and *OAM FastPacket threshold* usage. On any Frame Relay port (UNI or NNI) that is using a signaling protocol (Cisco LMI, Annex A, or Annex D), the FRP or FRM provides a Status message to the attached equipment in response to a Status Enquiry message or as an Asynchronous Update. These Status messages contain details about every PVC configured on the port. In particular, the “PVC Active” bit (the Abit) represents whether a PVC is active (Abit=1) or out of service (Abit = 0). If the other end of the connection PVC on a UNI port, the only conditions that can cause the local Frame Relay card to send an Abit=0 are: • The PVC being “down” (intentionally taken out of service) • The PVC being failed for any reason (such as a hardware failure, trunk failure with no ability to reroute, and so on) If the other end of the PVC terminates on an NNI port, one additional condition can cause the local UFM, FRP, or FRM to send an Abit=0 to the local device: if the remote NNI port on the card receives an Abit=0 from the remote network over the remote NNI, then the local card can propagate an Abit=0 out the local port. The mechanism by which the remote card notifies the local card of the Abit=0 coming from the remote network is OAM FastPackets. The local node sends one OAM FastPacket every 5 seconds for as long as the Abit coming from the remote network is 0.
link integrity timer (T391)	Specifies the interval after which the system sends Status Enquiry messages across the NNI port. The range for the interval is 5–30 seconds. The default is 6 seconds. Both networks do not need to have the same T391 value. On a Frame Relay NNI port, the Link Integrity Timer (T391) specifies how often the UFM, FRP, or FRM generates a Status Enquiry message to the attached network using the selected NNI signaling protocol (Annex A or Annex D). The card should receive a Status message for every Status Enquiry message it transmits. If the Frame Relay card receives either no responses or invalid responses, a Port Communication Failure results (and causes a minor alarm). Using the default values for N392 Error Threshold and N393 Monitored Events Count in an example: an error occurs when no response (or a bad response) arrives for 3 out of the last 4 Status Enquiry messages. (The default for N392 Error Threshold is 3. For N393 Monitored Events Count, the default is 4.)

Table 8-16 cnffrport—Parameters (Continued)

Parameter	Description
N392 error threshold	Specifies the number of bad or undelivered responses to Status Enquiry messages that can occur before the system records a Port Communication Failure. The range is 1–10. The default is 3. See the description of the *link integrity timer* parameter for example usage.
N393 monitored events count	Specifies the number of Status Enquiry messages in a period wherein the system waits for responses to the enquiries. The range is 1–10. The default is 4. See the description of the *link integrity timer* parameter for example usage.
full status polling cycle (N391)	Specifies the interval at which the system sends the Full Status Report request for all PVCs across the NNI port. The range is 1–255 polling cycles. The default is 10 cycles. The Full Status reports the status of *all* the connections across the NNI.
card type	Specifies the card type when you enter the **cnffrport** command in a job. This parameter is not available except when you specify **cnffrport** in a job by using the **addjob** command. During the job specification, you enter the *card type* just after the *slot.port* during the command specification phase of **addjob**. Valid *card types* are "V.35," "X.21," "port," and "line," where "line" indicates a T1 or E1 line.
CLLM status Tx Timer	Specifies an interval for the system to send ForeSight congestion messages across the NNI. The range is 40 ms–350 ms. The default is 100 ms. Both networks must be Cisco WAN Switching networks.
IDE to DE mapping	Specifies whether the destination system should map the internal DE bit (IDE) status in the FastPacket or ATM cell to the Frame Relay DE bit at the destination. Enter y (yes) or n (no). If you specify the non-standard case of CIR=0 with either **addcon** or **cnffrcls**, you must first enable *IDE to DE mapping*. Refer to the section titled "Using Frame Relay Classes" for important information on setting CIR=0.
interface control template	Specifies the control leads available on the V.35 and X.21 physical Frame Relay ports and the meaning for each lead.
channel range	Specifies the DS0s for the T1 or E1 logical port. The value can be 1 or a contiguous combination in the range 1–24 for T1 or 1–31 for E1. For example, 7–12 indicates 6 DS0s for the port, starting with DS0 7. Before you use this command, specify the valid channel range with the **addfrport** command.
channel speed	Specifies the bandwidth available to a logical port. The speed is 64 Kbps times the number of DS0s you specify with the *channel range* parameter.

cnfict

Configures the interface control template signals. Each interface control lead must be individually configured. (Each data channel has a default interface control template for its active, conditioned, and looped-near and far states.) The signals available to **cnfict** depend on the type of back card and whether the port mode is DCE or DTE. On an IPX node, the applicable front cards are the SDP, LDP, FRP, CDP (for data), and FTC (for data). On an IGX node, the applicable front cards are the LDM, HDM, FRM, UFM, CVM (for data), and FTM (for data).

Note The **cnfict** command is not valid for V.11 and X.21 interfaces. For FRP V.35 and Port Concentrator V.35 and V.28 interfaces, only the active template is usable, and you can configure the leads to on or off.

When Y-cable redundancy is in effect, the control template configuration for the data channels terminating at the primary slot also applies to the data channels of the secondary slot. Any configuration information you attempt to apply to the secondary slot is ignored. The following lists which leads are configurable for each type of data interface supported by the IGX node. The entries under the "IGX Name" column indicate the abbreviations to use when you specify input or output leads on the command line.

Table 8-17 Configurable Lead Listing

Source	IGX Name	EIA/TIA-232C	EIA/TIA-232D	EIA/TI-449	V.35	X.21	Fast EIA	CCITT (ITU-T) Equivalent	Function
DTE	RTS	CA	CA	RS	C		F4	105	Request to Send
DCE	CTS	CB	CB	CS	D		F4	106	Clear to Send
DCE	DSR	CC	CC	DM	E		F3	107	Data Set Ready
DCE	DCD	CF	CF	RR	F		F7	109	Data Carrier Detect (
DCE	QM	QM	QM						Equalizer Mode
DTE	pin 11	11	11						Sometimes used for
DCE	SDCD	SCF	SCF					122	Secondary Data Carr
DCE	SCTS	SCB	SCB					121	Secondary Clear to S
DTE	STxD	SBA	SBA				F5	118	Secondary Transmit
DTE	NS			NS			F7		New Sync
DCE	SRxD	SBB	SBB				F5	119	Secondary Receive D
DCE	DCR	DCR							Divided Receiver Cl
DTE	RL		RL	RL			F6		Remote Loopback
DTE	SRTS	SCA	SCA					120	Secondary Request t
DTE	DTR	CD	CD	TR	H		F3	108.2	Data Terminal Ready
DCE	SQ	CG	CG	SQ				110	Signal Quality Detec
DCE	RI	CE	CE	IC	J**			125	Ring Indicator
DTE	SF	CH	CH	SF				111	Signal Rate Select (t
DCE	SI	CI	CI	SI				112	Signal Rate Select (t
DTE	BSY	BSY		IS			F1		Busy (In Service)

Table 8-17 Configurable Lead Listing (Continued)

Source	IGX Name	EIA/TIA-232C	EIA/TIA-232D	EIA/TI-449	V.35	X.21	Fast EIA	CCITT (ITU-T) Equivalent	Function
DCE	SB		TST	SB			F1		Test Indicator
DTE	LL			LL			F2		Local Loopback
DCE	TM			TM	K**		F6		Test Mode
DTE	SS			SS					Select Standby
DTE	C					C			Control
DCE	I					I			Indicator

Asterisks (**) indicate the listing is applicable to only an SDP or HDM card. Pins 11 and 23 on an RS-232 port are bi-directional, and their default direction is input. See the **cnfcldir** command for information on changing the direction of these pins. The **cpyict** command can be used to copy an interface control template from one data channel to another. The template can then be edited using the **cnfict** command. The **dspbob** command displays the state of leads at specified intervals.

The preceding list shows the equivalence between RS-232C, RS-232D, RS-449, V.35, and X.21 interfaces. An IGX treats leads impartially for non-interleaved connections. Any signal arriving on an EIA pin at one end may be transmitted to any pin at the other end. An imposed maximum of 12 EIA leads applies to any interface type. For interleaved EIA connections, the “Fast EIA” column shows which leads are carried in the interleaved bytes in the data packets. All remaining leads are carried in traditional control lead packets.

Full Name

Configure interface control template

Syntax

cnfict <port> <template> <output> <source>

Related Commands

addextlp, dspict, tstport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cnfict 25.1 a cts on
```

Description

Configure the active interface control template for channel 25.1 to CTS-on. CTS-on means that when the port is active, the CTS lead is asserted.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:36 MST

Data Channel:      25.1
Interface:         RS232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                       Lead    Output Value
 RI      OFF                                DSR     ON
 CTS     ON                                 SRxD    ON
 DCR     OFF                                DCD     ON
 SCTS    ON                                 SDCD    ON
 SQ      ON




Last Command: cnfict 25.1 a cts on


Next Command:
```

Example 2

cnfict 9.1 a rts on

Description

Configure the active interface control template to have RTS-on. This means that when the port is active. the RTS lead is asserted.

System Response

```
alpha          TRM   YourID:1        IGX 8430    9.2    Aug. 23 1998 10:23 PST

Port:       9.1               [ACTIVE  ]
Interface:  FRI-V35 DTE                        Configured Clock:   256 Kbps
Clocking:   Normal                             Measured Rx Clock:    0 Kbps
Port ID                        7
Port Queue Depth           65535       OAM Pkt Threshold             3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer          6 sec
DE Threshold                 100 %     N391 Full Status Poll        10 cyl
Signalling Protocol         None       ForeSight (CLLM)             No
Asynchronous Status           No       CLLM Status Tx Timer          0 msec
T392 Polling Verif Timer      15       Interface Control Template
N392 Error Threshold           3          Lead       State
N393 Monitored Events Count    4           RTS        ON
Communicate Priority          No           DTR        ON
Upper/Lower RNR Thresh  75%/ 25%
Min Flags / Frames            1

Last Command: cnfict 9.1 a rts on


Next Command:
```

Example 3

cnfict 31.1 n dsr on

Description

Configure the near interface control template for 31.1, to DSR on (DDS trunk).

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:38 MST

Data Channel:      31.1
Interface:         DDS-4   OCU Config
Clocking:          Looped

            Interface Control Template for Connection while NEAR EXT LOOPED

 Lead    Output Value                   Lead    Output Value
 DSR     ON                             CTS     ON
 DCD     ON




Last Command: cnfict 31.1 near dsr on


Next Command:
```

Table 8-18 cnfict—Parameters

Parameter	Description		
port	Specifies the data channel or Frame Relay port whose interface control template you want to configure. Specify the port in the format *slot.port*		
template	Specifies which interface control template to configure for the channel and has the format: a/c/l/n/f. Valid entries are:		
	Entry	**Template**	**Description**
	a	Active	The active" control template is in effect while the data channel is active (normal operation).
	c	Conditioned	The conditioned control template is in effect when conditioning is applied to the data channel. The conditioned template is used when the network detects that it cannot maintain the connection because of card failures or lack of bandwidth (The connection is failed.)
	l	Looped	The looped template is in effect when the data channel is being looped back in either direction. The looped template is used when the **addloclp** command or the **addrmtlp** command has been used to loop the connection within the network.
	n	Near loopback	The near template is in effect when running a **tstport n** command or an **addextlp n** command on a port. The port is configured such that the external near modem is placed in a loopback.
	f	Far loopback	The far template is in effect when running a **tstport f** command or an **addextlp f** command on a port. The port is configured such that the external far-end modem is placed in a loopback.
	The only valid template for a Frame Relay port, X.21 or V.35, is the ACTIVE template. Also, all the output leads have steady state values and do not follow local or remote inputs.		
output	Specifies the output lead to configure. Valid abbreviations for output leads are listed in the previous parameter (template). Configurable output leads vary depending on the type of data interface: RS-232, V.35, X.21, or RS-449.		
source	Specifies how the lead is to be configured and has the format: on | off |local|remote input delay Delay is an optional parameter. The following lists the valid source choices:		
	on	The output lead is asserted.	
	off	The output lead is inhibited.	
	l	(for local) indicates that the output follows a local lead.	
	r	(for remote) indicates that the output follows a remote lead.	
	input	The name of the local or remote input lead that the output lead follows.	
	delay	The time in milliseconds that separates the "off" to "on" lead transitions. Delay is valid *only* when the output lead is CTS and the input lead is local RTS. "On" to "Off" lead transitions are not subject to this delay.	

cnfmode

Selects a *mode* of the card for a UFM-U back card. The mode of a card is combination of maximum port speeds and for specific port numbers. Table 8-18 lists the maximum port speeds and active ports for each mode. The **cnfmode** command lets you select 1 of 27 modes for either a UFI-12V.35 back card or a UFI-12X.21 back card. For a UFI-4HSSI back card, 3 modes are available. Note that you specify the actual speed of an individual port by using **cnffrport**. The IGX documentation describes the application of the modes and the sequence of execution of these commands.

Note that **cnfmode** and **cnfufmumode** are the same command.

Table 8-19 Card Modes for Unchannelized Back Cards

	V.35 and X.21 Ports												HSSI Ports			
	Group A				Group B				Group C				A		B	
Mode	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
1	3	3	3	3	3	3	3	3	3	3	3	3	8	8	8	8
2	8	-	8	-	8	-	8	-	8	-	8	-	16	-	16	-
3	10	-	-	-	10	-	-	-	10	-	-	-	16	-	-	-
4	8	-	8	-	3	3	3	3	3	3	3	3				
5	10	-	-	-	3	3	3	3	3	3	3	3				
6	8	-	8	-	8	-	8	-	3	3	3	3				
7	10	-	-	-	8	-	8	-	3	3	3	3				
8	10	-	-	-	10	-	-	-	3	3	3	3				
9	10	-	-	-	8	-	8	-	8	-	8	-				
10	10	-	-	-	10	-	-	-	8	-	8	-				
11	3	3	3	3	8	-	8	-	3	3	3	3				
12	3	3	3	3	3	3	3	3	8	-	8	-				
13	3	3	3	3	10	-	-	-	3	3	3	3				
14	3	3	3	3	3	3	3	3	10	-	-	-				
15	8	-	8	-	3	3	3	3	8	-	8	-				
16	3	3	3	3	8	-	8	-	8	-	8	-				
17	8	-	8	-	10	-	-	-	3	3	3	3				
18	8	-	8	-	3	3	3	3	10	-	-	-				
19	3	3	3	3	8	-	8	-	10	-	-	-				
20	3	3	3	3	10	-	-	-	8	-	8	-				
21	10	-	-	-	3	3	3	3	8	-	8	-				
22	10	-	-	-	3	3	3	3	10	-	-	-				
23	3	3	3	3	10	-	-	-	10	-	-	-				
24	8	-	8	-	10	-	-	-	8	-	8	-				
25	8	-	8	-	8	-	8	-	10	-	-	-				
26	10	-	-	-	8	-	8	-	10	-	-	-				
27	8	-	8	-	10	-	-	-	10	-	-	-				

Full Name

Configure mode

Syntax

cnfmode <port> <mode>

Related Commands

cnffrport, dspmode, dspmodes

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Node	Yes	IGX	Yes

Example 1

`cnfmode 13 4`

Description

Configure the UFM-U card set in slot 13 to have mode 4. Note that the display shows which ports are active for each mode number but does not show the current mode of the UFM-U. To see the current mode of the UFM-U, use **dspmode**.

System Response

```
w180          TN    SuperUser       IGX 16    9.2 July 30 1997 01:25 GMT


                    UFMU MODES AND PORT AVAILABILITY BITMAP

Mode[ 1]:111111111111   Mode[ 2]:101010101010   Mode[ 3]:100010001000
Mode[ 4]:101011111111   Mode[ 5]:100011111111   Mode[ 6]:101010101111
Mode[ 7]:100010101111   Mode[ 8]:100010001111   Mode[ 9]:100010101010
Mode[10]:100010001010   Mode[11]:111110101111   Mode[12]:111111111010
Mode[13]:111110001111   Mode[14]:111111111000   Mode[15]:101011111010
Mode[16]:111110101010   Mode[17]:101010001111   Mode[18]:101011111000
Mode[19]:111110101000   Mode[20]:111110001010   Mode[21]:100011111010
Mode[22]:100011111000   Mode[23]:111110001000   Mode[24]:101010001010
Mode[25]:101010101000   Mode[26]:100010101000   Mode[27]:101010001000

This Command: cnfmode 13


Enter The New UFMU Mode [1]: 4
```

Table 8-20 cnfmode—Parameters

Parameter	Description
slot	Specifies the slot of the UFM-U card.

Table 8-20 cnfmode—Parameters (Continued)

Parameter	Description
mode	Specifies the mode of the UFM-U card set. The range for V.35 and X.21 ports is 1–27. The range for HSSI ports is 1–3. You may have to delete connections and down one or more ports before you execute **cnfmode.** To determine if you must delete connection or for a detailed description of the modes of a UFM-U, see the *Cisco IGX 8400 Series Reference*.

cpyict

Copies all control template information associated with a given channel: the active template information, the conditioned template information, and the looped template information near, far. Once copied, you can edit the control template information with the **cnfict** command. See the **cnfict** command for more information on interface control templates.

Full Name

Copy SDP/LDP/FRP interface control template

Syntax

cpyict <source_port> <destination_port>

Related Commands

cnfict, dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
cpyict 25.1 25.2
```

Description

Copy the interface control template on channel 25.1 to channel 25.2.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:40 MST

Data Channel:      25.2
Interface:         RS232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                    Lead    Output Value
 RI      OFF                             DSR     ON
 CTS     ON                              SRxD    ON
 DCR     OFF                             DCD     ON
 SCTS    ON                              SDCD    ON
 SQ      ON



Last Command: cpyict 25.1 25.2


Next Command:
```

Example 2

cpyict 25.1 25.2

Description

Copy the Frame Relay interface control template on port 25.1 to 25.2.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 17:40 MST

Data Channel:      25.2
Interface:         RS232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                    Lead    Output Value
 RI      OFF                             DSR     ON
 CTS     ON                              SRxD    ON
 DCR     OFF                             DCD     ON
 SCTS    ON                              SDCD    ON
 SQ      ON



Last Command: cpyict 25.1 25.2


Next Command:
```

Table 8-21 cpyict—Parameters

Parameter	Description
source channel	Specifies the data channel or Frame Relay port.
destination channel	Specifies the data channel or Frame Relay port you want to receive the copied control template information.

delcon

Removes connections from the network. A prompt appears for confirming the deletion. Connections can be deleted from the node at either end of the connection. Do not delete a connection when the node at the other end of the connection is unreachable. The unreachable node will not recognize the deletion. It is especially important not to delete a connection to an unreachable node and then connect that channel to another node. Channel connections are added to the network with the **addcon** command.

Full Name

Delete connections

Syntax

delcon <channel(s)>

Related Commands

addcon, dspcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
delcon 25.1
```

Description

Delete connection 25.1. The connections to delete are highlighted. A prompt asks you to confirm the deletion. Respond with “y” for yes. Connection 25.1 is deleted.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:43 MST

 Local      Remote      Remote                                          Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 19.1.101   gamma       8.2.300    Ok     fr                                0  L
 19.2.302   alpha       9.2.400    Ok     fr                                0  R
 25.2       gamma       6.1        Ok     256                  7/8          0  L









Last Command:


Next Command: delcon 25.1
```

Table 8-22 delcon—Parameters

Parameter	Description
channel	Specifies the channel or set of channels in the following format: slot.port.DLCI. On an FRP or FRM, the range for *port* is 1–24 or 1–31. On a UFM-C, the range for *port* is 1–250. (For connections on a UFM-C, *line* is not necessary because of the port-to-line mapping through **addfrport**). For a UFM-U, the range for *port* is 1–12 for V.35 or X.21 and 1–4 for HSSI (unless Y-cable redundancy exists on the HSSI, in which case *port* can be only “1”). The range for *DLCI* is typically 16–1007.

delfrport (T1/E1)

The information in this description applies to only Frame Relay ports using a T1 or E1 line. The **delfrport** command deletes logical ports on FRP, FRM, or UFM-C cards and “unassigns” associated DS0/timeslots. The deleted DS0/timeslots are available for you to assign to new logical ports (with the **addfrport** command). The port display (normally visible through **dspfrport** command) appears regardless of whether the port has been successfully deleted. The screen displays the defined port numbers for the specified line. The following lists the error and warning messages for this command.

Table 8-23 delfrport—Warnings and Error Messages

Messages	Reason for Message
"Slot is out of range"	Line number is not correct for FRP T1/E1.
"Port does not exist"	Logical port number does not exist.
"You must first down the port"	Logical port is up.
"You must first down the port"	Specified port is not first DS0/timeslot of logical port.

Full Name

Delete Frame Relay port

Syntax

For FRM or FRP: **delfrport** <slot.port>

For UFM: **delfrport** <slot.port> <line.ds0_range>

Related Commands

addfrport, dspfrport, dnfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX	Yes

Example 1

```
delfrport  8.1
```

Description

Delete Frame Relay port 8.1.

System Response

```
alpha TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 17:28 CST

Port configuration for FRP 8

From     Chan     Speed     Interface     State
1        9-15     448       FRI T1        ACTIVE
20       20-24     320        FRI T1         ACTIVE









Last Command: delfrport 8.1


Next Command:
```

Table 8-24 delfrport (T1/E1)—Parameters

Parameter	Description
slot	Specifies the physical FRP or FRM T1 or E1 line. The range of logical port numbers is 1–24 for T1 lines and 1–31 for E1 lines.
port	Specifies the logical port number of the port to delete.

dnfrport

Deactivates ("downs") the specified Frame Relay port. Before deactivating a port, you must delete all connections on the port (see **delcon** description).

Full Name

Down Frame Relay port

Syntax

For UFM-U, FRM, or FRP: **dnfrport** <slot.port>

For UFM-C: **dnfrport** <slot.port> <line.ds0_range>

Related Commands

cnffrport, dspfrport, upfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
delfrport 3.1
```

Description

Down Frame Relay port 3.1.

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2      Aug. 14 1997 03:49 GMT

Port:       3.1               [INACTIVE]
Interface:  FRI-T1                          Configured Clock:    64 Kbps
Clocking:   None                            Measured Rx Clock: None
                                     Min Flags / Frames           1
Port ID                        -     Channel Range                1
Port Queue Depth           65535     OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535     T391 Link Intg Timer        10 sec
DE Threshold                 100 %   N391 Full Status Poll        6 cyl
Signalling Protocol         None     EFCI Mapping Enabled        No
Asynchronous Status           No     CLLM Enabled/Tx Timer       No/  0 msec
T392 Polling Verif Timer      15     IDE to DE Mapping          Yes
N392 Error Threshold           3     Channel Speed               64
N393 Monitored Events Count    4
Communicate Priority          No
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dnfrport 3.1


Next Command:
```

Table 8-25 dnfrport—Parameters

Parameter	Description
slot	Specifies the slot number of the Frame Relay card with the port to down.
port	Specifies the port number to deactivate on the card specified by *slot*. On an FRP or FRM, the range is 1–24 or 1–31. On a UFM-C, the range is 1–250. On a UFM-U with a V.35 or X.21 interface, the range is 1–12. On a UFM-U with a HSSI interface, the range is 1–4.
line	The physical line on UFM-C card sets (not used for UFM-U cards).

dspchcnf

Displays configuration details for voice, data, or Frame Relay channels.

Voice channels display:	Utilization, Adaptive Voice, Gain, Dial Type, Interface Type, and OnHook and Conditioning specifications.
Data channels display:	Maximum EIA Update Rate, Percentage Utilization, DFM Pattern Length, and DFM Status.
Frame relay channels display:	Minimum Information Rate, VC Queue Buffer Size or Bc, Peak Information Rate or Be, Maximum Credits, ECN Queue Buffer Size, Quiescent Information Rate, ForeSight enabled or not, and Percentage Utilization.

If the channel specified is a voice channel, the display includes configuration details for all channels on the specified circuit line starting with the specified channel. If the channel specified is a data channel, the display includes configuration details for all channels on the specified data card (CDP, SDP or LDP) starting with the specified channel. If the channel specified is a Frame Relay channel, the display includes configuration details for all channels on the specified FRP port starting with the specified channel. If you specify a Frame Relay port only with no DLCI, the display includes configuration details for all channels on the Frame Relay port specified. The display also indicates either Cisco parameters or standard Frame Relay parameters where appropriate.

Full Name

Display channel configuration

Syntax

dspchcnf <start_channel>

Related Commands

cnfchadv, cnfchdfm, cnfchdl, cnfcheia, cnfchgn, cnfchpri, cnfchutl, cnffrcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dspchcnf 9.1
```

Description

Display configuration values for all channels on Frame Relay port 9.1.

```
alpha          TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:56 PST

                Frame Relay Channel Configuration  Port: 9.1

 Channel    MIR   CIR  VC Q Depth    PIR  Cmax  ECN QThresh   QIR   FST   % Util
 9.1.100    9.6   9.6          5     256    10     65535      9.6    n      100









Last Command: dspchcnf 9.1


Next Command:
```

Table 8-26 dspchcnf—Parameters

Parameter	Description
channel	Specifies the channel at which the display begins. The format is *slot.port.DLCI*. The DLCI parameter is optional.

dspchstats

Displays traffic statistics and the statistics collection period for the specified channel. The display shows when the statistics were last cleared and the time that has elapsed during the current collection period. The statistical parameters include:

- Number of frames transmitted
- Average frame size in bytes
- Average frame rate in frames per second
- Number of packets transmitted
- Average packet rate in packets per second
- Percent of the channel in use

For each parameter, the values appear in the following categories:

- From the port (something coming into a port, typically from an external device/box)
- To the network (something going out of the switch; typically trunks)
- Discarded (received from the attached device but not transmitted to the network)
- From the network (received in; typically, into the trunk)
- To the port (transmitted out of the port, to an external device or cloud)
- Discarded (received from the network but not transmitted to the attached device)

The **dspchstats** command also displays ECN (Explicit Congestion Notification) statistics.

• FECN:	Lists number of frames sent to the receiving end router with the FECN (Forward Explicit Congestion Notification) bit set and the ratio of these frames to the total number of frames sent. This is a measure of Frame Relay congestion and the extent to which the receiving router has been informed of frames received that encountered congestion.
• BECN:	Lists number of frames sent to the transmitting end router with the BECN (Backward Explicit Congestion Notification) bit set and the ratio of these frames to the total number of frames sent. This is a measure of Frame Relay congestion and the extent to which the transmitting router has been informed of frames received that encountered congestion.
• Min-Pk. bytes rcvd:	Lists number of bytes received at the receiving end router during the greatest minute-peak of bytes received.
• minutes congested:	Lists number of congested minutes of received data since the command started.

Description of Frame Relay Channel Statistics

The following 35 statistics are available for each Frame Relay PVC (channel. Note that the statistic field name listed may be slightly different from the field name on the dspchstats screen.

1) Frames Received
2) Receive Frames Discarded
3) Frames Transmitted
4) Transmit Frames Discarded

5) Packets Received
6) Receive Packets Discarded
7) Packets Transmitted
10) Bytes Received
11) Receive Bytes Discarded
12) Bytes Transmitted
13) Transmit Bytes Discarded
17) Seconds In Service
18) Frames Transmitted with FECN
19) Frames Transmitted with BECN
21) Minutes Congested
22) DE Frames Received
23) DE Frames Transmitted
24) DE Frames Dropped
25) DE Bytes Received
26) Frames Received in Excess of CIR
27) Bytes Received in Excess of CIR
28) Frames Transmitted in Excess of CIR
29) Bytes Transmitted in Excess of CIR
32) Rx Frames Discarded - Deroute/Down
33) Rx Bytes Discarded - Deroute/Down
34) Rx Frames Discarded - VC Q Overflow
35) Rx Bytes Discarded - VC Q Overflow
36) Tx Frames Discarded - Q Overflow
37) Tx Bytes Discarded - Q Overflow
38) Tx Frames Discarded - Ingress CRC
39) Tx Bytes Discarded - Ingress CRC
40) Tx Frames Discarded - Trunk Discard
41) Tx Bytes Discarded - Trunk Discard
42) Tx Frames During Ingress LMI Fail
43) Tx Bytes During Ingress LMI Fail

Table 8-27 Frame Relay Channel Statistics in IGX

Statistic	Description
Frames Received (Ingress)	This statistic provides a count of the number of frames received from the attached equipment. This statistic is incremented even when the received frame is invalid or discarded for any reason. (See possible reasons below.)

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Receive Frames Discarded (Ingress)	This statistic provides a count of the number of frames received from the attached equipment which were discarded before being sent into the network or aborted after some portion had been already sent into the network. Possible reasons for discard are: —Invalid CRC - that is, the CRC calculated by the IGX does not match the CRC provided by the attached equipment in the last 2 octets of the frame. (Frames received with an invalid CRC are also included in the port Receive Frame CRC Errors statistic.) —Invalid Frame Length - that is, the length of the received frame, including the header and frame check sequence (FCS, or CRC) octets, is either too short (less than 5 octets) or too long (more than 4510 octets). (Frames received with an invalid frame length are also included in the port Illegal Length Receive Frames statistic.) —Invalid Alignment - that is, the length of the received frame is not an integral number of octets. (Frames received with an invalid alignment are also included in the port Receive Frame Alignment Errors statistic.) Frame received with DE = 1 and the PVC's ingress queue is filled at least to the DE threshold and the global DE feature is enabled (using the cnfsysparm command). Frames discarded for this reason are specifically counted in the PVC DE Frames Dropped statistic (below). —PVC “failed” (due to endpoint hardware failure/absence or inability to find a route through the network) or “downed” (intentionally out of service due to operator action). Frames discarded for this reason are specifically counted in the PVC Rx Frames Discarded - Deroute/Down statistic (below). —PVC ingress queue full. The queue may fill (and overflow) due to sustained transmission above the PVC's MIR or as a result of MUXBUS oversubscription. Frames discarded for this reason are specifically counted in the PVC Rx Frames Discarded - VC Q Overflow statistic (below). This statistic is a subset of the PVC Frames Received statistic.)
Frames Transmitted (Egress)	This statistic provides a count of the number of frames transmitted to the attached equipment.

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Transmit Frames Discarded	This statistic provides a count of the number of frames which were not able to be transmitted to the attached equipment. Possible reasons for discard are: Port transmit queue overflow - that is, the frame traversed the network successfully but encountered a full egress port queue. Frames discarded for this reason are specifically counted in the PVC **Tx Frames Discarded - Q Overflow** statistic (below) and the port **Tx Frames Discarded - Queue Overflow** statistic (above). Incomplete frame at egress (that is, no end-of-frame (EOF) packet received) for any reason The most common cause is a CRC error detected at ingress - that is, the beginning of the frame traversed the network successfully but the end of the frame was never sent because a CRC error was detected at the end of the frame at ingress. Frames discarded due to a missing EOF packet (because of ingress CRC error or EOF packets dropped in a trunk) are specifically counted in the PVC **Tx Frames Discarded - Ingress CRC** statistic (below). Ingress CRC errors are also counted in the ingress port **Receive Frame CRC Errors** statistic (above). Incorrect frame length, that is, the expected frame length (recorded in the end-of-frame packet) is different than the total payload of all the packets which arrive. Such a frame length error could be caused by: —one or more packets being missing due to discard(s) on a trunk, or —a transmission bit error on the frame length field in the end-of-frame packet. Frames discarded for this reason are counted in the PVC **Tx Frames Discarded - Trunk Discard** statistic (below). Invalid frame length, that is, the frame is longer than 4510 octets long. This could occur if the end-of-frame packet from one frame and the start-of-frame packet of the next frame are both missing due to discards on a trunk, resulting in a concatenated frame. Frames discarded for this reason are counted in the PVC **Tx Frames Discarded - Trunk Discard** statistic (below). Frame CRC error - that is, the calculated CRC at the destination does not match the original frame's CRC (contained within the received packets). This situation can occur as a result of transmission bit errors on payload bits on one or more packets of the frame. Frames discarded for this reason are specifically counted in the PVC **Tx Frames Discarded - Trunk Discard** statistic (below).
Packets Received	This statistic provides a count of the number of packets received across the network. These are the packets that are used to re-create all the frames which are counted in the PVC **Frames Transmitted** and **Transmit Frames Discarded** statistics (above).
Receive Packets Discarded	This statistic provides a count of the number of packets received across the network but whose payload was ultimately discarded because they contained portions of the frames which are discarded and counted in the **Transmit Frames Discarded** statistic (above).

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Packets Transmitted	This statistic provides a count of the number of packets submitted to the network. These packets are **all** the packets that were generated from the ònon-erroredó received frames (**Frames Received** minus **Receive Frames Discarded**) as well as **some** of the packets from the errored received frames (**Receive Frames Discarded**). Some packets from errored receive frames may be submitted to the network because the IGX does not wait to receive the entire frame before starting to packetize the frame and send it through the network. Consequently, if an error is detected at the end of the frame (for example, CRC error, alignment error, length error), the frame is aborted only after some packets may have been sent.
Bytes Received	This statistic provides a count of the number of octets in the frames counted in the **Frames Received** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.
Receive Bytes Discarded	This statistic provides a count of the number of octets in the frames counted in the **Receive Frames Discarded** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.
Bytes Transmitted	This statistic provides a count of the number of octets in the frames counted in the **Frames Transmitted** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.
Transmit Bytes Discarded	This statistic provides a count of the number of octets in the frames counted in the **Transmit Frames Discarded** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.
Seconds in Service	This statistic provides a count of the number of seconds during which the PVC was òin serviceó. The PVC is considered in service any time the PVC is not òfailedó (due to endpoint hardware failure/absence or inability to find a route through the network) or òdownedó (intentionally out of service due to operator action).
Frames Transmitted with FECN	This statistic provides a count of the number of frames transmitted to the attached equipment with the Forward Explicit Congestion Notification (FECN) bit set, regardless of where in the network the congestion was experienced. This statistic is a subset of the PVC **Frames Transmitted** statistic. This statistic is also a subset of the port **Frames Transmitted with FECN** statistic.
Frames Transmitted with BECN	This statistic provides a count of the number of frames transmitted to the attached equipment with the Backward Explicit Congestion Notification (BECN) bit set, regardless of where in the network the congestion was experienced. This statistic is a subset of the PVC **Frames Transmitted** statistic. This statistic is also a subset of the port **Frames Transmitted with BECN** statistic.

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Minutes Congested	This statistic provides a count of the number of minutes during which 50% or more of the frames transmitted to the attached equipment have the Forward Explicit Congestion Notification (FECN) bit set.
	The threshold (default: 50%) which defines congestion is configurable (by a SuperUser) using the **cnffstparm** command.
DE Frames Received	This statistic provides a count of the number of frames received from the attached equipment with the Discard Eligible (DE) bit already set. This statistic is a subset of the PVC **Frames Received** statistic
DE Frames Transmitted	This statistic provides a count of the number of frames transmitted to the attached equipment with the Discard Eligible (DE) bit set, regardless of why or where the DE bit was set. If IDE-to-DE mapping is enabled on the port, this statistic includes those frames which have their DE bit set by the IDE-to-DE mapping function This statistic is a subset of the PVC **Frames Transmitted** statistic.
DE Frames Dropped	This statistic provides a count of the number of frames received from the attached device which were discarded because the frame's DE bit is set and the PVC's ingress buffer has reached the DE threshold. The DE threshold is configured as part of the port configuration (**cnfport** command). This statistic is a subset of the PVC **Frames Received** statistic. This statistic is a subset of the PVC **Receive Frames Discarded** statistic. This statistic is a subset of the PVC **DE Frames Received** statistic.
DE Bytes Received	This statistic provides a count of the number of octets in the frames counted in the **DE Frames Received** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Bytes Received** statistic.
Frames Received in Excess of CIR	This statistic provides a count of the number of frames received from the attached equipment which exceed the configured Committed Information Rate (CIR) for the PVC. Whether a frame is considered òin excess of CIRó depends on whether the DE feature is enabled (using the **cnfsysparm** command). **—If the DE feature is enabled**, only frames with DE=0 are counted against Bc. Thus, this statistic only counts those frames which exceeded Bc **and** had DE=0. (If a frame is received with DE=1, only the **DE Frames Received** statistic is incremented and the frame is not counted against Bc.) **If the DE feature is not enabled**, all frames are counted against Bc. If the frame exceeds Bc, it is included in this statistic. This statistic is a subset of the PVC **Frames Received** statistic

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Bytes Received in Excess of CIR	This statistic provides a count of the number of octets in the frames counted in the **Frames Received in Excess of CIR** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Bytes Received** statistic.
Frames Transmitted in Excess of CIR	This statistic provides a count of the number of frames transmitted to the attached equipment which: —were determined at ingress to exceed the configured Committed Information Rate (CIR) for the PVC, or —were received at ingress with DE=1 and the DE feature is enabled, or —were received at ingress when the VC_Q exceeded the configured DE threshold and the DE feature is enabled. All of these conditions have in common that the packets carrying these frames all have CLP=1. It is actually the status of the CLP bits in the arriving packets that is monitored at egress. This statistic is a subset of the PVC **Frames Transmitted** statistic.
Bytes Transmitted in Excess of CIR	This statistic provides a count of the number of octets in the frames counted in the **Frames Transmitted in Excess of CIR** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Bytes Transmitted** statistic.
Rx Frames Discarded - Deroute/Down	This statistic provides a count of the number of frames received from the attached equipment which are discarded because the PVC is routed (due to endpoint hardware failure/absence or inability to find a route through the network) or downed (intentionally out of service due to operator action). This statistic is a subset of the PVC **Frames Received** statistic.
Rx Bytes Discarded—Deroute/Down	This statistic provides a count of the number of octets in the frames counted in the **Rx Frames Discarded - Deroute/Down** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Bytes Received** statistic. This statistic is also a subset of the PVC **Receive Bytes Discarded** statistic.
Rx Frames Discarded - VC Q Overflow	This statistic provides a count of the number of frames received from the attached equipment which are discarded because the PVC ingress buffer (VC Q) is full. This statistic is a subset of the PVC **Frames Received** statistic.
Rx Bytes Discarded—VC Q Overflow	This statistic provides a count of the number of octets in the frames counted in the **Rx Frames Discarded - VC Q Overflow** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Bytes Received** statistic. This statistic is also a subset of the PVC **Receive Bytes Discarded** statistic.

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Tx Frames Discarded—Q Overflow	This statistic provides a count of the number of frames which were not able to be transmitted to the attached equipment because the port's egress buffer is full. The port's egress buffer may fill (and overflow) due to oversubscription. This statistic is a subset of the PVC **Transmit Frames Discarded** statistic. This statistic is a subset of the port **Tx Frames Discarded - Q Overflow** statistic.
Tx Bytes Discarded—Q Overflow	This statistic provides a count of the number of octets in the frames counted in the **Tx Frames Discarded - Q Overflow** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Transmit Bytes Discarded** statistic. This statistic is a subset of the port **Tx Bytes Discarded - Q Overflow** statistic.
Tx Frames Discarded - Ingress CRC	This statistic provides a count of the number of frames which were not able to be transmitted to the attached equipment because the frame is incomplete. Specifically, this statistic is incremented any time an end-of-frame (EOF) packet is missing. In other words: —a start-of-frame packet is followed by another start-of-frame packet, or start-of-frame packet is followed by an encapsulated-frame packet, or —a middle-of-frame packet is followed by a start-of-frame packet, or —middle-of-frame packet is followed by an encapsulated-frame packet The most likely cause of any of these conditions is a CRC error detected at ingress causing the end of the frame (including at least the end-of-frame packet and maybe one or more middle-of-frame packets) to not be sent. A less likely cause for the missing EOF packet is that the packet was dropped due to a transmission bit error in the packet header that is detected by a trunk along the PVC's path. Such conditions are included in this statistic. This statistic is a subset of the PVC **Transmit Frames Discarded** statistic.
Tx Bytes Discarded—Ingress CRC	This statistic provides a count of the number of octets in the frames counted in the **Tx Bytes Discarded - Ingress CRC** statistic (above). The octets counted include the Frame Relay header octets as well as any octets which arrived successfully. This statistic is a subset of the PVC **Transmit Bytes Discarded** statistic.

Table 8-27 Frame Relay Channel Statistics in IGX (Continued)

Statistic	Description
Tx Frames Discarded - Trunk Discard	This statistic provides a count of the number of frames that were not able to be transmitted to the attached equipment because the frame: has an incorrect length, that is, the expected frame length (recorded in the end-of-frame packet) is different than the total payload of all the packets which arrive. Such a frame length error could be caused by: —one or more packets being missing due to discard(s) on a trunk, or —a transmission bit error on the frame length field in the end-of-frame packet. —has an invalid length, that is, the frame is longer than 4510 octets long. This could occur if the end-of-frame packet from one frame and the start-of-frame packet of the next frame are both missing due to discards on a trunk, resulting in a concatenated frame. In any of the cases above, a packet could be discarded on a network trunk either due to extreme trunk congestion or a detected transmission bit error on the packet header. This statistic is a subset of the PVC **Transmit Frames Discarded** statistic.
Tx Bytes Discarded - Trunk Discard	This statistic provides a count of the number of octets in the frames counted in the **Tx Bytes Discarded - Trunk Discard** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the PVC **Transmit Bytes Discarded** statistic.
Tx Frames During Ingress LMI Failure	This statistic provides a count of the number of frames that were transmitted to the attached equipment while the signaling protocol on the local port was failed (that is, when the port was in a Port Communication Failure state). This statistic is a subset of the PVC **Frames Transmitted** statistic
Tx Bytes During Ingress LMI Failure	This statistic provides a count of the number of octets in the frames counted in **the Tx Frames During Ingress LMI Failure** statistic (above). The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.

Table 8-28 At Ingress (before FRP firmware Release FDS/FES)

DE Feature Enabled	DE = 1	> CIR	VC_Q > DE Threshold	Action
No	Don’t care	No	Don’t care	Send
No	Don’t care	Yes	Don’t care	Set CLP=E1 in all packets
Yes	No	No	No	Send
Yes	No	No	Yes	Set CLP=E1 in all packets
Yes	No	Yes	No	Set CLP=E1 in all packets

Table 8-28 At Ingress (before FRP firmware Release FDS/FES) (Continued)

Yes	No	Yes	Yes	Set CLP=E1 in all packets Set IDE=1 in last packet
Yes	Yes	Don't care	No	Set CLP=E1 in all packets
Yes	Yes	Don't care	Yes	Discard frame

Table 8-29 At Ingress (FRP firmware Release FDS/FES and later)

DE Feature Enabled	DE=1	> CIR	VC_Q > DE Thresh	Action
No	Don't care	No	Don't care	Send
No	Don't care	Yes	Don't care	Set CLP=1 in all packets
Don't care	No	No	No	Send
Don't care	No	No	Yes	Set CLP=1 in all packets
Don't care	No	Yes	No	Set CLP=1 in all packets
Don't care	No	Yes	Yes	Set CLP=1 in all packets Set IDE=1 in last packet
Yes	Yes	Don't care	No	Set CLP=1 in all packets
Yes	Yes	Don't care	Yes	Discard frame

Table 8-30 At Ingress (FRP firmware Release FDV/FEV and later)

DE Feature Enabled	DE=1	> CIR	Action
No	Don't care	No	Send
No	Don't care	Yes	Set CLP=1 in all packets
Don't care	No	No	Send
Don't care	No	Yes	Set CLP=1 in all packets Set IDE=1 in last packet
Yes	Yes	Don't care	Set CLP=1 in all packets

AT EGRESS (DE bit setting)

IDE = 1	IDE = 1	IDE to DE Mapping Enabled	Action
Yes	Don't care	Don't care	DE=1 (No change to DE bit) --> Tx_Q
No	No	Don't care	DE=1 (No change to DE bit) --> Tx_Q
No	Yes	No	DE=1 (No change to DE bit) --> Tx_Q
No	Yes	Yes	DE=1 (Change DE bit) --> Tx_Q

Table 8-31 At Egress (Transmit queue behavior)

DE Feature Enabled	DE=1	Tx_Q > DE Threshold	Action
No	Don't care	Don't care	If space available, put frame into Tx_Q
Yes	No	Don't care	If space available, put frame into Tx_Q
Yes	Yes	No	If space available, put frame into Tx_Q
Yes	Yes	Yes	Discard frame

Full Name

Display Frame Relay channel statistics

Syntax

dspchstats <channel> [interval]

Related Commands

clrchstats, cnfchstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspchstats 5.1.100`

Description

Display the channel statistics for connection 5.1.100.

System Response

```
pubsigx1       TN    SuperUser       IGX 8420    9.2    Aug. 7 1998 04:04 PDT

Channel Statistics: 5.1.100       Cleared: July 25 1997 06:07
MIR: 9.6 kbps          Collection Time: 12 day(s) 21:48:41     Corrupted: YES
                     Frames   Avg Size Avg    Util          Packets     Avg
                              (bytes) (fps) (%)                        (pps)
From Port:                0          0      0    0
To Network:               0          0      0    0           58732         0
Discarded:                0          0      0    0
From Network:             1          5      0    0               1         0
To Port:                  0          0      0    0
Discarded:                1          5      0    0               1         0
                   ECN Stats:  Avg Rx VC Q:            0    ForeSight RTD    --
Min-Pk bytes rcvd:          0  FECN Frames:            0    FECN Ratio (%)    0
Minutes Congested:          0  BECN Frames:            0    BECN Ratio (%)    0
Frames rcvd in excess of CIR:       0  Bytes rcvd in excess of CIR:         0
Frames xmtd in excess of CIR:       0  Bytes xmtd in excess of CIR:         0

This Command: dspchstats 5.1.100


Hit DEL key to quit:
```

Table 8-32 dspchstats–Parameters

Parameter	Description
channel	Specifies the channel. The command displays connection information for one channel at a time, so you cannot specify a range of channels. The format for channel is *slot.port*.

Table 8-33 dspchstats—Optional Parameters

Parameter	Description
interval	Specifies the refresh interval for displaying data. The range is 1–60 seconds. The default is 10 seconds. If you do not specify a value for the refresh interval, the screen refresh defaults to 10. If the Rx Q depth and the Tx Q depth fields remain “0”, make sure that a value other than “0” is specified for the *interval* parameter.

dspcon

Displays connection information for a channel. The information displayed includes:

- The channel number at both the local and remote ends of the connection
- The node name at both ends of the connection
- The type or data rate of the connection
- The routing restriction
- The class of service (COS) of the connection
- The connection route, which lists the end nodes and any intermediate nodes
- The preferred route for the connection (if configured)
- If cost-based AutoRoute is configured, displays maximum and current costs for a connection route.
- The status of the cards associated with the connection
- Any Y-cable conflicts (LDI, CDP for example)
- The compression status (VAD on or off, ADPCM on or off, DFM on or off, Frame Relay compression on or off)
- The connection bandwidth parameter values for Frame Relay
- The circuit round trip delay (RTD) if ForeSight is enabled

A failure that affects the connection flashes on the screen. For Frame Relay NNI ports, the NNI value indicates the Abit value was received over the NNI from the remote network. The possible status messages are:

• OK	Connection OK.
• FAILED	Connection failed.
• MISSING	DLCI was deleted in other network at NNI. A previous status report indicated a valid DLCI was present but an updated report did not.
• UNUSED	Indicates the UNI port does not support reporting of NNI Abit status.

Full Name

Display connections

Syntax

dspcon <slot.port.DLCI>

Related Commands

addcon, cnfcos, cnfpref, cnfrtcost, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspcon 19.1.101

Description

Display connection information for Frame Relay channel 19.1.101 (cost based routing is configured).

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:42 MST

Conn:  19.1.101   gamma       8.2.300     fr
   MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR    FST
 9.6/9.6   9.6/9.6  65535/65535   256/256    10/10  65535/65535  9.6/9.6   n
% Util: 100/100
Owner: LOCAL      Restriction: NONE COS: 0                     Status: OK
TestRTD: 0 msec   Trunk Cell Routing Restrict: Y   Max Cost: 100 Route Cost: 36

Path:     beta    15--15gamma
Pref:     Not Configured


beta 19.1.101                                    gamma 8.2.300
FRP:   OK                                        FRP:   OK
FRI:   OK                                        FRI:   OK


Last Command: dspcon 19.1.101


Next Command:
```

Table 8-34 dspcon–Parameters

Parameter	Description
channel	Specifies the channel in the format *slot.port.DLCI*. The **dspcon** command displays information for one connection at a time.

dspcons

Displays information about the connections on an IGX node. The following table lists all possible information headings that appear in the display. The actual headings that appear depend on the choice of selected optional parameters—including no parameters. Entering the command with no parameters displays all connections. The screen examples in this description reflect various parameter options, including no parameters.

Viewing Results from OAM Loopback Test

The OAM Loopback Test (configured with **cnfoamlpbk** command) will consider a PVC to be failed if ten consecutive loopback cells do not return. When a failure occurs, this information will be stored in switch software. The test will continue to run even when connections are in a failed state. You can view the results of the test by using the **dspcons -oam** command.

You can view a display of connections that have failed the OAM Loopback Test by using the **dspcons** command. The **dspcons** command with no optional parameters will show all connections, and those that have failed the OAM Loopback Test *but are otherwise OK* will show a state of “OAM”. Other states will supersede OAM. You can use the **dspcons -oam** command to view all connections that have failed the OAM Loopback Test. When an OAM Loopback failure occurs, the state field shows “OAM-F”.

Table 8-35 dspcons Output

Fields	Description	
Local Channel	The connection’s channel at this node.	
Remote Node Name	The name of the node at the other end of the connection.	
Remote Channel	The connection’s channel at the remote node.	
State	The possible connections states are as follows:	
	State	**Description**
	OK	routed, Abit = 1.
	Down	downed.
	Failed	unrouted, but trying; Abit = 0.
	Unused	The UNI port does not support reporting of NNI Abit status.
	OAM	Connections that have failed OAM Loopback test, but are otherwise OK.
	OAM-F	Indicates OAM Loopback failure
Type	The type of connection. For example, this can be Frame Relay, Frame Relay with interworking, voice, data, and so on.	
Only __	If one parameter pre-empts another, this heading appears with the accepted parameter type. To name two examples: if the parameter is –d for data or –fail for failed connections only, this heading becomes either “Only d” or Only fail,” respectively.	
Code	The encoding used for data connections (7/8 = data byte is 7 bits of user data plus a “1” in the last bit position, 8/8 = data byte is 8 bits of user data, 8/8I = data byte is 8 bits of inverted user data).	
Route Avoid	The type of lines to avoid when routing (satellite lines, terrestrial lines, lines with zero code suppression).	

Table 8-35 dspcons Output (Continued)

Fields	Description
Compression	The type of compression applied to the connection (PCM, PCM and VAD, ADPCM, VAD and ADPCM for voice connections), (DFM for data connections).
COS	The Class Of Service.
Abit	Abit status at both ends of the connection.
Loopback	This is not a heading but rather the standard loopback symbols indicating the presence of a test loop. See the “Troubleshooting” chapter for an explanation of these symbols.

Full Name

Display connections

Syntax

dspcons [*start_channel*] [*nodename*] [–f] [–v] [–d] [–atfr] [–abit] [–fabit] [–fail] [–down]

where

start_channel	is the starting channel to display
nodename	specifies that connections for only the named node appear in the display
–f	equals display Frame Relay connection only
–v	equals display only voice connections
–d	equals display only data connections and do so in Kbps.
–atfr	equals Frame Relay to ATM interworking connections (also displays atfr with ForeSight)
–abit	equals show status of the Abit
–fabit	equals show only connections with failed A-bits
–fail	equals show only failed connections
–down	equals show only downed connections

Note Some parameters may supersede other parameters.

Related Commands

addcon, cnfchadv, chfchdfm

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspcons

Description

Displays all connections

System Response

```
sw83          VT    SuperUser       IGX 8430    9.2       Aug. 14 1998 12:58 PST

 From           Remote      Remote
 3.1.27         NodeName    Channel         State  Type      Compress  Code COS
 3.1.27         sw86        13.1.1.27       Ok     atfst                     0
 3.1.28         sw86        13.1.1.28       Ok     atfst                     0
 3.1.29         sw86        13.1.1.29       Ok     atfst                     0
 3.1.30         sw86        13.1.1.30       Ok     atfst                     0
 3.1.31         sw86        13.1.1.31       Ok     atfst                     0
 3.1.32         sw86        13.1.1.32       Ok     atfst                     0
 3.1.33         sw86        13.1.1.33       Ok     atfst                     0
 3.1.34         sw86        13.1.1.34       Ok     atfst                     0
 3.1.35         sw86        13.1.1.35       Ok     atfst                     0
 3.1.36         sw86        13.1.1.36       Ok     atfst                     0
 3.1.37         sw86        13.1.1.37       Ok     atfst                     0
 3.1.38         sw86        13.1.1.38       Ok     atfst                     0
 3.1.39         sw86        13.1.1.39       Ok     atfst                     0

This Command: dspcons


Continue?
```

Example 2

dspcons 19.1

Description

Display connections starting with 19.1. This example shows frame and data connections.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:37 MST

 Local      Remote      Remote                                          Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 19.1.101   gamma       8.2.300    Ok     fr                                0  L
 19.2.302   alpha       9.2.400    Ok     fr                                0  R
 25.1       alpha       5.1        Ok     256                  7/8          0  L
 25.2       gamma       6.1        Ok     256                  7/8          0  L











Last Command: dspcons 19.1


Next Command:
```

Example 3

dspcons -f

Description

Display Frame Relay connections only.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:38 MST

 Local      Remote      Remote            Only                              Route
 Channel    NodeName    Channel    State  f       Compression  Code Avoid COS O
 19.1.101   gamma       8.2.300    Ok     fr                                0  L
 19.2.302   alpha       9.2.400    Ok     fr                                0  R



Last Command: dspcons -f


Next Command:
```

Example 4

dspcons -abit

Description

Display connections and show the status of the Abit on the local and remote nodes.

System Response

```
sw83          VT    SuperUser       IGX 8410    9.2      Aug. 14 1998 13:02 PST

 Local          Remote      Remote                     Local     Remote
 Channel        NodeName    Channel         State       Abit     Abit
 3.1.1          sw86        13.1.1.1        Ok         OK        OK
 3.1.2          sw86        13.1.1.2        Ok         OK        OK
 3.1.3          sw86        13.1.1.3        Ok         OK        OK
 3.1.4          sw86        13.1.1.4        Ok         OK        OK
 3.1.5          sw86        13.1.1.5        Ok         OK        OK
 3.1.6          sw86        13.1.1.6        Ok         OK        OK
 3.1.7          sw86        13.1.1.7        Ok         OK        OK
 3.1.8          sw86        13.1.1.8        Ok         OK        OK
 3.1.9          sw86        13.1.1.9        Ok         OK        OK
 3.1.10         sw86        13.1.1.10       Ok         OK        OK
 3.1.11         sw86        13.1.1.11       Ok         OK        OK
 3.1.12         sw86        13.1.1.12       Ok         OK        OK
 3.1.13         sw86        13.1.1.13       Ok         OK        OK

This Command: dspcons -abit


Continue?
```

Example 5

dspcons

Description

Display connections

System Response

```
sw99       TN        StrataCom     BPX 8620   9.2.10         Aug. 27 1998 08:59 GMT

Local        Remote        Remote                                   Route
Channel      NodeName      Channel       State  Type                Avoid     COS  O
-------     --------     -------        -----  ----                -----     ---  --
3.2.6.16      sw14       10.1.6.16      Ok     vbr                            0    L
3.2.6.17      sw14       10.1.6.17      Ok     vbr                            0    L
3.2.6.18      sw14       10.1.6.18      Ok     vbr                            0    L
3.2.6.19      sw14       10.1.6.19      Ok     vbr                            0    L
3.2.6.20      sw14       10.1.6.20      Ok     vbr                            0    L
3.2.6.21      sw14       10.1.6.21      Ok     vbr                            0    L
3.2.6.22      sw14       10.1.6.22      Ok     vbr                            0    L
3.2.6.16      sw157      16.1.6         Failed atfr                           0    L
3.2.6.17      sw157      16.1.7         Failed atfr                           0    L
3.2.8.18      sw157      16.1.8         OAM-F  atfr                           0    L
3.2.8.19      sw157      16.1.9         OAM-F  atfr                           0    L


Last Command: dspcons
```

Example 6

dspcons -oam

Description

Display connections that have failed the OAM Loopback test

System Response

```
sw99        TNStrataComBPX 159.2.10        Aug. 27 1998 08:59 GMT

Local          Remote        Remote                           Route
Channel        NodeName      Channel        State    Type       Avoid      COS   O
-------       --------     -------        -----    ----        -----     ---   --
3.2.6.16      sw157        16.1.6         OAM-F   atfr                   0     L
3.2.6.17      sw157        16.1.7         OAM-F   atfr                   0     L
3.2.8.18      sw157        16.1.8         OAM-F   atfr                   0     L
3.2.8.19      sw157        16.1.9         OAM-F   atfr                   0     L


Last Command: dspcons -oam

Next Command:
```

Table 8-36 dspcons—Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. Specify *start channel* in one of the following formats: *slot.port.DLCI* (Frame Relay channel) *remote node.group_name*(Frame Relay group connection) If you do not specify a starting channel, the display begins at the first connection.
node name	Specifies that only connections to this remote node from the local note be displayed. If no *nodename* is designated, connections from the local node to all other nodes are displayed.

Table 8-36 dspcons—Optional Parameters (Continued)

Parameter	Description
(connection types)	Specifies that only connections of a certain type be displayed. If you do not add at least one argument to specify a particular connection type, all connections appear. When you enter the connection type on the command line, precede it with a hyphen (-). In some cases, you can add more than one connection type (with a space between), but not all compound arguments are compatible, so you may not always see the expected combination of types. The connection types are: -v displays only voice connections. -d displays only data connections. -f displays only Frame Relay connections. -abit shows Abit (nni) status. -fabit shows connections with failed Abit (nni) status. -fail shows only failed connections. -siw shows service interworking connections. -atfr shows only network interworking connections.

dspfrcls

Displays the configuration of a Frame Relay class. Network-wide classes are available to provide a shortcut for adding Frame Relay connections. Refer to the section titled "Using Frame Relay Classes" at the beginning of this chapter for a definition of a Frame Relay class.

The */* in the PIR (Peak Information Rate) column means that if a connection is added using this Frame Relay class, the PIR for this connection will be equal to that of the port speed on which the connection was added. For example, if the port speed for port 6.1 = 64 kbps, and if a connection 6.1.100 is adding using the Frame Relay class, it will have a value of 64 kbps for the PIR parameter.

Full Name

Display Frame Relay classes

Syntax

dspfrcls

Related Commands

addcon, cnffrcls

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX	No

Example 1

`dspfrcls`

Description

Display the Frame Relay class configurations.

The screen display is the same as that for the **cnffrcls** command.

System Response

```
sw83           TN    SuperUser       IGX 8420    9.2      Aug. 23 1998 13:43 GMT

                        Frame Relay Connection Classes

 #    MIR       CIR     VC Q Depth       PIR      Cmax     ECN QThresh
 1 9.6/9.6   9.6/9.6 65535/65535       */*      10/10    65535/65535
   QIR:  9.6/9.6  FST: n % Util: 100/100 Description: "Default 9.6"
 2 19.2/19.2 19.2/19.2 65535/65535       */*      10/10    65535/65535
   QIR: 19.2/19.2 FST: n % Util: 100/100 Description: "Default 19.2"
 3   16/16     16/16   65535/65535       */*      10/10    65535/65535
   QIR:   16/16   FST: n % Util: 100/100 Description: "Default 16"
 4   32/32     32/32   65535/65535       */*      10/10    65535/65535
   QIR:   32/32   FST: n % Util: 100/100 Description: "Default 32"
 5   56/56     56/56   65535/65535       */*      10/10    65535/65535
   QIR:   56/56   FST: n % Util: 100/100 Description: "Default 56"



This Command: dspfrcls


Continue?
```

dspfrport

Displays information on Frame Relay cards and physical and logical ports. The applicable card sets are the FRP, FRM, and UFM. The content of the information display depends on the arguments you include with the command. The information can be:

- The status of all Frame Relay ports in a node
- General information on all ports on a selected FRP, FRM, or UFM card
- Configuration information on a single Frame Relay port.

The following are examples of the **dspfrport** command syntax:

dspfrport	Display the states of all Frame Relay ports in the node.
dspfrport 8	Display the port states for FRP in slot 8.
dspfrport 8.1	Display the configuration for port 1 of the FRP in slot 8.
dspfrport 6.44	Display the configuration for logical port 44 of the FRP-2 in slot 6.

The following is a list of possible displayed port parameters for a single port. For a more detailed description of these parameters, refer to the **cnffrport** command.

Table 8-37 Frame Relay Port Parameters

Parameters	Parameters
Port number	Polling Verification Timer
DLCI number	Error Threshold
State: Active or inactive	Monitored Events Count
Interface Type: V.35 or X.21, DCE or DTE	Priority Communicated
Configured clock speed in Kbps	The lead states in the Interface Control Template
Measured clock speed in Kbps	Receiver Not Ready Thresholds
The port VC queue depth in bytes	Flags per frame
The VC queue ECN threshold in bytes	OAM FastPacket Threshold (for NNI ports)
The DE threshold	Link Integrity Timer (for NNI ports FRP rev. F/H or above)
The Signaling Protocol	Full Status Polling cycle (for NNI ports)
Asynchronous Status	

Full Name

Display Frame Relay port

Syntax

dspfrport [slot | slot.port]

Related Commands

cnffrport, upfrport, dnfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX	No

Example 1

dspfrport

Description

Display the port status of the Frame Relay ports in the node.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 15 1997 15:48 PST

FRP Port States
Port  ID   State
9.1   0    ACTIVE
9.2   0    ACTIVE
9.3   0    INACTIVE
9.4   0    INACTIVE









Last Command: dspfrport


Next Command:
```

Example 2

dspfrport 5

Description

Display the status of the ports on the FRP in slot 5.

System Response

```
pubsipx1       TN    SuperUser       IGX 8420    9.2    Sep. 7 1997  02:11 PDT

Port configuration for FRP 5

Port   ID       Speed     Interface          State       Protocol     Port Type
1      0        256       FRI-V35 (DCE)      ACTIVE      None         FR
2      0        256       FRI-V35 (DCE)      INACTIVE    None         FR
3      0        256       FRI-V35 (DCE)      INACTIVE    None         FR
4      0        256       FRI-V35 (DCE)      INACTIVE    None         FR









Last Command: dspfrport 5


Next Command:
```

Example 3

dspfrport 5.1

Description

Display port status for logical Frame Relay port 5.1. In the example, note the range of channels.

System Response

```
sw109          VT    SuperUser       IGX 16    9.2 Aug. 21 1997 18:14 GMT

Port:       5.1               [ACTIVE  ]
Interface:  E1B                              Configured Clock:   960 Kbps
Clocking:   None                             Measured Rx Clock: None

Port ID                        -       Min Flags / Frames           1
Port Queue Depth           32000       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer        10 sec
DE Threshold                 100 %     N391 Full Status Poll        6 cyl
Signalling Protocol         None       EFCI Mapping Enabled        No
Asynchronous Status           No       CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Channel Speed               64
N393 Monitored Events Count    4       Line Number                  1
Communicate Priority          No       Channel Range             1-15
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dspfrport 5.1


Next Command:
```

Example 4

dspfrport 5

Description

Display port status for all the Port Concentrator ports at slot 5.

System Response

```
tecate         LAN   SuperUser       IGX 8420    9.2     Aug. 6 1997 09:59 PST

Port configuration for FRP 5

Port   ID       Speed     Interface          State       Protocol
1      0        64        V.35    (DCE)      ACTIVE      None
2      0        64        V.35    (DCE)      ACTIVE      None
3      0        38.4      V.11    (DTE)      ACTIVE      None
4      0        38.4      V.11    (DCE)      ACTIVE      None
5      0        38.4      V.11    (DCE)      ACTIVE      None
6      0        38.4      V.11    (DTE)      ACTIVE      None
7      0        19.2      V.11    (DCE)      ACTIVE      None
8      0        19.2      V.28    (DCE)      ACTIVE      None
9      0        19.2      V.28    (DTE)      ACTIVE      None
10     0        38.4      V.28    (DCE)      INACTIVE    None
11     0        38.4      V.28    (DCE)      INACTIVE    None
12     0        38.4      V.28    (DCE)      INACTIVE    None

Last Command: dspfrport 5


Continue?
```

Example 5

dspfrport 6.44

Description

Display port configuration for Frame Relay port 6.44 (a Port Concentrator port).

System Response

```
singha         TN    SuperUser       IPX 32    9.2       July 7 1997 13:38 GMT

Port:       6.44               [FAILED]
Interface:  V.11    DCE                        Configured Clock:  38.4 Kbps
Clocking:   Normal                             Startup Rx Clock:     0 Kbps
                                       Min Flags / Frames           1
Port ID                        0
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer        10 sec
DE Threshold                 100 %     N391 Full Status Poll        6 cyl
Signalling Protocol         None       EFCI Mapping Enabled        No
Asynchronous Status           No       CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead      I
Communicate Priority          No          State   ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dspfrport 6.44


Next Command:
```

dspfrcport

Displays physical port configuration for FRM-2 or FRP-2 ports connected to a Port Concentrator. The following is a list of possible displayed parameters for a port.

Note The screen displayed with this command includes fields for standard Frame Relay ports on the FRM card. Only the fields in the following table have meaning for a Port Concentrator.

Table 8-38 dspfrcport—Displayed PCS Parameters

Field	Meaning
Interface	Always *FRI-X.21 DCE* for PCS ports.
Clocking	Always *Normal* for PCS ports.
Port Type	Specifies port type, always FR (Frame Relay) for PCS ports.
Port ID	Specifies the DLCI for the port, always 1022 for PCS ports.
Port Queue Depth	Specifies the maximum bytes queued for transmission from the FRM-2 or FRP-2 port. The range is 0–65535; 65535 is the default.
DE Threshold	Specifies the port depth queue above which frames with the Discard Eligibility bit set will be discarded. Valid entries are 0–100%, with a default of 100%. 100% effectively disables DE for the port.
Signaling Protocol	For Frame Relay ports, specifies LMI operation mode. For PCS ports, this is set to *None*.
Measured Rx Clock	The actual speed of received data as clocked by the FRM-2 or FRP-2. Under normal operation, this should always display the fixed concentrated link speed of 512 Kbps. Clock speed is measured by the FRM-2 or FRP-2 once per minute.
Concentrated Link Util	Current utilization percentage of the concentrated link. Utilization is defined as the percentage of the fixed link speed (512K) used for data. Since the maximum allowable aggregate for each link's 11 ports is 448 Kbps, 88% is the maximum value for this field.
Min Flags / Frames	Specifies the minimum number of flags per frame. All values greater than zero are valid; the default is 1.
OAM Pkt Threshold	Specifies the OAM FastPackets used within the local node to transmit the NNI status from the remote network. The range of values is 0–15 packets. The default is 3. A 0 disables this function.

Full Name

Display FRC-2/FRM-2 port configuration

Syntax

dspfrcport <slot.port> <interval>

Related Commands

dspfrcport, dspbob

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX, IGX	No

Example 1

dspfrcport 3.1

Description

Display the configuration of port 3.1.

System Response

```
tecate         LAN   SuperUser       IGX 8420   9.2     Aug. 6 1998 10:25 PST
Physical Port:       3.1           [ACTIVE]
Interface:  FRI-X.21 DCE                       Configured Clock:   512 Kbps
Clocking:   Normal                           Measured Rx Clock:  512 Kbps
Port Type                     FR       Min Flags / Frames           1
Port ID                     1022
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer         6 sec
DE Threshold                 100 %     N391 Full Status Poll       10 cyl
Signalling Protocol         None       ForeSight (CLLM)            No
Asynchronous Status           No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead I
Communicate Priority          No          State   ON
Upper/Lower RNR Thresh  75%/ 25% Concentrated Link Util 88%


Last Command: dspfrcport 3.1


Next Command:
```

Table 8-39 dspfrport–Parameters

Parameter	Description
slot.port	Specifies the physical slot and port of the Frame Relay card set. The range is 1–4.
interval	Specifies the screen update interval in seconds. The default is five seconds

dspict

Displays interface control template information for data channels and Frame Relay ports. The information includes:

The specified channel.
The type of template: a, c, l, n, or f.
The associated output leads and their status:

ON.
OFF.
Following a local input.
Following a remote input.

For Frame Relay ports, the entire port configuration screen is displayed (see **dspfrport** command). The input being followed is specified, when applicable. Any RTS to CTS delay is also shown.

Full Name

Display interface control template

Syntax

dspict <port> <template>

Related Commands

cnfict, cpyict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX, IGX	No

Example 1

```
dspict 25.1 a
```

Description

Display the active interface control template for channel 25.1.

System Response

```
beta           TRM   YourID:1        IPX 32    9.2    Aug. 15 1997 17:33 MST

Data Channel:      25.1
Interface:         RS232   DCE
Clocking:          Normal

            Interface Control Template for Connection while ACTIVE

 Lead    Output Value                    Lead    Output Value
 RI      OFF                             DSR     ON
 CTS     ON                              SRxD    ON
 DCR     OFF                             DCD     ON
 SCTS    ON                              SDCD    ON
 SQ      ON



Last Command: dspict 25.1 a


Next Command:
```

Example 2

dspict 9.1 a

Description

Display the Frame Relay data channel 9.1 interface control template.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1997 10:26 PST

Port:       9.1               [ACTIVE  ]
Interface:  FRI-V35 DTE                        Configured Clock:   256 Kbps
Clocking:   Normal                             Measured Rx Clock:    0 Kbps
Port ID                         7
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer         6 sec
DE Threshold                 100 %     N391 Full Status Poll       10 cyl
Signalling Protocol         None       ForeSight (CLLM)           No
Asynchronous Status           No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer      15       Interface Control Template
N392 Error Threshold           3          Lead       State
N393 Monitored Events Count    4           RTS        ON
Communicate Priority          No           DTR        ON
Upper/Lower RNR Thresh  75%/ 25%
Min Flags / Frames             1

Last Command: dspict 9.1 a


Next Command:
```

Table 8-40 dspict—Parameters

Parameter	Description
port	Specifies the physical slot and port of the Frame Relay card set.
template	Specifies the template. Choices are a, c, n, l, and f.

dspmode

Displays the *mode* of the card. The mode applies only to a UFM-U back card. The UFM-U back cards are the UFI-12V.35, UFI-12X.21, and UFI-4HSSI. A card mode is a combination of maximum port speeds and for specific port numbers. Table 8-40 lists the maximum port speeds and active ports for each mode. For a description of the UFM-U modes, see the UFM-U description in the *Cisco IGX 8400 Series Reference*.

Table 8-41 Card Modes for Unchannelized Back Cards

	V.35 and X.21 Ports												HSSI Ports			
	Group A				Group B				Group C							
Mode	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
1	3	3	3	3	3	3	3	3	3	3	3	3	8	8	8	8
2	8	-	8	-	8	-	8	-	8	-	8	-	16	-	16	-
3	10	-	-	-	10	-	-	-	10	-	-	-	16	-	-	-
4	8	-	8	-	3	3	3	3	3	3	3	3				
5	10	-	-	-	3	3	3	3	3	3	3	3				
6	8	-	8	-	8	-	8	-	3	3	3	3				
7	10	-	-	-	8	-	8	-	3	3	3	3				
8	10	-	-	-	10	-	-	-	3	3	3	3				
9	10	-	-	-	8	-	8	-	8	-	8	-				
10	10	-	-	-	10	-	-	-	8	-	8	-				
11	3	3	3	3	8	-	8	-	3	3	3	3				
12	3	3	3	3	3	3	3	3	8	-	8	-				
13	3	3	3	3	10	-	-	-	3	3	3	3				
14	3	3	3	3	3	3	3	3	10	-	-	-				
15	8	-	8	-	3	3	3	3	8	-	8	-				
16	3	3	3	3	8	-	8	-	8	-	8	-				
17	8	-	8	-	10	-	-	-	3	3	3	3				
18	8	-	8	-	3	3	3	3	10	-	-	-				
19	3	3	3	3	8	-	8	-	10	-	-	-				
20	3	3	3	3	10	-	-	-	8	-	8	-				
21	10	-	-	-	3	3	3	3	8	-	8	-				
22	10	-	-	-	3	3	3	3	10	-	-	-				
23	3	3	3	3	10	-	-	-	10	-	-	-				
24	8	-	8	-	10	-	-	-	8	-	8	-				
25	8	-	8	-	8	-	8	-	10	-	-	-				
26	10	-	-	-	8	-	8	-	10	-	-	-				
27	8	-	8	-	10	-	-	-	10	-	-	-				

Full Name

Display mode

Syntax

dspmode <slot>

Related Commands

cnffrport, cnfmode, dspmodes

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX	Yes

Example 1

`dspmode 13`

Description

Display the mode of the UFM-U in slot 13.

System Response

```
sw180          TN    SuperUser       IGX 16    9.2 July 30 1997 01:39 GMT

                         UFMU Card Mode Configuration

Slot Number   Configured Mode     Available Ports    Currently Activated Ports

    13               1            [111111111111]        [100000000000]






Last Command: dspmode 13

Next Command:
```

Table 8-42 dspmode–Parameters

Parameter	Description
slot	Specifies the slot of the UFM-U card.

dspmodes

Displays the ports that are active with each *mode* of an unchannelized UFM. The mode applies only to a UFM-U back card. The UFM-U back cards are the UFI-12V.35, UFI-12X.21, and UFI-4HSSI. A card mode is a combination of maximum port speeds and specific port numbers. Refer to the description of **dspmode** for the table that lists the maximum port speeds and active ports for each mode. For a description of the UFM-U modes, see the UFM-U description in the *Cisco IGX 8400 Series Reference*.

The **dspmode**s command takes no parameters. Also, note that only the first three modes apply to a UFI-4HSSI.

Full Name

Display mode

Syntax

dspmode

Related Commands

cnffrport, cnfmode, dspmode

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IPX, IGX	Yes

Example 1

`dspmodes`

Description

Display the possible modes.

System Response

```
sw180          TN    SuperUser       IGX 16    9.2 July 30 1997 01:39 GMT

                         UFMU Card Mode Configuration

Slot Number   Configured Mode     Available Ports    Currently Activated Ports

    13               1            [111111111111]        [100000000000]







Last Command: dspmode 13


Next Command:
```

dsppcs

Displays status and level information for either a specific Port Concentrator Shelf or all Port Concentrators attached to the node. When the command has a specific slot number for an argument, information appears for each concentrated link. The information for each concentrated link is as follows (see also Example 1):

Status, where "OK" means the FRM-2 or FRP-2 is communicating with the PCS, and "Failed" means the FRM-2 or FRP-2 is not communicating with the PCS on the concentrated link.

- Status, where "OK" means the FRM-2 or FRP-2 is communicating with the PCS, and "Failed" means the FRM-2 or FRP-2 is not communicating with the PCS on the concentrated link.
  - No Test means no test (**tstpcs** command) has occurred since last reset.
  - Passed means the last PCS test (**tstpcs** command) detected no errors in the PCS hardware.
  - Failed means the last PCS test (**tstpcs** command) detected errors in the PCS hardware.
  - Testing means a test (**tstpcs** command) is in progress.
- FW Revision is the firmware revision of the PCS module.
- Boot PROM Date is the boot firmware date of PCS module.
- Boot PROM Revision is the boot firmware revision of PCS module.

When the command executes without a specified slot, a general status statement and the firmware revision for each port appear (see Example 2).

Full Name

Display Port Concentrator Shelf

Syntax

dspport [slot]

Related Commands

cnffrport, dspfrcport, dspfrcbob, dspportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	No	No	IPX, IGX	No

Example 1

```
dsppcs 6
```

Description

Display PCS information for port 6.

System Response

```
singha         TN    SuperUser       IPX 32    9.2       July 7 1997 14:04 GMT

Detailed Port Concentrator Display For FRP in slot 6

Link Number:         1                 Link Number:         3
Status:              Failed            Status:              OK
Test Status:         No Test           Test Status:         Passed
FW Revision:                           FW Revision:         P3
Boot PROM Date:                        Boot PROM Date:      11/9/95
Boot PROM Revision:                    Boot PROM Revision:  P3

Link Number:         2                 Link Number:         4
Status:              Failed            Status:              OK
Test Status:         No Test           Test Status:         Passed
FW Revision:                           FW Revision:         P3
Boot PROM Date:                        Boot PROM Date:      11/9/95
Boot PROM Revision:                    Boot PROM Revision:  P3


Last Command: dsppcs 6

 Next Command:
```

Example 2

dsppcs

Description

Display information for all Port Concentrator Shelves.

System Response

```
singha         TN    SuperUser       IPX 32    9.2    July 7 1997 14:02 GMT

Port Concentrator Status

Slot.Port    Status        FW Revision
6.1          Failed
6.2          Failed
6.3          OK            P3
6.4          OK            P3



Last Command: dsppcs


Next Command:
```

Table 8-43 dsppcs—Optional Parameters

Parameter	Description
slot	Specifies slot associated with the ports you want to display.

dspportids

Displays *port IDs*. The port ID is a user-specified identifier for a particular Frame Relay port where several virtual circuits share the same physical interface. The port ID can be any numeric value in the range 1–1024. The command for specifying a port ID is **cnffrport**. Note that a Port Concentrator does not use port IDs.

Full Name

Display port IDs

Syntax

dspport IDs

Related Commands

cnffrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX, IGX	No

Example 1

```
dspportids
```

Description

Display the port IDs throughout the network.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 15 1997 15:55 PST

Frame Relay Port IDs
ID   Node
7    alpha    |
9    alpha    |










Last Command: dspportids


Next Command:
```

dspportstats

Displays a summary of port statistics for a Frame Relay port. Statistics include the data byte count in the transmit and receive directions and error counts associated with the port. The display indicates the date and time the statistics were cleared and the amount of time since the node last cleared the statistics. *Bytes transmitted* indicates the amount of data transmitted from the port to the user device. *Bytes received* indicates the amount of data received at the port from the user device.

Corrupted statistics result from channel/port loopbacks or port tests. A "yes" in this field indicates that loopback or port tests have occurred since the statistics were last cleared. The statistics for User-to-Network Interface (UNI) ports (connections to user devices) are displayed with one screen. The following lists usage statistics displayed in screen 1.

The **dspportstats** command also displays the following statistics: IMA port summary statistics. A summary and description of these statistics follows:

Table 8-44 IMA Port Statistics

Statistics	Description
IMA Unavailable Seconds	
IMA Near end Failed counts	
Last IMA protocol failure code	

Table 8-45 UNI Port Statistics for Frame Relay

Frame Errors	LMI Statistics	Miscellaneous Statistics
Invalid CRC	Status Enquiries Received	Average TX Port Q
Invalid Alignment	Status Transmitted	FECN Frames
Invalid Frame Length	Update Transmit	FECN Ratio (%)
Invalid Frame Format	Invalid Requests	BECN Frames
Unknown DLCIs	Sequence # Mismatches	BECN Ratio (%)
Last Unknown DLCI	Timeouts	Resource Overflow
	Signaling Protocol	DE Frames Dropped (Egress)

Network to Network (NNI) ports require two screens to display all the parameters. The first screen is the same as described previously for UNI ports—you display the second screen by responding with a "y" for yes to the Continue? prompt. The second screen compares receive LMI statistics with transmit LMI statistics. The LMI receive statistics are repeated from the middle column of the first screen and displayed again so you can compare them. The following lists the usage statistics in screen 2.

Table 8-46 LMI Statistics for Frame Relay

LMI Receive Protocol Stats	LMI Transmit Protocol Statistics
Status Enquiries Received	Status Inquiries Transmitted
Status Enquiries Transmitted	Status Received
Asynchronous Status Transmitted	Asynchronous Status Received

Table 8-46 LMI Statistics for Frame Relay (Continued)

LMI Receive Protocol Stats	LMI Transmit Protocol Statistics
Sequence # Mismatches	Sequence # Mismatches
Timeouts	Timeouts
Invalid Frames	
Signaling Protocol	

The command displays the following statistics: frame error, LMI, and miscellaneous. A summary and description of these statistics follows:

Table 8-47 Frame Error Statistics

Statistics	Description
CRC Errors	Based on a CRC CCITT 16-bit frame check sequence, which is a cyclic redundancy check. If the frame received at a port has an incorrect CRC, it is flagged as a CRC error, and the frame is discarded. **Receive Frame CRC Errors (Ingress)**. Provides a count of the number of frames received from the attached equipment in which the CRC calculated by the IGX does not match the CRC provided by the attached equipment in the last 2 octets of the frame. Any frame received with an incorrect CRC is discard by the network. However, the IGX does not wait to receive the entire frame before starting to packetize the frame and send it through the network. As long as the frame header format is valid (see Invalid Format Receive Frames statistic) and the DLCI field in the frame header is recognized (see Receive Frames Undefined DLCI Count statistic below), packets containing the beginning of the frame are created (one start-of-frame (SOF) packet and subsequent middle-of-frame (MOF) packets) and sent as soon as possible. If the frame is short and if there are other packets already waiting to be sent, the detection of the CRC error will cause all the packets of the frame to be discarded. However, if the frame is long and there is no congestion in the ingress VC queue, some packets are sent through the network before the CRC error is detected. As soon as the CRC error is detected, any portion of the frame that has not yet been sent is discarded. In particular, no end of frame (EOF) packet is ever sent. At the far end, when an SOF packet arrives that does not immediately follow an EOF packet, the incomplete frame is discard and counted in the PVC statistic of Transmit Frames Discarded. If the CRC is incorrect because of a bit error in the DLCI field in the frame header, then the error will also be recorded as a Receive Frame with Undefined DLCI unless the reerrored’s DLCI is also configured on the port. This statistic is a subset of the Frames Received statistic.

Table 8-47 Frame Error Statistics (Continued)

Statistics	Description
Alignment error	Frame was not an integral number of bytes. Receive Frame Alignment Errors (Ingress). This statistic provides a count of the number of frames received from the attached equipment in which the total frame length is not an integral number of octets. Any frame received with an incorrect alignment is discarded by the network. However, the IGX does not wait to receive the entire frame before starting the packetize the frame and send it to the network. As long as the frame header format is valid (See Invalid Format Receive Frames statistic), and the DLCI field in the frame header is recognized (see Receive Frames Undefined DLCI Count statistic), packets containing the beginning of the frame are created (one start-of-frame (SOF) packet and subsequent middle-of-frame (MOF) packets) and sent as soon as possible. If the frame is short or if there are other packets already waiting to be sent, the detection of the alignment error will cause all the packets of the frame to be discarded. However, if the frame is long and there is no congestion in the ingress VC queue, some packets are sent through the network before the alignment error is detected. As soon as the alignment error is detected, any portion of the frame that has not yet been sent is discarded. In particular, no end-of-frame (EOF) packet is ever sent. When the next frame arrives, a new SOF packet is sent, etc. At the far end, when a SOF packet arrives that does not immediately follow an EOF packet, the incomplete frame is discarded and counted in the PVC statistic of Transmit Frames Discarded. This statistic is a subset of the Frames Received statistic.
Frame length errors	Frames < 5 bytes or >4096 bytes. **Illegal Length Receive Frames (Ingress)**. Provides a count of the number of frames received from the attached equipment in which the total frame length is either too short or too long. To be accepted, a frame must be at least five octets, but no more than 4510 octets long, including the header and frame check sequence (FCS, or CRC) octets. Any frame received with an invalid length is discard by the network. A frame that is too short is immediately detected and discarded. For a frame that is too long, the IGX does not wait to receive the entire frame before starting to packetize the frame and send it through the network. As long as the frame header format is valid (see Invalid Format Receives Frames statistic), and the DLCI field in the frame header is recognized (see Receive Frames Undefined DLCI Count statistic below), packets containing the beginning of the frame are created (one start of frame (SOF) packet and sent as soon as possible. Since the frame is very long, it is very likely that some packets are sent through the network before the length error is detected. As soon as the length error is detected, any portion of the frame that has not yet been sent is discarded. In particularly, no end-frame (EOF) packet is ever sent. When the next frame arrives, a new SOF packet arrives that does not immediately follow an EOF packet, the incomplete frame is discarded and counted in the PVC statistic of Transmit Frames Discarded. This statistic is a subset of the Frames Received statistic.

Table 8-47 Frame Error Statistics (Continued)

Statistics	Description
Frame format errors	Occurs when either of the least significant bits in the first two bytes of the Frame Relay header are set incorrectly. These two bytes are the frame's address field. The first byte's least significant bit is defined to be a zero, meaning that there is a second byte to the address. The second byte's least significant bit is defined to be a one, meaning this is the last byte of the address because it's a two byte address field. **Invalid Format Receive Frames (Ingress).** Provides a count of the number of frames received from the attached equipment in which the Extended Address (EA) bits (the least significant bit in each of the two Frame Relay header octets) is incorrect. The IGXIGX must see a r0s as the least significant bit of the first octet and a r1s as the least significant bit of the second octet. Any frame received with incorrect EA bits is discarded immediately. This statistic is a subset of the Frames Received statistic.
Unknown DLCIs	Occurs when a frame arrives at a Frame Relay port and the DLCI has not been mapped and the frame is discarded. Received Frames Undefined DLCI Count (Ingress). Provides a count of the number of frames received with a DLCI for which no PVC is provisioned on this port. This count includes any signalling protocol frames received while no signaling protocol is enabled or the wrong signalling protocol is enabled (such as by enabling the StrataLMI signaling protocol while the attached equipment is generating Annex A or Annex D signaling protocol frames, or vice versa). Any frame received with an undefined DLCI is discarded immediately. This statistic is a subset of the Frames Received statistic.
Last unknown DLCI	Displayed so that the user can see the unknown DLCI.

Table 8-48 LMI Statistics

Statistics	Description
Status inquiries transmitted/received	Provides a count of the number of status enquiry frames received from the attached equipment as part of the selected signaling protocol. This statistic is valid for any UIN signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is a subset of the Frames Received statistic. LMI UNI Status Enquiries (Ingress). Provides a count of the number of status enquiry frames received from the attached equipment as part of the selected signaling protocol. This statistic is valid for any UNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is also valid for any NNI signaling protocol chosen (ANSI Annex D, or CCITT Annex A). This statistic is a subset of the Frames Received statistic. LMI NNI Status Enquiries (Egress). Provides a count of the number of status enquiry frames transmitted to the attached equipment as part of the selected signaling protocol. This statistic is valid for any NNI signaling protocol chosen (ANSI Annex D or CCITT Annex A). This statistic is a subset of the Frames Transmitted statistic.

Table 8-48 LMI Statistics (Continued)

Statistics	Description
Status transmit/received	The number of Status messages sent to the user device. LMI UNI Status Transmit Count (Egress). Provides a count of the number of status frames transmitted to the attached equipment as part of the selected signaling protocol. This statistic is valid for any UNI signalling protocol. This statistic is valid for any UNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is a subset of the Frames Transmitted statistic. LMI NNI Status Transmit Count (Egress). Provides a count of the number of status frames transmitted to the attached equipment as part of the selected signaling protocol. This statistic is valid for any UNI signalling protocol. This statistic is valid for any NNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is a subset of the Frames Transmitted statistic.
Async status Xmit	The number of asynchronous status messages sent to the user device. Provides a count of the number of asynchronous status update frames transmitted to the attached equipment as part of the selected signaling protocol. This statistic is valid for any UNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is also valid for any NNI signaling protocol chosen (ANSI Annex D, or CCITT Annex A). If enabled as part of the port configuration (**cnfport** command), an asynchronous status update frame is generated any time a PVC is failed or downed and again any time a PVC is repaired or upped. This statistic is a subset of the Frames Transmitted statistic.
Invalid requests	The number of invalid requests received from the user device. LMI Invalid Status Enquiries (Ingress). Provides a count of the number of status enquiry frames with an invalid format received from the attached equipment as part of the selected signaling protocol. This statistic is valid for any UNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). This statistic is also valid for any NNI signaling protocol chosen (ANSI Annex D, or CCITT Annex A). This statistic is a subset of the Frames Received statistic.
Timeouts	The number of LMI protocol timeouts. LMI UNI Link Timeout Errors. Provides a count of the number of times that the rT392 Polling Verification Timers times out without a Status Enquiry frame having been received. This statistic is valid for any UNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). The rT392 Polling Verification Timers is configured as part of the port configuration (**cnfport** command). LMI NNI Link Timeout Errors. Provides a count of the number of times that the rT392 Polling Verification Timers times out without a Status Enquiry frame having been received. This statistic is valid for any NNI signaling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). The rT392 Polling Verification Timers is configured as part of the port configuration (**cnfport** command).

Table 8-48 LMI Statistics (Continued)

Statistics	Description
Sequence number mismatches	The number of LMI protocol sequence number mismatches. LMI UNI Keepalive Sequence Errors. Provides a count of the number of times that there was a discontinuity in the (normally consecutive) sequence numbers contained the Status Enquiry frames received from the attached equipment. This statistic is valid for any UNI signalling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). LMI NNI Keepalive Sequence Errors. rovides a count of the number of times that there was a discontinuity in the (normally consecutive) sequence numbers contained the Status Enquiry frames received from the attached equipment. This statistic is valid for any NNI signalling protocol chosen (StrataLMI, ANSI Annex D, or CCITT Annex A). .
Signaling protocol	The protocol selected for this Frame Relay port interface: Cisco LMI, Annex A UNI, Annex D UNI, Annex A NNI, or Annex D NNI.

Table 8-49 Miscellaneous Frame Relay Use Statistics

Miscellaneous Statistics	
Statistics	**Description**
Average queue depth	The average fill of the VC queue at the input of the FRP or FRM. Transmit Frames Discarded—Queue Overflow (Egress). Provides a count of the number of frames that were discarded because the port's transmit queue (egress queue) was full. The size of the port's transmit queue is configured as part of the port configuration (**cnfport**) command. Transmit Bytes Discarded—Queue Overflow (Egress). Provides a count of the number of octets in the Transmit Frames Discarded—Queue Overflow statistic. The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets.
BECN frames	Number Explicit Congestion Notification frames transmitted to the receiving router. Number of Explicit Congestion Notification frames transmitted to the transmitting router. Percentage of BECN frames sent to the total number of frames sent. Frames Transmitted with BECN (Egress). Provides a count of the number of frames transmitted to the attached equipment with the Backward Explicit Congestion Notification (BECN) bit set, regardless of where in the network the congestion was observed.
FECN frames	The percentage of FECN frames sent to the total number of frames sent. Frames Transmitted with FECN (Egress). Provides a count of the number of frames transmitted to the attached equipment with the Forward Explicit Congestion Notification (FECN) bit set, regardless of the where in the network the congestion was experienced. This statistic is a subset of the Frames Transmitted statistic.
Rsrc overflow	Resource overflow indicates the number of times the port shut down due to receive frame buffer overflow or receive queue entries.
DE Frames Dropped (Egress)	The total number of frames with Discard Eligibility that were discarded. Provides a count of the number of frames to be transmitted to the attached device that were discarded because the frame's DE bit is set and the port's egress buffer has reached the DE threshold. The DE threshold is configured as part of the port configuration (**cnfport** command). This statistic is a subset of the corresponding PVCs Transmit Frames Discarded statistic.

The **dspportstats** command also displays the following statistics: IMA port summary statistics. A summary and description of these statistics follows:

Table 8-50 IMA Port Statistics

Statistics	Description
IMA Unavailable Seconds	
IMA Near end Failed counts	
Last IMA protocol failure code	

Table 8-51 CLLM (ForeSight) Statistics

Statistics	Description
CLLM Frames Received	Provides a count of the number of Consolidated Link Layer Management (CLLM) frames received from the attached equipment. CLLM frames are used to exchange PVC congestion information over an NNI port to allow the ForeSight algorithm to regulate the flow of traffic on each PVC based on congestion in the local network as well as congestion in the attached network. This is not intended to be a full implementation of the CLLM suite. The CLLM mechanism is enabled as part of the port configuration (**cnfport** command). This statistic is a subset of the Frames Received statistic.
CLLM Bytes Received (Ingress)	Provides a count of the number of octets in the frames counted in the CLLM Frames Received statistic. The octets counted include the Frame Relay header octets as well as the frame check sequence (FCS, or CRC) octets. This statistic is a subset of the Bytes Received statistic.
CLLM Frames Transmitted (Egress)	Provides a count of the number of Consolidated Link Layer Management (CLLM) frames transmitted to the attached equipment. CLLM frames are used to exchange PVC congestion information over an NNI port to allow the ForeSight algorithm to regulate the flow of traffic on each PVC based on congestion in the local network as well as congestion in the attached network. This is not intended to be a full implementation of the CLLM suite. The CLLM mechanism is enabled as part of the port configuration (**cnfport** command). This statistic is a subset of the Frames Transmitted statistic.
CLLM Bytes Transmitted (Egress)	Provides a count of the number of Consolidated Link Layer Management (CLLM) frames transmitted to the attached equipment. CLLLM frames are used to exchange PVC congestion information over an NNI port to allow the ForeSight algorithm to regulate the flow of traffic on each PVC based on congestion in an attached network. This is not intended to be a full implementation of the CLLM suite. The CLLM mechanism is enabled as part of the port configuration (**cnfport** command). This statistic is a subset of the Frames Transmitted statistic.
CLLM Failures	Provides a count of the number of times that: % no CLLM frame was received within one second (not configurable), or% a CLLM frame was received with any invalid internal format. An invalid CLLM frame that is discarded is included in the statistic of Frames Received.

Full Name

Display Frame Relay port statistics

Syntax

dspportstats <slot.port> [interval]

Related Commands

clrportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX	Yes

Example 1

`dspportstats 4.1`

Description

Display the port statistics for Frame Relay port 4.1.

System Response

```
alpha32        LAN   SuperUser       IPX 32    9.2     Aug. 21 1997 12:44 PST

Port Statistics for 4.1         Cleared: Aug. 21 1997 09:45          Snapshot
Port Speed: 256 kbps    Collection Time: 0 day(s) 02:56:48      Corrupted: NO

                      Bytes      Average (kbps)     Util (%)         Frames
From Port:                0            0               0                  0
To Port:                  0            0               0                  0
Frame Errors               LMI Receive Protocol Stats   Misc Statistics
Invalid CRC            0   Status Enq Rcvd         0   Avg Tx Port Q         0
Invalid Alignment      0   Status Xmit             0   FECN Frames           0
Invalid Frm Length     0   Asynch Xmit             0        Ratio (%)        0
Invalid Frm Format     0   Seq # Mismatches        0   BECN Frames           0
Unknown DLCIs          0   Timeouts                0        Ratio (%)        0
Last Unknown DLCI      0   Invalid Req             0   Rsrc Overflow         0
                           Sig Protocol:  None         DE Frms Dropd         0


Last Command: dspportstats 4.1


Continue to next page? (y/n)
```

Enter “y” to see subsequent screens.

```
alpha32        LAN   SuperUser       IPX 32    9.2     Aug. 21 1997 12:49 PST

Port Statistics for 4.1         Cleared: Aug. 21 1997 09:45
Port Speed: 256 kbps    Collection Time: 0 day(s) 03:03:42      Corrupted: NO

                      Bytes      Average (kbps)     Util (%)         Frames
From Port:                0            0               0                  0
To Port:                  0            0               0                  0
LMI Receive Protocol Stats LMI Transmit Protocol Stats  CLLM (ForeSight) Stats
Status Enq Rcvd          0 Status Enq Xmit      --      Frames Rcvd       --
Status Xmt               0 Status Rcd           --      Bytes Rcvd        --
Asynch Xmit              0 Asynch Rcvd          --      Frames Xmt        --
Seq # Mismatches         0 Seq # Mismatches     --      Bytes Xmt         --
Timeouts                 0 Timeouts             --      CLLM Failures     --
Invalid Frames           0

Sig Protocol: None

This Command: dspportstats 4.1


Hit DEL key to quit:
```

Table 8-52 dspportstats—Parameters

Parameter	Description
slot	Specifies the Frame Relay card set slot.
port	Specifies the port on the back card. The range is 1–4 for the FRI-V.35 or FRI-X.21 back cards. For channelized ports, the range is 1–24 or 1–31 for a FRI-T1 or FRI-E1, respectively, and 1-250 for a UFI back card.

Table 8-53 dspportstats—Optional Parameters

Parameter	Description
interval	Specifies the refresh interval time for data. The range is 1–60 seconds. The default interval is 1 second.

dsprtcache

This command displays the cache of all cost-based routing connections. The optional 'index' parameter lets you specify a cache entry index. The optional 'c' parameter clears the cache. The information displayed includes:

Full Name

Display cost-based route cache

Syntax

dsprtcache [index] [c]

[index] specifies the cache entry index

[c] specifies to clear the entire cache or a single entry

Related Commands

dspcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX, BPX	No

Example 1

`dsprtcache`

Description

Display route cache contents, and let you monitor and manually clear the cache.

System Response

```
pissaro     TN      StrataCom          BPX 15      9.1     Jun. 18 1997 11:11 GMT
Route Cache (Summary)
Index Use    No.    Cost     Delay     Restrict   Load     VPC     Hops     RemoteNode
0      Yes     1      Yes       No       None       VBR      No      2          lautrec
1      Yes     6      Yes       No       *s         BDB      No      3          vangogh
2      Yes     9      Yes       No       None       BDA      No      3          matisse
3      Yes     3      Yes       No       *t         BDB      No      3          rousseau
4      Yes     1      Yes       No       None       CBR      No      3          seurat
     <- current
5      No      0       No        No       None     ---       No      0          ---
6      No          0       No          No       None     ---      No      0        ---
7      No          0       No          No      None     ---      No      0         ---
8      No          0       No          No      None     ---      No      0         ---
9      No          0       No          No      None     ---      No      0         ---
```

```
10     No          0      No          No      None     ---      No    0        ---
11     No          0      No          No     None     ---      No     0         ---

Last Command: dsprtcache

Next Command:
```

Table 8-54 dsprtcache—Parameters

Parameter	Description
index	Specifies a particular route entry within the cache. When used with the c parameter, the route is either displayed or cleared from the cache.
c	Clears the cache, or if you also enter the index parameter, clears the route cache specified by the index number.

prtchcnf

Prints the configuration details for voice channels or data channels. This command uses the same syntax, and prints the same information as is displayed using the **dspchcnf** command. See the **dspchcnf** command for syntax and output information.

Full Name

Print channel configurations

Syntax

prtchcnf [start_channel] (see **dspchcnf** description)

Related Commands

dspschcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

prtcons

Prints a summary of connections terminated at the IPX or IGX node. This command uses the same syntax and prints the same information as is displayed using the **dspcons** command. See the **dspcons** command for syntax and output information.

Full Name

Print connection

Syntax

prtcons [start_channel] [nodename] [type] [+d]

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IPX, IGX	Yes

Table 8-55 prtcons—Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. Specify *start channel* in one of the following formats: *slot.port.DLCI*(Frame Relay channel) *remote node.group_name*(Frame Relay group connection) If no starting channel is specified, the display begins with the first connected channel.
node name	Specifies that only connections to the remote node from the local note are displayed. If no “nodename” is designated, connections from the local node to all other nodes are displayed.
–v	Voice only.
–d	Data only.
–f	Frame relay only.
–atfr	Interworking connections.
–g	Grouped connections.
+d	Connection descriptor.
–abit	Abit status.
–fabit	Abit errors.
–fail	Failed connections.
–down	Downed connections.

Table 8-55 prtcons—Optional Parameters (Continued)

Parameter	Description
type	Types listed in Syntax section. The state that may be displayed for Frame Relay and NNI connection types includes: OK: Connection OK, Abit = 1. FAILED: Connection failed, Abit = 0. MISSING: DLCI was deleted in other network NNI. A previous status report indicated a valid DLCI present but an updated report did not. UNUSED: The UNI port does not support reporting of NNI Abit status.

prtict

Prints a data channel's interface control template. The **prtict** command uses the same syntax and prints the same information as **dspict**. See the **dspict** description for output information.

Full Name

Print interface control template

Syntax

prtict <port> <template>

Related Commands

dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	IPX, IGX	Yes

Table 8-56 prtict—Parameters

Parameter	Description
port	Specifies the physical slot and port of the Frame Relay card set.
template	Specifies the template. Choices are a, c, n, l, and f.

upfrport

Activates a port on a Frame Relay card. The applicable cards are all versions of the FRP, FRM, and UFM series of cards. If the port has not been configured through the **cnffrport** command, a set of default configuration values apply.

With a Port Concentrator Shelf (PCS), *upping* the first port causes the FRP-2 or FRM-2 to begin communicating with the four PCS modules and to download code to them if necessary.

Full Name

Up Frame Relay port

Syntax

For UFM-U, FRM, or FRP: **upfrport** <slot.port>

For UFM-C: **upfrport** <slot.port> <line>

Related Commands

dnfrport, cnffrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Example 1

upfrport 9.2

Description

Activate port 2 on the FRP in slot 9.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 15 1997 15:51 PST

Port:       9.2               [ACTIVE  ]
Interface:  FRI-V35 DTE                        Configured Clock:   256 Kbps
Clocking:   Normal                             Measured Rx Clock:    0 Kbps
Port ID                         0
Port Queue Depth            65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold         65535       T391 Link Intg Timer         6 sec
DE Threshold                  100 %     N391 Full Status Poll       10 cyl
Signalling Protocol          None       ForeSight (CLLM)            No
Asynchronous Status            No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer       15       Interface Control Template
N392 Error Threshold            3          Lead       State
N393 Monitored Events Count     4           RTS        ON
Communicate Priority           No           DTR        ON
Upper/Lower RNR Thresh  75%/ 25%
Min Flags / Frames             1

Last Command: upfrport 9.2


Next Command:
```

Table 8-57 upfrport—Parameters

Parameter	Description
slot	Specifies slot number of the card containing the port.
port	Specifies the port. The ranges are: 1–250 on a UFM-C 1–12 on UFM-U with a UFI-12V.35 or UFI-12X.21 1–4 on UFM-U with a UFI-4HSSI 1–4 on an FRP or FRM 1–44 on an FRP-2 or FRM-2.
line	Applies to UFM-C only. The line is the physical connector. The range is 1–8 for T1 or E1.

ATM Connections

This chapter describes the ATM commands that let you activate and configure ATM connections as well as statistical reporting for these connections at an ATM UNI in a BPX or IGX node. You can add ATM connections to an ASI or BXM in a BPX node, or to an ALM/A or UXM in an IGX node. Table 9-1 lists the ATM UNI card combinations for BPX and IGX nodes. For details on ATM commands and other support on an MGX 8220 shelf, refer to the MGX 8220 documentation. For details on ATM commands on an MGX 8550 shelf, refer to the MGX 8550 documentation.

Table 9-1 ATM UNI Cards

Front Card	Back Card
ALM/A	BC-UAI-1T3 or BC-UAI-1E3
ASI-T3	LM-2T3 (Two ports)
ASI-E3	LM-2E3 (Two ports)
ASI-155	MMF-2-BC, SMF-2-BC, or SMF LR-2-BC
UXM	UAI-4OC3MMF, UAI-4OC3SMF, UAI-2OC3SMF, UAI-8T1-IMA DB15, UAI-8E1-IMA DB15, UAI-8E1-IMA BNC
BXM-T3-8 or BXM-T3-12	BPX-T3/E3-8/12 (a universal back card for BXM-T3 or E3)
BXM-E3-8 or BXM-E3-12	BPX-T3/E3-8/12 (a universal back card for BXM-T3 or E3)
BXM-155-4	MMF-155-4, SMF-155-4, or SMFLR-155-4
BXM-155-8	MMF-155-8, SMF-155-8, or SMFLR-155-8
BXM-622	SMF-622 or SMFLR-622
BXM-622-2	SMF-622-2 or SMFLR-622-2

Setting Up an ATM Connection

To set up an ATM connection, perform the following steps:

Step 1 Activate a line with the **upln** command. Activating a line makes it available so you can configure it. Also, it starts statistics collection. Subsequently, you can begin to add connections with **addcon**. You can verify that the line has been activated by using the **dsplns** command. (See the chapter titled “Setting Up Lines” for descriptions of **upln** and **dsplns**.)

Step 2 Activate the ATM port with the **upport X.X** command, where X.X is the slot and port of the ATM card set.

Step 3 Use the **cnfport** command to establish the characteristics for the ATM port.

Step 4 If a suitable class is already configured, note its number and use this class when adding the ATM connection with the **addcon** command. (The **dspcls** command displays the parameters for each connection class. The **cnfcls** command allows you to modify an individual class.)

Step 5 Use the **vt** command to log in to the node at the remote end of the proposed ATM connection.

Step 6 At the remote node, use the **upln**, **upport,** and **cnfport** commands, as listed in steps 1 and 2, to activate and configure the remote port.

Step 7 Use the **addcon** command at one end of the connection to activate the ATM connection.

Managing Bandwidth

There are several commands that assist you in managing bandwidth to achieve satisfactory traffic patterns.

- cnfpref — You can use the configure preference command to specify preferred routing for intra-domain connections. You can use this command to assist in balancing the load on the network's trunks.
- dsprts, prtrts — Use the display and print routes commands in conjunction with the cnfpref command to display the current connection routing information.
- upcon, dncon — You can use the up and down connection commands to temporarily down connections, thus releasing bandwidth for other services. Frequently, to provide more bandwidth for data, Frame Relay, or ATM traffic, you can down some voice connections.

Other Commands

The following commands are useful in establishing connections.

- delcon Deletes a connection from an ATM line.
- dspcons Displays the connections on a specified ATM line.
- dsplnutl Displays the line utilization for an ATM line.

Summary of Commands

Table 9-2 shows the name of each ATM connection command and the page the command description starts on.

Table 9-2 ATM Connection Commands

Mnemonic	Description	Page
addcon	Add connection	9-6
clrchstats	Clear channel statistics	9-35
cnfabrparm	Configure ABR parameters (applies to BXM)	9-37
cnfatmcls	Configure ATM class	9-39
cnfcdparm	Configure channel statistic level on UXM/BXM cards	9-42
cnfcls	Configure class	9-42
cnfcon	Configure connection	9-45
cnfport	Configure port	9-47
cnfportq	Configure port queue	9-54
delcon	Delete connection	9-58
dnport	Down port	9-60
dspatmcls	Display ATM class	9-62
dspchstats	Display channel statistics	9-65
dspcls	Display class	9-73
dspcon	Display connection	9-76
dspconcnf	Display connection configuration	9-83
dspcons	Display connections	9-86
dsplmistats	Display LMI statistics	9-93
dspport	Display port	9-97
dspportq	Display port queue	9-99
dspportstats	Display port statistics	9-102
upport	Up port	9-107

addcon

Establishes an ATM connection between the current node and one or more nodes in the network. You can add ATM connections at a UNI port on either an ASI or a BXM in a BPX node, or an ALM/A or a UXM in an IGX node. When used with the syntax in this chapter, **addcon** adds either a standard ATM connection or an ATM-Frame Relay interworking connection. You can also use **addcon** to add a virtual path connection (or VP tunnelling DAX connection) between a line port on an IGX-UXM as the VP side, and the line port at the ATM cloud entry point as the VCC side. For a description of the **addcon** command as it applies to Frame Relay connections, voice connections, or serial data connections, refer to the chapter in this manual that describes the applicable traffic type. For descriptions of the ATM commands that operate on an MGX 8220 shelf, see the MGX 8220 documentation. For descriptions of the ATM commands that operate on an MGX 8850 shelf, see the MGX 8850 documentation.

Note that in this release, on BXM and UXM cards, you can configure port and trunk (routing and feeder trunk) interfaces on the same card slot. For example, you can have port 1 on a BXM slot upped as a trunk interface while having port 2 on the same card slot upped as a line interface. For more information on the Port and Trunks feature, refer to Chapter 4, "Setting Up Trunks."

In Release 9.2.10, you can add VP tunnelling DAX connections. This type of connection has a VP connection as one end of the connection, and the other end as a VC connection. This VP tunnelling DAX connection can be between different port interfaces on the same UXM card, or on different UXM cards. See Example 2.

In Release 9.2.20, you can add both rt-VBR and nrt-VBR connections. The parameter prompts are the same for both rt-VBR and nrt-VBR, except for Trunk Cell Routing Restrict, which displays for all ATM connections except real-time VBR connections. (This is because rt-VBR connections should only be routed over ATM trunks such as BXM, UXM, and ASI trunks; rt-VBR connections should not be routed over FastPacket trunks such as BTM or ALM/B trunks.)

Note In Release 9.2.20, the rt-VBR class of service is supported on the IGX UXM and BPX BXM, ASI, and BNI cards only. It is not supported for BTM or ALM-A/B connection endpoints. The rt-VBR class of service is not supported on FastPacket trunks, nor is it supported on MGX 8850 or MGX 8220 (AXIS) interface shelves.

Note that for segment connections, all 2- and 3-segment connections must be the same, that is, all rt-VBR or all nrt-VBR. The CLI will not block you from adding any combination of rt-VBR or nrt-VBR segment connections.

The CLI will block you from adding rt-VBR connections in a network of nodes running releases previous to Release 9.2. All nodes in the network must be first upgraded to Release 9.2.10. In a mixed network of Release 9.1 and 9.2.20, or Release 9.2.10 and 9.2.20, the rt-VBR class of service is not supported— in this scenario, all VBR connections will function as nrt-VBR connections. To support rt-VBR, all nodes in the network must be running switch software 9.2.20. See the *Cisco WAN Switching 9.2 Release Notes* for more information.

The **addcon** command for ATM adds any one of the following types of ATM connections:

- Constant Bit Rate (CBR)
- Variable Bit Rate (VBR)—rt-VBR and nrt-VBR
- Frame relay-to-ATM interworking connection (ATFR)
- Frame relay-to-ATM interworking with ForeSight (ATFST) connection
- Available Bit Rate according to ATM Forum standards (ABRSTD)

- Available Bit Rate with ForeSight (ABRFST)
- Frame relay to ATM transparent Service Interworking (ATFT)
- Frame Relay to ATM transparent Service Interworking (ATFTFST)
- Frame Relay to ATM translational Service Interworking (ATFX)
- Frame Relay to ATM translational Service Interworking (ATFXFST)
- Unspecified Bit Rate (UBR)

This description has the following explanations in the form of figures and tables

- Flow diagrams showing the sequence of parameter prompts for each connection type
  - — Figure 9-1 shows the prompt sequence for CBR connections.
  - — Figure 9-2 shows the prompt sequence for VBR connections. (The prompts for rt-VBR and nrt-VBR connections are the same.)
  - — Figure 9-3 shows the prompt sequence for ATFR connections.
  - — Figure 9-4 shows the prompt sequence for ATFST connections
  - — Figure 9-5 shows the prompt sequence for ABRSTD connections.
  - — Figure 9-6 shows the prompt sequence for ABRFST connections.
  - — Figure 9-11 shows the prompt sequence for UBR connections.
  - — Figure 9-7 shows the prompt sequence for ATFT connections.
  - — Figure 9-8 shows the prompt sequence for ATFTFST connections.
  - — Figure 9-9 shows the prompt sequence for ATFX connections.
  - — Figure 9-10 shows the prompt sequence for ATFXFST connections.
- A table that names each type of policing
- A table showing each connection parameter, possible values, and defaults
- A table with a brief definition of each connection parameter
- Example screens from the command line interface

For detailed descriptions of the connection types, traffic classes, policing, and ATM-related topics, refer to the *Cisco BPX 8600 Series Installation and Configuration* guide, the *Cisco WAN Switching System Overview,* and the ATM Forum specifications.

The node on which **addcon** executes is the "owner" of the connection. Connection ownership is important because automatic rerouting and preferred routing information is entered on the node that owns the connection. See the **cnfpref** and **cnfcos** descriptions for details on automatic rerouting.

The parameter prompts depend on the connection type. The figures on this and the following pages are flow diagrams showing the sequence of possible parameter prompts according to the connection type. The flow diagrams begin at the point after you have entered the remote node name and VPI and VCI (which are common parameters). The subsequent tables define the parameters and list the defaults and ranges for each parameter.

A form of notation appears for some parameters that may need explanation. The notation is either (0), (1), or (0+1). This refers to the state of the Cell Loss Priority (CLP) bit. The usage of the CLP bit is in the traffic policing schemes. (0+1) means cells with CLP=0 or 1. (0) means cells with CLP=0. (1) means cells with CLP=1. The CLP bit is used in different contexts. For example, CDVT (0+1) refers to Cell Delay Variation Tolerance (CDVT) for cells with CLP=0 or 1.

Before a connection is added, the proposed connection appears on the screen prompting you to confirm. After **addcon** executes, the system software automatically routes the connection.

Instead of entering a class of service, the user can instead enter a class number to select a pre-configured template, for example, class 4 for NTR-VBR, and class 3 for RT-VBR. The class of service templates can be modified as required using the **cnfcls/cnfatmcls** command and displayed using the **dspcls/dspatmcls** command.

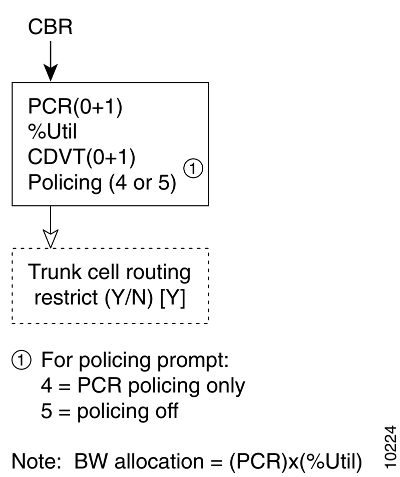
Note For a new node running 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node will retain existing connection classes. Therefore, it won't have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command.

Network and Service Interworking

Frame Relay to ATM Interworking enables Frame Relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking.

Two types of Frame Relay to ATM interworking are supported, Network Interworking and Service Interworking. The Network Interworking function is performed by the BTM card on the IGX switch. The FRSM card on the MGX 8220 supports both Network and Service Interworking.

Figure 9-1 Prompt Sequence for a CBR Connection



rt-VBR and nrt-VBR Connections

VBR (variable bit rate) connections may be classified as rt-VBR or nrt-VBR connections.

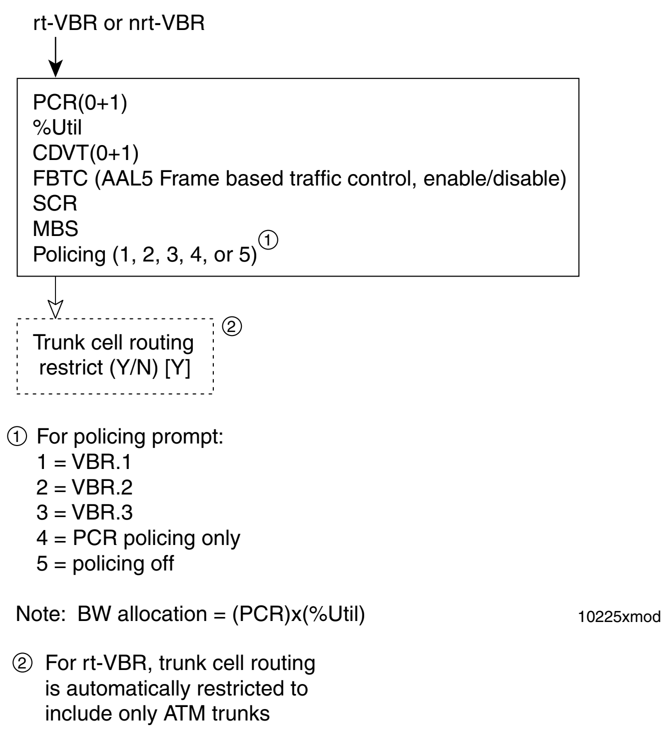
The rt-VBR (real-time variable bit rate) category is used for connections that transmit at a rate varying with time and that can be described as bursty, often requiring large amounts of bandwidth when active. The rt-VBR class is intended for applications that require tightly constrained delay and delay variation such as compressed voice video conferencing—for example, video conferencing which requires real-time data transfer with bandwidth requirements that can vary in proportion to the dynamics of the video image at any given time. The rt-VBR category is characterized in terms of PCR, SCR (sustained cell rate), and MBS (maximum burst size).

The nrt-VBR (non-real time variable bit rate) category is used for connections that are bursty but are not constrained by delay and delay variation boundaries. For those cells in compliance with the traffic contract, a low cell loss is expected. Non-time critical data file transfers are an example of an nrt-VBR connection. A nrt-VBR connection is characterized by PCR, SCR, and MBS.

Configuring VBR connections. The characteristics of rt-VBR or nrt-VBR are supported by appropriately configuring the parameters of the VBR connection.

Note When configuring a rt-VBR connection, the trunk cell routing restriction prompt does not display, as rt-VBR connection routing is automatically restricted to ATM trunks.

Figure 9-2 rt-VBR and nrt-VBR Connection Prompt Sequence



Connection Criteria for real-time VBR and non-real-time VBR Connections

- Default utilization for voice traffic is 100%
- For rt-VBR connections, all nodes must be running at least Release 9.2.20. The command line interface will block you from adding rt-VBR connections in a network running pre-9.2.20 switch software
- When upgrading to Release 9.2.20, all existing VBR connections are re-designated as nrt-VBR connections.
- BXM, ASI, and UXM (IGX switch) cards can terminate rt-VBR connections and support rt-VBR queues.

- On the BPX switch, BXM and BNI trunks support rt-VBR queues, and on the IGX switch only UXM trunks support rt-VBR queues.
- In Release 9.2.20, you can add both rt-VBR and nrt-VBR connections.The parameter prompts are the same for both rt-VBR and nrt-VBR, except for Trunk Cell Routing Restriction prompt. (For rt-VBR connections, the "Trunk Cell Routing Restriction" prompt will not display because rt-VBR traffic should only be routed over ATM trunks; rt-VBR traffic should not be routed over FastPacket trunks.)
- With Release 9.2.20, rt-vbr is supported only on single-segment connections (for example, CPE to BXM to BXM to CPE). Later releases will support 2 and 3 segment connections, for example with the UXM card on the IGX switch (2 segment: CPE to IGX feeder UXM to BXM to BXM to CPE) or (3 segment: CPE to IGX feeder UXM to BXM to BXM to IGX feeder UXM to CPE).

The parameters for a VBR connection are shown in Figure 9-2 in the sequence in which they occur during the execution of the **addcon** command. The VBR policing definitions are summarized in Table 9-6.

Connection Management

The BPX Command Line Interface (CLI) and Cisco WAN Manager accept the same connection policing and bandwidth parameters as in previous releases for both rt-VBR and nrt-VBR service.

The displayed **addcon** parameter prompts for both rt-VBR and nrt-VBR connections are the same. These prompts are: PCR, %util, CDVT, FBTC flag, SCR, MBS, and Policing Type.

There is no change in CDVT usage and the previous policing system.

When using the **addcon** command without the extended parameters, rt-VBR connections automatically use the parameters provided by connection class 3 which contains pre-determined values. Similarly, nrt-VBR connections use connection class 2. You can modify the values of a connection class by using the **cnfcls/cnfatmcl** command. You can display these values by using the **dspcls/dspatmcls** commands.

Figure 9-3 Prompt Sequence for an ATFR Connection

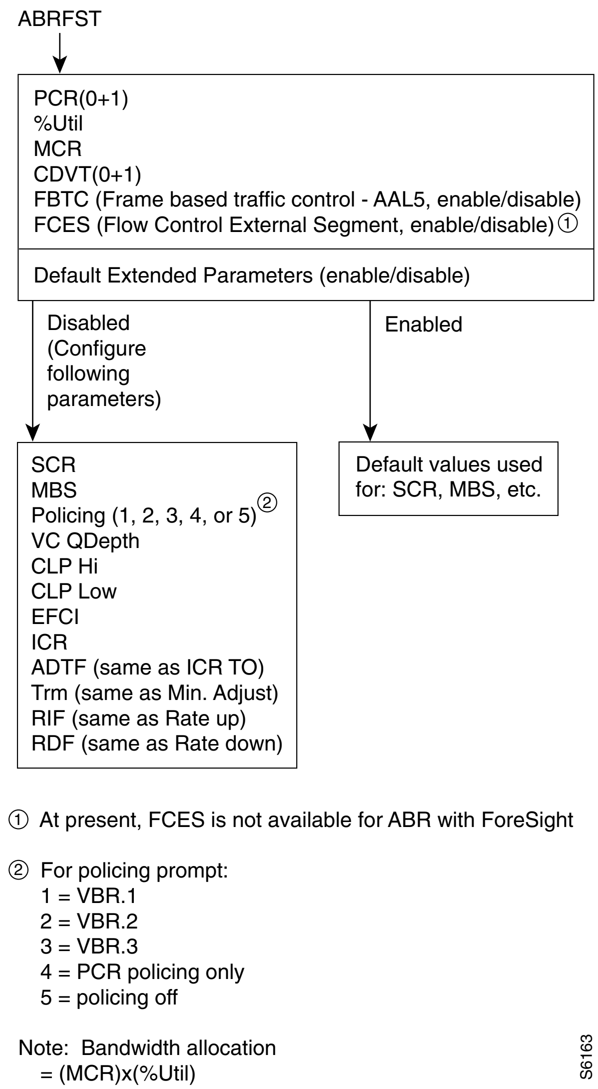
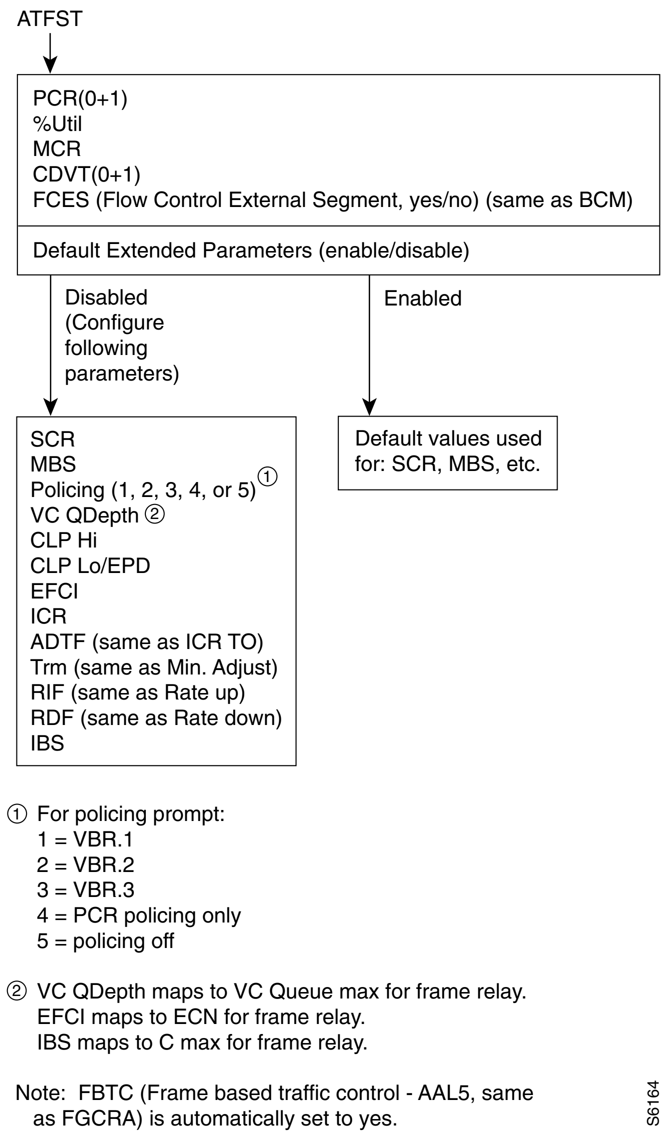


Figure 9-4 Prompt Sequence for a ATFST Connection



ABR Notes

The term ABR is used to specify one of the following:

- ABR standard without VSVD (This is ABR standard without congestion flow control.)
  - Supported by BXM, ASI-T3 (& ASI-E3), and ASI OC-3 cards.
- ABR standard with VSVD. (This is ABR standard with congestion flow control as specified by the ATM Traffic Management, Version 4.0)
  - Also, referred to as ABR.1.
  - Supported only by BXM cards.
  - Feature must be ordered.
- ABR with ForeSight congestion control

— Also, referred to as ABR.FST.

— Supported by BXM and ASI-T3 (& ASI-E3) cards.

— Feature must be ordered.

ABR Connections

The **ABR** (available bit rate) category utilizes a congestion flow control mechanism to control congestion during busy periods and to take advantage of available bandwidth during less busy periods. The congestion flow control mechanism provides feedback to control the connections flow rate through the network in response to network bandwidth availability. The ABR service is not restricted by bounding delay or delay variation and is not intended to support real-time connections. ABR is characterized by: PCR and MCR.

Policing for ABR connections is the same as for VBR connections which are summarized in Figure 9-8.

The ABR connections are configured as either ABR Standard (**ABRSTD**) connections or as ABR ForeSight (**ABRFST**) connections.

The parameters for an ABRSTD connection are shown inFigure 9-5 in the sequence in which they occur during the execution of the **addcon** command.

The ABRSTD connection supports all the features of ATM Standards Traffic Management 4.0 including VSVD congestion flow control.

VSVD and flow control with external segments are shown in Figure 9-6.

Figure 9-5 Prompt Sequence for an ABRSTD Connection

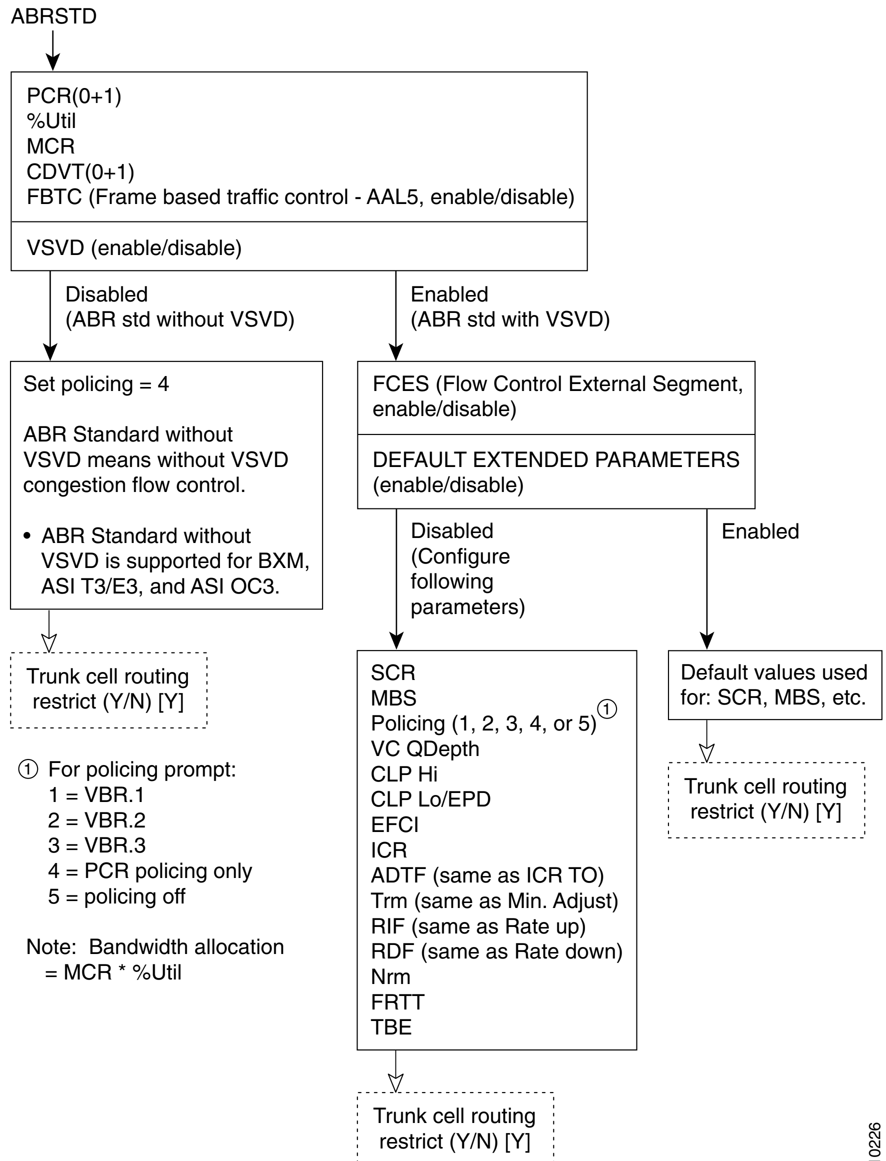
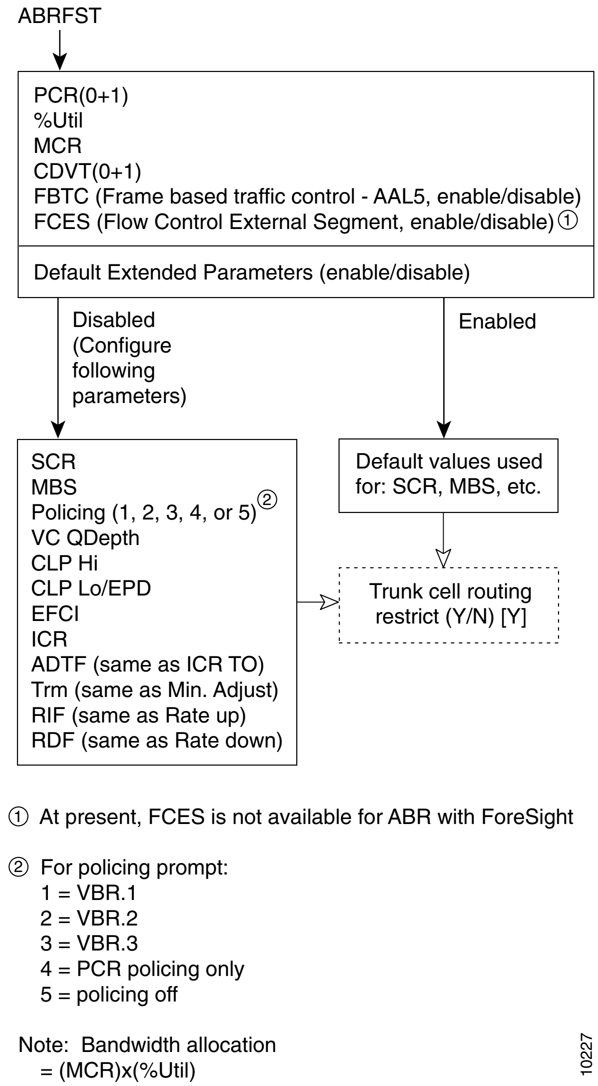


Figure 9-6 Prompt Sequence for ABRFST Connection

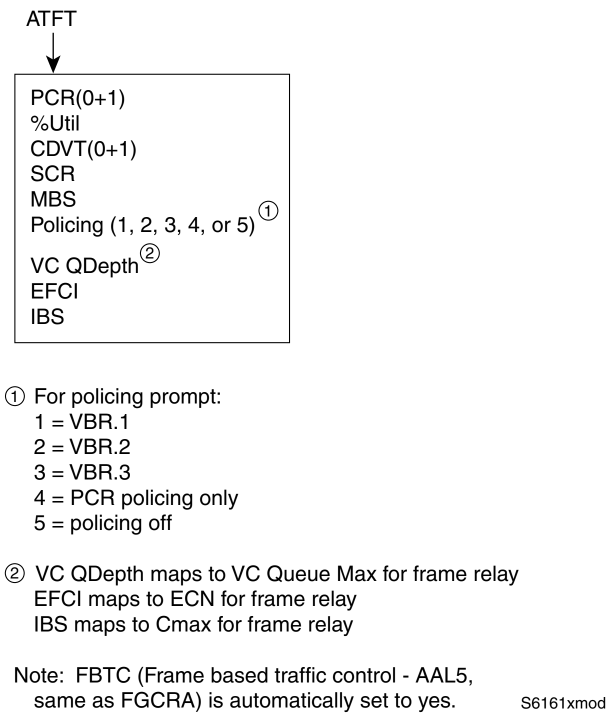


ATFT Transparent Service Interworking Connections

An **ATFT** connection is a Frame Relay to ATM transparent Service Interworking connection and is configured as a VBR connection, with a number of the ATM and Frame Relay connection parameters being mapped between each side of the connection.

The parameters for an ATFT connection are shown in Figure 9-7 in the sequence in which they occur during the execution of the **addcon** command.

Figure 9-7 ATFT Connection Prompt Sequence

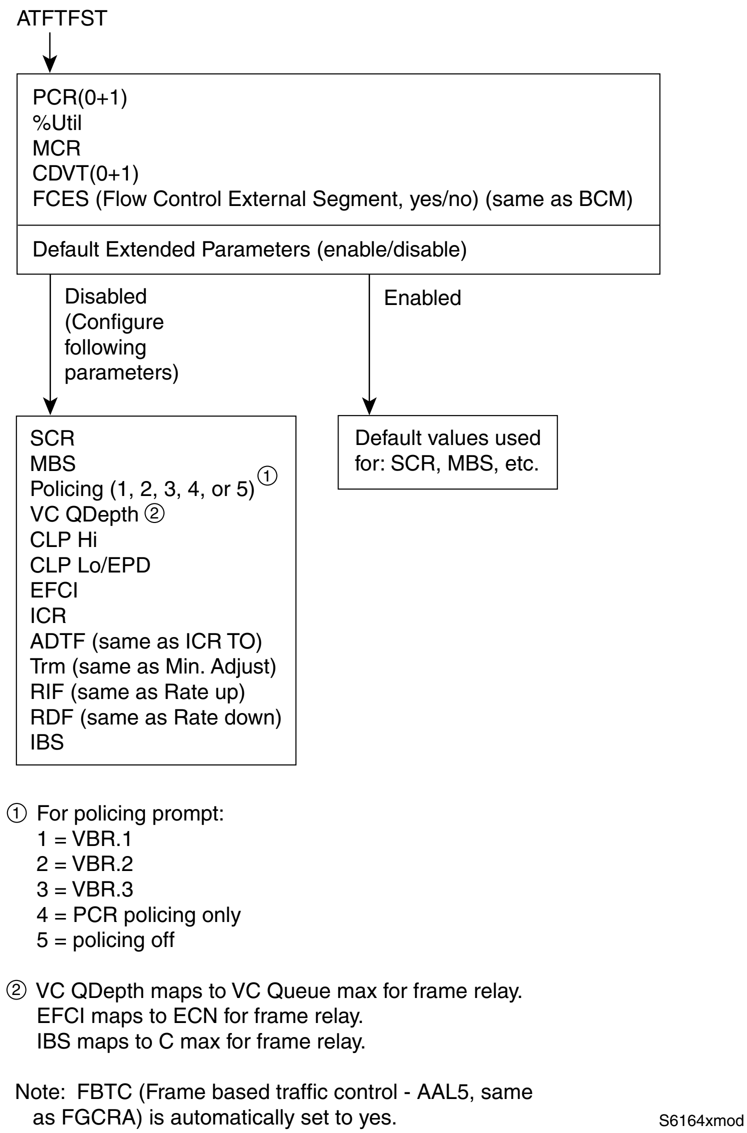


ATFTFST Transparent Service Interworking Connections

An **ATFTFST** connection is a Frame Relay to ATM transparent Service Interworking connection that is configured as an ABR connection with ForeSight. ForeSight congestion control is automatically enabled when connection type ATFTFST is selected. A number of the ATM and Frame Relay connection parameters are mapped between each side of the connection.

The parameters for an ATFTFST connection are shown in Figure 9-8 in the sequence in which they occur during the execution of the **addcon** command.

Figure 9-8 ATFTFST Connection Prompt Sequence

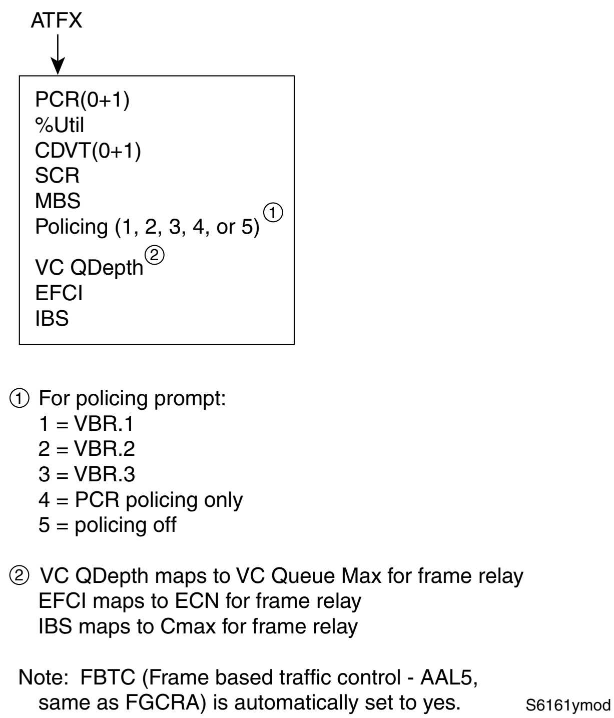


ATFX Translational Service Interworking Connections

An **ATFX** connection is a Frame Relay to ATM translational Service Interworking connection and is configured as a VBR connection, with a number of the ATM and Frame Relay connection parameters being mapped between each side of the connection.

The parameters for an ATFX connection are shown in Figure 9-9 in the sequence in which they occur during the execution of the **addcon** command.

Figure 9-9 ATFX Connection Prompt Sequence

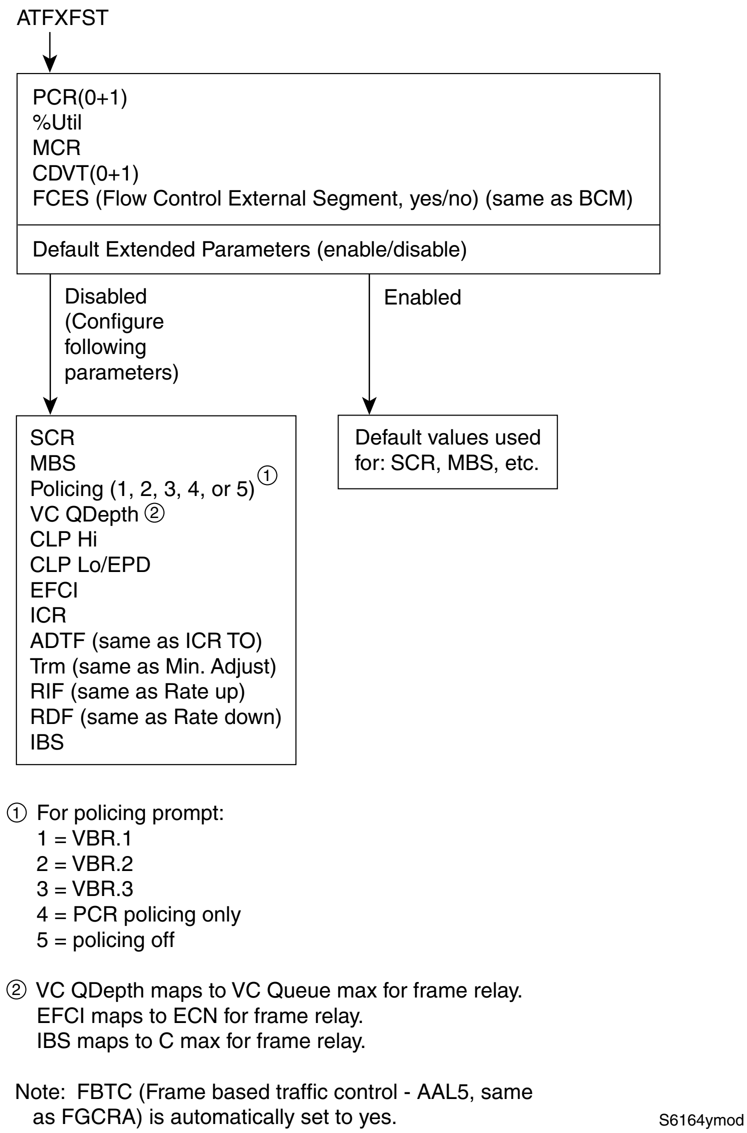


ATFXFST Translational Service Interworking Connections

An **ATFXFST** connection is a Frame Relay to ATM translational Service Interworking connection that is configured as an ABR connection with ForeSight. ForeSight congestion control is automatically enabled when connection type ATFXFST is selected. A number of the ATM and Frame Relay connection parameters are mapped between each side of the connection.

The parameters for an ATFXFST connection are shown in Figure 9-10 in the sequence in which they occur during the execution of the **addcon** command.

Figure 9-10 ATFXFST Connection Prompt Sequence



UBR Connections

The unspecified bit rate (UBR) connection service is similar to the ABR connection service for bursty data. However, UBR traffic is delivered only when there is spare bandwidth in the network. This is enforced by setting the CLP bit on UBR traffic when it enters a port.

Therefore, traffic is served out to the network only when no other traffic is waiting to be served first. The UBR traffic does not affect the trunk loading calculations performed by the switch software.

The parameters for a UBR connection are shown in Figure 9-11 in the sequence in which they occur during the execution of the **addcon** command.

The UBR policing definitions are summarized in Table 9-3.

Figure 9-11 UBR Connection Prompt Sequence

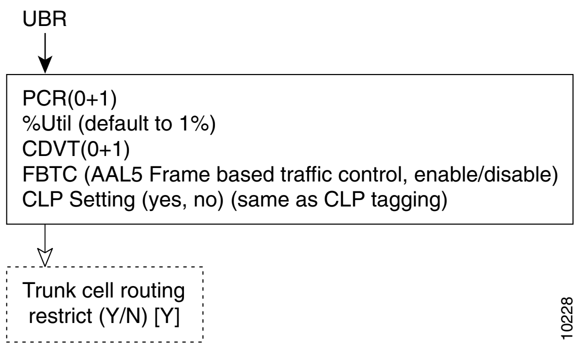


Table 9-3 UBR Policing Definitions

Connection Type	ATM Forum TM spec. 4.0 conformance definition	PCR Flow (1st leaky bucket)	CLP tagging (for PCR flow)	SCR Flow (2nd leaky bucket)	CLP tagging (for SCR flow)
UBR	**UBR.1** when CLP setting = no	**CLP(0+1)**	no	off	n/a
UBR	**UBR.2** when CLP setting = yes	**CLP(0+1)**	no	**CLP(0)**	**yes**

Table 9-4 contains descriptions of the ATM parameters that appear on screen. Table 9-5 gives the defaults, ranges (or values), and applicable connection type (marked with an X) for each parameter. Table 9-7 gives a shorthand definition of each type of traffic policing. In Table 9-6 and Table 9-7, note that VBR.1, VBR.2, VBR.3, CBR.1, UBR.1, and UBR.2 are ATM Forum standards for traffic policing. The columns in Table 9-6 and Table 9-7 indicate the actions involved with each policing type. For descriptions of the *traffic types*, *connection types*, and *traffic policing*, refer to the *Cisco BPX 8600 Series Reference* and the *Cisco WAN Switching System Overview*. The preceding flow diagrams help clarify the information in the forthcoming tables. The remaining parts of this description contain attributes and screen examples.

Note If the description states the parameter is transmit/receive, the system is prompting for two values: one is for the transmit direction, the other for the receive direction. Also, not all parameters apply to OC-3/STM1 or OC-12/STM4, as the text shows.

Table 9-4 addcon—Parameters

Parameter/Prompt	Description
local channel	Specifies the local slot, port, virtual path identifier (vpi), and virtual connection identifier (vci) for the connection. The format is *slot.port.vpi.vci*. The VPI range for a UNI connection is 1–255. The VPI range for an NNI connection is 1–4095. When adding an MGX 8850 interface shelf with a UNI interface to a BPX routing node, the VPI range is 1–255. The VCI range is 1–65535. When adding an MGX 8850 interface shelf with an NNI interface to a BPX routing node, the VPI range is 1–255. The VCI range is 1–65535. When adding an SES (Service Expansion Shelf) to an IGX 8400 routing node, for VCC addressing, the VPI range is 1–255. The VCI range is 1–65535. For VPC addressing, when adding an SES interface shelf to an IGX 8400 routing hub with a UNI interface, the VPI range is 1–255. The VCI range is 1–65535. For VPC addressing, when adding an SES shelf to an IGX 8400 routing with an NNI interface, the VPI range is 1–4095. The VCI range is 1–65535. Note that when adding an SES to an IGX 8400 routing node, the VPI/VCI configured on the IGX 8400 routing hub should match the VPI/VCI configured on the SES interface shelf endpoint address. When adding a VP tunnelling DAX connection to an IGX-UXM card, either end of the connection can be the VPI or VCI side. This connection type can be any of the ATM connection types supported by UXM virtual trunks, for example, ABR, CBR, UBR, and VBR. The VCI range is 1–65535. The vci can be an asterisk (*) to indicate the connection is a *virtual path connection* (so the vci has no meaning within the network).
remote node name	Specifies the name of the node at the other (or remote) end of the connection.
remote channel	Specifies the remote node’s slot, port, vpi, and vci for this connection. The format is *slot.port.vpi.vci*. The vpi and vci ranges are: The vpi range for a UNI connection is 1–255. The vpi range for an NNI connection is 1–4095. The range for a vci is 1–65535. The vci can be an asterisk (*) to indicate the connection is a *virtual path* (the vci does not provide a distinction within the network).

Table 9-4 addcon—Parameters (Continued)

Parameter/Prompt	Description
connection class/ traffic type	Specifies one of the following traffic types—VBR (rt-VBR or nrt-VBR), UBR, CBR, ATFST, ATFR, ABRSTD, ABRFST, ATFT, ATFX, ATFTFST, or ATFXFST; or connection classes—for example, for rt-VBR, connection class 3 for a new node running Release 9.2.20. The subsequent displayed parameters depend on the connection type you choose. To see the parameters associated with each connection type, refer to the appropriate flow diagrams (Figure 9-1 through Figure 9-11). For a definition of each class, refer to the *Cisco BPX Series Installation and Configuration* and the *Cisco WAN Switching System Overview*. The option for choosing a class *number* is also available. The class is a *template* for a connection type. The class serves as an alternative to specifying each parameter for a connection type. To specify a connection class, enter a digit in the range 1–10. To see the parameter values for a class, use the **dspcls** commands. To customize any class template, use **cnfcls**. **Note** For a new node running 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node will retain existing connection classes. Therefore, it won't have the rt-VBR connection class 3. However, you can configure the connection classes to whatever service and parameters you want by using the **cnfcls/cnfatmcls** command. Note that for VP tunnelling DAX connections, a VP tunnelling connection type is represented by CBRVP, ABRSTVP, ABRFSTVP, etc. (The letters "VP" are appended to the connection class or connection type, to indicate that it is a VP tunnelling connection.) This connection type must be the same as the VCC connection type provisioned within the public ATM cloud.
PCR	Peak Cell Rate: the cell rate that the source cannot exceed.
%Util	Specifies the percentage of bandwidth utilization.
MCR	Minimum Cell Rate: the committed, minimum cell rate for a connection in a network.
CDVT	Cell Delay Variation Tolerance: controls time scale over which the PCR is policed.
FBTC (AAL5 Frame-based Traffic Control)	To enable the possibility of discarding the whole frame, not just one non-compliant cell. This is used to set the Early Packet Discard bit at every node along a connection. **Note** With the ASI, FBTC means packet discard on both policing and queueing. With the BXM, FBTC means packet discard on queueing only.
VSVD	Virtual Source Virtual Destination.
Flow Control External Segments	Enables Cisco WAN switches to perform flow control on external segments (on the CPE, for example) in addition to the Cisco WAN Switching segments.
SCR	Sustainable Cell Rate: the long-term limit on the rate that a connection can sustain.
MBS	Maximum Burst Size: the maximum number of cells that can burst at the PCR and still be compliant. MBS is used to determine the Burst Tolerance (BT), which controls the time period over which the SCR is policed.
Policing	(see Table 9-5, "addcon—Parameter Defaults and Ranges"). **Note** With the ASI, FBTC means packet discard on both policing and queueing. With the BXM, FBTC means packet discard on queueing only.
VC QDepth	The depth of the queue VC QDepth.
CLP Hi	Cell Loss Priority Hi threshold (% of VC QDepth). When the high threshold is exceeded, the node discards cells with CLP=1 until the number of cells in the queue drops below the level specified by CLP Lo/EPD.

Table 9-4 addcon—Parameters (Continued)

Parameter/Prompt	Description
CLP Lo/EPD	Cell Loss Priority Low threshold (% of VC QDepth)/Early Packet Discard. When the number of cells in the queue drops below the level specified by CLP Lo/EPD, the node stops discarding cells with CLP=1. If the card is a BXM and AAL5 FBTC=yes, the percent of VC QMax equals the value of EPD. Frame-based Traffic Control (FBTC) is FGCRA for AAL5. **Note** The BXM does not support Frame-based Policing. For an ASI card, the percent of VC QMax is CLP Lo regardless of the FBTC setting.
EFCI	Explicit Forward Congestion Indication threshold (% of VC QDepth).
ICR	Initial Cell Rate: the rate at which a source initially transmits after an idle period.
IBR	Initial Burst Size: the maximum burst size a source can initially transmit after an idle period. IBR applies to only BXM cards.
ADTF (ATM Forum TM 4.0 term)	The Allowed-Cell-Rate Decrease Factor. Time permitted between sending RM-cells before the rate is decreased to ICR. (In previous software releases, ADTF was ICR TO—Initial Cell Rate Time Out.)
Trm (ATM Forum TM 4.0 term)	An upper bound on the time between forward RM-cells for an active source: an RM cell must be sent at least every *Trm* milliseconds. (In previous software releases, Trm was Min. Adjust.)
RIF (ATM Forum TM 4.0 term)	Rate Increase Factor: controls the amount by which the cell transmission rate may increase upon receipt of an RM cell. (In previous software releases, RIF was Rate Up.)
RDF (ATM Forum TM 4.0 term)	Rate Decrease Factor: controls the amount decrease in cell transmission rate when an RM cell arrives. (In previous software releases, RDF was Rate Down.)
Nrm (ATM Forum TM 4.0 term)	Nrm. Maximum number of cells a source may send for each forward RM cell: an RM cell must be sent for every *Nrm*–1 data cells.
FRTT (ATM Forum TM 4.0 term)	Fixed Round Trip Time: the sum of the fixed and propagation delays from the source to a destination and back.
TBE (ATM Forum TM 4.0 term)	Transient Buffer Exposure The negotiated number of cells that the network would like to limit the source to sending during start-up periods, before the first RM-cell returns.
PCR	Peak cell rate: the cell rate which the source may never exceed.

Table 9-5 addcon—Parameter Defaults and Ranges

PARAMETER WITH [DEFAULT SETTINGS]	UXM and BXM T1/E1, T3/E3, OC-3, and OC-12 RANGE	ASI RANGE
PCR(0+1)[50/50]	50–max. T1/E1 cells/sec.	T3: MCR–96000
	50–max. T3/E3 cells/sec.	E3: MCR–80000
	50–max. OC-3 cells/sec	OC-3 (STM1): 0–353200
	50–max. OC-12 cells/sec	Limited to MCR–5333 cells/sec for ATFR connections.
%Util [100/100] for UBR [1/1]	0–100%	1–100%

Table 9-5 addcon—Parameter Defaults and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTINGS]	UXM and BXM T1/E1, T3/E3, OC-3, and OC-12 RANGE	ASI RANGE
MCR [50/50]	cells/sec 6–max. of T3/E3/OC-3/OC-12	T3: 0–96000 cells/sec E3: 0–80000 cells/sec
AAL5 Frame-Based Traffic Control: for rt/nrt-VBR [disable] for ABR/UBR [enable] for Path connection [disable]	enable/disable **Note** With the BXM card, FBTC means packet discard on both policing and queueing.	enable/disable **Note** With the ASI card, FBTC means packet discard on both policing and queueing.
CDVT(0+1): for CBR [10000/10000], others [250000/250000]	0–5,000,000 microsecs.	T3/E3 1–250,000 usecs. OC-3/STM1: 0–10000 usecs.
ForeSight [disable]	0 = disable 1 = enable	0 = disable 1 = enable
VSVD [disable]	enable/disable	enable/disable
Flow Control External Segment [disable]	enable/disable	enable/disable
Default Extended Parameters [enable]	enable/disable	enable/disable
CLP Setting [enable]	enable/disable	enable/disable
SCR [50/50]	c50–max. T1/E1 cells/sec. 50–max. T3/E3 cells/sec. 50–max. OC-3 cells/sec 50–max. OC-12 cells/sec	T3: MCR–96000:T3 E3: MCR–80000: E3 OC-3/STM1: 0–353200 Limited to MCR–5333 cells/sec for ATFR connections.
MBS [1000/1000]	1-5,000,000 cells	T3/E3: 1–24000 cells OC-3 (STM1): 10–1000 cells
Policing [3] For CBR: [4]	1 = VBR.1 2 = VBR.2 3 = VBR.3 4 = PCR policing only 5 = off	1 = VBR.1 2 = VBR.2 3 = VBR.3 4 = PCR policing only 5 = off
ICR: max [MCR, PCR/10]	MCR - PCR cells/sec	MCR - PCR cells/sec
ADTF [1000]	62–8000 msecs.	1000–255000 msecs.
Trm [100]	ABRSTD: 1–100 msecs. ABRFST: 3–255 msecs.	20–250 msecs.
VC QDepth [16000/16000] For ATFR/ATFST [1366/1366]	0–61440 cells	Applies to T3/E3 only ABR: 1–64000 cells ATFR: 1–1366 cells
CLP Hi [80/80]	1–100%	1–100%
CLP Lo/EPD [35/35]	1–100%	1–100%

Table 9-5 addcon—Parameter Defaults and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTINGS]	UXM and BXM T1/E1, T3/E3, OC-3, and OC-12 RANGE	ASI RANGE
EFCI [30/30] For ATFR/ATFST [100/100]	1–100%	1–100%
RIF: For ForeSight: = max [PCR/128, 10] For ABRSTD [128]	If ForeSight, then in absolute (0–PCR) If ABR, then 2^n (1–32768)	If ForeSight, then in absolute (0–PCR) If ABR, then 2^n (1–32768)
RDF: For ForeSight [93] For ABRSTD [16]	IF ForeSight, then % (0%–100%) If ABR, then 2^n (1–32768)	IF ForeSight, then % (0%–100%) If ABR, then 2^n (1–32768)
Nrm[32]–BXM only	2–256 cells	not applicable
FRTT[0]–BXM only	0–16700 msec	not applicable
TBE[1,048,320]–BXM only	0–1,048,320 cells (different maximum range from TM spec. but limited by firmware for CRM (4095 only) where CRM=TBE/Nrm	not applicable
IBS [0/0]	0–24000 cells	T3/E3 ABR: 0–24000 cells ATFR: 1–107 cells OC-3: 0–999 cells
Trunk Cell Routing Restriction (y/n) [y]	yes or no For rt-VBR connections, this prompt will not display. (This is because rt-VBR connections should only be routed over ATM trunks such as BXM, UXM, and ASI, not over FastPacket trunks such as BTM or ALM/A-B.) Trunk Cell Routing Restriction will display for all other connections.	yes or no For rt-VBR connections, this prompt will not display. (This is because rt-VBR connections should only be routed over ATM trunks such as BXM, UXM, and ASI, not over FastPacket trunks such as BTM or ALM/A-B.) Trunk Cell Routing Restriction will display for all other connections.

Table 9-6 Traffic Policing Definitions

Connection Type	ATM Forum TM spec. 4.0 conformance definition	PCR Flow (1st leaky bucket)	CLP tagging (for PCR flow)	SCR Flow (2nd leaky bucket)	CLP tagging (for SCR flow)
CBR	**CBR.1** when policing set to 4 (PCR policing only)	**CLP(0+1)**	no	off	n/a
CBR	when policing set to 5 (off)	off	n/a	off	n/a
UBR	**UBR.1** when CLP setting = no	**CLP(0+1)**	no	off	n/a
UBR	**UBR.2** when CLP setting = yes	**CLP(0+1)**	no	**CLP(0)**	**yes**
rt/nrt-VBR, ABR, ATFR, ATFST	**VBR.1** when policing set to 1	**CLP(0+1)**	no	**CLP(0+1)**	no
rt/nrt-VBR, ABR, ATFR, ATFST	**VBR.2** when policing set to 2	**CLP(0+1)**	no	**CLP(0)**	no
rt/nrt-VBR, ABR, ATFR, ATFST	**VBR.3** when policing set to 3	**CLP(0+1)**	no	**CLP(0)**	**yes**
rt/nrt-VBR, ABR, ATFR, ATFST	when policing set to 4	**CLP(0+1)**	no	off	n/a
rt/nrt-VBR, ABR, ATFR, ATFST	when policing set to 5 (off)	off	n/a	off	n/a

Note 1: - For UBR.2, SCR = 0

Note 2:

- CLP = Cell Lost Priority
- CLP(0) means cells that have CLP = 0
- CLP(1) means cells that have CLP = 1
- CLP(0+1) means both types of cells: CLP = 0 & CLP = 1
- CLP(0) has higher priority than CLP(1)
- CLP tagging means to change CLP = 0 to CLP = 1, where CLP= 1 cells have lower priority

Table 9-7 VBR Policing Definitions

Connection Type	ATM Forum TM spec. 4.0 conformance definition	PCR Flow (1st leaky bucket)	CLP tagging (for PCR flow)	SCR Flow (2nd leaky bucket)	CLP tagging (for SCR flow)
rt/nrt-VBR, ABR, ATFR, ATFST, ATFT, ATFTST, ATFX, ATFXFST	**VBR.1** when policing set to 1	**CLP(0+1)**	no	**CLP(0+1)**	no
rt/nrt-VBR, ABR, ATFR, ATFST, ATFT, ATFTST, ATFX, ATFXFST	**VBR.2** when policing set to 2	**CLP(0+1)**	no	**CLP(0)**	no
rt/nrt-VBR, ABR, ATFR, ATFST, ATFT, ATFTST, ATFX, ATFXFST	**VBR.3** when policing set to 3	**CLP(0+1)**	no	**CLP(0)**	yes
rt/nrt-VBR, ABR, ATFR, ATFST, ATFT, ATFTST, ATFX, ATFXFST	when policing set to 4	**CLP(0+1)**	no	off	n/a
rt/nrt-VBR, ABR, ATFR, ATFS, ATFT, ATFTST, ATFX, ATFXFST	when policing set to 5 for off	off	n/a	off	n/a

Connection Types Supported for IGX 8400 over UXM/UXM-E Interface in Release 9.2

Tiered network, Frame Relay and ATM connections are supported as two or three-segment connections. Voice connections are supported for the three-segment connection. Simple gateway (SGW), complex gateway (CGW), cell forwarding (CF) gateway types are supported in the middle segment terminating on IGX 8400 hubs in the routing network, depending on the connection types.

Note the following changes in the switch software in the IGX 8400 feeder connection management area:

- The **addcon/delcon** commands let you add data and FRP connections that are terminated on UXM/UXM-E cards for IGX 8400 interface shelves and terminated on routing network interface shelf trunks or IGX 8400 routing nodes.
- The **addcon** and **delcon** commands let you add DACS connections for data, FRP and ATM connections terminated on an interface shelf trunk or node using an UXM/UXM-E interface.
- In Release 9.1, there was a limitation on the BTM-E1 interface shelf trunk. A two-segment voice connection is not supported, and there is a restriction on where you can add a three-segment voice connection. The master restriction applies only to the interface shelf segment in IGX feeders. You must add the interface shelf segment for LDM and CVM (low speed data and voice) from the port endpoint (LDM or CVM) and not BTM. This restriction does not apply for high-speed data or Frame Relay (FR) interface shelf segments. This should not be a limitation for the UXM/UXM-E feeder trunk on a three-segment voice connection, because the master of the connection determines the connection routing selection.

IGX 8400 and SES Feeder Connectivity over UXM/UXM-E Interface using ATM UNI and NNI Format

Previous to Release 9.2, the STI cell header format was used to pass cells between an IGX 8400 routing hub and a BTM E1 interface shelf (feeder) port.

In this release, the IGX 8400 routing hub can communicate with the SES interface shelves using the LMI-Annex G signalling protocol, which is similar to what the BPX routing hub uses to communicate with the MGX 8850 interface shelves.

addconn Parameters

The VPI and VCI ranges supported for UXM/UXM-E terminated feeder connections on an IGX 8400 feeder are different compared to BTM E1 terminated feeder connections. The UXM/UXM-E feeder interface can support the full VPI and VCI ranges for UNI or NNI.

- When connected to an IGX 8400 on a BTM E1 feeder interface, IGX 8400 feeder supports limited VPI and VCI ranges in STI format.
- When connected to an SES feeder, the standard VPI and VCI ranges for the ATM UNI and NNI cell format are supported. An SES feeder supports the full VPI and VCI ranges.

Unlike the BTM E1 which has a fixed number of channels per card, the number of user channels available per UXM/UXM-E card is subject to card capacity. The number of user channels available per feeder port is not a fixed number because UXM/UXM-E user channels are allocated to a given port from the card pool on a first come, first serve basis.

UXM/UXM-E Feeder Port Cell format and Addressing for SES Feeder to IGX Routing Hub

On the MGX 8220, the slot number is mapped to the certain VPI on the IGX 8400 hub. This does not apply to the SES feeder. The VPI/VCI configured on the IGX 8400 routing hub should match the VPI/VCI configured on the SES feeder endpoint address. The cell header format used for cells passing between an IGX 8400 and an SES feeder port is a standard ATM format, which may be UNI or NNI format.

The MGX 8800’s VPI field of the ATM cell depending on the interface type (UNI or NNI) and connection type (VCC or VPC):

- The VPI/VCI combination of 3/31 is used for the LMI signalling channel. When configuring the SES feeder, you must be careful not to allow 3/31 for anything else but the LMI signalling channel.
- For VCC addressing, the VPI range is 1-255 and the VCI range is 1-65535.
- For VPC addressing, the interface type is significant: UNI or NNI may be supported. When the interface type is UNI, the available VPI range is 1-255 and VCI range is 1-65535. When the interface type is NNI the available VPI range is 1-4095 and VCI range is 1-65535.

Table 9-8 illustrate the existing and new (in **bold**) connection types:

Table 9-8 Two Segment Connections Supported on UXM to PXM Feeder Trunks

Routing Endpoint (A)	Feeder Endpoint (B)	Connection Type	VCC or VPC	Gateway Type (if applicable)
UXM	AUSM	CBR.1	Both	CF
		VBR.[1-3]		CF
		ABR.FST		CF
		ABR w/o VSVD		CF
		UBR.[1-2]		CF
UFM	AUSM	ATFR, ATFST	N/A	CGW
UXM	FRSM	ATFR, ATFST	N/A	CGW
UFM	FRSM	FR	N/A	CGW
FRM	AUSM	ATFR, ATFST	N/A	CGW
FRM	FRSM	FR	N/A	CGW
UVM/CVM	Y	Not Supported		
HDM/LDM	Y	Not Supported		
X	VISM	Not Supported		

Note Y: Implies any card type among AUSM, FRSM, VISM.
X: Implies any card type of UXM, UVM, UFM, FRM, CVM, and HDM.

Table 9-9 lists supported three-segment connections for a three segment network consisting of two IGX-UXMs with two SES feeders attached to each UXM.

Table 9-9 Three-Segment Connection between ATM Endpoints on Two IGX 8400s

Feeder Endpoint (A)	Feeder Endpoint (B)	Connection Type	VCC or VPC	Gateway Type (if applicable)
AUSM	AUSM	CBR.1	both	CF
		VBR.[1-3]		CF
		ABR.FST		CF
		ABR w/o VSVD		CF
		UBR.[1-2]		CF
AUSM	FRSM	ATFR, ATFST	N/A	CF
FRSM	FRSM	ATFR, ATFST	N/A	CGW

Table 9-10 shows one-segment connections (between two IGX 8400s) that do not involve the SES interface shelf. There are UXM trunks only in the connection route. The cards are renamed for (for example, the UFM card is called UFSM, the UXM card is called UXSM, and so forth).

Note The CVM and LDM card types are not supported as remote endpoint connections with an IGX 8400.

Table 9-10 One-Segment Connections between IGX 8400s without an SES Shelf

Routing Endpoint (A)	Routing Endpoint (B)	Connection Type	VCC or VPC	Gateway Type (if applicable)
UXSM/UXSM-E	UXSM/UXSM-E	CBR.1	both	CF
		VBR.[1-3]		CF
		ABR.FST		CF
		ABR w/o VSVD		CF
		UBR.[1-2]		CF
		ATFR, ATFST		CGW
UFSM	UXSM	ATFR, ATFST	N/A	CGW
		ATFX, ATFXST		SIW
		ATFT, ATFTFST		SIW
UFSM	UFSM	FR	N/A	CGW
UVSM	UVSM	Voice	N/A	SGW
HDSM	HDSM	Data	N/A	SGW

Release 9.2 Nodes Can Interoperate with Release 9.1 and 8.4 Nodes

A node running Release 9.2 can interoperate with nodes running release 8.4 and Release 9.1. The switch software will not block you from adding a UXM/UXM-E interface shelf trunk to a Release 9.2 IGX 8400 node in a network of mixed releases (that is, nodes running Release 9.2, 9.1, and 8.4). However, the **addcon** command will be blocked if you add a two-segment connection from a Release 9.1 or release 8.4 UXM port to a Release 9.2 UXM interface shelf trunk. Similarly, the addcon command will be blocked if you add a two-segment connection from a Release 9.2 UXM port to a Release 9.1 or Release 8.4 UXM interface shelf trunk. Checking of switch software is done on the remote end of the connection.

ESP 4.0 Controller Support on BPX in Release 9.2

These changes support the ESP 4.0 VSI controller on BPX nodes:

- The addcon command will be blocked for VPI and VCI that are reserved for master-slave VCs.
- The addcon command will be blocked for VPI and VCI that are reserved/used for the LMI/ILMI channels.

Full Name

Add a connection

addcon ***parameters*** (see preceding flow diagrams and tables)

Related Commands

delcon, dspcons

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
addcon 9.1.100.100 pubsbpx2 9.1.102.102
```

Description

Add a standard ABR connection with VSVD and no Default Extended Parameters (which then require user input for SCR, MBS, and so on).

System Response

```
pubsbpx1       TN    SuperUser       BPX 15    9.2 Oct. 27 1997 05:22 GMT

 From            Remote      Remote                            Route
 9.1.100.100     NodeName    Channel         State  Type       Avoid COS O
 9.1.100.100     pubsbpx2 9.1.102.102     Ok     abrstd
 9.1.102.102     pubsbpx2 9.1.100.100     Ok     abrstd









This Command: addcon 9.1.100.100 pubsbpx2 9.1.102.102 abr * * * * e e * d * * 1
* * * * * * * * *

Add these connections (y/n)?
```

Example 2

```
addcon 5.2.10.* pubsigx1p 5.1.1.100 CBR ...
```

Description

Add a virtual path connection (VPC) to virtual circuit connection (VCC) between ports 1 and 2. (This is called a “VP tunnelling connection”.)

System Response

```
pubsigx1       TN    SuperUser     IGX 8400    9.2   Oct. 27 1998 05:22 GMT

 From          Remote        Remote                                Route
               NodeName      Channel       State   Type        Avoid COS O
 5.2.10.*      pubsigx2      5.1.1.100     Ok      abrstvp
 5.1.1.100     pubsigx2      5.2.10.*    s  Ok      abrstvp









This Command: addcon 5.2.10.* pubsigx1p 5.1.1.100 CBR ...

Add these connections (y/n)?
```

Example 3

```
addcon 5.2.10.* pubsigx1p 5.1.1.100 CBR ...
```

Description

Add a

System Response

```
pubsbpx1       TN    silves BPX 8620  9.2.2G    July 21 1999 21:32 PDT

 Local           Remote      Remote                            Route
 Channel         NodeName    Channel         State  Type       Avoid COS O
 2.2.1.4         pubsbpx1    2.3.5.7         Ok     nrt-vbr
 2.2.1.5         pubsbpx1    2.3.5.8         Ok     rt-vbr
 2.2.1.6         pubsbpx1    2.3.5.9         Ok     rt-vbr
 2.3.5.7         pubsbpx1    2.2.1.4         Ok     nrt-vbr
 2.3.5.8         pubsbpx1    2.2.1.5         Ok     rt-vbr
 2.3.5.9         pubsbpx1    2.2.1.6         Ok     rt-vbr




This Command: addcon 2.2.11.11 pubsbpx1 2.3.12.12


Enter (nrt/rt-VBR,CBR,UBR,ABRSTD,ABRFST,ATFR,ATFST,ATFT,ATFTFST,ATFX,ATFXFST)
or class number:
```

clrchstats

Clears the gathered statistics for either a specific channel or all channels. When you enter a specific channel number, the current channel statistics display appears, asking if you want to clear the display. If you enter "*" (all channels) for the channel specification, the display prompts you to confirm whether you want to clear all channel statistics. This is sometimes referred to as a "summary statistics" command.

The Multilevel Channel Statistics lets you configure and display additional levels of statistics beyond level 1 statistics (for example, levels 2 and 3), as supported by the multi-level channels statistics feature. You use the **cnfcdparm** command to configure the channels statistics level on the BXM or UXM cards. For example, if you configure slot 5 to support level 3 channel statistics, all connections on that particular card are set to provide level 3 statistics. Switch software collects, displays, and propagates to Cisco WAN Manager the various statistics types. The channel statistic type vary in number and type based on the level of support provided by the BXM and UXM cards. You use the **dspchstats** and **clrchstats** to display and clear the statistics.

Full Name

Clear channel statistics

Syntax

clrchstats <channel | *>

Related Commands

dspchstats

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
clrchstats 3.1.1
```

Description

Clear channel statistics for 3.1.1.

System Response

```
sw83           TN    SuperUser       IGX 8420    9.2       Aug. 23 1997 19:24 PST

Channel Statistics: 3.1.1         Cleared: Aug. 17 1997 08:10
MIR: 3.8 kbps           Collection Time: 6 day(s) 10:04:58      Corrupted: NO
                     Frames   Avg Size Avg    Util          Packets     Avg
                              (bytes) (fps) (%)                        (pps)
From Port:          1516586        198      2   35
To Network:         1516215        198      2   35        16678365        30
Discarded:              371        198      0    0
From Network:       1518665        197      2   35        16705146        30
To Port:            1518629        198      2   35
Discarded:               36        120      0    0             238         0
                   ECN Stats:  Avg Rx VC Q:             0    ForeSight RTD    40
Min-Pk bytes rcvd:      52470  FECN Frames:             0    FECN Ratio (%)    0
Minutes Congested:          0  BECN Frames:            16    BECN Ratio (%)    0
Frames rcvd in excess of CIR:       0  Bytes rcvd in excess of CIR:         0
Frames xmtd in excess of CIR:       0  Bytes xmtd in excess of CIR:         0

This Command: clrchstats 3.1.1


OK to clear (y/n)?
```

Table 9-11 clrchstats—Parameters

Parameter	Description
channel	Specifies the channel whose statistics are cleared.
*	Specifies all channel statistics.

cnfabrparm

Configures ABR parameters for a BXM or UXM.

Full Name

Configure ABR parameters

Syntax

cnfcls <slot> <*parameters*]

Related Commands

addcon

Attributes

Privilege	1–5
Jobs	Yes
Log	Yes
Node	BPX, IGX
Lock	Yes

Example 1

`cnfabrparm 2`

Description

Configure ABR parameters for the BXM in slot 2.

System Response

```
sw60           TN    SuperUser       BPX 15    9.2 Date/Time Not Set

ABR Configuration for BXM in slot 2

CI Control         : Y
Egress ER Stamping : N










Last Command: cnfabrparm 2 Y N


Next Command:
```

Table 9-12 cnfabrparm—Parameters

Parameter	Description
slot	Specifies the card.
CI Control	
Egress ER stamping	

cnfatmcls

The **cnfatmcls** command allows the ten Cisco-supplied class templates for ATM connection configuration to be modified. (The **addcon** command can take a class as an input).

When you enter the number of the class to configure, the display shows the current value of each parameter in the class. For each item in the class, a prompt appears for changing or keeping the current value.

In Release 9.2.20, you can use **cnfatmcls** and **cnfcls** to configure the rt-VBR ATM connection class. You can use **dspatmcls** and **dspcls** to display the connection parameters for the rt-VBR and nrt-VBR connection classes.

The rt-VBR connections are configured per class 3 service parameters, and nrt-VBR connections are configured per class 2 service parameters. You can change these class parameters by using the **cnfcls/cnfatmcls** command, or you can enter the parameters individually for each connection by specifying 'yes' to the extended parameters prompt of the **addcon** command.

Note For a new node running software Release 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node will retain existing connection classes. Therefore, it won't have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command. For nrt-VBR connections in a new node, running 9.2.20, a number of connection classes are pre-configured, including 2, 4, 5, and 6.

Full Name

Configure class

Syntax

cnfatmcls <class number> [*optional parameters*]

Related Commands

addcon, cnfatmcls, dspatmcls, cnfcls, dspcls

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
cnfatmcls 10
```

Description

Configure ATM connection class 10. The command line interface (CLI) displays the current settings and requests the class type (see System Response 1). After you enter a class type, the CLI prompts you to specify each parameter for the selected class type (ABRSTD as System Response 2 shows).

System Response 1

```
sw60          TN    SuperUser       BPX 8620    9.2 Date/Time Not Set

                        ATM Connection Classes
Class: 10                                                    Type: CBR
   PCR(0+1)     % Util       CDVT(0+1)         Policing
 4000/4000     100/100      10000/10000            4

       Description: "Default CBR 4000"








This Command: cnfatmcls 10


Enter class type (rt-VBR, nrt-VBR, UBR, CBR, ATFST, ATFR, ABRSTD, ABRFST, ATFT, ATFX,
ATFTFST, ATFXFST):
```

System Response 2

```
sw60          TN    SuperUser       BPX 8620    9.2 Date/Time Not Set

                        ATM Connection Classes
Class: 10                                                    Type: ABRSTD
   PCR(0+1)     % Util      MCR           CDVT(0+1)        AAL5 FBTC
 4000/4000     100/100  4000/4000        10000/10000            n

       Description: "Default CBR 4000"







This Command: cnfatmcls 10 abrstd * * * * *


Do you want this change (y/n)?
```

Example 2

`cnfatmcls 3`

Description

Configure ATM connection class 3 for rt-VBR class type connection parameters. The command line interface (CLI) displays the current settings and requests the class type.

System Response 3

```
sw60           TN    SuperUser       BPX 8620    9.2 Date/Time Not Set

                        ATM Connection Classes
Class: 3                                                   Type: rt-VBR
   PCR(0+1)     % Util       CDVT(0+1)         AAL5 FBTC       SCR
 2000/2000     100/100      10000/10000          n           2000/2000

 MBS       Policing
1000/1000       3

       Description: "Default rt-VBR 2000"







This Command: cnfatmcls 3


Enter class type (rt-VBR, nrt-VBR, UBR, CBR, ATFST, ATFR, ABRSTD, ABRFST, ATFT, ATFX,
ATFTFST, ATFXFST):
```

Table 9-13 cnfatmcls–Parameters

Parameter	Description
class	Specifies the class to configure. The class numbers are 1–10.

Table 9-14 cnfatmcls–Optional Parameters

Parameter	Description
optional parameters	Individual parameters are specific to the type of connection (rt-VBR, nrt-VBR, CBR, UBR, ATFST, ATFR, ABRSTD, ABRFST, ATFT, ATFX, ATFTFST, ATFXFST). Each is prompted one at a time. Refer to the **dspcls** command to see the parameters in each of the classes.

cnfcls

The **cnfcls** command allows the ten Cisco-supplied class templates for connection configuration to be modified. (The **addcon** command can take a class as an input).

When you enter the number of the class to configure, the display shows the current value of each parameter in the class. For each item in the class, a prompt appears for changing or keeping the current value.

In Release 9.2.20, you can use **cnfatmcls** and **cnfcls** to configure the rt-VBR ATM connection class. You can use **dspatmcls** and **dspcls** to display the connection parameters for the rt-VBR and nrt-VBR connection classes.

The rt-VBR connections are configured per class 3 service parameters, and nrt-VBR connections are configured per class 2 service parameters. These class parameters can be changed using the **cnfcls/cnfatmcls** command, or the parameters can be entered individually for each connection by specifying ‘yes’ to the extended parameters prompt of the **addcon** command.

Note For a new node running software Release 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node will retain existing connection classes. Therefore, it won’t have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command. For nrt-VBR connections in a new node, running 9.2.20, a number of connection classes are pre-configured, including 2, 4, 5, and 6.

Full Name

Configure class

Syntax

cnfcls <class number> [*optional parameters*]

Related Commands

addcon, dspcls, cnfatmcls, dspatmcls

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
cnfcls 10
```

Description

Configure connection class 10. The command line interface (CLI) displays the current settings and requests the class type (see System Response 1). After you enter a class type, the CLI prompts you to specify each parameter for the selected class type (ABRSTD as System Response 2 shows).

System Response 1

```
sw60          TN    SuperUser      BPX 8620    9.2 Date/Time Not Set

                        ATM Connection Classes
Class: 10                                                         Type: CBR
   PCR(0+1)     % Util      CDVT(0+1)        Policing
 4000/4000     100/100     10000/10000           4

       Description: "Default CBR 4000"







This Command: cnfcls 10


Enter class type (VBR, CBR, UBR, ABRSTD, ABRFST, ATFR):
```

System Response 2

```
sw60          TN    SuperUser      BPX 8620    9.2 Date/Time Not Set

                        ATM Connection Classes
Class: 10                                                         Type: ABRSTD
   PCR(0+1)     % Util      MCR           CDVT(0+1)        AAL5 FBTC
 4000/4000     100/100  4000/4000        10000/10000            n

       Description: "Default CBR 4000"







This Command: cnfcls 10 abrstd * * * * *


Do you want this change (y/n)?
```

An example of a **cnfcls/cnfatmcls** command and response is shown in the following example:

System Response 3

```
pubsbpx1       TN    silves:1       BPX 8620 9.2.2G    July 16 1999 10:42 PDT

                        ATM Connection Classes
Class: 2                                                       Type: nrt-VBR
   PCR(0+1)     % Util       CDVT(0+1)       AAL5 FBTC        SCR
 1000/1000     100/100      10000/10000          n        1000/1000

     MBS         Policing
 1000/1000           3

       Description: "Default nrt-VBR 1000 "



This Command: cnfcls atm 2


Enter class type (rt-VBR, nrt-VBR, CBR, UBR, ABRSTD, ABRFST, ATFR, ATFST, ATFT,
ATFTFST, ATFX, ATFXFST):
```

Table 9-15 cnfcls–Parameters

Parameter	Description
class	Specifies the class to configure. The class numbers are 1–10.

Table 9-16 cnfcls–Optional Parameters

Parameter	Description
optional parameters	Individual parameters are specific to the type of connection (CBR, rt-VBR, nrt-VBR, ABR, ATFR). Each is prompted one at a time. Refer to the **dspcls** command to see the parameters in each of the classes.

cnfcon

Configures the ATM bandwidth parameters for a specified connection. The initial cell rate (ICR) normally is set to the port speed. It may be lower if other constraints exist on the data generation rate. If ICR is too low, cells are dropped. If it is too high, bandwidth may be wasted unless ForeSight is used. Statistical reports are the best source of information for deciding what to adjust.

If the connection type includes ForeSight (abr enabled), the results of the last test round trip delay command (**tstdelay**) appear. Note that this is not the current RTD but the result of the last test that ran. Connection priority — high or low — is displayed for standard Frame Relay connections and ForeSight connections. Several checks are done on the parameters that specify bandwidth to assist users in efficient use of network bandwidth. The following messages describe the performance evaluation.

- Error Min cannot exceed peak.
- Warning Min exceeds this port's speed.
- Warning Sum of mins exceeds port's speed.
- Warning Peak exceeds this port's speed.

Warning messages are informational only, so the related operation continues. If an error message appears, the operation does not continue.

Full Name

Configure connection

Syntax

cnfcon <slot.port.vpi.vci> [bandwidth parameters]

Related Commands

addcon, dspcon

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

```
cnfcon 12.1.1.6
```

Description

Configure ASI port 12.1.1.6.

System Response

```
a20          LAN   SuperUser       BPX 15    9.2     Aug. 29 1997 11:43 PST

Conn:  12.1.1.6         ca19        4.1.1.6           ABR
Description:

    SCR           IBS         MBS     ABR     MCR          PCR           ICR
 100/100        10/10       10/10     y     10/10    96000/96000      10/10

ICR TO Rate Up Rate Dn Rate FastDn Max Adjust    VC Qdepth     EFCI     % Util
  10      100     100       100        100      64000/64000   100/100   100/100

CLP   CLP Hi    CLP Lo
 y   100/100    90/90




This Command: cnfcon 12.1.1.6

MBS (10) must exceed IBS (10)
Enter the MBS [10/10]:
```

Table 9-17 cnfcon—Parameters

Parameter	Description
channel	Specifies the connection to configure. This command configures one connection at a time. The channel specification has the following format: slot.port.vpi.vci

Table 9-18 cnfcon—Optional Parameters

Parameter	Description
bandwidth parameters	Refer to the **addcon** command in this chapter for descriptions and connection types.

cnfport

Configures the parameters of an ATM port on an ASI or BXM card on the BPX or a UXM card on the IGX. Press Return to keep the current value of a parameter. See the parameter table for important information.

Previous to Release 9.2, on the BXM card, only ABR VSVD connections are subject to VC scheduling policies on the egress and that is only when the FCES (external segment) option is enabled. With the introduction of traffic shaping, you can choose whether to perform VC scheduling on CBR, VBR, and UBR traffic streams.

In this release, the Ports and Trunks feature lets you configure multiple trunk lines and circuit lines on a single BXM or UXM card simultaneously. In previous releases, when you upped a single port as a trunk (by using the **uptrk** command), all the remaining ports on that card were treated as a trunk. Similarly, when you up a single port as a circuit line (by using the upln command), all the remaining ports on the card are treated as circuit line ports. This feature allows BXM and UXM cards to be trunk line cards as well as circuit line cards at the same time. This allows trunks as well as circuit lines to coexist on these interface cards.

Feature Mismatching to Verify LMI/ILMI Support

The **cnfport** commands, in addition to other configuration commands, perform mismatch verification on the BXM and UXM cards. For example, the **cnfport** command will verify whether the cards both have LMI/ILMI configured.

The command **cnfport** will prevent disabling ILMI protocol on a port interface, if a VSI ILMI session is active on a VSI partition on the port interface and configure ILMI protocol running on a port interface to run on the BCC instead of the BXM.

Refer to “Feature Mismatching” section on page 18-1 for more information on Feature Mismatching in Release 9.2; also refer to Table 18-1, “Upgrading Firmware when Single Active Card and Y-Cable Are in Use”.

The Feature Mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Traffic Shaping on the UXM Card in Release 9.2

Traffic shaping lets you choose whether to have VC scheduling performed to your CBR, VBR, and UBR traffic streams. You can configure the traffic shaping (which involves weighted fair queuing) option on each BXM interface. A cnfport parameter will prompt you to enable/disable traffic shaping. (The default is for traffic shaping to be disabled.)

Traffic shaping is performed on a per-port basis. When traffic shaping is enabled, all traffic exiting the port is subject to the VC scheduling based on the appropriate service parameters you provision. When a particular port is configured to perform traffic shaping, all ATM cells, regardless of class of service, pass through the VC queues before leaving the card. Where a port is not configured for traffic shaping, the CBR, VBR, and UBR PVCs circumvent the VC queues and are scheduled by the Qbins.

No connections should exist on the port before changing the port traffic shaping parameter. If there are existing connections when the port traffic shaping parameter is toggled, then these connections will not be updated unless the card is reset, connections are rerouted, a switchcc occurs, or you modify the connection parameters. Also, traffic shaping is not enabled on a VSVC endpoint if an external segment has been enabled.

Redundant cards must both support traffic shaping, or neither support traffic shaping. In the non-redundant case, traffic shaping is configurable regardless of whether the BXM card in the target slot supports traffic shaping. If the card does not support traffic shaping, then a BXM card that does support traffic shaping can be inserted later and the traffic shaping configuration will take effect. System software will not perform "mismatch" checking on the traffic shaping capabilities of the BXM.

The traffic shaping rate parameters are in Table 9-18. The MCR is the minimum cell rate for the connection. This is the lowest rate that the connection will be scheduled from the VC queue into the Qbin. The PCR is the peak cell rate, or the highest rate at which the connection will be scheduled from the VC queue into the Qbin.

Table 9-19 cnfport—Traffic Shaping Rates

Service Type	MCR	PCR
CBR	PCR	PCR
VBR	SCR[1]%Util	PCR
UBR	0	PCR
ABR	MCR %Util	PCR

1 Indicates that the system software issues a warning that traffic shaping is not supported on that specific BXM.

Note that traffic shaping does not generate any alarms. There is no mismatch checking for BXMs that support traffic shaping, so if you insert a BXM card with firmware that does not support it, then the traffic shaping functionality will not exist.

Also, cells can be momentarily received out of order when you reconfigure connections between traffic shaping and non-traffic shaping. This is a limitation of the hardware for which there is no workaround.

Configuring Traffic Shaping

Traffic shaping involves passing ATM traffic through the ATM interface at a VC queue, scheduled rate. Currently, in the BXM-only ABR VSVD connections are subject to VC scheduling policies. With the introduction of traffic shaping, the customer will have the option to perform VC scheduling to his/her CBR, VBR, and UBR traffic streams. Traffic shaping is performed by the BXM hardware.

Traffic shaping will be performed on a per-port basis. When enabled, all traffic exiting the port will be subject to the VC scheduling based on the appropriate service parameters provisioned by the user. Note that all ATM cells, regardless of class of service, pass through the VC queues before leaving the card.

No connections should exist on the port before you change the port traffic shaping parameter. If there are existing connections when you toggle the port traffic shaping parameter, then these connections will not be updated unless you reset the card (by using the **resetcd** command), connections are rerouted, a **switchcc** occurs, or you modify the connection parameters. Also, it should be noted that traffic shaping is not enabled on a VSVD endpoint if external segment has been enabled.

Switch software requires that redundant cards either both support the feature or neither supports the feature. In the non-redundant case, the feature is configurable regardless of whether the BXM card in the target slot supports traffic shaping[1]. If the card does not support the feature, then you can insert

1. Indicates that switch software issues a warning that traffic shaping is not supported on that specific BXM.

a BXM card that does support traffic shaping and the traffic shaping configuration will take effect. Switch software will not perform “mismatch” checking on the traffic-shaping capabilities of the BXM.

Redundancy Architecture

Software requires that redundant cards either both support the feature or neither supports the feature. In the non-redundant case, the feature is configurable regardless of whether the BXM card in the target slot supports traffic shaping. If the card does not support the feature, then a BXM card that does support traffic shaping can be inserted later and the traffic shaping configuration will take effect. Switch software will not perform “mismatch” checking on the traffic-shaping capabilities of the BXM.

Cisco WAN Manager in Release 9.2 has no changes to support traffic shaping. Switch software functionality is limited to enabling the traffic shaping option (involving weighted fair queuing) on a per-BXM interface case. The cnfport command has a new parameter which will prompt you to enable or disable traffic shaping. The parameter default is to disable the feature.

Refer to the WAN Switch Software Release 9.2 release notes for additional information on traffic shaping. No connections should be on the port before changing the port traffic shaping parameter. If there are existing connections when the port traffic shaping parameter is toggled, then these connections will not be updated unless the card is reset, connections are rerouted, a **switchcc** occurs, or you modify the connection parameters*. Also, it should be noted that traffic shaping is not enabled on a VSVD endpoint if an external segment has been enabled. In this case, the scheduling policies are based upon the ATMF 4.0 ABR rules.

The MCR is the minimum cell rate for the connection. This is the lowest rate that the connection will be scheduled from the VC queue into the Qbin. The PCR is the peak cell rate, or the highest rate at which the connection will be scheduled from the VC queue into the Qbin.

Firmware Functionality (BXM)

The BXM firmware supports a new Commbus parameter to enable/disable traffic shaping. When you add a connection, the BXM firmware checks its database to see if traffic shaping is enabled for the port that the connection is to be mapped to. If traffic shaping is enabled, the BXM firmware sets up the ASIC hardware to perform the weighted fair queuing. In the background, the BXM firmware runs a rate-based algorithm.

Existing functionality, such as VC queuing, is used by the traffic shaping feature.

In this release, the BXM firmware supports a new CommBus (CBUS) parameter to enable/disable traffic shaping. When a connection is added, the BXM firmware checks its database to see if traffic shaping is enabled for the port that the connection is to be mapped to. If traffic shaping is enabled, the BXM firmware sets up the ASIC hardware to perform the weighted fair queuing. In the background, the BXM firmware runs a rate-based algorithm similar to what is done today for ERS (explicit rate stamping). The only other interface change includes an egress SCR parameter in the channel (0x52) message.

The algorithm executed by the firmware involves the BXM firmware polling the cell arrival and transmit counters of the qbins approximately every 15 msec. During this time, the firmware determines the congestion ratio:

— rc = rp * out/in

where rp is the previous value of rc, “out” is the number of cells leaving the QBIN, and “in” is the number of cells arriving into the QBIN. Note that if the ratio of out/in is less than 1, then the QBIN is experiencing congestion. The BXM firmware takes the resulting “rc” and divides this value into the sum of all of the PCRs for the Qbin and uses this result as the congestion factor to be programmed into the hardware (SABRE).

Performance of Traffic Shaping

The weighted-fair queuing (WFQ) algorithm for traffic shaping runs the same algorithm as the explicit rate stamping (ERS). Today, this processing consumes 12 percent. Because the algorithm runs once (even if both ERS and WFQ are enabled), traffic shaping will not increase the worst-case demand for BXM processor time.

Errors and Alarm Handling

No alarms will be generated regarding the Traffic Shaping feature. As previously mentioned, there is no mismatch checking for BXMs that do not support the feature, so if you insert a BXM with firmware that does not support the feature, then the traffic shaping functionality will not be supported on that card.

It should be noted that cells can be momentarily received out of order when connections are reconfigured between traffic shaping and non-traffic shaping. This is a limitation of the hardware for which there is no work-around.

Full Name

Configure port

Syntax

cnfport <port> [<params>]

Related Commands

upport, dnport, dspport, dspports

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	BPX, IGX
Lock	Yes

Example 1

```
cnfport 12.1 N N N H N N
```

Description

Configure port 12.1 to have a UNI cell header format; not to be an MGX 8220 shelf; not to have a Metro Cell Header format; shift on HCF; use no protocol; and not to apply %util.

System Response

```
batman          TN    SuperUser       BPX 15    9.2      Date/Time Not Set

Port:       12.1
Interface:          T3-2
Type:               UNI                         %Util Use:        Disabled
Speed:              96000
Shift:              SHIFT ON HCF (Normal Operation)
VBR Queue Depth:    1000

Protocol:           NONE






Last Command: cnfport 12.1 N N N H N N


Next Command:
```

Table 9-20 cnfport—Parameters

Parameter	Description
slot.port	Specifies the ASI, BXM, or UXM card slot and port number.
nni/uni	Specifies whether the cell header format is NNI or UNI. UNI is the default.
axis	Specifies MGX 8220 queue depth for each slot.
metro data cell header	Specifies whether the metro data cell header type is used.

Table 9-20 cnfport—Parameters (Continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>shift h | n</td><td>
Specifies whether a one-byte shift on the HCF field of the cell header occurs. The choice of H (shift) or N (no shift) depends on whether the ATM cloud includes non-Cisco WAN Switching nodes and whether virtual trunking is in operation:

You typically select H (the default, or Shift on) if the cloud includes non-Cisco WAN Switching nodes or if only a physical trunk is configured for the ASI port.
You typically select N (Shift off) if virtual trunks are configured and the ATM cloud consists of Cisco WAN Switching nodes only.

For BPX or IGX ports performing virtual trunking within an ATM cloud to external Cisco equipment, ports should be configured to Shift on (that is, Shift h) for BNI cards; BXM ports should typically be configured to Shift off (Shift n).
Note For UXM cards, you cannot configure the Shift parameter—the Shift setting is always N, or Shift off.
For example, if the public ATM cloud consists of BPX nodes, the access points to the cloud might be ASI ATM-UNI ports. Because the cells transmitted to the ASI trunk interface are coming from a Cisco device, for example, a BNI card, the 16 VCI bits have already been left shifted by four (4) bits and contain 12 bits of VCI information and four (4) bits of ForeSight information. Therefore, the ASI cards at either end of the cloud should be configured to not shift (that is, Shift off). In this case, you would configure “shift n” on the ASI port.
If the ATM cloud consists of non-Cisco nodes, then the 12 VCI + 4 bits ForeSight bits in the cells coming from the BNI card in the BPX are then passed through untouched as 16 VCI bits. Because it is a non-Cisco network, the ForeSight bits are ignored.
Make sure that you set the HCF field correctly for your network configuration before you add connections. For example, if you are acting as a service provider, and one of your customers wants to configure virtual trunking through the network, if your ports have been previously configured with the incorrect HCF shift field setting, you may need to go back and delete all the connections from each port, configure the port, and add the connections again.
Below shows some guidelines on how to set the Shift parameter when using BNI virtual trunking through a cloud of Cisco equipment using BXMs, and a cloud using ASIs and BNIs. Also shown is how to set the Shift parameter when using either BXM or UXM virtual trunking through a cloud of Cisco equipment (BXM cards), and a cloud of ASIs and BNIs.
<table>
<tr><th></th><th>Non-Cisco cloud</th><th>Cisco BXM Cloud</th><th>Cisco ASI/BNI Cloud</th></tr>
<tr><td>BNI VT</td><td>X</td><td>No shift</td><td>No shift</td></tr>
<tr><td>BXM/UXM VT</td><td>X</td><td>No shift</td><td>Shift</td></tr>
</table>
Refer to the section “Overview of Virtual Trunking” section on page 4-4 for more information on virtual trunking and how to set the HCF Shift field.
</td></tr>
<tr><td>protocol</td><td>Specifies the use of either an LMI protocol, an ILMI protocol, or no specified protocol. No specified protocol is the default.</td></tr>
</table>

Table 9-20 cnfport—Parameters (Continued)

Parameter	Description
%util	Enables/disables percent utilization. This parameter supports ATM VBR/ABR fairness for ASI terminated connections and applies to only VBR and ABR connections. To change the %util status of a port, no connections can be currently terminating on the port. Therefore, if connections terminate on the port, they must be deleted before **cnfport** execution then re-added after execution of **cnfport**. When this feature is disabled, the port queue bandwidth is calculated using the sum of the MCRs or PCRs for the connections terminating on the port. This is identical to the port queue bandwidth calculation prior to the implementation of the %util feature. The port queue bandwidth with %util feature *disabled* is: • For ABR connections Port Queue BW = sum (MCR) • For VBR connections Port Queue BW = sum (PCR) • For CBR connections Port Queue BW = sum (PCR) When the %util feature is enabled, the port queue bandwidth is calculated for ABR and VBR connections as follows: for ABR connections, the port queue bandwidth is the sum of a percentage of the MCRs for the connections terminating on the port; for VBR connections, the port queue bandwidth is the sum of a percentage of the PCRs for connections terminating on the port. The feature is not applied to CBR connections. In summary, the port queue bandwidth with feature %util *enabled* is: • For ABR connections Port Queue BW = sum (MCR * %util) • For VBR connections Port Queue BW = sum (PCR * %util) • For CBR connections Port Queue BW = sum (PCR)

cnfportq

Configures queue parameters for a port on an ASI or BXM card on the BPX or a UXM card on the IGX. Pressing the Return key keeps the current value for the parameter.

In Release 9.2.20, the VBR class of service type can be either rt-VBR or nrt-VBR, depending on the way the corresponding port (service) queues (both ingress and egress) are configured. For the nrt-VBR class of service type in this release, the corresponding service queues are larger than in previous releases to provide more efficient bandwidth sharing with other non-real time service types. The service queues for both rt-VBR and nrt-VBR service types can be configured on a node-by-node basis.

You can use **cnfportq** to configure qbin values separately for rt-VBR and nrt-VBR connection types on ports. (To configure the qbin values for rt-VBR and nrt-VBR classes of service on trunks, use **cnftrkparm**.) The rt-VBR and nrt-VBR connections use different queues on a port: these are the rt-VBR and nrt-VBR queues, respectively. (See Example 3 for a **cnfportq** screen showing the configuration parameters available for a port queue.)

For information on configuring trunk queues used by rt-VBR and nrt-VBR connections, see the **cnftrkparm** command.

Configuring Port Queues used by rt-VBR and nrt-VBR Connections

The rt-VBR and nrt-VBR connections use different queues on a port, these are the rt-VBR and nrt-VBR queues, respectively. You can configure these separately, using the **cnfportq** command.

See Example 2 for a sample **cnfportq** screen showing configuration parameters available for a port queue.

Full Name

Configure port queue parameters

Syntax

cnfportq <port> [<params>]

Related Commands

upport, dnport, dspportq

Attributes

Privilege	2
Jobs	Yes
Log	Yes
Node	BPX, IGX
Lock	Yes

Example 1

cnfportq 4.2 200 80 60 80 1000 80 60 80 9800 80 60 80

Description

Configure port 4.2 to the parameters indicated.

System Response

```
ca19           VT    SuperUser       BPX 8620   9.2    June 23 1999 19:11 GMT

   ASI-T3

Port:       4.2     [ACTIVE]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)
SVC Queue Pool Size:              0
CBR Queue Depth:                200     rt-VBR Queue Depth:               1000
CBR Queue CLP High Threshold:     80%     rt-VBR Queue CLP High Threshold:    80%
CBR Queue CLP Low Threshold:      60%     rt-VBR Queue CLP Low Threshold      60%
CBR Queue EFCI Threshold:         80%     rt-VBR Queue EFCI Threshold         80%
nrt-VBR Queue Depth:             1000     UBR/ABR Queue Depth:              9800
nrt-VBR Queue CLP High Threshold: 80%     UBR/ABR Queue CLP High Threshold:    80%
nrt-VBR Queue CLP Low Threshold: 60%     UBR/ABR Queue CLP Low Threshold:     60%
nrt-VBR Queue EFCI Threshold:     80%     UBR/ABR Queue EFCI Threshold:        80%



Last Command: cnfportq 4.2 N N N 200 80 60 80 1000 80 60 80 9800 80 60 80


Next Command:
```

Example 2

cnfportq 2.2

Description

Configure the port queue parameters on port 2.2.

System Response

```
pubsbpx1       TN    silves:1        BPX 8620 9.2.2G    July 16 1999 10:47 PDT

Port:       2.2     [ACTIVE ]
Interface:          LM-BXM
Type:               UNI
Speed:              353208 (cps)

SVC Queue Pool Size:          0
CBR Queue Depth:              600     rt-VBR Queue Depth:               0
CBR Queue CLP High Threshold: 80%     rt-VBR Queue CLP High Threshold:   80%
CBR Queue CLP Low Threshold:  60%     rt-VBR Queue CLP Low/EPD Threshold: 60%
CBR Queue EFCI Threshold:     60%     rt-VBR Queue EFCI Threshold:       80%
nrt-VBR Queue Depth:          5000    UBR/ABR Queue Depth:              20000
nrt-VBR Queue CLP High Threshold: 80% UBR/ABR Queue CLP High Threshold:  80%
nrt-VBR Queue CLP Low Threshold:  60% UBR/ABR Queue CLP Low/EPD Threshold:60%
nrt-VBR Queue EFCI Threshold: 60%     UBR/ABR Queue EFCI Threshold:      20%


This Command: cnfportq 2.2
```

Table 9-21 cnfportq—ASI Parameters

Parameter	Description
slot.port	Specifies the ASI card slot and port number.
nni/uni	Specifies whether the cell header format is NNI or UNI. UNI is the default.
cbr queue parms	Specifies the CBR queue parameters of depth, cbr-hi, cbr-lo, and efci. The ranges are 0 to 24000 for depth and 0 to 100% for all others.
nrt-vbr queue parms	Specifies the nrt-VBR queue parameters of depth, vbr-hi, vbr-low, and efci. The ranges are 0 to 24000 for depth and 0 to 100% for all others.
rt-vbr queue parms	Specifies the rt-VBR queue parameters of depth, vbr-hi, vbr-low, and efci. The ranges are 0 to 24000 for depth and 0 to 100% for all others.
ubr/abr queue parms	Specifies the ABR queue parameters of depth, abr-hi, abr-low, and efci. The ranges are 0 to 24000 for depth and 0 to 100% for all others.

Table 9-22 cnfportq—UXM Parameters

Parameter	Description
slot.port	Specifies the UXM card slot and port number.
nni/uni	Specifies whether the cell header format is NNI or UNI. UNI is the default.

Table 9-22 cnfportq—UXM Parameters (Continued)

Parameter	Description
cbr queue parms	Specifies the CBR queue parameters of depth, cbr-hi, cbr-lo, and efci. The ranges are 0 to 97250 for depth and 0 to 100% for all others.
nrt-vbr queue parms	Specifies the nrt-VBR queue parameters of depth, vbr-hi, vbr-low, and efci. The ranges are 0 to 97250 for depth and 0 to 100% for all others.
rt-vbr queue parms	Specifies the rt-VBR queue parameters of depth, vbr-hi, vbr-low, and efci. The ranges are 0 to 97250 for depth and 0 to 100% for all others.
ubr/abr queue parms	Specifies the ABR queue parameters of depth, abr-hi, abr-low, and efci. The ranges are 0 to 97250 for depth and 0 to 100% for all others. UBR traffic shares this queue with the ABR traffic.

Note The total queue size of the UXM card is 97250 cells.

delcon

Removes connections from the network. The same command with differing syntax may be used to delete voice connections, data connections, Frame Relay connections, or ATM connections. The syntax in this section deletes an ATM connection. You can verify connection deletions by using the **dspcons** command.

In Release 9.2.20, you can use **delcon** to delete data or FRP connections that are terminated on UXM/UXM-E cards for IGX 8400 interface shelves, and terminated on routing network feeder trunks for IGX 8400 routing nodes.

Full Name

Delete connections

Syntax

delcon <channel(s)>

Related Commands

addcon, dspcon, dspcons

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IGX, BPX
Lock	Yes

Example 1

`delcon 4.1.1.4`

Description

Delete connection 4.1.1.4. The connections to delete are highlighted, and a prompt appears asking you to confirm the deletion. Respond with “y”, for yes, and connection 4.1.1.4 is deleted.

System Response

```
ca19          VT    SuperUser       BPX 15    9.2    Aug. 23 1997 20:36 GMT

 Local           Remote      Remote                              Route
 Channel         NodeName    Channel         State  Type         Avoid COS O
 4.1.1.4         ca20        12.1.1.4        Ok     CBR                  0  R
 4.1.1.5         ca20        12.1.1.5        Ok     VBR                  0  R
 4.1.1.6         ca20        12.1.1.6        Ok     ABR                  0  R
 4.1.1.7         ca20        12.1.1.7        Ok     VBR                  0  R
 4.2.1.1         ca20        12.2.1.1        Ok     CBR                  0  L
 4.2.1.2         ca20        12.2.1.2        Ok     VBR                  0  L
 4.2.1.3         ca20        12.2.1.3        Ok     ABR                  0  L







Last Command: delcon 4.1.1.4

Delete connections? (y)
Next Command:
```

Table 9-23 delcon—Parameters

Parameter	Description
channel	Specifies the channel or set of channels for deleting connections. <channel> is specified in the following format: slot.port.vpi.vci

dnport

Deactivates (or "downs") the specified ATM port. Before downing a port, you must remove all connections from the port.

Full Name

Down port

Syntax

dnport <port>

Related Commands

cnfport, dspport, upport

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	BPX, IGX
Lock	Yes

Example 1

```
dnport  4.2
```

Description

Down port 4.2.

System Response

```
ca19           VT    SuperUser       BPX 15    9.2    Aug. 23 1997 19:49 GMT

ASI Port States
Port  State
4.1   ACTIVE
4.2   INACTIVE











Last Command: dspports


Next Command: dnport 4.2
```

Table 9-24 dnport—Parameters

Parameter	Description
port	Specifies the slot number and port number in the format *slot.port.*

dspatmcls

Displays the current parameters for an ATM connection class template. The number of classes is ten. The parameters and the values for each varies with the type of connection (CBR, VBR, ABR, and ATFR).

In Release 9.2.20, both the **dspatmcls** and **dspcls** commands display

Full Name

Display ATM connection class

Syntax

dspatmcls <class number>

Related Commands

addcon, cnfatmcls, dspcls, cnfcls, dspcon, dspcons

Attributes

Privilege	1–2
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

```
dspatmcls 1
```

Description

Display the parameters for configuration class 1.

System Response

```
night          TN    SuperUser       BPX 8620    9.2    July 28 1997 13:22 GMT

                        ATM Connection Classes
Class: 1
Type: VBR

UPC       SCR           IBS           MBS      ABR       PCR          ABR PCR
 y     500/500        10/10       1000/1000     -    500/500           -/-

     ICR        ICR TO Rate Up Rate Dn Rate FastDn Max Adjust    CDVT[in cells]
     -/-          -       -       -         -          -        64000/64000

 EFCI    % Util FGCRA      MFS      CLP  CLP Hi  CLP Lo   BCM
100/100  100/100  n/n       -/-       y  100/100 100/100   n/n

       Description: "Default VBR 500"


Last Command: dspatmcls 1


Next Command:
```

Example 2

dspatmcls 1

Description

Display the parameters for configuration class 1.

System Response

```
night          TN    SuperUser       BPX 8620    9.2    July 28 1997 13:22 GMT

                  ATM Connection Classes
Class: 3                                        Type: rt-VBR
PCR(0+1)     %Util       CDVT(0+1)        AAL5 FBTC       SCR
2000/2000    100/100     10000/10000        n           2000/2000

  MBS        Policing
1000/1000       3


       Description: "Default rt-VBR 2000"



Class:  4                                        Type:  rt-VBR
PCR(0+1)     %Util       CDVT(0+1)        AAL5 FBTC       SCR
8000/8000    100/100     10000/10000        n           8000/8000

  MBS        Policing
1000/1000       3


       Description: "Default nrt-VBR 8000"

Last Command: dspatmcls 1


Next Command:
```

Table 9-25 dspatmcls—Parameters

Parameter	Description
class number	Specifies the class whose current parameters you want to see. Values are 1–10.

dspchstats

Displays statistics for a channel. You can specify an optional parameter *interval*, and the statistics display will be refreshed by the number of seconds you specify. (You can press the Delete key to stop the screen refresh.) If you do not specify the *interval* parameter, the screen refresh interval defaults to 10 seconds.

In this release, the multilevel channels statistics feature provides additional levels of channel statistics configuration for the BXM/UXM cards. You can use the **cnfcdparm** command to configure the channel statistic level on the BXM and UXM cards. For more information see the **cnfcdparm** command description.

Full Name

Display channel statistics

Syntax

dspchstats <channel> [interval]

Related Commands

clrchstats

Attributes

Privilege	5
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Table 9-26 dspchstats— field descriptions

Field	Description
From the Port	Entering a port, typically from an external device/box.
To the Network	Going out of the switch; typically trunks.
Discarded	Received from the attached device but not transmitted to the network.
From the Network	Received in; typically, into the trunk.
To the Port	Transmitted out of the port, to an external device or cloud
Discarded	Received from the network but not transmitted to the attached device.

Example 1

```
dspchstats 4.1.50.1
```

Description

Display the channel statistics for connection 4.1.50.1.

System Response

```
night          TN    SuperUser       BPX 15    9.2     July 17 1997 02:46 GMT

Channel Statistics for 4.1.50.1    Cleared: July 13 1997 02:53 (|)
MCR: 0 cps              Collection Time: 0 day(s) 18:10:22      Corrupted: NO
   Traffic      Cells      CLP      Avg CPS   %util  Discards:        Cells
From Port   :     14710          0        0       0  VcQ > CLP:            0
To Network  :     14710    ---            0       0  VcQ Full :            0
From Network:     14710    ---            0       0  Qbin Full:            0
To Port     :     14710      14710        0       0  Qbin> CLP:            0
                                                     Failed   :        14710
                            OAM          Cells       RsrcOVL  :            0
VC Q        :         0   Tx OAM :          29608    NonCompliant:         0
Rx EFCI     :         0   Rx AIS :          14710
Tx EFCI     :         0   Rx FERF:              0    ForeSight       Cells
                          Rx BCM :              0     Adj Up :             0
                          Tx BCM :              0     Adj Dn :             0
AAL-5 Frames:         0                               Adj Fdn:             0

This Command: dspchstats 4.1.50.1


Hit DEL key to quit:
```

Example 2

dspchstats 13.1.100 10

Description

Display statistics for connection 13.1.100 with a 10-second interval between screen updates. The card in slot 13 is an ALM/A.

System Response

```
sw142          TN    SuperUser       IGX 16    9.2 July 31 1997 14:38 PDT

Channel Statistics: 13.1.100      Cleared: July 31 1997 11:50   (/)
MCR:   150 cps          Collection Time: 0 day(s) 00:00:00      Corrupted: NO

                  Cells         Avg       Util
                               (cps)       (%)

From Port:            0           0          0
To Network:           0           0          0
Discarded:            0           0          0
From Network:         0           0          0
To Port:              0           0          0
Discarded:            0           0          0




This Command: dspchstats 13.1.100


Hit DEL key to quit:
```

Example 3

dspchstats 9.2.1.100

Description

Display statistics for connection 9.2.1.100. The card in slot 9 is a UXM.

System Response

```
sw199          TN    SuperUser       IGX 16    9.0.s6    Aug. 28 1997 09:25 PDT

Channel Statistics: 9.2.1.100                                      Snapshot
Collection Time: 0 day(s) 13:28:47                      Clrd:  08/27/97 19:47:24
Type                                      Count
Cells Received from Port                        0
Cells Transmitted to Network                    0
Cells Received from Network                     0
Cells Transmitted to Port                       0
EOF Cells Received from Port                    0
Cells Received with CLP=1                       0
Cells Received with CLP=0                       0
Non-Compliant Cells Received                    0
Average Rx VCq Depth in Cells                   0
Average Tx Vcq Depth in Cells                   0
Cells Transmitted with EFCI=1                   0
Cells Transmitted with EFCI=0                   0
Ingress Vsvd Allowed Cell Rate                  0
Egress Vsvd Allowed Cell Rate                   0
OAM state (0:OK,1:FERF,2:AIS)                   0
Good Pdu's Received by the Sar                  0
Good Pdu's Transmitted by the Sar               0
Rx pdu's discarded by the Sar                   0
Tx pdu's discarded by the Sar                   0
Invalid CRC32 pdu rx by the sar                 0
Invalid Length pdu rx by the sar                0
Shrt-Lgth Fail detected by the sar              0
Lng-Lgth Fail detected by the sar               0

Last Command: dspchstats 9.2.1.100
```

Example 4

`dspchstats 2.1.1.1 1`

Description

Display statistics for connection 2.1.1.1 (with a VPI of 1, and VCI of 1), and an interval of 1.

System Response

```
sw57           TRM   StrataCom       BPX 8620    9.2.zR    Date/Time Not Set

Channel Statistics for 2.1.1.1     Cleared: Date/Time Not Set   (\) Snapshot
MCR: 96000/96000 cps    Collection Time: 0 day(s) 00:01:45      Corrupted: NO
   Traffic      Cells      CLP      Avg CPS   %util  Chan Stat Addr: 30EBB36C
From Port   :         0          0        0       0
To Network  :         0    ---            0       0
From Network:         0          0        0       0
To Port     :         0    ---            0       0

NonCmplnt Dscd:         0  Rx Q Depth    :         0  Tx Q Depth    :         0
Rx Vsvd ACR   :         0  Tx Vsvd ACR   :         0  Bkwd SECB     :         0
Bkwd Lost Cell:         0  Bkwd Msin Cell:         0  Bkwd BIPV     :         0
Fwd SECB      :         0  Fwd Lost Cell :         0  Fwd Msin Cell :         0
Fwd BIPV      :         0

Last Command: dspchstats 2.1.1.1 1


Next Command:

                      CD                                               Minor Alarm
```

Example 5

dspchstats 10.1.205.101

Description

Display statistics for connection 10.1.205.101 (with a VPI of 205 and VCI of 101).

System Response

```
m2a            TN    StrataCom       IGX 8420    9.2.zR    May 14 1998 14:19 GMT

Channel Statistics: 10.1.205.101
Collection Time: 0 day(s) 23:02:58                    Clrd:  05/13/98 14:33:00
Type                                      Count     Traffic       Rate (cps)
Cells Received from Port                    82978   From port              0
Cells Transmitted to Network                82978   To network             0
Cells Received from Network                 82978   From network           0
Cells Transmitted to Port                   82978   To port                0
EOF Cells Received from Port                    0
Cells Received with CLP=1                       0
Cells Received with CLP=0                   82978
Non-Compliant Cells Received                    0
Average Rx VCq Depth in Cells                   0
Average Tx Vcq Depth in Cells                   0
Cells Transmitted with EFCI=1                   0
Cells Transmitted with EFCI=0               82978

This Command: dspchstats 10.1.205.101
```

Table 9-27 dspchstats—Parameters

Parameter	Description
channel	Specifies the channel for statistics display, with format of *slot.port.vpi.vci*.

Table 9-28 dspchstats—Optional Parameters

Parameter	Description
interval	Specifies the interval (in seconds) between updates of the statistics display. If you specify an interval, you can either press Delete to terminate the command or wait until the command times out. The default is 10 seconds. If the Rx Q depth and the Tx Q depth fields remain “0”, make sure that a value other than “0” is specified for the interval parameter.

Functional Description

The table provides some statistics information regarding the BXM SAR. The switch software collects miscellaneous statistics regarding the Monarch SAR (Segmentation, Assembly, and Reassembly).

SAR (Segmentation, Assembly, and Reassembly) Statistics for BXM Card

The table below provides some statistics information for SAR on the BXM card. Note that the object name typically maps to the screen field name on the **dspchstats** screen.

Table 9-29 SAR Statistics for BXM Card

Object ID	Object Name	Range/Values	Default	Description
01	Message Tag	Byte 0-3: Tag ID Byte 4-7: IP Address	0	Identifier and source IP address sent with Commbus message. Both will be copied into the response, if any is to be sent.
02	Ingress Unknown AAL5 Discards	0 - 2^{32}-1	N/A	Number of unknown AAL5 PDUs discarded in the ingress.
03	Egress Unknown ALL5 Discards	0 - 2^{32}-1	N/A	Number of unknown AAL5 PDUs discarded in the egress.
04	Ingress Frame Ready FIFO Overruns	0 - 2^{32}-1	N/A	Number of ingress frame-ready FIFO overruns.
05	Egress Frame Ready FIFO Overruns	0 - 2^{32}-1	N/A	Number of egress frame-ready FIFO overruns.
06	Ingress Frame Ready FIFO Fulls	0 - 2^{32}-1	N/A	Number of ingress frame-ready FIFO fulls.
07	Egress Frame Ready FIFO Fulls	0 - 2^{32}-1	N/A	Number of egress frame-ready FIFO fulls.
08	Ingress Frame Ready FIFO Half-Fulls	0 - 2^{32}-1	N/A	Number of ingress frame-ready half-fulls.
09	Egress Frame Ready FIFO Half-Fulls	0 - 2^{32}-1	N/A	Number of egress frame-ready half-fulls.
0A	Inverse ARP Requests Rcv	0 - 2^{32}-1	N/A	Number of inverse ARP requests received.
0B	Inverse ARP Replies Rcv	0 - 2^{32}-1	N/A	Number of inverse ARP replies received.
0C	Bad /errored ARP packets rcv	0 - 2^{32}-1	N/A	Number of invalid or unknown type ARP packets received
0D	Inverse ARP Requests Xmt	0 - 2^{32}-1	N/A	Number of inverse ARP requests transmitted.
0E	Inverse ARP Replies Xmt	0 - 2^{32}-1	N/A	Number of inverse ARP replies transmitted.

Table 9-29 SAR Statistics for BXM Card (Continued)

Object ID	Object Name	Range/Values	Default	Description
0F	Errored ARP packet Xmt	0 - 2^{32}-1	N/A	Number of invalid or unknown type ARP packets transmitted.
10	Bad LLC/NSAP PDUs Rcv	0 - 2^{32}-1	N/A	Number of illegal LLC/NSAP packets received.

dspcls

Displays the current parameters for a connection class template. The number of classes is ten. The parameters and the values for each varies with the type of connection (CBR, rt-VBR, nrt-VBR, ABR, and ATFR). (Note that connection parameters for the rt-VBR and nrt-VBR connection classes display separately.)

Full Name

Display connection class

Syntax

dspcls <class number>

Related Commands

addcon, cnfcls, dspcon, dspcons

Attributes

Privilege	1–2
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

```
dspcls 1
```

Description

Display the parameters for configuration class 1.

System Response

```
night          TN    SuperUser       BPX 8620    9.2    July 28 1997 13:22 GMT

                  ATM Connection Classes
Class: 3                                        Type: rt-VBR
PCR(0+1)     %Util       CDVT(0+1)        AAL5 FBTC       SCR
2000/2000    100/100     10000/10000        n           2000/2000

 MBS        Policing
1000/1000       3


       Description: "Default rt-VBR 2000"




Class: 4                                        Type: rt-VBR
PCR(0+1)     %Util       CDVT(0+1)        AAL5 FBTC       SCR
8000/8000    100/100     10000/10000        n           8000/8000

 MBS        Policing
1000/1000       3


       Description: "Default nrt-VBR 8000"

Last Command: dspatmcls 1


Next Command:
```

Example 2

dspcls 1

Description

Display the parameters for configuration class 1.

System Response

```
night          TN    SuperUser       BPX 15    9.2    July 28 1998 13:22 GMT

                        ATM Connection Classes
Class: 1
Type: VBR

UPC       SCR           IBS           MBS      ABR       PCR          ABR PCR
 y     500/500        10/10       1000/1000     -    500/500           -/-

     ICR        ICR TO Rate Up Rate Dn Rate FastDn Max Adjust    CDVT[in cells]
     -/-          -       -       -         -          -        64000/64000

  EFCI    % Util  FGCRA      MFS      CLP  CLP Hi  CLP Lo   BCM
100/100  100/100  n/n       -/-       y  100/100 100/100   n/n

       Description: “Default VBR 500"


Last Command: dspcls 1


Next Command:
```

Table 9-30 dspcls—Parameters

Parameter	Description
class number	Specifies the class whose current parameters you want to see. Values are 1–10.

dspcon

Displays connection information for a specified channel. The information displayed includes:

- The channel numbers for both the local and remote ends of the connection.
- The node names at both ends of the connection.
- The type or data rate of the connection.
- The routing restriction.
- Trunk cell routing restriction.
- The class of service (COS) of the connection.
- The connection route, listing the end nodes and any intermediate nodes.
- If cost-based AutoRoute is configured, displays maximum and current costs for a connection route.
- The preferred route for the connection (if configured).
- The status of the cards associated with the connection.
- Any Y-cable conflicts.
- The compression status.
- The connection bandwidth parameter values.
- The connection/type descriptor (if configured). (If the connection is a VP tunnelling DAX connection, the type is displayed as “cbrvp”, “abrstvp”, “abrfsvp”, etc.)
- The circuit round trip delay (if ForeSight is enabled).

Any failures that affect the connection flash on the screen. For Frame Relay NNI ports, the NNI value indicates the Abit value received across the NNI from the remote network. The status that may be displayed includes:

OK	Connection OK
FAILED	Connection failed
MISSING	VPI.VCI was deleted in other network at NNI. A previous status report indicated a valid VPI.VCI was present but an updated report did not.
UNUSED	Indicates the UNI port does not support reporting of NNI Abit status

Release 9.2 switch software for a IGX 8400 routing hub does the following:

- **dspcon** shows the new connection segment. Because the connection type is based on the master end of the connection (either voice, data, Frame Relay or ATM connections), the **dspcon** command displays that and shows the feeder trunk endpoint as the slave end and the incoming Abit status.
- **dspcon** indicates connection failures at feeder endpoints.

In Release 9.2.20, rt-VBR and nrt-VBR connection service types display separately.

Full Name

Display connections

Syntax

dspcon <channel>

Related Commands

addcon, cnfcon, cnfpref, cnfrtcost

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

```
dspcon 12.1.1.5
```

Description

Display connection information for channel 12.1.1.5 (a VBR connection).

System Response

```
ca20           LAN   SuperUser       BPX 15    9.2     Aug. 29 1997 10:44 PST

Conn:  12.1.1.5         ca19        4.1.1.5           VBR   Status: Down
    SCR           MBS           PCR          ABR PCR     UPC FST CLP  % util
 1000/1000       10/10        500/500        --/--       y   n   y  100/100
Owner: LOCAL  Restriction: NONE  COS: 0
Group: NONE  TestRTD: 16705 msec


Path:   Downed by user
Pref:   Not Configured



ca20          ASI-T3    : OK           ca19      ASI-T3    : OK
              Line 12.1 : OK                     Line  4.1 : OK


Last Command: dspcon 12.1.1.5


Next Command:
```

Example 2

dspcon 12.1.1.4

Description

Display connection information for channel 12.1.1.4 (CBR).

System Response

```
ca20           LAN   StrataCom       BPX 15    9.2     Aug. 29 1997 10:42 PST

Conn:  12.1.1.4         ca19        4.1.1.4           CBR   Status: Down
    PCR           CDVT          MCR         ABR PCR     UPC FST CLP  % util
  100/100        10/10         --/--         --/--       y   n   y  100/100
Owner: LOCAL  Restriction: NONE  COS: 0
Group: NONE TestRTD: 0 msec  Trunk Cell Routing Restrict: Y   Max Cost: 100  Route
Cost: 36


Path:   Downed by user
Pref:   Not Configured



ca20          ASI-T3    : OK           ca19      ASI-T3    : OK
              Line 12.1 : OK                     Line  4.1 : OK


Last Command: dspcon 12.1.1.4


Next Command:
```

Example 3

dspcon 12.1.1.100

Description

Display connection information for channel 12.1.1.100 (an ABR connection.)

System Response

```
ca20           LAN   SuperUser       BPX 15    9.2     Aug. 29 1997 10:31 PST

Conn:  12.1.1.100       ca20
    SCR           MBS           MCR         ABR PCR     UPC FST CLP  % util
20000/20000      50/50      20000/20000   96000/96000    y   y   y  100/100
 ForeSight RTD: 0 msec



Path:   Route information not applicable for local connections




ca20          ASI-T3    : OK           ca20      ASI-T3    : OK
              Line 12.1 : OK                     Line 12.2 : OK


Last Command: dspcon 12.1.1.100


Next Command:
```

Example 4

dspcon 4.1.2.1

Description

Display connection information for channel 4.1.2.1 (an ATFST connection.)

System Response

```
sw53           TN    SuperUser       BPX 8620    9.2    July 26 1997 13:40 GMT

Conn: 4.1.2.1          sw53        4.3.2.1           atfst    Status: OK
    SCR           MBS           MCR         ABR PCR     UPC FST CLP  % util
   25/25       1000/1000       25/25         25/25       y   y   y 100/100
 ForeSightRTD: 0 msec


Path:   Route information not applicable for local connections




sw53          BNI-T3    : OK           sw53      BNI-T3    : OK
              Line  4.1 : OK                     Line  4.3 : OK
              OAM Cell RX: Clear                 NNI       : OK
              NNI       : OK

Last Command: dspcon 4.1.2.1


Next Command:
```

Example 5

dspcon 12.1.1.*

Description

Display connection information for channel 12.1.1.* (a CBR VP tunnelling DAX connection.)

System Response

```
sw224          TRM            IGX 8420 9.2.a5          Mar. 5 1999 11:10 PST

Conn: 12.2.1.*          sw224       12.1.1.100         cbrvp      Status:OK

   PCR(0+1)     % Util    CDVT(0+1)     Policing

   1000/1000   100/100   10000/10000     4/4

Pri: L  Test-RTD: 0 msec

Path:   Route information not applicable for local connections


sw224     UXM:   OK                    sw224     UXM:   OK

          Line 12.2 : OK                         Line 12.1 : OK

          OAM Cell RX: Clear                     NNI:   OK

          NNI:   OK

This Command: dspcon 12.2.1.*
```

Table 9-31 dspcon—Parameters

Parameter	Description
channel	Specifies the channel for which to display connection details. The command displays connection information for one channel at a time. You cannot specify a set of channels. Channel is specified in the following format: slot.port.vpi.vci

dspconcnf

Displays the following information for a connection's configuration:

- The channel numbers for both the local and remote ends of the connection.
- The node names at both ends of the connection.
- The preferred route for the connection (if configured).
- The bandwidth parameter values for ATM connections.
- VC queue depth.
- The connection type (if configured).
- Other values (see example screen).

The rt-VBR and nrt-VBR connection service types will display separately.

Full Name

Display connection configuration

Syntax

dspconcnf <channel>

Related Commands

addcon, dspcon, dspcons, delcon

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	BPX
Lock	No

Example 1

`dspconcnf 3.1.1.1`

Description

Display the configuration for 3.1.1.1.

System Response

```
sw60           TN    SuperUser       BPX 8620    9.2 Date/Time Not Set

Conn: 3.1.1.1          sw60        3.1.1.1           abrstd
Description:

   PCR(0+1)     % Util      MCR            CDVT(0+1)         AAL5 FBTC
96000/96000    100/100 96000/96000        10000/10000            n









Last Command: dspconcnf 3.1.1.1


Next Command:
```

Example 2

dspconcnf 2.1.1.101

Description

Display the configuration for 2.1.1.101.

System Response

```
sw60          TN    SuperUser       BPX 8620    9.2 Date/Time Not Set

Conn: 3.1.1.1          sw60        3.1.1.1           rt-vbr
Description:

 PCR(0+1)   % Util      CDVT(0+1)        AAL5 FBTC        SCR
----------   ------      ---------        ---------        -----
50/50        100/100     250000/250000    n                50/50

MBS         Policing
----        ---------
500/500        3

Trunk Cell Routing Restrict:  Y




Last Command: dspconcnf 3.1.1.1


Next Command:
```

Table 9-32 dspconcnf—Parameters

Parameter	Description
channel	Specifies the channel for which to display connection configuration. The command displays connection information for one channel at a time. You cannot specify a set of channels. Channel is specified in the following format: slot.port.vpi.vci

dspcons

Displays information about the connections on an IGX or BPX node. (For information about **dspcons** for an MGX 8220 card, refer to the *MGX 8220 Command Reference*.)

Table 9-32 lists all possible information headings that appear in the display. The actual headings that appear depend on the choice of selected optional parameters—including no parameters. The screen examples reflect various optional parameters.

Note This description contains all parameters that are displayed even though some parameters are meaningless on a BPX.

You can also use **dspcons** to display those connections that have failed the OAM Loopback test. See the **cnfoamlpbk** and **dspoamlpbk** commands for more information.

In Release 9.2.20, dspcons will display the rt-VBR and nrt-VBR service types separately.

As you configure VP tunnelling connections on a node, you can display all the VP tunnelling connections on a particular node by using the **dspcons -tun** command. VP tunnelling connections are indicated by a connection type of "cbrvp", for example, in the Type column of the **dspcons** screen. (For more information on VP tunnelling on UXM cards, see the "Virtual Trunking through a Public ATM Cloud using VP (Virtual Path) Tunnelling on IGX-UXM Cards" section on page 18-14.)

Table 9-33 Headings in Connection Display

Fields	Description
Local Channel	The connection's channel at this node.
Remote Node Name	The name of the node at the other end of the connection.
Remote Channel	The connection's channel at the remote node.
State	The state of the connection(s) are as follows. State Parameter OK routed Down downed Failed unrouted, but trying
Type	The type of connection (nrt-vbr, cbr, abr, atfr, or atfst).
Route Avoid	The type of lines to avoid when routing (satellite lines, terrestrial lines, lines with zero code suppression).
COS	The Class Of Service.
Owner	The end of the connection in control of re-routing.

Full Name

Display connections

Syntax

dspcons [*start_channel*] [*nodename*] [-f] [-v] [-d] [-atfr] [-abit] [-fabit] [-fail] [-down] where

start_channel	is the starting channel to display.
nodename	specifies that connections for only the named node appear in the display.
-f	specifies that the display show Frame Relay connections only.
-v	specifies that the display show only voice connections.
-d	specifies that the display show only data connections (in Kbps).
-atfr	specifies that the display show Frame Relay to ATM interworking connections (as well as atfr with ForeSight).
-abit	specifies that the display show status of the Abit.
-fabit	specifies that the display show only connections with failed A-bits.
-down	specifies that the display show only downed connections.

Note Some parameters may cause other parameters not to appear. Therefore, if you specify all parameters, some do not appear.

Related Commands

addcon, delcon

Attributes

Privilege	1–6
Jobs	No
Log	No
Node	IGX, BPX
Lock	No

Example 1

dspcons 4.1.1.4

Description

Displays all connections starting with 4.1.1.4.

System Response

```
ca19           VT    SuperUser       BPX 15    9.2    Aug. 23 1997 19:44 GMT

 Local           Remote      Remote                             Route
 Channel         NodeName    Channel         State  Type        Avoid COS O
 4.1.1.4         ca20        12.1.1.4        Ok     CBR                0  R
 4.1.1.5         ca20        12.1.1.5        Ok     rt-VBR             0 R
 4.1.1.6         ca20        12.1.1.6        Ok     ABR                0  R
 4.1.1.7         ca20        12.1.1.7        Ok     nrt-VBR            0 R







Last Command: dspcons


Next Command:
```

Example 2

dspcons -abit

Description

Display the Abit status for all connections starting with 1.1.3.66.

System Response

```
sw81           TN    SuperUser       BPX 15    9.2       Aug. 14 1997 10:32 PST

 Local           Remote      Remote                      Local      Remote
 Channel         NodeName    Channel         State        Abit      Abit
 1.1.3.66        sw81        1.1.3.66        Ok          OK         OK
 1.1.3.67        sw81        1.1.3.67        Ok          OK         OK
 1.1.3.68        sw81        1.1.3.68        Ok          OK         OK
 1.1.3.69        sw81        1.1.3.69        Ok          OK         OK
 1.1.3.70        sw81        1.1.3.70        Ok          OK         OK
 1.1.3.71        sw81        1.1.3.71        Ok          OK         OK
 1.1.3.72        sw81        1.1.3.72        Ok          OK         OK
 1.1.3.73        sw81        1.1.3.73        Ok          OK         OK
 1.1.3.74        sw81        1.1.3.74        Ok          OK         OK
 1.1.3.75        sw81        1.1.3.75        Ok          OK         OK
 1.1.3.76        sw81        1.1.3.76        Ok          OK         OK
 1.1.3.77        sw81        1.1.3.77        Ok          OK         OK
 1.1.3.78        sw81        1.1.3.78        Ok          OK         OK

This Command: dspcons -abit


Continue?
```

Example 3

dspcons

Description

Display connections

System Response

```
sw99     TN     StrataCom      BPX 8620      9.2.10      Aug. 27 1998 08:59 GMT

Local       Remote      Remote                          Route
Channel     NodeName    Channel   State     Type       Avoid   COS   O
-------     --------    -------   -----     ----       -----   ---  --
3.2.6.16    sw14        10.1.6.16  Ok      rt-vbr              0    L
3.2.6.17    sw14        10.1.6.17  Ok      rt-vbr              0    L
3.2.6.18    sw14        10.1.6.18  Ok      rt-vbr              0    L
3.2.6.19    sw14        10.1.6.19  Ok      rt-vbr              0    L
3.2.6.20    sw4         10.1.6.20  Ok      rt-vbr              0    L
3.2.6.21    sw14        10.1.6.21  Ok      nrt-vbr             0    L
3.2.6.22    sw14        10.1.6.22  Ok      atfr                0    L
3.2.6.16    sw157       16.1.6     Failed  atfr                0    L
3.2.6.17    sw157       16.1.7     Failed  atfr                0    L
3.2.8.18    sw157       16.1.8     OAM-F   atfr                0    L
3.2.8.19    sw157       16.1.9     OAM-F   atfr                0    L


Last Command: dspcons
```

Example 4

dspcons -oam

Description

Display connections that have failed the OAM Loopback test

System Response

```
sw99        TN     StrataCom     BPX 8620        9.2.10       Aug. 27 1998 08:59 GMT

Local          Remote       Remote                              Route
Channel        NodeName     Channel     State   Type          Avoid      COS      O
-------       --------     -------      -----   ----          -----      ---      --
3.2.6.16      sw157        16.1.6       OAM-F   atfr                      0       L
3.2.6.17      sw157        16.1.7       OAM-F   atfr                      0       L
3.2.8.18      sw157        16.1.8       OAM-F   atfr                      0       L
3.2.8.19      sw157        16.1.9       OAM-F   atfr                      0       L


Last Command: dspcons -oam

Next Command:
```

Table 9-34 dspcons—Optional Parameters

Parameter	Description
start channel	Specifies the beginning channel to display. The *start channel* format is: *slot.port.vpi.vci* If no starting channel is specified, the display begins with the first connected channel.
node name	Specifies that connections to a specific remote node are displayed.
-atfr	Frame relay to ATM interworking connections
-abit	Abit status
-fabit	Connections with Abit errors
-fail	Failed connections
-down	Downed connections

Example 5

dspcons -tun

Description

Display only VP tunnelling connections on that node.

System Response

```
sw224          TRM   StrataCom       IGX 8420 9.2.a5    Mar. 5 1999 11:10 PST

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type     Compress   Code COS
 12.1.1.100     sw224       12.2.1.*        Ok     cbrvp
 12.2.1.*       sw224       12.1.1.100      Ok     cbr




Last Command: dspcons
```

dsplmistats

Displays LMI statistics for a specified channel.

Full Name

Display LMI/ILMI statistics

Syntax

dsplmistats <port> [clear]

Note On an access shelf, the **dsplmistats** command takes no arguments. On an IPX or IGX node, **dsplmistats** requires a trunk number. On a BPX node, **dsplmistats** requires the slot and port number.

Related Commands

none

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

```
dsplmistats 1.1
```

Description

Display LMI statistics for channel 1.1.1.1.

System Response

```
sw81          TN    SuperUser       BPX 15    9.2       Aug. 29 1997 14:44 PST

              Annex G  LMI Statistics for slot:1 port:1
VPI.VCI:       0.0                     Lmi enabled         Lmi polling enabled
Invalid Pdu      Rx:          0        Status Polling Timer (T396)    :    10
Invalid Pdu Len  Rx:          0        Status Enquiry Timer (T393)    :    10
Unknown Pdu Type Rx:          0        Max Status Enquiry Retry (N394):     5
Unknown IE Type  Rx:          0        Update Status Timer (T394)     :    10
Bad Transaction  Rx:          0        Max Update Status Retry (N395) :     5
Status           Rx:      77715        Spc Polling Timer              :     3
Status Enq       Tx:      77711        Spc Retry Timer                :     0
Status Enq       Rx:      77897        Spc Retry Counter              :     1
Status           Tx:      77897        Node Status Retry Timer        :     0
Status Ack       Rx:       1505        Node Status Retry Counter      :     0
Update Status    Tx:       1507        Node Status Polling Timer      :     7
Update Status    Rx:       2042
Status Ack       Tx:       2042

Last Command: dsplmistats 1.1


Next Command:
```

Table 9-35 dsplmistats—Parameters

Parameter	Description
port	Channel is specified in the format *slot.port*.

Table 9-36 dsplmistats—Optional Parameters

Parameter	Description
clear	On a BPX node only, the optional **clear** argument clears the current statistics after **dsplmistats** executes.

Functional Description of LMI Stats for BXM Card

An internal firmware command provides the capability for the controller card to fetch ILMI/LMI stats on ILMI/LMI sessions on the BXM card. The BXM must be firmware-capable. Refer to LMI Statistics and Descriptions for dsplmistats (ATM) for BXM Card

Table 9-37 LMI Statistics and Descriptions for dsplmistats (ATM) for BXM Card

Object ID	Object Name	Range/Values	Default	Description
01	Message Tag	Byte 0-3: Tag ID Byte 4-7: IP Address	0	Identifier and source IP address sent with Commbus message. Both will be copied into the response, if any is to be sent.
02	Port Number	1 - 12	R	Identifies the target port. If multiple port numbers are sent during the operation, then each port number object terminates the configuration for the string of objects for the previous port number.
03	Virtual Port #	1 - 255	R	Identifies the target virtual port.
04	Status Sync	0 - Clear 1 - Get Status	R	Sync up ingress status information to bcc
05	Session Status	0 - Okay 1 - Failed	0	Indicates whether or not the ILMI/LMI session on this logical interface is failed.
06	BPX/Feeder IP Address	0 - 2^{32}-1	0	Valid for feeder connections. Indicates the IP address of the Feeder
07	BPX/Feeder Name	Byte 0..8: String	N/A	Valid for feeder connections. Indicates the name of the Feeder
08	BPX/Feeder Serial Number	Byte 0..8: String	N/A	Valid for feeder connections. Indicates the serial number of the Feeder
09	BPX/Feeder Alarm Status	0: Clear 1: Minor 2: Major	N/A	Valid for feeder connections. Indicates the alarm status of the Feeder
0A	BPX/Feeder Line Rate	0 - 2^{32}-1	N/A	Valid for feeder connections. Indicates the line receive rate of the Feeder
0B	BPX/Feeder LAN IP Address	0 - 2^{32}-1	0	Valid for feeder connections. Indications the LAN IP address of the feeder
0C-0F	RESERVED			
10	ILMI Number of Get Req Rx’d	0 - 2^{32}-1	N/A	ILMI number of Get Requests received.
11	ILMI No. of Get Next Req Rx’d	0 - 2^{32}-1	N/A	ILMI number of Get Next Requests received.
12	ILMI No. of Get Next Req Tx’d	0 - 2^{32}-1	N/A	ILMI number of Get Next Requests transmitted.
13	ILMI No. of Set Req Rx’d	0 - 2^{32}-1	N/A	ILMI number of Set Requests received.
14	ILMI No. of Traps Rx’d	0 - 2^{32}-1	N/A	ILMI number of traps received.
15	ILMI No. of Get Resp. Rx’d	0 - 2^{32}-1	N/A	ILMI number of Get Responses received.
16	ILMI No. of Get Req. Tx’d	0 - 2^{32}-1	N/A	ILMI number of Get Requests transmitted.
17	ILMI No. of Get Resp. Tx’d	0 - 2^{32}-1	N/A	ILMI number of Get Responses transmitted.

Table 9-37 LMI Statistics and Descriptions for dsplmistats (ATM) for BXM Card (Continued)

Object ID	Object Name	Range/Values	Default	Description
18	ILMI No. of Traps Tx'd	0 - 2^{32}-1	N/A	ILMI number of traps transmitted.
19	ILMI Unknown PDUs Rx'd	0 - 2^{32}-1	N/A	ILMI number of unknown PDUs received.
1A-1F	RESERVED			
20	LMI No. of Status Tx'd	0 - 2^{32}-1	N/A	LMI number of Status transmitted.
21	LMI No. Update Status Tx'd	0 - 2^{32}-1	N/A	LMI number of Update Status transmitted.
22	LMI No. of Status Ack. Tx'd	0 - 2^{32}-1	N/A	LMI number of StatusAck. transmitted.
23	LMI No. of Status Enq. Rx'd	0 - 2^{32}-1	N/A	LMI number of Status Enquiries received.
24	LMI No. of Status Enq. Tx'd	0 - 2^{32}-1	N/A	LMI number of Status Enquiries transmitted.
25	LMI No. of Status Rx'd	0 - 2^{32}-1	N/A	LMI number of Status received.
26	LMI No. Update Status Rx'd	0 - 2^{32}-1	N/A	LMI number of Update Status received.
27	LMI No. of Status Ack. Rx'd	0 - 2^{32}-1	N/A	LMI number of StatusAck. received.
28	LMI No. of Invalid PDU Rx'd	0 - 2^{32}-1	N/A	LMI number of invalid PDUs received.
29	LMI No. of Invalid PDU Len. Rx'd	0 - 2^{32}-1	N/A	LMI number of invalid PDU lengths received.
2A	LMI No. Unknown PDUs Rx'd	0 - 2^{32}-1	N/A	LMI number of unknown PDUs received.
2B	LMI No. of Invalid IEs Rx'd	0 - 2^{32}-1	N/A	LMI number of Information Elements received.
2C	LMI No. of Invalid T.ID Rx'd	0 - 2^{32}-1	N/A	LMI number of invalid Transaction IDs received.

dspport

Displays detailed status on a single specified ATM port. The more specific the port address in the command, the more detail is provided. A full description of these parameters is provided in the **cnfport** command.

Full Name

Display port

Syntax

dspport <slot.port>

Related Commands

cnfport, upport, dnport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX, BPX	No

Example 1

```
dspport 4.1
```

Description

Display the status of ASI port 4.1.

System Response

```
swstorm        TN    SuperUser       BPX 15    9.2    July 26 1997 17:57 GMT

Port:       4.1     [ACTIVE  ]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)
VBR Queue Depth:    10800

Protocol:           NONE










Last Command: dspport 4.1


Next Command:
```

Table 9-38 dspport—Parameters

Parameter	Description
slot.port	Specifies the slot number and port to display.

dspportq

Displays the port queue configuration for an ASI or BXM card on a BPX or a UXM card on an IGX. After you enter this command with the required slot and port number parameter, the display shows the detailed port queue configuration information shown in the example figure.

Full Name

Display port queue configuration.

Syntax

dspportq <slot.port>

Related Commands

cnfportq

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IGX, BPX	No

Example 1

`dspportq 4.2`

Description

Display the port queue configuration for 4.2.

System Response

```
ca19          VT    SuperUser       BPX 8620   9.2    June 23 1999 19:11 GMT

   ASI-T3

Port:       4.2     [ACTIVE]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)
SVC Queue Pool Size:               0
CBR Queue Depth:                 200     rt-VBR Queue Depth:                1000
CBR Queue CLP High Threshold:     80%     rt-VBR Queue CLP High Threshold:    80%
CBR Queue CLP Low Threshold:      60%     rt-VBR Queue CLP Low Threshold      60%
CBR Queue EFCI Threshold:         80%     rt-VBR Queue EFCI Threshold         80%
nrt-VBR Queue Depth:            1000     UBR/ABR Queue Depth:               9800
nrt-VBR Queue CLP High Threshold: 80%     UBR/ABR Queue CLP High Threshold:    80%
nrt-VBR Queue CLP Low Threshold: 60%     UBR/ABR Queue CLP Low Threshold:     60%
nrt-VBR Queue EFCI Threshold:     80%     UBR/ABR Queue EFCI Threshold:        80%



Last Command: cnfportq 4.2


Next Command:
```

Example 2

dspportq 2.1

Description

Display the port queue configuration for 2.1

System Response

```
swstorm        TN    SuperUser       BPX 8620    9.2    June 26 1998 18:01 GMT

ASI-T3

Port:       2.1     [ACTIVE ]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)
SVC Quque Pool Size:          0
CBR Queue Depth:              200        rt-VBR Queue Depth:              1000
CBR Queue CLP High Threshold: 80%        rt-VBR Queue CLP Hi-Threshold:     80%
CBR Queue CLP Low Threshold:  60%        rt-VBR Queue CLP Low Threshold:    60%
CBR Queue EFCI Threshold:     80%        rt-VBR Queue EFCI Threshold:       80%
rt-VBR Queue Depth:             10800   UBR/ABR Queue Depth:             9800
rt-VBR Queue CLP High Threshold: 80%     UBR/ABR Queue CLP High Threshold:  80%
rt-VBR Queue CLP Low Threshold:  60%     UBR/ABR Queue CLP Low Threshold:   60%
rt-VBR Queue EFCI Threshold:     80%     UBR/ABR Queue EFCI Threshold:      80%



Last Command: dspportq 2.1


Next Command:
```

Table 9-39 dspportq—Parameters

Parameter	Description
slot or slot.port	Specifies either the slot number or the slot and port number.

dspportstats

Displays a summary of port statistics for the ATM port specified. These include the cell count in the transmit and receive directions, and error counts associated with the port. The display indicates the date and time that the statistics were cleared and the statistics collection time since they were last cleared. Cells transmitted indicates the amount of data transmitted out the port to the user device. Cells received indicates the amount of data received from the user device at the port. Corrupted statistics result from channel/port loopbacks or port tests. A “yes” in this field indicates that such loopback or port tests have occurred since the statistics were last cleared.

Full Name

Display port statistics

Syntax

dspportstats <port> [interval]

Related Commands

clrportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX	No

Example 1

`dspportstats 11.1`

Description

Display the statistics for ASI port 11.1.

System Response

```
PABPX001       VT    StrataCom       BPX 15    8.5.04    Feb. 27 1998
16:38 G+01

Port Statistics for 11.1        Cleared: Feb. 19 1998 18:26
Port Speed: 80000 cps   Collection Time: 5 day(s) 09:54:37      Corrupted: NO

              Cells           CLP          (EFCI)
Rx Port:   41735369             0               0
Tx Port:   55704628             0               0

Unknown Addr :    144592  Cell Buf Ovfl :         0  Nonzero GFC Ct:
   0
Rcv Ais Count :         0  Rcv Ferf Count:       343  Rx BCM Cells  :
   0
Tx Pyld Err Ct:         0  Tx H Err Dscd :         0  Lst Un Vpi/Vci:    0.16



This Command: dspportstats 11.1


Hit DEL key to quit:
```

Table 9-40 dspportstats—Parameters

Parameter	Description
slot.port	Specifies the ATM card set and port number.

Table 9-41 dspportstats—Optional Parameters

Parameter	Description
interval	Specifies the refresh interval time for data. It can be specified between 1 and 60 seconds. The default interval is 1 seconds. Note that you must specify a value other than 0 for the “interval” parameter. Otherwise, the screen displayed for a UXM and BMX card will be just a snapshot—it will not be updated periodically. If the Rx Q depth and the Tx Q depth on the BXM and UXM cards remain “0”, specify a value for the interval parameter other than 0.

Statistics Supported for BPX ATM Ports (ASI or BXM Front Card)

The following 45 statistics are available for each BPX ATM port, with an ASI or BXM front card type, and T3, E3, or OC-3 back card type. (Note that the statistics names listed below are what displays in Cisco WAN Manager; the field name that appears on the **dspportstats** screen may vary slightly from the Cisco WAN Manager parameter/field name.)

1) Cell Buffer Overflow

2) Cells Rx w/CLP discarded

3) Cells Rx w/CLP=0

4) Cells Rx w/CLP=0 discarded

5) Cells Tx w/CLP=0
6) Egress OAM Cell Count
7) Egress RM Cell Count
8) Get Request Rx
9) Get Request Tx
10) Get Response Rx
11) Get Response Tx
12) GetNext Request Rx
13) GetNext Request Tx
14) Ingress RM Cell Count
15) Invalid LMI IE Rx
16) Invalid LMI Rx
17) Invalid LMI length Rx
18) Invalid Transaction IDs
19) Non-zero GFC Count
20) Number of BCM Cell Rx
21) Number of Cells Rx
22) Number of Cells Rx w/CLP set
23) Number of Cells Rx w/EFCI set
24) Number of Cells Tx
25) Number of Cells Tx w/CLP set
26) Number of Cells Tx w/EFCI set
27) OAM Cells Rx Count
28) Rx AIS Cell
29) Rx FERF Cell
30) SetRequest Rx
31) Status Ack Rx
32) Status Ack Tx
33) Status Enq Rx
34) Status Enq Tx
35) Status Rx
36) Status Tx
37) Trap Rx
38) Trap Tx
39) Tx Header Err Discard
40) Tx Payload Err Due to BIP-16 Err

41) Unknown LMI Rx
42) Unknown LMI Tx
43) Unknown VPI/VCI
44) Update Status Rx
45) Update Status Tx

Table 9-42 BPX Port Statistics Supported for ASI and BXM Front Cards

Statistics Name in Cisco WAN Manager	Statistics ID
Cell Buffer Overflow	1
Cells Rx w/CLP discarded	42
Cells Rx w/CLP=0	40
Cells Rx w/CLP=0 discarded	41
Cells Tx w/CLP=0	43
Egress OAM Cell Count	44
Egress RM Cell Count	46
Get Request Rx	17
Get Request Tx	23
Get Response Rx	22
Get Response Tx	24
GetNext Request Rx	18
GetNext Request Tx	19
Ingress RM Cell Count	45
Invalid LMI IE Rx	38
Invalid LMI Rx	35
Invalid LMI length Rx	36
Invalid Transaction IDs	39
Non-zero GFC Count	2
Number of BCM Cell Rx	10
Number of Cells Rx	7
Number of Cells Rx w/CLP set	8
Number of Cells Rx w/EFCI set	9
Number of Cells Tx	11
Number of Cells Tx w/CLP set	14
Number of Cells Tx w/EFCI set	15
OAM Cells Rx Count	12
Rx AIS Cell	5
Rx FERF Cell	6
SetRequest Rx	20

Table 9-42 BPX Port Statistics Supported for ASI and BXM Front Cards (Continued)

Status Ack Rx	34
Status Ack Tx	29
Status Enq Rx	30
Status Enq Tx	31
Status Rx	32
Status Tx	27
Trap Rx	21
Trap Tx	25
Tx Header Err Discard	16
Tx Payload Err Due to BIP-16 Err	13
41) Unknown LMI Rx	37
Unknown LMI Tx	26
Unknown VPI/VCI	0
Update Status Rx	33
Update Status Tx	28

dsprtcache

This command displays the cache of all cost-based routing connections. The optional *index* parameter lets you specify a cache entry index. The optional *c* parameter clears the cache. The information displayed includes:

Full Name

Display cost-based route cache

Syntax

dsprtcache [index] [c]

[index] specifies the cache entry index

[c] specifies to clear the entire cache or a single entry

Related Commands

dspcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsprtcache`

Description

Display route cache contents, and let you monitor and manually clear the cache.

System Response

```
pissaro     TN      StrataCom          BPX 15      9.1     Jun. 18 1997 11:11 GMT
Route Cache (Summary)
Index Use    No.   Cost Delay   Restrict Load   VPC      Hops   RemoteNode
0      Yes    1       Yes   No      None      VBR     No       2      lautrec
1      Yes    6       Yes   No      *s        BDB     No       3      vangogh
2      Yes    9       Yes   No      None      BDA     No       3      matisse
3      Yes    3       Yes   No      *t        BDB     No       3      rousseau
4      Yes    1     Yes   No      None     CBR     No      3     seurat  <- current
5      No     0     No    No      None      ---    No      0           ---
6      No     0     No    No      None      ---    No      0           ---
7      No     0     No    No      None      ---    No      0           ---
8      No     0     No    No      None      ---    No      0           ---
9      No     0     No    No      None      ---    No      0           ---
10     No     0     No    No      None      ---    No      0           ---
11     No     0     No    No      None      ---    No      0           ---

Last Command: dsprtcache

Next Command:
```

Table 9-43 dsprtcache—Parameters

Parameter	Description
index	Specifies a particular route entry within the cache. When used with the c parameter, the route is either displayed or cleared from the cache.
c	Clears the cache, or if you also enter the index parameter, clears the route cache specified by the index number.

upport

Activates a single port on an ASI or BXM card on a BPX or a UXM card on an IGX. If the port has not been configured, the default configuration values are used to configure the port.

Full Name

Up port

Syntax

upport <slot.port>

Related Commands

dnport, cnfport, upln

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

```
upport 4.2
```

Description

Activate port 2 on the ASI in slot 4.

System Response

```
ca19          VT    SuperUser       BPX 15    9.2    Aug. 23 1997 19:17 GMT

Port:       4.2     [ACTIVE  ]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)

CBR Queue Depth:              200
CBR Queue CLP High Threshold: 80%
CBR Queue CLP Low Threshold:  60%
CBR Queue EFCI Threshold:     80%
VBR Queue Depth:              1000    ABR Queue Depth:               9800
VBR Queue CLP High Threshold: 80%     ABR Queue CLP High Threshold:  80%
VBR Queue CLP Low Threshold:  60%     ABR Queue CLP Low Threshold:   60%
VBR Queue EFCI Threshold:     80%     ABR Queue EFCI Threshold:      80%



Last Command: upport 4.2


Next Command:
```

Table 9-44 upport—Parameters

Parameter	Description
slot.port	Specifies the slot number of the card and the port to activate.

CHAPTER 10

Optimizing Traffic Routing and Bandwidth

To achieve peak network performance, the routing of traffic and use of available bandwidth is configurable. The information used in configuring traffic routing and bandwidth is gathered from historical network trends. The tasks required to optimize the network are: specifying channel utilization, specifying the class of service, and managing bandwidth. These tasks are discussed in the paragraphs that follow.

Specifying Channel Utilization

Use the **cnfchutl** command to specify the expected utilization of Frame Relay, data, or voice channel as a percentage of the channel's total capacity. The specified value can be in the range of 0% to 100%. 100% is the default for data and Frame Relay channels. The default for voice channels is 40%. To display the utilization of a particular trunk, use the **dsptrkutl** command. This command displays a details on the packets transmitted over the trunk. The user can specify the rate in seconds at which the screen is updated. Use the **dspload** command to display the load for a specified trunk at a node.

Specifying Class of Service

Use the **cnfcos** command to specify a class of service (COS) for a Frame Relay, data, or voice channel. The class of service is the delay in seconds before the network reroutes a connection in the event of a trunk failure. The range is 0–15. By spreading out the COS numbers to vary the rerouting delay, one class of channels has a chance to reroute before the another class starts to reroute.

Managing Bandwidth

There are a number of commands that assist in managing bandwidth to achieve satisfactory traffic patterns.

upcon, dncon The up and down connection commands can be used to temporarily down connections of a specified COS, thus releasing bandwidth for other services. Often it is possible to down some voice connections to provide more bandwidth for data and Frame Relay connections.

cnfpref The configure preference command can be used to specify preferred routing for intra-domain connections. This command can be used to assist in balancing the load on the network's trunks.

dsprts, prtrts The display and print routes commands can be used in conjunction with the **cnfpref** command to display the current connection routing information.

Summary of Commands

shows the full command name and starting page for each description.

Table 10-1 Bandwidth Management Commands

Command	Description	Page
cnfchutl	Configure channel utilization	10-3
cnfcmb	Configure combined timeout parameters	10-7
cnfcos	Configure class of service	10-9
cnfpref	Configure preferences	10-11
cnfrtcost	Configure cost based routing	10-14
dncon	Down connections	10-16
dspload	Display load	10-19
dspospace	Display open space for routes	10-23
dsprts	Display routes	10-25
dsptrkutl	Display trunk utilization	10-29
prtrts	Print routes	10-32
upcon	Up connections	10-33

cnfchutl

Informs the system software of the expected utilization rate of connections with traffic-dependent compression algorithms (voice connections with VAD, data connections with DFM, Frame Relay connections, FastPAD voice connections with ATC-8K, ATC-12K, ATC-16K, or CELP-8K compression). The software load model then takes the user-specified rate of the connection and modifies it by using the percent of utilization you specify with **cnfchutl**. The resulting rate is used in calculations for loading trunks. The load model uses these figures instead of calculated estimates from real traffic patterns.

On a FastPAD channel, the compression rate adapts to the congestion level within the network. The configured compression rate indicates the maximum rate for the channel. FastPAD channels detect FAX signals and adapt their rates for FAX transmittal. For the full benefits of the compression algorithms to be used, the default utilizations should be modified after traffic studies have been performed. Also, traffic studies of Frame Relay connections should be used to determine optimum utilization settings. When calculating loads in a network, the load allocated to a connection is:

channel utilization x full load for the connection type

For example, with a channel utilization of 50% and a full load of 480 packets per second, the load allocated to a connection is:

0.50 x 480 pps = 240 pps

For data connections with DFM turned off, for voice connections with VAD turned off, and for all FastPAD data connections, the bandwidth allocated is always the maximum bandwidth for the connection type. In other words, the utilization, although configurable, is ignored for a voice channel without VAD, a data channel without DFM and all FastPAD data channels.

If you use **cnfchutl** to increase the utilization of a connection, the system verifies that the additional bandwidth is available on the connection's current route. If the bandwidth is not available, the system attempts to reroute the connection. If no other route is found, the connection is failed.

If you use **cnfchutl** to decrease the utilization of a connection, the system makes the bandwidth available to other connections that require a route. The screen displayed by the **cnfchutl** command depends upon whether a data channel, voice channel, or Frame Relay channel is specified.

Full Name

Configure channel utilization

Syntax

cnfchutl <channel(s)> <%_util>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

cnfchutl 5.1 40

Description

Set utilization on data channel 5.1 at 40%.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:45 PST

            Maximum EIA     %      DFM Pattern     DFM
Channels    Update Rate    Util      Length       Status
5.1              15         40         8         Enabled
5.2-4             2        100         8         Enabled









Last Command: cnfchutl 5.1 40


Next Command:
```

Example 2

cnfchutl 14.1 55

Description

Set utilization on voice channel 14.1 at 55%.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 10:10 PST

           %    Adaptive  Gain (dB)   Dial                        OnHk      Cond
Channels  Util  Voice     In  Out      Type   Interface Type    A  B  C  D  Crit.
14.1       55   Enabled   -4    -     User    Unconfig          ?  ?  -  -    a
14.2-24    40   Enabled    0    -     Inband  Unconfig          ?  ?  -  -    a









Last Command: cnfchutl 14.1 55


Next Command:
```

Example 3

cnfchutl 8.1.100 60

Description

Set utilization on Frame Relay channel 8.1.100 at 60%.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:45 PST

          Frame Relay Channel Configuration Port: 8.1

From      Minimum   Peak  AvgFrame   Cmax   VC Q    ECN Q   % Util
8.1.100   9.6       *     70         10     65535   65535   60
8.1.301   9.6       *     70         10     65535   65535   100











Last Command: cnfchutl 8.1.100 60


Next Command:
```

Table 10-2 cnfchutl—Parameters

Parameter	Description
channel	Specifies the channel for configuring utilization. The channel can be in voice, data, Frame Relay, or FastPAD voice or data. The format for *channel* depends on the technology, as follows: • Voice connection: *slot.channel* • Data connection: *slot.port* • Frame relay connection: *slot.port.DLCI* • Access device connection: *slot.port.device_ID* • FastPAD voice connection: *slot.port.subport* • FastPAD data connection: s*lot.port.subslot.subport*
percent utilization	Specifies the percentage of utilization of the channel. The is range 0–100. The default value for data or Frame Relay is 100%. The default value for voice is 40%.

cnfcmb

Configures a time the node waits for a second packet to become available for placing in an ATM cell. You can use the **cnfcmb** command to control the time that the node waits for individual traffic types. When you enter a value for a parameter, switch software multiplies the value by 125 microseconds to derive the timeout.

Full Name

Configure combine timeout parameters

Syntax

cnfcmb <parameter number> <value>

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
service	Yes	No	IGX	Yes

Example 1

cnfcmb 1 1

Description

Change the timeout for voice packets from the default of 2 * 125 microseconds to 1 * 125 microseconds.

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2    Sep. 17 1998 23:38 PDT

                     System-Wide Combine Timeout Parameters

1 Packet Combining Timeout for Voice (125 usec *).....................     2
2 Packet Combining Timeout for Time Stamped Traffic (125 usec *).......     2
3 Packet Combining Timeout for High Priority Traffic (125 usec *)......     0
4 Packet Combining Timeout for Non Time Stamped Traffic (125 usec *)...     2
5 Packet Combining Timeout for Bursty Data 1 Traffic (125 usec *)......   255
6 Packet Combining Timeout for Bursty Data 2 Traffic (125 usec *)......   255







This Command: cnfcmb


Which parameter do you wish to change: 1 1
```

Table 10-3 cnfcmb—Parameters

Parameter	Description	Default
1	Timeout for Voice (multiplied by 125 microseconds)	**2**
2	Timeout for Time Stamped Traffic (multiplied by 125 microseconds).	2
3	Timeout for High Priority Traffic (multiplied by 125 microseconds)	0
4	Timeout for Non Time Stamped Traffic (multiplied by 125 microseconds)	2
5	Timeout for Bursty Data 1 Traffic (multiplied by 125 microseconds)	255
6	Timeout for Bursty Data 2 Traffic (multiplied by 125 microseconds)	255

cnfcos

Determines the priority for rerouting a connection. You determine the priority by specifying a delay before the network reroutes one or more failed connections. The COS applies to:

- A single connection
- A range of connections
- A connection group

When connections have failed (typically due to a trunk failure), the network reroutes them according to priorities that are set primarily by the class of service (COS). The value of COS is the number of seconds the network waits before it begins to reroute the connection, so the COS determines the rerouting order for connections owned by a node. The range of possible COS values is 0–15.

The number of connections in a network has an effect on the increment between COS values you should use. For larger numbers of connections, you should allow more time to reroute the connections in a class. To facilitate the greater time required to reroute larger numbers of connections, use a larger increment between COS values. In a larger network, for example, you could specify COS values that are 3 seconds apart (such as 0, 3, 6, 9, 12, and so on, for example). For a network with less traffic, assign COS values in increments of 1 or 2. This strategy ensures that all connections of a given COS reroute before the connections with the next COS start to reroute.

Full Name

Configure class of service for connections

Syntax

cnfcos <group | channel(s)> <cos>

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

cnfcos 5.1 0

Description

Set the COS for channel 5.1 to 0.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 10:12 PST

 Local      Remote      Remote                                         Route
 Channel    NodeName    Channel     State   Type    Compression   Code Avoid COS O
 5.1        beta        25.1        Ok      256                   7/8          0  L
 9.1.100    gamma       8.1.200     Ok      fr                                 0  L
 9.2.400    beta        19.2.302    Ok      fr                                 0  L
 14.1       gamma       15.1        Ok      v                                  0  L









Last Command: cnfcos 5.1 0


Next Command:
```

Table 10-4 cnfcos—Parameters

Parameter	Description
channels	Specifies the voice, data, Frame Relay, or Fast PAD voice/data channel(s), where *channel* is one of the following: • Voice connections: *slot.channel* • Serial data connections: *slot.port* • Frame Relay connections: *slot.port.DLCI* • FastPAD switched voice connections: *slot.port* • FastPAD voice connections: *slot.port.subslot* • FastPAD data connections: *slot.port.subslot.subport*
cos	Specifies the class of service number to assign to the channel, range of channels, or connection group. The range is 0–15 seconds, so the rerouting priority is inversely proportional to the COS (a low COS values means a high routing priority).

cnfpref

Specifies the preferred route for a connection or range of connections. Enter **cnfpref** only at a node that is an end point of the connection. This command applies only to connections that exist *within* a domain. Do not attempt to execute **cnfpref** on connections that exist between domains.

The preferred route for a connection is used when possible. If the preferred route is different from the existing route, the connection automatically moves to the preferred route whenever network conditions allow (for example, when trunks are out of alarm and sufficient bandwidth exists).

Full Name

Configure preferred route for connections

Syntax

cnfpref <channel(s) | *> <route> < + | -> [d]

Related Commands

dsprts

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

cnfpref 14.1 13/beta 15/gamma d

Description

Select the preferred route for channel 14.1 to be through beta trunk 13 to beta then to gamma trunk 15. For gamma, the “d” in the command specifies that the route is *directed*.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 10:22 PST

From 14.1          Route
14.1
          alpha   14--13beta    15--15gamma
Pref:(D) alpha   14--13beta    15--15gamma









Last Command: cnfpref 14.1 13/beta 15/gamma d


Next Command:
```

Example 2

cnfpref 6.4 -

Description

Remove the preferred route for channel 6.4.

Example 3

cnfpref * +

Description

Designate the current routing of all locally owned connections to be the preferred routing. Using a “-” instead of a “+” in the command would remove the preferred routing designation of all locally owned connections.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:48 PST

Chan/Grp  Route
5.1
          alpha   10-- 7beta
Pref:     alpha   10-- 7beta
9.1.100
          alpha   14--13beta    15--15gamma
Pref:     alpha   14--13beta    15--15gamma
9.1.200
          alpha   10-- 7beta    15--15gamma
Pref:     alpha   10-- 7beta    15--15gamma
9.2.400
          alpha   10-- 7beta
Pref:     alpha   10-- 7beta



Last Command: cnfpref * +


Next Command:
```

Table 10-5 cnfpref—Parameters

Parameter	Description
channels	Specifies the channel or range of channels for preferred route configuration. The channel specifier has one of the following formats • Voice connection: *slot.channel* • Data connection: *slot.port* • Frame Relay connection: *slot.port.DLCI* • FastPAD voice connection: *slot.port.subport* • FastPAD data connection: *slot.port.subslot.subport* A “*” specifies all locally owned connections and applies only to the “+” and “-”.
route	Designates the preferred route for the connection(s) to take through the network. The route is designated by one or more “trunk/node name” pairs. At a given node *alpha*, for example, entering a route of "12/delta 6/epsilon", would route the connection from alpha to delta via delta's trunk 12. The connection would then go from delta to epsilon via epsilon's trunk 6. A "+" causes the connection's current route to become the preferred route. A "-" removes the connection's preferred route designation.

Table 10-6 cnfpref–Optional Parameters

Parameter	Description
d	Specifies directed routing. If the preferred route is not available, the connection is failed.

cnfrtcost

Configures the cost cap for a connection when cost-based routing is configured.

A maximum allowable cost value (cost cap) is used during route determination to prevent selection of a route which exceeds an acceptable cost. For routing based on delay, the cost cap is the acceptable end-to-end delay for the connection type. This cap is configured network-wide per delay-sensitive connection type.

For routing based on trunk cost, the cost cap is the acceptable end-to-end cost. This cap is configured per connection. The default cost cap is 100, which is derived from the maximum hops per route (10) and default cost per trunk (10). The cost cap can be changed at any time. If the cost cap is decreased below the current route cost, the connection is not automatically rerouted. A manual reroute is required to route the connection to fit under the new cost cap. This gives the user more control over the connection reroute outage.

Note **cnfrtcost** is only valid at the node where the connection was added.

Full Name

Display connection loading

Syntax

cnfrtcost <connection> <max cost>

<connection> indicates the connection endpoint (that is, slot.port.vpi.vci)

<max cost> indicates the maximum allowable route cost

Valid values = 1 - 500

Related Commands

dspcon, cnfpref, dsprtcache

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example

cnfrtcost 9.2.5.100 40 1

After configuring the cost cap for a connection, you can check to see the configured value with the **dspcon** command, as is shown in the System Response example. This is the **dspcon** response for 9.2.5.100 with the additional fields of Max Cost (40) and Route Cost (1). For a route optimized on trunk delay, the cost labels are updated to indicate delay: Max Cost becomes Max Delay and Route Cost becomes Route Delay.

Description

Select route cost for channel 9.2.5.100.

System Response

```
sw203          TN    StrataCom       BPX 8620    9.1.a4    Sep. 24 1998 18:18 GMT

Conn:  9.2.5.100        sw242       14.2.5.100        cbr       Status:OK
   PCR(0+1)      % util    CDVT(0+1)     Policing
     50/50     100/100   10000/10000     4/4
Owner: LOCAL  Restriction: NONE  COS: 0
TestRTD: 0 msec  Trunk Cell Routing Restrict: Y   Max Cost: 40  Route Cost: 1

Path:   sw203    3.1.1-- 2.1.1sw242
Pref:   Not Configured



sw203         ASI-T3    : OK           sw242     ASI-OC-3   : OK
              Line  9.2 : OK                     Line 14.2 : OK
              OAM Cell RX: Clear                 NNI       : OK
              NNI       : OK

Last Command: dspcon 9.2.5.100


Next Command:
```

dncon

Deactivates (downs) a connection, bundle of connections, a connection group or all connection in a COS or COS range. The **dncon** command temporarily removes one or more connections from the network. This command is useful for temporarily removing voice connections when additional bandwidth is necessary for other types of connections.

Connections can be downed immediately or with courtesy. Even with immediate downing, a prompt appears that requests confirmation. With courtesy downing, the system waits until the connection is onhook before downing the connection. Courtesy downing is possible only if the onhook status has been configured with the **cnfvchtp** command. Courtesy downing is not available for FastPAD connections because the signaling information between the end points is not visible to the IPX or IGX node. The **upcon** command reactivates the voice connections. The up/down status of the voice connections appears in the "State" column of the **dspcons** screen. Table 10-6 shows each item in the State column.

Table 10-7 Connection Status

State	Description
"OK" (routed)	Connection is activated and able to carry traffic.
"Down"	Connection has been added to the network database but is not activated and is not able to carry traffic.
"OK(Dn)"	Waiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command.
"Failed"	Unrouted, but trying to reroute.

Full Name

Down connection

Syntax

dncon {<group | local_chan(s)> | COS <cos_range>} {i | c}

Related Commands

upcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

dncon 14.1 c

Description

Down connection 14.1 with courtesy.

Example 2

dncon 14.1 i

Description

Down connection 14.1 immediately.

Example 3

dncon cos 4–8 c

Description

Courtesy down on-hook connections network-wide with COS 4 through 8. This command marks all connections that may be courtesy downed at one time and does not monitor new connections or those that later fit the COS.

Example 4

dncon 3.1.100 i

Description

Immediately down connection 3.1.100.

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2      Aug. 26 1998 16:51 GMT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type       Compress  Code COS
 3.1.100        pubsigx1    3.2.200         Ok     fr
 3.2.200        pubsigx1    3.1.100         Ok     fr










This Command: dncon 3.1.100 i


Down these connections (y/n)?
```

Example 5

dncon cos 4–8 i

Description

Immediately down all connections network-wide with COS 4 through 8. This command executes once, so if individual connections are subsequently upped or new connections added in this COS range, they remain up.

Example 6

dncon cos 14.1.3

Description

Down FastPAD voice connection 14.1.3.

Example 7

dncon cos 14.1.1.5

Description

Down FastPAD data connection 14.1.1.5.

Table 10-8 dncon–Parameters

Parameter	Description
channels or group	Specifies a group, a channel, or a range of channels to down.
cos range	Specifies the COS or COS range. The range is 0–15.

Table 10-9 dncon—Optional Parameters

Parameter	Description
i/c	Specifies immediate downing (i) of the specified connections or courtesy downing (c) of the specified connections.

dspload

Displays both the used and available bandwidth (both in the transmit and receive directions) for each trunk at the specified node. The "transmit" direction is *from* the node specified and *to* the node at the other end of the trunk. In the screen display, the numbers of disabled trunks appear in dim, reverse video on the screen.

The **dspload** display reflects the static load model stored by the node and used to determine the bandwidth available for new connections and reroutes. The display does not represent changes due to the dynamic utilization of the trunks. Some types of connections, such as voice connections using adaptive voice and data connections using Data Frame Multiplexing (DFM), suppress packets. In contrast, Frame Relay connections may generate additional packets when bandwidth permits.

When this command is executed at a local node in structured networks, the information displayed is for any node on the intra-domain lines belonging to the same domain. When this command is executed at a junction node, the information displayed is for all inter-domain lines between all junction nodes. The node uses the terminating and through routed connections' calculated load to calculate the trunk load. The connection type (v, c, a, or d) or baud rate (9.6 Kbps, 56 56 Kbps, and so on) and other factors determine its basic load. The calculated trunk load is also modified by the **cnfchutl** command for connections that use VAD, DFM, or Frame Relay.

A certain amount of bandwidth is reserved for each trunk (using **cnftrk**). The reserved bandwidth is available only for high priority packets (for example, PCC traffic). The node cannot route connections using this reserved bandwidth. The following loading, in packets per second, is calculated for each trunk in each direction:

total trunk capacity = current load + open space + statistical reserve

If the **dspload** arguments include a trunk number, detailed information for each of the packet types on that line appears. See Example 2. Additional categories of information for Frame Relay loads on the trunk include Cmax In Use, Cmax Available, and Cmax Capacity.

As shown in Example 3, the **dspload** screen will also display the configured Trunk Cost and the Trunk Qdelay when cost-based routing is configured.

In Release 9.2, as shown in Example 3, the **dspload** screen will also display the bandwidth used by rt-VBR and nrt-VBR connections on a trunk.

Full Name

Display connection loading

Syntax

dspload [nodename] [line number] [-j | -l]

Related Commands

dsptrkutl, cnfcmparm

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dspload

Description

Display the load for all trunks that terminate on the current node.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 11:54 PST

Trunk loads for node 'alpha'

        Units       Used        Available   Reserved    Cmax In Use Cmax In Use
PLN      Xmt   Rcv   Xmt   Rcv   Xmt   Rcv   Xmt   Rcv   XmtA  RcvA  XmtB  RcvB
10      Pkts  Pkts   1760  1744  8304  8320   600   600     0     0     0     0
14      Pkts  Pkts    504   504  6896  6896   600   600    20    20     0     0


Last Command: dspload


Next Command:
```

Example 2

dspload 10

Description

Display the load for the trunk in slot 10 of the current node.

System Response

```
sw151          TN    SuperUser       IGX 16    9.2       Aug. 26 1998 17:05 GMT

Configured Trunk Loading:  TRK sw151 10--10 sw150

       Load Type        Xmt-p  Rcv-p                           lcl
       NTS               2016   2016   Conid In Use             11
       TS                 432    432   Conid Available        1760
       Voice              208    208   Total Capacity         1771
       BData A              0      0
       BData B              0      0   Line type is Terrestrial
       CBR                  0      0   Line supports BData Load
       rt-VBR               0      0   Line does not use ZCS
       nrt-VBR             50     50
       ABR                  0      0   Traffic class:
       Total In Use      2656   2656        V TS NTS FR FST CBR nrt-VBR ABR rt-VBR
       Reserved           992    992
       Available        76352  76352
       Total Capacity   80000  80000

Last Command: dspload 10


Next Command:
```

Example 3

dspload 1.1

Description

Display the load for trunk 1 in slot 1 of the current node, which includes the Trunk Cost because cost-based routing is configured. The trunk queue delay is also displayed if routing with delay is enabled.

System Response

```
sw203          TN    SuperUser       BPX 8620    9.2       Sep. 24 1998 17:05 GMT

Configured Trunk Loading:  TRK sw203 1.1-- 1.1 sw242

       Load Type        Xmt-c  Rcv-c                         lcl
       NTS                  0      0   Conid In Use         1068
       TS                   0      0   Conid Available       703
       Voice                0      0   Total Capacity       1771
       BData A              0      0
       BData B              0      0   Trunk cost:  26
       CBR              23100  23100   Trunk V Qdelay:  2.5 msec
       rt-VBR           14300  14300   Trunk NTS Qdelay:  31.9 msec
       nrt-VBR          14300  14300   Trunk end doesn't support complex gateway
       ABR              18901  18901   Trunk is Terrestrial
       Total In Use     56301  56301   Trunk does not use ZCS
       Reserved          1000   1000   Trunk end doesn't support complex gateway
       Available        38699  38690   Traffic class:  V TS NTS FR FST CBR nrt-VBR ABR
       Total Capacity   96000  96000                   rt-VBR

Last Command: dspload 1.1


Next Command:
```

Table 10-10 dspload—Optional Parameters

Parameter	Description
nodename	Specifies the node. If you do not specify a node, the display shows loading on the local node. The node must be in the domain where the command is entered unless the node is a junction node. If the specified node is a junction node, the display shows loading for junction domain lines.
line number	Specifies the physical line whose loading information is displayed.
l | j	Specifies either a local or a junction node.

dspospace

Displays the open space for a connection route.

Full Name

Display open space for a route

Syntax

dspospace <connection | group>

Related Commands

none

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dspospace 4.1.1

Description

Display the open space for the ATM Frame Relay connection 4.1.1. The line interface card is a UFM-8C.

System Response

```
sw110          TN    SuperUser       IGX 16    9.2 Jan. 22 1998 19:11 GMT

Open Space for 4.1.1                                                 Snapshot

Domain
Local:  sw110      8--10.3sw86     6.2-- 6.1sw81
          ms_cur_pkts: 524272      ms_cur_cells: 12576
          sm_cur_pkts: 4368        sm_cur_cells: 11296





Last Command: dspospace 4.1.1


Next Command:
```

Table 10-11 dspospace—Parameters

Parameter	Description
connection	Specifies the connection.

dsprtcache

This command displays the cache of all cost-based routing connections. The optional ‘index’ parameter lets you specify a cache entry index. The optional “c” parameter clears the cache. The information displayed includes:

Full Name

Display cost-based route cache

Syntax

dsprtcache [index] [c]

[index] specifies the cache entry index

[c] specifies to clear the entire cache or a single entry

Related Commands

dspcon, cnfrtcost, cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsprtcache`

Description

Display route cache contents, and let you monitor and manually clear the cache.

System Response

```
pissaro  TN       StrataCom BPX 8620 9.2      Jun. 18 1998 11:11 GMT
Route Cache (Summary)
Index    Use      #   Cost  Delay     Restrict Load      VPC      Hops  RemoteNode
0        Yes      1   Yes   No        None     VBR       No       2     lautrec
1        Yes      6   Yes    No       *s       BDB       No       3      vangogh
2        Yes      9   Yes    No       None     BDA       No       3      matisse
3        Yes      3   Yes    No       *t       BDB       No       3      rousseau
4        Yes      1   Yes    No       None     CBR       No       3      seurat<- current
5        No       0   No     No       None     ---       No       0      ---
6        No       0   No     No       None     ---       No       0     ---
7        No       0   No     No       None     ---       No       0     ---
8        No       0   No     No       None     ---       No       0      ---
9        No       0   No     No       None     ---       No       0      ---
10       No       0   No     No       None     ---       No       0      ---
11       No       0   No     No       None     ---       No       0      ---

Last Command: dsprtcache

Next Command:
```

Table 10-12 dsprtcache—Parameters

Parameter	Description
index	Specifies a particular route entry within the cache. When used with the c parameter, the route is either displayed or cleared from the cache.
c	Clears the cache, or if you also enter the index parameter, clears the route cache specified by the index number.

dsprts

Displays the routes used by all connections at a node. The display shows the trunk numbers and names of all nodes in the path. For FastPAD connections, the displayed connection routes terminate at the IPX or IGX nodes. A blinking trunk indicates a failed line. A tilde trunk (~) indicates a satellite line.

The command **dsprts** displays the current cost for all connection routes. A derouted connection shows no current cost. A connection route optimized with trunk delay shows the current total delay. A highlighted connection on the display has exceeded the maximum route cost.

Full Name

Display connection routing

Syntax

dsprts [start group | chan] [nodename]

Related Commands

cnfpref

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dsprts

Description

Display the connection routes.

System Response

```
sw203          TN    SuperUser       BPX 8620    9.2    Sep. 24 1998 17:47 GMT

Conn    Route
9.1.1.*             (Cost =  5)
        sw203    1.1-- 1.1sw242
Pref:   Not Configured
9.2.5.100           (Cost =  1)
        sw203    3.1.1-- 2.1.1sw242
Pref:   Not Configured
9.2.5.101           (Cost =  1)
        sw203    3.1.1-- 2.1.1sw242
Pref:   Not Configured
9.2.5.102           (Cost =  5)
        sw203    1.1-- 1.1sw242
Pref:   Not Configured



This Command: dsprts


Continue?
```

Table 10-13 dsprts—Optional Parameters

Parameter	Description
start group or channel	Specifies the starting group or channel with which to begin the display. Channel displays are in numeric order. If no starting channel is specified, the display begins with the first connected channel. Start channel is specified in one of the following formats: Voice connection: *slot.channel* Data connection: *slot.port* Frame relay connection: *slot.port.DLCI* Frame relay connection group: *remote node.groupname* Access device connection: *slot.port.device_ID* FastPAD voice connection: *slot.port.subport* FastPAD data connection: s*lot.port.subslot.subport*
node name	Specifies that connections from only the local node to the current node are displayed. If no *nodename* is entered, connections from the local node to all other nodes are displayed.

dsptrkutl

Displays dynamic utilization information for a specified trunk. The trunk must be upped and added to use this command. The following lists the trunk utilization and terminated connection parameters included in the display. The parameter values are updated according to the specified or default interval and the screen remains displayed until the DEL key is depressed. Disabled trunks have their trunk number displayed in dim, reverse video on the screen.

If you notice that data traffic has slowed or stopped due to the very high trunk utilization due to network traffic, it may be because a node is receiving excessive volumes of network traffic (CC) traffic. In this case, the node may start dropping messages, which will result in communication breaks with other nodes as well as possible communication failures on some of its trunks.

You can detect the excessive traffic by displaying various statistics such as network statistics (**nwstats**), SAR statistics (**srstats**), and check utilization of the node's trunks by using the **dsptrkutl** command. In the event of excessive traffic, these command displays will show values that are increasing at a high rate. (See the **cnfnodeparm** parameters Enable Degraded Mode, Auto Switch on Degrade, and Max Degraded Aborts for descriptions of how to set parameters so that if a node has exhausted its internal resources due to excessive messaging (among other possible causes), which leads the node to abort, the node will either switch to the standby CC if available, or it will enter degraded mode (if the **cnfnodeparm** Enable Degraded Mode parameter is enabled).

Table 10-14 Trunk Utilization Parameters and Statistics

Trunk Utilization Parameters and Statistics	Description
Elapsed Time (seconds)	Elapsed time in seconds.since the command was started
Total Packets Transmitted	Number of packets transmitted during the elapsed time.
Overall Packet Rate	Number of packets transmitted per second during the (pkts/sec)elapsed time.
Overall utilization	Bandwidth used, expressed as a percentage of the available bandwidth during the elapsed time. This is: 100 x ("Total packets transmitted")/("Elapsed Time" x bandwidth (in packets per second)).
Peak Interval Utilization	Bandwidth used, expressed as a percentage of the available bandwidth during the peak interval. This is: 100 x ("Total packets transmitted")/("Peak Interval" x bandwidth (in packets per second)).
Last Interval (seconds)	Elapsed time, in seconds, for the last screen update interval.
Interval packets generated	Number of packets transmitted during the last interval.
Interval packet rate (pkts/sec)	Number of packets transmitted per second during the last interval.
Interval utilization	The used bandwidth expressed as a percentage of the available bandwidth during the last interval. The derivation of interval utilization is as follows: 100 x ("Interval packets transmitted") / ("Last Interval" x bandwidth (in packets per second)).
Total Connections	Total number of connections routed over the trunk.
Terminated/Via	Terminated: Number of connections routed over the trunk that terminate at this node. Via: Number of connections routed over the trunk that do not terminate at this node.

Table 10-15 Terminated Connection Statistics

Terminated Connection Statistics	Description
Voice terminated	Number of voice connections terminated at this node that are routed over his trunk.
Data terminated	Number of data connections terminated at this node that are routed over this trunk.
Frame relay terminated	Number of Frame Relay connections terminated at this node that are routed over this trunk.
Num voice offhook	Number of voice connections off-hook that are terminated at this node and routed over this trunk.
Connection Type	Voice connection types: c, a, v, p or t.
Connection Num	Number of terminated voice connections of each type: c, a, v, p and t.
Modem On	Number of terminated connections with modem detected.
Modem V.25	Number of terminated connections with V.25 modem detected.
VAD Enabled	Number of terminated connections with VAD enabled.

Full Name

Display trunk utilization

Syntax

dsptrkutl <trunk number> [interval]

Related Commands

dspload, dspchhist, dsptrkhist

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	Yes

Example 1

dsptrkutl 5.3

Description

Display trunk utilization for port 3 of the BNI in slot 5. The node is a BPX.

System Response

```
bootzilla         TN    SuperUser       BPX 8620  9.2       Aug. 27 1998 15:21 GMT

TRK  5.3 Utilization Display

Elapsed time (seconds)         160.1         Terminated Connection Statistics
Total cells transmitted        30            Voice terminated         0
Overall cell rate (cells/sec)  0             Data terminated          0
Overall utilization            0%            ATM and FR terminated    1584
Peak interval utilization      1%            Num voice OffHook        0
Last interval (seconds)        5.1
Interval cells generated       0             Connection   Modem Modem VAD
Interval cell rate (cells/sec) 0             Type   Num   On    V.25  Enabled
Interval utilization           0%            c      0     0     0     0
                                             a      0     0     0     -
Terminated Connections         1584          v      0     0     0     0
Via Connections and Groups     0             p/t    0     0     0     -


This Command: dsptrkutl 5.3


Hit DEL key to quit:
```

Table 10-16 dsprtkutl—Parameters

Parameter	Description
trunk number	Specifies the number of the trunk in the format *slot.trunk*. If the card has only one trunk, you can enter just the slot.

Table 10-17 dsptrkutl—Optional Parameters

Parameter	Description
interval	Specifies the number of seconds between screen updates. The range is 1–60. The default is 5.

prtrts

Prints the connection routes for channels on the IGX node. It uses the same syntax and prints the same information as the **dsprts** command. See the **dsprts** description for output information.

Full Name

Print connection routes

Syntax

prtrts [start_channel] [dest_nodename]

Related Commands

dsprts

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

prtrts

Description

Print connection routes.

System Response

None available as command produces hardcopy.

Table 10-18 prtrts—Optional Parameters

Parameter	Description	
start channel	Specifies the channel with which to print. Channels are printed in numeric order. If no starting channel is specified, the display begins with the first connected channel. Start channel is specified in one of the following formats:	
	slot.channel	voice connection.
	slot.port	data connection.
	slot.port.DLCI	Frame Relay connection.
	remote node.groupname	Frame Relay connection group.
	slot.port.subport	FastPad voice connection.
	slot.port.subslot.subport	FastPAD data connection.
destination node name	Specifies the printing of connection routes from only the local node to the current node. Without a specified node name, the printout shows connections from the local node to all other nodes.	

upcon

Ups (activates) a connection, bundle of connections, group of connections, or all connections with a COS or COS range. When a connection is upped, the system tries to route. If the connection cannot immediately be routed, the connection is failed and generates a major alarm. The State display column in an **upcon** or **dspcons** screen has the following meaning:

- "OK" (routed).
- "Down" (downed).
- "OK(Dn)" (waiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command.
- "Failed" (not routed, but trying).

Full Name

Up a connection

Syntax

upcon {<group | local_chan(s)> | COS <cos_range>}

Related Commands

dncon, dspcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

upcon 5.1

Description

Activate connections 5.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:33 PST

 Local      Remote      Remote                                         Route
 Channel    NodeName    Channel    State   Type    Compression   Code Avoid COS O
 5.1        beta       )25.1       Ok      256                   7/8          0  L
 9.1.100    gamma       8.1.200    Ok      fr                                 0  L
 9.1.200    gamma       8.1.300    Ok      fr                                 0  L
 9.2.400    beta        19.2.302   Ok      fr(Grp)                            0  L
 14.1      )gamma       15.1       Ok      v                                  0  L









Last Command: upcon 5.1


Next Command:
```

Example 2

upcon 9.1-4

Activate a range of connections 9.1-4

Example 3

upcon alpha

Activate a Frame Relay group connection

Example 4

upcon 9

Activate all downed connections with a COS of 9

Example 5

upcon cos 9-12

Activate all downed connections with a COS of 9-12

Table 10-19 upcon—Parameters

Parameter	Description
group or channel(s)	Specifies a group, a channel, or a range of channels to activate.
COS /cos range	Specifies the COS or COS range. The range is 0–15.

Synchronizing Network Clocks

This chapter describes how to synchronize a network and the commands related to synchronization.

Understanding Network Synchronization

Available clock sources are defined within the network as primary (p), secondary (s), or tertiary (t). This hierarchy is based on clock source stability. Each trunk that can pass clock synchronization is defined. Each network node's clock is based on the most stable clock source. If multiple, equal clock sources are available, each node chooses the closest one (measured in number of hops).

Clock sources can be changed by you or automatically by a node. If there are no primary, secondary, or tertiary clock sources defined or working in a network, then the internal oscillator of one node is automatically selected as the active network clock source.

Whenever a clock source changes—because of a line repair or an operator's command, for example—the node ensures that the clock path remains hierarchical. Also, whenever a subnetwork is merged with another subnetwork, each node in the new network verifies that it has the nearest, most stable clock that is available.

A continuous clock test compares the frequency of the node clock source to a reference on the control card. If it detects a clock source outside preset frequency limits, the controller declares the source defective and selects another source.

Defining Clocks and Lines

Ordinarily, a network's clock sources and line characteristics are configured as part of the node installation process. Thereafter, clock sources are redefined when a network is reconfigured or a line status is changed.

Clock sources are manually defined as primary, secondary, or tertiary. The definition depends on the stability of the clock source. Considerations for assessing and defining clock sources include:

- Stratum level of each clock source
- Reliability of each clock source (Figure 11-1 illustrates clock source reliability)
- Network configuration (topology, backbone, ring, star, mesh, and so on)
- Availability of multiple clock sources in a plesiochronous network

A plesiochronous network is a network in which there are two or more independent, active clock sources. For example, a network in which multiple vendors provide multiple lines that require clock mastership can be a plesiochronous network. The following depicts clock source reliability.

Figure 11-1 Clock Provided by Vendor

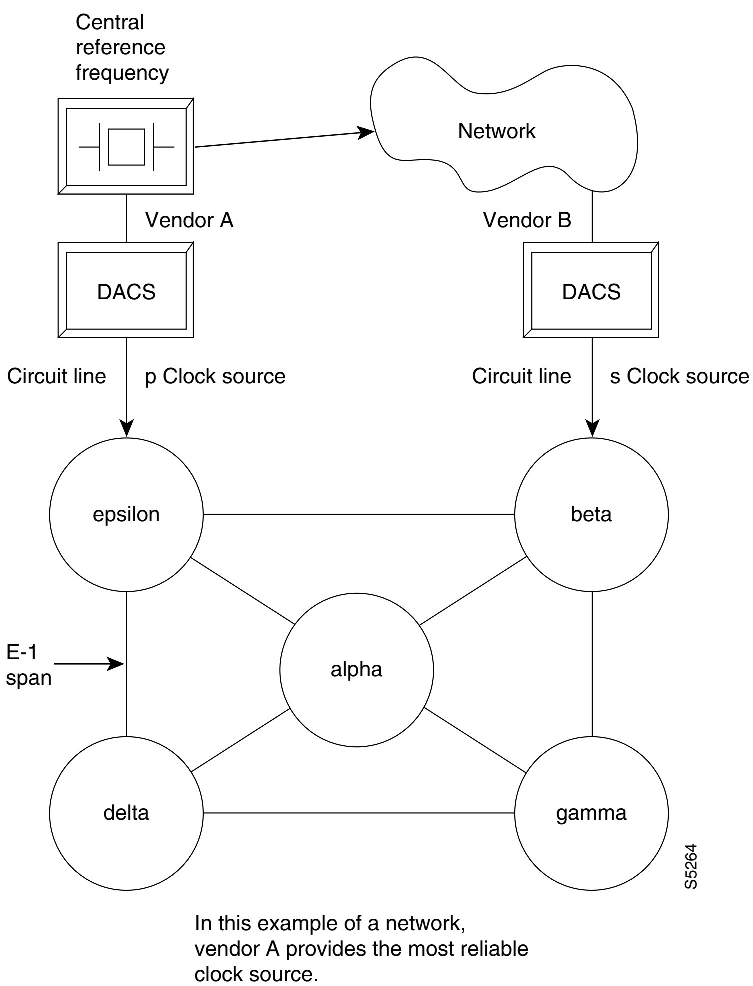
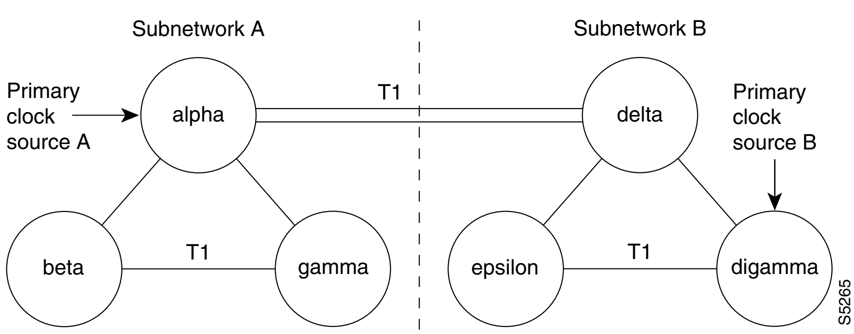


Figure 11-2 Clock Source in Node



If the packet lines in the T1 span between nodes alpha and delta are defined to pass clock synchronization, then node delta could attempt to synchronize with primary clock source A as well as with primary clock source B, because the distance in hops (instead of miles or kilometers) is the same: one.

If the packet lines in the T1 span from node alpha to node delta are defined not to pass clock synchronization, then a plesiochronous network would result.

One trunk parameter is the ability to pass a clock. A line passes a clock if the clock information transmitted from one end arrives as the identical clock at the other end. Normal T1 or E1 lines pass clock. Lines that do not normally pass clock include:

- Satellite lines.
- Lines that pass through a DACS (Digital Access Cross-connect Switch).
- Subrate lines

A long-distance line that passes through another provider's network may or may not pass clock. The default ability for an IGX trunk is to pass clock. The following applies to clocks and lines:

- Defining a trunk as a *clock source* is incompatible with defining it as passing clock.
- In an IGX/BPX network, a *clock source* functions as a source for the entire network.
- A trunk should be defined as a clock source only if a DACS-type device connects to the trunk.

Synchronizing the Network

Network synchronization includes specification of primary, secondary, and tertiary clock sources. The latter two sources serve as backups in case of clock failures. The **cnfclksrc** command specifies the source of a clock and can remove a previously specified clock source. Multiple primary sources, multiple secondary sources, and multiple tertiary sources are allowed.

The designation of the clock source depends on the stratum (or stability) of the clock source. Each node in the network synchronizes to the nearest (fewest number of hops) primary clock source. If no primary source is available, the nearest secondary clock source is used, and so on. If no other source is available, the network synchronizes to the internal oscillator of one of the nodes in the network. The following commands manage the network clocks.

- **cnfclksrc** Specifies a primary, secondary, or tertiary clock source in a network.
- **dspclksrcs** Displays all the currently defined clock sources.
- **dspcurclk** Displays the current clock source that the network is currently using.
- **clrclkalm** Clears an alarm associated with a clock source. The cause of an alarm usually clock source that fails or is outside of the frequency limits. You must clear a clock alarm before the corresponding clock source is usable.

Summary of Commands

Table 11-1 shows the name and starting page for the description of synchronization commands.

Table 11-1 Commands for Clock Synchronization

Command	Description	Page
clrclkalm	Clear clock alarm	11-4
cnfclksrc	Configure clock source	11-5
dspclksrcs	Display clock source	11-7
dspcurclk	Display current clock	11-9

clrclkalm

Clears the alarm status of a clock source after a problem is cleared. (The alarm can be a “Bad Clock Source” or “Bad Clock Path.”) Before the node can use the original clock source, you must clear the alarm with **clrclkalm**. The system displays no messages after execution.

Full Name

Clear clock alarm

Syntax

clrclkalm <line type> <line number>

Related Commands

cnfclksrc, dspclksrcs, dspclns, dspcurclk, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX, BPX	Yes

Example 1

```
clrclkalm  c  12
```

Description

Clear a clock alarm on circuit line 12.

Example 2

```
clrclkalm  p  12
```

Description

Clear clock alarm on trunk 12.

Table 11-2 clrclkalm—Parameters

Parameter	Description
c/p	Specifies the type of line. A "c" indicates a circuit line. A "p" indicates a trunk.
line number	Specifies the number of the circuit line or trunk.

cnfclksrc

Specifies a network-wide clock source. The clocking scheme ensures that all nodes in the network automatically synchronize to the nearest, most stable clock available. After you specify a clock source, the location and type of the network clock source goes out to all nodes in the network. This synchronization remains in effect despite line failures, power outages, controller card switchovers, line repairs, and the joining of subnetworks and all other network topology changes. Each node in the network maintains a list of the available clock sources for the network.

A clock *source* can be either circuit line (C), a trunk (P), or an external source (E). The clock *type* can be primary (P), secondary (S), or tertiary (T). To remove a clock source, enter its type as "r" at the end of the **cnfclksrc** command line.

Designation of the clock type depends on the stratum (or stability) of the clock source. In a large network, for example, you could designate all stratum 2 clocks as "primary," all stratum 3 clocks as "secondary," and all stratum 4 clocks as "tertiary." The network regards all primary clocks as equal in the network clocking hierarchy, regards all secondary clocks as equal, and regards all tertiary clocks as equal. Each node synchronizes to the highest stratum clock source that is available. If multiple, equal clock sources are available, the node synchronizes to the source that is physically the closest. If none of the sources is available, the network synchronizes to the internal oscillator of one of the nodes in the network. When you are planning clock sources, consider the following:

- The **dspclksrcs** command displays all clock sources in a network. The **dspcurclk** command displays the clock source that a specific node is currently using and the path between the source and the local node.
- To avoid unnecessary clock disruptions, configure all primary clock sources for the network first.
- A line must be *upped* and not in an alarm before you can configure it as a network clock source.
- Before you define a trunk as a clock source, use **cnftrk** to specify that the trunk does not pass synchronization.

Full Name

Configure network clock source

Syntax

cnfclksrc <line type> <line number> <source type> [freq]

Related Commands

dspclksrcs, dspcurclk

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
1	No	Yes	IGX, BPX	Yes

Example 1

```
cnfclksrc c 15 p
```

Description

Configure circuit line 15 as a primary clock. The network clock sources screen shows that circuit line 15 has been configured as a primary clock source for the network.

System Response

```
bootzilla       TRM   YourID:1        IGX 8420   9.2    Aug. 15 1998 15:31 MST

                            Network Clock Sources

Primary
bootzilla CLN   15

Secondary
None

Tertiary
None






Last Command: cnfclksrc c 15 p


Next Command:
```

Table 11-3 cnfclksrc—Parameters

Parameter	Description
line type	Specifies whether the clock source is a trunk (p), circuit line (c), or external (e).
line number	For a network clock source of either a circuit (c) or trunk (p), this specifies the back slot location of the source. For external clock sources (e), enter either front card slot 1 or 2 as long as either slot has a card. This external source designation applies to IGX, and BPX nodes.
source type	Specifies where the clock fits in the hierarchy: p = primary; s = secondary; and t = tertiary. To remove the clock source configuration for the current type and line, enter an “r.”

Table 11-4 cnfclksrc—Optional Parameters

Parameter	Description
freq	Specifies the frequency of the clock source. An entry is necessary only if the *line type* is an external line. The supported frequencies are 1.544 MHz and 2.048 MHz. Enter a “1” for 1.544 MHz or a “2” for 2.048 MHz.

dspclksrcs

Displays all clock sources for the network. The display for unreachable or failed clock sources flashes on and off.

Full Name

Display network clock sources

Syntax

dspclksrcs

Related Commands

cnfclksrc, dspcurclk

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

```
dspclksrcs
```

Description

Display the network clock sources.

System Response

```
bootzilla       TRM   YourID: Numba 1   IGX 8430    9.2    Aug. 15 1998 15:32 MST

                            Network Clock Sources

Primary
bootzilla CLN   15

Secondary
None

Tertiary
None





Last Command: dspclksrcs


Next Command:
```

dspcurclk

Displays the current clock source. The display for **dspcurclk** contains the following information:

- Source Node: The node in the network where the clock source originates.
- Source Line: the type of line used as the clock source and its back slot number (for example, “CLN 15", TRK 22, “EXTERNAL 2”, or “INTERNAL”).
- Clock Type: the clock type configured for the source clock (primary, secondary, or tertiary). If the source clock for the node is an internal oscillator, no clock type is given.
- Clock Frequency: the received clock frequency as measured by the local NPC/BCC.
- Path to Source: the path from the current node to the node of the originating clock source. This includes all intermediate nodes and trunks.

Full Name

Display current clock sources

Syntax

dspcurclk

Related Commands

cnfclksrc, dspclksrcs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspcurclk`

Description

Display the current clock source.

System Response

```
bootzilla           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:33 MST

                             Current Clock Source

Source Node:     gamma
Source Line:     Internal
Clock Type:
Clock Frequency: 1544015

Path to Source:
   bootzilla 9--10gamma







Last Command: dspcurclk


Next Command:
```

Managing Jobs

A *job* is a user-specified string of commands. A job can automatically execute on a prearranged schedule or upon an event trigger. This chapter describes the commands that let you:

- Create a job
- Run a job
- Stop a job
- Display one or more jobs
- Edit a job
- Delete a job
- Create a job trigger

The system assigns a number to a new job. This *job number* identifies the job and is a required parameter for most job control commands. When you create a new job, the current privilege level is automatically saved as the privilege level of the job. Only commands that are available at your privilege level can be in your job specification. For example, a user whose highest privilege level is 3 cannot include the **addtrk** command in a job because **addtrk** requires a level 1 privilege. This privilege requirement also applies to other job functions, such as running, editing, or stopping a job.

Not all Cisco WAN Switching commands can execute as a part of a job. For this reason, the Attributes section of each command description in this manual states whether the command can function in a job.

Creating (Adding) a Job

Consider the following before creating a job:

- The **addjob** command creates a new job. When you use **addjob**, the system prompts for optional and required arguments. Unlike other commands, the **addjob** command begins with optional parameters. A job can run when you execute the **runjob** command or at a time and date you specify with **addjob**. Note that the system increments the job number, but you can assign a job description to indicate the function of the job. The following list describes the **addjob** parameters:
  - Description (optional): this can contain up to 16 characters and include spaces.
  - Execution time (optional): if you specify an execution time, the first (unprompted) parameter to enter is four digits indicating the year. The system subsequently prompts for the month, day, hour, minute, and (optional) second of the start time for the job.

- Interval (optional): the Interval prompt appears only if you have specified an execution time. The first interval prompts you for units: *days*, *hours*, and *minutes*. The system then prompts you for the number of units.
- Command (required): without a command specified, the **addjob** command terminates, so this is how you exit **addjob**. After each command and its parameters, the system prompts you for an action to take if a failure occurs (see the **addjob** description for details).

- Because commands in a job do not immediately execute, the system does not check the validity of the commands and parameters to the same degree as it does for standard command entry. For example, if you enter **dncd** for a card slot that is out of range, the system flags the error, but it does not flag a card that is missing from a valid card slot.

Running a Job

The following steps aid in running a job:

- Use the **runjob** command to run a job manually. Specify the job number to run.
- While a job is running, "executing" flashes in the upper-left area of the screen.
- The **runjob** command runs a job regardless of the assigned execution time. The **runjob** command does not change the specified execution time.
- The **runjob** command itself can be in a job. Therefore, running one job can cause another job to start. The limitation to this is that a job cannot cause itself to run. For example, Job 1 cannot contain the command "runjob 1." Also, Job 1 cannot have the command "runjob 2" if Job 2 contains the command "runjob 1."
- After **runjob** executes, the screen displays the results for each command in the job.

Stopping a Job

The following steps aid in stopping a job:

- Use the **stopjob** command to stop a running job. The template for the current job appears on the screen along with the prompt, "Stop this and all currently executing jobs (y/n)?"
- The **stopjob** command works only on a job that is running. Because stopping a job can leave a task partially completed, use **stopjob** with caution.

Displaying Jobs

For displaying one or all jobs:

- Use the **dspjob** command to display the status of a job. This command displays the template for the specified job and includes the results of the last run for each command in the job.
- To display details of all current jobs, use the **dspjobs** command.

Editing a Job

The following information applies to editing a job. Before using an edited job, test it to ensure that it works.

- Use the **editjob** command to edit job parameters.

- When you enter the **editjob** command, the template of the specified job appears. The system prompts you to keep or change each item in the template. To change an item, type over the existing information, then press Return. (You can use any of the Control keys to edit existing information.) To keep the same parameter specification, press Return at the prompt.
- To insert a new command between existing commands in a job, press the ^ key while holding down the Control key. A new line opens above the command that is currently highlighted. Enter the new command at the “Enter Cmd” prompt.
- To delete a command from a job, two methods are available. One way is to backspace over the command when it appears on the command line, then press Return. The other way is to press the “x”-key while holding down the Control key.
- When commands are added to or deleted from a job, the system re-numbers the remaining commands.

Deleting a Job

Use the **deljob** command to delete a job. You cannot delete a job that is running. If necessary, stop the job with the **stopjob** command before deleting it.

Creating a Job Trigger

The following information applies to creating a job trigger:

- Use the **addjobtrig** command to configure a job to run if a line failure or repair-alarm occurs. (A “repair-alarm” occurs when a line or trunk is back up, and a message is sent to the event log.)
- The template on the screen prompts for a line type: “p” for packet line or trunk, “c” for circuit line, or “d” for a T3 (DS3) line. (Do not use the “d” option, as it represents the MT3 card, which is obsolete.)
- The template on the screen prompts for the slot number of the line on which an alarm triggers the job.
- The prompt requests you to specify whether the trigger should occur on the failure (“f”) or repair (“r”) of a line. Typically, you write a job that would run whenever a line fails, so you create its trigger with the “f”. Then you would write another job (to reverse the effects of the first job) that would run when the line repairs. This trigger would occur on the “r”, or repair of the line.

Summary of Commands

Table 12-1 shows the full command name and starting page for the description of each command.

Table 12-1 List of Job Commands

Command	Description	Page
addjob	Add a job	12-5
addjobtrig	Add a job trigger	12-8
deljob	Delete a job	12-11
deljobtrig	Delete job trigger	12-13
dspjob	Display a job	12-15
dspjobs	Display jobs	12-17
editjob	Edit a job	12-19
prtjob	Print a job	12-19
prtjobs	Print jobs	12-22
runjob	Run a job	12-23
stopjob	Stop a job	12-25

addjob

This command creates a new job. When you create a new job with **addjob**, your privilege level becomes the privilege level of the job itself. When adding commands to the job, you cannot add a command that requires a privilege higher than your privilege level. Furthermore, you must have a privilege level at least as high as the job to run the job (with **runjob**, for example).

The system does not check the commands' validity with respect to the current state of the network or for relationships to other commands in the job. To ensure that it works as expected, try running the job with **runjob**.

Full Name

Add a job

Syntax

addjob [description] [execution time, execution interval] <commands>

Related Commands

deljob, dspjob, dspjobs, editjob, prtjob, runjob, stopjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

```
addjob
```

Description

The system response is a series of prompts requesting details of the job. The system requests a job description (or name), an execution time for the job, a unit for the interval at which the job is to run (hours, for example), the number of units in the interval, the commands to execute, and what to do with the result.

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:15 PST

                                  Job 1   test
Last Execution Results: None                     Status: Idle
Next Execution Time: 08/17/97 20:20:30           Interval: 1 days

 1: prtlog
   - Failure Reaction: Repeat 2 Times and Abort        Exec. Results: None








Last Command: addjob


Next Command:
```

In this example, a new job is being created. The job number is “1.” The job description (or name) is “test.” The job is scheduled to run on August 17, at 2:20:30 PM and every day thereafter at the same time. The command in the job is **prtlog**. If this command fails when the job runs, it tries twice again and aborts if unsuccessful.

The “Enter Cmd” prompt at the bottom of the screen indicates you can enter the next command for the job. To exit **addjob**, press the **Return** key without entering a command.

Table 12-2 addjob–Parameters

Parameter	Description
command	Specifies the syntax for a command to include in the job. The number of commands that can be included in a job is limited only by available memory. Not all commands can be included in a job. A job cannot contain commands that are above your privilege level. For example, if you have privilege level 3, your job cannot include the **addtrk** command because this command requires privilege level 1.
failure reaction	Specifies the desired reaction to the failure of a command in the job. Each command in the job must have a failure reaction. The failure reaction is specified in the following format <c | a | rc | ra> <*number of repetitions*>. In this format: **c** specifies that the job continues running. **a** specifies that the job must abort. **rc** specifies that the command should retry for the specified number of times and continue running the job even if the command fails during the retries. **ra** specifies that the command should retry for the specified number of times and abort the job if the command always fails during the retries.

Table 12-3 addjob–Optional Parameters

Parameter	Description
job description	A user-specified description of the job. This description can be up to 16 characters, including spaces.
execution time	Specifies the date and time to run the job. Without an execution time, the job can begin running only by the **runjob** command. Execution time is specified in the following format. (The *seconds* parameter is optional.) year (four digits) month (two digits) day hour (0–23) minute [seconds]
execution interval	Specifies an interval between job repetitions. The three possible execution intervals are: **d** (days) **h** (hours) **m** (minutes) The interval range is 1 minute to 45 days. If you do not specify an execution interval, the job runs once at execution time. If you specify an execution interval (**d**, **h**, or **m**), you must also specify the number of units in the interval.

addjobtrig

Configures a job to run if a failure or repair occurs on a trunk (narrowband or broadband), a line (voice, data, Frame Relay, ATM, narrowband, broadband), or a T3 (DS3). You can also use **addjobtrig** to allocate or release bandwidth from other connections. This bandwidth decision depends on whether the EIA lead status is "up" or "down." For example, a job can be triggered to run if the RTS lead of an HDM/LDM port changes state. If the FRM you are using is an FRM-T1 or E1, it qualifies as a line and can be used as a job trigger.

A "line failure" is any alarm condition that takes the trunk or line out of service. Such a condition is always a major alarm. However, not all major alarms cause the trunk or line to be considered failed. Those that are considered failed are the ones that appear on the **dsptrks** or **dsplns** screens with a color associated with it, such as "Major - Local All Ones" or "Major - Remove Packet Out of Frame (Yel)". Specifically excluded are all the statistical alarms, some of which may be major.

A "line repair" is the opposite of a "line failure". A "repair" of a line occurs when the alarms on the line are removed.

In this release, the lead type on HDM/LDM is based on the configuration from **cnfleadmon**. The display now show "Front Card Supports Lead State Trap".

Full Name

Add a job trigger

Syntax

addjobtrig <job_number> <line_type> <line_specifier> <fail/repair>

Related Commands

addjob, dspjob, dspjobs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	No	IGX, BPX	Yes

Examples

addjobtrig	1 p 14 f	trigger job 1 when TRK 14 fails
addjobtrig	3 c 15 r	trigger job 3 when CLN 15 repairs
addjobtrig	2 p 14 r	trigger job 2 when TRK 14 repairs
addjobtrig	3 d 27 E f	trigger job 3 when DS3 27 E (East) fails

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:22 PST

Job   Description       Next Execution      Status     Interval    Access Group
1     test              08/17/97 11:00:00   Idle       1 days      Group 1
      Trigger 1 -  CLN 14         REPAIR









Last Command: addjobtrig 1 c 14 r


Next Command:
```

Example 2

`addjobtrig 1 c 14 r`

Description

Trigger job 1 whenever a repair of line 14 occurs.

Table 12-4 addjobtrig—Parameters

Parameter	Description
job number	Specifies the number of the job to trigger.
line type	Specifies the type of line. A “p” indicates any type of trunk (TRK). A “c” indicates any type of circuit line. (A “d” indicates a DS3 line. Do not specify the “d” option, as this represents a now-obsolete card—the MT3.)

Table 12-4 addjobtrig—Parameters (Continued)

Parameter	Description
line specifier	Specifies the slot number for trunks and lines. Use the standard nomenclature to designate trunks and lines. For example, depending on the card type (single-line or multi-line), specify either <*slot.port*>, or just <*slot*>.
fail/repair	Specifies whether the trigger occurs on the failure or repair of a line.
fail/repair	If the card is an SDP, LDP, HDM, or LDM, the fail and repair triggers occur only on the transitions of RTS (regardless of whether the port is DCE or DTE). If you select “fail,” the trigger is the transition of RTS from “on” to “off.” If you select “repair,” the trigger is the transition of RTS from “off” to “on.” To enable triggering on leads other than RTS, use the **cnfict** command.

deljob

Deletes a job. To delete a job, you must have a privilege level at least as high as the job itself. A job that is currently running cannot be deleted. If necessary, use **stopjob** to stop the job so that you can delete it.

Full Name

Delete a job

Syntax

deljob <job_number>

Related Commands

addjob, dspjob, dspjobs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

deljob 4

Description

Delete job 4.

```
pubsigx1       TN    SuperUser       IGX 32    9.2       Sep. 3 1998 19:54 GMT

                                  Job 4
Last Execution Results: None                        Status: Locked
Next Execution Time:                                Interval:

 1: prtlog
   - Failure Reaction: Abort                              Exec. Results: None
 2: dncd 6
   - Failure Reaction: Repeat 12 Times and Abort          Exec. Results: None
 3: dncd 6
   - Failure Reaction: Repeat 12 Times and Continue       Exec. Results: None





This Command: deljob 4


Delete this job (y/n)?
```

Table 12-5 deljob—Parameters

Parameter	Description
job number	Specifies the number of the job.

deljobtrig

Deletes a job trigger. The **deljobtrig** command deletes one trigger at a time. If you delete a job by using the **deljob** command, all associated job triggers are deleted.

Full Name

Delete a job trigger

Syntax

deljobtrig <job_number> <trig_num>

Related Commands

addjobtrig, dspjobs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

`deljobtrig 1 1`

Description

Delete job trigger 1 for job 1.

```
pubsigx1       TN    SuperUser       IGX 32    9.2    Sep. 3 1998 18:19 GMT

Job   Description       Next Execution      Status     Interval    Access Group
1     test1                                 Idle                   SuperUser
      Trigger 1 -  PLN     2             FAILURE
2                                           Idle                   SuperUser
3     test3             09/02/97 11:11:11   Idle       1 days      SuperUser
4                                           Idle                   SuperUser
5                                           Idle                   SuperUser
6                                           Idle                   SuperUser




This Command: deljobtrig 1


Enter trigger number:
```

Table 12-6 deljobtrig—Parameters

Parameter	Description
job number	Specifies the number of the job.
trigger number	Specifies the number of the trigger to delete.

dspjob

The **dspjob** command displays the following information about a job.

- Job number and description
- Next execution date and time
- Status
- The time interval between successive executions of the job
- The results of the last execution of the job

This command requires at least the same privilege level as the person who created the job.

Full Name

Display jobs

Syntax

dspjob <job_number>

Related Commands

addjob, deljob, dspjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspjob 2`

Description

Display job number 2.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:17 PST

                                  Job 1   test
Last Execution Results: None                   Status: Idle
Next Execution Time: 08/17/97 20:20:30         Interval: 1 days

 1: prtlog
   - Failure Reaction: Repeat 2 Times and Abort        Exec. Results: None










Last Command: dspjob 1


Next Command:
```

Table 12-7 dspjob—Parameters

Parameter	Description
job number	Specifies the the number of the job to display.

dspjobs

Displays the following information on each job:

- Job number
- Job description
- Next execution date and time
- Execution interval between jobs
- Access Group: The privilege level required to run or display the job

To see details of an individual job, use the **dspjob** command.

Full Name

Display jobs

Syntax

dspjobs

Related Commands

addjob, deljob, dspjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspjobs`

Description

Display a summary of all jobs stored at the node.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:16 PST

Job   Description       Next Execution      Status     Interval    Access Group
1     test              08/17/97 20:20:30   Idle       1 days      Group 1











Last Command: dspjobs


Next Command:
```

editjob

Allows you to change any of the following items in a job:

- The job description
- Execution time
- Execution interval
- Individual commands in the job
- Failure reactions for each command

After you enter the **editjob** command, the system displays the template for the job. With **editjob**, you can edit, delete, or add a command. Each item in the template is successively displayed on the command line so that you can confirm or change the item.

You cannot change the privilege level of a job.

The following is a list of actions you can take with **editjob**:

- To change an item in the job template, enter or type over the existing information on the command line and press the Return key.
- Use any of the control keys to change information on the command line. To keep the same value of an item, press the Return key at the prompt.
- To add a new command between existing commands in a job, hold down the Control key while you press the ^ key. A new line appears above the command that is highlighted. Enter the new command after the "Enter Cmd:" prompt and press Return.
- To add a new command to the end of a job, press the Return key after the last command in the job template.
- To delete a command from a job, either backspace over the command when it appears on the command line and press the Return key, or hold down the Control key while you press the "x"–key.
- To end the editing session, press the Return key when prompted for a new command or press the Del key.

When commands are added to or deleted from a job, the system re-numbers the commands. To test an edited job, run it with the **runjob** command.

Full Name

Edit a job

Syntax

editjob <job_number>

Related Commands

addjob, deljob, dspjob, dspjobs, runjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

`editjob 1`

Description

Edit job 1. The template for job 1 appears on the screen. The system displays the existing job description, which you can change or keep. To keep it, press Return. The system then displays the execution time. To change it to August 17, 1998 at 11:00:, for example, enter:

1998 8 17 11 00

If no other items need changing, press the Return key.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:19 PST

Job 1 prtlog
Last Execution Results: None                     Status: Editing
Next Execution Time: 08/17/97 11:00:00           Interval: 1 days

 1: prtlog
   - Failure Reaction: Repeat 2 Times and Abort        Exec. Results: None
 2:








Last Command: editjob 1


Next Command:
```

Table 12-8 editjob–Parameters

Parameter	Description
job number	Specifies the number of the job to edit.

prtjob

Prints the following information about a specific job:

- Job number
- Job description
- Next execution date and time
- Status
- Interval. The time interval between successive executions of the job
- Execution. The results of the last execution of the job

To print a job, you must have at least the same (or higher) privilege level as the person who wrote the job). See the **addjob** description for more information. The **prtjob** command uses the same syntax and prints the same information the **dspjob** command.

Full Name

Print job

Syntax

prtjob <job_number>

Related Commands

dspjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

prtjobs

Prints the following information about all existing jobs:

- Job number
- Job description
- Next execution date and time
- Status
- Execution interval between jobs
- Access Group: The privilege level required to run or display the job

For a printout on a single job, use the **prtjob** command. This command uses the same syntax, and prints the same information as is displayed using the **dspjobs** command. See the **dspjobs** command for syntax and output information.

Full Name

Print jobs

Syntax

prtjobs

Related Commands

dspjobs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

runjob

Runs a job. The **runjob** command runs a job regardless of its execution time. The **runjob** command does not change a Job's assigned execution time.

When you enter **runjob**, the system displays the job template and prompts, "Run this job (y/n)?" Enter "y" to start the job. Enter "n" to exit **runjob**.

After you enter "y,." four seconds pass before a job begins running. Press any keys briefly to suspend a job. Four seconds of no keyboard activity must pass before the jobs resume. While a job is running, the system highlights the current command and updates command results.

You can include the **runjob** command in a job. Therefore, running one job can cause another job to run. The only limitation is that a job cannot cause itself to run. For example, Job 1 cannot include the command "runjob 1." Also, Job 1 cannot include the command "runjob 2" if Job 2 contains the command "runjob 1."

Full Name

Run a job

Syntax

runjob <job_number>

Related Commands

addjob, dspjobs, editjob, stopjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX, BPX	Yes

Example 1

```
runjob 1
```

Description

Run job 1

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:23 PST

                                  Job 1   test
Last Execution Results: None                     Status: Idle
Next Execution Time: 03/17/96 11:00:00           Interval: 1 days

 1: prtlog
   - Failure Reaction: Repeat 2 Times and Abort        Exec. Results: None










This Command: runjob 1


Run this job (y/n)?
```

Table 12-9 runjob—Parameters

Parameter	Description
job number	Specifies the number of the job to run.

stopjob

Stops all running and all waiting jobs. When you enter the **stopjob** command, the system prompts, "Stop all running and waiting jobs (y/n)?" Enter a "y" to stop running jobs and prevent all waiting jobs from beginning. Enter an "n" to exit **stopjob**. Because the **stopjob** command can leave a task partially executed, use **stopjob** with caution. You must have at least the same or higher privilege level of the creator of the jobs you want to stop.

Full Name

Stop job

Syntax

stopjob

Related Commands

runjob

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`stopjob`

Description

Stop all jobs currently running or queued to run on the node. Confirm by entering: y.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 14:24 PST

                                  Job 1   test
Last Execution Results: None                  Status: Idle
Next Execution Time: 03/17/96 11:00:00        Interval: 1 days

 1: prtlog
   - Failure Reaction: Repeat 2 Times and Abort        Exec. Results: None








This Command: stopjob


Stop all running and waiting jobs (y/n)?
```

Managing the Network

This chapter tells you how to use network administration commands. Examples of the tasks these commands perform are: creating a password, setting the network date and time, and adding a user.

Signing on to the System

Signing on to a node is a two-step process that requires you to enter a User ID and a password. The system or network administrator can provide a User ID and password to you. The User ID can be up to 12 characters. To protect the security of the system, you should change your password regularly. Only your system administrator can change the User ID. To sign on to a node:

Step 1 Enter your user ID at the system prompt "Enter User ID."

Step 2 Enter your password at the "Enter Password" prompt. For initial sign-on, enter the password that the system administrator provides. You can change the password with the **cnfpwd** command.

After you sign on, the system is ready and so prompts you for the next command.

Signing Off the System

When you have completed a session and want to sign off, use the **bye** command. This command returns the display to the initial system sign-on prompt. If you enter the **bye** command when you have a virtual terminal connection to another node, the **bye** command ends the virtual terminal session and returns to the a local session. To end the local session and thus sign-off the system, again enter the **bye** command.

Creating a New Password

To change the password, takes the step in the list that follows. given to you by your System Administrator, or to change your present password to a different one, perform the following. To ensure the security of your system, your password should be changed on a regular basis. See the System Administrator for the recommended frequency of change.

Step 1 Enter the **cnfpwd** command. The system prompts for your current password.

Step 2 Enter your current password. The system prompts for a new password.

Step 3 Enter a new password. Passwords must have 6–15 characters. The system prompts you to confirm the new password by typing it again.

Set Date and Time

Date and time are network-wide parameters. You can set the time zone for each node. The **cnfdate** command lets you set both time and date. The **cnftime** command lets you set the time for the entire network.

Summary of Commands

Table 13-1 shows the full name and starting page for the description of each network management command.

Table 13-1 Commands for Managing a Network

Command	Description	Page
adduser	Add user(s)	13-3
cnfpwd	Configure password	13-5
cnffwswinit	Configure Cisco WAN Manager node IP address firmware/software initiator	13-6
cnfsnmp	Configure SNMP parameters	13-7
cnfstatmast	Configure statistics master SV+ address	13-8
cnfsysparm	Configure system parameters	13-9
deluser	Delete user	13-14
dsplanip	Display LAN IP address of all nodes in network	13-15
dspnwip	Display network IP interface	13-17
dsppwd	Display password	13-18
dspsnmp	Display SNMP parameters	13-20
dspsnmpstats	Display SNMP statistics	13-22
dspsv3	Display WAN Manager Layer 3 Link Control Blocks	13-24
dspusers	Display users	13-24
dspusertask	Display user task	13-33
dspusertasks	Display all user tasks	13-36

adduser

Adds a user to the network. The first time the new user ID is used for logon, a prompt appears asking the user to change from the default password to a new password which they enter using the **cnfpwd** command. Users with privilege levels 1 through 5 may add users with lower privilege levels. Since privilege level 6 has no user levels below it, level 6 cannot add any users.

Full Name

Add a user

Syntax

`adduser` <user_id> <privilege_level>

Related Commands

cnfpwd, **deluser**, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX, BPX	Yes

Example 1

`adduser` sarah 5

Description

Add a user sarah with privilege level 5.

System Response

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 16 1998 13:48 PST

YourID       1
Sarah        5












Last Command: adduser Sarah 5


Next Command:
```

Table 13-2 adduser—Parameters

Parameter	Description
userid	Specifies the name of the user to add.
privilege level	Specifies the privilege level to grant to the added user. The range of levels is 1–6, where 1 is the highest level and 6 is the lowest.

cnfpwd

Changes the password associated with a User ID. To change a password, you must log into the node with the User ID whose password you want to change. Passwords are case-sensitive.

In a structured network, each domain requires you to have a password. In each domain, your password and associated privilege level can be the same of different from those in the other domains. For each domain, you can change the password at any node within the domain, including a junction node.

Full Name

Configure password

Syntax

`cnfpwd` <old password> <new password>

Related Commands

dsppwd, **adduser**, **deluser**, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

`cnfpwd`

Description

Change your password.

Table 13-3 cnfpwd—Parameters

Parameter	Description
old password	Specifies the old password.
new password	Specifies the new password. Passwords must have 6–15 characters. Only letters, numbers, "_", and "-" are allowed in a password. Spaces are not allowed.

cnffwswinit

Use the **cnffwswinit** command to inform the IGX/BPX the IP address of the machine that will be used to initiate a firmware or software download. This is used as a sort of a safety measure, to prevent downloads from being started anywhere in the network. You must have access to a node, and use the **cnffwswinit** command to set the IP address before a download will be accepted from that address.

Full Name

Configure firmware and software downloader's WAN Manager IP address

Syntax

cnffwswinit <IP address of download initiator>

Related Commands

dsppwd, **adduser**, **deluser**, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example

cnffwswinit 172.29.52.17

Description

Configures the IP address of the machine running WAN Manager from which the firmware and software download will be initiated to other nodes. If you do not provide the IP address for the WAN Manager node from which to initiate the firmware/software download, you will be prompted to enter it.

Table 13-4 cnffwswinit–Parameters

Parameter	Description
IP address	Specifies IP address of machine running WAN Manager from which the firmware and software download will be initiated to other nodes in the network.

cnfsnmp

Configures the SNMP GET and SET community strings.

Full Name

Configure SNMP parameters

Syntax

`cnfsnmp` <GET community string> <SET community string>

Related Commands

dspsnmp, **dspsnmpstats**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

`cnfsnmp`

Description

Configure the SNMP GET and SET community string parameters.

Table 13-5 cnfsnmp—Parameters

Parameter	Description
get community string	Specifies the GET community string.
set community string	Specifies the SET community string.

cnfstatmast

Configures an IP address for the Statistics Master process in WAN Manager. The **cnfstatmast** command defines the IP address for routing the messages to and from the Statistics Master in WAN Manager.

The Statistics Master process requests and receives network statistics by using TFTP Get and Put messages. These TFTP messages pass between the node and the Statistics Master over IP Relay. See the **cnfnwip** description for details on setting a node address.

Full Name

Configure statistics master SV+ address

Syntax

`cnfstatmast` <IP Address>

Related Commands

cnfnwip, **dspnwip**

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

`cnfstatmast 199.35.96.217`

Description

Configure 199.35.96.217 as the IP address for the Statistics Master.

Table 13-6 cnfstatmast—Parameters

Parameter	Description
ip address	Specifies the IP address for the Statistics Master. IP addresses have 32-bits. The format of an IP address is x.x.x.x, where x is a value in the range 1–255.

cnfsysparm

Configures various system (or network) parameters. Network-wide parameters are configurable only when all nodes in the network are reachable. The parameters you specify with this command apply throughout the network regardless of which node you execute the command from. Take special note of the consequences of how you resolve conflicting values when networks are joined.

You can select each parameter by its index number. The paragraphs that follow describe each parameter by index number. Table 13-6 lists the defaults and ranges for each parameter.

Note Using **cnfsysparm** requires caution because network rerouting or loss of data may result from changes in system parameters. If necessary, consult with the TAC before you use **cnfsysparm**.

The following paragraphs describe the user-configurable system parameters by index number.

- 1: *Maximum Time Stamped Packet Age* is the maximum age a time-stamped packet can have before the switch discards it. If networks are joined and the *Maximum Time Stamped Packet Age* in the networks differ from each other, the lower value becomes the maximum.
- 2: *Fail Connections On Communication Break* - Determines whether connections are conditioned if the node at the other end of the connection becomes unreachable. If networks with different settings are joined, the resolution is to *enable* this parameter for the new network.
- 3–7: *Maximum Network Delay* for various types of compressed voice and high-speed data connections using SDP/LDP on an IPX node or LDM/HDM on an IGX node. When the total queueing delay on a route exceeds this value, connection traffic cannot use the route. The units of measure are milliseconds. When networks with different values are joined, the lower value becomes the *Maximum Network Delay.*
- 8–12: *Maximum Network Delay* for compressed voice and high-speed data connections. When the total queueing delay on a route exceeds the specified number of milliseconds, a connection traffic cannot use the route. When networks with different values are joined, the higher value becomes the *Maximum Network Delay.* Applicable cards are the UVM, CDP, or CVM.

  Note In Release 9.1, when cost-based routing is configured, the delay cost cap is the maximum allowable end-to-end delay for the connection type. Use parameters 3 through 12 to configure this delay network-wide for all delay sensitive connections.

- 13: *Enable Discard Eligibility* (DE) bit for Frame Relay connections. Frames received with DE set have been sent on connections where the PIR has been exceeded and are eligible to be discarded. Enabling DE automatically enables CLP. CLP is disabled when Discard Eligibility is turned off except on the bursty data B queue when ForeSight is enabled.
- 14: *Use Frame Relay Standard Parameters Bc and Be* allows you to substitute the Frame Relay Forum standard Bc for VC Q depth and Be for PIR when you configure Frame Relay ports and connections. (The affected commands are **cnffrport**, **addcon** for Frame Relay, and **cnfcon**.) Screen displays for Frame Relay ports and connections reflect the choice for this parameter. Note that, if you change this parameter, a network-wide reset to the default values takes place for all Frame Relay classes, and the terminal displays a warning that the reset occurred.
- Obsolete: 15–20: *Maximum Local Delay for Interdomain UVM, CDP, or CVM to UVM, CDP, or CVM* connections is similar to parameters 8–12 described above. These parameters specify the maximum delay at the local domain in a structured network. These delays can be set only on a domain-by-domain basis (not end-to-end).

- 21: *FastPAD Jitter Buffer Size* is the size of the buffer for neutralizing jitter in connections that terminate on a FastPAD. The units of measurement are milliseconds.
- 22: *Number of Consecutive Invalid Login Attempts to Cause Major Alarm* specifies the number of failed login attempts that causes a major alarm. The default of 0 means that failed login attempts do not cause an alarm. If the threshold is set to 0, the Too Many Invalid Login Attempts service-affecting alarm is disabled and no alarm will be generated.
- 23: *Enable Connection Deroute Delay* is an enable that causes the network to wait a period of time before rerouting connections because of an error on a trunk. With *Enable Connection Deroute Delay* enabled, the network does not immediately reroute connections when statistical errors are occurring or when a trunk momentarily moves into a failure state then returns to normal operation. This feature is relevant when rerouting the connections is more of a disruption than the errors caused by the intermittent trunk.
- 24: *Frame Relay VCs Polling Rate* is the period between the start of polling cycles for both ATM and Frame Relay virtual connections. The possible values are 5, 10, and 15 seconds. As the number of connections in a network grows, greater intervals between cycles may be appropriate. The suggested intervals for the numbers of connections are:
  - — 5 minute polling for up to 4000 connections
  - — 10 minute polling for up to 8000 connections
  - — 15 minute polling beyond 8000 connections.
- 25: *Port Polling Rate* is the time between the start of polling cycles for interval statistics. The possible values are 5, 10, and 15 minutes. (To specify the particular statistics, use the statistics manager in WAN Manager.) As the number of connections in a network grows, greater intervals between cycles may be appropriate. The suggested intervals for the numbers of connections are:
  - — 5 minutes for up to 300 connections
  - — 10 minutes for up to 500 connections
  - — 15 minutes for more than 500 connections.

Table 13-7 Defaults and Ranges of cnfsysparm Parameters

System Parameters			
Index	**System-Wide Parameter**	**Default**	**Range**
1	Max Time Stamped Packet Age (in milliseconds).	40	1–60
2	Fail Connections On Communication Break.	No	y or n
3	Max Network Delay for “v” connections (in milliseconds).	14	1–255
4	Max Network Delay for “c” connections (in milliseconds).	27	1–64
5	Max Network Delay for “d” connections (in milliseconds).	14	1–255
6	Max Network Delay for “a” connections (in milliseconds).	27	1–255
7	Max Network Delay for High Speed Data connections (in milliseconds).	40	1–255
8	Max Network Delay for CDP or CVM to CDP or CVM “v'' connections (in milliseconds).	64	1–255
9	Max Network Delay for CDP or CVM to CDP or CVM “c” connections (in milliseconds).	64	1–64
10	Max Network Delay for CDP or CVM to CDP or CVM “t & p” connections (in milliseconds).	64	1–255

Table 13-7 Defaults and Ranges of cnfsysparm Parameters (Continued)

System Parameters (Continued)			
Index	**System-Wide Parameter**	**Default**	**Range**
11	Max Network Delay for CDP or CVM to CDP or CVM "a" connections (in milliseconds).	64	1–255
12	Max Network Delay for CDP or CVM to CDP or CVM High Speed Data connections (in milliseconds).	64	1–255
13	Enable Discard Eligibility (DE).	No	y or n
14	Use Frame Relay standard parameters Bc and Be.	No	y or n
15	Obsolete: Max Local Delay for Interdom CDP to CDP "v" connections.	27	1–255
16	Obsolete: Max Local Delay for Interdom CDP to CDP "c" connections.	27	1–64
17	Obsolete: Max Local Delay for Interdom CDP to CDP "t & p" connections.	27	1–255
18	Obsolete: Max Local Delay for Interdom CDP to CDP "a" connections.	27	1–255
19	Obsolete: Max Local Delay for Interdom CDP to CDP High Speed Data connections.	27	1–255
20	Obsolete: Max Local Delay for Interdom High Speed Data connections (in milliseconds).	28	1–255
21	FastPAD De-jitter Buffer Depth (in milliseconds).	15	0–255
22	Number of Consecutive Invalid Login Attempts to Cause Major Alarm.	0	3–9
23	Enable Connection Deroute Delay.	Yes	y or n
24	Frame Relay VCs Polling Rate is the number of minutes between polling cycles for both ATM and Frame Relay virtual connections in the network.	5	5, 10, or 15
25	Port Polling Rate is the number of minutes between polling cycles for interval statistics gathered for all ports in the network.	5	5, 10, or 15

Full Name

Configure system parameters

Syntax

cnfsysparm <index> <value>

Related Commands

none

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

cnfsysparm

Description

Configure system-wide parameters. In response to the prompt "Continue" at the bottom of the display enter a "y", or press Return to display the second screen, or enter "n" to not display the next screen. If you enter an "n," the prompt line requests an index number.

System Response

```
sw171          VT    SuperUser       IGX 8420    9.2 Oct. 14 1998 17:37 GMT

                           System-Wide Parameters

1  Max Time Stamped Packet Age (msec) ...............................   32
2  Fail Connections On Communication Break ..........................   No
3  Max Network Delay for 'v' connections (msec)......................   14
4  Max Network Delay for 'c' connections (msec)......................   27
5  Max Network Delay for 't' & 'p' connections (msec)................   14
6  Max Network Delay for 'a' connections (msec)......................   27
7  Max Network Delay for High Speed Data connections (msec)..........   32
8  Max Network Delay for CDP-CDP 'v' connections (msec)..............   32
9  Max Network Delay for CDP-CDP 'c' connections (msec)..............   32
10 Max Network Delay for CDP-CDP 't' & 'p' connections (msec)........   32
11 Max Network Delay for CDP-CDP 'a' connections (msec).............    32



This Command: cnfsysparm


Continue? n
```

System Response

In response to the "Continue" prompt at the bottom of the display, enter an "n," then enter a "1" to enter the maximum allowable age for a time-stamped packet.

```
sw171          VT    SuperUser       IGX 8420    9.2 Oct. 14 1998 17:37 GMT

                           System-Wide Parameters

1  Max Time Stamped Packet Age (msec) ...............................   40
2  Fail Connections On Communication Break ..........................   No
3  Max Network Delay for 'v' connections (msec)......................   14
4  Max Network Delay for 'c' connections (msec)......................   27
5  Max Network Delay for 't' & 'p' connections (msec)................   14
6  Max Network Delay for 'a' connections (msec)......................   27
7  Max Network Delay for High Speed Data connections (msec)..........   32
8  Max Network Delay for CDP-CDP 'v' connections (msec)..............   32
9  Max Network Delay for CDP-CDP 'c' connections (msec)..............   32
10 Max Network Delay for CDP-CDP 't' & 'p' connections (msec)........   32
11 Max Network Delay for CDP-CDP 'a' connections (msec).............    32



This Command: cnfsysparm 1


Enter new value (in Decimal):
```

Enter the number of the parameter you wish to change, along with the value. For example, to change the Maximum Time-Stamped Packet Age (1) from 40 milliseconds to 42 milliseconds, enter:

1 42

Note If you change item 15, the following prompt appears on the screen:

Changing this parameter will reset Frame Relay classes to their defaults. Continue (y/n)?

Changing parameter 15 requires a change in the Frame Relay classes. Since Frame Relay classes are not associated with a specific port (or port speed 0), no translation can be made. The values for Bc and Be, or VC Q depth and PIR are reset to their default values.

Table 13-8 cnfsysparm—Parameters

Parameter	Description
index	Specifies a numerical value that refers to the specific parameter to be changed. Index numbers and descriptions of the system-wide parameters are in the table that precedes the command summary.
value	Specifies a numerical value that applies to the selected parameter. See Table 13-6.

deluser

Deletes a user from the network. A user can delete users at any lower privilege level.

Full Name

Delete a user

Syntax

deluser <user_id>

Related Commands

adduser, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX, BPX	Yes

Example 1

deluser john

Description

Delete user "john."

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 16 1998 13:52 PST

YourID       1
Sarah        5






\








Last Command: deluser John


Next Command:
```

Table 13-9 deluser—Parameters

Parameter	Description
userid	Specifies the name of the user to delete from the network.

dsplanip

The **dsplanip** command is similar to the **dspnwip** command. It displays the LAN IP address and subnet mask of the local node, and also displays the LAN IP address of all other nodes in the network, including feeder nodes. (Feeder nodes are displayed with a blank node name, and they appear immediately beneath the hub node to which they are attached.)

The **dsplanip** command displays the LAN IP address of all nodes reachable from a given node in the network.

The **dsplanip** command is new in Release 9.2 in support of the Out-of-Band network management feature which enables management traffic to be sent over IP to the switches' LAN Ethernet interface, thereby reducing the load on trunk bandwidth and node processor times.

Service-Affecting Alarms and Out of Band Network Management Features in Release 9.2

The service-affecting alarms feature enhances reporting of switch alarm conditions to Cisco WAN Manager, and to a customer network management system (NMS) through the Cisco WAN Manager RTM Proxy. New Robust Alarm messages are generated from existing switch events that could affect service.

The Out-of-Band network management feature in Release 9.2 enables management traffic to be sent over IP to switches' LAN Ethernet interface to Cisco WAN Manager, thereby reducing the load on trunk bandwidth and node processor times. For WAN Manager to be able to manage a switch out-of-band, the following things must be done:

- To support out of band management feature and service-affecting alarms, SV+ must be running Release 9.2 or higher.
- The LAN IP address of the switch must be configured.
- LAN Ethernet access must be provided from the Cisco WAN Manager workstation to the switches' LAN port.
- You may only use the "lanip" option for Cisco WAN Manager, which enables out of band management, if all switch nodes in the network are running switch software Release 9.2 or higher.
- For an MGX 8220 (AXIS) interface shelf to be able to send LAN IP address changes to a routing node, it must be running MGX 8220 release 4.0.20 or higher.

To change the LAN IP address of a routing node you use the **cnflan** user command. The Out-of-Band network management software in Release 9.2 detects a change to the LAN IP address on a routing or feeder note and forwards an update message to Cisco WAN Manager. It also detects

---

Note The service-affecting alarms and out of band network management features in Release 9.2 can interoperate in mixed networks containing one or more nodes running switch software Release 9.1 or 8.5.

Full Name

Display LAN IP address of local node, and all nodes in the network

Syntax

dsplanip

Related Commands

dspphyslns, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

dsplanip

Description

Display the LAN IP address of local node, and all other reachable nodes in network.

System Response

```
sw248      TN      StrataCom       BPX 15 9.2.0     May 4 1998 18:28 GMT

Active LAN IP Address:           172.29.9.155
Active LAN IP Subnet Mask:       255.255.255.0

NodeName      LAN IP Address
sw252         172.29.9.159
              172.29.9.175
sw263         172.29.9.167
              172.29.9.163
sw8           172.29.9.124
sw248         172.29.9.155
              172.29.9.134
              172.29.9.173


Last Command: dsplanip
```

dspnwip

Displays the IP address for each node in the network. The IP address is used to route TFTP messages transferring bulk statistics between the node and the WAN Manager Statistics Master.

Full Name

Display network IP interface

Syntax

dspnwip

Related Commands

cnfwip

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dspnwip

Description

Display network IP addresses.

```
axiom1       TN    bootzilla       IGX 32    9.2       Sep. 5 1998  18:18 GMT

Active Network IP Address:             169.134.90.106
Active Network IP Subnet Mask:         255.255.255.0

NodeName   IP Address
axiom1   169.134.90.111
         169.134.90.105
         169.134.90.101
axiom2   169.134.90.102
axiom3   169.134.90.103
axiom1   169.134.90.106


Last Command: dspnwip


Next Command:
```

dsppwd

Displays the password of the current user or any user at any lower privilege level.

Full Name

Display password

Syntax

dsppwd <user_id>

Related Commands

adduser, **cnfpwd**, **deluser**, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dsppwd yourid

Description

Display the password for user YourID.

System Response

```
alpha          TRM   YourID:1        IGX 8410    9.2    Aug. 16 1998 13:56 PST


The password for YourID is liftoff
```

```
This Command: dsppwd YourID

This screen will self-destruct in ten seconds
Next Command: dsppwd YourID
```

Table 13-10 dsppwd—Parameters

Parameter	Description
userid	Specifies the user whose password is displayed.

dspsnmp

Display the following SNMP parameters for the current node:

- Get Community String
- Set Community String
- Trap Community String
- SNMP Set Request Queue Size
- SNMP Queued Request Timeout, in seconds
- SNMP Trap Event Queue Size

Full Name

Display SNMP parameters

Syntax

`dspsnmp`

Related Commands

cnfsnmp, **dspsnmpstats**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspsnmp`

Description

Display the SNMP parameters for the current node.

System Response

```
sw91           TN    SuperUser       IPX 8     9.2       Aug. 29 1998 13:45 GMT

Get Community String:                  NOACCESS
Set Community String:                  NOACCESS
Trap Community String:                 NOACCESS

SNMP Set Request Queue Size:           110
SNMP Queued Request Timeout (secs):    30
SNMP Trap Event Queue Size:            100






Last Command: dspsnmp


Next Command:
```

dspsnmpstats

Displays the following SNMP statistics for the node:

- SVC Requests Received, the number of SVC requests received.
- SVC Current Queue Length, the number of outstanding SVC requests in the queue.
- SVC Maximum Queue Length, the high watermark of the number of outstanding SVC requests in the queue.
- SVC Requests Timed Out, the number of SVC requests that have timed out.
- Current Trap Managers, the number of managers (up to 10) that are currently registered, their IP addresses and UDP ports.
- Traps Transmitted, the number of traps transmitted.
- TRAP Current Queue Length, the number of outstanding traps in the queue.
- TRAP Maximum Queue Length, the high watermark of the number of outstanding traps in the queue.
- TRAP Queue Events Discarded, the number of traps discarded due to queue overflow.
- Overflow Traps Transmitted, the number of overflow traps transmitted due to queue overflow.

Full Name

Display SNMP parameters

Syntax

dspsnmpstats

Related Commands

cnfsnmp, **dspsnmp**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

```
dspsnmpstats
```

Description

Display SNMP statistics for the current node.

System Response

```
sw91          TN    SuperUser      IPX 8     9.2      Aug. 29 1998 13:21 GMT

SVC Requests Received:       256       Traps Transmitted:            256

SVC Current Queue Length:    0         TRAP Current Queue Length:    0
SVC Maximum Queue Length:    0         TRAP Maximum Queue Length:    0
SVC Requests Timed Out:      0         TRAP Queue Events Discarded:  196864
                                       Overflow Traps Transmitted:   100925440

Current Trap Managers:       0/10      Snmp_Trap_Db Ptr:             30DDCD02




Last Command: dspsnmpstats


Next Command:
```

dspsv3

Displays the Cisco WAN Manager L3 (Layer 3) Link Control Blocks.

The **dspsv3** command displays the LCBs (Link Control Blocks) used by a switch to communicate with one or more SV+ workstations. The display shows whether the out-of-band (lanip) option is being used. Previous to Release 9.2, the **dspsv3** screen indicated whether or not NWIP was being used. In Release 9.2, the dspsv3 screen distinguishes between the three modes supported in Release 9.2:

- nwip_off
- nwip_on
- lanip

This command supports the Out-of-Band network management feature, which enables management traffic to be sent over IP to switches' LAN Ethernet interface, thereby reducing the load on trunk bandwidth and node processor times.

The **dspsv3** command displays counts of pending SONET APS (Automatic Protection Switching) alarms.

Full Name

Display Cisco WAN Manager L3 (Layer 3s) Link Control Blocks

Syntax

dspsv3

or

dspsv3 <LCB number>

Table 13-11 Description of the Fields in the dspsv3 Display

Field	Explanation
Serial Admin	Serial link admin window
LAN Admin	LAN Admin window
LCB	Link Control Block number (0 is the gateway link)
Node	SV+ gateway node number (0 is local IO)
IP	IP address (* indicates nwip is enabled)

Related Commands

dsplanip

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dspsv3

Description

Display Cisco WAN Manager L3 Link Control Blocks.

System Response

```
nsaigx2       TN    StrataCom     IGX 8420    9.2    June 8 1998 06:11 GMT

Number of Active SV3 Links: 2        Serial Admin: None     LAN Admin: None
LCB:  0 Node:   0 IP:*172.16.64.20
LCB:  1 Node:   3 IP:*172.16.64.20



>Last Command: dspsv3
```

Example 2

dspsv3

System Response

```
sw248     TN      StrataCom     BPX 15 9.2.0            May 4 1998 18:05 GMT

Number of Active SV3 Links: 2        Serial Admin: None       LAN Admin: None
LCB:    0 Node: 128 IP:N172.29.9.29
LCB:    1 Node: 128 IP:L172.29.9.53
LCB:    2 Node: 128 IP: 172.29.9.115



Last Command: dspsv3
```

In Example 2, the summary display shows three Link 1 LCBs which connect to three different SV+ workstations. The “N” next to the first IP address indicates the nwip_on option. The “L” next to the second address indicates the lanip option. The absence of a symbol on the third line indicates the nwip_off option.

Example 3

dspsv3

System Response

```
sw248      TN      StrataCom      BPX 15 9.1.a5       May 4 1998 18:11 GMT

LCB: 1 Alloc: 1 sv3_lcb_ptr: 31514034
IP Address: 172.29.9.53 (lanip)
Response Timer: 0
Idle Timer: 393
Retry Count: 120
Current Protocol State: SV3_TRANSFER
No. of Buffers in the data_q: 0
No. of Buffers in the xmit_q: 0
No. of Buffers in the nflow_q: 0
Comm Break Alarm: Update: 0, Pending: 0
Comm Break Alarm Bitmaps: Update: 314741FC, Pending: 3147449C




Last Command: dspsv3 1
```

In Example 3, the detailed display below shows the state on an individual link control block. The display indicates the use of the *lanip* option.

Table 13-12 Description of the Fields in the dspsv3 Display

Field	Explanation
Serial Admin	Serial link admin window
LAN Admin	LAN Admin window
LCB	Link Control Block number (0 is the gateway link)
Node	SV+ gateway node number (0 is local IO)
IP	IP address (* indicates nwip is enabled)

Example 1

dspsv3 0

Description

Display Cisco WAN Manager L3 Link Control Blocks.

Table 13-13 Description of the Fields in the Previous dspsv3 Display

Field	Explanation
LCB	LCB number
Alloc	LCB allocated (1) or no (0)

Table 13-13 Description of the Fields in the Previous dspsv3 Display (Continued)

Field	Explanation
sv3_lcb_ptr	Address of LCB in memory
IP Address	SV+ IP Address
Response Timer	SV+ Link Response Timer
Idle Timer	Display SV+ Link Idle Timer
Retry Count	SV+ Link Retry Count
Current Protocol State	Link state (idle, reset, transfer, poll)
No. of buffers in the data_q	Messages in the data queue
No. of buffers in the xmit_q	Messages in the transmit queue
No. of buffers in the nflow_q	Messages in the non-flow-controlled queue
Subscribed applications	Applications to which SV+ has subscribed
Update object(s)	Robust object types that have updated status
Pending	Robust object types that have been updated to SV+, and are waiting for an acknowledgement from SV+.
Robust database update bitmap addresses	

System Response

```
nsaigx2       TN    StrataCom     IGX 8420    9.2    June 8 1998 06:11 GMT


LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
IP Address: 172.29.9.60
Response Timer: 0
Idle Timer: 600
Retry Count: 120
Current Protocol State: SV3_TRANSFER
No. of Buffers in the data_q: 0
No. of Buffers in the xmit_q: 0
No. of Buffers in the nflow_q: 0

This Command: dspsv3 0

Continue?

LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
Subscribed Applications: Topology MaintLog
                         312024C0

               Update      Pending
Revision:      0           0
Stats Rebuild: 0           0
Subscription:  0           0            APS Alarm:     0 31202EB6  0 31202EDB
Feeder Obj:    0 312029D2  0 312029D4   Feeder Alarm:  0 31202ED8  0 31202EDA
Port Obj:      0 312029C6  0 312029CC   Port Alarm:    0 31202ECC  0 31202ED2
Conn Obj:      0 312024D0  0 31202741   Conn Alarm:    0 312029D6  0 31202C47
Cline Obj:     0 312029B2  0 312029B7   Cline Alarm:   0 31202EB8  0 31202EBD
Trunk Obj:     0 312029BC  0 312029C1   Trunk Alarm:   0 31202EC2  0 31202EC7

Last Command: dspsv3 0

Continue?

LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
Robust Database Updates data:
db_update_flags:     30D6E16C db_pending_flags:    30D6E355
flag_offset_table:   30D6E56C
  1:0    2:0    3:0    4:0    5:0    6:0    7:0    8:1    9:16  10:1A
11:59  12:0   13:D6  14:D7  15:0   16:DC  17:FC  18:0   19:13B 20:0
21:17B 22:17D 23:0   24:0   25:17F 26:0   27:180 28:0   29:181 30:183
31:0   32:0   33:0   34:185 35:0   36:0   37:186 38:0   39:0   40:0
41:0   42:0   43:0   44:0   45:0   46:187 47:0   48:0   49:0   50:0
51:18C 52:0   53:0   54:0   55:0   56:0   57:0   58:0   59:0   60:0
61:0   62:0   63:0   64:0   65:0   66:18D 67:0   68:0   69:0   70:0
71:0   72:0   73:18E 74:0   75:0   76:0   77:0   78:0   79:0   80:0
81:0   82:0   83:0   84:0   85:0   86:0   87:0   88:0   89:0   90:0
91:0   92:18F 93:18F 94:190 95:1A5 96:1A9 97:0   98:0   99:1E8 100:0
101:0   102:0   103:0   104:0



Last Command: dspsv3 0

LCB                          - LCB number
Alloc                        - LCB allocated (1) or not (0)
sv3_lcb_ptr                  - address of LCB in memory
IP Address                   - SV+ IP Address
Response Timer               - SV+ Link Response Timer
Idle Timer                   - Display SV+ Link Idle Timer
Retry Count                  - SV+ Link Retry Count
```

```
Current Protocol State       - Link state (idle, reset, transfer, poll)
No. of Buffers in the data_q - Messages in the data queue
No. of Buffers in the xmit_q - Messages in the transmit queue
No. of Buffers in the nflow_q- Messages in the non-flow-controlled queue

Subscribed Applications      - Applications to which SV+ has subscribed

Update                       - Robust object types that have updated object(s)
                               status.
Pending                      - Robust object types that have been updated to
                               SV+, and are waiting for an acknowledge from
                               SV+.

Robust database update bitmap addresses.
```

dsptsmap

Displays the following SNMP statistics for the node:

- SVC Requests Received, the number of SVC requests received.
- SVC Current Queue Length, the number of outstanding SVC requests in the queue.
- SVC Maximum Queue Length, the high watermark of the number of outstanding SVC requests in the queue.
- SVC Requests Timed Out, the number of SVC requests that have timed out.
- Current Trap Managers, the number of managers (up to 10) that are currently registered, their IP addresses and UDP ports.
- Traps Transmitted, the number of traps transmitted.
- TRAP Current Queue Length, the number of outstanding traps in the queue.
- TRAP Maximum Queue Length, the high watermark of the number of outstanding traps in the queue.
- TRAP Queue Events Discarded, the number of traps discarded due to queue overflow.
- Overflow Traps Transmitted, the number of overflow traps transmitted due to queue overflow.

Full Name

Display SNMP parameters

Syntax

dspsnmpstats

Related Commands

cnfsnmp, **dspsnmp**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspsnmpstats`

Description

Display SNMP statistics for the current node.

System Response

```
sw91           TN    SuperUser      IPX 8     9.2      Aug. 29 1998 13:21 GMT

SVC Requests Received:       256       Traps Transmitted:            256

SVC Current Queue Length:    0         TRAP Current Queue Length:    0
SVC Maximum Queue Length:    0         TRAP Maximum Queue Length:    0
SVC Requests Timed Out:      0         TRAP Queue Events Discarded:  196864
                                       Overflow Traps Transmitted:   100925440

Current Trap Managers:       0/10      Snmp_Trap_Db Ptr:             30DDCD02





Last Command: dspsnmpstats


Next Command:
```

dspusers

Displays users. The privilege levels in the display are restricted to those of the current user and any privileges below the current user.

Full Name

Display users

Syntax

dspusers

Related Commands

adduser, **deluser**, **dspusers**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspusers`

Description

Display the users on a network.

dspusertask

Displays information about the current user-task. The displayed information varies with the user task. For example, information about a vt session slightly differs from a telnet session. The command takes a user task number as an argument. If the user task number is unknown, enter the command without a number to see a list of possible user tasks and the current user task. The types of user tasks are as follows:

- User, which can be the control terminal user, auxiliary port user, or StrataView
- A telnet session
- A virtual terminal session (vt)
- An SNMP agent
- A job

Full Name

Display user task

Syntax

`dspusertask` [user task number]

Related Commands

adduser, **cnfpwd**, **deluser**, **dspusers**, **dsppwd**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspusertask`

Description

Display user task information—without specifying a task in this case. This example shows a case in which the user has started a vt session on a node. See also step 2 of this example.

System Response

```
sw78           VT    SuperUser       BPX 15    9.2      Jan. 31 1998 15:52 PST

 #  TASK PURPOSE      USER ID            #  TASK PURPOSE      USER ID
 -- ---- ------------ -------            -- ---- ------------ -------
 1  USR1 control port none               13 VT-5 VT           none
 2  USR2 auxilry port none               14 VT-6 VT           none
 3  USR3 lan port(SV) none               15 SNMP agent        n/a
 4  TN-1 lan (telnet) none               16 JOBS runs jobs    n/a
 5  TN-2 lan (telnet) none
 6  TN-3 lan (telnet) none
 7  TN-4 lan (telnet) none
 8  TN-5 lan (telnet) none
 9  VT-1 VT: sw81     SuperUser   < You
 10 VT-2 VT           none
 11 VT-3 VT           none
 12 VT-4 VT           none


This Command: dspusertask


Please Enter User Number:9
```

Example 1

9

Description

This example shows the screen after the you enter a 9 at the prompt in the *previous* screen, a case in which you already started a vt session on a node. Note that the display shows the status as a vt slave, and the node on which the vt session originated is sw81.

```
sw78           VT    SuperUser       BPX 15    9.2      Jan. 31 1998 15:53 PST


    Task: VT-1
    Logged in as: SuperUser
    VT master:  no
    VT slave:   yes    Master node is: sw81
    VT pending: no

    Public  lock: no
    Private lock: none

    No command is currently running.
    Previous command: dspusertask 9


Last Command: dspusertask 9


Next Command:
```

Table 13-14 dspusertask—Parameters

Parameter	Description
user task number	Specifies the number of the user task whose information is displayed.

dspusertasks

Displays general information about all current user-tasks. The types of user tasks are as follows:

- User, which can be the control terminal user, auxiliary port user, or Cisco WAN Manager
- A telnet session
- A virtual terminal session (vt)
- An SNMP agent
- A job

Full Name

Display user tasks

Syntax

`dspusertasks`

Related Commands

adduser, **cnfpwd**, **deluser**, **dspusers**, **dsppwd**, **dspusertask**

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspusertasks`

Description

Display user task information.

System Response

```
sw151          TN    SuperUser       IGX 8420    9.2       Aug. 14 1998 18:02 GMT

 #  TASK  PURPOSE     USER ID            #  TASK  PURPOSE     USER ID
 -- ---- ------------ -------            -- ---- ------------ -------
 1  USR1 control port SuperUser          13 VT-5 VT           none
 2  USR2 auxilry port none               14 VT-6 VT           none
 3  USR3 lan port(SV) none               15 SNMP agent        n/a
 4  TN-1 lan (telnet) none               16 JOBS runs jobs    n/a
 5  TN-2 lan (telnet) SuperUser   < You
 6  TN-3 lan (telnet) none
 7  TN-4 lan (telnet) none
 8  TN-5 lan (telnet) none
 9  VT-1 VT           none
 10 VT-2 VT           none
 11 VT-3 VT           none
 12 VT-4 VT           none


Last Command: dspusertasks


Next Command:
```

Troubleshooting Commands

Table 14-1 lists the troubleshooting commands.

Table 14-1 Troubleshooting Command List

Command	Full Name	Page
addalmslot	Add alarm slot	14-3
addextlp	Add external loopback	14-5
addloclp	Add local loopback	14-11
addlocrmtlp	Add local-remote loopback	14-16
addrmtlp	Add remote loopback	14-18
clrchstats	Clear channel statistics	14-23
clrclkalm	Clear clock alarm	14-25
clrclnalm	Clear circuit line alarm	14-30
clrclnerrs	Clear circuit line errors	14-30
clreventq	Clear the events queues	14-26
clrlnalm	Clear line alarm	14-30
clrlnerrs	Clear line errors	14-30
clrlog	Clear log	14-31
clrmsgalm	Clear message alarm	14-33
clrphyslnalm	Clear physical line alarms	14-34
clrphyslnerrs	Clear physical line errors	14-38
clrportstats	Clear port statistics	14-40
clrslotalms	Clear slot alarms	14-42
clrsloterrs	Clear slot errors	14-43
clrtrkalm	Clear trunk alarm	14-44
clrtrkerrs	Clear trunk errors	14-47
clrtrkstats	Clear trunk statistics	14-49
cnfbus	Configure bus	14-50
cnfleadmon	Monitor IGX LDM/HDM data port control leads.	14-52
cnflnalm	Configure line alarm	14-57
cnfoamlpbk	Configure OAM loopback test	14-61

Table 14-1 Troubleshooting Command List (Continued)

Command	Full Name	Page
cnfslotalm	Configure slot alarm	14-61
cnftrkalm	Configure trunk alarm	14-67
dellp	Delete loopback	14-69
dncd	Down card	14-71
dspalms	Display alarms	14-72
dspbob	Display Breakout Box	14-78
dspbusbw	Display cell bus allocated bandwidth	14-81
dspbuses	Display Buses	14-84
dspclnerrs	Display circuit line errors	14-86
dspeventq	Display the event queue names and the data in each.	14-26
dspfrcbob	Display FRC-2/FRM-2 breakout box	14-90
dsplog	Display event log	14-92
dsplnalmcnf	Display line alarm configuration	14-102
dsplnerrs	Display line errors	14-105
dspoamlpbk	Display OAM loopback test	14-107
dsppwr	Display power	14-117
dspslotalms	Display slot alarms	14-122
dspsloterrs	Display slot errors	14-124
dspslotstatcnf	Display slot statistics configuration	14-127
dspsv3	Display Cisco WAN Manager L3 (layer 3) Link Control Blocks	14-129
dsptrafficgen	Display whether Traffic Generation feature for card slot is enabled	14-129
dsptrkerrs	Display individual or all trunk errors	14-135
prtclnerrs	Print circuit line errors	14-139
prtlnerrs	Print line errors	14-141
prtlog	Print log	14-140
prttrkerrs	Print trunk errors	14-143
resetcd	Reset card	14-144
resetpc	Reset Port Concentrator	14-146
switchcc	Switch controller card	14-147
tstcon	Test connection	14-149
tstconseg	Test connection segment	14-153
tstdelay	Test delay	14-156
tstpcs	Test Port Concentrator Shelf	14-159
tstport	Test port	14-160
tstubus	Test cell bus	14-160

addalmslot

Enables the MAJOR and MINOR alarm indicators on an Alarm Relay Card (ARC) or Alarm Relay Module (ARM). It also configures the slot to support external alarms from the Alarm Relay Interface (ARI) back card. You can use this command at any node that can provide external alarm indications to an alarm reporting system. The ARC or ARM can reside in any front slot but usually resides in the right-most slot.

Full Name

Add alarm slot

Syntax

addalmslot <slot number>

Related Commands

delalmslot, dspalms

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	IGX	Yes

Example 1

```
addalmslot 16
```

Description

Enable alarm reporting from slot 16 in a node.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2      Aug. 3 1998 14:27 MST

Alarm summary   (Configured alarm slots: 16)
Connections Failed:       None
Groups Failed:            None
PLN Alarms:               1 Major
CLN Alarms:               None
Cards Failed:             1
Missing Cards:            None
Remote Node Alarms:       1 Major








Last Command: addalmslot 16


Next Command:
```

addextlp

Places an external device in loopback mode. The **addextlp** command applies to existing connections on an SDP, HDM, LDP, or LDM. A “near” loopback causes the NEAR EIA template to be applied. A ‘far’ loopback causes the FAR EIA template to be applied to the data port. The loopback remains in place until removed by the **dellp** command.

The **dspcons** command shows which connections are in loopback mode. Specifying an “n” after the channel indicates a near loopback, and an “f” indicates a far loopback. Because **addextlp** takes the specified connections out of service, use it only when a service disruption is tolerable.

Full Name

Add External Loop to Connection

Syntax

addextlp <channel> < n | f >

Related Commands

dellp, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
addextlp 5.1 n
```

Description

Place the device connected to channel 5.1 in near loopback.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 12:53 PST

 Local      Remote      Remote                                       Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 N5.1       beta        25.1       Ok     256                  7/8          0  L
 9.1.100    gamma       8.1.200    Ok     fr                                0  L
 9.2.400    beta        19.2.302   Ok     fr                                0  L
 14.1       gamma       15.1       Ok     v                                 0  L







Last Command: addextlp 5.1 n


Next Command:
```

Table 14-2 addextlp—Parameters

Parameter	Description
channel	Specifies the channel to loopback in the format *slot.port*.
n /f	Specifies whether the loopback is near or far. An “n” specifies near; an “f” specifies far. For a non-DDS port, the near or far modem is placed in loopback, if it supports this function. For a DDS port, the external DDS device is placed in CSU loopback. Local channels must be configured as OCU in order to place them in external loopback.

addlnloclp

Establishes a local-remote loopback on a trunk or port card in a BPX. Applicable cards are the ASI, BNI, BME, and BXM.

While a line loop is present, software suspends the card self-test and the line diagnostic test that normally run when a line goes into alarm. Suspending these tests prevents background test loops from interfering with the user-specified loop.

Line loops are set for a line on the local node, so you cannot specify a remote node, and no network messaging is supported for setting a line loop of any type on a remote node.

Line loop status is displayed on the **dsplns** screen for an ASI, BME, or a BXM in port mode and the **dsptrks** screen for a BNI, BME, or a BXM in trunk mode. Line loop status is not displayed for connections (**dspcons**) affected by a line loop. Instead, a warning is printed if the line has connection traffic travelling on it, and an event is logged when a line loop is set or cleared. A line loop on a trunk generates Comm Fail, causing connections to fail and be rerouted.

For both of the **dsplns** and **dsptrks** screens, the "]" character appears before the back card type in the "Type" column to indicate that the line local loopback is active.

The line loop state is not saved in BRAM or on a rebuild but is preserved on a switchover. After a rebuild, a line's loop state is cleared.

Exercise caution when you set up loops on a BNI, BME, or BXM trunk because looping an added BNI/BXM/BME trunk causes Comm Failure and connection rerouting. BNI/BXM/BME **addlnlocrmtlp** is not supported because of a lack of useful purpose, and Cisco recommends that you use **addlnloclp** only when the trunk is upped but not added. On the other hand, the system does not prevent you from looping an added BNI/BXM/BME trunk port.

Full Name

Add local loopback to line

Syntax

addlnloclp <slot.port>

Related Commands

dellnlp, dsptrks, dsplns, addlnlocrmtlp

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	BPX	Yes

Example 1

```
addlnloclp 9.1
```

Description

The **dsplns** display appears with the connection highlighted and a prompt for confirmation.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    8.4 Feb. 28 1998 01:25 GMT

Line    Type   Current Line Alarm Status
 3.1    OC-3    Clear - OK
 3.2    OC-3    Clear - OK
 3.3    OC-3    Clear - OK
 3.4    OC-3    Clear - OK
 3.5    OC-3    Clear - OK
 3.8    OC-3    Clear - OK
 5.1    T3     Clear - OK
 5.2    T3     Clear - OK
 9.1   [OC-3    Clear - OK




Last Command: addlnloclp 9.1

Warning - Looping will interrupt data flow on the line
Next Command:
```

Table 14-3 addlnloclp—Parameters

Parameter	Description
slot.port	Specifies the port.

addlnlocrmtlp

Establishes a local-remote loopback on a trunk or port card in a BPX. Applicable cards are the ASI, BNI, and BXM/BME.

While a line loop is present, software suspends the card self-test and the line diagnostic test that normally run when a line goes into alarm. Suspending these tests prevents background test loops from interfering with the user-specified loop.

Line loops are set for a line on the local node, so you cannot specify a remote node, and no network messaging is supported for setting a line loop of any type on a remote node.

Line loop status is displayed on the **dsplns** screen for an ASI or a BXM/BME in port mode and the **dsptrks** screen for a BNI or a BXM/BME in trunk mode. Line loop status is not displayed for connections (**dspcons**) affected by a line loop. Instead, a warning is printed if the line has connection traffic travelling on it, and an event is logged when a line loop is set or cleared. A line loop on a trunk generates Comm Fail, causing connections to fail and be rerouted.

For both of the **dsplns** and **dsptrks** screens, the "[" character appears before the back card type in the "Type" column to indicate that the line local-remote loopback is active.

The line loop state is not saved in BRAM or on a rebuild but is preserved on a switchover. After a rebuild, a line's loop state is cleared.

Exercise caution when you set up loops on a BNI or BXM/BME trunk because looping an added BNI/BXM/BME trunk causes Comm Failure and connection rerouting. BNI/BXM/BME **addlnlocrmtlp** is not supported because of a lack of useful purpose, and Cisco recommends that you use **addlnloclp** only when the trunk is upped but not added. On the other hand, the system does not prevent you from looping an added BNI/BXM/BME trunk port.

In this release, you can use the **addloclp** and **addlocrmtlp** commands to enable a two-segment connection at the hub node port endpoint in a network of IGX hubs and MGX 8800 interface shelves. The **addloclp** and **addlocrmtlp** commands are blocked at the interface shelf trunk endpoint. The **addrmtlp** command is not supported at either endpoint of the connection. You can use the **dellp** command to remove the local (or local remote) loopbacks that have been added; however, you cannot use the **dellp** command at the trunk endpoint of the connection—it will be blocked. Loops of any kind are not supported for the middle segment of a three-segment connection.

Full Name

Add local-remote loopback to line

Syntax

addlnlocrmtlp <slot.port>

Related Commands

dsptrks, dsplns, dellnlp, addlnloclp

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	BPX	Yes

Example 1

`addlnlocrmtlp 10.1`

Description

The **dsptrks** screen appears with the loopback highlighted by the “[“ character.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    8.4 Feb. 28 1998 01:27 GMT

TRK     Type   Current Line Alarm Status               Other End
 1.1    T3     Clear - OK                              pubsaxi1(AXIS)
 1.3    T3     Clear - OK                              pubsipx1/8
 4.1    OC-3    Clear - OK                              -
10.1   [OC-3    Clear - OK                              -









Last Command: addlnlocrmtlp 10.1


Next Command:
```

Table 14-4 addlnlocrmtlp—Parameters

Parameter	Description
slot.port	The port on the local node.

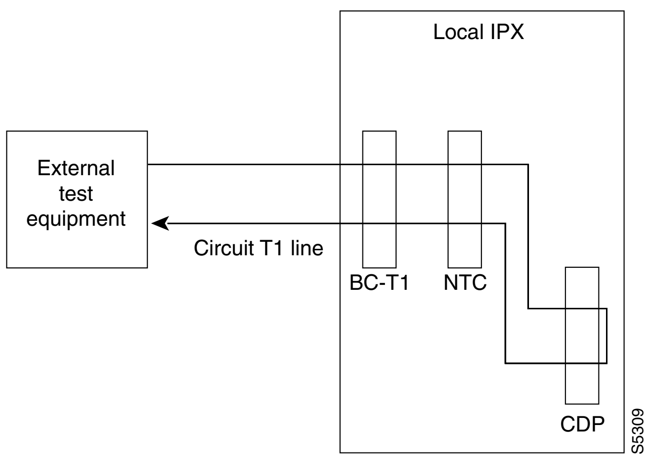
addloclp

The **addloclp** command places the following types of channels in local loopback mode:

- Voice
- Data
- Frame Relay port
- Frame Relay connection
- ATM connection
- Access device port

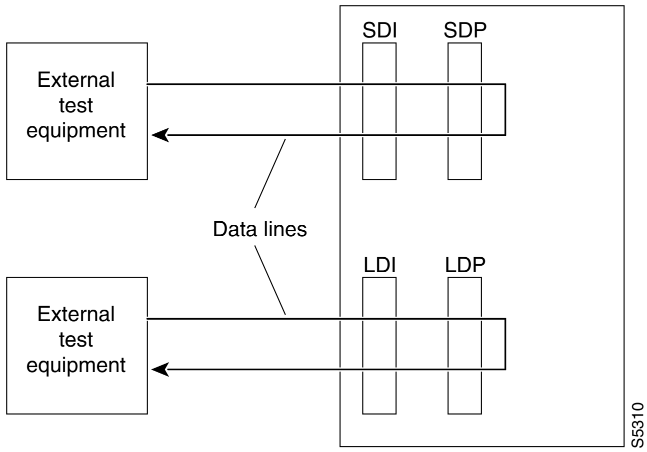
For voice connections, **addloclp** creates a signal path from a channel or group of channels on an incoming line then back out to the line. External test equipment can test the integrity of the path at the T1 DS0 level. Figure 14-1 shows a local loopback on a voice channel.

Figure 14-1 Local Loopback on a Voice Channel



For data connections, **addloclp** creates a signal path from the incoming data port or set of ports back to these same port(s) through the local CDP/CVM, SDP/HDM, or LDP/LDM. External test equipment can then test the integrity of the path. Figure 14-2 illustrates a local loopback on a data connection.

Figure 14-2 Local Loopback on a Data Connection



A local loopback can simultaneously exist at both ends of a connection. However, a local loopback and a remote loopback cannot co-exist on a connection. (See the **addrmtlp** description for more information.)

Before executing a loopback, the IGX node performs signal and code conditioning to remove the connection from service. The loopback remains in place until removed by the **dellp** command. Only existing connections can be looped back. Use the **dspcons** command to see which connections are looped back. A flashing right parenthesis ")" or left parenthesis "(" is used in the connections display to indicate a loopback. The direction and location of the parenthesis depends on whether the loopback is local or remote and which end of the connection was used to establish the loopback. A local loopback initiated from the local end of the connection looks like this in the connections display:

Local Channel	Remote Node	Remote Channel
12.1	alpha	15.1

A local loopback initiated from the remote end of the connection looks like this:

Local Channel	Remote Node	Remote Channel
12.1	alpha	15.1

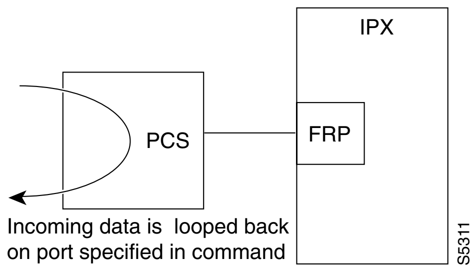
In Frame Relay connection loopback mode (DLCI included in command), all packets from the far-end of the connection are dropped. The far-end system software is informed of the loopback. In port loopback mode (port specified without a DLCI), all packets for this port are dropped and each opposite end is informed of the loopback mode. Use the format *slot.port* in port mode to loop just the port. The data is looped directly in the FRI back card, so no data reaches the MUXBUS or CELLBUS. Use the format *slot.port.DLCI* in connection (channel) mode to loop a specific channel. Note that this can affect up to 252 connections (channels) in port loopback mode.

Because the **addloclp** command causes the connection(s) to be removed from service, you should use loopbacks only when a service disruption can be tolerated. You establish remote loopbacks with the **addrmtlp** command. You remove local and remote loopbacks with the **dellp** command. You can also initiate loopbacks for data channels by pressing a button on the front of the associated data card.

Frame Relay Local Loops with Port Concentrator

When a Frame Relay port or connection is located on a Port Concentrator instead of directly on an FRP or FRM card, the data test path is different. When just the <*port*> parameter is used, incoming data is looped back out on the Port Concentrator port:

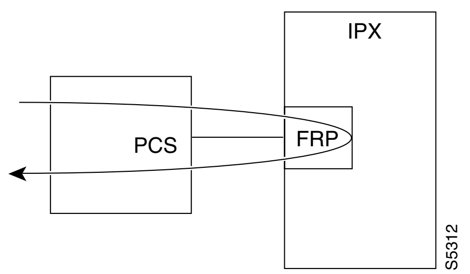
Figure 14-3 Local Loop on Port Concentrator



This loop disrupts all Frame Relay connections on the port that is under test.

When you specify a connection with <*port.dlci*> parameters, the connection is looped back at the FRM-2 or FRP-2 interface with the IGX card bus:

Figure 14-4 Local Loop on FRM-2 or FRP-2



As shown, this test verifies the operation of all components from the Port Concentrator to the IGX interface with the FRP-2 or FRM-2 card.

This tests interrupts *only* the specified connection on the Port Concentrator port.

In this release, the **addloclp** and **addlocrmtlp** commands support the two-segment connection at the hub node port endpoint in a network of IGX hubs and SES interface shelves. The **addloclp** and **addlocrmtlp** commands are blocked at the interface shelf trunk endpoint. The **addrmtlp** command is not supported at either endpoint of the connection. You can use the **dellp** command to remove the local (or local remote) loopbacks that have been added; however, you cannot use the **dellp** command at the trunk endpoint of the connection—it will be blocked. Loops of any kind are not supported for the middle segment of a three-segment connection.

Full Name

Add local loopback to connections on a port

Syntax

addloclp ***channel***

Related Commands

addrmtlp, dellp, dspcons, dspfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

addloclp 14.1

Description

The connections screen appears with connection 14.1 highlighted. The system prompts you to confirm the loopback. To confirm it, enter y.

System Response

```
Next Command:
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:03 PST

 Local      Remote      Remote                                      Route
 Channel    NodeName    Channel    State  Type    Compression   Code Avoid COS O
 5.1        beta       )25.1       Ok     256                   7/8          0  L
 9.1.100    gamma       8.1.200    Ok     fr                                 0  L
 9.1.200    gamma       8.1.300    Ok     fr                                 0  L
 9.2.400    beta        19.2.302   Ok     fr(Grp)                            0  L
 14.1      )gamma       15.1       Ok     v                                  0  L









Last Command: addloclp 14.1


Next Command:
```

Table 14-5 addloclp—Parameters (voice)

Parameter	Description
slot	Specifies the slot number of the card containing the port to loop at the local node.
channel (s)	Specifies the channel or set of channels to loop at the local node.
port	Where applicable for the connection type, specifies the port.

Table 14-6 addloclp—Parameters (data)

Parameter	Description
slot	Specifies the slot number of the card containing the port to loop at the local node.
port	Specifies the local port to loop at the local node.

Table 14-7 addloclp—Parameters (Frame Relay)

Parameter	Description
slot	Specifies the slot number of the FRP card containing the port to be looped at the local node.
port	Specifies the local port to loop at the local node.

Table 14-8 addloclp—Parameters (Frame Relay connection)

Parameter	Description
slot	Specifies the slot number of the FRP card containing the port to loop at the local node.
port	Specifies the local port to loop at the local node.
DLCI	Specifies the Data Link Connection Identifier (DLCI) number of the channel to loop at the local node.

Table 14-9 addloclp—Parameters (ATM connection)

Parameter	Description
slot	Specifies the slot number of the ATM card containing the port to loop at the local node.
port	Specifies the local port to loop at the local node.
vpi.vci	The vpi range is 0–7, and the vci range is 1–255. An asterisk (*) indicates a virtual path.

Table 14-10 addloclp—Parameters (FTM connection with an Access Device attached)

Parameter	Description
slot	Specifies the slot number of the ATM card containing the port to loop at the local node.
port	Specifies the local port to loop at the local node.
Access Device ID	The Access Device ID range is 1–255. Omit to loopback all access devices on the local port.
Connection ID	The Connection ID range is 1–252. Omit to loopback all connections on the local port.

addlocrmtlp

Adds support of a local-remote loopback for testing multi-segment connections in a tiered network. The effect is to instruct the remote node to set up a remote loopback. You must execute the **addlocrmtlp** command before using **tstcon** and **tstdelay** for multisegment connections. For interface shelves, you can execute **addlocrmtlp** on either the interface shelf (after telnetting to it). After testing is complete, remove the local-remote loop by executing **dellp**. A parenthesis on the screen shows the loop's endpoint.

In this release, the **addloclp** and **addlocrmtlp** commands support a two-segment connection at the hub node port endpoint in a network of IGX hubs and SES interface shelves. The **addloclp** and **addlocrmtlp** commands are blocked at the interface shelf trunk endpoint. The **addrmtlp** command is not supported at either endpoint of the connection. You can use the **dellp** command to remove the local (or local remote) loopbacks that have been added; however, you cannot use the **dellp** command at the trunk endpoint of the connection—it will be blocked. Loops of any kind are not supported for the middle segment of a three-segment connection.

Full Name

Add local-remote loopback in a tiered network

Syntax

addlocrmtlp <channel(s)>

Related Commands

tstcon, tstdelay, dellp, dspcons, dspfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

```
addlocrmtlp 5.1.3.100
```

Description

The connections screen appears with the connection highlighted and prompts you to confirm.

System Response

```
pubsbpx1       TN    SuperUser       BPX       9.2    July 13 1998 14:41 PDT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type       Compress  Code COS
 5.1.3.100 (       pubsbpx3    7.1.2.49         Ok   aftr                       0










This Command: addlocrmtlp 5.1.3.100


Loopback these connections (y/n)?
```

Table 14-11 addlocrmtlp—Parameters

Parameter	Description
channels(s)	The connection endpoint on the local node.

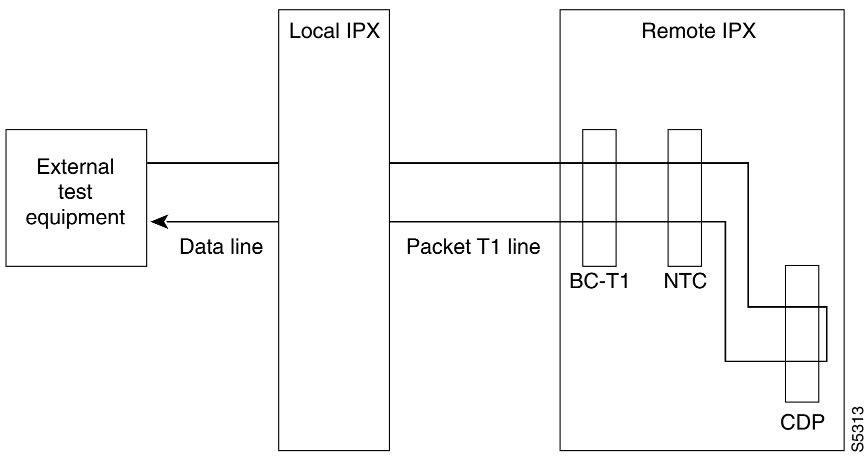
addrmtlp

The **addrmtlp** command places the following types of channels in remote loopback mode:

- Voice
- Data
- Frame Relay port
- Frame Relay connection
- ATM connection

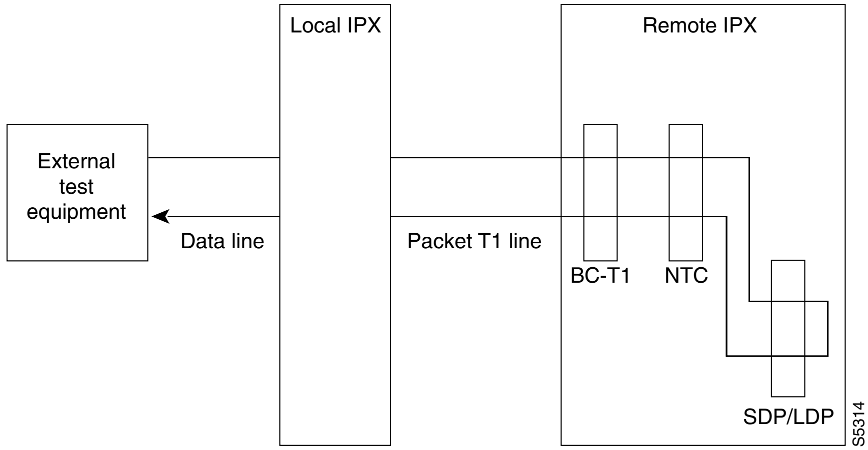
For voice connections, **addrmtlp** loops the information stream from the designated channel or group of channels on an incoming circuit line across the network and loops it back to the circuit line by way of the remote CDP or CVM. External test equipment can then test the integrity of the path at the T1 DS0 level. The following illustrates a remote loopback on a voice channel.

Figure 14-5 Remote Loopback on a Voice Channel



For data connections, **addrmtlp** transfers the information stream from the designated channels through the network and loops it back to the data port(s) through a remote SDP, HDM, LDM, or LDP. External test equipment can then test the integrity of the path. The following illustrates a data connection remote loopback.

Figure 14-6 Remote Loopback on a Data Connection



Prior to executing the loopback, the IPX or IGX node applies signalling template bit patterns to the A, B, C, and D signalling bits at the remote end to remove the connection from service. The loopback remains in place until removed by the **dellp** command. Only existing connections (those that have been entered with the **add-on** command) can be looped back. You cannot establish a remote loopback on a connection that is already looped back, either locally or remotely. (See the **addloclp** command for more information on local loopbacks.)

Use the **dspcons** command to see which connections are looped back. A flashing left parenthesis "(" or right parenthesis ")" is used in the connections display to indicate a loopback. The direction and location of the parenthesis depends on whether the loopback is local or remote and which end of the connection was used to establish the loopback. A remote loopback initiated from the local end of the connection looks like this:

Local Channel	Remote Channel	Remote Node
3.2	alpha	12.1

A remote loopback initiated from the remote end of the connection looks like this:

Local Channel	Remote Node	Remote Channel
3.2	alpha	12.1

For remote loopback of Frame Relay connections, note that in remote loopback mode, if the transmit minimum bandwidth exceeds the receive minimum bandwidth, then loopback data may be dropped. For this reason, the connection speeds will be checked and the user will receive the following message if there is a problem:

"Warning—Receiver's BW < Originator's BW-Data may be dropped."

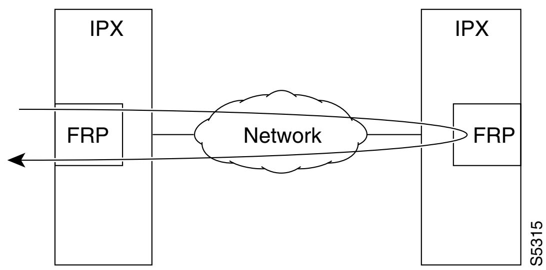
Because the **addrmtlp** command causes the connection to be removed from service, loopbacks should be used only when a service disruption can be tolerated. Local loopbacks are established with the **addloclp** command. Both local and remote loopbacks are removed by the **dellp** command. Loopbacks for data channels can also be initiated by pressing a push-button on the front of the associated data card.

Remote Loopbacks and the Port Concentrator Shelf

For Frame Relay remote loops, DLCI MUST be specified; entering only port number only generates an error message.

Unlike local loopbacks, remote loopbacks are not supported for Frame Relay *ports*; connections must be specified. Data incoming on the Frame Relay port is looped at the remote end FRM-2 or FRP-2 card.

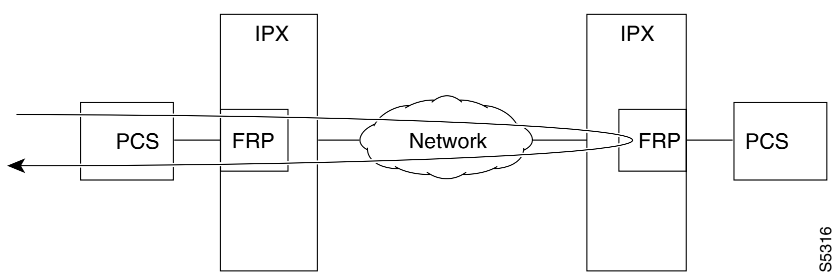
Figure 14-7 Frame Relay Remote Loops



As shown, this test verifies the operation of IPX/IGX network components up to the interface with the remote-end FRM-2 or FRP-2. This test interrupts data traffic for *only* the connection specified by DLCI.

If a port concentrator is attached to the FRM-2 or FRP-2, the only difference in the loop is that the port specified to loop data is on the Port Concentrator:

Figure 14-8 Frame Relay Remote Loops with Port Concentrator



The **addloclp** and **addlocrmtlp** commands support the two-segment connection at the hub node port endpoint in a network of IGX hubs and SES interface shelves. The **addloclp** and **addlocrmtlp** commands are blocked at the interface shelf trunk endpoint. The **addrmtlp** command is not supported at either endpoint of the connection. You can use the **dellp** command to remove the local (or local remote) loopbacks that have been added; however, you cannot use the **dellp** command at the trunk endpoint of the connection—it will be blocked. Loops of any kind are not supported for the middle segment of a three-segment connection.

Full Name

Add remote loopback to connections

Syntax

addrmtlp (see parameter tables)

Related Commands

addloclp, dellp, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

`addrmtlp 5.1`

Description

The connections screen appears with connection 5.1 highlighted. The system prompts to confirm the loopback. To confirm it, enter y. A flashing parenthesis “)” appears in the “Remote Channel” column of the connection to indicate that the connection is looped back.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 12:57 PST

 Local      Remote      Remote                                      Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 5.1        beta       )25.1       Ok     256                  7/8          0  L
 9.1.100    gamma       8.1.200    Ok     fr                                0  L
 9.2.400    beta        19.2.302   Ok     fr                                0  L
 14.1       gamma       15.1       Ok     v                                 0  L








Last Command: addrmtlp 5.1


Next Command:
```

Table 14-12 addrmtlp—Parameters (voice)

Parameter	Description
slot	Specifies the slot number of the card containing the port to loop at the local node.
channel (s)	Specifies the channel or set of channels to loop at the local node.

Table 14-12 addrmtlp—Parameters (voice) (Continued)

Parameter	Description
port	Where applicable for the connection type, specifies the port.

Table 14-13 addrmtlp—Parameters (data)

Parameter	Description
slot	Specifies the slot number of the card containing the port to loop at the local node.
port	Specifies the local port to loop at the local node.

Table 14-14 addrmtlp—Parameters (Frame Relay connections)

Parameter	Description
slot	Specifies the slot number of the FRP card containing the port to loop at the local node
port	Specifies the local port to loop at the local node.
DLCI	Specifies the Data Link Connection Identifier (DLCI) number of the channel to loop at the local node.

Table 14-15 addrmtlp—Parameters (ATM)

Parameter	Description
slot	Specifies the slot number of the card containing the port to loop at the local node.
channel (s)	Specifies the channel or set of channels to loop at the local node.
port	Where applicable for the connection type, specifies the port.
vpi.vci	Specifies vpi/vci.

Table 14-16 addloclp–Parameters (FTM connection with an Access Device attached)

Parameter	Description
slot	Specifies the slot number of the FTM card containing the port to loop at the local node
port	Specifies the local port to loop at the local node.
Access Device ID	The Access Device ID range is 1–255.
Connection ID	The Connection ID range is 1–252..

clrchstats

Clears the channel utilization statistics for either all Frame Relay channels or a specified Frame Relay channel. Statistics generated within the last one minute are not cleared.

Full Name

Clear channel statistics

Syntax

clrchstats <channel | *>

Related Commands

dspchstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	Yes

Example 1

```
clrchstats  9.2.400
```

Description

Clear the statistics of channel 9.2.400.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:24 PST

Channel Statistics for 9.2.400    Cleared: Aug. 16 1998 13:23
MIR: 9.6 kbps          Collection Time: 0 day(s) 00:02:42      Corrupted: NO
                     Frames   Avg Size Avg    Util          Packets     Avg
                              (bytes)  (fps)  (%)                       (pps)
From Port:                0          0      0    0
To Network:               0          0      0    0                0         0
Discarded:                0          0      0    0
From Network:             0          0      0    0                0         0
To Port:                  0          0      0    0
Discarded:                0          0      0    0                0         0

                   ECN Stats:  Avg Rx VC Q:             0    ForeSight RTD    --
Min-Pk bytes rcvd:          0  FECN Frames:             0    FECN Ratio (%)    0
Minutes Congested:          0  BECN Frames:             0    BECN Ratio (%)    0


This Command: clrchstats 9.2.400


OK to clear (y/n)?
```

Table 14-17 clrchstats—Parameters

Parameter	Description
channel	Specifies the Frame Relay channel in the format *slot.port.DLCI*. A "*" specifies all channels.

clrclkalm

Clears the alarm condition attached to a clock source, either circuit line or trunk. The clock test runs continuously in a node, comparing the frequency of the node's clock source to a reference on the NPC/BCC/CC/control card. If a clock source is found to be outside preset frequency limits, it is declared defective and another clock source is selected. In order for the node to return to the original clock source, the alarm must be cleared using the **clrclkalm** command. The alarm may be either a “Bad Clock Source” or “Bad Clock Path” alarm.

Full Name

Clear clock alarm

Syntax

clrclkalm <line type> <line number>

Related Commands

cnfclksrc, dspclksrcs, dspclns, dspcurclk, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX	Yes

Example 1

```
clrclkalm c 12
```

Description

Clear a clock alarm on circuit line 12

Example 2

```
clrclkalm p 12
```

Description

Clear a clock alarm on packet line 12

Table 14-18 clrclkalm—Parameters

Parameter	Description
c/p	Specifies the type of line. A "c" is entered for a circuit line, and a "p" is entered for a trunk.
line number	Specifies the number of the circuit or trunk.

clreventq

Clears high water marks for fail handler event queues.

Full Name

Clear event queues from the fail handler

Syntax

clreventq

Related Commands

dspeventq

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	Yes	IGX, BPX	Yes

Example 1

`clreventq`

Description

Clear the fail handler event queue.

System Response

```
sw151          TN     SuperUser       IGX 16    9.2       Sep. 12 1998 19:18 GMT

  QUEUE                  LENGTH          THROTTLING
NUM NAMES          MAX   HIGH CURRENT      POINT
 1  Fail_Xid              26      1         7000
 2  Fail_ Q               25      0
 3  Mt_Sv_Q[0]      300     9      0          270
 4  sv_mt_bufq             9      0







This Command: clreventq


OK to clear HIGH counts(y/n)?
```

clrlnalm

Clears the alarms associated with a circuit line. Since the statistical alarms associated with a circuit line have associated integration times, they can keep a major or minor alarm active for some time after the cause has been rectified. This command allows these alarms to be cleared, allowing any new alarms to be quickly identified. The **clrlnalm** command can only clear alarms caused by the collection of statistical data. Alarms caused by a network failure cannot be cleared. For example, an alarm caused by a collection of bipolar errors can be cleared, but an alarm caused by a card failure cannot.

Full Name

Clear circuit line alarm

Syntax

clrlnalm <line_number> <fail_type>

Related Commands

dsplns, dsplnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX	Yes

Example 1

```
clrlnalm 14 2
```

Description

Clear the minor alarm caused by frame slips on circuit line 14.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:10 PST

                             Line Alarm Configuration

                       Minor                                   Major

 Violation    Rate    Alarm Time Clear         Rate    Alarm Time Clear
 1) Bpv        10E-7  10 min       3 min         10E-3   10 sec      10 sec
  2) Fs          .01%  10 min       3 min           .1%   10 sec      10 sec
  3) Oof       .0001%  10 min       3 min          .01%   10 sec      10 sec
  4) Vpd          2%    5 min       3 min            5%   60 sec      10 sec
  5) Tsdp        .01%    5 min       3 min           .1%   60 sec      10 sec
  6) Ntsdp       .01%    5 min       3 min           .1%   60 sec      10 sec
  7) Pkterr      .01%  10 min       3 min           .1%  125 sec      10 sec
  8) Los       .0001%  10 min       3 min          .01%   10 sec      10 sec


This Command: clrlnalm 14 2


Continue?
```

Table 14-19 clrlnalm—Parameters

Parameter	Description
line number	Specifies the number of the line.
failure type	Specifies the type of alarm to clear.

clrlnerrs

Clears the errors associated with a circuit line. Since the statistical alarms associated with a circuit line have associated integration times, they can keep a major or minor alarm active for some time after the cause has been rectified. This command allows these alarms to be cleared, allowing any new alarms to be quickly identified. The **clrlnerrs** command can clear only those alarms that the collection of statistical data has caused. You cannot clear alarms caused by a network failure cannot be cleared by **clrlnerrs**.

Full Name

Clear line errors

Syntax

clrlnerrs [<line_number>]

Related Commands

dsplnerrs, prtlnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	Yes

Example 1

`clrlnerrs`

Description

Clear line error counts. In response to the prompt, enter “y” to reset all line error counts to “0.”

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:12 PST

Total Errors

From Code    Frame   Out of Loss of Frame   CRC     Out of
CLN   Errors Slips   Frames Signal BitErrs Errors  MFrames AIS-16
14          0       0       0       -       0       -       -       -



Last Command: clrlnerrs


Next Command:
```

clrlog

Clears the event log. When the log is cleared, one entry remains, “Info Log Cleared”. Before the event log is cleared, a prompts asks you to confirm. See the **dsplog** command for more information on the event log.

Full Name

Clear event log

Syntax

clrlog

Related Commands

dsplog

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	Yes

Example 1

`clrlog`

Description

Clear the event log. When the log is cleared, one entry remains, “Info Log Cleared.” Enter “y” to confirm.

System Response

```
sw151          TN    SuperUser       IGX 16    9.2       Sep. 12 1998 19:19 GMT

Most recent log entries (most recent at top)
Class  Description                                               Date     Time
Info   User SuperUser logged out (Local)                         09/12/96 18:18:57
Major  LN 5.6 Loss of Sig (RED)                                  09/12/96 18:12:22
Info   User SuperUser logged out (Local)                         09/12/96 18:11:17
Info   Clock switch to oscillator of SCC                         09/12/96 18:10:46
Clear  LN 5.6 OK                                                 09/12/96 18:05:11
Minor  LN 5.6 Out of Multi-Frames                                09/12/96 18:03:27
Info   Clock switch to LINE 5.6                                  09/12/96 18:03:12
Clear  LN 5.6 OK                                                 09/12/96 18:02:42
Info   Clock switch to oscillator of SCC                         09/12/96 17:59:24
Major  LN 5.6 Loss of Sig (RED)                                  09/12/96 17:59:24
Info   Clock switch to LINE 5.6                                  09/12/96 17:59:20
Clear  LN 5.6 OK                                                 09/12/96 17:59:20
Major  LN 5.6 Loss of Sig (RED)                                  09/12/96 17:58:51

This Command: clrlog


OK to clear (y/n)?
```

clrmsgalm

Clears the minor alarm due to an alarm message received at an alarm collection port.

Full Name

Clear message alarm

Syntax

clrmsgalm

Related Commands

dspalms, dsplog

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX, BPX	Yes

Example 1

`clrmsgalm`

Description

Clear a minor alarm due to an alarm message.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:59 PST










Last Command: clrmsgalm

No message alarm set
Next Command:
```

clrphyslnalm

Clears the specified statistical alarm associated with a physical line on a UXM card. The physical line statistical alarms include LOS, LOF, AIS, YEL, LOP, Path AIS, and Path YEL. You can display these alarms using the **dspphysln** command. These alarms are shown as the physical line status, at the top of the display, when you run the **dspphysln** command. Alarms caused by a network failure cannot be cleared. For example, an alarm caused by a collection of bipolar errors can be cleared, but an alarm caused by a card failure cannot.

Full Name

Clear physical line alarm

Syntax

clrphyslnalm <line_number> <fail_type>

Related Commands

dspphyslns, dspphyslnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX	Yes

Example 1

`clrphyslnalm 10.1`

Description

Clear an alarm on physical line 10.1.

System Response

```
sw199         TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998 18:10 GMT

                             Line Alarm Configuration

                       Minor                               Major

 Violation    Rate    Alarm Time Clear         Rate    Alarm Time Clear
 1) Bpv        10E-7  10 min       3 min         10E-3   30 sec      10 sec
  2) Fs          .01%  10 min       3 min           .1%   30 sec      10 sec
  3) Oof       .0001%  10 min       3 min          .01%   30 sec      10 sec
  4) Los       .0001%  10 min       3 min          .01%   30 sec      10 sec
  5) Fer         .01%  10 min       3 min           .1%  200 sec      10 sec
  6) CRC         .01%  10 min       3 min           .1%  200 sec      10 sec
  7) Oom        .001%  10 min       3 min           .1%   30 sec      10 sec
  8) Ais16     .0001%  10 min       3 min          .01%   30 sec      10 sec



This Command: clrphyslnalm 10.1


Continue?


sw199         TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  18:11 GMT

                             Line Alarm Configuration

                       Minor                               Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  9) Pkoof       .01%  10 min       3 min           .1%  200 sec      10 sec
  10) Pkterr     .01%  10 min       3 min           .1%  125 sec      10 sec
  11) Badclk      .1%  10 min       3 min            1%   50 sec      10 sec
  12) Vpd          2%   5 min       3 min            5%   60 sec      10 sec
  13) Tsdp       .01%   5 min       3 min           .1%   60 sec      10 sec
  14) Ntsdp      .01%   5 min       3 min           .1%   60 sec      10 sec
  15) Pccpd     .001%   5 min       3 min           .1%   60 sec      10 sec
  16) Bdapd     .001%   5 min       3 min           .1%   60 sec      10 sec



This Command: clrphyslnalm 10.1


Continue?

sw199         TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  18:11 GMT

                             Line Alarm Configuration

                       Minor                               Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  17) Bdbpd     .001%   5 min       3 min           .1%   60 sec      10 sec
  18) Lcv       10E-5  10 min       3 min         10E-3   30 sec      10 sec
  19) Pcvl      10E-7  10 min       3 min         10E-3   30 sec      10 sec
  20) Pcvp      10E-7  10 min       3 min         10E-3   30 sec      10 sec
  21) Bcv       10E-7  10 min       3 min         10E-3   30 sec      10 sec
  22) Rxvpd        1%   5 min       3 min            4%   60 sec      10 sec
  23) Rxtspd     .01%   5 min       3 min           .1%   60 sec      10 sec
  24) Rxbdapd   .001%   5 min       3 min           .1%   60 sec      10 sec
```

```
This Command: clrphyslnalm 10.1


Continue?

sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  18:11 GMT

                             Line Alarm Configuration

                       Minor                                 Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  25) Rxbdbpd   .001%   5 min       3 min           .1%   60 sec      10 sec
  26) Rxntspd    .01%   5 min       3 min           .1%   60 sec      10 sec
  27) Rxhppd    .001%   5 min       3 min           .1%   60 sec      10 sec
  28) Atmhec      .1%  10 min       3 min            1%  120 sec      10 sec
  29) FSyncErr   .01%  10 min       3 min           .1%  200 sec      10 sec
  30) Rxspdm     .01%   4 min       2 min         .001%   30 sec       5 sec
  31) CGWpktds   .01%   5 min       3 min            1%   60 sec      10 sec
  32) CGWcelld   .01%   5 min       3 min            1%   60 sec      10 sec



This Command: clrphyslnalm 10.1


Continue?
 sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  18:12 GMT

                             Line Alarm Configuration

                       Minor                                 Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  33) Txntscds  .001%   5 min       3 min           .1%   60 sec      10 sec
  34) Txhpcdsc  .001%   5 min       3 min           .1%   60 sec      10 sec
  35) Txvcdscd    .1%   5 min       3 min        .0001%   60 sec      10 sec
  36) Txtscdsc   .01%   5 min       3 min           .1%   60 sec      10 sec
  37) Txbdacds  .001%   5 min       3 min           .1%   60 sec      10 sec
  38) Txbdbcds  .001%   5 min       3 min           .1%   60 sec      10 sec
  39) Txcbrcds  .001%   5 min       3 min           .1%   60 sec      10 sec
  40) Txabrcds  .001%   5 min       3 min           .1%   60 sec      10 sec



This Command: clrphyslnalm 10.1


Continue?
 sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  18:12 GMT

                             Line Alarm Configuration

                       Minor                                 Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  41) Txvbrcds  .001%   5 min       3 min           .1%   60 sec      10 sec
  42) TxGwFPds   .01%   5 min       3 min            1%   60 sec      10 sec
  43) RxGwCLds   .01%   5 min       3 min            1%   60 sec      10 sec
```

```
This Command: clrphyslnalm 10.1

Enter Type:
```

Table 14-20 clrphyslnalm—Parameters

Parameter	Description
line number	Specifies the number of the physical line.The format is either *slot* (for a single-trunk card) or *slot.port*.
failure type	Specifies the type of alarm to clear. If not specified, the system prompts with `Enter Type:`.

clrphyslnerrs

Clears the errors associated with a UXM physical line. Since the statistical alarms associated with a circuit line have associated integration times, they can keep a major or minor alarm active for some time after the cause has been rectified. This command allows these alarms to be cleared, allowing any new alarms to be quickly identified. The **clrphyslnerrs** command can clear only those alarms that the collection of statistical data has caused. Alarms caused by a network failure cannot be cleared by **clrphyslnerrs**.

Full Name

Clear UXM physical line errors

Syntax

clrphyslnerrs [<line_number>]

Related Commands

dspphyslnerrs, prtphyslnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	Yes

Example 1

```
clrphyslnerrs 11.3
```

Description

Clear UXM physical line error counts from line on port 3 of slot 11. In response to the prompt, enter “y” to reset all circuit line error counts to “0.”

System Response

```
sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998 18:10 GMT

                              Line Alarm Configuration

                       Minor                                Major

 Violation    Rate    Alarm Time Clear         Rate    Alarm Time Clear
 1) Bpv        10E-7  10 min       3 min         10E-3   30 sec      10 sec
  2) Fs          .01%  10 min       3 min           .1%   30 sec      10 sec
  3) Oof       .0001%  10 min       3 min          .01%   30 sec      10 sec
  4) Los       .0001%  10 min       3 min          .01%   30 sec      10 sec
  5) Fer         .01%  10 min       3 min           .1%  200 sec      10 sec
  6) CRC         .01%  10 min       3 min           .1%  200 sec      10 sec
  7) Oom        .001%  10 min       3 min           .1%   30 sec      10 sec
  8) Ais16     .0001%  10 min       3 min          .01%   30 sec      10 sec


This Command: clrphyslnalm 10.1
```

Table 14-21 clrphyslnerrs—Parameters

Parameter	Description
line number	Specifies the physical line.The format is either *slot* (for a single-trunk card) or *slot.port*.

clrportstats

Clears the statistics for any port on an FRP. This includes the data byte count in the transmit and receive directions and error counts associated with the port. Statistical accumulation then resumes for that port.

Statistics collecting takes place once per minute, so **clrportstats** may not clear statistics that are less than one minute old.

Full Name

Clear port statistics

Syntax

clrportstats <port | *>

Related Commands

dspportstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX	Yes

Example 1

```
clrportstats 9.1
```

Description

Clear the port statistics for port 1 on an FRP card in slot 9. Type “y” to confirm.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2   Aug. 23 1998 10:57 PST

Port Statistics for 9.1         Cleared: Aug. 11 1998 15:32
Port Speed: 256 kbps    Collection Time: 11 day(s) 19:22:09     Corrupted: YES

                      Bytes      Average (kbps)     Util (%)         Frames
From Port:                0            0               0                  0
To Port:                  0            0               0                  0
Frame Errors               LMI Receive Protocol Stats   Misc Statistics
Invalid CRC            0   Status Enq Rcvd          0   Avg Tx Port Q         0
Invalid Alignment      0   Status Xmit              0   FECN Frames           0
Invalid Frm Length     0   Asynch Xmit              0        Ratio (%)        0
Invalid Frm Format     0   Seq # Mismatches         0   BECN Frames           0
Unknown DLCIs          0   Timeouts                 0        Ratio (%)        0
Last Unknown DLCI      0   Invalid Req              0   Rsrc Overflow         0
                           Sig Protocol:  None          DE Frms Dropd         0


This Command: clrportstats 9.1


OK to clear port statistics (y/n)?
```

clrslotalms

Clears the alarm messages associated with the alarms displayed for the Display Slot Alarms command. Alarm messages are cleared for the specified slot only. These counters should be cleared before beginning any monitoring session. This command prompts the user with a “OK to Clear?” message before actually clearing the counters. Use dspslotalms to observe the slot alarms. Refer to the dspslotalms command for a description of the counters cleared by the **clrslotalms** command.

Full Name

Clear slot alarms

Syntax

clrslotalms parameters

Related Commands

dspslotalms

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	BPX	Yes

Example 1

```
clrslotalms 3
```

Description

Clear alarm on slot 3.

Table 14-22 clrslotalms–Parameters

Parameter	Description
slot number	Specifies shelf slot in the BPX node.

clrsloterrs

Clears the counters for the error counts displayed for the Display Slot Errors command. Counters are cleared for the specified slot only. These counters should be cleared before beginning any monitoring session. This command prompts the user with a “OK to Clear?” message before actually clearing the counters. Use dspsloterrs to observe the **slot errors**. Refer to the **dspsloterrs** command for a description of the counters cleared by the **clrsloterrs** command.

Full Name

Clear slot errors

Syntax

clrsloterrs <slot number | *>

Related Commands

dspsloterrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

```
clrsloterrs 3
```

Description

Clear the slot errors in slot 3.

Table 14-23 clrsloterrs–Parameters

Parameter	Description
slot number	Specifies the shelf slot in the node.

clrtrkalm

Clears statistical alarms associated with either a physical or virtual trunk. Note that if a virtual trunk is specified for a command that configures information related to the physical port, then the physical port information is configured for all virtual trunks. This means that using **clrtrkalm** clears parameters on a logical trunk basis, but any changes automatically affect all trunks on the port when you change a physical option. Any changes you make to a virtual trunk on a port affect all virtual trunks on that port.

Since the statistical alarms associated with a trunk have associated integration times, they can keep a major or minor alarm active for some time after the cause has been rectified. The **clrtrkalm** allows these alarms to be cleared, allowing any new alarms to be quickly identified.

The **clrtrkalm** command can only clear alarms caused by the collection of statistical data. Alarms caused by a network failure cannot be cleared. For example, an alarm caused by a collection of bipolar errors can be cleared, but an alarm caused by a card failure cannot.

Note that a virtual trunk also has trunk port alarms that are shared with all the other virtual trunks on that port. You clear and set these alarms together for all the virtual trunks sharing the same port.

Alarms for the BXM and UXM card types are cleared and displayed differently.

Full Name

Clear trunk alarm

Syntax

clrtrkalm <trunk number> <failure type>

Related Commands

dsptrks, dsptrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	No	Yes	IGX, BPX	Yes

Example 1

```
clrtrkalm
```

Description

Statistical trunk alarms are cleared.

System Response

```
sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998 18:10 GMT

                              Line Alarm Configuration

                       Minor                                 Major

 Violation    Rate    Alarm Time Clear         Rate    Alarm Time Clear
 1) Bpv        10E-7  10 min       3 min         10E-3   30 sec      10 sec
  2) Fs          .01%  10 min       3 min           .1%   30 sec      10 sec
  3) Oof       .0001%  10 min       3 min          .01%   30 sec      10 sec
  4) Los       .0001%  10 min       3 min          .01%   30 sec      10 sec
  5) Fer         .01%  10 min       3 min           .1%  200 sec      10 sec
  6) CRC         .01%  10 min       3 min           .1%  200 sec      10 sec
  7) Oom        .001%  10 min       3 min           .1%   30 sec      10 sec
  8) Ais16     .0001%  10 min       3 min          .01%   30 sec      10 sec


This Command: clrtrkalm 10.1
```

Example 2

clrtrkalm 7 4

Description

Clear the minor alarm type 4 caused by dropped voice packets on trunk 7. Respond to the “Continue?” prompt with “y” (for yes) to clear and display the remaining alarms.

System Response

```
beta           TRM   YourID:1        IGX 8430    9.2    Aug. 15 1998 15:15 MST

PLN  Type      Current Line Alarm Status              Other End
7    E1/32     Clear - Line OK                        alpha.10
9    T1/24     Clear - Line OK                        gamma.10
13   T1/24     Clear - Line OK                        alpha.14
15   T1/24     Clear - Line OK                        gamma.15
20   T3/3      Clear - ATM Missing                    -









Last Command: clrtrkalm 7 4


Next Command:
```

Table 14-24 clrtrkalm—Parameters

Parameter	Description
trunk number	Specifies the trunk. Note that, for virtual trunks, no virtual trunk parameter is required—just *slot.port*. The format is either *slot* (for a single-trunk card) or *slot.port*.
failure type	Specifies the type of alarm to clear.

clrtrkerrs

Clears the statistical error counters at the node for the specified physical or virtual trunk. You should do this before you begin any monitoring session and periodically thereafter to determine exactly when a trunk problem begins. Use **dsptrkerrs** to observe errors without clearing counters.

Full Name

Clear trunk errors

Syntax

clrtrkerrs <trunk_number | *>

Related Commands

dsptrkerrs, prttrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

```
clrtkerrs *
```

Description

Clear all trunk errors.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2       Sep. 12 1998 19:37 PST

Total Errors

      Code    Rx Cell Out of  Loss of Frame   HCS     Tx Cell Cell    Cell
TRK   Errors  Dropped Frames  Signal  BitErrs Errors  Dropped Errors  Oofs
 1.1        0       0       0       0       -       0       0       -       -
 1.2        0       0       0       0       -       0       0       -       -









This Command: clrtrkerrs *


Clears errors on all trunks. Continue (y/n)?
```

Table 14-25 clrtrkerrs—Parameters

Parameter	Description
trunk number	Specifies the trunk counter to clear.

clrtrkstats

Clears the node counters used for the Display Trunk Statistics. Counters are cleared for a physical or virtual trunk. You should clear these counters before beginning any monitoring session. This is similar to the **clrtrkerrs** command for errors. This command prompts you with an "OK to Clear?" message before actually clearing the counters. Use **dsptrkstats** to observe the trunk statistics. See the **dsptrkstats** command for a description of the counters cleared by the **clrtrkstats** command.

Full Name

Clear trunk statistics

Syntax

clrtrkstats <*trunk number*>

Related Commands

dsptrkstats

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

```
clrtrkstats
```

Description

Clear the statistics on trunk 3.

Table 14-26 clrtrkstats–Parameters

Parameter	Description
trunk number	Specifies the trunk. Note that, for virtual trunks, no virtual trunk parameter is required—just slot.port. The format is either slot (for a single-trunk card) or slot.port.

cnfbus

Selects the active System Bus. It should only be necessary to use this command when a problem is suspected with the currently active System Bus. As a safeguard against bus failure, each node is equipped with redundant System Buses, Bus A and Bus B. Either bus can be configured as the active bus and the remaining bus is reserved as standby. Use the **dspbuses** command to display the current bus configuration when configuring the buses with the **cnfbus** command.

Full Name

Configure active bus

Syntax

cnfbus <a/b/t/l>

Related Commands

dspbuses

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	Yes	IGX	

Example 1

```
cnfbus t
```

Description

Configure the system bus to toggle.

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2       Sep. 12 1998 19:42 GMT

                                Bus Info

Bus Bandwidth usage in Fastpackets/second   (Snapshot)

    Allocated = 20000      ( 2%)

    Available = 1148000    (98%)



-----------
Bus A: Standby - OK
Bus B: Active - OK


Last Command: cnfbus t


Next Command:
```

Table 14-27 cnfbus—Parameters

Parameter	Description
a	Select Bus A as the active bus.
b	Select Bus B as the active bus.
t	Toggles between buses. It changes the standby bus to the active bus and the active bus to the standby bus.
l	Toggles between buses and lanes. It changes the standby bus to the active bus and the standby lane to the active lane and the active bus to the standby bus and the active lane to the standby lane.

cnfleadmon

Monitors the IGX node's LDM/HDM ports for failures. You can set each of the twelve control lead types to be monitored by firmware on the LDM/HDM card. The monitor reports only lead state changes; no event is reported if the lead remains up from one poll to the next.

You can also set the interval value that determines how frequently the firmware will check the card's serial port leads. To turn off the feature, set the interval value to zero.

Full Name

Monitor LDM/HDM data port leads.

Syntax

cnfleadmon <index> <interval>

Related Commands

dsplogcd, dspcd, addjobtrig

Attributes

Privilege	Jobs	Log	Node	Lock
2	Yes	Yes	IGX	

Example 1

```
cnfleadmon 4 5
```

Description

Tells the LDM/HDM card firmware to monitor data port lead number 4, every 5 seconds.

System Response

```
swsw1          TRM   StrataCom       IGX 8420 9.2.m8    Date/Time Not Set
        |        LDM       | HDM/SDI-RS232 | HDM/SDI-RS449 |   HDM/SDI-V35   |
        |   DCE |   DTE |   DCE |   DTE |   DCE |   DTE |   DCE |   DTE |
     1 |        |        |        |TST/25 |IS/28   |SB/36   |        |        |
     2 |        |        |LL/18   |RI/22   |LL/10   |IC/15   |        |RI/J    |
     3 |DTR/20 |DSR/6   |DTR/20 |DSR/6   |TR/12&30|DM/11&29|DTR/H   |DSR/E   |
==> 4 |RTS/4   |CTS/5   |RTS/4   |CTS/5   |RS/7&25 |CS/9&27 |RTS/C   |CTS/D   |
     5 |        |        |STxD/14 |SRxD/16 |        |        |        |        |
     6  |RL/21   |        |RL/21   |        |RL/14   |TM/18   |        |TM/K    |
     7  |        |DCD/8   |        |DCD/8   |NS/34   |RR/13&31|        |DCD/F   |
     8  |        |        |SRTS/19 |SCTS/13 |        |        |        |        |
     9  |        |        |        |SDCD/12 |        |        |        |        |
     10 |        |        |SF/23   |SI/23   |SF/16   |SI/2    |        |        |
     11 |        |        |        |        |        |SQ/33   |        |        |
     12 |        |        |***/11  |QM/11   |SS/32   |        |        |        |
 Sampling interval for HDM or LDM control lead shown above...........  5 seonds

 This Command: cnfleadmon


 Enter index of data port control lead to be monitored (1-12) :  4
                                                                           MAJO

 swsw1          TRM   StrataCom       IGX 8420  9.2.m8    Date/Time Not Set
        |        LDM       |  HDM/SDI-RS232  |  HDM/SDI-RS449  |   HDM/SDI-V35   |
        |   DCE  |   DTE  |   DCE  |   DTE  |   DCE  |   DTE  |   DCE  |   DTE  |
     1  |        |        |        |TST/25  |IS/28   |SB/36   |        |        |
     2  |        |        |LL/18   |RI/22   |LL/10   |IC/15   |        |RI/J    |
     3  |DTR/20  |DSR/6   |DTR/20  |DSR/6   |TR/12&30|DM/11&29|DTR/H   |DSR/E   |
 ==> 4  |RTS/4   |CTS/5   |RTS/4   |CTS/5   |RS/7&25 |CS/9&27 |RTS/C   |CTS/D   |
     5  |        |        |STxD/14 |SRxD/16 |        |        |        |        |
     6  |RL/21   |        |RL/21   |        |RL/14   |TM/18   |        |TM/K    |
     7  |        |DCD/8   |        |DCD/8   |NS/34   |RR/13&31|        |DCD/F   |
     8  |        |        |SRTS/19 |SCTS/13 |        |        |        |        |
     9  |        |        |        |SDCD/12 |        |        |        |        |
     10 |        |        |SF/23   |SI/23   |SF/16   |SI/2    |        |        |
     11 |        |        |        |        |        |SQ/33   |        |        |
     12 |        |        |***/11  |QM/11   |SS/32   |        |        |        |
 Sampling interval for HDM or LDM control lead shown above...........  5 seonds

 This Command: cnfleadmon 4

 Enter sampling interval for selected control lead (0, 5-255): 5
                                                                           MAJO
```

Table 14-28 cnfleadmon—Parameters

Parameter	Description
index	Index number of the serial data port leads. Values 1through 12. When you enter a different lead index number, an arrow moves to highlight the current monitoring data on that lead.
interval	The timer value in seconds. This determines how frequently the firmware on the LDM/HDM card will check the specified lead. Values 5 through 255 seconds. Default = 0 Enter 0 to turn off the feature.

cnflnalm

Sets the trunk and line alarm values for failures that are statistical in nature. Statistical alarms are declared by the switch software when a cards supporting these trunks or lines report too many errors. The switch declares an alarm if the detected error rate equals the **cnflnalm** parameter *error rate* for the period of time designated by the *alarm time* parameter. Error rates that exceed the specified error rate cause an alarm in a proportionately shorter period of time. An alarm is cleared when the error rate remains below the rate specified by *error rate* for a period of time designated by the *clear time*.

You can configure the thresholds for alarms caused by the collection of statistics but not for the alarms caused by a network failure. For example, you can configure the threshold for an alarm caused by a collection of bipolar errors, but you cannot configure an alarm caused by a card failure.

Six parameters exist for each *failure type*—three for minor alarms and three for major alarms. When configuring any item for a minor or major alarm, you must enter a value. You can enter a new value or enter the current value.

Table 14-28 describes the parameters for **cnflnalm**. For each *failure type* listed in Table 14-28, the *alarm classes*, the possible *error rate* options, and default *alarm times* and *clear times* are listed in Table 14-29. Table 14-30 describes the *error rate* options listed in Table 14-29.

Full Name

Configure line alarms

Syntax

cnflnalm <fail_type> <alarm_class> <rate> <alarm_time> <clear_time>

Related Commands

clrclnalm, clrtrkalm, dspclnerrs, dsplnalmcnf, dsptrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	No	Yes	IGX	Yes

Example 1

`cnflnalm`

Description

Display current alarm types.

System Response

```
sw224          TN    SuperUser       IGX 16    9.0.n2    Aug. 27 1998 16:16 GMT

  Line Alarm Types

  1) Bpv           13) Tsdp         25) Rxbdbpd         37) Txbdacdscd
  2) Fs            14) Ntsdp        26) Rxntspd         38) Txbdbcdscd
  3) Oof           15) Pccpd        27) Rxhppd          39) Txcbrcdscd
  4) Los           16) Bdapd        28) Atmhec          40) Txabrcdscd
  5) Fer           17) Bdbpd        29) FSyncErr        41) Txvbrcdscd
  6) CRC           18) Lcv          30) Rxspdm          42) TxGwFPdscd
  7) Oom           19) Pcvl         31) CGWpktdscd      43) RxGwCLdscd
  8) Ais16         20) Pcvp         32) CGWcelldscd
  9) Pkoof         21) Bcv          33) Txntscdscd
  10) Pkterr       22) Rxvpd        34) Txhpcdscd
  11) Badclk       23) Rxtspd       35) Txvcdscd
  12) Vpd          24) Rxbdapd      36) Txtscdscd


Last Command: cnflnalm


Next Command:
```

Example 2

`cnflnalm 27 1 4 4 3`

Description

Set Alarm Type 27, the Minor alarm time threshold, to 4 minutes. In this example, the **cnflnalm** command is followed by the alarm type (27), the alarm minor or major (1 for minor, 2 for major), the current rate (which is the default of 0.001%, (which is a 4), the new value for Alarm Time of 4 minutes (which is a “4” entry), and the existing Alarm Clear time of “3.”

System Response

```
pubsigx1       TN    SuperUser       IGX 32    9.2        Aug. 20 1998 17:19 GMT

                             Line Alarm Configuration

                       Minor                                  Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  25) Rxbdapd   .001%   5 min       3 min           .1%   60 sec      10 sec
  26) Rxbdbpd   .001%   5 min       3 min           .1%   60 sec      10 sec
  27) Rxhppd    .001%   4 min       3 min           .1%   60 sec      10 sec
  28) Atmhec      .1%  10 min       3 min            1%  120 sec      10 sec
  29) FSyncErr   .01%  10 min       3 min           .1%  200 sec      10 sec
  30) Rxspdm     .01%   4 min       2 min         .001%   30 sec       5 sec




Last Command: cnflnalm 27 1 4 4 3


Next Command:
```

Table 14-29 cnflnalm—Parameters

Parameter	Description
Failure type	Specifies the failure type. The list that follows gives the number for each failure type. (Items with an asterisk pertain to ATM only.) **1** Bpv—Bipolar violations **2** Fs —Frame slip **3** oof—Out of frame **4** Vpd -Voice packets dropped (TX) **5** Tspd—Time stamped packets dropped (TX) **6** Ntspd—Non-time stamped packets dropped **7** Pkterr—Packet error **8** Los—Loss of signal **9** Fer—Frame error **10** CRC—Cyclic Redundancy Check **11** Pkoof—Packet out of frame **12** Oom—Out of multiframe **13** Ais16—Alarm information signal—E1/E3 Only **14** Bdapd—Bursty data A packets dropped **15** Bdbpd—Bursty data B packets dropped **16** Badclk—Bad clock **17** Pccpd—PCC packets dropped **18** * Lcv—Line code violations **19** * Pcv1—P-bit parity code violations **20** * Pcvp—C-bit parity code violations **21** * Bcv—PLCP BIP-8 code violations **22** * Rxvpd—Receive voice packets dropped **23** * Rxtspd—Receive time stamped packets dropped **24** * Rxntspd—Receive non-time stamped packets dropped **25** * Rxbdapd—Receive bursty data A packets dropped **26** * Rxbdbpd—Receive bursty data B packets dropped **27** * Rxhppd—Receive high priority packets dropped **28** * Atmhec—Cell header HEC errors **29** * Plcpoof—PLCP out of frame **30** * 30—Rxspdm: Receive spacer packets dropped
alarm class	Specifies the class of alarm to be configured for the specified alarm type. Valid alarm classes are: • Minor alarm • Major alarm

Table 14-29 cnflnalm—Parameters (Continued)

Parameter	Description
rates	Specifies the error rate at which the error must occur before an alarm is declared. The choices for error rates vary depending on the *failure type* and the *alarm class*. The choices are called out as Error Rate Options. The default error rates are indicated. With the exception of a Vpd (voice packets dropped) failure, you enter the number corresponding to the error rate. For Vpd (voice packets dropped) failures, you enter a percentage for the dropped packet rate in the range 1%–10%. See Table 14-29 for failure type and Table 14-30 for error rate options.
alarm time	Specifies the time that a condition must exceed a threshold before an alarm is declared. For minor alarms, the alarm time has a range of 3–10 minutes. For major alarms, the alarm time has a range of 10–250 seconds.
clear time	Specifies the time that the condition must exceed the selected threshold before the alarm is cleared. For minor alarms, the clear time has a range of 3–10 minutes. For major alarms, the clear time has a range of 10–250 seconds.

Table 14-30 Failure Type Parameters

Failure Type	Alarm Class	Error Rate Options *	Alarm Time	Clear Time
		Option B		
1–Bpv	1–minor	Default = 4	10 Minutes	3 Minutes
	2- major	Default = 2	10 Seconds	10 Seconds
		Option A		
2–Fs	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 2	10 Seconds	10 Seconds
3–Oof	1–minor	1: 1% 2: 0.1% 3: 0.01% 4: 0.001% 5: 0.0001% (Def.)	10 Minutes	3 Minutes
	2–major	1: 1% 2: 0.1% 3: 0.01% (Def.) 4: 0.001%	10 Seconds	10 Seconds
4- Vpd	1–minor 2–major	Any dropped packet rate from 1% to 10%	5 Minutes 60 Seconds	3 Minutes 10 Seconds
		Option A		
5- Tspd	1–minor	Default = 3	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
6–Ntspd	1–minor	Default = 3	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
7- Pkterr	1–minor 2–major	Any error count from 1–10,000	10 Minutes 125 Seconds	3 Minutes 10 Seconds
		Option A		
8-Los	1–minor	Default = 5	10 Minutes	3 Minutes
	2–major	Default = 3	10 Seconds	10 Seconds
		Option A		
9- Fer	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 2	200 Seconds	10 Seconds

Table 14-30 Failure Type Parameters (Continued)

Failure Type	Alarm Class	Error Rate Options *	Alarm Time	Clear Time
		Option A		
10- CRC	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 2	200 Seconds	10 Seconds
		Option A		
11–Pkoof	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 2	200 Seconds	10 Seconds
		Option A		
12- Oom	1–minor	Default = 4	10 Minutes	3 Minutes
	2–major	Default = 2	10 Seconds	10 Seconds
		Option A		
13- Ais16	1–minor	Default = 5	10 Minutes	3 Minutes
	2–major	Default = 3	10 Seconds	10 Seconds
		Option A		
14–Bdapd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
15- Bdbpd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
16–Badclk	1–minor	Default = 2	10 Minutes	3 Minutes
	2–major	Default = 1	50 Seconds	10 Seconds
		Option A		
17–Pccpd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option B		
18–Lcv	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 1	10 Seconds	10 Seconds
		Option B		
19–Pcv1	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 1	10 Seconds	10 Seconds
		Option B		
20–Pcvp	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 1	10 Seconds	10 Seconds
		Option B		
21–Bcv	1–minor	Default = 3	10 Minutes	3 Minutes
	2–major	Default = 1	10 Seconds	10 Seconds
		1–10%		
22–Rxvpd	1–minor	Default =1%	5 Minutes	3 Minutes
		1–10%		
	2–major	Default = 4%	60 Seconds	10 Seconds
		Option A		
23–Rxtspd	1–minor	Default = 3	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
24–Rxbdapd	1–minor	Default = 3	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds

Table 14-30 Failure Type Parameters (Continued)

Failure Type	Alarm Class	Error Rate Options *	Alarm Time	Clear Time
		Option A		
25–Rxbdbpd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
26–Rxntspd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
27–Rxhppd	1–minor	Default = 4	5 Minutes	3 Minutes
	2–major	Default = 2	60 Seconds	10 Seconds
		Option A		
28–Atmhec	1–minor	Default = 4	10 Minute	3 Minutes
	2–major	Default = 2	120 Seconds	10 Seconds
		Option A		
29–Plcpoof	1–minor	Default = 4	10 Minutes	3 Minutes
	2–major	Default = 2	200 Seconds	10 Seconds
		Option A		
30–Rxspdm	1–minor	Default = 4	4 Minutes	2 Minutes
	2–major	Default = 2	10 Seconds	5 Seconds

Table 14-31 Parameters for Error Rate Options

Error Rate Options		
Option	**Alarm Class**	**Error Rate**
A	**1** - minor	**1** - 1% **2** -.1% **3** -.01% **4** -.001% **5** -.0001%
	2 - major	**1** - 1% **2** -.1% **3** -.01%
B	**1** - minor	**1** - 10E-4 **2** - 10E-5 **3** - 10E-6 **4** - 10E-7 **5** - 10E-8
	2 - major	**1** - 10E-2 **2** - 10E-3 **3** - 10E-4 **4** - 10E-5 **5** - 10E-6

cnfoamlpbk

The **cnfoamlpbk** command configures the RAS OAM Loopback tests. RAS OAM stands for Reliability, Availability, and Serviceability–Operations, Administration, and Maintenance. The **cnfoamlpbk** command interacts with the firmware, and informs the card that the functionality should be turned on or off.

The OAM Loopback test is a nonintrusive test used to send OAM cells only on idle PVCs. Its purpose is to verify connection continuity, and to log alarms when significant continuous cell loss is encountered. You enable or disable this test is enabled at a card level, not at a connection level.

The OAM cell is initiated at an endpoint and sent into the network, where it will be returned by the card at the remote end of the connection. If the end points reside in Fast Packet cards, then 'test delay' cells are transmitted instead of OAM loopback cells. The cells will not go through NNI trunks. When ten consecutive cells are not received, the PVC is declared to be failed.

When an OAM Loopback failure is detected, it is not seen by the end point unless the OAM Loopback test is enabled locally at the end point.

No remote end loopback is necessary for this test to run. OAM cells are automatically recognized and returned without the remote end having to loop back all data.

The OAM cell will be transmitted on each idle PVC. You can configure the preferred transmission rate by using the **cnfoamlpbk** command. The actual transmission rate will vary, depending upon how idle the connection is. An idle PVC is defined to be one that does not receive any data for a whole minute. In order not to consume too much trunk bandwidth or real time on the interface cards, the cells are transmitted only on connections that are not receiving data. If the connection is receiving data, it is assumed that the PVC has not failed. The test is conducted at both the end points. Since the OAM Loopback Test is enabled on a card level, the loopback cell will be transmitted on all connections that are configured, upped and idle.

In the case of BXM and UXM endpoints, cells are transmitted on all connections rather than just idle ones. This is because it take more CPU time to determine if there is no traffic on the PVC.

The OAM Loopback Test will be enabled or disabled with the user command **cnfoamlpbk**. This command will interact with the firmware, and will inform the card that the functionality is to be turned on or off.

The OAM Loopback test will report failures in two forms. First, switch software sends Robust Connection Alarm messages to WAN Manager. The Robust Alarm messages will result in SNMP traps being generated and forwarded to StrataView's RTM Proxy. The second way in which test will report results is through the user command **dspcons** on the node. The OAM failure is not propagated and the CLI will only show OAM failures on the node that has OAM Loopback feature enabled.

The OAM Loopback Test will consider a PVC to be failed if ten consecutive loopback cells do not return. When a failure occurs, this information will be stored in switch software. The test continues to run even when connections are in a failed state. You can still view the results of the test by using the **dspcons** *-oam* command.

Using RAS–OAM Loopback Feature in Networks with Mixed Releases

To use the commands **cnfoamlpbk** and **dspoamlpbk**, the node must be running Release 9.2 or higher. The OAM Loopback test commands are supported on the BXM, UXM, UFM, and FRM cards. The cards must have upgraded firmware. In mixed switch software environments where one end point's switch software is below Release 9.2 (that is, nodes running 9.1, 8.5, or 8.4 releases, for example, the RAS–OAM Loopback tests will be disabled. For all nodes in the network to use the RAS–OAM loopback feature, all nodes must be running Release 9.2 switch software.

The RAS–OAM Loopback test feature is supported for 2 and 3 segment connections and when the remote endpoint is terminated on an Cisco MGX 8220 (AXIS) interface shelf provided the card supports the testcon feature. (See the **tstcon** command on page 14-149.)

Redundancy Issues When Using the RAS–OAM Loopback Feature

In this release, to use the OAM-RAS Loopback Test features, two cards can be in a Y-redundant configuration only if both cards have firmware versions installed that support the Release 9.2 RAS-OAM and Traffic Generation features. If a Y-redundant pair contains one card with a firmware revision that supports the new RAS-OAM functionality, and a second card that does not support it, this configuration will NOT be allowed. The switch software will report a "Mismatch" condition.

You have the option to enable or disable the OAM Loopback Test from the perspective of software regardless of whether the particular version of firmware actually supports the test. Switch software stores the enabled or disabled state in BRAM. If the firmware on the active card of a Y-redundant pair supports the functionality, then software will notify the firmware when this configurable state is modified.

During Y-redundancy card switchovers, the configuration is checked and firmware is notified as appropriate. With this strategy, if the test is enabled for a particular pair, then cards can be swapped without regard to firmware level, and switch software will ensure that the test is run whenever it is supported. This allows the OAM Loopback Test to continue if the cards firmware and both endpoints support it.

The RAS–OAM Traffic Generation Test is stopped when a line card switchover occurs because this feature is mainly for troubleshooting.

OAM Loopback Test

To enable or disable the OAM loopback test, the switch software sends a "Background Loopback Test Command" to the card with parameters for enable/disable, and frequency. Once enabled the test continues until disabled by command. Firmware will allow for polling and/or event type test result messaging. The test if enabled and in event message mode generates unsolicited CBUS events (BXM/UXM cards use CMI instead of CBUS communications) when the pass/fail status transition changes only. The firmware is to protect against false failure for all cases even when the end point node doesn't support the loopback feature.

Full Name

Configure OAM loopback test on specified card slot

Syntax

cnfoamlpbk <*logical slot*> <*e/d*> <*frequency in seconds*>

Related Commands

dspoamlpbk, cnftrafficgen, dsptrafficgen a

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

`cnfoamlpbk`

Description

The **cnfoamlpbk** command will enable or disable the OAM Loopback Test from the perspective of software regardless of whether the particular version of firmware actually supports the test. Software will store the enabled or disabled state in BRAM. If the firmware does support the functionality, then software will notify firmware when this configurable state is modified. During card resets or node rebuilds, this configuration will be checked by software, and firmware will be notified as appropriate. With this strategy, if the test is enabled for a particular slot, then cards can be swapped without regard to firmware level and software will ensure that the test is run whenever it is supported.

The **cnfoamlpbk** command will not accept requests to enable the test for card types other than BXM, UXM, FRM and UFM cards. An appropriate error message will be displayed. On the other hand, software will accept a request to enable the OAM loopback test on one of these cards containing a firmware version that does support the feature. In this case, it will notify you that the firmware is a down-level revision and that the test is not actually running.

To use the ***cnfoamlpbk*** command, you need to have SuperUser level permission.

The ***cnfoamlpbk*** command will take as input the following values:

- the logical slot number of the card
- a flag indicating to enable or disable
- a value indicating the frequency in seconds that cells should be sent, per idle PVC, with a range of 60–600 seconds

The syntax for the command will be:

cnfoamlpbk <*logical slot*> <*e/d*> <*frequency in seconds*>

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:04 PST

From Type      Current Line Alarm Status              Other End
14   T1/24     Major - Tx NTS Packets Dropped         beta.13











Last Command: cnftrkalm 14 d


Next Command:
```

Example 2

cnftrkalm 14 e

Description

Enable the alarms after they have been disabled.

Table 14-32 cnftrkalm—Parameters

Parameter	Description
e | d	Enable or disable trunk alarms.

cnfslotalm

Configures the alarm parameters for the various card types. Upon command entry, the system displays a screen with a choice of 8 card-alarm types. It then displays “Enter Type” and waits for a number in the range 1–12. Upon entry of the alarm type, the system displays the error rates of the selected type.

Full Name

Configure slot alarm parameters

Syntax

cnfslotalm <fail_type> <alarm_class> <rate> <alarm_time> <clear_time>

Related Commands

dspslotalms

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	BPX	Yes

Example 1

```
cnfslotalm 10
```

Description

Configure the alarm parameters.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2 Sep. 12 1998 19:43 PST

  Slot Alarm Types

  1) Standby PRBS Errors                  11) Poll Clk Errors
  2) Rx Invalid Port Errs                 12) CK 192 Errors
  3) PollA Parity Errors
  4) PollB Parity Errors
  5) Bad Grant Errors
  6) Tx Bip 16 Errors
  7) Rx Bip 16 Errors
  8) Bframe parity Errors
  9) SIU phase Errors
  10) Rx FIFO Sync Errors




This Command: cnfslotalm


Enter Type:
```

The screen display after selecting alarm type 10:

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2       Sep. 12 1998 19:47 PST

                             Slot Alarm Configuration

                       Minor                               Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  1) SPRBS        .1%  10 min       3 min            1%  100 sec     100 sec
  2) InvP         .1%  10 min       3 min            1%  100 sec     100 sec
  3) PollA        .1%  10 min       3 min            1%  100 sec     100 sec
  4) PollB        .1%  10 min       3 min            1%  100 sec     100 sec
  5) BGE          .1%  10 min       3 min            1%  100 sec     100 sec
  6) TBip         .1%  10 min       3 min            1%  100 sec     100 sec
  7) RBip         .1%  10 min       3 min            1%  100 sec     100 sec
  8) Bfrm         .1%  10 min       3 min            1%  100 sec     100 sec
  9) SIU          .1%  10 min       3 min            1%  100 sec     100 sec
  10) RFifo       .1%  10 min       3 min            1%  100 sec     100 sec

Last Command: cnfslotalm 10


Next Command:
```

cnftrkalm

Configures trunk alarm reporting. When trunks are upped and added to the network, alarm reporting automatically is enabled. The **cnftrkalm** command lets you disable alarms on a trunk. Disabling alarms may be useful, for example, for trunks that are connected to the node but not yet in service or if the node is experiencing occasional bursts of errors but is still operational. (When the alarms are enabled, they cause an alarm output from the DTI Group Alarm Connector (if present) and an alarm indication on the Cisco WAN Manager terminal.)

Full Name

Configure trunk alarms

Syntax

cnftrkalm <trunk number> <e | d>

Related Commands

dspalms, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

```
cnftrkalm 14 d
```

Description

Disable trunk alarms on trunk 14, which has a major alarm. After using this command to disable the alarms, the only indication that the alarms have been disabled is to observe the **dspalms** screen while a trunk alarm exists. The **dspalms** screen displays the word “disabled” after “PLN Alarms.” Therefore, when you disable trunk alarms, be sure to note this action so you remember to enable alarms after the cause of the trunk failure has been corrected.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:04 PST

From Type      Current Line Alarm Status               Other End
14   T1/24     Major - Tx NTS Packets Dropped          beta.13











Last Command: cnftrkalm 14 d


Next Command:
```

Example 2

cnftrkalm 14 e

Description

Enable the alarms after they have been disabled.

Table 14-33 cnftrkalm—Parameters

Parameter	Description
e | d	Enable or disable trunk alarms.

dellp

Deletes an external, local, remote, or local-remote (tiered nets) loopback form the designated channel, set of channels, or port. After the loopback is deleted, any conditioning applied during the loopback process is removed and service is restored.

Add local loopbacks with the **addloclp** command.

Add remote loopbacks by using the **addrmtlp** command.

Add external loopbacks by using the **addextlp** command.

A local loop can be deleted only from the node that added it. However, a remote loop can be deleted from the node at either end of the connection.

Add local-remote loopbacks by using the **addlocrmtlp** command. Note that with local-remote loopbacks, execution of **dellp** is mandatory after testing is complete, otherwise continuity errors will follow.

In this release, the **addloclp** and **addlocrmtlp** commands support the two-segment connection at the hub node port endpoint in a network of IGX routing hubs and SES interface shelves. The **addloclp** and **addlocrmtlp** commands are blocked at the interface shelf trunk endpoint. The **addrmtlp** command is not supported at either endpoint of the connection. You can use the **dellp** command to remove the local (or local remote) loopbacks that have been added; however, you cannot use the **dellp** command at the trunk endpoint of the connection—it will be blocked. Loops of any kind are not supported for the middle segment of a three-segment connection.

Full Name

Delete loopback from connections or a port

Syntax

dellp <channel(s)>

Related Commands

addextlp, addloclp, addlocrmtlp, addrmtlp

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX, BPX	Yes

Example 1

`dellp 5.1.121`

Description

Delete the loopback on channel 5.1.121. The connections screen appears with connection 5.1.121 highlighted. (The highlighting is not visible in the screen example, but the loop symbols indicates loopback.) The display prompts you to confirm deletion of the loopback. To confirm, enter “y.”

System Response

```
pubsipx1       TN    SuperUser       IGX 8420    9.1.00    May  29 1998 19:16 PDT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
 5.1.121       )pubsipx1    8.33.133        Ok     atfr
 5.1.122        pubsipx1    8.34.134        Ok     atfr
 5.2.111        pubsipx1    8.45.155        Ok     atfr
 5.2.112        pubsipx1    8.45.156        Ok     atfr
 8.33.133       pubsipx1   (5.1.121         Ok     atfr
 8.34.134       pubsipx1    5.1.122         Ok     atfr
 8.45.155       pubsipx1    5.2.111         Ok     atfr
 8.45.156       pubsipx1    5.2.112         Ok     atfr




This Command: dellp 5.1.121


Delete these loopbacks (y/n)?
```

Table 14-34 dellp—Parameters

Parameter	Description
channels	Specifies the channel or set of channels whose loopback is to be deleted. The format for *channel* depends on the type of connection, as follows: Voice connection: *slot.channel* Data connection: *slot.port* Frame Relay connection: *slot.port.DLCI* ATM connections: *slot.port.vpi.vci* Access device: *slot.port.connection_ID*

dncd

Downs (or deactivates) a card. When you down a card, it is no longer available as a node resource. You should down a card before you remove it from a card cage. Before it actually downs an active card, the node determines if a standby card is available. If no standby card is present, the node gives you an opportunity to abort the command. If a standby card of the same type is available and you execute **dncd**, the standby card is activated. If no standby card is available and you execute the command, a major alarm results. To activate a downed card, use the **upcd** command.

Note If you remove a card from a card cage without first executing **dncd**, no warning appears.

You cannot down a control card (NPC, NPM, or BCC). Use **switchcc** for control cards.

If the Abit Notifications on LMI/ILMI Interface feature is enabled (with **cnfnodeparm**), after downing the trunk, the master node will deroute the connections or condition the connections due to path fail. (For information on the Abit Notifications on LMI/ILMI Interface feature in Release 9.1.07, refer to "Summary of Commands" section on page 4-83.)

Full Name

Down card

Syntax

dncd <slot number>

Related Commands

dspcds, resetcd, upcd

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	Yes	IGX, BPX	Yes

Example 1

```
dncd 9
```

Description

Down card 9.

Table 14-35 dncd—Parameters

Parameter	Description
slot number	Specifies the slot number of the card to be downed.

dspalms

Displays major and minor alarms throughout the network and more specific alarms at the local node. The **dspalms** command displays the following information:

- The number of failed connections on the node.
- The number of sources failed.
- The number of major and minor circuit line alarms on the node.
- The number of major and minor trunk alarms on the node.
- The number of failed cards on the node.
- The number of missing cards on the node.
- The number of alarms on other nodes in the network.
- The number of APS lines in alarm.
- When the Cisco WAN Manager terminal is at a junction (physically, or **vt**), the number of junction node alarms is displayed.
- The number of unreachable nodes in the network.
- The power supply and power monitor failures on the node.
- Bus failures (either “Failed” or “Needs Diagnostics”).
- FR/ATM Port Communication Failed (OAM Packet Threshold exceeded).
- FR/ATM NNI A-bit Alarms (connections with A bits=0).
- Slot alarms on IGX due to insufficient bus bandwidth allocation on a slot containing a UXM card.
- Any alarm on the ASM card if the node is a BPX.

Trunk alarms are differentiated between those trunks that are disabled and trunks that are not disabled. For more details on each type of alarm, use the “display” command associated with each failed item. Table 14-35 shows the display commands that show error information.

Table 14-36 Commands that Display Error Information

Command	Description
dspcds	Displays cards in the node, with "F" for failures.
dspclns	Displays circuit lines.
dspcons	Displays connections.
dsplog	Displays events affecting the node.
dspnds	Displays unreachable nodes within a network.
dspnw	Displays the network topology and includes alarm status of each node in the network.
dsptrks	Displays trunks.
dsppwr	Displays power supply status and internal temperature.

The **dspalms** command displays the number of APS lines that are in alarm. The **dspalms** command’s display is similar to the **dsplog** command.

Note Statistical alarms are not cleared on an APS switch. This is done to maintain to provide consistency with the way card redundancy works (sometimes referred to as “YRED”). Statistical alarms are not cleared on a YRED switch.

Full Name

Display current node alarms

Syntax

dspalms

Related Commands

dspcds, dspclns, dspcons, dsplog, dspnw, dsptrks, dsppwr

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dspalms

Description

See a summary of all alarms affecting the node.

System Response

```
sw181          TN    SuperUser       BPX 8620    9.2 Oct. 2 1998 12:26 GMT

Alarm summary   (Configured alarm slots: None)
Connections Failed:     None
Groups Failed:          None
TRK Alarms:             None
Line Alarms:            None
Cards Failed:           None
Slots Alarmed:          None
Missing Cards:          1
Remote Node Alarms:     2 Minors
APS Alarms:             1 Minor

Interface Shelf Alarms: None
ASM Alarms:             None



Last Command: dspalms


Next Command:
```

Example 2

`dspalms`

Description

The current alarms on a BPX.

System Response

```
sw53           TN    SuperUser       BPX 8620    9.2     July 21 1998 15:18 GMT

Alarm summary   (Configured alarm slots: None)
Connections Failed:       100
Groups Failed:            None
TRK Alarms:               None
Line Alarms:              None
Cards Failed:             None
Slots Alarmed:            None
Missing Cards:            None
Remote Node Alarms:       1 Unreachable, 5 Majors, 5 Minors
APS Alarms:               1 Minor

Interface Shelf Alarms:   2 Unreachables, 2 Minors
ASM Alarms:               None



Last Command: dspalms


Next Command:
                   SW                                                 MAJOR ALARM
```

Example 3

dspalms

Description

The current alarms on a BPX.

System Response

```
sw118          TN    StrataCom       BPX 8620    9.2    Date/Time Not Set

Alarm summary   (Configured alarm slots: None)
Connections Failed:     None
TRK Alarms:             None
Line Alarms:            None
Cards Failed:           None
Slots Alarmed:          1 Major
Missing Cards:          1
Remote Node Alarms:     1 Minor
APS Alarms:             1 Minor

Interface Shelf Alarms: None
ASM Alarms:             None




Last Command: dspalms
```

Example 4

dspalms

Description

Display APS alarms

System Response

```
alexa       TRM    genre         BPX 8620      9.2         Sep. 9 1998   16:35 PDT


Alarm summary   (Configured alarm slots: None)
Connections Failed:                                        None
TRK Alarms:                                                None
Line Alarms:                                               None
Cards Failed:                                              None
Slots Alarmed:                                             1 Major
Missing Cards:                                             1
Remote Node Alarms:                                        1 Minor
APS Alarms:                                                1 Minor

Interface Shelf Alarms:                                    None
ASM Alarms:                                                None



Last Command: dspalms
```

dspbob

Shows the current state of all inputs from user equipment to the node the state of all outputs from the node to the user equipment. The display is real-time and updated at a user-specified interval. The display refreshes at the designated interval until the Delete key is pressed or until it times out. See the **cnfict** description for information on configuring data interfaces. When used with Frame Relay T1/E1 applications, **dspbob** displays the message "This FRP does not support V.35 ports."

Displaying Signal Status for Port Concentrator Ports

If an FRM-2 or FRP-2 card connects to a Port Concentrator Shelf (PCS), up to 44 ports can be specified with the *port* parameter. In this case, **dspbob** displays the signal status for ports on the PCS. The PCS relays any changes in signal states to the FRM-2 or FRP-2, so a slight delay occurs when signals are updated.

When used for PCS ports, **dspbob** has an optional parameter of measuring port clock speed. Selection of this parameter temporarily interrupts all traffic on the logical port. The events that take place upon input of this parameter are:

1. The port is disabled.
2. Two invalid frames are timed as they go out the port.
3. The port is reactivated.

Full Name

Display breakout box

Syntax

dspbob <port> [interval] [(measure clock speed) y | n]

Related Commands

cnfict, dspcon, dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	Yes

Example 1

`dspbob 5.1`

Description

See the breakout box display for channel 5.1.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:29 PST

Port:           5.1
Interface:      V35   DCE
Clocking:       Normal       (255999 Baud)

      Inputs from User Equipment              Outputs to User Equipment
 Lead Pin State   Lead Pin State     Lead Pin State   Lead Pin State
 RTS   C    Off                          CTS   D    On
 DTR   H    Off                          DSR   E    On
 TxD   P/S  Idle                         DCD   F    Off
 TT    U/W  Unused                       RI    J    Off
                                         TM    K    Off
                                         RxD   R/T  Idle
                                         RxC   V/X  Active
                                         TxC   Y/a  Active


This Command: dspbob 5.1


Hit DEL key to quit:
```

Example 2

dspbob 9.1

Description

See the breakout box display for Frame Relay connections.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:29 PST

Port:           9.1
Interface:      FRI-V35   DTE
Clocking:       Normal

      Inputs from User Equipment              Outputs to User Equipment
 Lead Pin State   Lead Pin State     Lead Pin State   Lead Pin State
 CTS   D    Off                          RTS   C    On
 DSR   E    Off                          DTR   H    On
 DCD   F    Off                          LT    L    Off
 (TM) n    Off                          (RLB) N    Off




This Command: dspbob 9.1


Hit DEL key to quit:
```

Table 14-37 dspbob—Parameters

Parameter	Description
slot	Specifies the slot number of the card containing the port whose input and output pins are to be displayed.
port	Specifies the data port or Frame Relay port whose input and output pins are to be displayed.

Table 14-38 dspbob—Optional Parameters

Parameter	Description
interval	Specifies the time in seconds, between updates of the breakout box display. The range is from 1 to 60 seconds. If no interval is specified, the display is updated at five second intervals. Do not use an interval of "1" second in a busy network.
measure clock speed	For Port Concentrator Shelf (PCS) only, directs the system to measure the clock speed. If a Port Concentrator port is selected, the last measured clock speed is displayed on the Clocking line. When Measure Clock Speed is entered as an optional parameter, the clock is measured first, and the results are displayed. Clock speed measurement for PCS ports is described in the *Cisco WAN Switching System Overview* information for the PCS.

dspbusbw

Displays the amount of bandwidth allocated on the Cell Bus on an IGX node.By default, the system will allocate enough bus bandwidth for one OC-3 when the first line is upped using the **upln** command. If there is not enough allocated Cell Bus bandwidth, the line will not be upped. Cell Bus bandwidth must be allocated before adding connections on the UXM card.

Full Name

Display Cell Bus bandwidth allocated for UXM card.

Syntax

dspbusbw <slot> [u]

Related Commands

cnfbusbw

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX (with UXM)	Yes

Example

```
dspbusbw 6
```

Description

Display the amount of bandwidth allocated on the Cell Bus on the UXM card in slot 6 of the IGX node.

System Response

```
Get updated bandwidth info from card (Y/N)? n

sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998 17:52 GMT

1\NBus Bandwidth Usage for UXM card in slot 6   Last Updated on 04/07/98 12:03:0
0
                          FPkts/sec   Cells/sec    UBUs
Minimum Reqd Bandwidth:          0           0      0
Average Used Bandwidth:          0           0      0
Peak    Used Bandwidth:          0           0      0
Maximum Port Bandwidth:          -       10866      3

Allocated    Bandwidth:                             8
           (Cell Only):          -       32000
           (Cell+Fpkt):      16000       24000
           (Fpkts / 2 + Cells)   <=      32000


Reserved     Bandwidth:          -        4000      1

Last Command: dspbusbw 6


Next Command: dspbusbw 6

Get updated bandwidth info from card (Y/N)? y

sw199          TN    StrataCom       IGX 16    9.1.w9    Apr. 9 1998  17:53 GMT

1\NBus Bandwidth Usage for UXM card in slot 6   Last Updated on 04/09/98 17:53:2
2
                          FPkts/sec   Cells/sec    UBUs
Minimum Reqd Bandwidth:          0           0      0
Average Used Bandwidth:          0           0      0
Peak    Used Bandwidth:          0           0      0
Maximum Port Bandwidth:          -       10866      3

Allocated    Bandwidth:                             8
           (Cell Only):          -       32000
           (Cell+Fpkt):      16000       24000
           (Fpkts / 2 + Cells)   <=      32000


Reserved     Bandwidth:          -        4000      1

Last Command: dspbusbw 6
```

Table 14-39 dspbusbw–Parameters

Parameter	Description
slot	Specifies the slot number of the card containing the universal bus bandwidth information to display.

Table 14-40 dspbusbw–Optional Parameters

Parameter	Description
u	Specifies that the card should update the information with the latest information calculated in firmware. If not provided, the system will prompt you.

Table 14-41 dspbusbw—Screen Information

Display	Description
Minimum Required Bandwidth	Minimum bandwidth in FastPackets per second and cells per second required for all connections currently configured on this card. This is calculated by UXM firmware as connections are added.
Maximum Port Bandwidth	Total bandwidth of all active trunks/ports on this card in FastPackets per second, cells per second and UBUs.
Average Bandwidth and Peak Used Bandwidth	Statistics counters maintained by UXM firmware.These statistic counters display FastPackets per second, cells per second and UBUs. Use this information when calculating the amount of Bus Bandwidth to be allocated. These counters will be cleared when the UXM card is reset.
Last Updated time	Shows the time when the counters were last updated. This will be the current time if you answered yes to the `Get updated bandwidth info from card (Y/N)?` prompt or entered the command with the `u` parameter.
Allocated Bandwidth	The bandwidth allocated for this card using the **cnfbusbw** command. Refer to the *Cisco WAN Switching SuperUser Commands* manual for more information. Allocated bandwidth is specified in FastPackets per second, cells per second and converted to UBU units by the system.

dspbuses

Displays the status of the System Buses on an IPX or IGX node. As a safeguard against bus failure, each node is equipped with redundant System Buses: Bus A and Bus B. Either bus can be configured as the active bus with the other bus as standby. The **cnfbus** command is used to switch the active bus. Each System Bus contains the following buses: Control Bus, Time Division Multiplex (TDM) bus, clock bus and power bus. In addition to showing which System Bus is active and which is standby, the **dspbuses** command also shows which sub-bus needs diagnostics or has failed. Bus status is displayed at the bottom of the screen. Table 14-41 shows the possible status displays and their meaning.

Table 14-42 Possible Bus Status Displays

Status	Description
OK	Bus operation satisfactory
Failed TDM	A failed TDM Bus
Failed CNTL	A failed Control Bus
Needs Diagnostics TDM	The TDM bus needs diagnostics
Needs Diagnostics CNTL	The Control Bus needs diagnostics

The remaining MUXBUS or CELLBUS bandwidth available to assign to cards and circuits is displayed. This is primarily used when configuring the AIT card on the IPX node or BTM card on the IGX node. The user can assign MUXBUS or CELLBUS bandwidth for the IPX or IGX node, respectively. Available bandwidth falls into two categories, namely, *dedicated* and *pooled*. Dedicated bandwidth is reserved by the system for specific purposes, such as Statistical Reserve for PCC traffic. Pooled bandwidth can be assigned to any use but primarily is used for an ATM trunk.

MUXBUS or CELLBUS bandwidth is assigned in quantities of “switches,” “slices,” and “circuits” and the available bandwidth is displayed in three rows accordingly. A single DS0 circuit occupies 333 packets/second of MUXBUS or CELLBUS bandwidth, a “slice” of bandwidth is equivalent to three DS0 circuits for a total of 1000 packets/second. And a switch is 8 slices for a total of 8000 packets/second of bus bandwidth. In a newly installed node with no cards and no circuits installed, the total bus bandwidth that is available to be assigned is listed in the right column of the following table, which is the sum of the dedicated and pooled bandwidth. As cards and circuits are added to the node, the available bandwidth decreases accordingly.

Table 14-43 Bandwidth Units and Capacity

Unit of BW	Quantity	MUXBUS/CELLBUS Capacity
switch	8 slices or 8000 packets/sec.	20
slice	3 DS0's or 1000 packets/sec.	160
DS0	333 packets/sec.	480

Full Name

Display status of buses

Syntax

dspbuses

Related Commands

cnfbus

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX (non-UXM)	No

Example 1

dspbuses

Description

Display status and bandwidth available. The status of Bus A and Bus B is displayed. In this example, both buses are OK and B is the active Control bus (normal operation is for bus A to be the active bus).

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:34 PST

                                Bus Info

Available MUXBUS bandwidth (snapshot)

Dedicated Pooled Units
--------- ------ -----
0          13      8000 pkts/sec
5          104     1000 pkts/sec
22         312     ds0 circuits

Bus Status
-----------
Bus A: Standby - OK
Bus B: Active - OK


Last Command: dspbuses


Next Command:
```

dspclnerrs

Displays the accumulated error count since the last time errors were reset. Table 14-43 lists the types of circuit line errors. The **clrclnerrs** command clears the error counters for circuit lines.

Note The **dsplnerrs** and **dspclnerrs** commands are the same.

Table 14-44 Errors Displayed by the dsplnerrs Command

Type	Explanation
Bipolar errors	Number of times that two consecutive pulses had the same polarity (applies to AMI coding only).
Frame slips	Number of times a frame was discarded to re-establish synchronization.
Out of frames	Number of times a loss of-frame synchronism was detected on this circuit line.
Loss of signal	Number of times the signal level at the circuit line input went below the minimum acceptable level.
Frame bit errors	Number of times the frame bit failed to alternate (frame error).
CRC errors	Number of times the generated CRC character did not match the received CRC character (applies only if CRC checking is enabled).
Out of MFrames	Number of times a multiframe synch error was detected (E1 lines only).
AIS - 16	Number of times the Alarm Information Signal (Blue signal) was received.

Full Name

Display circuit line errors

Syntax

dspclnerrs [slot | slot.line]

Related Commands

clrclnerrs, prtclnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspclnerrs`

Description

Display a summary of all circuit line errors.

System Response

```
sw151          TN    SuperUser       IGX 16    9.2       June 20 1998 12:45 GMT

Total Errors

      Code    Frame   Out of Loss of Frame   CRC     Out of
CLN   Errors Slips   Frames Signal BitErrs Errors  MFrames AIS-16
 9         0       -       0       0       -       0       -       -
 5.1       0       -       0       0       -       0       -       -
12         0       0       0       0       -       0       -       -
 5.2       0       -       0       0       -       0       -       -







Last Command: dspclnerrs


Next Command:
```

Example 2

dspclnerrs 5.1

Description

Display the circuit line errors for line 5.1 on the UFM card in slot 5.

System Response

```
sw151          TN    SuperUser       IGX 16    9.2       June 20 1998 12:38 GMT

Circuit Line 5.1 Status:Major - Out of Frm (RED)       Clrd: 06/20/96 12:08:38
Type                 Count ETS   Status    Type                 Count ETS   Status
Bipolar Err              0     0           Loss of Sig (RED)      0     -
Frame Slips              -     -           AIS         (BLU)      0     -
Out of Frms              0     0           Out of Frms (RED)      2     -
Loss of Sig              0     0           Frm Err Rate(RED)      -     -
Frame BitErrs            -     -           AIS-16      (RED)      -     -
CRC Err                  0     0           Rmt Oof     (YEL)      0     -
AIS-16                   -     -           Out of MFms (RED)            -
Out of MFms              -     -           Rmt Oom     (YEL)      -     -
                                           Local CGA   (RED)      -     -
                                           Remote CGA  (YEL)      -     -




Last Command: dspclnerrs 5.1


Next Command:

                  SW                                                  MAJOR ALAR
```

Table 14-45 dspclnerrs—Optional Parameters

Parameter	Description
slot or slot.line	For most circuit lines, the slot number is the line number. To use this optional parameter on a UFM, enter one of the line numbers. With no optional parameter specification, a summary screen for all line errors appears.

dspeventq

Display information about any configured event queues from the *fail event handler*.

Full Name

Display event queue

Syntax

dspeventq

Related Commands

clreventq

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dspeventq`

Description

Display the contents of the fail event handler on the current node.

System Response

```
swstorm        TN    SuperUser       BPX 8620    9.2    Aug. 24 1998 11:00 GMT

  QUEUE                 LENGTH          THROTTLING
NUM NAMES          MAX   HIGH CURRENT      POINT
 1  Fail_Xid              4      1       14000
 2  Fail_ Q               4      0




Last Command: dspeventq


Next Command:
```

dspfrcbob

Displays the current state of the signals on the FRM-2 or FRP-2 physical port. The display is real-time and updated according to the *interval* parameter. The display refreshes at a user-specified interval until either the Delete key is pressed or until a timeout occurs.

This command does not show inputs from the user equipment. It shows inputs from the Port Concentrator module to the FRI-2.

For the Inputs from the User Equipment, the display shows the signals as either On, Off, Active, or Inactive For the Outputs to User Equipment, the display shows the signals as either On, Off, Active, or Inactive. X.21 State Names and Leads for DTC and DCE interfaces are also displayed as ON or OFF.

Full Name

Display FRC/FRM breakout box

Syntax

dspfrcbob <slot.pot> <interval>

Related Commands

dspbob, dspfrcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	No	No	IGX	Yes

Example 1

`dspfrcbob 5.2`

Description

Display the signals states for port 2 in slot 5.

System Response

```
bootzilla LAN   SuperUser       IGX 8430    9.2    Aug. 4 1998  15:09 GMT

Physical Port:  5.2
Interface:      FTI-X21   DCE
Clocking:       Normal       (512224 bps)

      Inputs from User Equipment              Outputs to User Equipment
 Lead  Pin  State   Lead  Pin  State     Lead  Pin  State   Lead  Pin  State
 C     3/10 On                           I     5/12 On
 T     2/9  Active                       R     4/11 Active


              X.21 State Name    DTE Lead T  C    DCE Lead R  I
               1 Ready                    1  OFF           1  OFF
              13 S Send Data              D  ON            1  OFF
              13 R Receive Data           1  OFF           D  ON
              13 Data Transfer            D  ON            D  ON

This Command: dspfrcbob 6.2 1


Hit DEL key to quit:
```

Table 14-46 dspfrcbob—Parameters

Parameter	Description
slot.pot	Specifies the slot and port of an FRM-2/FRC-2 physical port. Port range is 1–4.
interval	Specifies the screen update interval in seconds. The default is 5 seconds.

dsplog

Displays the event log for a node. Events affecting the node are displayed in chronological order with the most recent events at the top of the log. Events from the FastPAD are integrated into the log. The display includes a description of the event, the date and time of the event, and the alarm class of the event. A “Continue?” prompt is displayed if more than one screen is required to display all the log entries. Events generating alarms are marked “Major” or “Minor”, and events clearing alarms are marked “Clear.”

In this release, **dsplog** entries show the virtual trunk number of a trunk, for example, *slot.port.vtrk*.

For UXM cards with ATM Forum IMA compliant trunks, a trunk is displayed in **dsptrks** as:

<*slot*>.<*primary_port*>*x*<*num ports*>

For example, an IMA trunk would display in the TRK column in the **dsptrks** display as the following:

5.1x4

In this case, 5.1x4 indicates an ATM Forum compliant IMA trunk 5.4 which consists of four physical lines. To see all physical lines belonging to this IMA trunk, you can enter the **dspphyslns** command.

Note that in this release, for IMA trunks, you can configure non-consecutive physical lines. In Release 9.1, an IMA trunk required that consecutive physical lines be configured on the same card. In this release, non-consecutive physical lines are supported.

Note also that to support ATM Forum compliant IMA trunks, the UXM card must have Model B firmware. (Model A firmware supports Cisco proprietary IMA protocol trunks, but not the ATM Forum compliant trunks.)

The **dsplog** displays an SES interface shelf (feeder) when it is added or removed from an IGX 8400 routing hub.

A message displays when you execute the **dsplog** command that tells you when a Hitless Rebuild of the node occurred. See Example 2, which shows even log entries indicating that a hitless rebuild has occurred.

When a hitless rebuild occurs, event log entries indicating the occurrence of the rebuild will be logged. You view these event log entries using ***dsplog***.

Whenever the polling type changes, this event is logged in the event log (displayed using **dsplog** command) on the switch.

Degraded Mode Conditions

Related to “degraded mode” conditions, which may occur when a node has exhausted its internal resources due to excessive messaging (among other possible causes) which leads the node to abort, the node will either switch to the standby CC if it is available, or else it will go to into the degraded mode, assuming that this mode has been enabled. A node indicates that it is in degraded mode by: displaying “degraded” on the console screen; remote nodes generating degraded mode alarms; remote nodes showing the degraded mode as unreachable/degraded (“UNDeg”). The abort that put the node into degraded mode is logged in the switch software log, which you can display using the **dsplog** command.

After a node enters the degraded mode, communication is halted with the rest of the network. All the network nodes immediately transition to communication break with the node in degraded mode.

The communication break generates a Minor Alarm for the network nodes. Each node inserts a special communication break message into the local event log (**dsplog**). For a locally attached Cisco WAN Manager, the message is also inserted into the Cisco WAN Manager event log. This message indicates the communication break was caused by a degraded mode at the remote node.

In addition to the log entries, a Communication Break Robust Alarm trap is generated to Cisco WAN Manager. This trap contains a new alarm type (code 997) which indicates the communication break was caused by a degraded mode at the remote node.

After a node exits the degraded mode, communication resumes with the rest of the network. All the network nodes clear communication break with the node.

The clearing of the communication break clears the Minor Alarm for the network nodes. Communication break clear messages are inserted into the local and Cisco WAN Manager event logs. A Communication break Robust Alarm trap is generated with the clear alarm type (code 998). The log messages and the robust trap for the communication break clear do not indicate that the communication break was caused by the node being in a degraded mode.

APS Alarms displayed with **dsplog** Command

The **dsplog** command displays SONET APS (Automatic Protection Switching) events and alarms.

APS alarms are also propagated to Cisco WAN Manager (called StrataView Plus in previous releases). Refer to "APS Alarms" section on page 4-63 for a list of APS alarms and events. Table 14-47 lists the APS alarms displayed with the **dsplog** command. (APS events are indicated in the table by "Info" class type. Note that events can be displayed with the **dsplog** command, but are not displayed by the **dspapsln** command.)

Table 14-47 APS Alarms displayed with dsplog Command

Class	Description/dsplog text	
Minor	APS standard mismatch	In a two-card APS 1+1 configuration, one card is programmed for GR-253 and the other card is programmed for ITUT.
Minor	APS redundant protection back card missing	Not supported
Minor	APS redundant working back card missing	Not supported
Minor	APS 1+1 Protection hardware Front Card missing	Not supported
Minor	APS 1+1 Working Hardware Front card missing	Not supported
Minor	APS 1/2 channels parameter mismatch front card	Not supported
Minor	APS Firmware missing Protection card	Not supported
Minor	APS Firmware missing Working Card	Not supported
Minor	APS Firmware missing Working card	Not supported
Minor	APS card missing	Indicates that either a BXM front card or back card supporting this APS line is detected as missing by a BXM.
Minor	APS front card missing	Not supported
Minor	APS working back card missing	Not supported
Minor	APS card mismatch	Not supported
Clear	APS OK	APS line is up with no alarms
Clear	APS deactivated	APS line is down
Minor	APS lines looped	APS line is looped

Table 14-47 APS Alarms displayed with dsplog Command (Continued)

Class	Description/dsplog text	
Minor	APS remote signal failure	A remote signal indicates that there is a problem with the far end signalling information in the K1K2 bytes.
Minor	APS Channel Mismatch	Can only happen in bidirectional mode and indicates that there is a problem with the underlying APS channel protocol. The receive K2 channel number does not equal the transmit K1 channel number.
Minor	APS Protection Switch byte failure	Protection switch byte failure or PSB. In bidirectional mode, indicates that there is an invalid K1 byte. The receive K1 request does not match the reverse request and is less than the transmit K1 request. In all modes, a PSB alarm indicates that K1/K2 protocol is not stable.
Minor	APS far end protection failure	Far end protection failure indicates that the far end's protection line is failing. When there is signal failure on the protection channel, the remote end sees Far End Protection Fail.
Minor	APS architecture mismatch[1]	Architecture mismatch means that the APS configuration on one end of the line does not match the APS configuration at the other side of the line. Specifically, GR-253 at one end and ITUT at the other or 1+1 at one end and 1:1 at the other.
Info	APS Init/Clear/Revert	A BXM APS event indicating that the BXM APS has been initialized or a clear switch has occurred or a revert switch has occurred.
Info	Cannot perform a Clear/Revert switch	A BXM APS event indicating that the BXM APS was unable to perform a clear/revert switch.
Info	APS manual switch	A BXM APS event indicating that the BXM APS has performed a user requested manual switch.
Info	Cannot perform a manual switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested manual switch.
Info	APS signal degrade LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal degrade condition. An automatically initiated switch due to a "soft failure" condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Info	Cannot perform a signal degrade LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal degrade condition.

Table 14-47 APS Alarms displayed with dsplog Command (Continued)

Class	Description/dsplog text	
Info	APS signal degrade HiPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a high priority signal degrade condition. An automatically initiated switch due to a “soft failure” condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Info	Cannot perform a signal degrade HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal degrade condition.
Info	APS signal failure LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a signal failure LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal failure condition.
Info	APS signal failure HiPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a high priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a signal failure HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal failure condition.
Info	APS forced switch	A BXM APS event indicating that the BXM APS has performed a user requested forced switch.
Info	Cannot perform a forced switch.	A BXM APS event indicating that the BXM APS was unable to perform a user requested forced switch.
Info	APS lockout switch	A BXM APS event indicating that the BXM APS has performed a user requested switch which prevents switching from working line to protection line from taking place.
Info	Cannot perform a lockout switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested lockout of protection switch.
Info	WTR switch	A BXM APS event indicating that the BXM APS performed a switch due to a Wait to Restore timeout. A state request switch due to the revertive switch back to the working line because the wait-to-restore timer has expired.
Info	Cannot perform a WTR switch.	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a WTR condition.

Table 14-47 APS Alarms displayed with dsplog Command (Continued)

Class	Description/dsplog text	
Info	Exercise switch	Not supported.
Info	Cannot perform an Exercise switch.	Not supported
Info	Reverse switch	A BXM APS event indicating that the BXM APS performed a switch due to a reverse request. A state request switch due to the other end of an APS bi-directional line performing an APS switch.
Info	Cannot perform a Reverse switch.	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a reverse switch request.
Info	No Revert switch	A BXM APS event indicating that the BXM APS performed a switch due to a Do not Revert. A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
Info	Cannot perform a No Revert switch.	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a Do not Revert switch request.
Minor	Standby Line Section Trace	APS standby line alarm
Minor	Standby line path trace	APS standby line alarm
Minor	Standby line path yellow alarm	APS standby line alarm
Minor	Standby line path AIS	APS standby line alarm
Minor	Standby line loss of pointer	APS standby line alarm
Minor	Standby line loss of cell	APS standby line alarm
Minor	Standbyline pclp yellow alarm	APS standby line alarm
Minor	Standby line plcp out of frame alarm	APS standby line alarm
Minor	Standby line yellow alarm	APS standby line alarm
Minor	Standby line alarm indication signal (AIS)	APS standby line alarm
Minor	Standby line out of frame alarm (LOF)	APS standby line alarm
Minor	Standby line loss of signal alarm (LOS)	APS standby line alarm

1 Architecture mismatch indicates that one side supports APS 1+1, and the other end of line is configured for 1:1, or the directional or revertive parameter does not match. Firmware cannot bring the two ends into compliance on the fly—the user must correct the configuration error.

There is no APS power supply alarm.

Logging into a Node in High Priority Login Mode

Example 4 shows a **dsplog** screen where notification is given when high priority mode is in use by the High Priority! string on the screen. The local event log indicates when the high priority mode is entered and exited. (For information on the high priority login feature and when you typically would use it, see “High Priority Login Feature” on page 6.) The following strings are logged:

— “Info User StrataCom logged in (Local High Priority)

— "Info User StrataCom logged out (Local High Priority)

When in local high priority mode, using the **vt** command to execute commands on another node provides a high priority virtual terminal session. If you log into a control port at high priority, and then use the **vt** command to remotely log into another node with high priority VT, then both nodes will be servicing you at a high priority. The local node will service you at the control port high priority, while the remote node serves you at a priority just below the network handler. When using the high priority **vt** command, the screen shows "High Priority VT" and the local event log shows the following strings.

— "Info User StrataCom logged in (Virtual Terminal High Pro)"

— "Info User StrataCom logged out (Virtual Terminal High Pro)"

Similar to the console screen, the Cisco WAN Manager and maintenance log only show the normal VT strings (listed previously).

Full Name

Display event log

Syntax

dsplog

Related Commands

clrogs, dspphyslns, dsptrks

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dsplog

Description

Display the event log for a BPX node.

System Response

```
sw288          TN   YourID: 1        BPX 8620   9.2.j2   Dec. 10 1998 15:39 GMT

Most recent log entries (most recent at top)
Class Description                                             Date     Time
Info   AAL5 shelf on TRK 4.1: Added                           12/10/98 15:31:41
Info   User UserID:1 logged in (Local)                         12/10/98 13:31:14
Info   Invalid Login Attempt via LAN Port (Local)              12/10/98 13:27:50
Info   Invalid Login Attempt via LAN Port (Local)              12/10/98 13:27:41
Info   sw221 added to Network                                  12/10/98 13:27:39
Clear TRK 11.3 OK                                             12/10/98 13:27:31
Info   User UserID:1 logged out (Virtual Terminal)             12/10/98 13:27:31
Minor TRK 11.1 Line Parity Errors                             12/10/98 13:27:31
Info   sw113 at other end of TRK 11.3                          12/10/98 13:27:30
Major TRK 11.3 Path Parity Errors                             12/10/98 13:27:05
Info   sw113 added to Network                                  12/10/98 13:26:55
Info   AAL5 shelf on TRK 4.1: Deleted                        12/10/98 13:18:43
Clear sw221 removed from Network                              12/10/98 13:18:31

This Command: dsplog
```

Example 2

dsplog

Description

Display the event log for a BPX node.

System Response

```
sw99        TN     StrataCom     BPX 8620     9.2.10      Aug. 27 1998 08:59 GMT

Info   BCC 8 Completed hitless rebuild                   04/07/98 14:28:09
Info   User StrataCom logged in (Local)                  04/07/98 14:27:16
Info   BCC 8 Starting hitless rebuild                    04/07/98 14:27:09
Info   CC 8 Starting rebuild due to User Reset Request   04/07/98 14:27:09
Info   T3-2 3 Inserted                                   04/07/98 14:26:40
Info   BNI-155 1 Inserted                                04/07/98 14:25:03







Last Command: dsplog

Next Command:
```

Example 3

dsplog

Description

Display the event log for an IGX node (showing an SES added and then deleted).

System Response

```
oo1          TN   SuperUser        IGX 8450   9.2.zR   Dec. 10 1998 15:39 GMT

Most recent log entries (most recent at top)
Class  Description                                              Date     Time
Clear  AAL5 shelf on on TRK 6.1: Deleted                       12/10/98 15:31:41
Info   AL/5 shelf on TRK 6.1: Added                             12/10/98 13:31:14
Info   AAL5 shelf on TRK 6.1: Added                            12/10/98 13:27:50
Info   AAL5 shelf on TRK 6.1: Deleted                          12/10/98 13:27:41
Info   User SuperUser logged in (Local)                         12/10/98 13:27:39
Info   sw221 added to Network                                   12/10/98 13:27:31
Info   User SuperUser logged out (Virtual Terminal)             12/10/98 13:27:31
Info   User SuperUser logged in (Virtual Terminal)              12/10/98 13:27:31
Info   sw113 added to Network                                   12/10/98 13:27:30
Clear  sw221 removed from Network                               12/10/98 13:27:05
Clear  sw113 removed from Network                               12/10/98 13:26:55
Info   User SuperUser logged out (Virtual Terminal)             12/10/98 13:18:43
Info   User SuperUser logged in (Virtual Terminal)              12/10/98 13:18:31

This Command: dsplog
```

Example 4

dsplog

Description

Display local event log for a BPX node (shows when high priority mode is entered and exited).

System Response

```
sazu       TRM      StrataCom      BPX 8620       9.2        Apr. 23 1999   23:11 GMT

Most recent log entries (most recent at top)

Class  Description                                           Date          Time

Info   User StrataCom logged out(Local)                      04/23/98     23:04:59
Info   User StrataCom logged in(Local)                       04/23/98     23:04:43
Info   User StrataCom logged out(Local High Priority)        04/23/98     23:04:40
Info   User StrataCom logged in (Local High Priority)        04/23/98     23:04:32



Last Command: dsplog

Next Command:

High Priority!                                                       Major Alarm
```

dsplnalmcnf

Displays alarm configuration by alarm type. Each alarm type includes:

- The minor alarm threshold
- The minor alarm time
- The minor alarm clear time
- The major alarm threshold
- The major alarm time
- The major alarm clear time

The alarm threshold, alarm time, and alarm are set in the **cnflnalm** command. See the **cnflnalm** command for descriptions of these parameters.

Full Name

Display line alarm configuration

Syntax

dsplnalmcnf

Related Commands

cnflnalm, dspclnerrs, dsptrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dsplnalmcnf`

Description

View the line alarm threshold configured for a node.

System Responses

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:51 PST

                              Line Alarm Configuration

                       Minor                                    Major

 Violation    Rate    Alarm Time Clear         Rate    Alarm Time Clear
 1) Bpv        10E-7  10 min       3 min         10E-3   10 sec      10 sec
  2) Fs          .01%  10 min       3 min           .1%   10 sec      10 sec
  3) Oof       .0001%  10 min       3 min          .01%   10 sec      10 sec
  4) Vpd           2%   5 min       3 min            5%   60 sec      10 sec
  5) Tsdp        .01%   5 min       3 min           .1%   60 sec      10 sec
  6) Ntsdp       .01%   5 min       3 min           .1%   60 sec      10 sec
  7) Pkterr      .01%  10 min       3 min           .1%  125 sec      10 sec
  8) Los       .0001%  10 min       3 min          .01%   10 sec      10 sec



This Command: dsplnalmcnf


Continue?

---------------

alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:51 PST

                              Line Alarm Configuration

                       Minor                                    Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  9) Fer         .01%  10 min       3 min           .1%  200 sec      10 sec
  10) CRC        .01%  10 min       3 min           .1%  200 sec      10 sec
  11) Pkoof      .01%  10 min       3 min           .1%  200 sec      10 sec
  12) Oom       .001%  10 min       3 min           .1%   10 sec      10 sec
  13) Ais16    .0001%  10 min       3 min          .01%   10 sec      10 sec
  14) Bdapd     .001%   5 min       3 min           .1%   60 sec      10 sec
  15) Bdbpd     .001%   5 min       3 min           .1%   60 sec      10 sec
  16) Badclk      .1%  10 min       3 min            1%   50 sec      10 sec



This Command: dsplnalmcnf


Continue?



alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:52 PST

                              Line Alarm Configuration

                       Minor                                    Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  17) Pccpd     .001%   5 min       3 min           .1%   60 sec      10 sec
  18) Lcv       10E-6  10 min       3 min         10E-2   10 sec      10 sec
  19) Pcvl      10E-6  10 min       3 min         10E-2   10 sec      10 sec
  20) Pcvp      10E-6  10 min       3 min         10E-2   10 sec      10 sec
  21) Bcv       10E-6  10 min       3 min         10E-2   10 sec      10 sec
```

```
  22) Rxvpd        1%   5 min       3 min            4%   60 sec      10 sec
  23) Rxtspd     .01%   5 min       3 min          .1%   60 sec      10 sec
  24) Rxntspd    .01%   5 min       3 min          .1%   60 sec      10 sec


This Command: dsplnalmcnf


Continue?

----------------

alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 10:52 PST

                             Line Alarm Configuration

                       Minor                                  Major

  Violation    Rate    Alarm Time  Clear         Rate    Alarm Time  Clear
  25) Rxbdapd   .001%   5 min       3 min          .1%   60 sec      10 sec
  26) Rxbdbpd   .001%   5 min       3 min          .1%   60 sec      10 sec
  27) Rxhppd    .001%   4 min       3 min          .1%   60 sec      10 sec
  28) Atmhec      .1%  10 min       3 min           1%  120 sec      10 sec
  29) Plcpoof    .01%  10 min       3 min          .1%  200 sec      10 sec
  30) Rxspdm     .01%   4 min       2 min        .001%   10 sec       5 sec




Last Command: dsplnalmcnf


Next Command:
```

dsplnerrs

Displays the accumulated error count since the last time errors were reset. Table 14-47 lists the error types displayed. The **clrlnerrs** command clears the error counters for circuit lines by resetting all error counts to 0.

Table 14-48 Line Error Types

Type	Explanation
Bipolar errors	Number of times two consecutive pulses have the same polarity (occurs only when the line uses AMI coding).
Frame slips	Number of times a frame is discarded to re-establish synchronization.
Out of frames	Number of times a loss of-frame synchronism is detected on this line.
Loss of signal	Number of times the signal level at the circuit line input went below the minimum acceptable level.
Frame bit errors	Number of times the frame bit failed to alternate (frame error).
CRC errors	Number of times the generated CRC character did not match the received CRC character (applies only if CRC checking is enabled).
Out of MFrames	Number of times a multiframe synch error was detected (E1 lines only).
AIS - 16	Number of times the Alarm Information Signal (Blue signal) was received.

Full Name

Display line errors

Syntax

dsplnerrs [line_number]

Related Commands

clrclnerrs, prtclnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

```
dsplnerrs
```

Description

Display the circuit line errors for all lines.

Table 14-49 dsplnerrs—Optional Parameters

Parameter	Description
line number	Specifies the circuit for the error count display. Otherwise, a summary screen for all lines appears.

dspoamlpbk

Use the **dspcons** command to display connections that have failed the OAM Loopback Test.

The enabled or disabled status of the OAM Loopback Test will be displayed for all slots on a single screen. This functionality will be available with the new command ***dspoamlpbk***. Slots will be shown only when they contain card types that support the functionality.

The transmission rate of the OAM Loopback cells is also a configurable value, and this will also be viewable through the same display command. All user levels have permission to use this command. A sample screen display is shown below.

Full Name

Display OAM loopback test state (enabled/disabled) for specified card slot

Syntax

dspoamlpbk, dspcons

Related Commands

cnfoamlpbk, cnftrafficgen, dsptrafficgen

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX, BPX	Yes

Example 1

`dspoamlpbk`

Description

Display OAM Loopback test state

System Response

```
sw99          TN     StrataCom    BPX 8620          9.2.10    Aug. 27 1998 08:59 GMT

         enabled       supported        Xmit rate
slot     in sw         in fw           (seconds/cell)
----     -----         -----           ---------
  2      No             Yes
  3      No             Yes
  5      No             No
  10     Yes            Yes                  120
  11     Yes            No                    60
  12     No             Yes
  14     Yes            Yes                  180




Last Command: dspoamlpbk

Next Command:
```

Example 2

cnftrkalm 14 e

Description

Enable the alarms after they have been disabled.

Table 14-50 cnftrkalm—Parameters

Parameter	Description
e | d	Enable or disable trunk alarms.

dspphyslnerrs

Displays the accumulated line error counts, by failure type, for the specified trunk(s). If no trunk number is entered, a one-line summary of errors for all trunks at the local node is displayed. If a specific trunk number is entered with the command, a detailed analysis, including error threshold (ETH), is displayed. Disabled trunks have their trunk number displayed in dim, reverse video on the screen. The **clrphyslnerrs** command resets all error counts to 0. Table 14-62 contains a brief description of each error.

In this release, on both the BPX and IGX, physical line statistics are displayed on the **dspphyslnstats, dspphyslnstathist,** and **dspphyslnerrs** screens. These commands only accept physical line numbers (that is, slot.port).

Table 14-51 Description of the Errors in the dspphyslnerrs Display

Line Type	Error	Explanation
All except ATM	Bipolar errors	Number of times two consecutive pulses have the same polarity (AMI coding only).
	Frame slips	Number of times a frame is discarded to re-establish synchronization.
	Out of frames	Number of times a loss of-frame synchronism is detected on this circuit line.
	Loss of signal	Number of times the signal level at the circuit line input went below the minimum acceptable level.
	Frame bit errors	Number of times the frame bit failed to alternate (frame error).
	CRC errors	Number of times the generated CRC character did not match the received CRC character (applies only if CRC checking is enabled).
	Out of MFrames	Number of times a multiframe synch error was detected (E1 lines only).
	AIS - 16	Number of times the Alarm Information Signal (Blue signal) was received.
Only ATM	Out of Frames	Number of times a momentary loss of-DS3 frame alignment was detected.
	Loss of sync (XX)	Number of times a loss of-DS3 frame alignment lasting more than XX seconds was detected.
	Packet Error	Number of CRC errors for a packet address.
	Line Code Errors	Number of B3ZS code errors detected.
	P-bit Parity Errors	Number of parity errors for the DS3 parity bit (P-bit) sequence.
	C-bit Parity Errors	Number of parity errors for the DS3 control bit (C-bit) sequence.
	Comm Fails	Number of BCC failed to communicate to the other node.
	Loss of signal	Number of times the signal level at the trunk line input went below the minimum acceptable level.
Only ATM	AIS (BLU)	Number of times the Alarm Information Signal (Blue signal) was received.
	Out of MFrames	Number of times a loss of-frame synchronism in the DS3 multiframe alignment was detected.
	Remote Oof	Number of times the DS3 remote alarm (indicating remote end was out of frame alignment) was received.

Full Name

Display physical line errors

Syntax

dspphyslnerrs [slot | slot.port]
or
dspphyslnerrs <slot.port> (for virtual physical lines)

Related Commands

clrphyslnerrs, prtphyslnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspphyslnerrs`

Description

Display a summary of all physical line errors at the local IGX node.

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:56 PST

Total Errors

       Code    Out of Loss of Frame   HCS
PHYSLN Errors Frames Signal BitErrs Errors
 6.2        0       0       0       0       0
 6.3        0       0       0       0       0
 8.1        0       0       0       0       0
10.1        0       0       0       0       0
11.3        -       0       0       0       0
11.4        -       0       0       0       0
11.5        -       0       0       0       0
11.6        -       0       0       0       0



Last Command: dspphyslnerrs
```

Example 2

`dspphyslnerrs 11.3`

Description

Display a detailed description of the errors for physical line 11.3 (an OC-3 trunk).

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:59 PST

PHYSLN 11.3       Status:Clear - OK
                                                          Clrd: 08/27/97 13:33:15
Type              Count ETS   Status    Type              Count ETS   Status
Out of Frms           0     0           Loss of Sig (RED)     0     -
Loss of Sig           0     0           AIS         (BLU)     0     -
Frame BitErrs         0     0           Out of Frms (RED)     0     -
CRC Err               0     0           Frm Err Rate(RED)     0     -
                                        AIS-16      (RED)     0     -
                                        Rmt Oof     (YEL)     0     -
                                        Loss of Cell          1     -







Last Command: dspphyslnerrs 11.3
```

Example 3

dspphyslnerrs 8.1

Description

Display a detailed description of the errors for physical line 8.1 (an E3/T3 trunk).

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:57 PST

PHYSLN  8.1       Status:Major - Loss of Sig (RED)
                                                          Clrd: 08/27/97 11:04:30
Type              Count ETS   Status    Type              Count ETS   Status
Bipolar Err           0     0           Loss of Sig (RED)     5     -
Out of Frms           0     0           AIS         (BLU)     0     -
Loss of Sig           0     0           Out of Frms (RED)     0     -
Frame BitErrs         0     0           Remote      (YEL)     0     -
CRC Err               0     0           Loss of Cell          0     -
P-bit Parity Errs     0     0           Loss of Pointer       0     -
C-bit Parity Errs     0     0           PLCP Out of Frame     0     -




Last Command: dspphyslnerrs 8.1
```

Example 4

dspphyslnerrs 11.3

Description

Display a detailed description of the errors for physical line 11.3 (an E1 trunk).

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:59 PST

PHYSLN 11.3       Status:Clear - OK
                                                        Clrd: 08/27/97 13:33:15
Type              Count ETS   Status    Type              Count ETS   Status
Out of Frms           0     0           Loss of Sig (RED)     0     -
Loss of Sig           0     0           AIS         (BLU)     0     -
Frame BitErrs         0     0           Out of Frms (RED)     0     -
CRC Err               0     0           Frm Err Rate(RED)     0     -
                                        AIS-16      (RED)     0     -
                                        Rmt Oof     (YEL)     0     -
                                        Loss of Cell          1     -





Last Command: dphyslnerrs 11.3
```

Example 5

dspphyslnerrs 10.1

Description

Display a detailed description of the errors for physical line 10.1 (a T1 trunk).

System Response

```
sb-reef        TN    SuperUser       IGX 16    9.1.l2    Aug. 27 1998 18:03 PDT

PHYSLN 10.1       Status:Clear - OK
                                                        Clrd: 08/27/97 16:43:20
Type              Count ETS   Status    Type              Count ETS   Status
Bipolar Err           0     0           Loss of Sig (RED)     0     -
Out of Frms           0     0           AIS         (BLU)     0     -
Loss of Sig           0     0           Out of Frms (RED)     0     -
Frame BitErrs         0     0           Rmt Oof     (YEL)     0     -
CRC Err               0     0           Loss of Cell          0     -







Last Command: dspphyslnerrs 10.1
```

Table 14-52 dspphyslnerrs—Parameters

Parameter	Description
physical line number	Specifies a physical line for the error display.The form of a specific physical line is *slot* for single-physical line cards or *slot.port* for multi-physical line cards.

dspphyslns

Displays a summary of the connection type and current alarm status for physical lines at the local IGX node. If no trunk number is entered, a one-line summary of errors for all trunks at the local node is displayed. If a specific slot number is entered with the command, a detailed analysis, including error threshold (ETH), is displayed. Disabled trunks have their trunk number displayed in dim, reverse video on the screen. The **clrphyslnerrs** command resets all error counts to 0. Table 14-62 contains a brief description of each error.

In this release, you can configure non-consecutive physical lines on the same IMA trunk. You can use **dspphyslns** to display all physical lines belonging to a particular IMA trunk.

Table 14-53 Description of the Errors in the dspphyslnerrs Display

Line Type	Error	Explanation
All except ATM	Bipolar errors	Number of times two consecutive pulses have the same polarity (AMI coding only).
	Frame slips	Number of times a frame is discarded to re-establish synchronization.
	Out of frames	Number of times a loss of-frame synchronism is detected on this circuit line.
	Loss of signal	Number of times the signal level at the circuit line input went below the minimum acceptable level.
	Frame bit errors	Number of times the frame bit failed to alternate (frame error).
	CRC errors	Number of times the generated CRC character did not match the received CRC character (applies only if CRC checking is enabled).
	Out of MFrames	Number of times a multiframe synch error was detected (E1 lines only).
	AIS - 16	Number of times the Alarm Information Signal (Blue signal) was received.
Only ATM	Out of Frames	Number of times a momentary loss of-DS3 frame alignment was detected.
	Loss of sync (XX)	Number of times a loss of-DS3 frame alignment lasting more than XX seconds was detected.
	Packet Error	Number of CRC errors for a packet address.
	Line Code Errors	Number of B3ZS code errors detected.
	P-bit Parity Errors	Number of parity errors for the DS3 parity bit (P-bit) sequence.
	C-bit Parity Errors	Number of parity errors for the DS3 control bit (C-bit) sequence.
	Comm Fails	Number of BCC failed to communicate to the other node.
	Loss of signal	Number of times the signal level at the trunk line input went below the minimum acceptable level.
Only ATM	AIS (BLU)	Number of times the Alarm Information Signal (Blue signal) was received.
	Out of MFrames	Number of times a loss of-frame synchronism in the DS3 multiframe alignment was detected.
	Remote Oof	Number of times the DS3 remote alarm (indicating remote end was out of frame alignment) was received.

Full Name

Display physical lines

Syntax

dspphyslns [slot]

Related Commands

clrphyslnerrs, prtphyslnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX	No

Example 1

`dspphyslns`

Description

Display a summary of the connection type and current alarm status for all the physical lines at the local IGX node.

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:52 PST

PHYSLN   Type   Current Line Alarm Status                  TRK
 6.2     OC-3    Major - Loss of Sig (RED)                   6.2
 6.3     OC-3    Clear - OK                                  6.3
 8.1     T3     Clear - OK                                  8.1
10.1     E3     Clear - OK                                 10.1
11.3     E1/30  Clear - OK                                 11.3
11.4     E1/30  Major - Loss of Sig (RED)                  11.4-6
11.5     E1/30  Major - Loss of Sig (RED)                  11.4-6
11.6     E1/30  Major - Loss of Sig (RED)                  11.4-6



Last Command: dspphyslns
```

Example 2

`dspphyslns  11`

Description

Display a detailed description of the type and current alarm status for the physical lines in slot 11 (an E1 IMA trunk).

System Response

```
sw228          TN    SuperUser       IGX 16    9.1.w2    Aug. 27 1998 17:53 PST

PHYSLN   Type   Current Line Alarm Status                  TRK
11.3     E1/30  Clear - OK                                 11.3
11.4     E1/30  Major - Loss of Sig (RED)                  11.4-6
11.5     E1/30  Major - Loss of Sig (RED)                  11.4-6
11.6     E1/30  Major - Loss of Sig (RED)                  11.4-6








Last Command: dspphyslns 11
```

Table 14-54 dspphyslns—Optional Parameters

Parameter	Description
slot number	Specifies a particular slot to display.

dsppwr

The **dsppwr** command displays the current status of the power supplies and the temperature in the cabinet.

Full Name

Display power

Syntax

dsppwr

Related Commands

resetcd

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

dsppwr

Description

Display the power status and temperature inside the current IPX node.

System Response

```
pubsipx1       TN    SuperUser       IGX 8420    9.2    Aug. 8 1998  04:24 PDT

         Power Supply Status                              Cabinet Temperature

Monitor      Status          Revision                        26        78
Installed    Active             FP
                                                          C  60  |  |  140  F
                                                          e      |  |       a
   Power Supply Type   +5v   +12v  -12v  -48v  Temp       n  50  |--|  122  h
                                                          t      |  |       r
A  Empty                                                  i  40  |  |  104  e
B  Empty                                                  g      |  |       n
C  AC 400W IPX         Ok    Ok    Ok          Ok         r  30  |  |  86   h
D  AC 400W IPX         Ok    Ok    Ok          Ok         a      |  |       e
                                                          d  20  |  |  68   i
                                                          e      `--'       t


Last Command: dsppwr


Next Command:
```

Example 2

dsppwr

Description

Display the power status and temperature inside the current IGX node.

System Response

```
sw151          TN     SuperUser       IGX 16    9.2       Aug. 23 1998 11:50 GMT

Power Supply Status                                         Cabinet Temperature

Monitor Rev AK, Ser # 247582  -  Status: Active                30        86

   AC Supply    Status                                      C  60  |  |  140  F
A  1  875W      OK                                          e      |  |       a
B  1  875W      OK                                          n  50  |--|  122  h
C  1  Empty                                                 t      |  |       r
D  2  Empty                                                 i  40  |  |  104  e
E  2  Empty                                                 g      |  |       n
F  2  Empty                                                 r  30  |  |  86   h
                                                            a      |  |       e
                                                            d  20  |  |  68   i
                                                            e      `--'       t


Last Command: dsppwr


Next Command:
```

Example 3

dsppwr

Description

Display the power status and temperature inside the current BPX node.

System Response

```
bootzilla TN    SuperUser       BPX 8620    9.2       May  17 1998 11:06 GMT

         Power Status                                     Cabinet Temperature

ASM Status: Active                                           21       69

Power voltage A/B:      0 / 49 V                          C  60  |  |  140  F
                                                          e      |  |       a
PSU  Ins Type Rev SerNum Failure                          n  50  |--|  122  h
 A    N  N/A  N/A   N/A    N/A                            t      |  |       r
 B    Y  ????  00 ......  None                            i  40  |  |  104  e
                                                          g      |  |       n
            Fan Status                                    r  30  |  |  86   h
                                                          a      |  |       e
     FAN   1    2    3                                    d  20  |  |  68   i
         0000 3300 3240 RPM                               e      `--'       t


Last Command: dsppwr


Next Command:
```

dspslotalmcnf

Displays the slot alarm configuration for the BPX node.

Full Name

Display slot alarm configuration.

Syntax

dspslotalmcnf [slot]

Related Commands

dspslotalms

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dspslotalmcnf 7

Description

Display the slot alarm configuration for the BPX.

System Response

```
D1.jea         TRM   SuperUser       BPX 8620    9.2    Aug. 30 1998 12:04 GMT

                             Slot Alarm Configuration

                       Minor                                 Major

  Violation    Rate     Alarm Time  Clear         Rate     Alarm Time  Clear
  1) SBus        .01%  10 min       3 min           .1%    10 sec      10 sec
  2) InvP        .01%  10 min       3 min           .1%    10 sec      10 sec
  3) PollA       .01%  10 min       3 min           .1%    10 sec      10 sec
  4) PollB       .01%  10 min       3 min           .1%    10 sec      10 sec
  5) BGE         .01%  10 min       3 min           .1%    10 sec      10 sec
  6) TBip        .01%  10 min       3 min           .1%    10 sec      10 sec
  7) RBip        .01%  10 min       3 min           .1%    10 sec      10 sec
  8) Bfrm        .01%  10 min       3 min           .1%    10 sec      10 sec
  9) SIU         .01%  10 min       3 min           .1%    10 sec      10 sec


Last Command: dspslotalmcnf 7


Next Command:
```

Table 14-55 dspslotstatcnf—Optional Parameters

Parameter	Description
slot number	Specifies the slot number of the card to be displayed.

dspslotalms

Displays statistical alarms associated with the SIU on each BPX card. The **dspslotalms** command displays a single line for each slot in a local BPX node occupied by a card. Both the card type and the current card alarm status appears. If a card is operating normally, the display shows “Clear - Slot OK.” If fault conditions continue to cause the slot errors to exceed a preset threshold, the column labeled Current Card Alarm Status reflects this fact. The **clrslotalms** command clears these alarm messages if the alarm condition has disappeared. For a list of slot errors, see the **dspsloterrs** description.

Full Name

Display slot alarms

Syntax

dspslotalms

Related Commands

dspsloterrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

`dspslotalms 1`

Description

Display the status of the card in slot 1.

System Response

```
D1.jea         TRM   SuperUser       BPX 8620    9.2    Aug. 30 1998 12:00 GMT

Slot  Type     Current Slot Alarm Status
   7 BCC       Clear - Slot OK
  11 BNI-T3    Clear - Slot OK









Last Command: dspslotalms


Next Command:
```

Table 14-56 dspslotalms—Parameters

Parameter	Description
slot number	Specifies the slot number of the card to display.

dspsloterrs

Displays statistical alarms associated with the SIU on each BPX card. The **dspsloterrs** command takes a slot number as an optional parameter: if you enter **dspsloterrs** without a slot number, the display shows a single line for each slot with statistics that have accumulated for all slots.

Both the card type and current status are displayed. If a card is operating normally, the status is "Clear - Slot OK." If fault conditions persistently cause the slot errors (described in the Display Slot Errors command) to exceed a preset threshold, this fact is displayed under the column labeled Current Card Alarm Status. The **clrslotalm** command clears the alarm messages if the alarm condition has been cleared. Table 14-56 describes the errors is the display.

Table 14-57 Errors Displayed by the dspsloterrs Command

Error	Description
Standby Bus Errors	Indicates a background test over the standby bus produced an error.
Invalid Port Errors	Indicates port number was out of the range 1–3.
Polling Bus A Errors	Parity error occurred on this polling bus.
Polling Bus B Errors	Parity error occurred on this polling bus.
Bad Grant Errors	Error indicates arbiter did not issue a grant to send data before a time-out.
Tx BIP-16 Errors	Data frame transmitted had a checksum error.
Rx BIP-16 Errors	Data frame received with a checksum error.
SIU Phase Errors	Serial Interface Unit on the card did not detect the frame synch properly.
Bframe Errors	Errors detected in the BPX frame on the StrataBus or in a memory operation.

Full Name

Display slot errors.

Syntax

dspsloterrs [slot]

Related Commands

dspslotalms

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

```
dspsloterrs 7
```

Description

Display the alarm statistics for the card in slot 7 of the BPX.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2 Aug. 6 1998  17:54 PDT

BCC 7           Status: Clear - Slot OK                 Clrd: Date/Time Not Set
Type              Count ETS   Status    Type              Count ETS   Status
Stby PRBS Errs        0     0
Rx Invld Prt Errs     0     0
Poll Bus A Parity     0     0
Poll Bus B Parity     0     0
Bad Grant Errs        0     0
Tx BIP-16 Errs        0     0
Rx BIP-16 Errs        0     0
SIU Phase Errs        0     0
Bfrm. Par. Errs       0     0
Rx FIFO Sync Errs     0     0
Poll Clk Errs         0     0
CK 192 Errs           0     0


Last Command: dspsloterrs 7


Next Command:
```

Example 2

dspsloterrs

Description

Display the error status for all slots.

System Response

```
pubsbpx1       TN    SuperUser       BPX 8620    9.2 Aug. 6 1998  18:01 PDT

                        Summary of Slot Errors

           Invld Poll  Poll        Tx    Rx          B-    Rx
     Stdby Rx    A Bus B Bus Bad   BIP-  BIP-  SIU   Frame FIFO  Poll  CK-
     PRBS  Port  Par   Par   Grant 16    16    Phase Par   Sync  Clk   192
Slot Errs  Errs  Errs  Errs  Errs  Errs  Errs  Errs  Errs  Errs  Errs  Errs
1        0     0     0     0     0     0     0     0     0     0     0     0
5        0     0     0     0     0     0     0     0     0     0     0     0
7        0     0     0     0     0     0     0     0     0     0     0     0







Last Command: dspsloterrs


Next Command:
```

Table 14-58 dspsloterrs—Optional Parameters

Parameter	Description
slot number	Specifies the slot number of a card for the display.

dspslotstatcnf

Displays the enabled statistics for the specified slot.

Full Name

Display statistics enabled for a slot.

Syntax

dspslotstatcnf [slot]

Related Commands

dspslotalmcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

```
dspslotstatcnf 7
```

Description

Display thresholds for slot 7.

System Response

```
D1.jea         TRM   SuperUser       BPX 8620    9.2    Aug. 30 1998 12:03 GMT

Statistics Enabled on Slot 7

Statistic                            Samples  Interval  Size  Peaks  Owner
-----------------------------------  -------  --------  ----  -----  ----------
Standby PRBS Errors                       60         0     4   NONE  Automatic
Rx Invalid Port Errors                    60         0     4   NONE  Automatic
Polling Bus A Parity Errors               60         0     4   NONE  Automatic
Polling Bus B Parity Errors               60         0     4   NONE  Automatic
Bad Grant Errors                          60         0     4   NONE  Automatic
Transmit Bip 16 Errors                    60         0     4   NONE  Automatic
Receive Bip 16 Errors                     60         0     4   NONE  Automatic
Bframe parity Errors                      60         0     4   NONE  Automatic
SIU phase Errors                          60         0     4   NONE  Automatic



Last Command: dspslotstatcnf 7


Next Command:
```

dspsv3

Displays the Cisco StrataView Plus L3 (Layer 3) Link Control Blocks. (StrataView Plus is now called Cisco WAN Manager.)

Full Name

Display Cisco StrataView Plus L3 (Layer 3) Link Control Blocks

Syntax

dspsv3

or

dspsv3 <LCB number>

Table 14-59 Description of the Fields in the dspsv3 Display

Field	Explanation
Serial Admin	Serial link admin window
LAN Admin	LAN Admin window
LCB	Link Control Block number (0 is the gateway link)
Node	SV+ gateway node number (0 is local IO)
IP	IP address (* indicates nwip is enabled)

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dspsv3

Description

Display Cisco StrataView Plus L3 Link Control Blocks.

System Response

```
nsaigx2       TN    StrataCom     IGX 16    8.4.18    June 8 1998 06:11 GMT

Number of Active SV3 Links: 2        Serial Admin: None     LAN Admin: None
LCB:  0 Node:   0 IP:*172.16.64.20
LCB:  1 Node:   3 IP:*172.16.64.20

>Last Command: dspsv3
```

Table 14-60 Description of the Fields in the dspsv3 Display

Field	Explanation
Serial Admin	Serial link admin window
LAN Admin	LAN Admin window
LCB	Link Control Block number (0 is the gateway link)
Node	SV+ gateway node number (0 is local IO)
IP	IP address (* indicates nwip is enabled)

Example 1

dspsv3 0

Description

Display Cisco StrataView Plus L3 Link Control Blocks.

Table 14-61 Description of the Fields in the Previous dspsv3 Display

Field	Explanation
LCB	LCB number
Alloc	LCB allocated (1) or no (0)
sv3_lcb_ptr	Address of LCB in memory
IP Address	SV+ IP Address
Response Timer	SV+ Link Response Timer
Idle Timer	Display SV+ Link Idle Timer
Retry Count	SV+ Link Retry Count
Current Protocol State	Link state (idle, reset, transfer, poll)
No. of buffers in the data_q	Messages in the data queue
No. of buffers in the xmit_q	Messages in the transmit queue
No. of buffers in the nflow_q	Messages in the non-flow-controlled queue
Subscribed applications	Applications to which SV+ has subscribed
Update object(s)	Robust object types that have updated status.
Pending	Robust object types that have been updated to SV+, and are waiting for an acknowledgement from SV+.
Robust database update bitmap addresses	What is this: Robust database update bitmap addresses.

System Response

```
nsaigx2       TN    StrataCom     IGX 16    8.4.18    June 8 1998 06:11 GMT


LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
```

```
IP Address: 172.29.9.60
Response Timer: 0
Idle Timer: 600
Retry Count: 120
Current Protocol State: SV3_TRANSFER
No. of Buffers in the data_q: 0
No. of Buffers in the xmit_q: 0
No. of Buffers in the nflow_q: 0

This Command: dspsv3 0

Continue?

LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
Subscribed Applications: Topology MaintLog
                         312024C0

               Update      Pending
Revision:      0           0
Stats Rebuild: 0           0
Subscription:  0           0
Feeder Obj:    0 312029D2  0 312029D4   Feeder Alarm:  0 31202ED8  0 31202EDA
Port Obj:      0 312029C6  0 312029CC   Port Alarm:    0 31202ECC  0 31202ED2
Conn Obj:      0 312024D0  0 31202741   Conn Alarm:    0 312029D6  0 31202C47
Cline Obj:     0 312029B2  0 312029B7   Cline Alarm:   0 31202EB8  0 31202EBD
Trunk Obj:     0 312029BC  0 312029C1   Trunk Alarm:   0 31202EC2  0 31202EC7

Last Command: dspsv3 0

Continue?

LCB: 0 Alloc: 1 sv3_lcb_ptr: 3120248C
Robust Database Updates data:
db_update_flags:     30D6E16C db_pending_flags:    30D6E355
flag_offset_table:   30D6E56C
  1:0    2:0    3:0    4:0    5:0    6:0    7:0    8:1    9:16  10:1A
11:59  12:0   13:D6  14:D7  15:0   16:DC  17:FC  18:0   19:13B 20:0
21:17B 22:17D 23:0   24:0   25:17F 26:0   27:180 28:0   29:181 30:183
31:0   32:0   33:0   34:185 35:0   36:0   37:186 38:0   39:0   40:0
41:0   42:0   43:0   44:0   45:0   46:187 47:0   48:0   49:0   50:0
51:18C 52:0   53:0   54:0   55:0   56:0   57:0   58:0   59:0   60:0
61:0   62:0   63:0   64:0   65:0   66:18D 67:0   68:0   69:0   70:0
71:0   72:0   73:18E 74:0   75:0   76:0   77:0   78:0   79:0   80:0
81:0   82:0   83:0   84:0   85:0   86:0   87:0   88:0   89:0   90:0
91:0   92:18F 93:18F 94:190 95:1A5 96:1A9 97:0   98:0   99:1E8 100:0
101:0   102:0   103:0   104:0

Last Command: dspsv3 0

LCB                          - LCB number
Alloc                        - LCB allocated (1) or not (0)
sv3_lcb_ptr                  - address of LCB in memory
IP Address                   - SV+ IP Address
Response Timer               - SV+ Link Response Timer
Idle Timer                   - Display SV+ Link Idle Timer
Retry Count                  - SV+ Link Retry Count
Current Protocol State       - Link state (idle, reset, transfer, poll)
No. of Buffers in the data_q - Messages in the data queue
No. of Buffers in the xmit_q - Messages in the transmit queue
No. of Buffers in the nflow_q- Messages in the non-flow-controlled queue

Subscribed Applications      - Applications to which SV+ has subscribed

Update                       - Robust object types that have updated object(s)
                               status.
```

```
Pending                       - Robust object types that have been updated to
                                SV+, and are waiting for an acknowledge from
                                SV+.

Robust database update bitmap addresses.
```

dsptrafficgen

The **dsptrafficgen** command displays for a given card slot the enabled state of the Traffic Generation feature, and when enabled, the PVC on which it is enabled. You must enable this feature by using the switch software command **cnftrafficgen**, and it must be supported by the firmware on the card. (See the **cnftrafficgen** command.) The **cnftrafficgen** command lets you enable the Traffic Generation test in switch software, which determines if the firmware supports Traffic Generation by checking the response from the **upcd** command. All user levels have permission to use this command.

The **dsptrafficgen** command will take as input the following value:

- the logical card slot number

The Traffic Generation test does not directly log alarms. To find out if traffic generation is enabled, use the **dsptrafficgen** command.

When the Traffic Generation or OAM Loopback Test is enabled, it affects the **dspchstats** command results in the following ways. The “To Network” and “From Network” totals include user traffic, OAM traffic, and RM traffic. The OAM traffic is generated by the Traffic Generation and OAM Loopback Tests. The “To Port” and “From Port” work as they did previous to Release 9.2.

Full Name

Display traffic generation test state (enabled/disabled)

Syntax

dsptrafficgen <*logical slot*>

Related Commands

dsptrafficgen, cnftrafficgen, cnfoamlpbk, dspoamlpbk, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX, BPX	Yes

Example 1

```
dsptrafficgen 2
```

Description

Display for the specified card slot 2 whether the Traffic Generation test is enabled or not. (If it is enabled, **dsptrafficgen** shows what PVC it is enabled on.

System Response

```
sw99     TN     StrataCom     BPX 8620          9.2.10     Aug. 27 1998 08:59 GMT

         generating       supported
slot     traffic          in fw         Channel
----     -----            -----         -------
 2       Yes              Yes           2.2.6.18







Last Command: dsptrafficgen 2

Next Command:
```

Description

Display whether the Traffic Generation Test is enabled on card slot 2. If it is enabled, shows you what PVC it is enabled on.

Table 14-62 dsptrafficgen—Parameters

Parameter	Description
card slot number	Specifies logical card slot number on which you want to see if the Traffic Generation test is enabled or not.

dsptrkerrs

Displays the accumulated line error counts, by failure type, for the specified trunk(s). If you do not enter a trunk number, a one-line summary of errors for all trunks at the local node is displayed. If you enter a specific trunk number with the command, a detailed analysis, including error threshold (ETH), is displayed. Disabled trunks have their trunk number displayed in dim, reverse video on the screen.

Error rates to be concerned about are any that are incrementing. For example, a yred- switchover may cause some statistical errors. These are expected. But if there are errors happening in a stable situation, then they indicate a problem.

The **clrtrkerrs** command resets all error counts to 0. Table 14-62 contains a brief description of each error.

Table 14-63 Description of the Errors in the dsptrkerrs Display

Line Type	Error	Explanation
All except ATM	Bipolar errors	Number of times two consecutive pulses have the same polarity (AMI coding only).
	Frame slips	Number of times a frame is discarded to re-establish synchronization.
	Out of frames	Number of times a loss of-frame synchronism is detected on this circuit line.
	Loss of signal	Number of times the signal level at the circuit line input went below the minimum acceptable level.
	Frame bit errors	Number of times the frame bit failed to alternate (frame error).
	CRC errors	Number of times the generated CRC character did not match the received CRC character (applies only if CRC checking is enabled).
	Out of MFrames	Number of times a multiframe synch error was detected (E1 lines only).
	AIS - 16	Number of times the Alarm Information Signal (Blue signal) was received.
Only ATM	Out of Frames	Number of times a momentary loss of-DS3 frame alignment was detected.
	Loss of sync (XX)	Number of times a loss of-DS3 frame alignment lasting more than XX seconds was detected.
	Packet Error	Number of CRC errors for a packet address.
	Line Code Errors	Number of B3ZS code errors detected.
	P-bit Parity Errors	Number of parity errors for the DS3 parity bit (P-bit) sequence.
	C-bit Parity Errors	Number of parity errors for the DS3 control bit (C-bit) sequence.
	Comm Fails	Number of BCC failed to communicate to the other node.
	Loss of signal	Number of times the signal level at the trunk line input went below the minimum acceptable level.
Only ATM	AIS (BLU)	Number of times the Alarm Information Signal (Blue signal) was received.
	Out of MFrames	Number of times a loss of-frame synchronism in the DS3 multiframe alignment was detected.

Table 14-63 Description of the Errors in the dsptrkerrs Display (Continued)

Line Type	Error	Explanation
	Remote Oof	Number of times the DS3 remote alarm (indicating remote end was out of frame alignment) was received.

Full Name

Display trunk errors

Syntax

dsptrkerrs [slot | slot.port]
or
dsptrkerrs <slot.port> (for virtual trunks)

Related Commands

clrtrkerrs, prttrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IGX, BPX	No

Example 1

`dsptrkerrs`

Description

Display a summary of all trunk errors at the local node.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 16 1998 13:13 PST

Total Errors

      Code    Rx Pkts Out of  Loss of Frame   CRC     Tx Pkts Packet  Packet
PLN   Errors  Dropped Frames  Signal  BitErrs Errors  Dropped Errors  Oofs
10         -       -       0       0       0       0       0       0       1
14         0       0       0       -       0       -    218M       0       -









Last Command: dsptrkerrs


Next Command:
```

The errors in the left column are statistical counts of transitions into alarm. Statistical alarms are based on these counts.

The errors in the right hand column are integrated alarm counts, in other words how many times has the LOS/OOF/ and so on alarm been declared on the trunk. There is no statistical alarm associated with the integrated alarm, so these have an ETS field of “-”

Example 2

dsptrkerrs 16

Description

Display a detailed description of the errors for trunk 16.

System Response

```
D2.ipx4        TRM   YourID:1        IGX 8420    9.2    Aug. 4 1998 16:34 PST

Packet Line 16 Status: Clear - Line OK               Clrd: Date/Time Not Set
Type               Count ETS   Status    Type              Count ETS   Status
Bipolar Err00Comm Fails0-
Out of Frms00Loss of Sig(RED)1-
Loss of Sig00AIS(BLU)0-
Frame BitErrs00Out of Frms(RED)0-
Tx Voice Pkt Drp00Rmt Oof(YEL)0-
Tx TS Pkt Drp00Packet Oofs(RED)1-
Tx Non-TS Pkt Drp00Rmt Alarms(YEL)0-
Tx NPC Pkt Drp00
Tx Bdata A Pkt Drp00
Tx Bdata B Pkt Drp00
Packet Err41
Packet Oofs00


Last Command: dsptrkerrs 16


Next Command:
```

Table 14-64 dsptrkerrs—Parameters

Parameter	Description
trunk number	Specifies a trunk for the error display. Without a trunk number, a summary for all physical trunks appears. To display error statistics for virtual trunks, however, you must specify a trunk number in the form *slot.port.vtrk*. For all physical trunk types, the trunk number is optional: entering **dsptrkerrs** without a trunk number lists all trunks with errors. For standard trunks, the form of a specific trunk is *slot* for single-trunk cards or *slot.port* for multi-trunk cards.

prtclnerrs

Prints the accumulated error count since the last time errors were reset. This command uses the same syntax and prints the same information as is displayed using the **dspclnerrs** command. The **clrclnerrs** command clears the error counters for circuit lines by resetting all error counts to 0.

Full Name

Print circuit line errors

Syntax

prtclnerrs

Related Commands

clrtrkerrs, prttrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX	Yes

Example 1

`prtclnerrs`

Description

Print a summary of all trunk errors at the local node.

System Response

None available as command produces hardcopy.

prtlog

Prints the event log for a node. Events affecting the node are displayed in chronological order with the most recent events at the top of the log. The printout includes a description of the event, the date and time of the event, and the alarm class of the event. This command uses the same syntax and prints the same information as is displayed using the **dsplog** command. See the **dsplog** command for output information.

Full Name

Print event log

Syntax

prtlog

Related Commands

dsplog

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

`prtlog`

Description

Print the event log for a node.

System Response

None available as command produces hardcopy.

prtlnerrs

Prints the accumulated error count since the last time errors were reset. This command uses the same syntax and prints the same information as is displayed using the **dsplnerrs** command. The **clrlnerrs** command clears the error counters for circuit lines by resetting all error counts to 0.

Full Name

Print line errors

Syntax

prtlnerrs

Related Commands

dsplnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

`prtlnerrs`

Description

Print errors for all upped lines on a node.

System Response

None available as command produces hardcopy.

prtlnerrs

Prints the accumulated error count since the last time errors were reset. This command uses the same syntax and prints the same information as is displayed using the **dsplnerrs** command. The **clrlnerrs** command clears the error counters for circuit lines by resetting all error counts to 0.

Full Name

Print physical line errors

Syntax

prtphyslnerrs

Related Commands

dspphyslnerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX	Yes

Example 1

`prtphyslnerrs`

Description

Print errors for all physical lines on an IGX node.

System Response

None available as command produces hardcopy.

prttrkerrs

Prints a summary of the trunk error counts for both physical and virtual trunks on the local node. This is the same information that displays when you use the **dsptrkerrs** command. See the **dsptrkerrs** command for output information.

Full Name

Print trunk errors

Syntax

prttrkerrs

Related Commands

dsptrkerrs

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IGX, BPX	Yes

Example 1

`prttrkerrs`

Description

Print a summary of trunk errors.

System Response

None available as command produces hardcopy.

resetcd

Resets the hardware and software for a card. The **resetcd** command lets you cause a switch between a primary and redundant service card that have been configured for Y-cable redundancy. (Normally, a failure would cause a switch between Y-cabled cards, but you may want to cause the switch to remove the active card to upgrade its hardware, for example.)

Do not use **resetcd** on an *active* NPC, NPM, or BCC because resetting an active controller card interrupts traffic while it boots. (Resetting a controller card does not destroy configuration information.) If a redundant controller card is present and you want to switch between controllers, use the **switchcc** command to switch the active controller card to standby and the standby controller card to active. You can subsequently reset the standby controller without bringing it to the active state (and therefore not disrupt service).

An example of when you might use the **resetcd r** command is if you ran out of memory and had no standby card. If there were a memory leak problem somewhere in the system, you might execute a **resetcd r** command before you run the **switchcc** command (if you do not have a standby card, or you are not sure of the health of the standby card if there is one), then you might execute it locally on the active processor card (BCC or NPM). Note that you do not need to enter the minus symbol before the "r" in the **resetcd** r command (just **resetcd r**) is acceptable.

The **resetcd** command takes an argument to indicate a hardware or failure reset. A hardware reset (**resetcd h**) is equivalent to physically removing and reinserting the front card and causes the card's logic to be reset. When you reset the hardware of an active card other than a controller card (an NPC, NPM, or BCC), a standby card takes over if one is available. A *failure* reset (**resetcd f**) clears the card failures associated with the specified slot. If a slot contains a front card and back card, **resetcd** resets both cards. A **resetcd r** performs a card reset on processor cards (such as an NPC, NPM, or BCC). Note when the node is in degraded mode, the 'r' option is disabled.

You can use the **resetcd** command to initiate a hitless rebuild manually. The Hitless Rebuild feature provides the ability to effectively rebuild without affecting user traffic. It substantially decreases the time it takes for the BPX to settle into its normal operating state after a rebuild.

Previous to Release 9.2, the **resetcd** command accepted the options "h" for Hard Reset, "f" for Failure Reset, and "b" for Arbitor. The "b" is for BPX nodes only. A new option "r" lets you manually initiate a hitless rebuild on processor cards only. You can use the "r" option to perform a hitless rebuild on processor cards. Note that the "r" option becomes disabled when the node is in degraded mode.

Full Name

Reset card

Syntax

resetcd <slot_num> <reset_type>

Related Commands

resetcd

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	Yes	IGX, BPX	Yes

Example 1

resetcd

Description

Reset the card in slot 23.

System Response

No display produced.

Table 14-65 resetcd—Parameters

Parameter	Description
slot number	Specifies the card number to be reset.
H/F	Specifies whether the hardware or failure history for the card is to be reset. An “H” specifies hardware; an “F” specifies failure history. (“H” performs a Hard Reset; “F” performs a failure reset.)
B	Specifies to use hardware to reset the card, not the CBUS message. (The “B” option is also referred to as the “arbiter” option.) You can use the B option only on BPX nodes.
R	Specifies that a hitless rebuild is performed only on processor cards.
B	Specifies to use hardware to reset the card, not the CBUS message. This applies only to the BPX.

resetpc

The **resetpc** command resets a PCS attached to a specified FRM-2 or FRP-2 physical port. Concentrated links, logical ports, and all connections are temporarily suspended while the PCS hardware performs a warm boot.

Once the PCS re-establishes communication with the FRM-2 or FRP-2, logical ports are reconfigured and connections repaired. A series of messages describing each of the concentrated links failing and being re-established is generated.

Full Name

Reset Port Concentrator

Syntax

resetpc <slot.port>

Related Commands

tstpcs, dsppcs

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	Yes	IGX, BPX	Yes

Example 1

```
resetpc 2.3
```

Description

Reset the card in slot 23.

System Response

No display produced. (Use **dsppcs** to check status.)

Table 14-66 resetpc–Parameters

Parameter	Description
slot.port	Specifies the card and port number to reset.

switchcc

Switches the standby BCC or NPC (or NPM) card to active and the active card to standby. If a standby BCC card is not available, the command is not executed. If a standby BCC is available but is not ready to go active, a prompt asks you to confirm or abort the switch of the control card. This command was previously called "**switchpcc**". Executing **switchcc** has the following effect:

- Control is transferred to the standby controller card.
- Any job currently running is aborted.
- The user is logged off.

Immediately after the switch, the controller card that was previously active reverts to a download mode. This is indicated by the flashing front panel FAIL lamp. The system software image that is always stored in ROM is downloaded to RAM in the event that the system software was corrupted.

After this is completed, the configuration database is downloaded from the newly active controller card to complete the download. This process takes a number of minutes so this controller card is not available for standby operation until this download process is completed. The **switchcc** command results in a very brief interruption of all traffic. Consequently, you should use **switchcc** only when the network can tolerate a brief interruption.

The [f] option for the **switchcc** command will force a CC switchover even if there are pending updates. If you don't specify the [f] option, the system will warn you about pending updates before the switch and give you a choice to not switch over.

In support of the Hitless Rebuild feature, there is no change directly to the user command **switchcc**. However, if the Hitless Rebuild feature is enabled (with **cnfnodeparm** command), the databases needed for a hitless rebuild will be preserved during the subsequent standby rebuild. This will allow for a hitless rebuild if the new standby processor encounters a fatal hardware error shortly after the switchover.

Full Name

Switch control card

Syntax

switchcc [f]

Related Commands

dspcd, dspcds

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	No	IGX, BPX	Yes

Example 1

```
switchcc
```

Description

Change the active NPC/BCC to standby, and the standby NPC/BCC to active.

System Response

No display produced.

tstcon

The **tstcon** command tests the integrity of an IPX or IGX data path by inserting node-generated test data. The connection service is affected for only a few seconds during the test. You can only test existing connections. One channel at a time is tested to minimize disruption. Because service is disrupted for a short time, no conditioning is applied during the test. If a failure is detected, the fault is isolated to a replaceable IPX or IGX node, and the standby card (if available) automatically goes into service. During fault isolation, conditioning is applied to both ends of the connection.

In addition to IPX and IGX routing nodes, the **tstcon** command can test an IPX that has been configured as an interface shelf (IPX/AF) in a tiered network but only after a local-remote loopback has been set up with the **addlocrmtlp** command. After testing is complete, you must remove the loopback established with **addlocrmtlp** by using **dellp**.

Table 14-66 describes the results of executing **tstcon**.

Table 14-67 Results of tstcon Execution

Result	Description
Completed	Total number of tests that were run.
Aborted	Number of tests that did not run because the connection was not testable because of loopbacks or missing or failed hardware.
Failures	Number of tests that failed.
Repaired	Number of connections that failed a previous test and have passed the current test.

If you enter a range of channels (with connections and some without), the unconnected channels are skipped. You can enter the **tstcon** command on the node at either end of the connection. Unlike the **addloclp** and **addrmtlp** commands, **tstcon** does not require external test equipment. You cannot test connections with the **tstcon** command if they are currently looped back with either the **addloclp** or **addrmtlp** commands.

Table 14-67 describes examples of the **tstcon** command with various arguments. Table 14-68 and Table 14-69 describe the required parameters and optional parameters in these examples.

Table 14-68 Examples of tstcon Specification

Command	Description
tstcon *	Test all connections.
tstcon * f	Test all Frame Relay connections.
tstcon * v x	Test all voice connections, abort on first failure.
tstcon 1.3	Test connection on channel 1.3.
tstcon 4.2.200	Test connection on channel 4.2.200.
tstcon 1.13-16	Test connections on channels 1.13-16.
tstcon 3.21-24 x	Test connections on channels 3.21-24, abort on first failure.
tstcon 3.11-20 v	Test voice connections only on channels 3.11-20.
tstcon 3.11-20 v x	Test voice connections only on channels 3.11-20, abort on first failure.
tstcon 3.21-22 v 5	Test voice connections only on channels 3.21-22 and repeat the test 5 times.
tstcon 3.14-15 d x 5	Test data connections on channels 3.14-15: repeat test 5 times. Abort on failure.

For V.35 ports configured for DTE, the following three bulleted items apply:

- Model D FRP along with software Release 8.1 or higher, supports Foresight dynamic congestion avoidance feature. The Model D FRP is required for the AIP application in system software Release 7.1. The enhanced V.35 loop back test is available with this card when using Firmware Revision F and system software 7.1.
- A loop back test pattern signal (Test Mode) is transmitted to a modem or NTU to initiate a loop back. Some modems and NTUs recognize this code but do not return the TM signal even though a loop has been set up. The FRPs, with the exception of the Model D Firmware Rev. F, wait to receive the TM signal from the external equipment before the data test is performed. If the FRP Model D Firmware Rev. F receives the TM signal return, it responds. If FRP Model D Firmware Rev. F does not receive the TM signal, it waits 10 secs and then sends the test pattern. If the external equipment is inoperative or disconnected, the test fails. After the test is completed, transmission of the codes is terminated and the circuit returns to normal operation. The test result is displayed on the node's terminal **tstport** screen.
- Some external equipment support loopback testing but do not recognize the loop test pattern signal (Test Mode) in the data stream. The FRP/FRI toggles the V.35 LLB (local loop back) or the LRB (remote loop back) leads and then sends the test pattern after the time-out period (10 secs). If the external equipment is inoperative or disconnected, the test fails. The IPX or IGX control terminal displays the result of **tstport** execution.

Full Name

Test connections

Syntax

testcon <channel(s)> [-nolp] [type] [failure abort] [repeat count]

Related Commands

dspcons, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

```
tstcon 9.1.100
```

Description

Test connection 9.1.100. The connections screen appears with the connection for channel 9.1.100 highlighted. The system prompts to confirm the test. A “T” after channel under test indicates that the test is currently running on that channel. When the first test is completed, a message appears indicating the results of the tests. As each test is completed, the T moves to the next channel to be tested and the message is updated to include the cumulative results of the tests. When the test is completed for all the specified connections, the “T” disappears and the message indicates the total number of tests and the cumulative results of the test.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:04 PST

 Local      Remote      Remote                                          Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 5.1 T      beta       )25.1       Ok     256                  7/8          0  L
 9.1.100    gamma       8.1.200    Ok     fr                                0  L
 9.1.200    gamma       8.1.300    Ok     fr                                0  L
 9.2.400    beta        19.2.302   Ok     fr(Grp)                           0  L
 14.1       gamma       15.1       Ok     v                                 0  L








Last Command: tstcon 9.1.100

Tests: Completed = 1, Aborted = 0, Failed = 1, Connections Repaired = 0
Next Command:
```

Table 14-69 tstcon—Parameters

Parameter	Description
channels	Specifies the specifies the channel or set of channels whose connections are to be tested. An "*" specifies all connections. Channel is specified in one of the following formats: slot.channelvoice connection slot.portdata connection slot.port.DLCIFrame Relay connection

Table 14-70 tstcon—Optional Parameters

Parameter	Description
-nolp	No automatic loopback. This parameter applies only to local-remote loopbacks and is mandatory for testing a multi-segment connection in a tiered network.
type	Restricts the test to the designated connection type. Valid connection types are listed below. If no connection type is designated, all connections are tested. v Tests only voice connections. d Tests only data connections. f Tests only Frame Relay connections.
x	Aborts the test as soon as a failure is detected. If an "x" is not entered, all specified connections are tested regardless of the test results for each individual connection.

Table 14-70 tstcon—Optional Parameters (Continued)

Parameter	Description
repeat count	Specifies the number of times the test is to be repeated.The range is 1–50. If no test count is specified, the test is run once.

tstconseg

Externally tests the integrity of a connection by sending OAM segment loopback cells over the specified channel for the specified number of times.

Table 14-70 describes the reported results of executing **tstconseg**.

Table 14-71 Results of the tstconseg Display

Result	Description
Completed	Total number of tests that were run.
Aborted	Number of tests that did not run because the connection was not testable because of loopbacks or missing or failed hardware.
Failures	Number of tests that failed.
Repaired	Number of connections that failed a previous test and have passed the current test.

Full Name

Test connection segment

Syntax

tstconseg <channel> <iteration count> [A | a]

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	BPX, IGX	Yes

Example 1

```
tstconseg 11.2.10.17
```

Description

Test connection segment 11.2.10.17. The connections screen appears with the connection for channel 11.2.10.17 highlighted. The system prompts to confirm that the test should begin. A "T" after the channel under test indicates the test is currently running on that channel. When the first test is complete, a message appears indicating the results of the tests. As each test is completed, the T moves to the next channel to be tested and the message is updated to include the cumulative results of the tests. When the test is completed for all the specified connections, the "T" disappears and the message indicates the total number of tests and the cumulative results of the test.

System Response

```
nmsbpx23       TN    SuperUser       BPX 8620    9.2    Aug. 16 1998 12:37 PST

 Local           Remote      Remote                            Route
 Channel         NodeName    Channel         State  Type       Avoid COS O
 11.2.10.17      nmsbpx23    11.1.11.17      Ok     atfst













This Command: tstconseg 11.2.10.17 1


Perform a tstconseg on this connection (y/n)?

----------------

nmsbpx23       TN    SuperUser       BPX 8620    9.2    Aug. 16 1998 12:38 PST

External Connection Segment Test

Status: Test Complete

Connection ID      Test Count     Failure Count  Success Count
11.2.10.17             1               1              0









Last Command: tstconseg 11.2.10.17 1


Next Command:
```

Table 14-72 tstconseg—Parameters

Parameter	Description
channel	Specifies the slot.port.vpi.vci of the channel to be tested.
iteration	Number of times to repeat the test.

Table 14-73 tstconseg—Optional Parameters

Parameter	Description
A|a	Specifies that the test be aborted if an error occurs (not case sensitive).

tstdelay

Puts the remote end of the connection into a loopback state, requests the FRP (Frame Relay) or ASI (ATM) to generate a test packet, calculates the round trip delay (RTD), and displays the round trip delay. This delay includes the FRP or ASI and trunk queuing and processing delays throughout the network. The measured delay using **tstdelay** differs from the ForeSight RTD, which uses a high-priority packet and does not include processing and queuing delays.

Using the **tstdelay** command requires that the FRP is at least a Model D. This test interrupts transmission on the connection during the test. Test results appear at the bottom of the screen (this may include a timeout message, as in Example 1).

Testing an IPX or IGX node that has been configured as an interface shelf requires execution of **addlocrmtlp** prior to **tstdelay** and a **tstdelay** parameter that applies only to tiered networks (see optional parameter table). After testing is complete, the loopback established with **addlocrmtlp** must be removed by **dellp**.

Full Name

Test Frame Relay connection delay

Syntax

tstdelay <slot.port.DLCI> [count] | tstdelay <slot.port.vpi.vci> [-nolp] [count] [y]

Related Commands

addlocrmtlp, dellp, dspcons, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–5	Yes	Yes	IGX, BPX	Yes

Example 1

```
tstdelay 9.1.100
```

Description

Test the delay on Frame Relay channel 9.1.100.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:05 PST

Conn:  9.1.100    gamma       8.1.200     fr
   MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR    FST
 9.6/9.6   9.6/9.6      5/5       256/256    10/10  65535/65535  9.6/9.6   n
% Util: 100/100
Owner: LOCAL  Restriction: NONE  COS: 0                     Status: Failed Test
Group: NONE  Priority: H  TestRTD: 0 msec

Path:     alpha   14--13beta    15--15gamma
Pref:     alpha   14--13beta    15--15gamma


alpha 9.1.100                                       gamma 8.1.200
FRP:   OK                                           FRP:   OK
FRI:   OK                                           FRI:   OK


Last Command: tstdelay 9.1.100

Test delay timed out
Next Command:
```

Example 2

tstdelay 9.1.1.1

Description

Test the delay on ATM connection 9.1.1.1. The first prompt that follows initial command entry is for whether the ForeSight RTD should be included. The second prompt is for confirming that the test should proceed.

System Response

```
bpx1           TN    SuperUser       BPX 8620    9.2       Aug. 31 1998 13:45 PST

Conn:  9.1.1.1         ]bpx6        11.1.1.1          abr      Status: OK
    SCR           MBS           MCR          ABR PCR     UPC FST CLP  % util
 4000/4000     1000/1000     4000/4000     4000/4000      y   y   y  100/100
Owner: REMOTE  Restriction: NONE  COS: 0
Group: NONE  ForeSightRTD: 40 msec  TestRTD: 10 msec

Path:   bpx1     1.3-- 3.3bpx6
Pref:   Not Configured


bpx1          ASI-T3    : OK           bpx6      ASI-T3    : OK
              Line  9.1 : OK                     Line 11.1 : OK
              OAM Cell RX: Clear


Last Command: tstdelay 9.1.1.1 n


Round trip delay is 10 msec.
Next Command:
```

Table 14-74 tsdelay—Parameters

Parameter	Description
channel	Specifies the channel of the connection to be tested. It can be a Frame Relay connection specified as slot. port. DLCI or an ATM connection specified as slot.port.vpi.vci.

Table 14-75 tstfdelay—Optional Parameters

Parameter	Description
-nolp	No automatic loopback. This parameter applies to only local-remote loopbacks and is mandatory for testing a multi-segment connection in a tiered network.
repeat count	Specifies the number of times the test is to be repeated. The range is 1–50. If you do not specify a count, the test runs once.
ForeSight RTD (y/n)	Specifies that the ForeSight RTD is included and applies to ATM connections only.

tstpcs

The **tstpcs** command tests the data path for PCS ports for a selected module. The *port* parameter specifies the particular PCS module. The *port* parameter specifies an FRM-2 or FRP-2 physical port to which one of the PCS modules connects.

Upon command entry, each of the 11 ports for the PCS goes into a loop state. In this state, data goes to each port and loops back to the PCS module. Test frames go to a port and are checked for integrity when they return. The test frames also go out on the port.

During this test, any Frame Relay connection data received by the FRM-2 or FRP-2 destined for one of the ports is discarded. The other three Port Concentrator modules are unaffected. After the test, the port is returned to its previous configuration.

The PCS tests available RAM, and sets each of the 11 ports into a loop mode. Ten frames of data are sent to each port and checked to make sure the same frames are received in entirety and order.

During a test, the **dsppcs** screen shows “Testing” then either “Passed” or “Failed.” The test takes about 15 seconds.

Full Name

Test Port Concentrator Shelf

Syntax

tstpcs <slot.port>

Related Commands

dsppcs, resetpc

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Table 14-76 tstpcs–Parameters

Parameter	Description
slot.port	*Slot* is the location of an FRM-2 or FRP-2 card. *Port* selects the physical port to which a PCS module connects. The range for port is 1–4.

tstport

Executes a port loopback test on the specified data port. Using **tstport** without the optional parameter performs an internal test. The loopback for the internal test is performed on the IPX or IGX back card and is used to test just the IPX or IGX front and back cards. The test disables the communications for that port and the back card is placed into a loopback mode. The applicable card sets for the **tstport** command are the FRP, FRM, SDP, HDM, LDP, and LDM. The card under test sends several frames of data to the port on the interface card, loops them back, and checks their integrity.

If connections exist on the port being tested, the **dspcons** screen appears. If no connections are present, the **dspfrport** screen appears. A flashing 'T' in the connections screen indicates those connections affected by the test. Either a "(" character or a ")" character indicates the loopback in the **dspfrport**. If a local or remote test fails, the port itself is automatically tested (internal) to determine if the IPX or IGX node caused the failure. The following are example command lines:

tstport 5.3	internal loopback port test—this is the default loopback
tstport 5.3 n	near external port loopback test
tstport 5.3 f	far external port loopback test.

For a Frame Relay port or an LDP or LDM port, an external loopback may be placed at the near (local) or far (remote) modem during the test. For a DDS port, the external loopback is a CSU or DSU loopback at the remote DSU device. If an external port loopback test fails, the internal port loopback test is executed to determine if the IPX or IGX node caused the failure. The **cnfict** command can be used to specify the interface control lead template used to condition the output control leads during loopback.

The local and remote modem tests that test the near end and far end modems or NTUs require the IPX or IGX back card to operate as a DTE, so the modem acts as a DCE in this case. The back card asserts the local or remote loopback pin of the V.35 port. For X.21 ports, which do not have a loopback pin defined, the back card sends a loopback command in the data stream to cause the NTU to go into loopback mode. The test then begins.

The loopback test operation sends several frames of test data, receives them back, compares them, and verifies their integrity. The loopback pin subsequently returns to the inactive state, and the modems return to normal operation. The local or remote test works with only those modems that recognize a local and remote loopback command.

Before starting a test, the user must be sure the cabling is correct for the specific equipment. The test conventions are described in CCITT V.54 and X.21 specifications. Only the near (n) and far (f) options are available for the Model C SDP. If the near or far tests fail, no internal test is executed on the SDP to isolate the problem. The SDP is not failed due to a **tstport** failure.

Full Name

Test port

Syntax

tstport <slot.port> [n | f]

Related Commands

cnfict, dspcons, dspfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IGX	Yes

Example 1

tstport 9.1

Description

Perform an internal port test on a Frame Relay port.

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Aug. 23 1998 11:27 PST

Conn: 9.1.100    gamma       8.1.200     fr
   MIR       CIR    VC Q Depth      PIR      Cmax   ECN QThresh    QIR    FST
 9.6/9.6   9.6/9.6      5/5       256/256    10/10  65535/65535  9.6/9.6   n
% Util: 100/100
Owner: LOCAL  Restriction: NONE  COS: 0                     Status: Failed Test
Group: NONE  Priority: H  TestRTD: 0 msec

Path:     alpha   14--13beta    15--15gamma
Pref:     alpha   14--13beta    15--15gamma


alpha 9.1.100                                    gamma 8.1.200
FRP:   OK                                        FRP:   OK
FRI:   OK                                        FRI:   OK


Last Command: tstport 9.1

No external clock is detected for DTE
Next Command:
```

Example 2

tstport 32.1 n

Description

Perform a local (near end) loopback test on port 32.1 (requires port to be configured as DTE).

Example 3

tstport 32.1 f

Description

Perform a remote (far end) loopback test on port 32.1 (requires port to be configured as DTE).

Example 4

```
tstport 9.1
```

Description

Perform a test of an FRP port.

Access Device Commands on a Node

This chapter describes the commands that apply specifically to the Cisco access devices (such as the Cisco 3801). The commands in this chapter apply to the trunk between the FTC or FTM card set in an IGX node and an access device.

The contents in this chapter are as follows:

- Introduction
- Descriptions of access device procedures
- Descriptions of access device commands

In addition to commands that are unique to the Cisco access devices, a larger number of commands are common to the Cisco access devices and the FastPAD series of access devices. The descriptions for these common commands appear in the chapter titled "FastPAD Connections."

The commands you enter at the terminal attached to the access device itself are IOS commands. Refer to the documentation for the access device for descriptions of the IOS commands.

Introduction

This chapter describes the commands that apply to an access device. When you use other, common commands such as **addcon**, **dspcon**, **cnfchutl**, and so on, use the following syntax to, for example, specify the access device when adding a connection:

addcon *slot.port.connection_ID*,

where *slot.port.connection_ID* is the slot and port number of the FTC or FTM and *connection_ID* is the connection identifier.

Summary of Commands

Table 15-1 shows the name and starting page for the description of each command.

Table 15-1 Access Device Commands

addad

Adds an access device to a node.

Full Name

Add access device

Syntax

addad <slot.port> <access_device_ID> <DLCI> [IP address] [number of mask bits]

Related Commands

dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Example 1

addad 12.3 3 990 0

Description

Add an access device at slot 12, port 3. The access device ID is 3. The DLCI is 990.

System Response

```
duvel          TRM   SuperUser       IGX 8420    9.2 Mar. 28 1998 08:19 GMT
                        Access Devices Information
 Slot.Port Name       ID DLCI Type    Alarm IP Address
   12.1                7   990              UNREACHABLE
   12.3     sbrin02    3   990  3800        OK 192.168.6.162/24
Last Command: dspads
This Command: addad 12.2 4 990
Enter Cong Mgmt. Timer (0=Disabled or 4-350 in 10ms units): 0






Last Command: addad 12.3 3 990



Next Command:
```

Table 15-2 addad—Parameters

Parameter	Description
slot.port	Specifies the slot and port number of the trunk to add.
access_device_ID	Device ID of the access device. The range for the ID is 0–255.
DLCI	The available range is 16–1007.

Table 15-3 addad–Optional Parameters

Parameter	Description
IP address	The IP address of the access device is optional. If you enter an IP address, it overrides the IP address that currently exists on the access device.
number of mask bits	The number of bits in the IP subnet mask.

addcon

Adds a connection between an access device and another endpoint. You add connections between the following endpoints:

- UVM and FTM/FTC
- FTM/FTC and FTM/FTC
- FTM/FTC and FRM/FRP
- CVM/CDP and FTM/FTC

Note that, if one end of the connection is a CVM or CDP, you must add the connection at the CVM/CDP.

Three connection types are possible for an access device. After you have specified the local and remote connection identifiers, the interface prompts you for a connection type. The type depends on the endpoint cards, as follows:

- For UVM and FTM/FTC endpoints, the connection type is "voice."
- For FTM/FTC and FTM/FTC endpoints, the connection type is "session."
- For FTM/FTC and FRM/FRP endpoints, you specify the type as a Frame Relay class.
- For CVM/CDP and FTM/FTC endpoints, the connection type is "voice."

Full Name

Add a connection

Syntax

The syntax depends on the endpoint cards.

UVM to FTM/FTC:

addcon <slot.line.channel> <node> <slot.port>.<Access Device ID>.<Connection ID> <Algorithm = a32 | c32 | g729r8 | g729r8v | g729ar8 | g729ar8v>

FTM/FTC to FTM/FTC:

addcon <slot.port>.<Access Device ID>.<Connection ID> <remote node> <slot.port>.<Access Device ID>.<Connection ID>

FTM/FTC to FRM/FRP:

addcon <slot.port>.<Access Device ID>.<Connection ID> <remote node> <slot.port>.<DLCI>

CVM/CDP to FTM/FTC:

addcon <slot.port> <remote node> <slot.port>.<Access Device ID>.<Connection ID>[compression algorithm]

Related Commands

dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Example 1

addcon 4.3.5.31 sw25 4.1.5.31

Description

Add a local connection from 4.3.5.31 to 4.1.5.31. The access device ID is 5, the connection ID is 31.

System Response

```
sw25           TN    SuperUser       IGX 8410     9.2 May  26 1998 00:26 GMT

 From           Remote      Remote
 4.3.31         NodeName    Channel         State  Type      Compress  Code COS
 4.3.31         sw25        4.1.31          Ok     session
 4.3.32         sw25        4.1.32          Ok     fst
 4.3.33         sw25        4.1.33          Ok     fst









This Command: addcon 4.3.5.31 sw25 4.1.5.31 session


Add these connections (y/n)?
```

Table 15-4 addcon—Parameters

Parameter	Description
slot.port	Specifies the slot and port number of the trunk to add. (FTM/FRM)
slot.line.channel	Specifies the slot, line, and channel number of the trunk to add. (UVM/CVM)
access device_ID	Specifies the access device ID number. The range for the access device_ID is 1–255.Access devices on the same trunk are assigned in increasing order.
connection_ID	Specifies a connection identifier. The range for the connection_ID is 1–252.
DLCI (only for FRP or FRM endpoints)	The available range is 16–1007.

Table 15-5 addcon—Optional Parameters

Parameter	Description
compression algorithm	The optional compression algorithm can be one of the following: • a16 • a24 • a32 • g729r8 • g729r8v • g729ar8 • g729ar8v

cnfadcmtmr

Configures the congestion management timer. The timer is applicable only if ForeSight is active.

The configuration management timer specifies how often rate-adjustment messages are passed between the FTC or FTM and the access device. This timer mechanism lets the congestion management provided by ForeSight extend to access devices. If you enter a 0 for the value, the interface card and device do not exchange rate adjustment messages.

Full Name

Configure access device congestion management timer

Syntax

cnfadcmtmr <slot.port> <Cong. Mgmt. Timer>

Related Commands

addad, dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	IPX, IGX	Yes

Example 1

cnfadcmtmr 4.3 350

Description

Configure the congestion management timer for port 3 of the card in slot 4 for 350 milliseconds.

System Response

```
sw25           TN    SuperUser       IGX 8410     9.2 Apr. 1 1998 11:17 GMT



   FrontCard  BackCard
   Type  Rev  Type     Rev  Status
1  NPC   BFF                Active
2  Empty reserved for NPC
3  CDP   BFC  E1       AD   Active
4  FTC   CF15 FPC-V35  AA   Active
5  AIT   AJF  AIT-T3   AE   Active
6  NTC   EUJ  E1       AN   Active
7  Empty
8  FTC   BHJ  FPC-V35  AA   Standby




This Command: cnfadcmtmr 4.3


Enter Cong Mgmt. Timer (0=Disabld or 40-350 in 10ms units): 350
```

Table 15-6 cnfadcmtmr—Parameters

Parameter	Description
slot.port	Specifies the slot and port number.
Cong. Mgmt. Timer	The setting for the timer. The number you enter is actually a multiplier for the base of 10 milliseconds, so the granularity is automatically 10 milliseconds. The range for the multiplier is 4–350, so the range for the timer is 40–3500 milliseconds. The default (no user-input) is 100 ms. To disable the timer, enter a 0.

cnfadcon

Configures bandwidth parameters for the trunk connection between an access device and the FTC or FTM. The parameters for **cnfadcon** are bi-directional. (Type a slash between the parameter for each direction.) The first parameter is from the node to the access device. The second parameter is from the access device to the node. An asterisk (*) indicates that the value is to remain unchanged for that direction. The only parameter that is not bi-directional is FST (ForeSight enable = “y” or “n”).

The command line interface does not prompt for individual bandwidth parameters. Therefore, refer to the **cnfadcon** options table to see the order in which you type the parameters.

Full Name

Configure access device connection

Syntax

cnfadcon <slot.port> <bw_parameters>

Related Commands

dspcon, cnffrcon, cnfcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Example 1

cnfadcon 4.2 76.8/76.8

Description

Configure the device trunk at port 2 of the card in slot 4 to have MIR (and so on) of 76.8 Kbps.

System Response

```
sw25           TN    SuperUser       IGX 8410     9.2 Apr. 2 1998  18:44 GMT

Conn:  4.2.100        ]  sw25        4.3.101           session      76 Kbps
                                                               Status:OK
   MIR       CIR     VC Q Depth       PIR      Cmax     ECN QThresh      QIR
76.8/76.8 76.8/76.8   600/600      76.8/76.8    1/1       300/300     76.8/76.8
Priority: H                         TestRTD: 0 msec    FST: n  % Util: 100/100


Path:   Route information not applicable for local connections




sw25      FTC:   OK                    sw25      FTC:   OK
          FPC:   OK                              FPC:   OK
          Access Device: OK                      Access Device: OK

Last Command: cnfadcon 4.2.100 76.8/76.8


Next Command:
```

Table 15-7 cnfadcon—Parameters

Parameter	Description
slot.port	Specifies the slot and port on an FTC/ FTM for an access device connection.

Table 15-7 cnfadcon—Parameters

Parameter	Description
bw_parameters	The bandwidth parameters are as follows: • **MIR/MIR** is defined as fr_MIR_Tx /fr_MIR_Rx, where fr_MIR is the minimum information rate for a connection. The range is 2.4 Kbps–2048 Kbps. • **CIR/CIR** is defined as fr_CIR_Tx and fr_CIR_Rx, where fr_CIR is defined as the committed information rate guaranteed to the user. The CIR range is 2.4 Kbps–2048 Kbps. • **VC_Q/VC_Q** is defined as fr_vc_q_Tx/fr_vc_q_Rx, where fr_vc_q Tx is the maximum transmit VC queue depth. The VC_Q range is 1–65535 bytes. (An alternative to this parameter is possible, as the description of *Bc* shows.) or **Bc/Bc** is defined as fr_Bc_Tx /fr_Bc_Rx. Bc has meaning for only ForeSight connections. If you have selected Frame Relay Forum standard parameters (through the **cnfsysparm** command), the Committed Burst (Bc) parameter appears instead of VC_Q. Bc is the amount of data the network can accept over a variable time interval (Tc) for committed delivery on a specific PVC. The range for Bc is 1–65535 bytes. The relationship between Bc and VC_Q is: Bc = VC_Q / ((1 – (CIR/port speed)) • **PIR/PIR** is defined as fr_PIR_Tx /fr_PIR_Rx, where fr_PIR_Tx is the peak transmit rate for the PVC. The PIR range is 2.4–2048 Kbps. You can also specify the value 0 to cause PIR to default to the port speed. Thus, you can modify PIR, leave it the same, or set it to the port speed. (An alternative specification for this parameter is possible, as the description of *Be* shows.) or **Be/Be** is defined as fr_Be_Tx /fr_Be_Rx. If you have selected Frame Relay Forum standard parameters (through the **cnfsysparm** command), the PVC uses Excess Burst (Be) instead of PIR. Be is the *amount* of transmit/receive data above the number of bytes set by Bc if enough bandwidth is available. Specify Be in bytes within the range 1–65535. Delivery of Be-data is not guaranteed. Be has meaning to only ForeSight. The relationship between Be and PIR is: Be = Bc * ((PIR/CIR) – 1) • **Cmax/Cmax** is defined as fr_cmax_Tx /fr_cmax_Rx, where cmax is the maximum credits the connection can accrue. The Cmax range is 1–255 packets per second (pps). • **ECNQ_thresh/ECNQ_thresh** are the transmit and receive threshold settings for the explicit congestion notification control queues. The range for ECNQ_thresh is 1–65535 bytes. • **QIR/QIR** is defined as fr_QIR_Tx /fr_QIR_Rx, where fr_QIR is the quiescent information rate for a connection, which is the initial transmit rate after a period of inactivity on the channel. If you do not specify the quiescent receive rate fr_QIR_Rx, the system sets it to the transmit value. The values are specified in Kbps and must be in the range MIR–PIR. In addition, you can specify the value 0 to default to the MIR. QIR has meaning for only ForeSight connections. • **FST** enables or disables (purchased) ForeSight option for a connection. Valid entries are "y" (use ForeSight) or "n" (do not use ForeSight). If the ForeSight status changes, the network reroutes the connection.

delad

Deletes an access device from a node. Before you can delete an access device, you must remove all connections from the device by using the **delcon** command.

Full Name

Delete access device

Syntax

delad <slot.port>

Related Commands

addad, dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	Yes	IPX, IGX	Yes

Example 1

delad 31.1

Description

Delete the access device at 31.1.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2 Date/Time Not Set

Access Device Information

 Slot.Port  Name       ID      DLCI     Port_ID  Alarm

   31.1     ad1         1       17        0      OK
   31.2     ad2         2       18        0      OK
   31.3     ad3         3       19        0      OK
   31.4     ad4         4       20        0      OK







This Command: delad 31.1


Delete access device (y/n)?
```

Table 15-8 delad—Parameters

Parameter	Description
slot.port	Specifies the slot and port number.

dspads

Displays all access devices in the node. The **dspads** command takes no parameters. The displayed information consists of the following:

- The IPX or IGX slot and port that connect to each access device
- The name of the access device
- The access device ID number of the channel between the interface card and the device. Multiple access devices on the same channel are displayed in increasing order.
- The DLCI of the device
- The type of access device (such as a Cisco 3810), as reported by the device
- The alarm status (which can be OK, init.., or failed)
- The setting for the Congestion Management Timer (in 10-millisecond multiples, 0 if the CMT is disabled)
- The IP address of the device and the number of bits in the subnet mask

---

Note If an access device name and IP address are not relevant, such as when an FTC/FTM port loopback is simulating access devices, blank spaces appear in the "Name," "Type," and "IP Address" fields of the display.

Full Name

Display (all) access devices

Syntax

dspads

Related Commands

addad, delad, cnfadcmtmr

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Example 1

`dspads`

Description

Display all the access devices in the current node.

System Response

```
sw25          TN    SuperUser       IGX 8410     9.2 Apr. 1 1998  13:12 GMT

                        Access Devices Information

 Slot.Port  Name       ID  DLCI  Type        Alarm       CMT  IP Address

    4.2                 8   990              OK            0
    4.3     sbrin01     4   990  3800        OK           91  192.168.6.161/24








Last Command: dspads


Next Command:
```

dspcon

Displays connection information for a connection. The information displayed includes:

- The channel number at both the local and remote ends of the connection
- The node name at both ends of the connection
- The type or data rate of the connection
- The connection priority (low or high)
- The preferred route for the connection (if configured)
- The status of the front and back cards and access devices associated with the connection
- Any Y-cable conflicts (LDI, CDP for example)
- If one endpoint is a CDP or CVM, the compression status (VAD on or off, ADPCM on or off
- The bandwidth parameters for the connection
- The ForeSight enable status
- The percent of utilization
- The connection descriptor (if configured)
- The circuit round trip delay (RTD) if ForeSight is enabled

A failure that affects the connection flashes on the screen. The possible status messages are:

- OK Connection OK.
- FAILED Connection failed.

Full Name

Display connections

Syntax

dspcon <channel>

Related Commands

addcon, cnfcondsc, cnfcos, cnfpref, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX	No

Example 1

`dspcon 4.1.33`

Description

Display connection information for Frame Relay channel 4.1.33.

System Response

```
sw25          TN    SuperUser      IGX 8410      9.2 May 25 1998 23:07 GMT

Conn:  4.1.33            sw25        4.3.33             fst
                                                                Status:OK
    MIR         CIR      VC Q Depth     PIR      Cmax   ECN QThresh     QIR
   56/56       56/56    65535/65535   512/512    10/10  65535/65535   128/128
Priority: L  ForeSightRTD: 40 msec  TestRTD: 0 msec    FST: y  % Util: 100/100


Path:   Route information not applicable for local connections




sw25      FTC:   OK                    sw25      FTC:   OK
          FPC:   OK                              FPC:   OK
          Access Device: OK                      Access Device: OK

Last Command: dspcon 4.1.33


Next Command:
```

Table 15-9 dspcon–Parameters

Parameter	Description
channel	Specifies the channel in the format *slot.port.connection_ID*. The range for *connection_ID* is 1–252. The **dspcon** command displays information for one connection at a time.

dspcons

Displays a summary of the connections on an IPX or IGX node. Table 15-10 shows the fields displayed in the **dspcons** screens.

Table 15-10 Information in the dspcons Display

Field	Description
Local Channel	The connection’s channel at this node.
Remote Node Name	The name of the node at the other end of the connection.
Remote Channel	The connection’s channel at the remote node.
State	The state of the connection(s) as follows: • OK Routed • Down Downed • OK Downed Waiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command. • Failed Unrouted, but trying
Type	The type of connection (v = voice, d = data, fr = Frame Relay, atfr = ATM to Frame Relay interworking, atfst = ATM to Frame Relay interworking with ForeSight, -fail = failed connections; data rate in kbps for data)
Route Avoid	The type of lines to avoid when routing (satellite lines, terrestrial lines, lines with zero code suppression).
Compression	The type of compression applied to the connection (PCM, PCM and VAD, ADPCM, VAD and ADPCM for voice connections), (DFM for data connections).
COS	The Class of Service.
Owner	The end of the connection in control of re-routing.
Descriptor	The connection descriptor string (if +d option specified).
Loopback	A connection with a local loopback is indicated by a right parenthesis symbol between the “Local Channel” and “Remote NodeName” columns. A Frame Relay connection with a port loopback is indicated by a right bracket symbol between the “Local Channel” and “Remote NodeName” columns. A connection with a remote loopback is indicated by a right parenthesis symbol before the channel number in the “Remote Channel” column.
Local/Remote A-bit	Abit status on the local and remote nodes if -abit option selected. Note that -abit is incompatible with -v, -d, and +d.

Full Name

Display connections

Syntax

dspcons [start_channel] [nodename] [state] [type]
[-g | +d | -v | -d | -f | -abit | -fabit | -atfr | -siw | -fail | -down]]

Related Commands

addcon, cnfchadv, chfchdfm, cnfcondsc

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX, IGX	No

Example 1

dspcons

Description

Display a summary of all connections.

System Response

```
sw25           TN    SuperUser       IGX 84208     9.2 May  25 1998 23:29 GMT

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type      Compress  Code COS
 4.1.32         sw25        4.3.32          Ok     fst
 4.1.33         sw25        4.3.33          Ok     fst
 4.3.32         sw25        4.1.32          Ok     fst
 4.3.33         sw25        4.1.33          Ok     fst







Last Command: dspcons


Next Command:
```

Table 15-11 dspcons—Optional Parameters

Parameter	Description
start channel	Specifies the channel to begin the display. The start channel on a CDP or CVM is specified as *slot.channel*.The start channel on a UVM is *slot.line.channel*.
node name	Specifies that only connections to this remote node from the local note be displayed. If no "nodename" is designated, connections from the local node to all other nodes are displayed.

Table 15-11 dspcons—Optional Parameters (Continued)

Parameter	Description
connection type	Specifies that only connections of a certain type be displayed. If you do not add at least one argument to specify a particular connection type, all connections appear. When you enter the connection type on the command line, precede it with a hyphen (-). In some cases, you can add more than one connection type (with a space between), but not all compound arguments are compatible, so you may not always see the expected combination of types. The connection types are: -v displays only voice connections. -d displays only data connections. -f displays only Frame Relay connections. -abit shows A-bit (nni) status. -fabit shows connections with failed A-bit (nni) status. -fail shows only failed connections -g shows only grouped connections -siw shows service interworking connections. -atfr shows only network interworking connections.
+d	Causes the display to show the user-configured descriptor for the connection instead of the compression and ownership fields.

resetad

Directs an access device to reset itself from a node terminal. The reset initiated by **resetad** is a cold-boot start of the access device. (The **restartad** command re-initiates the control session between the node and the access device.)

Full Name

Reset access device

Syntax

resetad <slot.port>.<Access Device ID>

Related Commands

restartad, dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1–3	Yes	Yes	IPX, IGX	Yes

Table 15-12 resetad—Parameters

Parameter	Description
slot.port	Specifies the slot and port number that connects to the access device.
access device_ID	Specifies the access device ID number. The range for the access device_ID is 1–255. Access devices on the same trunk are assigned in increasing order.

restartad

Restarts an access device session from a node's command terminal. The **restartad** command restarts the control session of an access device on an IGX node. A control session is first established when the following conditions are true:

1. You add an access device to the node with **addad**.
2. The port speed and other parameters on the device and the port match.

Once a control session is established, you can configure and manage the access device by commands you issue at the node. These commands are the access device commands in this chapter and the other, common commands in this manual.

The **restartad** command does not perform a hard reset of the access device itself. See **resetad** regarding a hard reset of the access device.

Full Name

Restart access device

Syntax

restartad <slot.port>.<Access Device ID>

Related Commands

resetad, dspads

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX, IGX	Yes

Table 15-13 restartad–Parameters

Parameter	Description
slot.port	Specifies the slot and port number.
access device_ID	Specifies the access device ID number. The range for the access device_ID is 1–255. Access devices on the same trunk are assigned in increasing order.

FastPAD Commands

Introduction to FastPAD Commands

The FastPAD commands are a set of commands that let you configure a FastPAD multiplexer for interconnection through your IPX network. FastPADs are interconnected by IPX Frame Relay Service PVCs. FastPAD/IPX interconnection requires you to use an FTC front card and FTI back card on the IPX. The FastPAD is connected to the FTI card installed in the IPX. The FRP/FRI cards provide the adaptation layer to convert data between Frame Relay format and IPX FastPacket format. In addition, because the Frame Relay/FastPAD connectivity is an option, you must enable this option for your system software.

The FastPAD acts as a feeder into the IPX. The FastPAD encapsulates this traffic into FastPAD type frames and transmits it over Frame Relay PVCs. These PVCs are transmitted over a FastPAD trunk that feeds into an IPX Frame Relay port on an FTC/FTI card set. FastPAD connections are mapped to Frame Relay virtual circuits within the IPX, switched to the remote IPX, and delivered to the remote FastPAD.

There are five types of FastPAD connections: switched voice connections, permanent voice connections, data connections, Frame Relay connections, and frame forwarding connections. FAX connections are not a separate connection type. They are transmitted over switched voice or voice connections. When a FAX connection is required, the FastPAD automatically detects the FAX transmission and suppresses the use of any voice compression algorithms. A voice, data, or FAX connection from one FastPAD must always terminate on another FastPAD. Frame relay and frame forwarding traffic may be terminated on another FastPAD or on an FRP in an IPX.

The FastPAD connects to an IPX through an FTC/FTI card set on the IPX, where the FTC is the front card and the FTI is the back card. There are four types of FTI back cards: V.35, X.21, T1, and E1.

You perform the initial FastPAD configuration at the FastPAD with either the StrataView FastPAD, FastPAD FP Tools, or by replacing the FastPAD FlashPak. Following this, you perform the FastPAD composite link (to the IPX) configuration and connection configuration by using the IPX commands described in this appendix.

FastPAD Description Summary

The FastPAD always contains a base card and can also contain expansion cards. The base card is designated “b”, while the expansion cards are designated 1–5 for the FastPAD Micro and 1–8 on the standard FastPAD. The expansion ports can contain either Voice FAX Cards (VFC-03) or Frame Relay Access Modules (FRAM-01).

The base card on the FastPAD Micro supports a composite port for connecting to the IPX, one high-speed data port, one low-speed data port, and an NMS port (for a PC running the StrataView FastPAD NMS application). The base card on the standard FastPAD supports a composite port for connecting to the IPX, one high-speed data port, five low-speed data ports, and an NMS port (Figure 16-1). When adding connections to the FastPAD base card ports, use the letter “b” for slot designation. When adding connections to the FastPAD expansion cards, use a number 1 through 8, as applicable.

Voice connections are supported by adding VFC-03 cards. Each VFC-03 card gives you the choice of connecting to either a RJ45 or RJ11 connector. On the VFC-03, there are three available modes selectable by software: Off Premise Extension (OPX), Single Line Telephone (SLT), and E & M. The VFC-03 supports Adaptive Transform Coding (ATC) voice compression algorithm. The VFC-03 supports other voice compression algorithms, for example, CELP. You cannot install the VFC-01 in the same chassis as the VFC-03, and you must manually switch its operating mode between OPX, SLT, and E & M.

The Frame Relay Access Module (FRAM-01) provides three high-speed data ports in addition to the one on the base circuit card. The FRAM has a single DB-68 connector that can be converted to three DB-25 connectors through the use of an adapter cable.

There can be multiple FRAMs, however you can configure only one for a Frame Relay switch. The others can only be used for data connections. On the FRAM used for Frame Relay connections, you can configure one port for a composite port, and configure the other two ports to interface to CPE such as routers with Frame Relay interfaces, for example (see Figure 16-2). One of the ports on the FRAM is used for a composite port because the baseboard composite port data rate is considerably slower. If a FRAM port is defined as the composite port (line interface to the IPX), the base board composite port (line) is disabled.

Figure 16-1 FastPAD Connection Configurations except Frame Relay

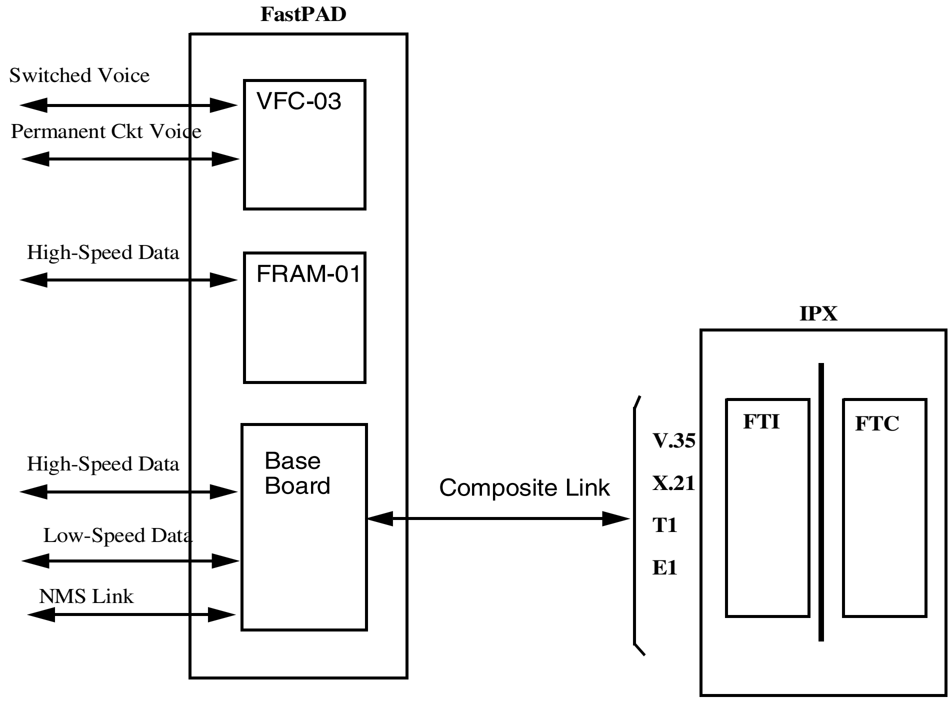
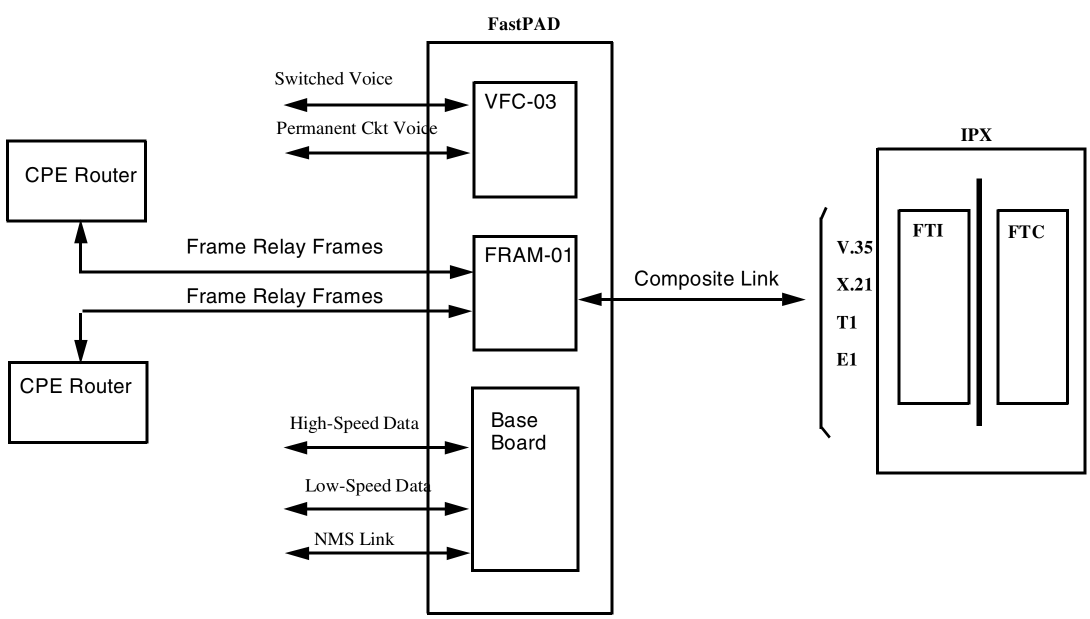


Figure 16-2 FastPAD Connection Configurations including Frame Relay



Configuration Summary

In setting up FastPAD connections across a network, you must perform a number of tasks. These include the following:

- Install the FTC card.
- Set up Frame Relay parameters for the composite link between the FTC and the FastPAD.
- Configure the V.35 and X.21 ports, as necessary.
- Up and configure the T1/E1 ports, as necessary.
- Configure the composite link between the IPX and the FastPAD.
- Add the FastPAD to the local IPX node.
- Set up the appropriate connections: switched voice, permanent voice, CELP voice, low-speed data, high-speed data, Frame Relay, or frame forwarding.
- Manage the bandwidth requirements.

General Considerations

Y-Cable Redundancy

The Y cable redundancy feature is supported for the FTC card, using the **addyred**, **delyred**, **dspyred** and **prtyred** commands. See the Node Commands chapter for details on setting up redundancy. The FTC/FTI card set supports V.35, X.21, T1, and E1 ports through the use of the corresponding four different FTI back cards

Managing FTC T1 and E1 Ports

Logical Frame Relay ports are collections of DS0 time slots that function as a port. They support up to 252 connections. The LMI signaling protocol is simultaneously supported on a maximum of 30 logical ports.

You use the **addftcport** and **delftcport** commands to create/delete logical ports. The **addftcport** command associates a line number and DS0 time slot to a logical port. Any number of contiguous DS0 time slots are optionally associated to form a logical port with the restriction of channel 16, which is used for signaling for E1. Logical ports are formed with DS0 time slots configured for either 56 or 64 Kbps. You can use the **cnfftcport** command to configure the port.

Managing Lines for FTC T1 and E1 Lines

FTC circuit line operations are included in the commands **upln, upcln, dnln,** and **dncln**. An FTI line can be configured as a network clock source with the command **cnfclksrc**.

Unassigned Channel Signaling

Unassigned channel signals are transmitted on a channel that is not mapped to a logical port. Data code values axon and TX apply to the T1 and E1 channels. signaling values 1111 and 1101 apply to T1/E1 ABCD signaling channels.

IGX/IPX and FastPAD Control Setup

The FastPAD can be monitored and managed by the IPX or the IGX through a control connection. This connection is a Frame Relay PVC connection between the CC on the IPX and the configuration application on the FastPAD. To configure the control connection:

1. Use the **dspftcport** command to display the FTC port parameters. Verify that the parameters of the FTC port (speed, clocking, port queue depth, ECN queue depth, and update protocol ID) match those of the FastPAD trunk port.
2. Use the **addfp** command to add a FastPAD to the local IPX or IGX node. With this command, specify the slot and port of the FTC or FTM card connected to the FastPAD, a name for the FastPAD, FastPAD ID, and the source DLCI (used to communicate with the FastPAD).

Initial Setup of FTM or FTC card and FastPAD Link

This section describes the steps for setting up the FTC card and FastPAD link.

1. Activate the FTC or FTM port providing the link to the FastPAD.

   The ports on the FTC or FTM card for V.35 and X.21 interfaces are upped automatically. The ports for T1 and E1 cards must be added using the **addftcport** command. The T1 and E1 ports are configured for logical channels by specifying groups of DS0s. If the port is not up, use the **upftcport** command to up it.

2. Configure an FTC or FTM port with the **cnfftcport** command. If the port is not up, use the **upftcport** command to up it. For Release 8.1 and above, the **cnfftcport** command includes the DE threshold. For Release 9.2 and above, the number of FastPADs and access devices per FTM/FTC card is increased from 31 to 63. Note, however, that each FTM/FTC card is still limited to 252 connections, which averages to four connections per device for an FTM/FTC with 63 access devices attached to it.

   There are two separate sets of syntax parameters, one for all ports except T1/E1 ports and the other for T1/E1 ports. In summary these are:

   For non-T1/E1 ports (for example, V.35, X.21)

   ```
   cnfftcport FTC_slot.port speed port_type  port_ID  port_Q_depth
              ecnq_thresh  DE_thresh signalling_protocol
   ```

   For T1/E1 ports, after adding the logical ports with the **addftcport** command, configure each port:

   ```
   cnfftcport FTC_slot.port   txq_depth  ecnq_depth  DE Threshold
               updt_prot_id
   ```

3. The next step is linking the FastPAD to the IPX or IGX. Once an FTC or FTM port has been configured, the FastPAD can be linked to the IGX or IPX using the **addfp** command:

   ```
   addfp FTC/FTM_slot.port name ID source_DLCI
   ```

   where `name` is up to eight characters to identify FastPAD, and ID must match the value entered at the FastPAD front panel (source DLCI = [S x 16] + P). Note that if an FTM or FTC card already has 64 devices attached to it, the **addfp** command will fail even if the port has no device attached to it. The command displays an error message.

Note Once communications have been established between the IGX or IPX and a FastPAD, the FastPAD is locked. The FastPAD may be unlocked with a power reset or reboot. Communications must be re-established after changes have been made locally on the FastPAD. This can be done with the **restartfp** command.

Line Management

The **upln** and **dnln** commands are used to bring the line up and down, respectively.

Feeder Management

1 Managing the FastPAD

   — The **dspfp** command displays the status of the cards in a FastPAD including expansion cards.

   — The **resetfp** command resets the FastPAD. This should be done with caution, as traffic is interrupted.

2 Configuring FastPAD Data Ports

   Two commands are used to configure FastPAD data ports. These are **cnfdclk** and **cnfict**. The **cnfdclk** command sets the data mode (transparent, H/SDLC, or asynchronous) and the clock mode (internal or external). **cnfict** allows limited control lead mapping from one data port to another.

Note The **cnfdclk** and **cnfict** commands are used to configure the parameters most often changed by the user. The SuperUser command **cnffpport** allows changing of all FastPAD data port parameters.

3 Configuring FastPAD Voice Ports and Channels

   Two commands are used to configure FastPAD voice ports and connections. These are **cnfvchtp** and **cnfchgn**. The **cnfvchtp** command defines interface type, signaling, SLT timeout period, and DTME detect timeout. The **cnfchgn** command configures the input gain and output gain values.

Note The **cnfvchtp** and **cnfchgn** commands are used to configure the parameters most often changed by the user. The SuperUser command **cnffpport** allows changing of all voice channel parameters.

4 Configuring and Displaying FastPAD Frame Relay Ports. Frame Relay connections can be made between a FastPAD and another FastPAD via FTCs over an IPX network, or between a FastPAD via an FTC over an IPX Network to an FRP termination on an IPX. FastPAD Frame Relay ports are configured on the FRAM-01 card. Typically, of the three ports on the FRAM-01 card, up to two may be connected to Frame Relay routers, and the third is used as the composite link to the IPX. Multiple FRAM-01 cards may be installed, but only one may be configured with Frame

Relay ports for Frame Relay connections. Applicable commands for configuring and displaying FastPAD Frame Relay ports on a FRAM-01 are: **cnffrport**, **dspfrport**, **upfrport**, and **dnfrport**. Their syntax is summarized in the following:

```
cnffrport FTC_slot.port.FP_slot.port [port_speed  rcv_clk_type
           xmt_clock_type  signalling_protocol  protocol_parameters
           data_coding

dspfrport  FTC_slot.port.FP_slot.port

upfrport   FTC_slot.port.FP_slot.port

dnpfrport  FTC_slot.port.FP_slot.port
```

Setting Up FastPAD Switched Voice Connections

Before two FastPADs can establish switched voice connections, they must be paired or associated to each other. Once paired, a PVC is created within the two FastPADs. Switched voice connections or sessions are established over this PVC. Each switched voice session does not have a dedicated PVC. Any FastPAD voice channel that has not been assigned a dedicated or permanent voice connection can be used for a switched voice connection. To set up a FastPAD switched voice connection:

1. First configure the voice channel at each FastPAD. The channel is expressed as FTC_slot.port where FTC_slot is the FTC card slot and port is the FTC port connected to the FastPAD. The configurable parameters and their associated commands are as follows:

cnfchgn	Configures the channel gain. This command allows the gain inserted in the receive and transmit directions to be adjusted to between -31 dB to +6 dB in 1 dB increments.
cnfchutl	Configures the channel utilization. See the Routing and Bandwidth commands chapter.
cnfvfpchtp	Configures the FastPAD voice channel interface type. This command configures the telecommunications interface type.

2. Use the **addcon** command.

Setting Up FastPAD CELP 8K or CELP 4.8K Voice Connections

Release 9.2 supports CELP-based voice connections that terminate on a pair of VCF03s and CELP-based switched voice connections between a pair of FastPADs. The compression type, for example, CELP 8k is not configurable from the IPX.

FastPAD Data Rate Summary

FastPAD Data Traffic

The base board low-speed data ports support the following:

- Asynchronous rates between 300 and 9600 bps
- Synchronous data rates between 1.2 and 19.2 kbps
- DCE RS-232 Interface

The base board high-speed data port supports the following:

- Synchronous data rates between 1.2 and 64 kbps
- DCE or DTE compatibility
- RS-232, RS-449, V.34, and V.11 interfaces

The optional FRAM high-speed ports support the following:

- Synchronous data rates between 1.2 and 512 kbps
- DCE or DTE compatibility
- RS-232, RS-449, V.35, and V.11 interfaces
- Frame Relay Traffic (one port used for connection to IPX, two used for connection to CPE)

Setting Up FastPAD Permanent Voice Connections

To set up a permanent FastPAD voice connection, you merely pair two FastPAD voice channels.

1 First configure the voice channel at each FastPAD. For permanent voice connections, the channel is expressed as FTC_slot.port.FP_slot, where FTC_ slot is the FTC card slot; port is the FTC port connected to the FastPAD; and FP_slot is the voice expansion card slot on the FastPAD. The configurable parameters and their associated commands are as follows:

cnfchgn	Configures the channel gain. This command allows the gain inserted in the receive and transmit directions to be adjusted to between -31 dB to +6 dB in 1 dB increments.
cnfchutl	Configures channel utilization. See the Routing and Bandwidth Commands chapter.
cnfvfpchtp	Configures the FastPAD voice channel interface type. This Command configures the telecommunications interface type.

2 Use the **addcon** command. The above configuration must have been completed at each end before the connection can be added.

Setting Up FastPAD Data Connections

To set up a permanent FastPAD data connection, perform the following tasks.

1 First configure the data channel at each FastPAD. The channel is expressed as FTC_slot.port.FP_slot.port, where FTC_slot is the FTC card slot; port is the FTC port connected to the FastPAD; FP_slot is the card slot on the FastPAD; and port is the data channel on the FastPAD card. The configurable parameters and their associated commands are as follows:

cnfcondsc	Configures the connection descriptor.
cnfdclk	Configures the clocking for the data channel.
cnfict	Configures the interface control template that determines the output lead behavior for data channels. Output leads can be configured as steady state (on or off) or can be programmed to follow an input lead. For the FastPAD, there is only one template–the active template.

cnfchutl Configures channel utilization. See the Routing and Bandwidth Commands chapter.

2 Use the **addcon** command. The above configuration must have been completed at each end before the connection can be added.

Setting Up Normal Frame Relay Connections

The FastPAD, in conjunction with the IPX, provides Frame Relay connections of CPE (routers, bridges, packet switches, etc.) via PVCs. The CPE is connected to the FRAM-01 card that supports Frame Relay. The FTI back card (V.35, X.21, T1, or E1) performs the adapter layer function to convert between the FastPAD special frame format and FastPackets.

The CPE transmits data to the FRAM-01 based upon the core functions of Q.922 (LAPD). The FastPAD scans the first two octets of the DLCI and forwards the frame to the destination CPE via the IPX.

For adding/deleting connections, the following commands are used:

- **addcon**
- **delcon**

1 Use the **addcon** command to add the desired Frame Relay connections to the FRAM-01 card, using the appropriate frame class and configuring the bandwidth parameters as applicable.

```
addcon  local_chan(s)  node  chan  class  [frp_bw  avoid]

chan(s) = FTC_slot.port.FP_slot.port.DLCI

frp_bw = MIR/MIR  VC-Q/VC_Q  PIR/PIR  Cmax/Cmax  ECNQ_thresh/ECNQ_thresh
         QIR/QIR  FST  %util/%util
```

Note These parameters have the same value options as defined for the **cnffrcls** command currently supported for FRP ports.

```
delcon  channel(s)

channels = FTC_slot.port.FP_slot.port.DLCI
```

2 For a large number of connections with similar bandwidth configuration, it may be useful to use the **cnffrcls** command to set up a class of Frame Relay bandwidth parameters applicable to these connections. See also **dspfrcls**.

Frame Forwarding Connections

Frame forwarding connections allow the connection of non-Frame Relay frames (HDLC and SDLC). Frame forwarding for FastPAD to FastPAD may be configured on either the FastPAD base card or FRAM-01 expansion card. However, for this release, frame forwarding from FastPAD to FRP is limited to the data ports on the FRAM-01 expansion card.

NOTE: The FTC port ID cannot be changed to a different value if a frame forwarded connection exists between the attached FastPAD and an FRP. This is because the FTC port ID is used as a unique identifier in the FTC card’s logical connection entry.

Managing Bandwidth

The following commands assist in managing bandwidth to achieve satisfactory traffic patterns.

cnfcos	Specifies a class of service (COS) for a data or voice channel. The COS is a number from 0 to 15 that determines the channel's priority for rerouting in a trunk fails.
cnfpref	Specifies preferred routing for intra-domain connections. This command can be used to assist in balancing the load on the network's trunks.
dsprts, prtrts	Displays/prints the current connection routing information. Used in conjunction with the **cnfpref** command. The display of the connection routes terminates at the IPX.
dncon, upcon	Temporarily downs/ups connections of a specified COS, thus releasing bandwidth for other services. Often it is possible to down some voice connections to provide more bandwidth for data and Frame Relay connections.

Monitoring Alarms and Statistics

1. Displaying Alarms. The **dspalms** command display includes failed connections and card failures. Line alarms are mapped to FTC port/FastPAD alarms. LMI failures show minor alarms on connections.
2. Statistics: For Release 9.1, FastPAD level statistics are not integrated in the IPX's statistics collections. The FTC card does collect statistics on the PVCs associated with the feeder channels within the IPX. The following statistics are available:

   Frames received and transmitted, packets received and transmitted, bytes received and transmitted, receive and transmit frames discarded, receive and transmit packets discarded, and receive and transmit bytes discarded.

   Applicable commands are: **cnfchstats**, **dspchstats**, **clrchstats**, **dspchstatscnf**, **dspchstathist**. The format is the same as in previous releases, except that the target Frame Relay port is specified as:

   ```
   FTC_slot.port.FP_slot.port.DLCI
   ```

General FastPAD Information

FastPAD Data Types

There are three data channel types and one Frame Relay Type on the FastPAD (see Table 16-1).

Table 16-1 Port and Channel Types

Port Type	Transparent	H/SDLC	Asynchronous	Frame Relay
Base-board low speed	Yes	Yes	Yes	No
Base-board high speed	Yes	Yes	No	No

Table 16-1 Port and Channel Types (Continued)

FRAM high speed	No	Yes	No	Yes

Transparent: The transparent mode is used for synchronous data applications. In order to reduce bandwidth utilization on the Composite Link, the FastPAD suppresses repeating patterns. After a synchronous data frame is built, the FastPAD searches for repeating patterns within the frame. The first occurrence of a repeating pattern of at least five in length is reduced to three octets and the smaller frame if sent out across the Composite Link. This process is called Run Length Compression (RLC).

H/SDLC: High-level Data Link Control (HDLC) and Synchronous Data Link Control (SDLC)_ are synchronous data protocols. SDLC is a subset of HDLC that was developed for use on SNA networks. The FastPAD recognizes HDLC frames and arranges them into 65 byte segments to be packetized into Frame Relay frames. All HDLC frames are separated by hexadecimal 7E flags. The FastPAD suppresses inter-HDLC frame idle flags to reduce utilization on the composite link.

Async: In asynchronous mode, the data channel protocol is preset to 8-bit characters with no parity and one stop bit, which cannot be changed. However, 7-bit protocols with parity can be used and the FastPAD forwards the parity bit as the eighth data bit. In order to reduce bandwidth use, frames are not generated during idle periods, and start and stop bits are not included in the frame. There is a configurable time period that the FastPAD waits to receive data from an asynchronous device before sending a frame that is 66 bytes long. This ensures propagation through the network with minimal delay.

Data Frame Format

The data traffic on the composite link of the FASTPAD is encapsulated into frames. FastPAD frames with synchronous data contain 65 data bytes, and frames with asynchronous data contain data bytes. Data frames may be shorter in some cases. Data frames may be marked as discard eligible.

The composite link can connect a FastPAD to a wide area network (for example, IPX) or to another FastPAD. The Frame Relay network can be either public or private.

The standard Frame Relay format is shown in Table 16-2. The standard Frame Relay format can be between 5 and 4096 bytes in length. There is at least one hex 7E lag between consecutive frames. On the composite link, the frame lengths used by the FastPAD can have up to 65 bytes of synchronous data, 66 bytes of asynchronous data, or between 5 and 4096 bytes of Frame Relay connection data.

Table 16-2 FastPAD Frame Format

0	1	1	1	1	1	1	0
DLCI (MSB)						C/R	EA (0)
DLCI (LSB)				FECN	BECN	DE	EA(1)
MUX							
CONTROL							

Table 16-2 FastPAD Frame Format (Continued)

.. User Data (ASYNC up to 66 bytes) Transparent & HDLC up to 65 bytes) . .							
CRC (MSB)							
CRC (LSB)							
0	1	1	1	1	1	1	0

Summary of Commands

The commands discussed in the previous sections are summarized in Table 16-3. The command name, a description, and the page on which more information can be found is included.

Table 16-3 Summary of Commands

Mnemonic	Description
addcon	Add Connection
addfp	Add FastPAD to IPX Node
addfpdial	Add FastPAD Speed Dial Number
addftcport	Add logical T1/E1 port link to FastPAD, using DS0 segments
addextlp	Add external loop. See the “Troubleshooting” chapter.
addrmtlp	Add remote loop. See the “Troubleshooting” chapter.
cnfchgn	Configure Gain Insertion for Channel(s)
cnfchpri	Configure FRP channel priority for a connection, supporting SNA applications
cnfchutl	Configure channel utilization for a channel. See the “Optimize Traffic Routing” chapter.
cnfcos	Configure class of service. Sets priority for rerouting a connection. See the “Optimize Traffic Routing” chapter.
cnfdclk	Configure Data Clock
cnffrcls	Configure frame class parameters for FastPAD to FastPAD or FastPAD to FRP Frame Relay connections via FRAM-01 card.
cnffrcon	Configure FastPAD to FastPAD or FastPAD to FRP Frame Relay connections via FRAM-01 card.
cnffrport	Configure Frame Port for FastPAD to FastPAD or FastPAD to FRP Frame Relay connections via FRAM-01 card.
cnfftcport	Configure FTC Port
cnfict	Configure Interface Control Template
cnfpref	Configures preferred route. See the “Optimize Traffic Routing” chapter.
cnfvchtp	Configure FastPAD Voice Channel Type
cpyict	Copy Interface Control Template
delcon	Delete Connection
delfp	Delete FastPAD from IPX or IGX Node
delftcport	Delete logical T1/E1 port
dncon	Down a connection. See the “Optimize Traffic Routing” chapter.
dnfrport	Down Frame Port on FRAM-01 for FastPAD to FastPAD or FastPAD to FRP Frame Relay connections, using syntax FTC_port.slot.FP_slot.port
dnftcport	Down FTC port for link to FastPAD composite port using syntax FTC_slot.port.
dnln	Down an FTC line
dspchcnf	Display Channel Configuration
dspcon	Display Connection
dspcons	Display Connections
dspfp	Display FastPAD Card Information
dspfps	Display Information for All FastPADs

Table 16-3 Summary of Commands (Continued)

Mnemonic	Description
dspfrcls	Display frame class parameters for FastPAD to FastPAD or FastPAD to FRP Frame Relay connections via FRAM-01 card.
dspfrport	Display Frame Port configuration on FastPAD FRAM-01.
dspftcport	Display FTC Port Configuration
dspict	Display Interface Control Template
dsprts	Displays routes used by connections at a node. See the "Optimize Traffic Routing" chapter.
prtchcnf	Print Channel Configuration
prtcons	Print connection(s)
prtict	Print Interface Control Template
resetfp	Reset FastPAD: do a cold boot and allow deletion of all PVCs.
restartfp	Restart FastPAD(s)
tstcon	Test Connection with a test pattern. See the "Troubleshooting" chapter.
tstdelay	Test round trip delay. See the "Troubleshooting" chapter.
tstport	Test Port, executing port loopback test. See the "Troubleshooting" chapter.
upcon	Up a connection that has been downed. See the "Optimize Traffic Routing" chapter.
upfrport	Up Frame Port on FRAM-01 for FastPAD to FastPAD or FastPAD to FRP Frame Relay connections, using syntax FTC_port.slot.FP_slot.port
upftcport	Up FTC port for link to FastPAD composite port using syntax FTC_slot.port.
upln	Up an FTC line.

addcon

Adds channel connections between entities in the network. The same command with differing syntax may be used to add voice connections, data connections, Frame Relay connections or FastPAD voice, switched voice, or data connections. This command establishes channel connections between entities in the network. This format of the command adds a FastPAD voice, switched voice or data connection. The same command with differing syntax can be used to add different types of network connections. After a connection is added with the **addcon** command, the connection is routed automatically by the system.

The node where the **addcon** command is entered is considered the "owner" of the added connections. The concept of ownership is important because automatic rerouting and preferred routing information for a connection must be entered from the node that owns the connection. See the **cnfpref** and **cnfcos** commands for more information on automatic rerouting. Before a connection is added, the proposed connection appears on the screen and you are asked to confirm the addition.

Switched Voice:	addcon FTC_slot.port Access Device ID.Connection ID node FTC_slot.port Access Device ID.Connection ID type [BW] [%utl] where BW = MIR
Auto-Dial Voice:	addcon FTC_slot.port.Access Device ID.Connection ID node FTC_slot.port Access Device ID.Connection ID slot type
Data:	addcon FTC_slot.port.Access Device ID.Connection ID FP_slot.port.Access Device ID.Connection ID node FTC_slot.port.FP_slot.port rate
Frame: [params]	addcon FTC_slot.port.FP_slot.port.DLCI node FTC_slot.port.FP_slot.port.DLCI

Full Name

Add a connection

Syntax

addcon parameters optional parameters

Related Commands

delcon, dncon, dspcon, dspcons, upcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
addcon 31.1.8 IPX 31.2.8 0 5 atc12
```

Description

Add a voice connection from FastPad port 31.1.8 to 31.2.3 with a connection ID of 5 that uses ATC12 compression. When prompted, type "y" to add the connection.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

 Local      Remote      Remote                                          Route
 Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
 31.1.8     IPX         31.2.8     Ok     atc12
 31.2.8     IPX         31.1.8     Ok     atc12








This Command: addcon 31.1.8 IPX 31.2.8 0 5 atc12


Add these connections (y/n)?
```

Table 16-4 addcon—Parameters

Parameter	Description
local channel	Specifies the local Frame Relay channel to connect in the following format: FTC_slot.port—For switched voice connections FTC_slot.port.FP_slot—For voice connections FTC_slot.port.FP_slot.port —For data connections FTCslot.port.FPslot.subport.DLCI—For Frame Relay connections In these formats, <FTC_slot> indicates the slot of the FTC card on the IPX, <port> is a port on the FTC card, <FP_slot> is the card slot on the FastPAD and <port> is the port or channel of the FastPAD data card. The <FPslot> range includes b and 1 - 8, with b being the base card and 1-8 the expansion cards. On the standard FastPAD, the base card provides six data channels; channels 1-5 are low speed, and channel 7 is high speed. Channel 6 is for NMS. Other expansion data cards (FRAM-01) provide three channels (1 - 3). One of these 3 channels can be use for the composite link. Also, on one FRAM-01 only, two of these channels can be used for Frame Relay connections. See Example 2, Fr Rly. A VFC-03 expansion card provides for voice connections.
node	Specifies the name of the IPX node at the other end of the connection.

Table 16-4 addcon—Parameters (Continued)

Parameter	Description
remote channel	Specifies the remote FastPAD channel or destination channel of the connection. It is specified in the same format as: FTC_slot.port For switched voice connections FTC_slot.port.FP_slotFor voice connections FTC_slot.port.FP_slot.port For data connections FTCslot.port.FPslot.subport.DLCIFor Frame Relay connections
type	Specifies the type of the connection. For switched voice connections, the type is “s” or “switch” to indicate the PVC is used for switched voice. For voice, type indicates the compression type. The following voice compression types are valid: ATC8, ATC12, ATC16 and CELP8, indicating ATC compression at 8K, 12K, or 16K and CELP compression at 8K. For data connections, the type is the data rate. The following Kbps values are valid: Base board low-speed ports: Asynchronous rates between 300 and 9600 bps. Synchronous rates between 1.2 and 19.2 Kbps Base board high-speed ports: Synchronous rates between 1.2 and 64 Kbps FRAM-01 expansion card: Synchronous rates between 1.2 and 512 Kbps Frame Relay Class: 1–10

Table 16-5 addcon—Optional Parameters

Parameter	Description
avoid	Specifies the type of trunk for the connection to avoid. The default is no avoidance. The choices are: ∗**s—**Avoid satellite trunks. ∗**t—**Avoid terrestrial trunks. ∗**z—**Avoid trunks using zero code suppression techniques that modify any bit position to prevent long strings of zeros.
bandwidth	Specifies the amount of bandwidth to dedicate to the voice channel. This parameter is optional and only valid for FastPAD switched voice connections.
hop count bumping	Specifies whether to use hop count bumping (adjustment) to improve the quality of the PVC carrying a switched voice connection. Bumping the hop count can lower the delay for the PVC. This parameter is optional and only valid for switched voice connections.
utilization	Specifies a utilization percentage to be used by the IPX for bandwidth assignment. This parameter is optional and only valid for switched voice connections.

addcon – FastPAD Frame Relay and Frame Forwarding Connections

Example 2

addcon 10.1.3.12.1000 beta 11.1.1.12.1001 10

Description

Add a Frame Relay connection between FastPADs.

System Response

```
gamma      TRM         YourID:1     Rev: 9.2         Mar 1 1998       PST

From            Rem        Rem
                NodeName   Channel         State    Type  Compression Code  COS

10.1.3.3.990   beta       11.1.1.2.991  Downed   fr                     10
11.1.100        beta       11.1.2.2.200   OK       fr                      3
12.1.1.3        beta       10.1            OK       fr                      2






Last Command:  addcon 10.1.3.3.990 beta 11.1.1.2.991 10

Next Command:
```

FastPad to FastPAD Frame Relay connection:
addcon 10.1.2.3.990 beta 11.1.1.2.991 10

FRP port to FastPAD Frame Relay connection:
addcon 11.1.100 beta 11.1.2.2.200 3

Frame Forwarding, FastPAD data channel to FRP port:
addcon 12.1.1.12.* beta 10.1.* 2

For Frame Relay connections, the **addcon** syntax is:

addcon local chan(s) node chan class [optional params = frp_bw avoid]

The frp_bw parameters have the same parameter values options as defined in the **cnffrcl** command for the frp ports. These are:

frp_bw = MIR/MIR VC_Q/VC_Q PIR/PIR Cmax/Cmax ECNQ_thresh/ECNQ_thresh

QIR/QIR %util/%util descr

avoid = s/z

local chan = the local FastPAD Frame Relay channel with format:

FTCslot.FRCport.FastPADsubslot.FastPADsubport[.DLCI | .*]

node = remote node name

chan = Frame Relay channel at the other end of the connection and has the following syntax described below.

For FastPAD destination:

FTC_slot.port.FP_slot.port [.DLCI | .*

For FRP destination:

FRP_slot.port [.DLCI | .*

Note If the connection is from FRP port to FastPAD, reverse the chan and local channel parameters in this example.

class = Class of Service

---

addfp

Adds a FastPAD to the IPX network. This enables the local IPX to map the FastPAD to an FTC port and communicate with it over a Frame Relay PVC to establish a control session. The **addfp** command defines the IPX slot and port to which the FastPAD is connected and assigns the FastPAD a unique name and ID. (The name and ID must be unique to the local node, and ID must match the value entered at the control panel of the FastPAD). This command also assigns a source (FastPAD) DLCI to identify the PVC connection over which the devices communicate. If the port speed and related parameters on the FTC card match those of the composite link of the FastPAD, the IPX establishes a control session with the FastPAD, allowing configuration management to be performed over this session.

```
addfp  FTC_slot.port name  ID  source_DLCI
```

Full Name

Add FastPAD to an IPX node

Syntax

addfp parameters

Related Commands

delfp, dspfp

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IPX
Lock	Yes

Example 1

`addfp  31.1 FP1 1 17`

Description

Add a FastPAD at slot port 31.1, specifying the name FP1, an ID of 1, and a source DLCI of 17.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

                        FastPADs Information

 Slot.Port  Name        ID  FP_DLCI  Port_ID  Alarm

   31.1     FP1          1       17        0  OK
   31.2     FP2          2       18        0  OK
   31.3     FP3          3       19        0  OK
   31.4     FP4          4       20        0  OK








 Last Command: addfp 31.1 FP1 1 17

Next Command:
```

Table 16-6 addfp—Parameters

Parameter	Description
slot	Specifies the slot containing the FTC card to which the FastPAD is to be added.
port	Specifies the port number on the FTC card to which the FastPAD is to be added.
name	Specifies the name of the FastPAD to be added to the node. This name must be unique to the local (physically connected IPX) node.
id	Specifies a value to be used as an identifier for the FastPAD. The value can be from 1 to 256 and must match the value entered into the FastPAD from the front panel. This value must be unique to the local (physically connected IPX) node.
source dlci	Specifies the DLCI used by the FastPAD to communicate with the local IPX node.

addfpdial

Adds a speed dial number to the FastPADs map table. The map table is used by the FastPAD to route a FastPAD end user's analog voice connection to the remote FastPAD channel. Number must be between 0 and 9999. If FFFF is specified, then no speed dial is set. For auto-dial voice channels, a specific map must be assigned to the calling channel.

```
addfpdial FTC_port.slot.FP_port dial number
```

Full Name

Add FastPAD speed dial number

Syntax

addfpdial parameters

Related Commands

None

Attributes

Privilege	1–2
Jobs	Yes
Log	Yes
Node	IPX
Lock	Yes

Example 1

`addfpdial 31.2.8 777`

Description

Add a speed dial number of 777 to FastPAD at 31.2.8

Table 16-7 addfpdial—Parameters

Parameter	Description
channel	Specifies the FastPAD channel to get a speed dial number
dial number	Specifies the phone number used by the local FastPAD. Number must be between 0 and 9999. If FFFF is specified, then no speed dial is set.

addftcport

Adds a logical Frame Relay port for T1/E1 by entering the slot number of the FTI/FTC and the DS0/time slots that make up the logical port. Table 16-8 lists the error/warning messages from this command.

Table 16-8 addftcport Command Error Messages

Messages	Reason for Message
"Slot is out of range"	Line number not correct for FTC T1/E1
"Line must first be upped"	Line is down
"invalid channel range"	Channel number is out of range (T1: 1-24) or (E1: 1–31, no 16)
"Channel is busy"	Channel is already assigned to a logical port
"You cannot use signaling channel 16" (E1)	CAS channel 16 included in logical port (E1)
"Invalid rate"	Entered rate is not 56 or 64 Kbps
"This rate is available for single channel only"	Entered rate is 56 Kbps and multiple channels were specified

Full Name

Add FastPAD port T1/E1

Syntax

addftcport parameters optional parameters

Related Commands

upcln, delftcport, cnfftcport, dspftcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
addftcport 21.9 -15
```

Description

Add a FTC port from a range of DS0/time slots.

System Response

```
gamma          TRM   YourID:1        IGX 8420    9.2.x    Mar. 15 1998 17:28 CST

Port configuration for FTC 21

FromChanSpeedInterfaceState
19-15448FRI T1INACTIVE









Last Command: addftcport 21.9-15


Next Command:
```

Table 16-9 addftcport—Parameters

Parameter	Description
line.channel	Specifies the FTI T1/E1 line number and the logical port number. For example, **addfrport** 8.14 (a period separates the line from the logical port number).

Table 16-10 addftcport—Optional Parameters

Parameter	Description
- *chan*	Specifies that multiple DS0/time slots should be aggregated into a logical port, for example, **addftcport** 8.1 – 5 (a hyphen is used to separate the DS0/time slots in a from – to range). The lowest DS0/time slot number becomes the logical port number.
rate	Specifies the rate of a single logical port. By default, multiple ports are all 64 Kbps. A single DSØ/time slot may be 56 Kbps or 64 Kbps. For example, **addftcport** 8.14 56 (if rate is not entered, 64 Kbps is assumed).

cnfchgn

Configures the amount of gain inserted by the IPX mode for the specified FastPAD voice channel. Gain can be configured between +6 dB and -8 dB. The input gain is inserted at the receive side of an FTC line, and is therefore applied before the signal is packetized. The output gain is inserted at the transmit side of a FTC line and is applied after the signal has been depacketized.

Full Name

Configure gain insertion for channels

Syntax

cnfchgn parameters

Related Commands

dspchcnf

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
1–2	Yes	Yes	IPX	Yes

Example 1

```
cnfchgn 31.1.8 -4 2
```

Description

Configure an input gain of -4db and an output gain of +2db for FastPAD channel 31.1.8

System Response

```
IPX           TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

          %     Gain  (db)
Channels Util    In     Out   Interface Type   DTMF  SLT Timeout
31.1.8   100     -4     2     FXS L/S           30









Last Command: cnfchgn 31.1.8 -4 2


Next Command:
```

Table 16-11 cnfchgn—Parameters

Parameter	Description
channel(s)	Specifies the FastPAD channel
gain	Specifies the gain, in decibels, to assign to the channel. The range is -8 dB to +6 dB.

cnfdclk

Configures the clocking for a FastPAD data channel. The FastPAD supports synchronous and asynchronous traffic. For synchronous traffic, the channel can support internal or external clocking. Asynchronous (character-oriented) traffic is sent as 8 bits, 1 stop bit, and no parity.

Note For a change of port type on an expansion card from Frame Relay to data (DLC), a prompt appears stating that the FastPAD must be reset. Use the **resetfp** command to do this.

Full Name

Configure data channel clocking type

Syntax

cnfdclk parameters optional parameters

Related Commands

cnfict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
cnfdclk 31.2.B.2 TRANS i
```

Description

Configure clock for channel 31.2.B.2 for transparent data and an internal clock mode.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Data Channel:      31.2.B.2
Interface:         RS232       DTE
Clocking:          Internal


            Interface Control Template for Connection while Active

      Lead       Output Value                Lead       Output Value
      DSR        ON                          RTS        N/A
      DCD        ON                          CTS        ON






Last Command: cnfdclk 31.2.B.2 TRANS i


Next Command:
```

Table 16-12 cnfdclk – Parameters

Parameter	Description
channel	Specifies the data channel to configure. Data channels are specified in the format slot.port.subslot.subport, where slot and port are the slot/port of the FTC card, subslot is the FastPAD card slot (1-8 for expansion, b for the base card), and subport is the port/channel on a FastPAD data card. The base card supports six ports/channels (1-5 are low speed, 6 is high speed). Other data cards support three ports/channels (1-3).
data mode	Specifies the data transmission mode as either: • TRANS—Transparent data transmission • DLC—H/SDLC data transmission • ASYNC—Asynchronous data transmission
clock type	Specifies a clocking type to assign to each channel. Valid clock types are: • **i**—Internal (FastPAD provides transmit/receive clocks.) • **e**—External (FastPAD provides transmit/receive clocks.)

cnffrport

Configures the parameters of a Frame Relay port. When configuring a Frame Relay port on a FastPAD, the user is prompted for each parameter. Pressing the Return key keeps the current value for the parameter. The screen display is shaded for parameters not configurable for some applications. The data rates for each of the four ports may be mixed and matched freely if the total for all four ports does not exceed the maximum data rate allowed (up to 512 Kbps.)

The rules for assigning data rates to the four ports when using the 1 Mbps FRI are as follows:

1. If a data rate of 672 Kbps or above is used in any port, no other port may be used.
2. If a data rate of between 384 Kbps and 512 Kbps is used in any port, a second port may be used at an available data rate of 512 Kbps or below.
3. If a data rate of 336 Kbps is used in any port, two other ports may used at any available data rates of 336 Kbps or below.
4. If the data rate of any port does not exceed 256 Kbps, all four ports may be used at any available data rates of 256 Kbps or below.

Full Name

Configure Frame Relay port

Syntax
(T1/E1 ports)

cnffrport Required parameters (left-to-right):

slot.logical port number	prot queue depth
ecn queue threshold	de threshold
signaling protocol	protocol parameters

Optional parameters:

None

Syntax
(All other ports)

cnffrport Required parameters (left-to-right):

slot.port number

Optional parameters:

speed	clocking
port type	port ID
prot queue depth	ECN q_threshold
de_threshold	signaling protocol
protocol parameters	min-flags-bet-frames

Related Commands

upfrport, dnfrport, dspfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

cnffrport 5.1 256 NORMAL 0 65535 65535 100 2 N

Description

Reconfigure the FR port to 5.1 to change Q depths

System Response

```
D2.ipx5        TRM   YourID:1        IGX 8420    9.2   Aug. 4 1998 16:40 PST

Port:       5.1               [ACTIVE ]
Interface:FRI-X21 DCEConfigured Clock:256Kbps
Clocking:NormalMeasured Rx Clock:256Kbps
Port TypeFRMin Flags/Frames1
Port ID0
Port Queue Depth65535OAM Pkt Threshold3pkts
ECN Queue Threshold65535T391 Link Intg Timer6sec
DE Threshold100%N391 Full Status Poll10cyl
Signalling ProtocolNoneForeSight (CLLM)No
Asynchronous StatusNoCLLM Status Tx Timer0msec
T392 Polling Verif Timer15IDE to DE MappingYes
N392 Error Threshold3Interface Control Template
N393 Monitored Events Count4LeadI
Communicate PriorityNoStateON
Upper/Lower RNR Thresh75%/25%

Last Command: cnffrport 5.1 256 NORMAL 0 65535 65535 100 2 N


Next Command:
```

Example 2

cnffrport 8.1 256 n 12000 10000 100 4 15 3 4 N 75 25 1

Description

Reconfigure an NNI FR port 8.1 to change Q depths

System Description

```
gamma TRM   YourID:1        IGX 8420    9.2    Mar. 15 1998 15:51 PST


Port:       8.1     [ACTIVE ]
Interface:  V35-4   DCE                   Configured Clock:         256 Kbps
Clocking:   Normal                        Measured Rx Clock:        256 Kbps
Port ID                  40
Port Queue Depth       12000
ECN Queue Threshold    10000              Min Flags / Frames          1
DE Threshold             100 %            OAM FastPacket Threshold    3 pkts
Signalling Protocol Annex A NNI           Link Integrity Timer (T391) 6 secs
Asynchronous Status      Yes              Full Status Polling (N391) 10 cycles
Polling Verif Timer       15              Interface Control Template
Error Threshold            3                 Lead       State
Monitored Events Count     4                  CTS        ON
Communicate Priority      No                  DSR        ON
Upper/Lower RNR Threshold 75/25 %             DCD        ON


Last Command: cnffrport 8.1 256 normal 12000 10000 100 6 15 3 4 N 75 25 1



Next Command:
```

The results for the update FR parameters as shown are as follows:

Port Queue Depth	65535	Depth of port queue is set at 65,535 bytes.
ECN Queue Depth	65535	Port queue must reach 65,535 bytes before FECN and BECN bits are set.
DE Threshold	100	Port buffer fill must be 100% before dropping DE frames.
signaling Protocol	2	LMI disabled.
Asynchronous Status	N	No asynchronous messages to user device; wait for polling from user device.
Polling Verify Timer	15	15 seconds heartbeat period.
Error Threshold	3	3 failures trigger port comm failure.
Monitored Events Count	4	4 events are monitored.
Communicate Priority	N	Do not communicate port priority to the user device.
Upper RNR Threshold	75	75% of buffer triggers receiver not ready condition.
Lower RNR Threshold	25	25% of buffer clears a receiver not ready condition.
Minimum Flags/Frame	1	There is only one flag for each FR data frame.

Table 16-13 cnffrport – Parameters

slot.port	Specifies the FRP card slot and port number. (Slot and logical port number for T1/E1)
speed	Specifies the port clock speed in kbps; for a 2.0 Mbps FRP. Speed configured is displayed as Configured Clock. Actual clock rate is displayed as Measured Rx Clock. The available speeds are: 1 port (selected speeds, 56 to 2048 Kbps) 2 ports (selected speeds, 56 to 1024 Kbps) 3 ports (selected speeds, 56 to 672 Kbps) 4 ports (selected speeds, 56 to 512 Kbps) The available clock rates for the 1, 2, 3, and 4 port combinations are provided in the command description.
clocking	Specifies the port clock type (normal/looped) [normal]. There are four combinations of clocking that may be used for the FRI-V.35 and two with the FRI-X.21. Refer to Chapter 2, Frame Relay Interface Card for a description of looped and normal clock modes. Not specified for T1/E1 ports. FRP is DCE with normal clocking (V.35 and X.21) FRP is DCE with looped clocking (V.35 only) FRP is DTE with normal clocking (V.35 and X.21) FRP is DTE with looped clocking (V.35 only)
port type	Specifies the port type as either FR for Frame Relay or ATM for Asynchronous Transfer Mode. Select ATM when using AIP to interface V.35 circuits to IPX FRP port. Configures alarm reporting and other miscellaneous functions for port.
port ID	Specifies the DLCI associated with the port (0 - 1024) {0}. The IPX uses this number only when adding bundled connections. Otherwise, it can be used by the customer as a network destination number in global addressing. Not specified for T1/E1 ports.
port queue depth	specifies the maximum bytes queued for transmission from the FRP port. The range is from 0–65535. The default is 65535.
ecn queue threshold	specifies the port explicit congestion notification. The range is from 0-65535. The default is 65535. This is the point at which the BECN and FECN bits will be set in the communications to the user device.
de threshold	Specifies the port queue depth above which frames with the Discard Eligibility bit set will be discarded. Valid entries are 0–100%, with a default of 100%. An entry of 100% effectively disables DE for the port.

Table 16-13 cnffrport – Parameters (Continued)

slot.port	Specifies the FRP card slot and port number. (Slot and logical port number for T1/E1)
signalling protocol	Specifies the LMI operation mode. The range is from 0-255. The following values are defined (the default is LMI=2): LMI = 0—LMI is disabled at this port. LMI = 1—Cisco LMI and the asynchronous update process is enabled at this port. Greenwich Mean Time is also enabled LMI = 2—LMI is disabled at this port. LMI = 3—Cisco LMI is enabled at this port, but asynchronous update process is disabled. LMI = 4—Port configured as User-Network Interface using CCITT Q.933 Annex A parameters. LMI = 5—Port configured as User-Network Interface using ANSI T1.617 Annex D parameters. LMI = 6—Port configured as Network-Network Interface using CCITT Q.933 Annex A parameters. LMI = 7—Port configured as Network-Network Interface using ANSI T1.617 Annex D parameters.
asynchronous status	Specifies whether the IPX should send unsolicited LMI update messages as they appear or whether to wait for the polling from the user device. Valid values are y (yes) or n (no)
polling verify timer	Specifies the Link Integrity Verification Timer heartbeat (keep-alive) period with a valid range of 5–30. This should be set to 5 seconds more than the heartbeat time set in the user equipment. Default is 15.
error threshold	Specifies the number of failures in the monitored events that causes the “keep alive” process to report an alarm. It has an accepted range of 0-255 and a valid range of 1–10. A value of zero defaults to 1, and a value more than 10 defaults to 10.
monitored events count	Specifies the number of monitored events for the “keep alive” process. It has an accepted range of 0-255 and a valid range of 1-10. A port communication fail condition is cleared after this number of successful polling cycles. A value of 0 defaults to 1, and a value more than 10 defaults to 10.
communicate priority	Specifies whether the connections SNA priority (H or L) should be communicated to the user device attached to the port. Valid entries are y (yes) or n (no); default is no.
upper/lower RNR threshold	Specifies the receiver not ready thresholds. Upper threshold is the number of receiver not ready indications from the user equipment before alarm is generated for this port. The lower receiver not ready threshold is the number of indications from the user equipment before an alarm is cleared. Valid values are 1-255; defaults to 75 for upper, 25 for lower threshold.
min. flags/frame	Specifies the minimum number of flags between frames. All values greater than 0 are valid and the default is 1.
OAM FastPacket threshold	Specifies the OAM FastPackets are used within the local IPX network to transmit the NNI status from the remote network. This counter allows the user to define the number of dropped OAM packets before setting Abit transmitted to the user device to 0 to indicate connection failure. This can be set from 0 to 15 packets and the default is 3 packets. A 0 disables this function. Set for both UNI and NNI ports.

Table 16-13 cnffrport – Parameters (Continued)

slot.port	Specifies the FRP card slot and port number. (Slot and logical port number for T1/E1)
link integrity timer (T391)	Specifies the interval to send Status Inquiry messages across the NNI port. This will result in a report of all failed connections. This can be set for 5–30 seconds and the default is 6 sec. Both networks must have the same value set for T391.
full status polling cycle (N391)	Specifies the interval to send the Full Status Report request for all PVCs across the NNI port. This can be set for 1–255 polling cycles and the default is 10 cycles. The Full Status reports the status of all the connections, failed or not, across the NNI.
card type	Specifies the card type (within a job only). This parameter is entered just after slot.port. The valid entries include V.35, X.21, port, and LINE with LINE indicating a T1 or E1 line. This parameter is not required in normal use of the command.
CLLM status Tx Timer	Specifies the interval to send ForeSight congestion messages across the NNI port. Can be set for 40 to 350 ms. and the default is 100 sec. Both networks must be Cisco WAN Switching networks.
IDE to DE mapping	Specifies whether the internal DE bit (IDE) status in the FastPacket or ATM cell should be mapped to the Frame Relay DE bit at the destination. Selection is YES or NO.
interface control template	Specifies the control leads available on the V.35 and X.21 physical Frame Relay ports and their status.
channel range	Specifies the DS0s used for the T1 or E1 logical port. Can range from 1 to 1–31, for example, 7–12 indicates six DS0s used for the port starting with DS0 #7. Channel range is specified in the **addfrport** command.
channel speed	Specifies the bandwidth provided for the logical port. Speed is 64 Kbps times the number of DS0s indicated by the Channel Range.

cnfftcport

Configures the parameters of an FTC port. When configuring an FTC port, the user is prompted for each parameter. Pressing the Return key keeps the current value for the parameter. The screen display is shaded for parameters not configurable for some applications. The data rates for each of the four ports may be mixed and matched freely provided the total for all four ports does not exceed the maximum composite data rate allowed by the FTC card (2.048 Mbps). Supported data rates are listed in Table 16-14.

Table 16-14 FTC Port Supported Data Rates

Data Rates at 56 Kbps Intervals				Data Rates at 64 Kbps Intervals			
56	112	168	224	64	128	192	256
280	336	392	448	320	384	448	512
504	560	616	672	576	640	704	768
728	784	840	896	832	896	960	1024
952	1008	1064	1120	1088	1152	1216	1280
1176	1232	1288	1344	1344	1408	1472	1536
1400	1456	1512	1568	1600	1664	1728	1792
1624	1680	1736	1792	1856	1920	1984	2048

When using **cnfftcport** in a job, an additional parameter, port type, is entered just after slot.port. Valid entries include V.35, X.21, port, and line, with line indicating a T1 or E1 line. This parameter is not required in normal use of the command.

Note For a change of port type on an expansion card from data (DLC) to Frame Relay, a prompt appears stating that the FastPAD must be reset. Use the **resetfp** command to do this.

The data rates for each of the four ports may be mixed and matched freely from the above data rates provided the total for all four ports does not exceed 2048 Kbps. Data rates (Kbps) available when using the 1 Mbps FTI are shown in Table 16-15.

Table 16-15 FTI Port Supported Data Rates

Port Data Rates for 1 Mbps FTI			
1024	512	256	128
896	448	224	112
768	384	192	64
672	336	168	56

When using **cnfftcport** in a job, an additional parameter, card type, is entered just after slot.port. Valid entries include V.35, X.21, T1, and E1. The data rates for each of the four ports may be mixed and matched freely from the above data rates provided the total for all four ports does not exceed 2048 kbps.

Full Name

Configure FTC port

Syntax (T1/E1 ports)

cnfftcport Required parameters (left-to-right):

slot.logical port number	port queue depth
ecn queue threshold	de threshold
signaling protocol	protocol parameters

Optional parameters:

None

Syntax

cnfftcport Required parameters:

slot.port number

Optional parameters (left to right):

speed	clocking
port ID (between 16–991)	port queue depth
de_threshold	ECN q_threshold
signaling protocol	asynchronous status
polling verify timer	error threshold
monitored events count	communication priority
upper/lower RNR threshold	min flags/frames

Related Commands

upftcport, dnftcport, dspftcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
cnfftcport 3.1.1 256 NORMAL 0 65535 65535 100 2 N
```

Description

Reconfigure the FTC port to change Q depths

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Port:       31.1              [ACTIVE  ]
Interface:  FTI-V35 DCE                        Configured Clock:    256 Kbps
Clocking:   Normal                             Measured Rx Clock:   256 Kbps
Port Type                     FR       Min Flags / Frames           1
Port ID                        4
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer         6 sec
DE Threshold                 100 %     N391 Full Status Poll       10 cyl
Signalling Protocol   STRATA LMI       ForeSight (CLLM)            No
Asynchronous Status           No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead    CTS    DSR    DCD
Communicate Priority          No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: cnfftcport 31.1  256  NORMAL 0 65535  65535  100  2  N


Next Command:
```

The results for the update FR parameters as shown are as follows:

Port Queue Depth	65535	Depth of port queue is set at 65,535 bytes.
ECN Queue Depth	65535	Port queue must reach 65,535 bytes before FECN and BECN bits are set.
DE Threshold	100	Port buffer fill must be 100% before dropping DE frames.
signaling Protocol	2	LMI disabled
Asynchronous Status	N	No asynchronous messages to user device; wait for polling from user device.
Polling Verify Timer	15	15 seconds heartbeat period
Error Threshold	3	3 failures trigger port comm failure
Monitored Events Count	4	4 events are monitored
Communicate Priority	N	Do not communicate port priority to the user device.
Upper RNR Threshold	75	75% of buffer triggers receiver not ready condition
Lower RNR Threshold	25	25% of buffer clears a receiver not ready condition
Minimum Flags/Frame	1	There is only one flag for each FR data frame.

Table 16-16 cnfftcport – Parameter

slot.port	Specifies the FRP card slot and port number. (Slot and logical port number for T1/E1)

Table 16-17 cnfftcport – Optional Parameters

speed	Specifies the port clock speed in kbps; for a 2.0 Mbps FRP. Speed configured is displayed as Configured Clock. Actual clock rate is displayed as Measured Rx Clock. The available speeds are: 1 port (selected speeds, 56 to 512 Kbps) 2 ports (selected speeds, 56 to 512 Kbps) 3 ports (selected speeds, 56 to 512 Kbps) 4 ports (selected speeds, 56 to 512 Kbps) The available clock rates for the 1, 2, 3, and 4 port combinations are as follows: 56 64 72 96 112 384 512
clocking	Specifies the port clock type (normal/looped) [normal]. There are four combinations of clocking that may be used for the FRI-V.35 and two with the FRI-X.21. Refer to Chapter 2, Frame Relay Interface Card for a description of looped and normal clock modes. Not specified for T1/E1 ports. FRP is DCE with normal clocking (V.35 and X.21) FRP is DCE with looped clocking (V.35 only) FRP is DTE with normal clocking (V.35 and X.21) FRP is DTE with looped clocking (V.35 only)
port ID	Specifies the DLCI associated with the port (16-991).
port queue depth	specifies the maximum bytes queued for transmission from the FRP port. The range is from 0–65535. The default is 65535.
ecn queue threshold	specifies the port explicit congestion notification. The range is from 0–65535. The default is 65535. This is the point at which the BECN and FECN bits will be set in the communications to the user device.
de threshold	Specifies the port queue depth above which frames with the Discard Eligibility bit set will be discarded. Valid entries are 0–100%, with a default of 100%. An entry of 100% effectively disables DE for the port.
signalling protocol	Specifies the LMI operation mode. The range is from 0-255. The following values are defined (the default is LMI=2): LMI = 0—LMI is disabled at this port. LMI = 1—Port configured as Network-Network Interface using ANSI T1.617 Annex D parameters. LMI = 2—Cisco LMI is enabled at this port.
asynchronous status	Specifies whether the IPX should send unsolicited LMI update messages as they appear or whether to wait for the polling from the user device. Valid values are y (yes) or n (no)
polling verify timer	Specifies the Link Integrity Verification Timer heartbeat (keep-alive) period with a valid range of 5–30. This should be set to 5 seconds more than the heartbeat time set in the user equipment. Default is 15.
error threshold	Specifies the number of failures in the monitored events that causes the “keep alive” process to report an alarm. It has an accepted range of 0–255 and a valid range of 1–10. A value of zero defaults to 1, and a value more than 10 defaults to 10.
monitored events count	Specifies the number of monitored events for the “keep alive” process. It has an accepted range of 0–255 and a valid range of 1–10. A port communication fail condition is cleared after this number of successful polling cycles. A value of 0 defaults to 1, and a value more than 10 defaults to 10.

Table 16-17 cnfftcport – Optional Parameters (Continued)

communicate priority	Specifies whether the connections SNA priority (H or L) should be communicated to the user device attached to the port. Valid entries are y (yes) or n (no); default is no.
upper/lower RNR threshold	Specifies the receiver not ready thresholds. Upper threshold is the number of receiver not ready indications from the user equipment before alarm is generated for this port. The lower receiver not ready threshold is the number of indications from the user equipment before an alarm is cleared. Valid values are 1–255; defaults to 75 for upper, 25 for lower threshold.
min. flags/frame	Specifies the minimum number of flags between frames. All values greater than 0 are valid and the default is 1.

cnfict

Sets the interface control template signals for a FastPAD data channel. The signals that can be set using **cnfict** are RTS, CTS, DSR and DCD.

Full Name

Configure interface control template

Syntax

cnfict parameters optional parameters

Related Commands

cpyict, dspict, prtict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
cnfict 31.1.B.7 act dcd   r
```

Description

Configure port 31.1.B.7 with the active interface control template as remote for DCD following RTS

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Data Channel:      31.1.B.7
Interface:         RS232       DTE
Clocking:          Internal
Framing:           DLC

            Interface Control Template for Connection while Active

      Lead       Output Value                Lead       Output Value
      DSR        ON                          RTS        N/A
      DCD        Remote RTS                  CTS        ON






Last Command: cnfict  31.3.B.7  act  dcd  r


Next Command:
```

Table 16-18 cnfict – Parameters

Parameter	Description
channel	Specifies the FastPAD data channel whose interface control template to configure in the format: slot.port.subport.subslot
template	Specifies the interface control template to configure for the channel. The only valid template for a FastPAD data channel is the ACTIVE template. It is specified as "a".
output	Specifies the output lead to configure. Valid output leads are RTS, CTS, and DCD. on—The output lead is asserted. off—The output lead is inhibited.

Table 16-19 cnfict – Optional Parameters

Parameter	Description
delay	Specifies the time in milliseconds that separates the "off" to "on" lead transitions. Delay is valid only when the output lead is CTS and the input lead is local RTS. "On" to "Off" lead transitions are not subject to this delay.
source	Specifies how the lead is to be configured and has the format: on | off | local | remote input delay Delay is an optional parameter. The following lists the valid source choices: on—The output lead is asserted. off—The output lead is inhibited. l—For local; indicates that the output follows a local lead. r—For remote; indicates that the output follows a remote lead.

Table 16-19 cnfict – Optional Parameters (Continued)

Parameter	Description
input	Specifies the time in milliseconds that separates the “off” to “on” lead transitions. Delay is valid only when the output lead is CTS and the input lead is local RTS. “On” to “Off” lead transitions are not subject to this delay.

cnfvchtp

This command configures an interface signaling type for a FastPAD voice channel. The following interface types are supported:

- E & M
- FXS
- FXO
- AC-15

Any of the five E & M signaling types are supported, as well as four-wire and two-wire facilities. FXS indicates the FastPAD emulates a single line telephone. It operates in loop start mode and provides loop to the connected device. FXO indicates the FastPAD emulates a central office. It operates in loop start or ground start mode and provides loop current and ring voltage to the attached device. AC-15 indicates the European signaling mode. This mode is similar to E & M. Both the A and B types are supported. This command also sets Dual Tone Multi Frequency detect period.

Full Name

Configure voice FastPAD channel type

Syntax

cnfvchtp parameters optional parameters

Related Commands

None.

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
1–2	Yes	Yes	IPX	Yes

Example 1

```
cnfvchtp 31.1.4 FXS   * * 1
```

Description

Configure FastPAD voice channel for interface type FXS and a DTMF value of 1

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Mar. 16 1998 1:06 PST

           %    Gain (dB)
Channels  Util   In  Out    Interface Type    DTMF    SLT Timeout
14.1      N/A    7    5     FXS  L/S            1











Last Command: cnfvchtp 31.1.4  FXS * * 1


Next Command:
```

Table 16-20 cnfvchtp – Parameters

Parameter	Description
channel	Specifies the FastPAD channel for which to configure the interface type where channel is specified in the format: slot.port.subslot
interface type	Specifies the interface type to assign to the channel. This specifies the operational mode of the channel. The possible values are: • E & M—Indicates E & M signaling mode. This choice is followed by two parameters: the type of E & M signaling [1-5] and the type of wiring [2w/4w]. • FXS—Indicates single line telephone mode. This choice is followed by the type of start signaling [LOOP/GND]. • FXO—Indicates off premise extension mode. • AC-15—Indicates the AC-15 European signaling mode. This choice is followed by signaling type [A/B].

Table 16-21 cnfvchtp – Optional Parameter

Parameter	Description
dtmf detect	Specifies whether the FastPAD sends DTMF in-band as a voice-wave signal or detects DTMF codes control frame for transmission and regenerates is detected.
slt timeout	Specifies the timeout period for single line telephone mode. Valid only with FXS ground start.

cpyict

Copies all control template information associated with a specified FastPAD data channel to another. Once copied, the control template information may be edited with the **cnfict** command. See the **cnfict** command for more information on interface control templates.

Full Name

Copy interface control template

Syntax

cpyict parameters

Related Commands

cnfict, dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
cpyict 31.1.B.1 31.1.B.2
```

Description

Copy the interface control template from channel 31.1.B.1 to channel 31.1.B.2

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Data Channel:      31.1.B.2
Interface:         RS232       DTE
Clocking:          Internal


            Interface Control Template for Connection while Active

      Lead       Output Value                Lead       Output Value
      DSR        ON                          RTS        N/A
      DCD        OFF                         CTS        ON






Last Command: cpyict 31.1.B.1 31.1.B.2


Next Command:
```

Table 16-22 cpyict – Parameter

Parameter	Description
source channel	Specifies the channel whose interface control template information to copy in the format slot.port.subport.subslot
destination channel	Specifies he channel that will receive the copied interface control template information in the format: slot.port.subport.subslot.

delcon

Deletes a FastPAD connection. All FastPAD connection types can be deleted with this command, including switched voice, voice and data connections. When you enter the **delcon** command, a prompt appears asking you to confirm the deletion. Connections can be deleted from the IPX node at either end of the connection.

Do not delete a connection when the node at the other end of the connection is unreachable. The unreachable node will not recognize the deletion. It is especially important not to delete a connection to an unreachable node and then connect that channel to another node. Channel connections are added to the network with the **addcon** command.

Full Name

Delete connections

Syntax

delcon parameters

Related Commands

addcon, dspcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

`delcon 31.1.B.1`

Description

Delete connection 31.1.B.1. The connections to delete are highlighted, and a prompt appears asking you to confirm the deletion. Respond with “y” for yes. Connection 25.1 is deleted.

System Response

```
Local      Remote      Remote                                        Route
Channel    NodeName    Channel    State  Type    Compression  Code Avoid COS O
31.1       IPX         31.3       Ok     session
31.1       IPX         31.2       Ok     session
31.1.B.1   IPX         31.2.B.2   Ok     16
31.1.8     IPX         31.2.8     Ok     atc12
31.2       IPX         31.1       Ok     session
31.2.B.2   IPX         31.1.B.1   Ok     16
31.2.8     IPX         31.1.8     Ok     atc12
31.3       IPX         31.1       Ok     session




This Command: delcon 31.1.B.1


Delete these connections (y/n)?
```

Table 16-23 delcon – Parameters

Parameter	Description
channel(s)	Specifies the FastPAD channel to delete. Channel is specified in the following format: slot.port—For switched voice connections slot.port.subslot—For permanent voice connections slot.port.subslot.subport—For data connections FTC_slot.port.FPslot.subport.DLCI—For Frame Relay connections, where subslot and subport refer to FastPAD

delfp

Deletes a FastPAD from the IPX network. The FastPAD to delete is specified by its unique name (assigned using the **addfp** command).

Full Name

Delete connection group

Syntax

delfp parameters

Related Commands

addfp, dspfp

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
delfp 31.1
```

Description

Delete FastPAD 31.1.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

                         FastPADs Information

 Slot.Port  Name       ID  FP_DLCI  Port_ID  Alarm

   31.1     FP1         1       17        0  OK
   31.2     FP2         2       18        0  OK
   31.3     FP3         3       19        0  OK
   31.4     FP4         4       20        0  OK








This Command: delfp 31.1


Delete FastPAD (y/n)?
```

Table 16-24 delfp – Parameters

Parameter	Description
slot.port	Specifies the location of the FastPAD to be removed.

Table 16-25 delfp – Optional Parameters

Parameter	Description
name	Specifies the name of the FastPAD to be removed.

delftcport

The following information applies only to FTC T1/E1 applications. Deletes logical FTC ports and unassigns associated DSØ/time slots. The unassigned DSØ/time slots may be recombined with the **addftcport** command to create new logical ports. Logical port numbers range from 1 to 24 for T1 lines and 1 to 31 (16 reserved) for E1 lines.

The port screen (normally seen with the **dspftcport** command) will be displayed regardless of successful port deletion. The screen will display defined port numbers for the specified line. Error messages are displayed when the procedure is incorrect. Table 16-26 lists the error/warning messages of this command.

Table 16-26 delftcport Command Error Messages

Messages	Reason for Message
"Slot is out of range"	Line number not correct for FRP T1/E1
"Port does not exist"	Logical port number does not exist
"You must first down the port"	Logical port is up
"You must first down the port"	Specified port is not first DSØ/time slot of logical port

Full Name

Delete FTC (T1/E1)

Syntax

delftcport parameters

Related Commands

addfrport, dspfrport, dnfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IPX	Yes

Example 1

```
delfrport 8 .1
```

Description

Delete FTC port 8.1

System Response

```
alpha TRM   YourID:1        IGX 8420    9.2.Z    Mar. 15 1998 17:28 CST

Port configuration for FRP 8

From     Chan     Speed     Interface     State
1       9-15      448 FTI      T1         ACTIVE
20       20-24      320 FTI       T1          ACTIVE









Last Command: delftcport 8.1


Next Command:
```

Table 16-27   delfrport – Parameter

Parameter	Description
slot	Specifies the FTC T1 or E1 line (cabinet slot) number of the port to delete
port	Specifies the logical port number of the port to delete.

dnfrport

Downs the specified FastPAD FRAM-01 Frame Relay port. All connections must be removed from the port before the port can be deactivated.

Full Name

Down Frame Relay port

Syntax

dnfrport parameters

Related Commands

cnffrport, dspfrport, upfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
dnfrport 6.3
```

Description

Down Frame Relay port 6.3

Table 16-28 dnfrport – Parameters

Parameter	Description
slot	Specifies the slot number of the Frame Relay card with the port to down.
port	Specifies the port number to down on the specified Frame Relay card.

dnftcport

Downs (deactivates) the specified FTC port. All connections must be removed from the port before the port can be deactivated.

Full Name

Down FTC port

Syntax

dnftcport parameters

Related Commands

cnfftcport, dspftcport, upftcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
dnftcport 31.1
```

Description

Down (deactivate) FTC port 3.1

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Port:        31.1               [INACTIVE]
Interface:  FTI-V35 DCE                        Configured Clock:    64 Kbps
Clocking:   Normal                             Measured Rx Clock:    0 Kbps
Port Type                    FR       Min Flags / Frames           1
Port ID                       4
Port Queue Depth          65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold       65535       T391 Link Intg Timer         6 sec
DE Threshold                100 %     N391 Full Status Poll       10 cyl
Signalling Protocol   STRATA LMI      ForeSight (CLLM)            No
Asynchronous Status          No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer     15       IDE to DE Mapping          Yes
N392 Error Threshold          3       Interface Control Template
N393 Monitored Events Count   4          Lead    CTS    DSR    DCD
Communicate Priority         No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dnftcport 31.1


Next Command:
```

Table 16-29 dnftcport – Parameters

Parameter	Description
slot	Specifies the slot number of the FTC to down.
port	Specifies the port number to down on the specified FTC card.

dspchcnf

Displays configuration details for FastPAD voice and data channels:

- FastPAD Voice channels display: Channel, Percentage Utilization, Gain In and Out, and the Interface Type.
- FastPAD Data channels display: Channel, Percentage Utilization, and the Type, i.e., data rate.

If the channel specified is a FastPAD voice channel, the display includes configuration details for all voice channels on the FTC port starting with the specified channel. If the channel specified is a data channel, the display includes configuration details for all channels on the specified FTC port starting with the specified channel.

In this release, the **dspchcnf** screen shows if a dta channel is configured for Idle Code Suppression (ICS). Idle code suppression feature provides a way to stop fast packet generation on a Nx64 super-rate PVC connection when the connected PBX has terminated a video call. Traffic on the data network will therefore be reduced. Bursty data will be able to use this un-used bandwidth. The Example 2 screen below indicates whether a data channel is configured for idle code suppression.

Full Name

Display channel configuration

Syntax

dspchcnf parameters

Related Commands

prtchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX	No

Example 1

`dspchcnf 31.1.8`

Description

Display configuration values for channel 31.1.8

```
IPX           TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

          %     Gain  (db)
Channels Util    In    Out   Interface Type   DTMF  SLT Timeout
31.1.8   100     -4    2     FXS L/S           30










Last Command: dspchcnf 31.1.8


Next Command:
```

Example 2

`dspchcnf 9.2.3`

Description

Display configuration values for channel 9.1.3

```
sw176         TRM   StrataCom       IGX 16    9.2.a2    Apr. 3 1998  17:32 PST

            Maximum EIA      %      DFM Pattern     DFM    Idle Code   PreAge
From 9.1.3  Update Rate    Util     Length        Status     Suppr      (usec)
9.1.3-8        -           -        -             -        Enabled         0



Last Command: dspchcnf 9.1.3
```

Table 16-30 dspchcnf – Parameters

Parameter	Description
start channel number	Specifies the channel with which to start the display in the format: slot.port.subport—For FastPAD voice connections slot.port.subport.subslot—For FastPAD data connections

dspcon

Displays connection information for a specified channel. The information displayed includes:

- Channel numbers for both the local and remote ends of the connection.
- Node names at both ends of the connection.
- Type ("s" for switched and "v" for voice) or data rate of the connection.
- Compression type (ATC, CELP, Negotiated).
- Routing restriction.
- Class of service (COS) of the connection.
- Connection route listing the end nodes and any intermediate nodes.
- Preferred route for the connection (if configured).
- Status of the cards associated with the connection. The status that may be displayed includes:

  OK—Connection OK

  FAILED—Connection failed
- Connection descriptor (if configured).
- Status of the "Feeder" connection. This is the connection between the FastPAD and the FTC. A failure is indicated as "End Point: Feeder Fail".

Full Name

Display connections

Syntax

dspcon parameters

Related Commands

addcon, delcon, dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX	No

Example 1

```
dspcon 31.1.8
```

Description

Display voice connection information for FTC channel 31.1.8

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Conn:  31.1.8     IPX         31.2.8      atc12


                                                              Status: OK


Path:   Route information not applicable for local connections




IPX       FTC:   OK                  IPX       FTC:   OK
          FTI:   OK                            FTI:   OK
          FastPAD: OK                          FastPAD: OK

Last Command: dspcon 31.1.8


Next Command:
```

Table 16-31 dspcon – Parameters

Parameter	Description
channel	Specifies the FastPAD channel for which to display connection details. The command displays connection information for one channel at a time. You cannot specify a set of channels. <channel> is specified in the following formats: slot.port—For switched voice connections slot.port.subslot—For permanent voice connections slot.port.subslot.subport—For data connections FTCslot.FTCport.subslot.subport.DLCI—For Frame Relay connections, where subslot and subport refer to FastPAD.

dspcons

Displays a summary of the connections on an IPX node. The fields displayed in the **dspcons** screens are shown in Table 16-32:

Table 16-32 dspcons Display Fields

Fields	Description
Local Channel	The connection's channel at this node.
Remote Node Name	The name of the node at the other end of the connection.
Remote Channel	The connection's channel at the remote node.
State	The state of the connection(s) are as follows: OK—Routed Down—Downed OK (Dn)—Waiting for onhook to occur to allow courtesy down to take place for connection(s) that have been courtesy downed using the **dncon** command. Failed—Unrouted, but trying
Type	The type of connection (v = voice, fr = Frame Relay. data rate in kbps for data).
Route Avoid	The type of lines to avoid when routing (satellite lines, terrestrial lines, lines with zero code suppression).
Compression	The type of compression applied to the connection (ATC8, ATC12, ATC16, CELP8).
COS	The Class of Service.
Owner	The end of the connection in control of re-routing.
Descriptor	The connection descriptor string (if +d option specified).
Loopback	A connection with a local loopback is indicated by a right parenthesis symbol between the "Local Channel" and "Remote NodeName" columns. A connection with a remote loopback is indicated by a right parenthesis symbol before the channel number in the "Remote Channel" column.

Full Name

Display connections

Syntax

dspcons optional parameters

Related Commands

addcon, delcon, dspcon

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	IPX	No

Example 1

dspcons 31.1.8

Description

Displays all connections starting with 31.1.8, in this case voice connections.

System Response

```
IPX           TRM   SuperUser       IGX 8430    9.2    Date/Time Not Set

Conn:  31.1.8     IPX         31.2.8      atc12


                                                            Status: OK


Path:   Route information not applicable for local connections




IPX       FTC:   OK                    IPX       FTC:   OK
          FTI:   OK                              FTI:   OK
          FastPAD: OK                            FastPAD: OK

Last Command: dspcon 31.1.8


Next Command:
```

Table 16-33 dspcons – Optional Parameters

start channel	Specifies the channel to begin the display. <start channel> is specified in one of the following formats: slot.port.DLCI—Frame Relay channel remote node.groupname—Frame Relay group connection If no starting channel is specified, the display begins with the first connected channel. All FastPAD connections are shown as part of Frame Relay connections on the IPX.
node name	Specifies that only connections to this remote node from the local note be displayed. If no "nodename" is designated, connections from the local node to all other nodes are displayed

Table 16-33 dspcons – Optional Parameters (Continued)

start channel	Specifies the channel to begin the display. <start channel> is specified in one of the following formats: slot.port.DLCI—Frame Relay channel remote node.groupname—Frame Relay group connection If no starting channel is specified, the display begins with the first connected channel. All FastPAD connections are shown as part of Frame Relay connections on the IPX.
connection type	Specifies that only connections of this type be displayed. If no "connection type" is designated, all connections appear. Valid connection types are: **-f**—Displays all FastPAD and Frame Relay connections. **+d** **+g** When you enter the connection type on the command line, it must be preceded with a hyphen, "-".
+d	Specifies that the display show the connection string in place of the usual compression and ownership fields.
start channel	Specifies the channel to begin the display. <start channel> is specified in one of the following formats: slot.port.DLCI—Frame Relay channel remote node.groupname—Frame Relay group connection If no starting channel is specified, the display begins with the first connected channel. All FastPAD connections are shown as part of Frame Relay connections on the IPX.

dspfp

Displays the header identifying the shelf slot and port of the specified FastPAD and a listing of the cards within that FastPAD. The header contains a blinking "off line" indicator when the FastPAD is unreachable. The card listing includes the base card and all expansion slot cards within FastPAD. A revision level and status field are included for each card. The status field values are:

- Active Card in use.
- Empty No card installed in slot.
- Failed Card failed.
- Standby Card in standby mode

Full Name

Display FastPAD card information

Syntax

dspfp parameter

Related Commands

addfp, delfp, dspfps

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX	No

Example 1

`dspfp 31.1`

Description

Display 31.1 card information

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set


                    FastPAD FP1      at shelf 31.1
    Card
    Type       Status

 B  BASE       Active                  | Lock Status:   Locked
 1  Empty                              | Composite Link: BASE.8
 2  Empty
 3  Empty
 4  VFC-01     Active(SWITCHED)
 5  Empty
 6  Empty
 7  Empty
 8  VFC-01     Standby


Last Command: dspfp 31.1


 Next Command: dspftcport
```

Table 16-34 dspfp – Parameters

Parameter	Description
slot.port	Specifies the slot and port for which information will be displayed.

dspfps

Displays a list of all FastPADs connected to an IPX node. The list includes the FastPAD name, ID, source DLCI, destination DLCI and alarm status (OK, Minor or Major). A FastPAD/IPX connectivity is added or deleted with the **addfp** and **delfp** commands respectively.

Full Name

Display information for all FastPADs

Syntax

dspfps

Related Commands

addfp, delfp, dspfp

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX	No

Example 1

`dspfps`

Description

Display card information for all FastPADs

System Response

```
cc7          VT    SuperUser      IGX 8430    9.2     Mar. 21 1998 15:39 PST

                        FastPADs Information

 Slot.Port  Name       ID  FP_DLCI  Port_ID  Alarm

   31.2     cc7FP       5       53        0  OK









Last Command: dspfps


Next Command:
```

dspfrport

Displays one of three choices; the state of all Frame Relay ports in a FastPAD, general information on all ports on the FRAM-01 card used for Frame Relay connections, or detailed status on a single specified Frame Relay port. The more specific the port address in the command, the more detail is provided. The following are examples of the **dspfrport** command:

dspfrport FTC_slot.port	displays all Frame Relay ports in a FastPAD
dspfrport FTC_slot.port.FPslot	displays the port states at the FastPAD card level
dspfrport FTC_slot.port.FPslot.port	detailed display of the designated FastPAD FRAM-01 port

Table 16-35 provides a list of displayed port parameters for a single port. A full description of these parameters is provided in the **cnffrport** command.

Table 16-35 Frame Relay Port Parameters

Parameters	Description
Port number	Polling Verification Timer
DLCI number	Error Threshold
State: Active or inactive	Monitored Events Count
Interface Type: V.35 or X.21, DCE or DTE	Priority Communicated
Configured clock speed in kbps	The lead states in the Interface Control Template
Measured clock speed in kbps	Receiver Not Ready Thresholds
The port VC queue depth in bytes	Flags per frame
The VC queue ECN threshold in bytes	OAM FastPacket Threshold (for NNI ports)
The DE threshold	Link Integrity Timer (for NNI ports FRP rev. F/H or above)
The signaling Protocol	Full Status Polling cycle (for NNI ports)
Asynchronous Status	The lead states in the Interface Control Template

Full Name

Display Frame Relay port

Syntax

dspfrport

Related Commands

cnffrport, upfrport, dnfrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX	

Example 1

dspfrport

Description

Display the port status of the FRPs in the node

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Mar. 15 1998 15:48 PST

FRP Port States
Port  ID   State
9.2   0     ACTIVE
9.2   0     ACTIVE
9.3   0     INACTIVE
9.4   0     INACTIVE









Last Command: dspfrport


Next Command:
```

Example 2

dspfrport 8

Description

Display the port status for the FRP in slot 8.

System Response

```
D2.ipx6        TRM   YourID:1        IGX 8420    9.2.B1    Aug. 12 1998 13:47 PST

Port configuration for FRP 8

Port   ID       Speed     Interface           State       Protocol     Port Type
1      0        256       FRI-V35 (DCE)       ACTIVE      None         FR
2      0        256       FRI-V35 (DCE)       ACTIVE      None         FR
3      0        256       FRI-V35 (DCE)       FAILED      Annex A UNI FR
4      0        256       FRI-V35 (DCE)       ACTIVE      Annex D UNI FR




Last Command: dspfrport 8


Next Command:
```

Example 3

dspfrport 5.1

Description

Display the port statuses for the Frame Relay port 5.1

System Response

```
D2.ipx5        TRM   YourID:1        IGX 8420    9.2    Aug. 4 1998 16:39 PST

Port:       5.1               [ACTIVE ]
Interface:     FRI-X21 DCE     Configured Clock:     256     Kbps
Clocking:     Normal     Measured Rx Clock:     256     Kbps
Port Type     FR          Min Flags / Frames     1
Port ID     0
Port Queue Depth     65535          OAM Pkt Threshold3pkts
ECN Queue Threshold     65535          T391 Link Intg Timer     6          sec
DE Threshold     100     %     N391 Full Status Poll     10     cyl
Signalling Protocol     None          ForeSight (CLLM)     No
Asynchronous Status     No          CLLM Status Tx Timer     0     msec
T392 Polling Verif Timer     15          IDE to DE Mapping     Yes
N392 Error Threshold     3          Interface Control Template
N393 Monitored Events Count     4          Lead     I
Communicate Priority     No          State     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dspfrport 5.1


Next Command:
```

dspftcport

Displays one of three choices; the state of all FTC ports in a node, general information on all four ports on a specified FTC card, or detailed status on a single specified FTC port. The more specific the port address in the command, the more detail is provided. The following are examples of the **dspftcport** command:

dspftcport	displays states of all FTC ports in the node
dspftcport 8	displays the port states for FTC in slot 8
dspftcport 8.1	displays the configuration for port 1 of the FTC in slot 8

Parameters displayed by the **dspftcport** command are shown in Table 16-36:

Table 16-36 dspftcport – Parameter

Parameters	Description
Speed	The port clock speed in Kbps. Speed configured is displayed as Configured Clock. Actual clock rate is displayed as Measured Clock. The available speeds are 19.2 Kbps, 38.4 Kbps, 56 Kbps, 64 Kbps, 128 Kbps.
Clocking	The port clock type (normal/looped) [normal].
Port queue depth	The maximum bytes queued for transmission from the FTC. Range is 0 to 65535. Default is 65535.
ECN queue threshold	The maximum bytes queued for transmission from the FTC. Range is 0 to 65535. Default is 65535.
Update protocol ID	The lead states in the Interface Control Template
Measured clock speed in kbps	The update protocol supported. The default is 2. The following values are defined as follows: 0—None 1—ANSI T1.617 Annex D 2—LMI Revision 1

Full Name

Display FTC port configuration

Syntax

dspftcport

Related Commands

cnfftcport, upftcport, dnftcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX	No

Example 1

dspftcport

Description

Display the port status of the FTCs on the node

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

FTC Port States
Port ID   State     Type
31.1 0    ACTIVE    FR
31.2 0    ACTIVE    FR
31.3 0    ACTIVE    FR
31.4 0    ACTIVE    FR









 Last Command: dspftcport


Next Command:
```

Example 2

dspftcport 31.1

Description

Display the status of FTC port 31.1, slot 31, port 1.

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Port:       31.1               [ACTIVE  ]
Interface:  FTI-V35 DCE                        Configured Clock:    64 Kbps
Clocking:   Normal                             Measured Rx Clock:   64 Kbps
Port Type                      FR       Min Flags / Frames           1
Port ID                         0
Port Queue Depth            65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold         65535       T391 Link Intg Timer         6 sec
DE Threshold                  100 %     N391 Full Status Poll       10 cyl
Signalling Protocol   STRATA LMI       ForeSight (CLLM)            No
Asynchronous Status            No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer       15       IDE to DE Mapping          Yes
N392 Error Threshold            3       Interface Control Template
N393 Monitored Events Count     4          Lead    CTS    DSR    DCD
Communicate Priority           No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dspftcport 31.1


Next Command:
```

dspict

Displays interface control template information for FastPAD data channels. The displayed information includes:

- The specified channel.
- The type of template: a or ACTIVE is the only valid for FASTPADs.
- The associated output leads and their status:

  ON
  OFF
  Following a local input
  Following a remote input

The input being followed, where applicable, is specified. Any RTS to CTS delay is also shown.

Full Name

Display interface control template

Syntax

dspict parameters

Related Commands

cnfict, cpyict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	No	No	IPX	No

Example 1

`dspict 31.1.8.1 a`

Description

Display the active interface control template for channel 31.1.8.1

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Data Channel:      31.1.8.1
Interface:         RS232       DCE
Clocking:          External


            Interface Control Template for Connection while Active

      Lead       Output Value                Lead       Output Value
      DSR        ON                          RTS        N/A
      DCD        Remote RTS                  CTS        Local RTS
                                             CTS Delay  12 (x10 msec)





Last Command: dspict 31.1.8.1 a


Next Command:
```

Table 16-37 dspict – Parameters

Parameter	Description
channel	Specifies the channel in the format slot.port.subslot.subport
template	Specifies the control template to display for the channel. There is only one template available for FastPAD data channels: "a" for the ACTIVE template.

prtchcnf

Prints the configuration details for FTC channels. This command uses the same syntax, and prints the same information as is displayed using the **dspchcnf** command. See the **dspchcnf** command for syntax and output information.

Full Name

Print channel configurations

Syntax

prtchcnf parameters (see the **dspchcnf** command)

Related Commands

dspchcnf

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IPX	No

prtcons

Prints a summary of connections terminated at the IPX node. This command uses the same syntax and prints the same information as is displayed using the **dspcons** command. See the **dspcons** command for syntax and output information.

Full Name

Print connection

Syntax

prtcons parameters optional parameters (see the **dspcons** command)

Related Commands

dspcons

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	IPX	Yes

prtict

Prints a data channel's interface control template. This command uses the same syntax, and prints the same information as is displayed using the **dspict** command. See the **dspict** command for syntax and output information.

Full Name

Print interface control template

Syntax

prtict parameters (see the **dspict** command)

Related Commands

dspict

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	IPX	Yes

resetfp

This command reboots a FastPAD.

Full Name

Reset FastPAD

Syntax

resetfp parameters

Related Commands

addfp, delfp, dspfp, dspfps

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
resetfp 31.1
```

Description

Restart port 31.1 on the FTC card

Table 16-38 resetfp – Parameters

Parameter	Description
slot.port	Specifies the slot and the port of the FTC card connecting the FastPAD.

restartfp

This command restarts a FastPAD to IPX control session. A control session is first established when a FastPAD is added to the node and the port speed and parameters match. Once a control session is established, the FastPAD can be configured and managed by commands issued at an IPX node.

Full Name

Restart FastPAD session establishment

Syntax

restartfp parameters

Related Commands

addfp, delfp, dspfp, dspfps

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
restartfp 31.1
```

Description

Restart port 31.1 on the FTC card

Table 16-39 restartfp – Parameters

Parameter	Description
slot.port	Specifies the slot and the port of the FTC card connecting the FastPAD whose session is to be reestablished.

upfrport

Activates a single port on an FRP. If the port has not been configured, the default configuration values are used to configure the port.

Full Name

Up Frame Relay port

Syntax

upfrport parameter

Related Commands

dnfrport, cnffrport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
upfrport 9.2
```

Description

Activate port 2 on the FRP in slot 9

System Response

```
alpha          TRM   YourID:1        IGX 8420    9.2    Mar. 15 1998 15:51 PST

Port:        9.2               [ACTIVE ]
Interface:   FRI-V35 DTE                          Configured Clock:   256 Kbps
Clocking:    Normal                               Measured Rx Clock:    0 Kbps
Port ID                         4
Port Queue Depth            65535       OAM Pkt Threshold             3 pkts
ECN Queue Threshold         65535       T391 Link Intg Timer          6 sec
DE Threshold                  100 %     N391 Full Status Poll        10 cyl
Signalling Protocol          None       ForeSight (CLLM)             No
Asynchronous Status            No       CLLM Status Tx Timer          0 msec
T392 Polling Verif Timer       15       Interface Control Template
N392 Error Threshold            3          Lead       State
N393 Monitored Events Count     4           RTS        ON
Communicate Priority           No           DTR        ON
Upper/Lower RNR Thresh  75%/ 25%
Min Flags / Frames             1

Last Command: upfrport 9.2


Next Command:
```

Table 16-40 upfrport – Parameters

Parameter	Description
slot	Specifies slot number of the FRP card containing the port to be upped.
port	Specifies the port to be upped. Range is 1-4.

upftcport

Activates a single port on an FTC. If the port has not been configured, the default configuration values are used to configure the port.

Full Name

Up FTC port

Syntax

upftcport parameter

Related Commands

dnftcport, cnfftcport

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	IPX	Yes

Example 1

```
upftcport 31.1
```

Description

Activate port 1 on the FTC in slot 31

System Response

```
IPX            TRM   SuperUser       IGX 8430    9.2     Date/Time Not Set

Port:       31.1               [ACTIVE  ]
Interface:  FTI-V35 DCE                       Configured Clock:    64 Kbps
Clocking:   Normal                            Measured Rx Clock:    0 Kbps
Port Type                     FR       Min Flags / Frames           1
Port ID                        6
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer         6 sec
DE Threshold                 100 %     N391 Full Status Poll       10 cyl
Signalling Protocol   STRATA LMI       ForeSight (CLLM)            No
Asynchronous Status           No       CLLM Status Tx Timer         0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead    CTS    DSR    DCD
Communicate Priority          No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: upftcport 31.1


Next Command:
```

Table 16-41 upftcport – Parameters

Parameter	Description
slot . port	Specifies slot and port number on the FTC card to be upped.

VSI Commands

Virtual Switch Interface (VSI) is a common control interface for MSSBU switches such as the BPX 8650 and the MGX 8850. Virtual Switch Interfaces (VSIs) allow a node to be controlled by multiple controllers, such as MPLS (Multiprotocol Label Switching, formerly called Tag Switching) and PNNI.

When a virtual switch interface (VSI) is activated on a port, trunk, or virtual trunk so that it can be used by a master controller, such as a SES PNNI or an MPLS controller, the resources of the virtual interface associated with the port, trunk or virtual trunk are made available to the VSI. These control planes can be external or internal to the switch. The Virtual Switch Interface provides a mechanism for networking applications to control the switch and use a partition of the switch resources.

VSI was implemented first on the BPX 8650 in Release 9.1, which uses VSI to perform Multiprotocol Label Switching. Release 9.1 allowed support for VSI on BXM cards and for partitioning BXM resources between Automatic Routing Management (formerly called AutoRoute) and a VSI-MPLS controller. In this release, you can configure partition resources to be shared between Automatic Routing Management PVCs and one VSI control plane, but not both. In this release, you can configure partition resources between Automatic Routing Management PVCs and two VSI controllers (LSC or PNNI).

The second implementation of VSI on the BPX provides the following extended functionality:

- class of service templates,
- virtual trunks support for VSI,
- support for VSI master redundancy,
- multiple VSI partitions, and
- SV+ support for VSI.

Caution VSI is supported in this release. You can use the VSI features (such as to configure a VSI-MPLS controller or a PNNI controller). You can still configure and use Automatic Routing Management PVCs. Refer to the **cnfrsrc** command in Chapter 4, “Setting Up Trunks” and Chapter 5, “Setting Up Lines” for information on configuring Automatic Routing Management PVCs.

Label Switching on the BPX 8650

Label switching enables routers at the edge of a network to apply simple packets (frames), allowing devices in the network core to switch packets according to these labels with minimal lookup activity. Label switching in the network core can be performed by switches, such as ATM switches, or by existing routers.

For more overview information and specific information on how to configure a BPX 8650 switch and a 7200 or 7500 router for MPLS operation, refer to the *Cisco BPX Series Installation and Configuration* and *Cisco BPX 8600 Series Reference*.

Commands Used to Configure VSIs

Following is a list of commands you use to configure VSIs. Refer to each specific command description later in this chapter.

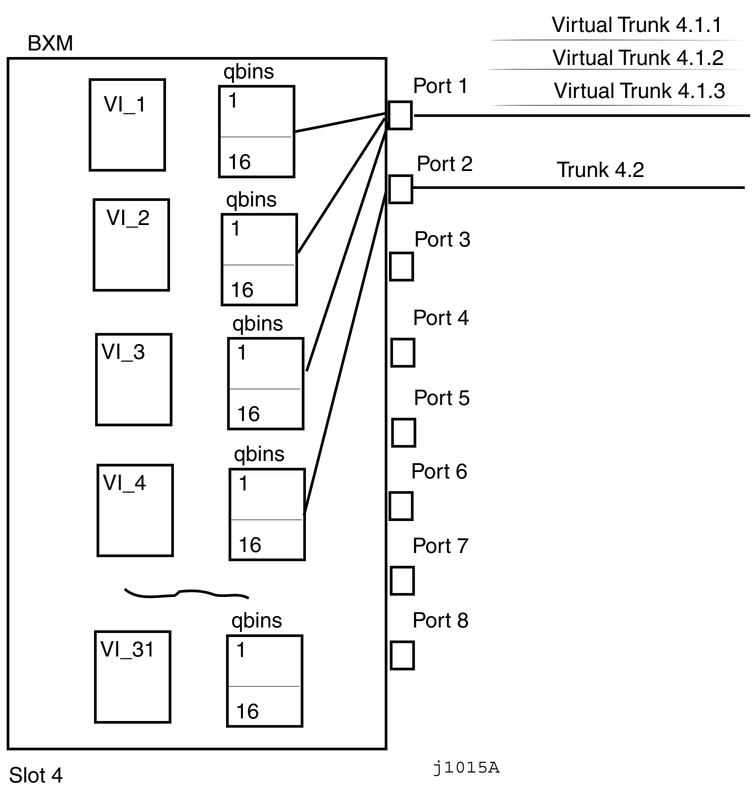
- **addctrlr**
- **addshelf**
- **cnfqbin**
- **cnfsvsiif**
- **cnfvsipart**
- **delctrlr**
- **dnport**
- **dspchuse**
- **dspctrlrs**
- **dntrk**
- **dspnode**
- **dspqbin**
- **dspqbint**
- **dsprsrc**
- **dspsct**
- **dspvsiif**
- **dspvsipartcnf**
- **dspvsipartinfo**
- **upport**
- **uptrk**

Introduction to Virtual Switch Interface

The BXM has 31 virtual interfaces that provide a number of resources including qbin buffering capability. With physical lines and trunks, one virtual interface is assigned to each port.

With virtual trunking, a physical trunk can comprise a number of logical trunks called virtual trunks, and each of these virtual trunks is assigned the resources of one of the 31 virtual interfaces on a BXM. Each virtual trunk equates to a virtual interface. You can enable a virtual switch interface on a port, trunk, or virtual trunk. The virtual switch interface will be assigned the resources of the associated virtual interface. See Figure 17-1 for an illustration of how BXM virtual interfaces (VIs) map to their associated qbins.

Figure 17-1 BXM Virtual Interfaces and Qbins



Each virtual interface has 16 qbins assigned to it. Qbins 0–9 are used for Automatic Routing Management and 10–15 are available for use by a VSI enabled on the virtual interface. (In Release 9.1, only qbin 10 was used. In this release, the qbins 10–15 support class of service (CoS) templates on the BPX.

Note Multiprotocol Label Switching (MPLS, called Tag Switching in Release 9.1) is a technology that Cisco has introduced which summarizes routing decisions in a way that enables switches to perform IP forwarding, as well as bringing other benefits that apply even when Label Switching is used in router-only networks. Label Switching integrates virtual circuit switching with IP routing to offer scalable IP networks over ATM providing multiservice ATM networks. For more information on configuring Multiprotocol Label Switching, see the *Cisco BPX Series Installation and Configuration* and *Cisco BPX 8600 Series Reference* guides.

Adding a VSI-based (Virtual Switch Interface) controller such as the Label Switching Controller (LSC) to the BPX is similar to adding an MGX 8220 interface shelf to the BPX. For example, you use the **addshelf** command to add the MPLS (Multiprotocol Label Switching) Controller to any BXM trunk.

You use the vsi option of the **addshelf** command identify VSI controllers and distinguish them from feeders.

You use **addctrlr** to add a SES PNNI controller to a BPX node through an AAL5 interface shelf or feeder type configured with VSI controller capabilities. See "Adding a Controller" later in this chapter.

The VSI controllers are allocated a partition of the switch resources. VSI controllers manage their partition through the VSI protocol. The controllers run the VSI master. The VSI master entity interacts with the VSI slave running on the BXMs through the VSI interface to set up VSI connections using the resources in the partition assigned to the controller. If you are adding two controllers that are intended to be used in a redundant configuration you must specify the same partition when you add them to the node by using the **addshelf** command.

After first using the **delshelf** command to delete the controller from the network, you then need to down the port and trunk with the **dnport** and **dntrk** commands.

VSI Terms and Acronyms

These terms relate to Virtual Switching Interface and MPLS (Multiprotocol Label Switching):

ATM Edge LSR

A label switching router that is connected to the ATM-LSR cloud through LC-ATM interfaces. The ATM edge LSR adds labels to unlabeled packets and strips labels from labeled packets.

ATM-LSR

An ATM-LSR is a MPLS (Multiprotocol Label Switching) router in which packets are forwarded by switching cells rather than frames, and all packet interfaces are MPLS (Label) Controller-ATM interfaces.

A label switching router with a number of LC-ATM interfaces. The router forwards the cells from these interfaces using labels carried in the VPI and/or VCI field.

BCC

The switch control card in the BPX is the Broadband Control Card, which has a 68040 processor.

BPX

A high-end ATM switch called the Cisco Broadband Packet Exchange (BPX). The BPX is a carrier-quality switch, with trunk and CPU hot standby redundancy.

BPX-LSR

An ATM label switch router consisting of a label switch controller (series 7200 or 7500 router) and a label controlled switch (BPX switch).

BXM

The Broadband Switch Module (BXM) cards are ATM port cards for the BPX switch that use the Monarch chipset. Various different port configurations are supported by the BXM card: 8× DS3, 12× DS3, 4× OC-3, 8× OC-3, 1× OC-12 or 2× OC-12. The Monarch architecture supports up to 64K bi-directional cross-connect legs per BXM card, although only 16k or 32k options are supported in the first release. The BXM has very flexible input and output queueing facilities, a SAR (Segmentation Assembly and Reassembly) capability, and a MIPS 4650 control processor.

Class of Service (CoS) Buffer

A buffer or queue that serves connections with similar QoS requirements. Also called "qbin" (though a qbin is a platform-specific instance, such as a BXM card, of the more general Class of Service Buffer (CoSB).

Class of Service (CoS) Buffer Descriptor Template

A component of a Service Class Template that contains Class of Service Buffer configurations indexed by CoSB number.

Note A qbin is a platform-specific (BXM in this case) instance of the more general Class of Service Buffer (or CosB).

CLI

There are two separate Command-Line Interfaces on the BPX-LSR: One on the BPX itself and one on the MPLS (Multiprotocol Label Switching) Controller. The Control Point integrate these into a single command line interface.

CommBus

The CommBus is the BPX's internal messaging protocol. The Switch Control Interface (SCI) that is used by PNNI on the ESP (Extended Services Processor) is based on CommBus messaging accessed through interfaces to the BPX cards.

CosB

See Class of Service (CoS) Buffer.

ESP

The Extended Services Processor (ESP) is the controller on which the BPX's PNNI implementation runs. It is SPARC-based. The Extended Services Processor 2.0 is an example of an adjunct processor shelf (formerly called an APS). Note that APS, or Automatic Protection Switching, is a feature introduced in Release 9.2.

Feeder

A feeder is a small switch that acts as an extension shelf, typically with lower-bandwidth interfaces, for a larger switch. The larger switch is referred to as the Routing node with the feeder(s) it supports. Collectively, the feeder(s) and routing node form a type of supernode.

LC-ATM Interface

A Label Controlled ATM interface is a MPLS (Multiprotocol Label Switching) interface where labels are carried in the VPI/VCI bits of ATM cells, and where VC (virtual circuit) connections are established under the control of MPLS (Multiprotocol Label Switching) control software.

LCN

Each interface card in a BPX has a certain number of Logical Connection Numbers. A Logical Connection Number is used for each cross connect leg through the card in question. "LCN" is often roughly synonymous with "cross connect leg". In VSI terminology, an LCN is an example of an Other End Reference.

Logical Interface

Each physical interface and every virtual trunk endpoint on a platform is represented to the VSI controllers as a different logical interface with partitions, and other VSI configuration. Logical Interface numbers are 32-bit with a format which is, in general, known only to the platform.

LSR

Label Switching router, which is an MPLS (Multiprotocol Label Switching) router.

PNNI

Private Network-to-Network Interface controller software that runs on the SES hardware platform. The term PNNI controller and SES may be used interchangeably.

Port

The VSI makes no distinction between trunk ports and end-point ports. "Port" is synonymous with "Interface".

Routing Node

In tiered networks terminology, a routing node is a larger switch to which one or more feeders is attached. Collectively, the feeder(s) and routing node form a type of supernode.

Service Class (aka Service Type)

A concept for grouping connections that share a common set of traffic characteristics and QoS requirements. The terms "service class" and "service type" are sometimes used interchangeably.

Note In this release, there are some major service categories, such as VbrRt, VbrNRt, CBR, Abr, and Ubr, and under these major service categories are service types such as VbrRt1, VbrRt2, VbrRt3, and VbrNRt1, VbrNrt2, and so on. Sometimes the terms service class and service type are used interchangeably.

Service Class database

The collection of data items that support the service class template concept, and implemented on a per-VI basis on the BXM. These items include a copy of the specific Service Class Template selected for a VI, as well as additional data as required.

Service Class Template (SCT):

A set of data structures that map VSI service types to sets of pre-configured VC and Qbin parameters. Consists of two sub-components—a VC Descriptor Template and a Class of Service Buffer descriptor template.

VC

ATM and Frame Relay traffic is carried in Virtual Channels which are set up between adjacent ATM or Frame Relay switches before data transmission occurs. An ATM link between switches may support up to 2^{28} different VCs, although a small number of VCs is reserved for special purposes.

VCI

Each VC within a specific Virtual Path on a link has a unique Virtual Channel Identifier, which is a 16-bit number.

VC Descriptor Template

A component of a Service Class Template which contains platform-specific VC configurations that are indexed primarily by service type. Together with a Class of Service Buffer (CoSB) descriptor template, it defines a Service Class Template (SCT).

VP, VPC, VPI

A Virtual Path is a bundle of 2^{16} Virtual Connections with the same Virtual Path Identifier, that is, the first 12 bits of the VPCI. Most ATM switches can switch VPs using only a single cross-connect (instead of up to 2^{16}). An end-to-end sequence of VPs cross-connected at the intermediate swi5tches is a Virtual Path Connection.

VPCI

Each VC on a link has a unique Virtual Path and Channel Identifier, which is a 28-bit number. The VPCI consists of a 12-bit VPI concatenated with a 16-bit VCI.

Virtual Trunks

A Virtual Trunks is a Virtual Path Connection which appears to VSI masters as ordinary trunk (except that the trunk supports 64k VCs at most). In a VSI platform, a virtual trunk endpoint has its own logical interface.

VSI

Virtual Switch Interface: this is a proposed common control interface to all Cisco MSSBU switches. It embodies both connection management and switch configuration discovery capabilities.

VSI 2

Virtual Switch Interface, Protocol Version 2: this is revision 2 of a proposed common control interface to all MSSBU switches. It embodies both connection management and switch configuration discovery capabilities.

VSI Controller

A controller, such as a PNNI SVC Controller, Portable AutoRoute or Label Switch Controller, which controls a switch using the VSI.

VSI Master

A VSI master process implementing the master side of the VSI protocol in a VSI controller. Sometimes the whole VSI controller might be referred to as a “VSI Master”, but this is not strictly correct.

1) A device that controls a VSI switch, for example, a VSI Label Switch Controller.

2) A process implementing the master side of the VSI protocol.

VSI Slave

1) A switch (in the “Single Slave model”) or a port card (in the “Multiple Slave Model”) that implements the VSI.

2) A process implementing the slave side of the VSI protocol.

Adding a Controller

To add a MPLS controller (or a generic VSI controller that does not need AnnexG protocol):

Step 1 **uptrk**—to up the trunk

Step 2 **addshelf**—with feeder type set to “V” to add an MPLS controller

Step 3 **dspnode**—to display the controllers and interface shelves attached to the node

Step 4 **dspctrlrs**—to display the VSI controllers, such as an PNNI controller, on a BPX node.

Note that **addshelf** and **addtrk** are mutually exclusive commands; that is, you can use either **addshelf** or **addtrk**, but not both on the same interface shelf.

To add a PNNI controller, use the following commands:

Step 1 **uptrk**—to up a trunk interface

Step 2 **cnfrsrc**—to configure resource on the trunk interface for the PNNI controller's control channels

Step 3 **addshelf**—with feeder type set to “X” to add the SES to the BP and enable AnnexG protocol to run between the BPX and the SES.

Step 4 **addctrlr**—to enable the VSI capabilities on the Trunk interface.

Viewing Controllers and Interfaces

Display commands such as **dspnw** and **dspnode** show interface shelves.

To view conditions on an interface shelf (feeder) trunk, use:

- **dspnode**—Identifies the hub and interface shelf (feeder) nodes and shows the alarm status.

To view conditions of VSI controllers, use:

- **dspctrlrs**—Displays all VSI controllers attached to the BPX. These controllers could be either a PNNI controller or an MPLS controller.

The designation for an MGX 8220 interface shelf is AXIS. The designation for a MPLS (Multiprotocol Label Switching) Controller serving as an interface shelf is LSC. Note that you add a controller in the same way you connect an interface shelf such as an MGX 8220 (AXIS) to a node such as a BPX.

Deleting a Controller

To delete an interface (feeder) shelf, use **delshelf**. You must first delete the interface shelf or controller to remove the controller from the network, then down the port and trunk with the **dnport** and **dntrk** commands.

To delete a MPLS controller or a generic VSI controller that does not need AnnexG protocols:

- **delshelf**—delete a MPLS controller from a BPX node.
- **dntrk**—to down a trunk

To delete a PNNI controller:

Step 1 **delctrlr**—to delete the VSI capabilities on the trunk interface.

Step 2 **delshelf**—to delete the SES attached to the trunk interface.

Step 3 **cnfrsrc**—to disable the VSI resource partition allocated for PNNI controller on the trunk interface

Step 4 **dntrk**—to down the trunk interface, provided no other VSI partitions are active on the trunk interface

For more information on adding VSI controllers to BPX nodes, refer to the *Cisco BPX 8650 Series Installation and Configuration* guide.

Enabling VSI ILMI Functionality

You can enable VSI ILMI functionality both on line (port) interfaces and trunk interfaces. Note that VSI ILMI functionality cannot be enabled on trunks to which feeders or VSI controllers are attached.

To enable VSI ILMI functionality on line (port) interfaces:

Step 1 **upln**—up a line interface

Step 2 **upport**—up the port interface

Step 3 **cnfport**—configure the port to enable ILMI protocol and ensure that the protocol runs on the BXM card by enabling the "Protocol by the card" option

Step 4 **cnfrsrc**—configure a VSI partition on the line interface

Step 5 **cnfvsipart**—to enable VSI ILMI functionality for the VSI partition

To enable VSI ILMI functionality on physical trunk interfaces:

Step 1 **uptrk**—up a physical trunk

Step 2 **cnftrk**—configure the trunk to enable ILMI protocol to run on the BXM card by enabling the "Protocol by the card" option

Step 3 **cnfrsrc**— configure a VSI partition on the trunk interface

Step 4 **cnfvsipart**—to enable VSI ILMI session for the VSI partition

To enable VSI ILMI functionality on virtual trunk interfaces:

Step 1 **uptrk**—up a physical trunk

Step 2 **cnftrk**—configure the trunk VPI
NOTE: ILMI automatically runs on the BXM card for virtual trunks and this is not configurable by using the **cnftrk** command

Step 3 **cnfrsrc**—configure a VSI partition on the virtual trunk interface

Step 4 **cnfvsipart**—to enable VSI ILMI functionality for the VSI partition
NOTE: VSI ILMI can be enabled for only one VSI partition on trunk interface.

To display VSI ILMI functionality on interfaces:

- **dspvsipartcnf**—display VSI ILMI status (whether enabled or not) for various VSI partitions on the interface.

Configuring Partition Resources on Interfaces

Prior to Release 9.1, all the LCNs for a BXM card were managed exclusively by the BCC. With the introduction of VSI in Release 9.1 and after, the BCC must allocate a range of LCNs for use by the BXM card.

When configuring resource partitions on a VSI interface, you typically use the following commands:

- **cnfrsrc**
- **dsprsrc**
- **dspvsipartinfo**
- **dspvsipartcnf**
- **uptrk**
- **upln**
- **upport**

The next step to complete when adding a VSI-based controller such as an LSC (Label Switching Controller) or a PNNI controller is to configure resource partitions on BXM interfaces to allow the controller to control the BXM interfaces. To do this, you must create resource partitions on these interfaces. Use the **cnfrsrc** command to add, delete and modify a partition on a specified interface.

Note This release supports the ability to have multiple VSI controllers on the same partition (referred to as VSI master redundancy). The master redundancy feature allows multiple VSI masters to control the same partition.

See Table 17-1 for a listing of **cnfrsrc** parameters, ranges and values, and descriptions. These descriptions are oriented to actions and behavior of the BXM firmware; in most cases, objects (messages) are sent to switch software. Most of these parameters appear on the **cnfrsrc** screen.

Table 17-1 cnfrsrc Parameters, Ranges/Values, and Descriptions

Parameter (Object) Name	Range/Values	Default	Description
VSI partition	1... 2	1	Identifies the partition
Partition state	0 = Disable Partition 1 = Enable Partition	NA	For Partition state = 1, Objects are mandatory
Min LCNs	0...64K	NA	Min LCNs (connections) guaranteed for this partition.
Max LCNs	0...64K	NA	Maximum LCNs permitted on this partition
Start VPI	0 .. 4095	NA	Partition Start VPI
End VPI	0 .. 4095	NA	Partition End VPI
Min Bw	0 .. Line Rate	NA	Minimum Partition bandwidth
Max Bw	0 .. Line Rate	NA	Maximum Partition bandwidth

Configuring Qbins

Use the following commands to configure qbins:

- **cnfqbin**
- **dspqbin**
- **dspqbint**

Overview of Qbin Templates and How They Are Used by VSI

A qbin template defines a default configuration for the set of qbins for a logical interface. When you assign a template assignment to an interface, the corresponding default qbin configuration is copied to this interface's qbin configuration and becomes the current qbin configuration for this interface. You can then adjust some of the parameters of this configuration on a per-interface basis. Changes you make to the qbin configuration of an interface only affect that interface's qbin configuration, and do not affect the qbin template assigned to that interface.

Qbin templates only deal with qbins that are available to VSI partitions, namely 10 through 15. Qbins 10 through 15 are used by VSI on interfaces configured as trunks or ports. The rest of the qbins are reserved and configured by Automatic Routing Management.

When you execute a **dspsct** command, it will give you the default service type, and the qbin number.

Configuring the BXM Card's Qbin

When you activate an interface, the default template gets assigned to an interface. The corresponding qbin template gets copied into the card's qbin data structure for that interface. When you want to change this by providing new values using the **cnfqbin** command, the qbin is now "user configured" as opposed to "template configured". This information is displayed on the **dspqbin** screen, which indicates whether the values in the qbin are from the template assigned to the interface, or whether the values have been changed to user-defined values.

Qbin Dependencies

The available qbin parameters are shown in Table 17-2. Notice that the qbins available for VSI are restricted to qbins 10–15 for that interface. All 32 possible virtual interfaces are provided with 16 qbins.

Table 17-2 Service Template Qbin Parameters

Parameter Name	Template Units	Template Range/Values
QBIN Number	enumeration	0–15 (10–15 valid for VSI)
Max QBIN Threshold	u sec	1–2000000
QBIN CLP High Threshold	% of max qbin threshold	0 – 100
QBIN CLP Low Threshold	% of max qbin threshold	0 – 100

Table 17-2 Service Template Qbin Parameters (Continued)

Parameter Name	Template Units	Template Range/Values
EFCI Threshold	% of max Qbin threshold	0 – 100
Discard Selection	enumeration	1 – CLP Hysteresis 2 – Frame Discard
Weighted Fair Queueing	enable/disable	0: Disable 1: Enable

Virtual Trunking

In this release, you can configure virtual trunking on the BXM card. Also, VSI controllers let you use BXM virtual trunk interfaces. Using this capability, VSI master controllers can terminate connections on virtual trunk interfaces.

The VSI virtual trunks allows a virtual trunk to be configured as a VSI interface. You configure VSI resources on a virtual trunk using the same command you use to configure physical interfaces. The syntax you use to identify a trunk has an optional virtual trunk identifier that you append to the slot and port information to identify virtual trunk interfaces.

VSI Virtual Trunks in Release 9.2

The *VSI virtual trunking* feature lets you use BXM virtual trunks as VSI interfaces. You activate and configure VSI resources on a virtual trunk using the same commands you use to configure physical interfaces (for example, **cnfrsrc**, **dsprsrc**).

Note In this release, virtual trunk interfaces cannot be shared between VSI and Automatic Routing Management. Therefore, configuring a trunk as a VSI interface prevents you from adding the trunk as an Automatic Routing Management trunk. Similarly, a trunk that has been added to the Automatic Routing Management topology cannot be configured as a VSI interface.

Virtual trunks on the BPX use a single configurable VPI. Because virtual trunk interfaces are dedicated to VSI, the entire range of VCIs is available to the VSI controllers.

Virtual Trunks

The virtual trunking feature introduces the concept of defining multiple trunks within a single trunk port interface. This creates a fan-out capability on the trunk card. Virtual trunking has already been implemented on the BNI cards previous to Release 9.2, and has been extended to work on UXM and BXM cards.

A virtual trunk is a VPC that terminates at each end on the switch port. Each virtual trunk can contain up to 64,000 VCCs, but it may not contain any VPCs. The setup is shown in Table 17-1.

The VSI virtual trunks feature will allow a virtual trunk to be configured as a dedicated VSI virtual trunk. Once VSI is enabled on the virtual trunk, Automatic Routing Management does not include this trunk in its route selection process.

The following is the sequence of events to configure a VSI virtual trunk:

Step 1 uptrk <slot.port.vtrunk> Activate the virtual trunk

Step 2 cnftrk <slot.port.vtrunk> Set up VPI value and trunk parameters

Step 3 cnfrsrc <slot.port.vtrunk> Enable VSI partition

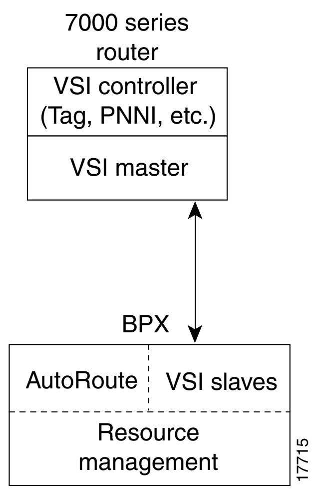
VSI Masters and Slaves

A controller application uses a VSI master to control one or more VSI slaves. For the BPX, the controller application and master VSI reside in an external 7200 or 7500 series router and the VSI slaves are resident in BXM cards on the BPX node (Figure 17-2).

The controller sets up the following types of connections:

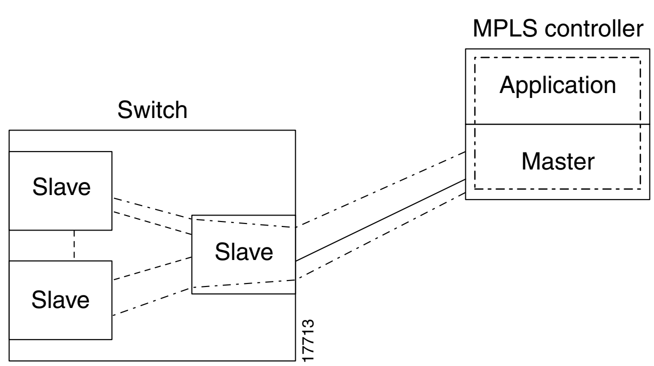
- Control virtual connections (VCs)
  - — Master to Slave
  - — Slave to Slave
- User Connection
  - — User connection (that is, cross-connect)

Figure 17-2 VSI Controller and Slave VSIs



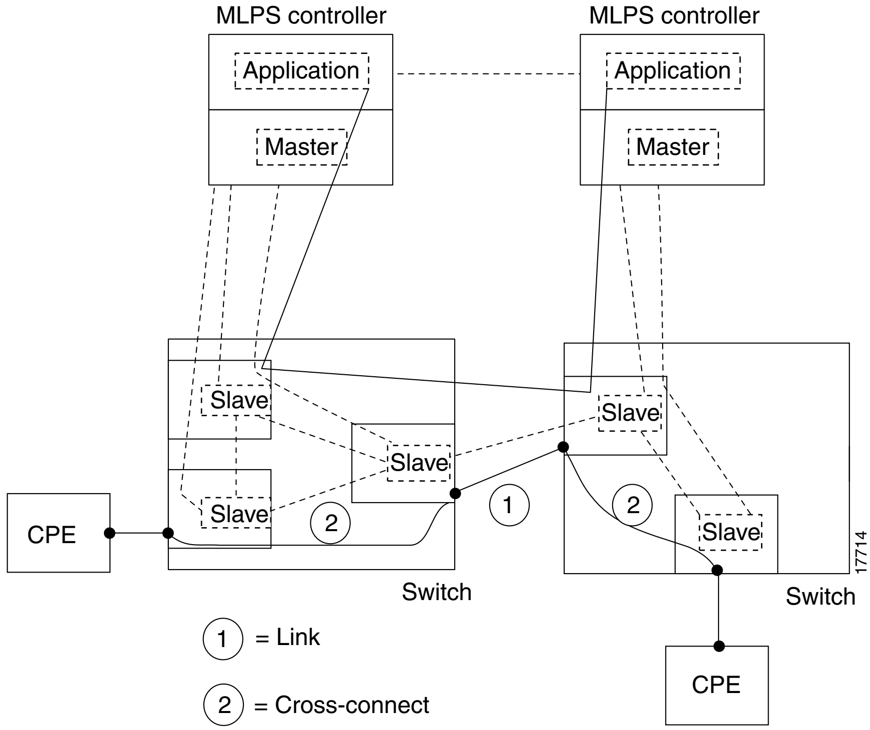
The controller establishes a link between the VSI master and every VSI slave on the associated switch. The slaves in turn establish links between each other (Figure 17-3).

Figure 17-3 VSI Master and VSI Slave Example



With a number of switches connected together, there are links between switches with cross connects established within the switch as shown in Figure 17-4.

Figure 17-4 Cross connects and links between switches



Partitioning

The VSI slaves need to partition the resources between competing controllers: Automatic Routing Management (formerly called AutoRoute) and MPLS (Tag), or Automatic Routing Management and PNNI, for example.

Note Earlier releases supported one partition only. This release supports two partitions.

Release 9.1 supports just one VSI controller type. For example, you can configure a partition's resources between an Automatic Routing Management and a VSI-MPLS controller, or Automatic Routing Management and a VSI-PNNI controller, but you cannot configure both a PNNI and MPLS controller. In this release, you can have both a PNNI controller and an LSC-6400 controller, each in its own partition, controlling the same VSI slave.

The resources that you need to configure for a partition are shown in Table 17-3 for a partition. The three parameters that need to be distributed are number of logical connections (LCNs), bandwidth (BW), and virtual path IDs (VPI).

Table 17-3 Partition Parameters

Partition Parameters	Min	Max
lcns	min_lcns	max_lcns
bw	min_bw	max_bw

Table 17-3 Partition Parameters (Continued)

Partition Parameters	Min	Max
vpi	min_vpi	max_vpi

The controller is supplied with a logical LCN connection number, that is slot, port, and so on., information that is converted to a logical connection number (LCN).

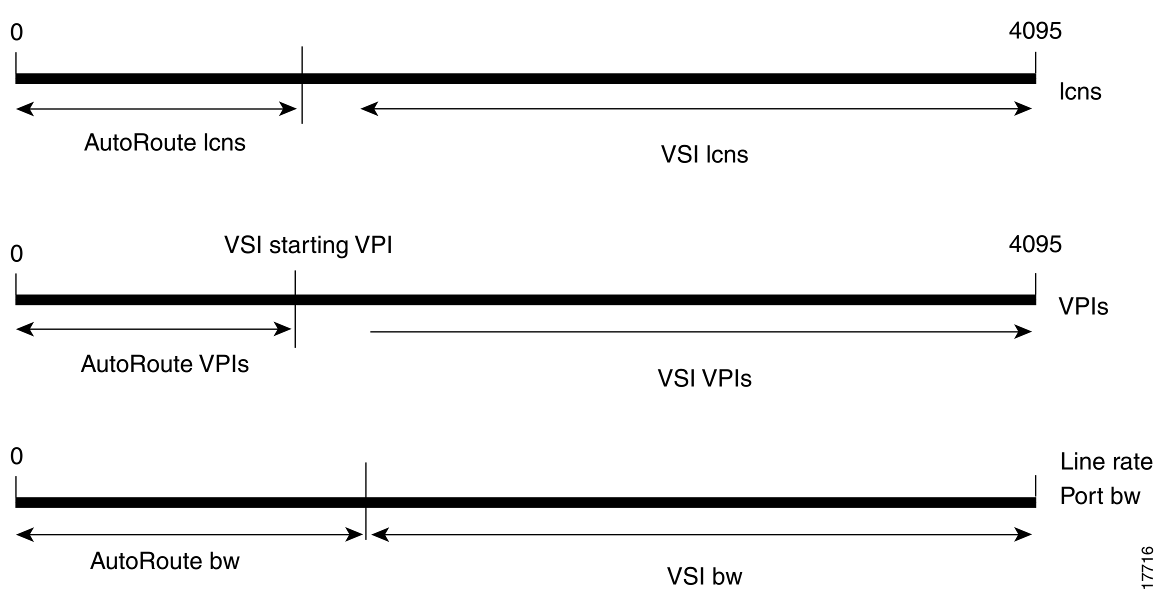
Some ranges of values available for a partition are listed in Table 17-4:

Table 17-4 Partition Criteria

	Range
trunks	1–4095 VPI range
ports	1–4095 VPI range for NNI; 1–256 for UNI
virtual trunk	only one VPI is available per virtual trunk since a virtual trunk is currently delineated by a specific VP
virtual trunk	Each virtual trunk can either be Automatic Routing Management or VSI, not both.

When a trunk is added, the entire bandwidth is allocated to Automatic Routing Management. To change the allocation in order to provide resources for a VSI, you use the **cnfrsrc** command on the BPX switch. A view of the resource partitioning available is shown in Figure 17-5.

Figure 17-5 Graphical View of resource partitioning (Automatic Routing Management and VSI)



Multiple Partitioning

In this release, you can configure partition resources between Automatic Routing Management PVCs and two VSI controllers (LSC or PNNI). Two VSI controllers in different control planes can independently control the switch with no communication between controllers. The controllers are essentially unaware of the existence of other control planes sharing the switch. This is possible because different control planes used different partitions of the switch resources.

You can add one or more redundant LSC controllers to one partition, and one or more redundant PNNI controllers to the other partition. Two new templates have been added for interfaces with multiple partitions controlled simultaneously by a PNNI controller and an LSC.

The master redundancy feature allows multiple controllers to control the same partition. In a multiple partition environment, master redundancy is independently supported on each partition.

These limitations apply to multiple VSI partitioning:

- Only one or two partitions are supported.
- Resources cannot be redistributed amongst different VSI partitions.
- The resources that are allocated to a partition are: LCNS, Bandwidth and VPI range.
- Resources are also allocated to AutoRoute. The resources allocated to AutoRoute can be freed from AutoRoute and then allocated to VSI.
- No multiple partitions on Virtual Trunks. A Virtual Trunk is managed by either AutoRoute or by a single VSI partition.
- Only one controller can be added to a BPX interface. Different controllers must be added to different switch interfaces.

Compatibility

The card uses a flag in the capability message to report multiple partition capability. Firmware releases that do not support multiple partitions set this flag off. The multiple partitions capability is treated as a card attribute and added to the attribute list.

Use of a partition with ID higher than 1 requires support for multiple VSI partitions in both switch software and BXM firmware, even if this is the only partition active on a the card. In a y-red pair configuration, the multiple partition capability is determined by the minimum of the two cards.

A card with no multiple partition capabilities will mismatch if any of the interfaces has an active partition with ID higher than 1. Attempts to enable a partition with ID higher than 1 in a logical card that does not support multiple partitions will be blocked.

Multiple Partition Example

Each logical switch can be seen as a collection of interfaces each with a set of resources associated with it. Consider a BPX switch with 4 interfaces 10.1, 10.2.1, 11.1 and 11.7.1. Also assume the resource partitioning in Table 17-5.

Figure 17-6 Virtual Switches

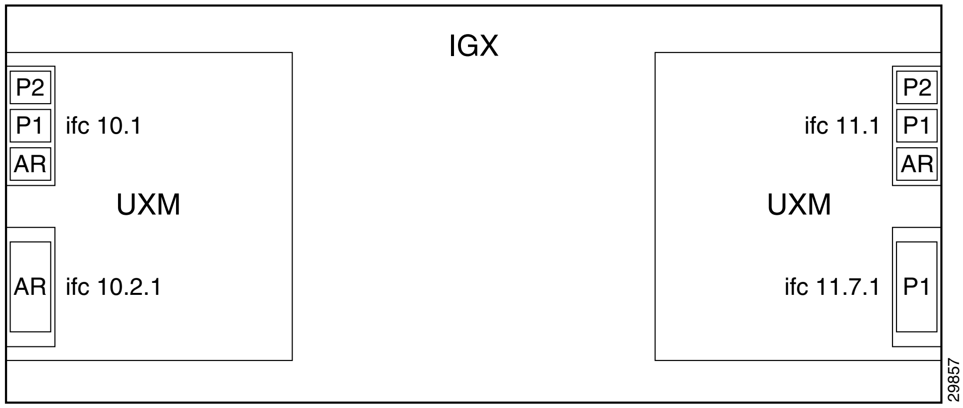


Table 17-5 Partitioning Example

Interface	AutoRoute	partition 1	partition 2
10.1	Enable lcns: 2000 bw: 20000 cps vpi: 1–199	Enable lcns: 4000 bw:30000 cps vpi: 200–239	Enable lcns: 4000 bw: 20000 cps vpi: 240–255
10.2.1	Enable lcns: 10000 bw:10000 cps vpi: 200–200	Disable	Disable
11.1	Enable lcns: 2000 bw: 100000 cps vpi: 1–199	Enable lcns: 3000 bw: 50000 cps vpi: 200–249	Enable lcns:4000 bw: 10000 vpi: 250–255
11.7.1	Disable	Enable lcns: 5000 bw: 200000cps vpi: 250–250	Disable

Three virtual switches are defined by this configuration:

AutoRoute:
10.1: 2000 lcns, 20000 cps, vpi: 1–199;
10.2.1: 10000 lcns, 10000 cps, vpi 200;
11.1: 2000 lcns, 100000 cps, vpi: 1–199}

Partition 1:
10.1: 4000 lcns, 30000 cps, vpi: 200–239;
11.1: 3000 lcns, 50000 cps, vpi: 200–249;
11.7.1: 5000 lcns, 200000 cps, vpi: 250–250}

Partition 2:
10.1: 4000 lcns, 20000 cps, vpi: 240–255;
11.1: 4000 lcns, 10000 cps, vpi: 250–255}

Resource Partitioning

A logical switch is configured by enabling the partition and allocating resources to the partition. This must be done for each of the interfaces in the partition. The same procedure must be followed to define each of the logical switches. As resources are allocated to the different logical switches a partition of the switch resources is defined.

The resources that are partitioned amongst the different logical switches are:

- LCNs
- Bandwidth
- VPI range

Resources are configured and allocated per interface, but the pool of resources may be managed at a different level. The pool of LCNs is maintained at the card level, and there are also limits at the port group level. The bandwidth is limited by the interface rate, and therefore the limitation is at the interface level. Similarly the range of VPI is also defined at the interface level.

You configure the following parameters on a VSI partition on an interface:

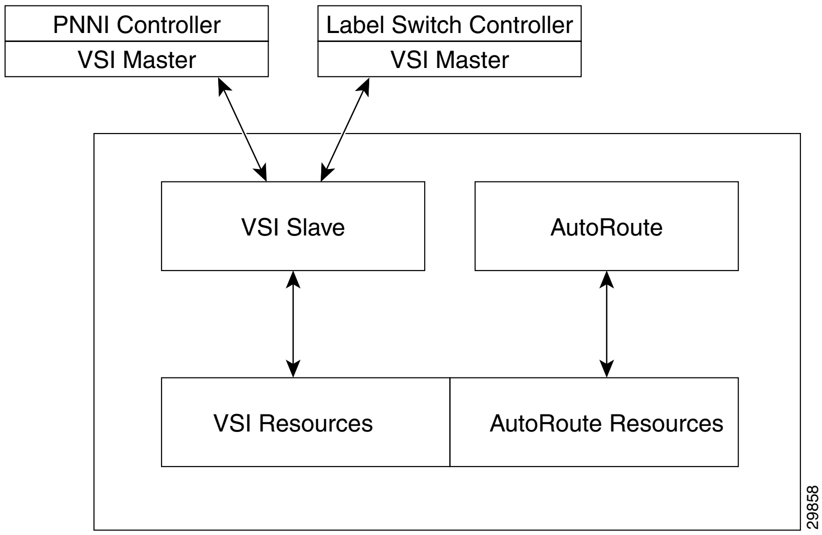
- **min lcn**: guaranteed LCNs for the partition on the interface.
- **max lcn**: total number of LCNs the partition is allowed for setting up connections on the interface.
- **min bw**: guaranteed bandwidth for the partition on the interface.
- **max bw**: maximum bandwidth for this partition on the interface.
- **start vpi**: the lower bound of the VPI range reserved for this partition on the interface.
- **end vpi**: the upper bound of the VPI range reserved for this partition on the interface.

Partitioning between AutoRoute and VSI

In addition to partitioning of resources between VSI and AutoRoute, multiple partitioning allows sub-partitioning of the VSI space amongst multiple VSI partitions. Multiple VSI controllers can share the switch with each other and also with AutoRoute.

The difference between the two types of partitioning is that all the VSI resources are under the control of the VSI-slave, while the management of AutoRoute resources remains the province of the switch software.

Figure 17-7 Resource Partitioning Between AutoRoute and VSI



These commands are used for multiple partitioning:

- **dspvsipartinfo**—display information about the current usage of partition resources.
- **dspchuse**—displays a summary of the channel distribution in a given slot.
- **dspvsiif**—displays the service class template assigned to an interface along with a summary of the resources allocated to each partition.
- **dspvsich**— displays the list and information for the LCNs used for VSI control channels, including inter-slave channels and master-slave controllers for all controllers in all partitions.

VSI Master and Slave Redundancy Functional Overview

This release supports the ability to have multiple VSI controllers (referred to as *VSI master redundancy).* This master redundancy feature enables multiple VSI masters to control the same partition.

You add a redundant controller by using the **addshelf** command, the same way you add an interface (feeder) shelf, except that you specify a partition that is already in use by another controller. This capability can be used by the controllers for cooperative or exclusive redundancy:

- *Cooperative redundancy*, where both controllers can be active in a partition, and can control the resources simultaneously.
- *Exclusive redundancy*, where only one controller is active at a time. It is up to the controllers to resolve who should be active.

The switch software has no knowledge of the state of the controllers. The state of the controllers is determined by the VSI entities. From the point of view of the BCC, there is no difference between cooperative redundant controllers and exclusive redundant controllers. Refer to Figure 17-3 for illustrations of a VSI Master and Slave, and Figure 17-4 for an illustration of a switch with redundant controllers that support master redundancy.

Switch software supports master redundancy in the following ways:

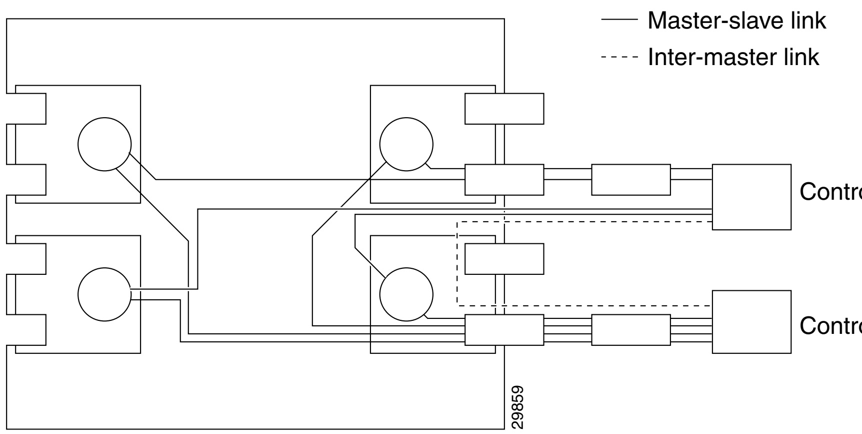
- It allows you to add multiple controllers to control the same partition.

- It sets up the control master-slave VCs between each of the controller ports and the slaves in the node.
- It provides controller information to the slaves. The slave advertises this information to the controllers in the partition. The controllers can then use this information to set up an inter-master channel.

The inter-controller communication channel is set up by the controllers. This could be an out-of-band channel, or the controllers can use the controllers interface information advertised by the VSI slaves to set up an inter-master channel through the switch.

Figure 17-8 below shows a switch with redundant controllers and the connectivity required to support master redundancy.

Figure 17-8 Switch with Redundant Controllers to Support Master Redundancy



Note The controller application and Master VSI reside in an external VSI controller (MPLS or PNNI), such as the Cisco 6400 or the MPLS controller in a 7200 or 7500 series router. The VSI slaves are resident in BXM cards on the BPX node.

VSI Slave Redundancy Mismatch Checking

To provide a smooth migration of the VSI feature on the BXM card, line and trunk Y-redundancy is supported for this feature. You can pair cards with and without the VSI capability as a Y-redundant pair if the feature is not configured on the given slot. As long as the feature is not configured on a given slot, switch software will not perform “mismatch checking” if the BXM firmware does not support the VSI feature.

This release supports a maximum of two partitions. The card uses a flag in the capability message to report multiple partition capability. Firmware releases that do not support multiple partitions set this flag off. The multiple partitions capability is treated as a card attribute and added to the attribute list.

In a y-red pair configuration, the multiple partition capability is determined by the minimum of the two cards. A card with no multiple partition capabilities will mismatch if any of the interfaces has an active partition with ID higher than 1. Attempts to enable a partition with ID higher than 1 in a logical card that does not support multiple partitions are blocked.

Slave Redundancy

Prior to Release 9.2, hot standby functionality was supported only for Automatic Routing Management connections. This was accomplished by the BCC keeping both the active and standby cards in sync with respect to all configuration, including all connections set up by the BCC. However, the BCC does not participate in, nor is it aware of the VSI connections that are set up independently by the VSI controllers. Therefore, the task of keeping the redundant card in a hot standby state (for all the VSI connections) is the responsibility of the two redundant pair slaves. This is accomplished by a bulk update (on the standby slave) of the existing connections at the time that (line and trunk) Y redundancy is added, as well as an incremental update of all subsequent connections.

In the current release, the hot standby slave redundancy feature enables the redundant card to fully duplicate all VSI connections on the active card, and to be ready for operation on switchover. On startup, the redundant card initiates a bulk retrieval of connections from the active card for fast sync-up. Subsequently, the active card updates the redundant card on a real-time basis.

The VSI Slave Hot Standby Redundancy feature provides the capability for the slave standby card to be preprogrammed the same as the active card so that when the active card fails, the slave card switchover operation can be done quickly (within 250 ms). Without the VSI portion, the BXM card already provided the hot standby mechanism by duplicating CommBus messages from the BCC to the standby BXM card.

Master Redundancy

You add a VSI controller, such as an MPLS or PNNI controller by using the **addshelf** command with the *vsi* option. The *vsi* option of the **addshelf** command identifies the VSI controllers and distinguishes them from interface shelves (feeders). The VSI controllers are allocated a partition of the switch resources. VSI controllers manage their partition through the VSI interface. The controllers run the VSI master. The VSI master entity interacts with the VSI slave running on the BXMs through the VSI interface to set up VSI connections using the resources in the partition assigned to the controller. Two controllers that are intended to be used in a redundant configuration must specify the same partition when added to the node with the **addshelf** command.

When a controller is added to the node, switch software will set up the infrastructure so that the controllers can communicate with the slaves in the node. The VSI entities decide how and when to use these communication channels.

In addition, the controllers require a communication channel between them. This channel could be in-band or out-of-band. When a controller is added to the switch, switch software will send controller information to the slaves. This information will be advertised to all the controllers in the partition. The controllers may decide to use this information to set up an inter-master channel. Alternatively the controllers may use an out-of-band channel to communicate.

The maximum number of controllers that can be attached to a given node is limited by the maximum number of feeders that can be attached to a BPX hub. The total number of interface shelves (feeders) and controllers is 16.

The following sections describe some of the communication between the switch software and firmware to support VSI master and slave redundancy.

When Happens When You Add a Controller

You add a controller, including Label Switch Controllers, to a node by using the **addshelf** command. You add a redundant controller in the same way, except that you specify a partition that may already be in use by another controller. The **addshelf** command allows for the addition of multiple controllers that manage the same partition.

Use the **addctrlr** command to attach a controller to a node for the purposes of controlling the node for controllers that require Annex G capabilities in the controller interface. Note that you must first add the shelf by using the **addshelf** command.

You add VSI capabilities to the interface by using the **addctrlr** command. The only interface that supports this capability is an AAL5 feeder interface.

When adding a controller, you must specify a partition ID. The partition ID identifies the logical switch assigned to the controller. In this release, the valid partitions are 1 and 2. The user interface blocks the activation of partitions with ID higher than 1 if the card does not support multiple partitions.

To display the list of controllers in the node, use the command **dspctrlrs**.

The functionality is also available via SNMP using the switchIfTable in the switch MIB.

You can add one or more redundant LSC controller to one partition, and one or more redundant PNNI controller to the other partition.

When using the **addshelf** command to add a VSI controller to the switch, you must specify the controller ID. This is a number between 1 and 32 that uniquely identifies the controller. Two different controllers must always be specified with different controller IDs.

The management of resources on the VSI slaves requires that each slave in the node has a communication control VC to each of the controllers attached to the node. When a controller is added to the BPX with the **addshelf** command, the BCC sets up the set of master-slave connections between the new controller port and each of the active slaves in the switch. The connections are set up using a well known VPI.VCI. The value of the VPI is 0. The value of the VCI is (40 + (*slot* - 1)), where *slot* is the logical slot number of the slave.

Note that once the controllers have been added to the node, the connection infrastructure is always present. The controllers may decide to use it or not, depending on their state.

The addition of a controller to a node will fail if there are not enough channels available to set up the control VCs in one or more of the BXM slaves.

The BCC also informs the slaves of the new controller through a VSI configuration CommBus message (the BPX's internal messaging protocol). The message includes a list of controllers attached to the switch and their corresponding controller IDs. This internal firmware command includes the interface where the controller is attached. This information, when advertised by the slaves, can be used by the controllers to set up an inter-master communication channel.

When the first controller is added, the BCC behaves as it did in releases previous to Release 9.2. The BCC will send a VSI configuration CommBus message to each of the slaves with this controller information, and it will set up the corresponding control VCs between the controller port and each of the slaves.

When a new controller is added to drive the same partition, the BCC will send a VSI configuration CommBus message with the list of all controllers in the switch, and it will set up the corresponding set of control VCs from the new controller port to each of the slaves.

What Happens When You Delete a Controller

To delete a controller from the switch, use either **delshelf** or **delctrlr**. Use the command **delshelf** to delete generic VSI controllers. Use the command **delctrlr** to delete controllers that have been added to Annex G-capable interfaces.

When one of the controllers is deleted through the **delshelf** command, the master-slave connections associated with this controller will be deleted. The control VCs associated with other controllers managing the same partition will not be affected.

The deletion of the controller triggers a new VSI configuration (internal) CommBus message. This message includes the list of the controllers attached to the node. The deleted controller will be removed from the list. This message will be sent to all active slaves in the shelf. In cluster configurations, the deletion of a controller will be communicated to the remote slaves by the slave directly attached through the inter-slave protocol.

Note Cluster configurations are not supported in the Release 9.2 time frame.

While there is at least one controller attached to the node controlling a given partition, the resources in use on this partition should not be affected by a controller having been deleted. Only when a given partition is disabled, the slaves will release all the VSI resources used on that partition.

The **addshelf** command allows multiple controllers on the same partition. You will be prompted to confirm the addition of a new VSI shelf with a warning message indicating that the partition is already used by a different controller.

What Happens When a Slave is Added

When a new slave is activated in the node, the BCC will send a VSI configuration CommBus (internal BPX protocol) message with the list of the controllers attached to the switch.

The BCC will also set up a master-slave connection from each controller port in the switch to the added slave.

What Happens when a Slave is Deleted

When a slave is deactivated in the node, the BCC will tear down the master-slave VCs between each of the controller ports in the shelf and the slave.

How Resources are Managed

VSI LCNs are used for setting up the following management channels: a) inter-slave; b) master-slave; c) intershelf blind channels.

Intershelf blind channels are used in cluster configuration for communication between slaves on both sides of a trunk between two switches in the same cluster node.

The maximum number of slaves in a switch is 12. Therefore a maximum of 11 LCNs are necessary to connect a slave to all other slaves in the node. This set of LCNs will continue to be allocated from the reserved range of LCNs as in release previous to Release 9.2.

If a controller is attached to a shelf, master-slave connections are set up between the controller port and each of the slaves in the shelf. For each slave that is not directly connected, the master-slave control VC consists of two legs: one from the VSI master to the backplane, through the directly connected slave, and a second leg from the backplane to the corresponding VSI slave. For the slave that is directly connected to the controller the master-slave control VC consists of a single leg between the controller port and the slave. Therefore, 12 LCNs are needed in the directly-connected slave, and 1 LCN in each of the other slaves in the node for each controller attached to the shelf. These LCNs will be allocated from the Automatic Routing Management pool. This pool is used by Automatic Routing Management to allocate LCNs for connections and networking channels.

For a given slave the number of VSI management LCNs required from the common pool is:

n X 12 + m

where:

n is the number of controllers attached to this slave

m is the number of controllers in the switch directly attached to other slaves

VSI Slave Redundancy (Hot Slave Redundancy)

The function of the slave hot standby is to preprogram the slave standby card the same as the active card so when the active card fails, the slave card switch over operation can be done quickly (within 250 ms). Without the VSI portion, the BXM card already provided the hot standby mechanism by duplicating CommBus (internal BPX protocol) messages from BCC to standby BXM card.

With VSI operation, since the master VSI controller does not recognize the standby slave card, the active slave card forwards VSI messages it received from the Master VSI controller to the standby Slave VSI card. When the standby slave VSI card is first started (either by having been inserted into the slot, or if the user issues the **addyred** command from the CLI console), the active slave VSI card needs to forward all VSI messages it had received from the Master VSI controller card to the standby Slave VSI controller card.

In summary, the hot standby operations between active and standby card are performed as listed below:

1. CommBus messages are duplicated to standby slave VSI card by the BCC.
2. VSI messages (from Master VSI controller or other slave VSI card) are forwarded to the standby slave VSI card by the active slave VSI card.
3. When the standby slave VSI card starts up, it retrieves all VSI messages from the active slave VSI card and processes these messages.

Operation 1 does not need to implement since it had been done by the BCC. Operation 2 and 3 are major functions of VSI slave hot standby,where Operation 2 is normal data transferring, which occurs after both cards are in-sync, and Operation 3 is initial data transferring, which occurs when the standby card first starts up.

The data transfer from the active card to the standby card should not affect the performance of the active card. Therefore, the standby card takes most actions and simplifies the operations in the active card. The standby card drives the data transferring and performs the synchronization. The active card functions just forward VSI messages and respond to the standby card requests.

Configuring Service Class Templates

The following sections provide an overview of service class templates.

The principle idea of a *service class template* (also called “Service Template”, or “SCT”) is to provide a method to infer extended parameters, which are generally platform-specific, from the set of standard ATM protocol parameters passed in VSI connection set-up primitives. A service template defines a set of platform-specific parameters for each service type. (Service type examples are CBR.1, VBR1.RT, UBR1., and so on.) A set of Service Templates are stored on the switch, and are downloaded to the BXM cards.

The template also defines a specific qbin for each service type. The qbin configuration (also called a *Class of Service Buffer* configuration) is also specified in the template. Each individual qbin configuration is defined to fulfill the quality of service requirement of the corresponding service types. These Service Templates have predefined, nonchangeable values that are suited to typical interface uses, such as MPLS or ATMF controlled interfaces.

Release 9.2 supports three predefined nonconfigurable service types. You can assign any of nine templates to any VSI interface. The templates are maintained in the BCC and downloaded to the BXM during the initial card configuration process. Classes of services supported in Release 9.2 are those in the MPLS (Multiprotocol Label Switching) and ATM Forum categories. Qbins 10 through 15 are dedicated to VSI—you can configure them by using the service templates. The rest of the qbins (0– 9) are used and configured by Automatic Routing Management (formerly called AutoRoute) connections.

In this release, two new templates have been added for interfaces with multiple partitions controlled simultaneously by a PNNI controller and an LSC. Other templates support FBTC with policing on PPD.

Assigning a Service Template to an Interface

A default service template is assigned to a logical interface when the interface is activated through the **upport** and **uptrk** commands. The default template has an identifier of 1. You can change the template assigned to an interface by using the **cnfvsiif** command. In Release 9.2.10, you cannot change the template when there are active VSI partitions on the BXM interface. Setting the template for one partition changes the template for all partitions in the interface. The **cnfvsiif** command will block you from changing the template when there are active VSI partitions on the BXM interface.

Two new commands in this release enable you to do the following:

- The **cnfvsiif** command lets you configure a new service class template for an interface that does not have any active VSI partitions.
- The **dspvsiif** command lets you view the service template associated with an interface.

A default service template is assigned to a logical interface (VI) when you up the interface by using the **upport** or **uptrk** commands.

For example:

- **uptrk 1.1**
- **uptrk 1.1.1 (virtual trunk)**
- **upport 1.1**

This default template has the identifier of 1. You can change the service template from service template 1 to another service template by using the **cnfvsiif** command. The **dspvsiif** command allows you to display the template associated with the interface. For example:

- **cnfvsiif 1.1 2**
- **cnfvsiif 1.1.1 2**
- **dspvsiif 1.1**
- **dspvsiif 1.1.1**

cnfvsiif example

You use the **cnfvsiif** command to assign a selected service template to an interface (VI) by specifying the template number. It has the following syntax:

```
cnfvsiif <slot.port.vtrk> <tmplt_id>
```

dspvsiif example

You use the **dspvsiif** command to display the type of service template assigned to an interface (VI). It has the following syntax:

```
dspvsiif <slot.port.vtrk>
```

Downloading Service Templates

Service templates are downloaded to a card (BXM) under the following conditions:

- add y-red card
- on a BCC (control card) switchover
- when a card has active interfaces and is reset (Hardware reset)
- on a BCC (control card) rebuild

Additional service template commands are:

dspsct: Use the **dspsct** command to display the service class template number assigned to an interface. The command has three levels of operation:

dspsct	With no arguments lists all the service templates resident in the node.
dspsct <tmplt_id>	Lists all the Service Classes in the template
dspsct <tmplt_id>	Service Classes lists all the parameters of that Service Class.
dspqbint	Displays the qbin templates
cnfqbin	Configures the qbin. You can answer yes when prompted and the command will use the card qbin values from the qbin templates.
dspqbin	Displays qbin parameters currently configured for the virtual interface.
dspcd	Displays the card configuration.

Refer to other sections within Virtual Trunking for further description on service class templates. Also refer to the *Cisco BPX Series Installation and Configuration Guide* for more information on service class templates and VSI.

Functional Description of Service Class Templates

A set of service templates is stored in each switch (for example, BPX) and downloaded to the service modules (for example, BXMs) as needed. These service templates have predefined, nonchangeable values that are suited to typical interface uses, such as an MPLS (Multiprotocol Label Switching) Controller or an ATMF standards interface.

In general, service templates contain two classes of data. One class consists of parameters to establish a connection (that is, per-VC), and includes entries such as UPC actions, various bandwidth-related items, per-VC thresholds, and some hardware-specific items. This is referred to as the *VC Descriptor* portion of the service template. The second class of data items includes those necessary to configure the associated class of service buffer (qbin) that provides Quality of Service support. This is referred to as the *Class of Service (CoS) Buffer Descriptor* portion of the service template.

Note The phrase "VC templates" and "service templates" are used interchangeably in this chapter to mean the same thing. Qbin templates are referred to explicitly as "qbin templates".
Also note that "service class", "service category", and "service type" are sometimes used interchangeably.

You use service templates to define a setting of platform-specific parameters to be applied to connections that are set up through the standard VSI interface. When a connection setup request is received from a *VSI master controller*, the *VSI slave controller* uses the class of service index of the request to retrieve the corresponding set of extended parameters defined in the template for the corresponding index. The firmware then programs the hardware with the applicable extended parameter values to complete the connection setup.

The general types of parameters passed from a VSI master to a slave include:

- The template identifier (template ID)
- A service type identifier
- QOS parameters (CLR, CTD, CDV)
- Bandwidth parameters (for example, PCR, MCR)
- Other ATM Forum Traffic Management 4.0 parameters

Each VC added by a VSI master is assigned to a specific service class by means of a service type identifier, which is a 32-bit number from a list maintained as part of the VSI specification. It currently includes identifiers for:

- ATMF Service Types
- Cisco Proprietary Service Types (Automatic Routing Management)
- MPLS (Multiprotocol Label Switching) Service Types

One of the parameters that you need to specify for each service type is the particular Class of Service Buffer (CoS Buffer, or "qbin" on the BXM) to use. The qbin buffers provide separation of service type to match the QoS requirements.

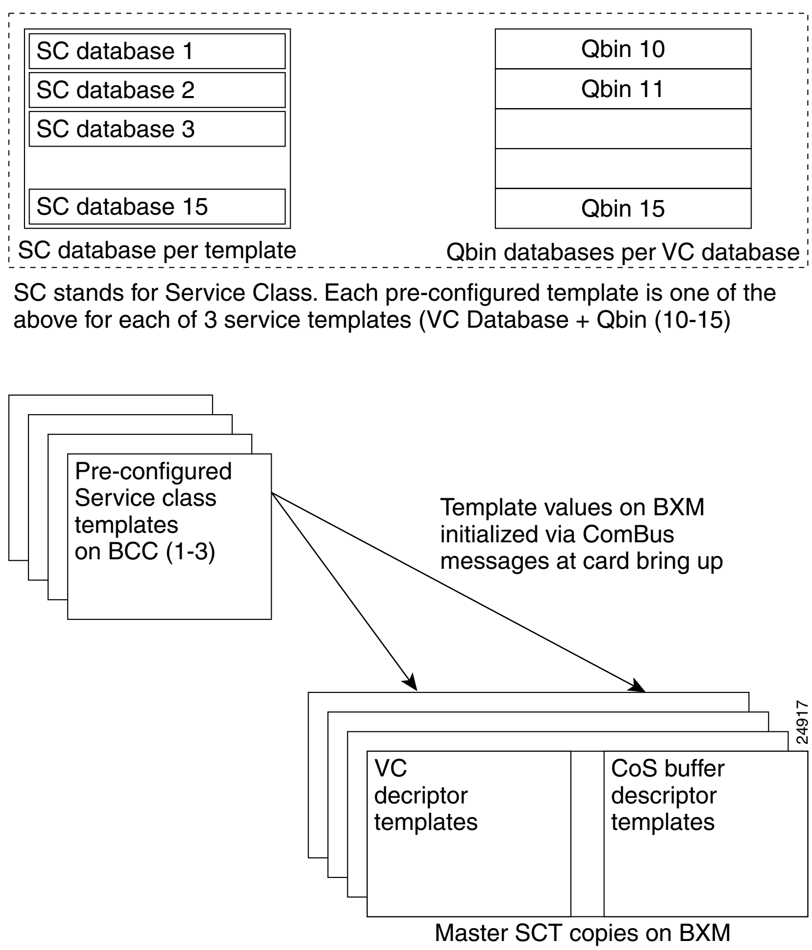
In this release, there are nine non-configurable templates. The supported service classes are VSI Special Types, MPLS (Multiprotocol Label Switching), and ATM Forum COS. You can assign any one of these templates to a virtual interface.

Structure of Service Class Templates

Each template table row includes an entry that defines the qbin to be used for that class of service. See Figure 17-9 for an illustration of how service class databases map to qbins. This mapping defines a relationship between the template and the interface qbin's configuration.

A qbin template defines a default configuration for the set of qbins for the logical interface. When a template assignment is made to an interface, the corresponding default qbin configuration becomes the interface's qbin configuration. Some of the parameters of the interface's qbin configuration can be changed on a per interface basis. Such changes affect only that interface's qbin configuration and no others, and do not affect the qbin templates.

Figure 17-9 Service Template Overview

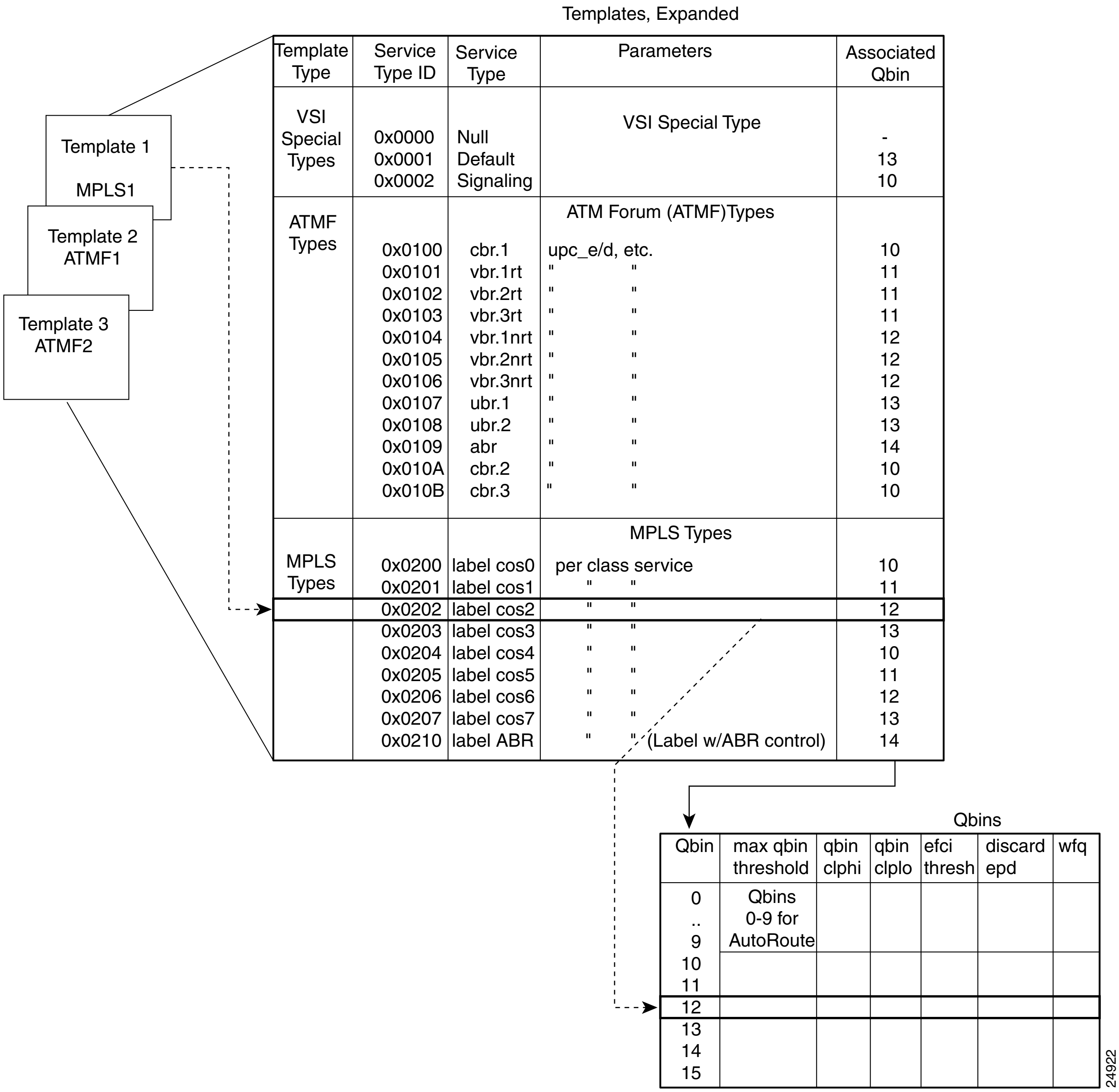


Qbin templates only are used with qbins that are available to VSI partitions, namely qbins 10 through 15. Qbins 10 through 15 are used by the VSI on interfaces configured as trunks or ports. The rest of the qbins (0–9) are reserved for and configured by Automatic Routing Management.

Each template table row includes an entry that defines the qbin to be used for that class of service. This mapping defines a relationship between the template and the interface qbin's configuration. As a result, you need to define a default qbin configuration to be associated with the template.

Note The default qbin configuration, although sometime referred as a “qbin template,” behaves differently from that of the class of service templates.

Figure 17-10 Service Template and Associated Qbin Selection



Extended Service Types Support

The service-type parameter for a connection is specified in the connection bandwidth information parameter group. The service-type and service-category parameters determine the service class to be used from the service template.

Supported Service Categories

There are five major service categories and several sub-categories. The major service categories are shown in Table 17-6. A list of the supported service sub-categories is shown in LCNs.

Table 17-6 Service Category Listing

Service Category	Service Type Identifiers
CBR	0x0100
VBR-RT	0x0101
VBR-NRT	0x0102
UBR	0x0103
ABR	0x0104

Supported Service Types

The service type identifier is a 32-bit number. The service type identifier appears on the **dspsct** screen when you specify a service class template number and service type; for example:

dspsct <2> <vbrrt1>

A list of supported service templates and associated qbins, and service types is shown in Table 17-7.

Table 17-7 Service Templates and Associated Qbin Selection

Template Type	Service Type ID	Service Type	Parameters	Associated Qbin
VSI Special Types	0x0001	Default		13
	0x0002	Signaling		10
ATMF Types	0x0100	cbr.1	**ATM Forum (ATMF) Types**	10
ATMF1 and	0x0101	vbr.rt1		11
ATMF2 templates	0x0102	vbr2.rt		11
(for PNNI controllers)	0x0103	vbr3.rt	See **dspsct** command for sample parameters for various service types, such as VbrRt1, Cbr1, etc.	11
	0x0104	vbr1.nrt		12
	0x0105	vbr.2nrt		12
	0x0106	vbr.3nrt		12
	0x0107	ubr.1		13
	0x0108	ubr.2		13
	0x0109	abr		14
	0x010A	cbr.2		10
	0x010B	cbr.3		10

Table 17-7 Service Templates and Associated Qbin Selection (Continued)

Template Type	Service Type ID	Service Type	Parameters	Associated Qbin
MPLS Types	0x0001	Default		13
(for MPLS controllers)	0x0200	Signaling		10
	0x0201	label cos0		10
	0x0202	label cos1		11
	0x0203	label cos2		12
	0x0204	label cos3		13
	0x0205	label cos4		10
	0x0206	label cos5		11
	0x0207	label cos6		12
	0x0210	label cos7		13
		label ABR		14

Qbin Default Settings

The qbin default settings are shown in Table 17-8. The Service Class Template default settings for Label Switch Controllers and PNNI controllers are shown in Table 17-9.

Note: Templates 2, 4, 6, and 8 support policing on PPD.

Table 17-8 Qbin Default Settings

QBIN	Max Qbin Threshold (usec)	CLP High	CLP Low/EPD	EFCI	Discard Selection
LABEL Template 1					
10 (Null, Default, Signalling, Tag0,4)	300,000	100%	95%	100%	EPD
11 (Tag1,5)	300,000	100%	95%	100%	EPD
12 (Tag2,6)	300,000	100%	95%	100%	EPD
13 (Tag3,7)	300,000	100%	95%	100%	EPD
14 (Tag Abr)	300,000	100%	95%	6%	EPD
15 (Tag unused)	300,000	100%	95%	100%	EPD
PNNI Templates 2 (with policing) and 3					
10 (Null, Default, CBR)	4200	80%	60%	100%	CLP
11 (VbrRt)	53000	80%	60%	100%	EPD
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Ubr)	105000	80%	60%	100%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Unused)	105000	80%	60%	100%	EPD
Full Support for ATMF and reduced support for Tag CoS without Tag-Abr Templates 4 (with policing) and 5					
10 (Tag 0,4,1,5, Default, UBR, Tag-Abr*)	300,000	100%	95%	100%	EPD
11 (VbrRt)	53000	80%	60%	100%	EPD
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Tag 2,6,3,7)	300,000	100%	95%	100%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Cbr)	4200	80%	60%	100%	CLP
Full Support for Tag ABR and ATMF without Tag CoS Templates 6 (with policing) and 7					
10 (Tag 0,4,1,5,2,6,3,7 Default, UBR)	300,000	100%	95%	100%	EPD
11 (VbrRt)	53000	80%	60%	100%	EPD

Table 17-8 Qbin Default Settings (Continued)

QBIN	Max Qbin Threshold (usec)	CLP High	CLP Low/EPD	EFCI	Discard Selection
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Tag-Abr)	300,000	100%	95%	6%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Cbr)	4200	80%	60%	100%	CLP
Full Support for Tag CoS and reduced support for ATMF Templates 8 (with policing) and 9					
10 (Cbr, Vbr-rt)	4200	80%	60%	100%	CLP
11 (Vbr-nrt, Abr)	53000	80%	60%	20%	EPD
12 (Ubr, Tag 0,4)	300,000	100%	95%	100%	EPD
13 (Tag 1, 5, Tag-Abr)	300,000	100%	95%	6%	EPD
14 (Tag 2,6)	300,000	100%	95%	100%	EPD
15 (Tag 3, 7)	300,000	100%	95%	100%	EPD

Table 17-9 Service Class Template Default Settings

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
MCR	Tag0–7: N/A TagAbr: 0% of PCR	Abr: 0%
AAL5 Frame Base Traffic Control (Discard Selection)	EPD	Hysteresis
CDVT(0+1)	250,000	250,000
VSVD	Tag0–7: N/A TagAbr: None	Abr: None
SCR	Tag0–7: N/A TagAbr: 0	Vbr: 100% Abr: 0
MBS	Tag0–7: N/A TagAbr: 0	Vbr: 1000

Table 17-9 Service Class Template Default Settings (Continued)

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
Policing	Policing Disable	VbrRt1: GCRA_1_2, CLP01_CLP01, DISCARD on both policing action VbrRt2: GCRA_1_2, CLP01_CLP0, DISCARD on both policing action VbrRt3: GCRA_1_2, CLP01_CLP0, CLP DISCARD for 1st policer and CLP for 2nd policer VbrNRt1: same as VbrRt1 VbrNRt2: same as VbrRt2 VbrNRt3: same as VbrRt3 Ubr1: GCRA_1 CLP01, Discard Ubr2: GCRA_1_2 CLP01 DISCARD on policer 1. CLP01 TAG on policer 2 Abr: same as ubr1 Cbr1: same as ubr1 Cbr2: GCRA_1_2 CLP01_CLP0, Discard on both policing action Cbr3: GCRA_1_2 CLP01_CLP0, CLP UNTAG for policer 1 and CLP for policer 2
ICR	Tag0–7: N/A TagAbr: NCR	Abr: 0%
ADTF	Tag0–7: N/A TagAbr: 500 msec	Abr: 1000 msec (ATM forum it's 500)
Trm	Tag0–7: N/A TagAbr: 0	Abr: 100

Table 17-9 Service Class Template Default Settings (Continued)

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
VC Qdepth	61440	10,000 160 – cbr 1280 – vbr
CLP Hi	100	80
CLP Lo / EPD	40	35
EFCI	TagABR: 20	20 (not valid for non-ABR)
RIF	Tag0–7: N/A TagAbr: 16	Abr: 16
RDF	Tag0–7: N/A TagAbr: 16	Abr: 16
Nrm	Tag0–7: N/A TagAbr: 32	Abr: 32
FRTT	Tag0–7: N/A TagAbr: 0	Abr: 0
TBE	Tag0–7: N/A TagAbr: 16,777,215	Abr: 16,777,215
IBS	N/A	N/A
CAC Treatment	LCN	vbr: CAC4 Ubr:LCN Abr: MIN BW Cbr: CAC4
Scaling Class	UBR – Scaled 1st	Vbr: VBR –Scaled 3rd Ubr: UBR – Scaled 1st Abr: ABR – Scaled 2nd Cbr: CBR – Scaled 4th
CDF	16	16

Configuring the Virtual Switch Interface

In the VSI control model, a controller sees the switch as a collection of slaves with their interfaces and it can establish connections between any two interfaces. The controller uses resources allocated to its partition. You can continue to configure VSI resources on a given interface by using the **cnfrsrc** command. You attach a controller to a node to control the node by using the **addshelf** command.

You can assign each VSI interface a default class of service template when you activate it. You can use the switch software CLI or Cisco WAN Manager to configure a different template to an interface.

VSI Commands

addctrlr: Use this command to enable the VSI capabilities on the trunk interface. New in this release.

cnfrsrc: Use this command to configure resource on the trunk interface for the PNNI controller's control channels.

cnfvsiif: Use this command to assign a template number to an active interface.

cnfvsipart: Use this command to configure VSI partition characteristics. New in this release.

delctrlr: Use this command to disable VSI capabilities on the trunk interface. New in this release.

dspchuse: Use this command to display a summary of the channel distribution in a given slot. New in this release.

dspctrlrs: Use this command to display all VSI controllers attached to the BPX. These controllers could be either a PNNI controller or an MPLS controller. New in this release.

dspvsiif*:* Use this command to display the template number assigned to an interface.

dspsct: Use this command to display the service class template. It has three levels of operation:

- **dspsct** without any arguments lists all the templates in the node.
- **dspsct** <tmplt_id> lists all the service classes in that template.
- **dspsct** <tmplt_id> service class lists all the parameters of that Service Class.

dspqbint: Use this command to display the Qbin templates.

dspvsipartinfo: Use this command to display VSI resource status information for the partition.

dspvsipartcnf: Use this command to display VSI partition characteristics. New in this release.

cnfqbin: Use this command to configure the Qbin parameters. Use this command to change accept the interface template as the values, as an option. For example, you can enter "Yes" when prompted whether the interface service class template should be used, and the command will use the card's qbin values from the qbin templates. You will not be able to enter desired values for any qbin parameter in this case. You can, however, enter desired values when the template option is not chosen.

dspqbin: Use this command to display the Qbin parameters currently configured for an interface. The **dspqbin** command shows whether the Qbin has been configured by a user OR by a template.

dspcmi: This is a debug command, which displays the current capabilities reported by the firmware on the card.

dspcd: This command displays the characteristics of the card. Changes will be made to reflect the current VSI version supported by the card.

Table 17-10 Maximum PVC Bandwidth for all Partitions on Logical Interface

Card Type	Bandwidth
BXM E3	80000
BXM T3	96000
BXM OC-3	353208
BXM OC-12	1412830

VSI Related Parameters and Descriptions

These tables provide parameters related to VSI configuration and some descriptions. In most cases, the object name is similar or identical to the screen field name as it appears on the CLI (for various VSI commands such as **cnfrsrc**, **cnfvsiif**, **dspsctmplt**, and so on.)

Troubleshooting VSI Problems

This section describes how different types of channels are allocated (VSI, Automatic Routing Management), and how to troubleshooting some problems related to VSI. Note that some or all of the commands discussed in this section require service-level or above user privileges. To access these commands, you must have debug (Service or StrataCom level) privileges and passwords. Check with the TAC for assistance.

How Channels are Allocated and Deallocated

To understand channel allocation and deallocations problems, it's important to understand how the channels are distributed. The BXM card can support *x* number of channels. The value *x* varies between different models of BXMs.

How Networking Channels are Allocated

Networking channels are assigned for trunk interfaces only. This includes physical, feeder, and virtual. Every physical and feeder trunk that is active is assigned 271 networking channels. For virtual trunks, the first virtual trunk upped on a port is assigned 271 networking channels. Every subsequent one requires an additional one. So if the second virtual trunk on the same port is upped, one more networking channel is reserved for that virtual trunk.

How Automatic Routing Management Channels are Allocated/Configured

When a port or trunk interface is upped, a default value of 256 PVC channels are assigned. You can use the **cnfrsrc** command to change this value to fit your needs. Note that this is only the number of PVC channels configured. Every time a connection is added on the port or trunk interface, a counter is incremented to keep count of the number of PVCs used. This counter can never exceed the number configured. For the trunk interface, connections will be rerouted if the new value configured is less than the old value. For the port interface, **cnfrsrc** will not allow you to decrease the configured value to be less than the used value. You will need to delete connections before decreasing the PVC value.

How SVC Channels are Allocated and Configured

You can configure the number of SVC channels by using the **cnftrk** or the **cnfport** command. SVC and VSI channels cannot co-exist. The command will block you from configuring channels if there are VSI channels allocated.

How VSI Channels are Assigned for VSI Master to Slave VCs

When a VSI shelf is added with the **addshelf** command on the feeder interface, 12 LCNs are reserved for master to slave VCs. The reason for 12 LCNs is that one LCN is needed to communicate to an active BXM (with VSI functionality). The BPX has 15 slots possible, two of which are used for the BCC and one used for the ASM card. The worse case is if the BPX has all BXM cards in the node, therefore the master endpoint (that is, the card with the VSI shelf added) needs 12 LCNs to communicate with all the cards on the node. The command **dspvsich** will display all the LCNs reserved for master to slave VCs and interslave VCs.

How VSI Channels Are Configured/Allocated

VSI channels are configured through the cnfrsrc command. The user specifies a vsi min and a vsi max for the partition. The number of channels that is allocated is max (sum_of_min, max_of_max).

For example:

port group 1:

port 1:minmax

partition 1: 10001000

port 2:

partition 1:2000 1000

port group 2:

port 3:

partition 1:20005000

port 4:

partition 1:20004000

For portgroup 1:

sum_of_min = 3000;   max_of_max = 1000

For portgroup 2:

sum_of_min = 4000; max_of_max = 5000

Therefore, the number of channels allocated for VSI is 8000.

How Background Redundancy Channels are Allocated

The formula for getting the LCN is num_chans + 1. These channels are used for y-redundancy cards to communicate with each other.

How IP Channels are Allocated

IP channels are used for ALL5 messaging. The LCNs are reserved within switch software. The formula for getting the LCN is num_chans + 14 + port (0 based). Twelve (12) LCNs are reserved for IP channels, one for each port.

How ILMI/LMI Channels are Allocated

The formula for getting the LCN is num_chans + 2 + port.

How ILMI Channels are Allocated for VSI Partitions on Trunk Interfaces

When ILMI functionality is enabled for a VSI partition on a trunk interface, a new ILMI session is started on the BXM card for the trunk interface. The LCN for this session is allocated from the LCNs available for the AutoRoute partition. This LCN is allocated from the port-based pool; not from the card-based pool.

Note that no new LCN is allocated when ILMI functionality is enabled for VSI partitions on port interfaces. This is because the ILMI functionality for VSI partitions on port interfaces use the same ILMI functionality that is started for AutoRoute. These use the pre-allocated LCN as discussed in the preceding section.

How VSI Channels are Assigned for Interslave VCs

Interslave vcs are assigned with LCNs that are reserved within switch software. These lcns are not taken from the pool. The formula for getting the lcn is num_chans + 26 + dest_slot where num_chans is the number of channels the card supports

mc_vsi_end_lcn

This value is shown in the **dsplogcd** command. If the value is 0, then there are no vsi channels configured on the card. If it is not zero, then there are VSI channels. It marks the first VSI channel.

num chans

This value is shown in the **dsplogcd** command as "Physical Chans". It is reported to switch software from the card. Each BXM will vary in the number of channels that it supports.

How Port Group Enters the Channel Assignment Picture

Note The **dsplogcd** command is for service level users and above. You must have "service" level privileges to use it.

There are some models of BXM cards which will support more than 1 port group. The command **dsplogcd** and **dspcd** will indicate the number of port groups supported. Even though each card supports *x* channels, there is a hardware limitation of how many channels can be supported between certain ports. A set of ports are grouped into port groups; that is, a BXM 8-port OC-3 card has two port groups, consisting of ports 1–4, and 5–8 respectively. Each port group will have an upper limit of the number of channels it can support, majority of the time it's

(num_chans / num_of_port_groups).

cnfrsrc fails with "available channels is 0"

Description of Problem

When the user thinks that there are channels available, but cnfrsrc says that the number of available channels is 0. The user will not be able to allocate any more vsi channels.

Initial Investigations

This may not be a problem, since the user may not have accounted for hidden channel assignments like networking and VSI vcs. Execute the **dspchuse** command to see where all the channels are allocated. Note any channel assignment that looks suspicious. Verify this page with the channels configured from the **cnftrk** and **cnfrsrc** command.

The **dspchuse** command is available to users in this release.

Workarounds

The work around depends on where the problem is. If it's with PVCs, try **cnfrsrc** and change the number of pvcs. Since **switchcc**, will rebuild the channel database, try executing **switchcc**.

Detailed Debugging

You should perform the following tasks:

- Capture the **dspchuse** screen and compare against the **cnfrsrc** and **cnftrk** command.
- Verify the number of trunks that are upped. This will indicate the number of networking channels assigned.
- Note the number of vsi shelves added. For each vsi shelf added, 12 lcns are reserved on the BXM attached to the controller and 1 lcn is reserved for all the other active BXM cards. Capture the **dspvsich** command. For example:
  - — slot 13:

    2 vsi shelf added
  - — slot 11:

    1 vsi shelf added
  - — slot 9:

    Two (2) trunks are upped

    One (1) port is upped
  - — On slot 13 – 25 lcns are reserved => 12 for each vsi shelf, and 1 for the shelf added to slot 11.
  - — On slot 11 – 14 lcns are reserved => 12 for the vsi shelf, and 2 for the 2 shelves added on slot 13.
  - — On slot 9 – 3 lcns are reserved => 2 for the 2 shelves added on slot 13, and 1 for the 1 shelf added on slot 11.

    Verify if anyone has disable a partition.

Disabling the partition will not recalculate the end_lcn value. The end_lcn will be recalculated by a card reset or a **switchcc** command or a node rebuild.

cnfrsrc fails with "Automatic Routing Management is currently using the channel space"

Description of Problem

This error is indicating that there are Automatic Routing Management channels currently configured on the space that the user wants for VSI.

For example: Let's say the BXM card supports 100 channels. Currently 50 of the channels are configured for PVCs and 50 for VSI ranging from 51–100. Let's suppose that the card has 5 connections on channel 45–49. Now change the configuration of PVCs to 10. The command will work since only five (5) are currently used. The available channels on the card is now 40. If **cnfrsrc** is executed now to increase the number of VSI channels, the command will fail, because channels 45–49 are currently in use.

Initial Investigations

- To check if a specific connection is using a channel out of range:
  - — Verify channel number (LCN) used by the connection by using the command **dcct**.
  - — Get VSI end LCN using **dsplogcd**—field mc_vsi_end_lcn

- In normal conditions, the value of mc_vsi_end_lcn should be greater than LCN.
- To check if any connection in the port or trunk card is using a channel out of range.
  - Get VSI end LCN using **dsplogcd**—field mc_vsi_end_lcn
  - Use **dspchmap** to display the map of lcns used by connection in the card; in normal conditions no LCN higher than mv_vsi_end_lcn should be associated with an Automatic Routing Management connection or trunk xlat.

Workarounds

The only work around is to somehow delete the connections currently using the high end of the channel range. On the trunk interface, causing the connections to reroute will likely cause the lower lcn range to be used first. On the port interface, deleting and re-adding the connection.

Detailed Debugging

Refer to the section "Initial Investigations" section on page 17-41.

Summary of Commands

Table 17-11 shows the command name and starting page for the description of each VSI-related command.

Table 17-11 Commands for Setting up a VSI (Virtual Switch Interface) Controller

Mnemonic	Description	Page
addctrlr	Attach a controller to a node; for controllers that require Annex G capabilities in the controller interface. Add a PNNI VSI controller to a BPX node through an AAL5 interface shelf	17-45
addshelf	Add a trunk between the hub node and interface shelf or VSI-MPLS (Multiprotocol Label Switching) controller).	17-48
cnfqbin	Configure Qbin card	17-57
cnfrsrc	Configure resources, for example, for Automatic Routing Management PVCs and MPLS (Multiprotocol Label Switching) Controller (LSC)	17-62
cnfvsiif	Configure VSI Interface or a different template to an interface.	17-74
cnfvsipart	Configure VSI partition characteristics for VSI ILMI.	17-76
delctrlr	Delete a controller, such as a PNNI ESP (Extended Services Processor) 4.0 controller, from a BPX node	17-77
delshelf	Delete a trunk between a hub node and access shelf	17-80
dspchuse	Display a summary of channel distribution in a given slot.	17-83
dspctrlrs	Display the VSI controllers, such as an PNNI controller, on a BPX node	17-86
dspqbin	Display Qbin card	17-88
dspqbint	Display Qbin template	17-93
dsprsrc	Display LSC (Label Switching Controller) resources	17-95
dspsct	Display Service Class Template assigned to an interface	17-101
dspvsiif	Display VSI Interface	17-119
dspvsipartcnf	Display information about VSI ILMI functionality.	17-122
dspvsipartinfo	Display VSI resource status for the partition.	17-123

addctrlr

Adds VSI capabilities to a trunk interface to which a feeder of type AAL5 is attached. The **addctrlr** command is used only to connect a Private Network to Network Interface (PNNI) controller. PNNI controller software resides on the SES hardware.

The **addctrlr** command is the second step in the adding of a PNNI controller to a BPX node.

The first step is to run the command **addshelf** with shelf type set to X to add a AAL5 feeder. This ensures that Annex G protocol runs between the BPX and the SES.

Then run the **addctrlr** command to set up the VSI control channels from the PNNI SES controller to the VSI slave processes running on the BXM cards to ensure full VSI functionality for the PNNI controller. You execute the **addctrlr** command on an existing AAL5 interface shelf.

Also note that you can add a PNNI controller to a Trunk interface only if the interface already has an active VSI partition corresponding to the partition that is controlled by the PNNI controller. Suppose a PNNI controller controlling the partition 1 were added to an trunk interface 12.1. Then it would be necessary that a VSI partition corresponding to partition 1 be active on the interface 12.1. Otherwise the **addctrlr** command would fail.

When you add VSI controller capabilities onto an AAL5 interface shelf (or feeder), the switch software prompts you for the specifics of the VSI controller:

- controller ID of the PNNI controller
- partition ID of the VSI partitions controlled by the PNNI controller
- VPI used for the VSI control channels set up by the PNNI controller
- Start VCI value for the VSI control channels set up by the PNNI controller

There could be 12 BXM cards on the BPX node and the PNNI controller would control VSI partitions on those BXM cards that support VSI capability. Hence a separate VSI control channel must be set up from the PNNI control to each BXM card that supports VSI. Suppose you specify a VPI value of 0 and start VCI value of 40 for the VSI control channels. Then the control channel corresponding to any BXM card on slot 1 would use VPI, VCI values <0, 40>. The VSI control channels to other slots would use the VPI, VCI values of <0, 40+slot-1>, where “slot” corresponds to the slot number of the BXM card.

Note ESP 2.x interface shelves can still be configured; however, an ESP 2.x shelf cannot coexist with an AAL5 interface shelf with VSI configured on the same node. The Annex G capabilities of the AAL5 interface shelf are the same as in Release 9.1.

Caution For feeder trunk interfaces, the **addctrlr** command will fail if the AutoRoute connections terminating on the feeder interface use the same VPI VCI as those specified for the VSI control channels. You must delete the connections before proceeding if connections with VPI and VCI in the range exist in the range you specified.

The addition of a controller to a node will fail if there are not enough channels available to set up the control VCs in one or more of the BXM slaves.

Full Name

Add VSI capabilities to a AAL5 feeder interface.

Syntax

addctrlr < slot.port> <controller id> <partition id> <control_vpi> <start_vci>

Table 17-12 Parameters—addctrlr

Parameter	Description
<slot.port>	Slot and Port numbers corresponding to the feeder trunk
<controller-id>	Controller ID corresponding to the PNNI controller. Values: 1 – 32
<partition-id>	Partition ID of the VSI partition controlled by the PNNI controller
<control_vpi>	Starting VPI of the VSI control channels used for communication between the VSI master residing on the SES and VSI slaves residing on the BXM cards. There can be a total of 12 such channels one for each slave residing on each BXM card. For a trunk interface with NNI header type: Valid values for this parameter are: 0–4095 For a trunk interface with UNI header type Valid values for this parameter are: 0–255. Default value: 0
<start_vci>	Starting VCI of the VSI control channels. This vci value is assigned to the first VSI control channel (between the VSI master and the VSI slave residing on the BXM card in slot 1). The last VSI control channel corresponding to communication with the VSI slave on slot 14 will use the vci value of (<start_vci>+14-1). The valid values are: 33 – 65521. Default value: 40

Related Commands

addshelf, delctrlr, dspctrlrs

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
1	No	Yes	BPX	Yes

Example 1

```
addctrlr 10.4 3 2 0 40
```

Description

Add controller to port 4 on slot 10,, partition ID of 2, and controller ID of 3.

System Response

```
night           TN   StrataCom     BPX 8600   9.2.00 Apr. 11 1998 14:31 GMT

                    BPX Controllers Information

 Trunk   Name       Type      Part Id   Ctrl ID   Ctrl IP       State
 10.3    PNNI    VSI       1         1         192.0.0.0     Enabled
 11.1    VSI        VSI       2         2         192.0.0.0     Disabled


Warning partition already in use do you want to add redundant controller

Last Command: addctrlr 10.4 3 2 0 40


Next Command:
```

Description

Adds a controller, such a PNNI controller, to a BPX interface shelf.

System Response

```
night           TN   StrataCom     BPX 8600   9.2.00 Apr. 11 1998 14:31 GMT

                    BPX Controllers Information

 Trunk   Name       Type      Part Id   Ctrl ID   Ctrl IP       State
 10.3    PNNI    VSI       1         1         192.0.0.0     Enabled
 11.1    VSI        VSI       2         2         192.0.0.0     Disabled


Warning partition already in use do you want to add redundant controller

Last Command: addctrlr 10.3 3 1 0 40


Next Command:
```

addshelf

Adds an ATM link between a hub node and an interface shelf such as an MGX 8220. an MGX 8850, or IGX shelf in a tiered network; or an ATM link between a BXM card on a BPX node and a MPLS (Multiprotocol Label Switching) controller such as a series 7200 or 7500 router; or an ATM link between a BXM card on a BPX node and an Extended Services Processor. (An MPLS Controller or an Extended Services Processor is considered an interface shelf from the BPX switch's perspective.) The routing hub can be either a BPX or an IGX.

The interface shelf can be one of the following:

- An MGX 8220 shelf connected to a BPX node
- An IGX shelf connected to an IGX routing node which serves as a hub for the IGX/AF
- An Extended Services Processor Controller connected to a BPX node
- An MGX 8850 shelf connected to a BPX node
- A MPLS (Multiprotocol Label Switching) Controller connected to a BPX node
- An SES (Service Expansion Shelf) connected to an IGX node

The signaling protocol that applies to the trunk on an interface shelf is Annex G. For example, in this release, the IGX 8400 interface shelf with a BTM E1 interface communicates with the routing hub through the Annex G LMI using STI cell format. However, the MGX 8850 interface shelf, or feeder, communicates over a UXM/UXM-E interface with the routing hub over Annex G LMI using AAL5 format.

Note Because tiered network capability is a paid option, personnel in the Cisco Technical Assistance Center (TAC) must telnet to the unit and configure it as an interface shelf before you can execute **addshelf**.

Each IGX/AF, MGX 8220, or MGX 8850 shelf has one trunk that connects to the BPX or IGX node serving as an access hub. A BPX routing hub can support up to 16 T3 trunks to the interface shelves, which can be IGX/AF, MGX 8220, or MGX 8850 interface shelves. An IGX hub can support up to four trunks to the interface shelves, which can be IGX/AF shelves only.

An IGX 8400 interface shelf can connect to an IGX 8400 routing hub over a BTM E1 interface using STI cell format. In Release 9.1, an IGX 8400 interface shelf can connect to an MGX 8800 over a UXM/UXM-E interface using ATM cell format.

Before it can carry traffic, you must "up" trunk on an interface shelf (using **uptrk**) on both the interface shelf and the hub node and "add" it to the network (using **addshelf**). Also, a trunk must be free of major alarms before you can add it with the **addshelf** command.

In this release, the new parameters "Control VPI" and "Control VCI start" have been added.

In this release, **addshelf** will prevent adding a feeder to a trunk if a VSI ILMI session is active on a VSI partition on the trunk interface.

Adding a VSI Controller

The maximum number of controllers that can be attached to a given node is limited by the maximum number of feeders (16) that can be attached to a BPX hub. Therefore the total number of feeders and controllers cannot exceed 16.

You add a VSI controller, such as an MPLS (Multiprotocol Label Switching) Controller, to a switch with the **addshelf** command using the *vsi* option. The *vsi* option of the **addshelf** command is used to identify VSI controllers and tell them apart from interface shelves (feeders). The VSI controllers are allocated a partition of the switch resources. VSI controllers manage their partition through the VSI interface. The controllers run the VSI master. The VSI master entity interacts with the VSI slave running on the BXMs through the VSI interface, to set up VSI connections using the resources in the partition assigned to the controller. Two controllers that are intended to be used in a redundant configuration must specify the same partition when added to the node through the **addshelf** command.

When a controller is added to the node switch software will set up the infrastructure so that the controllers can communicate with the slaves in the node. The VSI entities decide how and when to use these communication channels.

In addition, the controllers require a communication channel between them. This channel could be in-band or out-of-band. When a controller is added to the switch, switch software will send controller information to the slaves. This information will be advertised to all the controllers in the partition. The controllers may decide to use this information to set up an intermaster channel. Alternatively the controllers may use an out-of-band channel to communicate.

The maximum number of controllers that can be attached to a given node is limited by the maximum number of interface shelves (feeders) that can be attached to a BPX hub. This number in Release 9.2 is 16. Therefore the total number of feeders and controllers cannot exceed 16.

To add a controller to the node, use the **addshelf** command. A redundant controller is added in the normal way, except that it specifies a partition that may be already in use by another controller. In this release, the **addshelf** command allows for up to two controllers to manage the same partition.

One of the parameters that must be specified with the **addshelf** command when a VSI controller is added to the switch is the controller id. This is a number between 1 and 32 that uniquely identifies the controller. Two different controllers must always have different controllers id.

The management of resources on the VSI slaves requires that each slave in the node has a communication control VC to each of the controllers attached to the node. When a controller is added to the BCC via the **addshelf** command, the BCC sets up the set of master-slave connections between the new controller port and each of the active slaves in the switch. The connections are set up using a well known vpi.vci. The value of the vpi is 0. The value of the vci is (40 + (slot - 1)) where slot is the logical slot number of the slave.

Feature Mismatching to Verify VSI Support

The **cnfrsrc** and **addshelf** commands, in addition to other configuration commands, will perform mismatch verification on the BXM and UXM cards. For example, the **cnfrsrc** and **addshelf** commands will verify whether the cards both have VSI 2.0 support configured. Refer to "Feature Mismatching" section on page 18-1 for more information on Feature Mismatching in Release 9.2.

The Feature Mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Full Name

Add an interface shelf (feeder) or a controller to a routing node or hub.

Syntax

Interface shelf:

addshelf <slot.port> <shelf-type> <vpi> <vci>

MPLS (Multiprotocol Label Switching) controller:

addshelf <trunk slot.port> v <ctrlr id> <part id> <control vpi> <control vci start> <redundant ctrlr warning>

Note If you manage a tiered network through the command line interface, you can manage only Frame Relay interworking connections (ATFR) across the network. Three-segment connections for carrying serial data or voice between IGX/AFs is allowed, but you must manage them through WAN Manager.

Related Commands

addctrlr, delshelf, **dspnode**, **dsptrks**

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	Yes	Yes	BPX switch with IGX interface shelf IGX switch with IGX shelves BPX switch with the MGX 8220 shelf BPX with the MGX 8850 shelf BPX switch for MPLS (Multiprotocol Label Switching) controller (LSC) BPX switch for the Extended Services Processor (also called Adjust Processor Shelf, or APS at command line interface).	Yes

Example 1

Interface shelf: **addshelf** 11.1 a 21 200

MPLS (Multiprotocol Label Switching) controller: **addshelf** 4.1 vsi 1 1

Description

Interface shelf:

Add trunk 11.1 as an MGX 8220 interface shelf. After you add the shelf, the screen displays a confirmation message and the name of the shelf.

MPLS (Multiprotocol Label Switching) controller:

Add trunk 4.1 as a VSI-MPLS (Multiprotocol Label Switching) Controller interface shelf. After you add the LSC, the screen displays a confirmation message and the name of the shelf.

Description for Interface Shelves

An interface shelf can be one of the following:

- An MGX 8220 connected to a BPX node.
- An MGX 8850 connected to a BPX node.
- An IGX node connected to a BPX node, which serves as a hub for the IGX/AF.
- An IGX node connected to an IGX routing node, which serves as a hub for the IGX/AF.

Table 17-13 Interface Shelf Parameters—addshelf

Parameter	Description
slot.port (trunk)	slot.port Specifies the slot and port number of the trunk.
shelf-type	I or A or X On a BPX node, shelf type specifies the type of interface shelf when you execute **addshelf**. The choices are I for /AF or IGX/AF, A for the MGX 8220, P for EPS (Extended Services Processor, a type of Adjunct Processor Shelf), V for VSI, or X for the MGX 8800. On an IGX hub, only the IGX/AF is possible, so *shelf type* does not appear.
vpi vci	Specifies the vpi and vci (Annex G vpi and vci used). For the MGX 8220 only, the valid range for vpi is 5–14 and for vci is 16–271. For an IGX/AF interface shelf, the valid range for both vpi and vci is 1–255. On an IGX 8400 node, when using an MGX 8800 interface shelf, the following VPI/VCI limits apply: • Use the VPI/VCI combination of 3/31 for the LMI signalling channel. When adding an MGX 8800 as an interface shelf, do not use 3/31 for anything else but the LMI signalling channel. • For VCC addressing, the VPI range is 1–255 and the VCI range is 1–65535. • For VPC addressing, the interface type is significant: UNI or NNI may be supported. When the interface type is UNI, the available VPI range is 1–255 and VCI range is 1–65535. When the interface type is NNI the available VPI range is 1–4095 and VCI range is 1–65535.
control_vpi	Choose the value for <control_VPI> such that: if <control_VPI> = 0, <control_VCI_start> can be set to a value > 40. If any VSI partition exists on the interface, then control_VPI < start_VPI or control_VPI > end_VPI for all partitions on that interface. An error message appears if the control VPI falls into the VPI range belonging to a VSI partition. No AutoRoute connection exists on (VPI.start_VCI to VPI.start_VCI+14). If any AutoRoute connection exists on these VPI/VCI values, you are not allowed to use these VPI/VCI values. This VPI is reserved for control VCs. Default = 0
control_vci_start	Default = 40

The (VPI.VCI) of the 15 control VCs is:
(control_VPI.control_VCI_start) to (control_VPI.control_VCI_start+14).

The control VC used for slot n (1<= n<=15) is:
(control_VPI.control_VCI_start + n -1).

Example for Interface Shelves

Add an MGX 8220 at trunk 11.1 After you add the shelf, the screen displays a confirmation message and the name of the shelf. Add the MGX 8220 (may be referred to on screen as AXIS) as follows:

addshelf 11.1 a

The sample display shows a partially executed command prompting you for the interface shelf type:

System Response

```
nmsbpx23       TN    SuperUser       BPX 8620    9.2   Apr. 4 1998 13:28 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 1.3     AXIS240   AXIS      OK
 11.2    A242      AXIS      OK






This Command: addshelf 11.1

Enter Interface Shelf Type:  I (IGX/AF), A (AXIS), P (APS), V (VSI), X (AAL5)

Next Command:
```

Example for Adding an MGX 8850 AAL5 (ATM Adaptive Layer/5) Interface Shelf

Add an MGX 8850 at trunk 4.8. After you add the MGX 8800 shelf, the screen displays a confirmation message and the name of the shelf. Add the MGX 8850 (may be referred to on screen as AAL5) as follows:

addshelf 4.8 x

The sample display shows that an MGX 8850 was added on trunk 4.8 as an AAL5 (ATM Adaptive Layer/5 type of interface shelf. (Adding an MGX 8850 interface shelf is similar to adding a MPLS (Multiprotocol Label Switching) Controller interface shelf.)

System Response

```
pswbpx3       TN    SuperUser       BPX 8600    9.1   June 6 1998 13:28 PST

                         BPX Interface Shelf Information

Trunk    Name      Type      Part Id    Ctrl Id    Alarm
 4.8     SIMFDR0   AAL5         -           -      OK




This Command: addshelf 4.8 x

Enter Interface Shelf Type:  I (IGX/AF), A (AXIS), P (APS), V (VSI), X (AAL5)

Next Command:
```

Description for MPLS

For MPLS, before it can carry traffic, you need to “up” the link to a MPLS controller (by using either **uptrk** or **upport**) at the BPX node. You can then add the link to the network (by using **addshelf**). Also, the link must be free of major alarms before you can add it with the **addshelf** command.

Note Once you “up” a port on the BXM in either trunk or port mode by using either the **uptrk** or **upport** commands, respectively, you can only “up” the ports in the same mode.

Table 17-14 MPLS Parameters–addshelf

Parameter	Description
slot.port	Specifies the BXM slot and port number of the trunk. (You can configure the port for either trunk (network) or port (service) mode.
device-type	vsi, which is “virtual switch interface, specifies a virtual interface to a MPLS controller (TSR) such as a Cisco 7200 or 7500 series router.
control partition	
control ID	Control IDs must be in the range of 1 to 32, and you must set these identically on the LSC and in the **addshelf** command. A control ID of “1” is the default used by the MPLS (Multiprotocol Label Switching) controller (LSC).

Example for MPLS

Add a MPLS controller link to a BPX node by entering the **addshelf** command at the desired BXM port as follows:

addshelf 4.1 vsi 1 1

System Response

```
nmsbpx23       TN    SuperUser       BPX 15    9.1   Apr. 4 1998 13:28 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 5.1     j6c       AXIS      MIN
 5.3     j5c       /AF    MIN
 4.1     VSI       VSI       OK







This Command: addshelf 4.1 v 1 1

Next Command:
```

Example for VSI Controller

Add a VSI controller link to a BPX node by entering the **addshelf** command at the desired BXM port as follows:

addshelf 13.2

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:48 PST

TRK       Type     Current Line Alarm Status              Other End
 4.1     [T3       Clear - OK                             VSI(VSI)
10.1      OC-3      Clear - OK                             VSI(VSI)
10.5      OC-3      Clear - OK                             VSI(VSI)
13.1.1    OC-3      Clear - OK                             -
13.2      OC-3      Clear - OK                             -








This Command: addshelf 13.2
```

addyred

Enables card redundancy for IGX and BPX cards. Use the **addyred** command to specify the slots of the primary and secondary (standby) cards that form the redundant pair. Refer to the "Specifying Card Redundancy" section on page 3-3" section at the beginning of this chapter for a list of supported card sets.

You must use the **addyred** command to configure a VSI slave redundant card. When a standby slave card is first started (either by having been inserted into the slot, or if the user issues the **addyred** command from the CLI console), the active slave VSI forwards all VSI messages it had received from the Master VSI controller card to the standby slave VSI controller card.

Redundant card sets must have the following characteristics:

- The primary and secondary card sets must be identical.
- When configuring APS 1+1, primary and secondary card sets must be in adjacent slots. (Note that this restriction only applies to the BPX chassis for APS 1+1 redundancy.)
- Secondary card sets must not currently be active.
- Neither the primary nor secondary card set may already be part of a redundant set.
- Redundancy applies to the entire card and not specific trunks or lines.

In both the single and multiport card sets, if the secondary card set becomes active, the primary card set serves as its backup (assuming the primary card set is complete and not failed). You cannot use the **addyred** command if the primary and secondary slots are empty. If cards reside in the primary and secondary slots, the system checks for card compatibility. Two types of incompatibility can occur: back card and jumper or cable inconsistencies. (On SDI, FRI, and FTI cards, jumpers determine whether a port is configured as DCE or DTE. On LDI cards, either a DCE or DTE adapter cable connects to the LDI port. For descriptions of the jumper positions and cabling, see the *Cisco IGX 8400 Series Installation and Configuration* manual.)

Note that the **addyred** command prevents invalid configurations when you try to configure the SONET APS feature. When SONET Automatic Protection Switching (APS) is configured, you will not be able to use the **addyred** or **delyred** commands on a card configured for APS 1:1 architecture. That is, you will not be able to execute the **addyred** command, then configure the APS 1:1 architecture. Similarly, you will not be able to configure APS 1:1, then execute the **addyred** command. You will be blocked from executing these commands at the command line interface.

If incompatibilities exist, the message "Y-Cable Conflict" appears on the screen. Specific conflicts are listed in reverse video in the **dspyred** display. See the **dspyred** description for more information.

To ensure that only cards with the Idle Code Suppression feature enabled on them are allowed to be a Y-redundancy pair, **addyred** blocks cards that have different idle code suppression capability.

Full Name

Add Y-cable redundancy.

Syntax

addyred <primary slot> <secondary slot>

Related Commands

delyred, **dspyred**, **prtyred**

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	IGX, BPX	Yes

Example 1

addyred 25 26

Description

Add Y-cable redundancy to the SDP/SDI card sets in slots 25 and 26.

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 14:27 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
2    Pri    3   BXM    LM-BXM
3    Sec    2   BXM    LM-BXM









Last Command: addcdred 2 3


Next Command:
```

Table 17-15 baddyred–Parameters

Parameter	Description
primary slot	Specifies the slot number of the primary card set.
secondary slot	Specifies the slot number of the secondary card set.

cnfqbin

Use the **cnfqbin** command to configure the qbin (Class of Service Buffers parameters on a selected BXM port or trunk. The **cnfqbin** command prompts you to configure the qbin from the template assigned to a logical interface.

This command now lets you accept the interface template as the values, as an option. For example, you can type in “Yes” when prompted whether the interface SCT (service class template) should be used, and the command will use the card qbin values from the qbin templates. You will not be allowed to enter values for any qbin parameter in this case. You can, however, enter desired values if the “template” option has not been chosen.

When you activate an interface (VI) with **uptrk** or **upport**, the default service template is assigned to the interface (VI). The corresponding qbin template is then copied into the card’s (BXM) data structure of that interface. You can change some of the qbin parameters by using the **cnfqbin** command. The qbin is now “user configured” as opposed to “template configured.” You can view information on the **dspqbin** screen.

When a VSI interface is activated, the default template gets assigned to an interface. The corresponding qbin template gets copied into the card qbin data structure for that interface. When you want to change this, by giving new values using the **cnfqbin** command, the qbin is now “user configured” as opposed to “template configured.” This information is displayed on the **dspqbin** screen. It indicates whether the values in the qbin are from the template assigned to the interface OR the values have been changed to user-defined values.

The **cnfqbin** command was introduced in Release 9.1 to configure any Qbin on the BXM cards. In this release, it has been extended to support virtual trunks. When the virtual trunk is dedicated to the controller, you can only configure qbin 10–15.

The **cnfqbin** command will prompt you whether “template” should be used for Qbin parameters. In this release, the **dspqbin** command now displays all the fields of a qbin template. It also indicates whether the qbin is “user configured” or “template configured.”

VC connections are grouped into large buffers called qbins. (Per-VC queues can be specified on a connection-by connection basis also). In this release, all VSI connections use qbin 10 on each interface.

You configure Multiprotocol Label Switching (formerly Tag Switching) for VSIs on a BXM card is configured using the **cnfrsrc** and **cnfqbin** commands. Qbin 10 is assigned to tag switching.

Use the **cnfqbin** command is used to adjust the threshold for the traffic arriving in Qbin 10 of a given VSI interface as away of fine tuning traffic delay.

If you use the **cnfqbin** command to set an existing qbin to disabled, the egress of the connection traffic to the network is disabled. Re-enabling the qbin restores the egress traffic.

Note CDV (Cell Delay Variation) is based on the qbin depths and the transmission speed of the virtual switch interface. The default qbin depths are specified in the service class templates (SCTs). You can configure the qbin depths by using the **cnfqbin** command.
CTD (Cell Tolerance Delay), which is the fixed delay, is based on a fixed value, and is not configurable.

The **cnfqbin** command prompts you whether “template” should be used for qbin parameters.

Full Name

Configure qbin

Syntax

cnfqbin <slot number>.<port number>.<vtrk>

Related Commands

dspqbin

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	BPX	No

Example 1

```
cnfqbin 13.1
```

Description

Create a qbin configuration on the OC-3 trunk on port 1 of slot 13 on the BPX to support MPLS (Multiprotocol Label Switching).

System Response

```
sw57           TN    SuperUser       BPX 8600    9.2    Mar. 10 1997 10:41 GMT

Port/Trunk:       13.1    [ACTIVE ]
Qbin Id :
Enable Qbin (Y/N) :
Minimum Bandwidth :
Qbin Discard threshold:
Low CLP threshold: [80] %
High CLP threshold: [80] %
EFCI threshold:[30]%




Last Command: cnfqbin 13.1
```

Example 2

cnfqbin 4.1 10

Description

Configure the Qbin 10 for port 4.1; also configure ports 4.2 and 4.3, and enter port 4.2 and 4.3 where applicable.

If the qbin is not configured, configure the queues on the ports using the **cnfqbin** command:

cnfqbin 4.1 10

enable/disable: e

For all other parameters, accept the (default).

The previous parameters can also be set for qbin 10 as follows:

cnfqbin 4.1 10 e 0 65536 95 100 40

System Response

```
Sample Display:
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1998  16:41 PST
Qbin Database 4.1 on BXM qbin 10
Qbin State:                  Enabled
Minimum Bandwith:            0
Qbin Discard threshold:      65536
Low CLP/EPD threshold:       95%
High CLP/EPD threshold:      100%
EFCI threshold:              40%

This Command: cnfqbin 4.1 10
'E' to Enable, 'D' to Disable [E]:

Next Command:
```

System Response

```
n4            TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:41 PST

Qbin Database 4.1 on BXM qbin 10

Qbin State:                  Enabled
Minimum Bandwith:            0
Qbin Discard threshold:      65536
Low CLP/EPD threshold:       95%
High CLP/EPD threshold:      100%
EFCI threshold:              40%


Last Command: cnfqbin 4.1 10 e 0 65536 95 100 40

Next Command:
```

Table 17-16 cnfqbin—Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Qbin ID	Specifies the ID number of the qbin available for use by the LSC (MPLS Controller) for VSI. The range is 0 to 255. 0 is the default. Always use 10 in 9.1.
Enable Qbin	Answer yes or no to enable your qbin configuration.
Minimum Bandwidth	Specifies the minimum bandwidth in cps (cells per second) available for the Qbin. The range is 0 to 352207. 0 is the default.
Qbin Discard Threshold	Specifies the threshold in percentage for qbin discard. The range is 0 to 100.
CLP Low Threshold	Specifies the threshold in percentage for CLP low. The range is 0 to 100. 80% is the default.
CLP High Threshold	Specifies the threshold in percentage for CLP high. The range is 0 to 100. 80% is the default.
EFCI threshold	Specifies the threshold in percentage for EFCI. The range is 0 to 100. 30% is the default.
Template	Specifies that the interface service class template should be used to configure the qbin parameters. Thus the **cnfqbin** command will use the card's qbin values from the qbin template. If you do not chose the template option, you can enter your own desired values for the qbin parameters.

Qbin Dependencies

The available qbin parameters are shown in Table 17-17. Notice that the qbins available for VSI are restricted to qbins 10–15 for that interface. All 32 possible virtual interfaces are provided with 16 qbins.

Table 17-17 cnfqbin Parameters

Template Object Name	Template Units	Template Range/Values
QBIN Number	enumeration	0 –15 (10–15 valid for VSI)
Max QBIN Threshold	u sec	1–2000000
QBIN CLP High Threshold	% of max Qbin threshold	0 – 100
QBIN CLP Low Threshold	% of max Qbin threshold	0 – 100
EFCI Threshold	% of max Qbin threshold	0 – 100
Discard Selection	enumeration	1 – CLP Hysteresis 2 – Frame Discard
Weighted Fair Queueing	enable/disable	0: Disable 1: Enable

cnfrsrc

Use the **cnfrsrc** command to partition resources for Automatic Routing Management PVCs or VSI-MPLS (Multiprotocol Label Switching).

This command was introduced in Release 9.1 to support physical trunks. It has been extended to support virtual trunks. After VSI has been enabled, the virtual trunk becomes a "dedicated" VSI virtual trunk. Note that if the trunk has already been added or if the VPI value has not been configured, you will not be able to configure the VPI value. (Switch software will block you from doing so.)

You can configure a virtual trunk to be dedicated to VSI or to Automatic Routing Management. You cannot configure a virtual trunk for both VSI and Automatic Routing Management.

The switch software:

- Allows start VPI = 0 for a VSI partition on a port interface, provided there is only one VSI partition on the port interface.
- Prevents a second VSI partition from being enabled on a port interface if the first VSI partition uses a start VPI = 0.
- Prevents a VSI partition from being disabled on a trunk interface if a PNNI controller is attached to the trunk interface controlling partition being disabled.

Configurable resources (using **cnfrsrc**) are:

- Template number (new field in Release 9.2)
- Maximum PVC LCNs
- Maximum PVC Bandwidth
- Configure Partition (Y/N)
- Partition ID
- Enable Partition (Enable/Disable)
- Minimum VSI LCNs
- Maximum VSI LCNs
- Start VSI VPI
- End VSI VPI - **Warning message will tell you that the end vsi vpi is equal to the start vsi vpi for virtual trunks**
- Minimum VSI Bandwidth
- Maximum VSI Bandwidth

Resource Partitioning

The VSIs need to partition the resources between competing controllers: Automatic Routing Management, MPLS (Multiprotocol Label Switching), and PNNI for example. You can have different types of controllers splitting up a partition's assets. For example, Automatic Routing Management, and MPLS, or Automatic Routing Management and PNNI (SVCs), but not PNNI and MPLS.

This release supports one or two partitions only. In this release, two controllers of a single type are supported. The user interface will block the activation of partitions with ID higher than 1 if the card does not support multiple partitions.

When enabling a partition, If [start_VPI, end_VPI] of the partition contains any "reserved" VPI, an error message is displayed and you are prompted for different values for start_VPI, end_VPI. Thus, if VPI 10 is used for control VCs on an interface, then you cannot include VPI 10 in any VSI partition by using the **cnfrsrc** command. An error message would be displayed.

The resources that you need to configure for a partition are shown in Table 17-18 for a partition designated ifci, which stands for interface controller 1, in this example. The three parameters that need to be distributed are: 1) number of logical connections (lcns); 2) bandwidth (bw); and 3) virtual path identifiers (vpi).

Table 17-18 ifci parameters (virtual switch interface)

ifci parameters	Min	Max
lcns	min_lcnsi	max_lcnsi
bw	min_bwi	max_bwi
vpi	min_vpi	max_vpi

The controller is supplied with a logical LCN connection number, that is slot, port, and so on., information that is converted to a logical connection number (lcn).

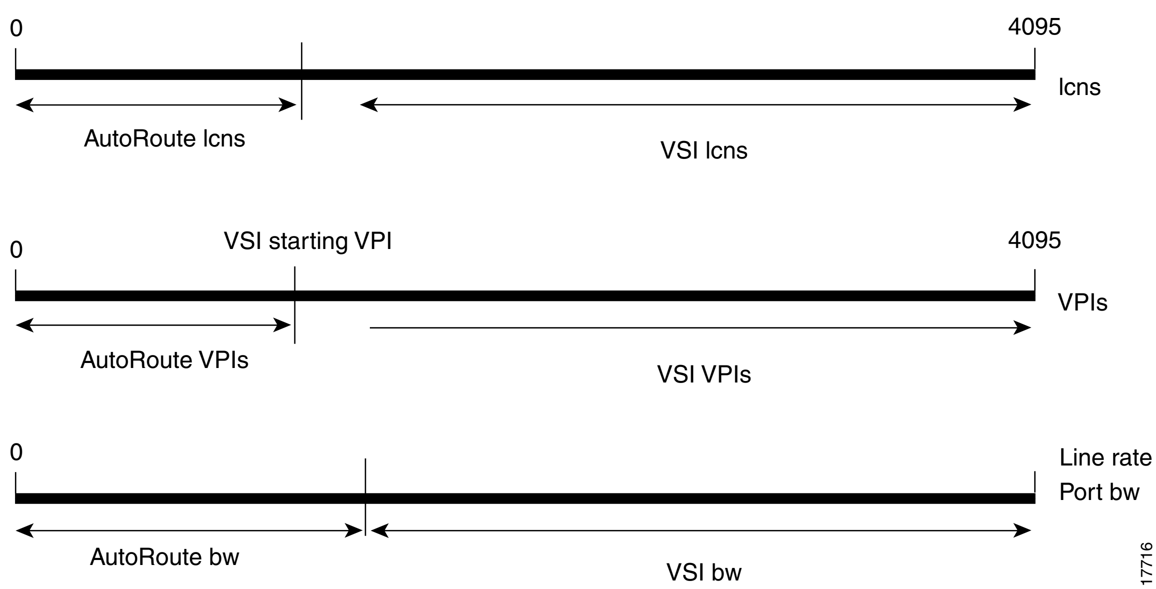
Some ranges of values available for a partition are listed in Table 17-19:

Table 17-19 Partition Criteria

	Range
trunks	1–4095 VPI range
ports	1–4095 VPI range
virtual trunk	Only one VPI available per virtual trunk since a virtual trunk is currently delineated by a specific VP
virtual trunk	Each virtual trunk can either be Automatic Routing Management or VSI, not both.

When you add a trunk, the entire bandwidth is allocated to Automatic Routing Management (formerly Automatic Routing Management). To change the allocation to provide resources for a VSI, use the **cnfrsrc** command on the BPX switch. A view of the resource partitioning available is shown in Figure 17-11.

Figure 17-11 Graphical View of resource partitioning, Automatic Routing Management and vsi



Partition Information Sent to Cisco WAN Manager

When the partition information is configured for the first time or any parameters are changed, Cisco WAN Manager will be updated through a robust message.

- vsi_min_channels:
  This field represents the minimum guaranteed channels available for a given port
- vsi_max_channels:
  This field represents the maximum number of channels available, but not guaranteed, for a port.
- vsi_vpi_start:
  This field represents the starting VPI that can be used by VSI.
- vsi_vpi_end:
  This field represents the end of the VPI range that can be used by VSI.
- vsi_min_bw:
  This field represents the minimum guaranteed bandwidth available for a port.
- vsi_max_bw:
  This field represents the maximum bandwidth available, but not guaranteed, for a port.

Partitioning

On each interface (port or trunk) on the BXM cards used for label switching, two sets of resources must be divided up between traditional PVC connections and tag switching connections. The traditional PVC connections are configured directly on the BPX platform, and tag switching connections are set up by the TSC using the VSI. The following resources are partitioned on each interface:

- Bandwidth
- Connections

As with all ATM switches, the BPX switch supports up to a specified number of connections. On the BPX switch, the number of connections supported depends on the number of port/trunk cards installed. On each interface, space for connections is divided up between traditional BPX switch permanent virtual circuit (PVC) connections, and Label Switching VCs (LVCs).

cnfrsrc Parameters, Possible Values, and Descriptions

See Table 17-20 for a listing of **cnfrsrc** parameters, ranges and values, and descriptions. These parameters appear on the **cnfrsrc** screen.

Table 17-20 cnfrsrc Parameters, Ranges/Values, and Descriptions

Object Name	Range/Values	Default	Description
VSI Start LCN	0... 64K–1	NA	Start LCN for the whole VSI partition. Each VSI sub-partition (specific partition-id) will be given lcns from this partition. subject to the min/max ranges for that partition-id specified in object 3. The Start LCN once set will not be permitted to change if there are any active/configured VSI partitions.

Table 17-20 cnfrsrc Parameters, Ranges/Values, and Descriptions (Continued)

Object Name	Range/Values	Default	Description
VSI End LCN	0...64 K–1	NA	End LCN for the whole VSI partition. If End LCN cannot be satisfied due to existing VSI connections or other constraints in this range then firmware will reject this request with a get response (same message tag) with this Object indicating the possible new End LCN that firmware can accommodate.
VSI partition	0...255	0	identifies the partition
Partition state	0 = Disable Partition 1 = Enable Partition	NA	For Partition state = 1, Objects (8, 9, A, B, C, D, E, F) are mandatory
Min LCNs	0...64K	NA	Min lcns (conns) guaranteed for this partition
Max LCNs	0...64K	NA	Maximum LCNs permitted on this partition
Start VPI	0 .. 4095	NA	Partition Start VPI
End VPI	0 .. 4095	NA	Partition End VPI
Min Bw	0 .. Line Rate	NA	Minimum Partition bandwidth
Max Bw	0 .. Line Rate	NA	Maximum Partition bandwidth

Feature Mismatching to Verify VSI Support

In this release, the **cnfrsrc** and **addshelf** commands, in addition to other configuration commands, performs mismatch verification on the BXM and UXM cards. For example, the **cnfrsrc** and **addshelf** commands will verify whether the cards both have VSI 2.0 support configured. Refer to “Feature Mismatching” section on page 18-1 for more information on Feature Mismatching in Release 9.2.

The Feature Mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Full Name

Configure resources

Syntax

cnfrsrc <slot.port.vtrk>

or

cnfrsrc <slot>.<port>.<vtrk> <maxpvclcns> <maxpvcbw> <partition> <e/d> <minvsilcns> <maxvsilcns> <vsistartvpi> <vsiendvpi><vsiminbw> <vsimaxbw>

Related Commands

dsprsrc

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

cnfrsrc 4.1 256 26000 1 e 512 16384 2 15 26000 100000

Description

Configure the VSI partition for port 4.1.

System Response

```
n4             TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:40 PST
Port/Trunk : 4.1
Maximum PVC LCNS:              256     Maximum PVC Bandwidth:26000
Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1
Partition State :              Enabled
Minimum VSI LCNS:              512
Maximum VSI LCNS:              7048
Start VSI VPI:                 2
End VSI VPI :                  15
Minimum VSI Bandwidth :        26000       Maximum VSI Bandwidth :        100000

Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000

Next Command:
```

Example 2

cnfrsrc 13.1

Description

Partition resources on the OC-3 trunk on port 1 of slot 13 on the BPX to support a service such as VSI-MPLS (or PNNI SVCs).

System Response

```
n4             TN    SuperUser       BPX 8620    9.2      Apr. 4 1998  16:40 PST
Port/Trunk : 4.1
Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000
Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1
Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                2
End VSI VPI :                 15
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000

Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000

Next Command:
```

Example 3

cnfrsrc 4.1

Description

Port 4.1 is the slave interface to the label switch controller. Configure the VSI partitions for port 4.1 as follows:

cnfrsrc 4.1

PVC LCNs: [256] {accept default value}

max PVC bandwidth: 26000

partition: 1

enabled: e

VSI min LCNs: 512

VSI max LCNs: 7048 {varies with BXM type

VSI start VPI: 2

VSI end VPI: 15

VSI min b/w: 26000

VSI max b/w: 100000

or with one entry as follows:

cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000

System Response

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1998  16:40 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                2
End VSI VPI :                 15
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000



Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000


Next Command:
```

Note It is possible to have PVCs terminating on the Tag Switch Controller itself. This example reserves approximately 10 Mbps (26000 cells/sec) for PVCs, and allows up to 256 PVCs on the switch port connected to the LSC.

Note The VSI max and min logical connections (LCNs) will determine the maximum number of tag virtual connections (TVCs) that can be supported on the interface. The number of TVCs required on the interface depends on the routing topology of the tag switch.

Note By default the LSC will use either a starting VSI VPI of 1 or 2 for tag switching, whichever is available. If both are available, a starting VSI VPI of 1 is used. The VPI range should be 2–3 on a BPX VSI connected to a 7200 or 7500 AIP. If VPI 2 is not to be used, the tag switching VPI interface configuration command can be used on the TSC to override the defaults

---

Note The VSI range for tag switching on the BPX switch is configured as a VSI partition, usually VSI partition number 1. VSI VPI 1 is reserved for Automatic Routing Management, so the VSI partition for tag switching should start at VPI 2. Two VPIs are sufficient for the current release, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 2–15.

Table 17-21 lists the **cnfrsrc** parameters, focusing more on configuring resources for VSI partitions (an MPLS controller, for example). For more information on configuring resources for Automatic Routing Management PVCs, refer to the **cnfrsrc** command in Chapter 4, “Setting Up Trunks” and Chapter 5, “Setting Up Lines.”

Table 17-21 cnfrsrc—Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>slot.port.vtrk</td><td>Specifies the BXM card slot and port number and virtual trunk.</td></tr>
<tr><td>Maximum PVC LCNs</td><td>The maximum number of LCNs allocated for Automatic Routing Management PVCs for this port. The range is 1 to 256. 256 is the default. For trunks, there are additional LCNs allocated for Automatic Routing Management that are not configurable.

You can use the dspcd <slot> command to display the maximum number of LCNs you can configure using the cnfrsrc command for the given port. For trunks, “configurable LCNs” represent the LCNs remaining after the BCC has subtracted the “networking LCNs” needed. A trunk has 270 networking LCNs, or channels. You can use the dspcd command to display VSI channels also.

For a port card, a larger number is shown, as compared with a trunk card. This is because a trunk uses 270 networking LCNs, as compared with a port card, which uses no networking LCNs. You can use dspcd to display VSI channels also.

Setting this field to “0” would disable Automatic Routing Management PVCs on the specified port.

Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management connections on a BXM card. Also, if these parameters do not have values greater than 0, you will be unable to change the connection channel amount when you configure the BXM trunk using cnftrk.

Logical Interface (slot.port.vtrk for trunks and slot.port for lines).

The bandwidth is logical interface based. The default value for this object is the line rate of this interface.

<table><tr><th>Card Type</th><th>Bandwidth</th></tr><tr><td>BXM E3</td><td>80000</td></tr><tr><td>BXM T3</td><td>96000</td></tr><tr><td>BXM OC-3</td><td>353208</td></tr><tr><td>BXM OC-12</td><td>1412830</td></tr></table></td></tr>
<tr><td>Maximum PVC Bandwidth</td><td>Specifies the maximum bandwidth of the port allocated for Automatic Routing Management use. The range is 0 to 352207. 0 is the default. You can configure the Maximum PVC Bandwidth value for ports, but not for trunks.

Note that you must specify a value greater than 0 for the Maximum PVC LCNs, Maximum PVC Bandwidth, and Maximum VSI LCNs parameters. Otherwise, you will not be able to create any Automatic Routing Management PVCs on the BXM card.</td></tr>
<tr><td>Configure Partition</td><td>Answer yes or no to begin configuring resources for the partition. To configure Automatic Routing Management PVCs, enter “n” for No. You will not be prompted to enter VSI options to configure VSI partition resources.
However, if you want to configure VSI options, enter “y” for yes, and you will be prompted to configure partition resources for VSI.</td></tr>
</table>

Table 17-21 cnfrsrc—Parameters (Continued)

Parameter	Description
Partition ID	Specifies the ID number of the partition. In Release 9.2, use 1. In Release 9.1, use 1 for the partition ID. (The default is 0. The range of values for Partition ID is 0–255.) In this release, you may use 2.
Enable Partition	Answer yes or no to enable your configured partition.
Minimum VSI LCNs	The minimum number of LCNs guaranteed for this partition. The range is 1 to 256. 0 is the default.The VSI controller guarantees at least this many connection endpoints in the partition, provided there are sufficient free LCNs in the common pool to satisfy the request at the time the partition is added. When a new partition is added or the value is increased, it may be that existing connections have depleted the common pool so that there are not enough free LCNs to satisfy the request. The BXM gives priority to the request when LCNs are freed. The net effect is that the partition may not receive all the guaranteed LCNs (min LCNs) until other LCNs are returned to the common pool. You can increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. To avoid this deficit condition, which could occur with maximum LCN usage by a partition or partitions, it is recommended that all partitions be configured ahead of time before adding connections. Also, it is recommended that all partitions be configured before adding a VSI controller using the **addshelf** command.
Maximum VSI LCNs	The total number of LCNs the partition is allowed for setting up connections. The min LCNs is included in this calculation. If max LCNs equals min LCNs, then the max LCNs are guaranteed for this partition. Otherwise, (max – min) LCNs are allocated from the common pool on a FIFO basis. If the common pool is exhausted, new connection setup requests will be rejected for the partition, even though the maximum LCNs has not been reached. You may increase this value dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. You may not decrease the value dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. Different types of BXM cards support different maximum values. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum value. Note that you must specify a value greater than 0 for the Maximum VSI LCNs, Maximum PVC Channels, and Maximum PVC Bandwidth parameters. Otherwise, you will not be able to add any connections on a BXM card.

Table 17-21 cnfrsrc—Parameters (Continued)

Parameter	Description
Start VSI VPI	By default the LSC (for example, the 7200 or 7500 series router) will use either a starting VSI VPI of 1 or 2 for MPLS (Multiprotocol Label Switching), whichever is available. If both are available, a starting VSI VPI of 1 is used. The VPI range should be 2–15 on a BPX 8620 VSI. The VSI range for MPLS (Multiprotocol Label Switching) on the BPX 8620 is configured as a VSI partition, usually VSI partition number 1. VSI VPI 1 is reserved for Automatic Routing Management PVCs. (This restriction applies only to trunks, not to ports. For a port, you can use any VPI value.) For a port UNI, the VPI range is 1 to 255. For a port NNI, the range is 1 to 4095. For trunks that do not have Automatic Routing Management configured, the VPI ranges are the same as for ports. The VSI partition for MPLS (Multiprotocol Label Switching) should start at VPI 2. If VPI 2 is not to be used, you can use the MPLS (Multiprotocol Label Switching) VPI interface configuration on the LSC (Label Switching Controller) to override the defaults. For trunks with Automatic Routing Management configured, the range is 2 to 4095. Always set to 2 for trunks. Should be set to "2" or higher for ports in trunk mode because "1" is reserved for Automatic Routing Management. For ports in port mode it should be set to "1". By default the TSC (for example, 7200 or 7500 series router) will use either a starting VSI VPI of 1 or 2 for tag switching, whichever is available. They default to 1.
End VSI VPI	Two VPIs are sufficient for Release 9.1, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 2–15. The range is the <*Start VSI VPI* > value to 4095.
Minimum VSI Bandwidth	The minimum port bandwidth that can be used by this partition in cells/second. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.
Maximum VSI Bandwidth	The maximum port bandwidth that can be used by this partition. This value is used for VSI Qbin bandwidth scaling. The range is 0 to <*Maximum Line Rate*>. For example, the OC-3 line rate is 352207. 0 is the default.

cnfvsiif

You can use the **dspvsiif** command to display a service class template assigned to an interface (VI). You can also display a summary of the resources allocated to the VSI partition on a given interface. Multiple users are allowed to use the **dspvsiif** at one time.

Assigning a Service Template to an Interface

A default service template is assigned to a logical interface (VI) when you up the interface by using **upport/uptrk**.

For example:

- **uptrk 1.1**
- **uptrk 1.1.1 (virtual trunk)**
- **upport 1.1**

This default template has the identifier of 1. You can change the service template from service template 1 to another service template using the **cnfvsiif** command. The **dspvsiif** command allows you to display the template associated with the interface. For example:

- **cnfvsiif 1.1 2**
- **cnfvsiif 1.1.1 2**
- **dspvsiif 1.1**
- **dspvsiif 1.1.1**

cnfvsiif example

You use the **cnfvsiif** command to assign a selected service template to an interface (VI) by specifying the template number. It has the following syntax:

```
cnfvsiif <slot.port.vtrk> <tmplt_id>
```

Full Name

Configure a service class template and assign it to an interface

Syntax

cnfvsiif <slot.port.vtrk> <tmplt_id>

Related Commands

cnfrsrc, dsprsrc, cnfqbin, dspqbin

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	BPX	Yes

Example 1

cnfvsiif 11.1 2

System Response

```
sw53           TN     StrataCom       BPX 8600   9.2.a5    Date/Time Not Set

              Port: 11.1

              Service Class Template ID: 2






Last Command: cnfvsiif 11.1 2


Next Command:
```

cnfvsipart

Use this command to configure VSI partition characteristics. Only VSI ILMI can be enabled by using this command.

Full Name

Configure VSI partition characteristics.

Syntax

cnfvsipart <slot.port.[vtrk]> <part_id> <enable_option>

Table 17-22 cnfvsipart–Parameters

Parameter	Description
slot.port.[vtrk]	Slot, port (and virtual port if applicable) of the interface.
part_id	Partition ID corresponding to the VSI partition.
enable_option	This parameter indicates whether to enable or disable VSI ILMI functionality. Valid values: • Y enables the VSI ILMI session. • N disables the VSI ILMI session.

Related Commands

cnfrsrc, **dspvsipartcnf, cnfport, cnftrk**

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	Yes	BPX	Yes

delctrlr

Deletes VSI capabilities on a trunk interface to which a Feeder of type AAL5 is attached. Use this command to delete a controller, such as a PNNI SES controller, from a BPX node. It deletes the VSI control channels used to communicate between the VSI master on the PNNI controller and the VSI slaves on the BXM cards.

You run this command as the first step in deleting a PNNI controller from a BPX node. The second step is to run the command **delshelf** to delete the AAL5 feeder.

(Do not use **delctrlr** to delete a VSI Label Switching controller from a BPX node; you must use **delshelf** to delete a VSI Label Switching controller from a BPX node.)

In this release, PNNI runs on the Service Expansion Shelf (SES) hardware.

To add VSI controller capabilities onto the newly-created AAL5 interface you use the **addctrlr** command. You are prompted to enter the controller ID and partition ID. This creates an interface through which a PNNI controller can use the VSI protocol to control the node resources that were previously specified by using the **cnfrsrc** command.

You remove a PNNI controller from a BPX node by using the **delctrlr** command. For example, this might be a VSI controller such as an PNNI controller configured with VSI capabilities as an AAL5 interface shelf to a BPX. When you delete one of the controllers by using the **delctrlr** command, the master-slave connections associated with this controller are deleted. The control VCs associated with other controllers managing the same partition will not be affected.

Note To add a VSI Label Switch Controller, you use **addshelf** and **delshelf** commands, as in releases previous to Release 9.2.

Full Name

Delete VSI capabilities from a AAL5 feeder interface.

Syntax

delctrlr <slot.port> <controller id>

Table 17-23 delctrlr–Parameters

Parameter	Description
slot.port	Slot and port numbers corresponding to the feeder trunk.
controller id	Controller ID number corresponding to the PNNI controller you are deleting. ID numbers should correspond to an active PNNI controller. Valid controller values are: 1 – 32

Related Commands

addctrlr, dspctrlrs, dspnode

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	BPX	Yes

Example 1

delctrlr 10.3

Description

Delete VSI controller with interface shelf (feeder) type of AAL5 connected on trunk 10.3 from the list of controllers connected to BPX node named "night".

System Response

```
night          TN    StrataCom       BPX 8600    9.2.00 Apr. 11 1998 14:31 GMT

                        BPX Controllers Information

Trunk    Name     Type    Part Id     Ctrl Id     Ctrl IP     State
10.3     PAR       VSI     1          2           192.0.0.0   Enabled
11.1     VSI       VSI     2          2           192.0.0.0   Disabled




Last Command: delctrlr 10.3
```

System Response

```
night          TN    StrataCom       BPX 8600    9.2.   Apr. 11 1998 14:31 GMT

                        BPX Controllers Information

Trunk    Name     Type    Part Id     Ctrl Id     Ctrl IP     State
10.3     PAR       VSI     1          2           192.0.0.0   Enabled
11.1     VSI       VSI     2          2           192.0.0.0   Disabled




Last Command: delctrlr 10.3
```

Example 2

delctrlr <slot.port><controller_id>

Description

Deletes controller from port 3 on slot 10, with controller name E, and controller ID of 1.

System Response

```
night          TN    StrataCom       BPX 8600    9.2.00 Apr. 11 1998 14:31 GMT

                        BPX Controllers Information

Trunk    Name     Type     Part Id    Ctrl Id    Ctrl IP      State
10.3     PAR      VSI      1          1          192.0.0.0    Enabled
11.1     VSI      VSI      2          2          192.0.0.0    Disabled




Last Command: delctrlr 10.3
```

delshelf

Deletes an interface shelf from a tiered network. The identifier for an interface shelf is either the trunk number or the name of the shelf. Normally, you do not execute **delshelf** only at the hub node, but on the IGX/AF itself. The command **delshelf** has the single function of letting you turn off LMI if the trunk is not allowing communication. In contrast to the **deltrk** command, you can execute **delshelf** at any time if no connections terminate at the trunk.

Deleting a Controller

You remove a controller from the node by using the **delshelf** command. When one of the controllers is deleted using the **delshelf** command, the master-slave connections associated with this controller will be deleted. The control VCs associated with other controllers managing the same partition will not be affected.

The deletion of the controller will trigger a new VSI configuration CommBus (internal BPX protocol) message. This message will include the list of the controllers attached to the node. The controller deleted will be removed from the list. This message will be sent to all active slaves in the shelf. In cluster configurations, deleting a controller will be communicated to the remote slaves by the slave directly attached through the inter-slave protocol.

While there is at least one controller attached to the node controlling a given partition, the resources in use on this partition should not be affected by a controller being deleted. Only when a given partition is disabled, the slaves will release all the VSI resources used on that partition.

Full Name

Delete an interface shelf.

Syntax

delshelf <trunk> | <shelf-name>

Related Commands

addshelf, dspnode

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	IGX, BPX	Yes

Example 1

```
delshelf 4.1
```

Description

Delete shelf trunk A241 from a BPX node.

System Response

```
nmsbpx23       TN    SuperUser       BPX 8600    9.2    Aug. 16 1998 13:26 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 1.3     AXIS240   AXIS      OK
11.2     A242      AXIS      OK









Last Command: delshelf A241

Shelf has been deleted
Next Command:
```

Table 17-24 delshelf–parameters

Parameter	Description
trunk or shelf name	Specifies the slot and port number of the trunk or the name of the interface shelf.

delyred

This command disables Y-redundancy for the card set in the specified primary slot number. If the secondary card slot is being used as the active slot at the time you use the **delyred** command, the system attempts to switch back to the primary slot. The substitution takes place only if the primary slot has a complete set of cards and the cards are in a Standby or a Standby-F state (not if they are Failed). See the **dspcds** description for information on card states. See the **addyred** and **dspyred** commands for more information on Y-cable redundancy.

When you issue the **delyred** command, it always completes. If the primary card is incomplete, control will still be given to the primary card.

Full Name

Delete Y-cable redundancy

Syntax

delyred <primary slot>

Related Commands

addyred, **dspyred**, **prtyred**

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	Yes	IGX, BPX	Yes

Example

`delyred` 16

Description

Disable Y-cable redundancy at slot 16.

dspchuse

The **dspchuse** command displays the a summary of the channel distribution in a given slot. It shows the distribution of channels between AutoRoute pvcs, networking channels, VSI management channels, and channels allocated to the VSI slave.

This command applies only to BXM cards. Previously a debug command; **dspchuse** is available to multiple users at all privilege levels in this release.

Full Name

Display channel distribution

Syntax

dspchuse <slot >

Related Commands

dspvsiif, dspvsipartinfo

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Parameters

Parameter	Description
max	Maximum number of channels supported on the card or port group.
used	Number of channels currently used; this includes all types of channels: networking channels, pvcs, svcs, vsi master-slave vcs, and channels allocated to VSI partitions.
avail	Number or channels still available for use.
netw	Number of network channels used. For each trunk interface (feeder trunk, physical trunk, or virtual trunk) that is upped some channels are reserved for networking. For a feeder or a physical trunk 271 channels are reserved. For a virtual trunk, the first one upped on the port will reserve 271, any subsequent virtual trunk on the same port will reserve 1 more channel.
pvc cnfg	Number of pvcs configured.
svc cnfg	Number of svcs configured.

Parameter	Description
vsi mgmt	Number of channels used for VSI master-slave vcs. Note: the sum of port group VSI management vcs may be less than the number of VSI management vcs at the card level. This is because the backplane management connection (the leg of the connection from the backplane to the slave) requires resources at the card level but not at the port group level.
vsi cnfg	VSI channels reserved for use by the slave to set up connections requested via the VSI interface. Although the configuration of the partitions is done on a per-interface basis, the pool of LCNs is managed at the card level and at the port group level.
pvc used	Channels currently used by AutoRoute connections.
vsi min	VSI min channels configured for a partition via the **cnfrsrc** command.
vsi max	VSI max channels configured for a partition via the **cnfrsrc** command.

Example 1

dspchuse 13

Description

Display channel management summary for slot 13.

System Response

```
sw53 TN StrataCom BPX 8600  9.2.10  Jan. 10 1999 14:31 GMT

            Channel Management Summary for Slot 13

          max    used   avail   netwpvc  cnfgvsi  mgmt vsi cnf

card 13:  16320  8675   7645    1358    2304     13    5000
port grp 1:8160  5849   2311    813     1024     12    4000
port grp 2:8160  2825   5335    545     1280      0    1000

          pvc cnfg pvc used nw used vsi mgmt vsi min vsi max

port 1:   256              0    271       0
part 1:                                      1000   4000
part 2:                                      2000   4000
port 2:   256              0    271       0
port 3:   256              0    271      12

This Command: dspchuse 13

Continue?
```

dspctrlrs

Use the **dspctrlrs** command to display all VSI controllers, such as a SES PNNI controller on a BPX or IGX node. This command lists:

- the controller ID
- the partition the controller use
- the trunk/interface to which a controller is attached
- the controller type (always a VSI controller)
- the interface type (AAL5, VSI (Label Switching)
- MGX 8220 (formerly called AXIS) interface shelf
- the name of the controller/entity on which the controller exists (that is, node name, equipment name).

(Note that you use **addshelf** and **delshelf** to add and delete a VSI controller such as a Label Switching Controller to a BPX node.)

You can also the **dspnode** command to display the VSI controllers on a BPX node.

Full Name

Displays all VSI controllers, for example, all PNNI controllers such as PNNI), on a BPX or IGX node.

Syntax

dspctrlrs <slot.port><controller name string><partition_id><controller_id>

Related Commands

addctrlr, addshelf, cnfctrlr, delctrlr, dspnode

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	IGX, BPX	Yes

Example 1

```
dspctrlrs
```

Description

Display VSI controllers on BPX node sw174.

System Response

```
sw174          TRM    StrataCom       BPX 8620    9.2.xS  Sep 20 1998 14:31 GMT


                        BPX 8620 VSI controller information

Ctrl Id   Part Id    Trunk   Ctrlr Type    Intfc Type    Name
1        1           2.1     VSI           AAL5         SIMFDR0



Last Command: dspctrlrs
```

dspqbin

The **dspqbin** command displays the qbin resources on the selected port. It displays the qbin parameters currently configured for an interface, and shows whether the qbin resources have been configured by the user OR by a template. The **dspqbin** command displays whether the qbin has been configured by a user or by the template assigned to the interface. It also displays whether the qbin has EPD enabled/disabled.

The **dspqbin** commands displays the current qbin configuration on this trunk/port/virtual trunk.

The **dspqbin** command displays all the fields of a qbin template in Release 9.2. It also indicates whether the qbin is “user configured’ or “template configured”.

For this release, Class of Service buffer 10 is used for tag switching connections. Check the queue buffer 10 configurations for port 4.1 as follows:

dspqbin 4.1 10

Full Name

Display qbin

Syntax

dspqbin <slot number>.<port number> [qbin-id]

Note To display a specific qbin configuration on the selected port, enter qbin-id as an optional parameter to the **dspqbin** command. For Release 9.1, use only qbin 10 for VSI connections.

Related Commands

cnfqbin

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	No	BPX	No

Example 1

dspqbin 13.1

Description

Display the current qbin configuration on the OC-3 trunk on port 1 of slot 13 on the BPX to support MPLS.

System Response

```
sw53           TN    StrataCom       BPX 8600  9.2.a5    Date/Time Not Set

Qbin Database 11.1 on BXM qbin 10       (Configured by ATMF1 Template)
                                         (EPD Disabled on this qbin)

Qbin State:                  Enabled
Qbin Discard threshold:      8
Low CLP threshold:           90%
High CLP threshold:          95%
EFCI threshold:              50%




Last Command: dspqbin 11.1 10


Next Command:
```

Example 2

dspqbin 4.1 10

Description

Display the current qbin configuration on slot 4, port 1, qbin 10.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:42 PST

Qbin Database 4.1 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       28800 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          100%






Last Command: dspqbin 4.1 10
```

Example 3

```
dspqbin 2.1.1 10
```

Description

Display qbin 10 on slot 2, port 1, virtual trunk 1.

System Response

```
Qbin Database 2.1.1 on BXM qbin 10

Qbin Discard threshold:       9800
Low CLP/EPD threshold:        60%
High CLP threshold:           80%
EFCI threshold:               80%
```

Example 4

`dspqbin 13.1.1 10`

Description

Display qbin 10 configuration for virtual trunk 1, on port 1 of card slot 13.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:42 PST

Qbin Database 13.1.1 on BXM qbin 10     (Configured by ATMF1 Template)
                                        (EPD Disabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       12 cells
Low CLP Threshold:       60%
High CLP Threshold:      80%
EFCI Threshold:          100%




Last Command: dspqbin 13.1.1 10
```

Table 17-25 dspqbin Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Qbin ID	Specifies the ID number of the qbin available for use by the LSC (MPLS Controller) for VSI. The range is 0 to 255. 0 is the default. Always use 10 in Release 9.1; use qbin 13 in Release 9.2.

Class of Service Buffer Descriptor Template Configuration

Table 17-26 below lists parameters included in the Class of Service (CoS) Buffer (qbin) portion of the Service Class Templates. (Note that a qbin is a platform-specific instance (for example, BXM) of the more general Class of Service Buffer. A firmware command sends a command (message) to switch software to initialize the CoS Buffer Descriptors in the Service Class Templates. This command may contain multiple instances of qbin number, each indicating a new qbin configuration.

Table 17-26 Class of Service Buffer Parameters That Display on dspqbin Screen

Object (Parameter) Name	Range/Values	Default	Description
Service Template ID	0 – 7	R	Service Class Template number for this parameter set.
QBIN Number	0 – 15	R	Identifies the target qbin to modify
Direction	0: Ingress 1 : Egress	R	Indicates whether the QBIN configuration applies to the ingress or egress of the card.
Priority	0 – 15	R	Parameter defines the relative priority of the QBIN in relationship to the other QBINs in the VI. Zero is the highest priority and 15 is the lowest priority.
Discard Selection	1 – CLP Hysteresis 2 – Frame Discard	R	Indicates whether QBIN should perform the CLP Hysteresis or the Frame Discard option. The QBIN can only be configured to do one or the other.
Max Threshold	0 – ? cells	R	Determines the amount of cell memory to dedicated to this Qbin
CLP High Threshold	0 – 100%	R	Parameter determines at which level in the QBIN CLP-tagged cells get discarded. Discard continues until the QBIN depth drops below the QBIN CLP Low Threshold.
CLP Low Threshold	0 – 100%	R	Parameter determines at which level in the QBIN CLP-tagged cells get admitted.
EFCI Threshold	0 – 100%	R	Parameter determines at which level in the QBIN EFCI bits get tagged in the departing cell(s).
EPD 0 Threshold	0 – 100%	R	QBIN Frame Discard threshold for CLP 0 traffic.
WFQ enable	0: Disable 1: Enable	R	Indicates whether weighted fair queueing/ traffic shaping is enabled for this qbin.

dspqbint

Display the qbin (class of service buffer) templates. You can enter optional parameters to display the service classes in a specified qbin template.

Use the **dspqbint** command to display the service class template number assigned to an interface (VI). The **dspsctmplt** command has three levels of operation:

dspqbint	With no arguments lists all the service templates resident in the node.
dspqbint <tmplt_id>	Lists all the service classes in the template
dspqbint <tmplt_id>	Lists all the parameters of that service class

Additional service template commands you can use are:

cnfqbin	Configures the qbin. You can answer yes when prompted and the **cnfqbin** command will use the card's qbin values from the qbin templates.
dspqbin	Displays qbin parameters currently configured for the virtual interface.
dspcd	Display the card configuration.

See the sections that precede the VSI commands at the front of this chapter for more high-level information on VSI and more detailed information on service class templates in Release 9.2 and how you use them to configure connections with specified service classes.

Full Name

Display qbin template

Syntax

dspqbint <template #><qbin #>

Description

Display a service class template number, which identifies one of the templates between 1–3, and the qbin number.

Related Commands

dspsct, dspqbin, cnfrsrc, dsprsrc, cnfvsiif, dspvsiif

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dspqbint <template #> <qbin>

Description

Displays the qbin template number 1 for a specified qbin (10).

System Response

```
sw53           TN    StrataCom       BPX 8600  9.2.a5    Date/Time Not Set

         Qbin Template:    1         Qbin:  10

CLP High        95        (% of Max Depth)
CLP Low         90        (% of Max Depth)
EFCI Threshold  50        (% of Max Depth)
EPD             Enabled
Vc Shaping      Enabled
Max Depth       2000      (micro secs)




Last Command: dspqbint 1 10


Next Command:
```

dsprsrc

The **dsprsrc** command displays the partition of all the resources on the specified trunk or port. It also displays virtual trunks for a specified trunk or port. Resources not applicable to virtual trunks are not displayed.

Full Name

Display resources

Syntax

dsprsrc <slot number>.<port number>.<vtrk> [partition_id]

Note To display a specific partition, you can enter the optional partition_id parameter for the **dsprsrc** command. In this release, the valid partitions are 1 and 2.

Related Commands

cnfrsrc, cnfqbin, dspqbin

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dsprsrc 3.2.1

Description

Display partition resources on the OC-3 trunk on card slot 3, port 2, and virtual trunk 1 on the BPX node.

System Response

```
sw57           TN    SuperUser       BPX 8620    9.2    Mar. 10 1998 10:41 GMT


Port/Trunk : 3.2.1
Template: 3
Maximum PVC LCNS:             256     Maximum PVC Bandwidth:1411679
Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1
Partition State :             Enabled
Minimum VSI LCNS:             0
Maximum VSI LCNS:             1       Used VSI LCNs: 25
Start VSI VP:               1
End VSI VPI :                 1
Minimum VSI Bandwidth :       0       Maximum VSI Bandwidth :        0
```

Example 2

`dsprsrc 13.1`

Description

Display partition resources on the OC-3 trunk on port 1 of slot 13 on the BPX to support MPLS.

System Response

```
sw57           TN    SuperUser       BPX 8620    9.2      Mar. 10 1997 10:41 GMT

Port/Trunk:       13.1    [ACTIVE  ]
Interface:          OC-3-2
Available Channels: 16000


  Maximum PVC Channels         :   256 (default)
  Maximum PVC Bandwidth        :   352207 cps

  Partition ID                             : 0
  VSI Signalling VCI                 : 32 (default)
  Minimum VSI LCNs                : 0
  Maximum VSI LCNs                : 0
  Start VSI VPI                          : 0
  End VSI VPI                            : 0
  Minimum VSI Bandwidth         : 0 cps
  Maximum VSI Bandwidth        : 0 cps




Last Command: dsprsrc 13.1
```

Example 3

dsprsrc 4.1 1

Description

Display partition resources on VSI trunk 4.1 (slot.port), specifying partition ID of 1. Note that if the partition is disabled, you only see the Max PVC LCNs Max. PVC Bandwidth available, and Partition ID number parameters.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:27 PST

Port/Trunk :4.1

Maximum PVC LCNS:           256     Maximum PVC Bandwidth:95000

Partition 1

Partition State :           Disable




Last Command:dsprsrc 4.1 1
```

Example 4

dsprsrc 4.1 1

Description

Display partition resources on VSI trunk 4.1, and partition ID 1. (If the partition is enabled, more parameters related to how resources are partitioned are displayed.)

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:35 PST

Port/Trunk :4.1

Maximum PVC LCNS:            256     Maximum PVC Bandwidth:92000

Partition 1

Partition State :            Enabled
Minimum VSI LCNS:            20
Maximum VSI LCNS:            30
Start VSI VPI:               4
End VSI VPI :                6
Minimum VSI Bandwidth :      2000    Maximum VSI Bandwidth :       3000



Last Command:dsprsrc 4.1 1
```

Example 5

dsprsrc 4.1 1

Description

Display partition resources on VSI trunk 4.1.

System Response

```
n4            TN    SuperUser       BPX 8620      9.2      Apr. 4 1998  16:47 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                2
End VSI VPI :                 15
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000



Last Command: dsprsrc 4.1 1


Next Command:
```

Table 17-27 dsprsrc–Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Partition ID	Specifies the ID number of the partition available for use by the LSC (MPLS Controller) for VSI. The range is 0 to 255. 0 is the default. Always use 1 in Release 9.1.

dspsct

The **dspsct** command has three levels of operation:

- **dspsctmplt** specified without any arguments (for example, **dspsct**) lists all the templates in the node.
- **dspsctmplt** <tmplt_id> lists all the service classes in that template.
- **dspsctmplt** <tmplt_id> <sc> lists all the parameters of that service class.

Extended Services Types Support

The service-type parameter for a connection is specified in the connection bandwidth information parameter group. The service-type and service-category parameters determine the service class to be used from the service template.

Connection Admission Control (CAC)

For this release, when a connection request is received by the VSI Slave, it is first subjected to a Connection Admission Control process before being forwarded to the firmware layer responsible for actually programming the connection. The granting of the connection is based on the following criteria:

LCNs available in the VSI partition

- Qbin
- Service Class

QoS guarantees

- max CLR
- max CTD
- max CDV

When the VSI slave accepts (that is, after CAC) a connection setup command from the VSI master in the Label Switch Controller, it receives information about the connection including service type, bandwidth parameters, and QoS parameters. This information is used to determine an index into the VI's selected Service Template's VC Descriptor table thereby establishing access to the associated extended parameter set stored in the table.

Supported Service Types

The service type identifier is a 32-bit number. The service type identifier appears on the **dspsct** screen when you specify a service class template number and service type; for example:

dspsct <2> <vbrrt1>

A list of supported service templates and associated qbins, and service types is shown in Table 17-28.

Table 17-28 Service Template and Associated Qbin Selection

Template Type	Service Type ID	Service Type	Parameters	Associated Qbin
VSI Special Types	0x0001	Default		13
	0x0002	Signaling		10
ATMF Types	0x0100	cbr.1	**ATM Forum (ATMF) Types**	10
ATMF1 and	0x0101	vbr.rt1		11
ATMF2 templates	0x0102	vbr2.rt		11
(for PNNI controllers)	0x0103	vbr3.rt	See **dspsct** command for sample parameters for various service types, such as VbrRt1, Cbr1, etc.	11
	0x0104	vbr1.nrt		12
	0x0105	vbr.2nrt		12
	0x0106	vbr.3nrt		12
	0x0107	ubr.1		13
	0x0108	ubr.2		13
	0x0109	abr		14
	0x010A	cbr.2		10
	0x010B	cbr.3		10
MPLS Types	0x0001	Default		13
(for MPLS controllers)	0x0200	Signaling		10
	0x0201	label cos0		10
	0x0202	label cos1		11
	0x0203	label cos2		12
	0x0204	label cos3		13
	0x0205	label cos4		10
	0x0206	label cos5		11
	0x0207	label cos6		12
	0x0210	label cos7		13
		label ABR		14

Details of Connection (VC) Parameters Used in Service Class Templates

Listed below is some detailed information on connection (VC) parameters used in service class templates. Some of these parameters may appear on the **dspsct** display.

```
Qbin #
Description      CoS Buffer (Qbin) to use for this CoS
Range/Values:    10 - 15 (for Release 9.2)
Units:           enumeration
UPC Enable
```

Description: Enable/Disable Policing function. The first 2 values are consistent with the definition for the older cards. Option #2 and #3 are new and provide the ability to turn on policing on just GCRA #1 (PCR policing) or #2 (SCR policing).
Range/Values: 0 –3
0: Disable both GCRAs
1: Enable both GCRAs
2: Enable GCRA #1 only (PCR policing)
3: Enable GCRA #2 only (SCR policing)
Units: enumeration
UPC CLP Selection
Description: Selects processing of policing Buckets based on the CLP bit.
Range/Values: 0 –2
0 - Bk 1: CLP (0+1), Bk 2: CLP (0)
1 - Bk 1: CLP (0+1), Bk 2: CLP (0+1)
2 - Bk 1: CLP (0+1), Bk 2: Disabled
Units: enumeration
Policing Action (GCRA #1)
Description: Indicates how cells that fail the second bucket (SCR bucket) of the policer should be handled, if policing is enabled.
Range/Values: 0 - Discard
1 - Set CLP bit
2 - Set CLP of untagged cells, disc. tag'd cells
Units: enumeration
Policing Action (GCRA #2)
Description: Indicates how cells that fail the second bucket (SCR bucket) of the policer should be handled, if policing is enabled.
Range/Values: 0 - Discard
1 - Set CLP bit
2 - Set CLP of untagged cells, disc. tag'd cells
Units: enumeration
PCR
Description: Peak Cell Rate; used as default value if not supplied in VSI connection request.
Range/Values: 0 - 100
Units: cells/sec
MCR
Description: Minimum Cell Rate; used as default value if not supplied in VSI connection request.
Range/Values: 0 – 100
Units: cells/sec
SCR
Description: Sustained Cell Rate; used as default value if not supplied in VSI connection request.
Range/Values: 0 – 100
Units: cells/sec
ICR
Description: Initial Cell Rate. Used only for ABR VCs to set initial ACR value after idle traffic period.
Range/Values: 0 – 100
Units: cells/sec
MBS
Description: Maximum Burst Size - used to set bucket depth in policer function.
Range/Values: 1 – 5M
Units: cell count
CoS Min BW
Description: Bandwidth reserved for this Class of Service; used to initialize the CoS Buffer (Qbin) Minimum Service Rate (HW param. = ICG), and for CAC purposes (subject to CAC treatment type).
Range/Values: 0% – 100%
Units: % of Partition Min BW.
CoS Max BW
Description: Maximum value allowed for the sum of VC Min. BW's for this CoS; used by CAC (subject to CAC treatment type).
Range/Values: 0% – 100%
Units: % of Partition Max BW
Scaling Class
Description: Scaling table used for modifying per-VC thresholds under VI or Global cell-memory congestion.

```
Range/Values:  choices are 0 - 3,
                0: CBR
                1: VBR
                2: ABR
                3: UBR
Units:          enumeration
CAC Treatment
Description:    Connection Admission Control algorithm used by this CoS
Range/Values:   0 - 256
0: No CAC performed; all connections admitted.
1: LCN_CAC; check for LCN availability only; no BW consideration.
2: MINBW_CAC; LCN + simple min. BW test (sum_of_VC_min_BW <= CoS_max_BW)
3: CAC_2 w/ overbooking allowed
4: ECR_CAC; LCN + ECR calculation (from table) & BW test (sum_of VC_ECR <= Cos_max_BW).
5: CAC_4 w/ overbooking allowed
6: MEASURED_CAC; LCN + ECR calculation (from dynamic measurement) & BW test (sum_of VC_ECR <=
Cos_max_BW).
Units:          enumeration
VC Max
Description:    Maximum VC-cell-count threshold; all cells are discarded on a VC when this
threshold has been exceeded.
Range/Values:   0 - VI_max_cell_count
Units:          cell count
VC CLPhi
Description:    VC cell count above which CLP=1 cells are discarded
Range/Values:   0 - 100
Units:          % of VC Max threshold
VC CLPlo
Description:    VC cell count below which CLP=1 cells are no longer discarded (discards having
begun when CLPhi was exceeded).
Range/Values: 0 - 100
Units:          % of VC Max threshold

VC EPD
Description:    VC cell count above which AAL-5 frames are discarded
Range/Values:   0 - 100
Units:          % of VC Max threshold
VC EFCI
Description:    VC cell count above which congestion notification is activated
Range/Values:  0 - 100
Units:          % of VC Max threshold
VC Discard Selection
Description:    Choice of frame-based discard (EPD) or CLP-hysteresis
Range/Values:   0 - 1
0: CLP Hysteresis
1: EPD
Units:          enumeration
VSVD/FCES
Description:    For ABR VC's, enable/disable Virtual Source/Virtual Destination (VSVD) and/or Flow
Control on External Segments (FCES) functionality
Range/Values:   0 -2
0: None
1: VSVD
2: VSVD w/ FCES
Units:          enumeration
ADTF            ABR only parameter
Description:    ACR decrease time factor; idle time before ACR -> ICR
Range/Values:   10 - 1023
Units:          milliseconds
RDF             ABR only parameter
Description:    Rate Decrease Factor
ACR = ACR - (ACR * RDF)
Range/Values: 2 - 512,  in powers of 2
Units:          Inverse decrease factor
RIF             ABR only parameter
```

```
Description:     Rate Increase Factor
ACR = ACR + (PCR * RDF)
Range/Values:    2 - 512,  in powers of 2
Units:           Inverse decrease factor
NRM              ABR only parameter
Description:     Number of data cells between FRM cells
Range/Values:    2 - 512, in powers of 2
Units:           cells
TRM              ABR only parameter
Description:
Range/Values:
Units:
CDF              ABR only parameter
Description:
Range/Values:
Units:
TBE              ABR only parameter
Description:
Range/Values:
Units:

FRTT             ABR only parameter
Description:
Range/Values:
Units:
```

Full Name

Display service class template (SCT)

Syntax

dspsct [template #][service_type]

Related Commands

dspqbintmplt, cnfvsiif, dspvsiif

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	No	No	BPX	No

Example 1

dspsct

Description

Displays all the templates in the node.

System Response

```
sw53           TN    StrataCom       BPX 8620  9.2.a5    May 11 1999 14:24 PST

                         Service Class Templates

Template   Name

   1       MPLS1
   2       ATMF1
   3       ATMF2



Last Command: dspsct


Next Command:
```

Example 2

`dspsct 2`

Description

Display service class template 2, which displays service classes (also referred to as service categories or service sub-categories) for the ATMF1 template, along with designated qbins (class of service buffers).

System Response

```
sw237          TN    StrataCom       BPX 8620      9.2.1G    June 91999  17:48PST

           Service Class Map for ATMF1 Template

Service Class    Qbin    Service Class    Qbin         Service Class    Qbin

Default       13          Cbr2          10
VbrRt1        11          Cbr3          10
VbrRt2        11
VbrRt3        11
VbrNRt1       12
VbrNRt2       12
VbrNRt3       12
Ubr1          13
Ubr2          13
Abr           14
Cbr1          10

Last Command: dspsct 2


Next Command:
```

Example 3

`dspsct 3`

Description

Display service class template 3, which displays service classes (also referred to as service categories or service sub-categories) for the ATMF1 template, along with designated qbins (class of service buffers).

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:45 PST

         Service Class Map for ATMF2 Template

Service Class    Qbin    Service Class    Qbin    Service Class   Qbin

    Default       13          Cbr2          10
    VbrRt1        11          Cbr3          10
    VbrRt2        11
    VbrRt3        11
    VbrNRt1       12
    VbrNRt2       12
    VbrNRt3       12
    Ubr1          13
    Ubr2          13
    Abr           14
    Cbr1          10

Last Command: dspsct 3


Next Command:
```

Example 4

`dspsct 2 vbrrt1`

Description

Display service class template (SCT) for template number 2 called “vbrrt1”.

System Response

```
sw53           TN       BPX 8620  9.2.a3      Apr. 13 1999     17:30 PST

         Service Template:ATMF1 (2)     Service Type:  VbrRt1 (101)

Service Category                   VbrRt (101)
Qbin                               11
UPC Enable                         GCRA_1_2
UPC CLP Selection                  CLP01_CLP01
Policing Action 1                  DISCARD
Policing Action 2                  DISCARD
Sustained Cell Rate                100              (% of PCR)
Maximum Burst Size                 1024             (cells)
Scaling Class                      Scaled 3rd
CAC Treatment                      CAC4
VC Max Threshold                   1280             (cells)
VC Dscd Selection                  Hysteresis
VC CLP High                        80               (% of Vc MAX
Threshold)

Last Command:dspsct 2 vbrrt1



sw236          TRM   StrataCom       BPX 8620  9.2.a8    May  11 1999 14:35 PST

        Service Template:ATMF1 (2)     Service Type:  VbrRt1 (101)

VC CLP Low                         35               (% of Vc MAX Threshold)
Cell Delay Variation Tolerance     250000











Last Command:dspsct 2 vbrrt1
```

Example 5

`dspsct 2 Abr`

Description

Display all the parameters of the service class template ID 2, specified by “Abr”.

System Response

```
sw53           TN    StrataCom       BPX 8600   9.2.a5    Date/Time Not Set

         Service Template: ATMF1 (2)      Class: Abr (104)

Service Class Type                 109
Qbin                               14
UPC Enable                         2
UPC CLP Selection                  2
Policing Action 1                  2
Peak Cell Rate                     100              (%age of PCR)
Minimum Cell Rate                  50               (% of PCR)
Initial Cell Rate                  50               (% of PCR)
Scaling Class                      0
CAC Treatment                      2
VC Max Threshold                   0                (cells)
VC CLP High                        75               (% of Vc MAX Threshold)
VC CLP Low                         30               (% of Vc MAX Threshold)

This Command: dspsct 2 abr

Continue?
```

Example 6

`dspsct 1 Default`

Description

Displays the parameters for service class template 1 (the MPLS1 service class template) for the Default service type.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:53 PST

         Service Template: MPLS1 (1)     Service Type:   Default (1)

Service Category                   Default (1)
Qbin                               13
UPC Enable                         NONE
Scaling Class                      Scaled 1st
CAC Treatment                      LCN
VC Max Threshold                   61440            (cells)
VC Dscd Selection                  EPD
VC CLP High                        100              (% of Vc MAX Threshold)
VC EPD                             40               (% of Vc MAX Threshold)
Cell Delay Variation Tolerance     250000




Last Command: dspsct 1 Default


Next Command:
```

Example 7

dspsct 1 Signaling

Description

Displays the parameters for service class template 1 (the MPLS1 service class template), for the Signaling service type.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:57 PST

         Service Template: MPLS1 (1)     Service Type:   Signaling (2)

Service Category                   Signaling (2)
Qbin                               10
UPC Enable                         NONE
Scaling Class                      Scaled 1st
CAC Treatment                      LCN
VC Max Threshold                   0                 (cells)
VC Dscd Selection                  Hysteresis
VC CLP High                        75                (% of Vc MAX Threshold)
VC CLP Low                         30                (% of Vc MAX Threshold)




Last Command: dspsct 1 signaling


Next Command:

                      CD                                              MAJOR ALARM
```

Example 8

dspsct 1 Signaling

Description

Displays the parameters for service class template 1 (the MPLS1 service class template), for the Signaling service type.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:59 PST

         Service Template: MPLS1 (1)     Service Type:   Tag0 (200)

Service Category                  Tag0 (200)
Qbin                              10
UPC Enable                        NONE
Scaling Class                     Scaled 1st
CAC Treatment                     LCN
VC Max Threshold                  61440            (cells)
VC Dscd Selection                 EPD
VC CLP High                       100              (% of Vc MAX Threshold)
VC EPD                            40               (% of Vc MAX Threshold)




Last Command: dspsct 1 Tag0


Next Command:
```

Example 9

dspsct 1 Tag0

Description

Displays the service classes in the service template 3, which is a service class template for use with a PNNI controller.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:59 PST

         Service Template: MPLS1 (1)     Service Type:   Tag0 (200)

Service Category                  Tag0 (200)
Qbin                              10
UPC Enable                        NONE
Scaling Class                     Scaled 1st
CAC Treatment                     LCN
VC Max Threshold                  61440            (cells)
VC Dscd Selection                 EPD
VC CLP High                       100              (% of Vc MAX Threshold)
VC EPD                            40               (% of Vc MAX Threshold)




Last Command: dspsct 1 Tag0


Next Command:
```

Example 10

dspsct 1 Tag1

Description

Displays the service classes in the service template 3, which is a service class template for use with a PNNI controller.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  18:02 PST

         Service Template: MPLS1 (1)     Service Type:   Tag1 (201)

Service Category                  Tag1 (201)
Qbin                              11
UPC Enable                        NONE
Scaling Class                     Scaled 1st
CAC Treatment                     LCN
VC Max Threshold                  61440             (cells)
VC Dscd Selection                 EPD
VC CLP High                       100               (% of Vc MAX Threshold)
VC EPD                            40                (% of Vc MAX Threshold)




Last Command: dspsct 1 Tag1


Next Command:
```

Example 11

dspsct 1 Tag2

Description

Displays the service classes in the service template 3, which is a service class template for use with a PNNI controller.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  18:02 PST

         Service Template: MPLS1 (1)     Service Type:   Tag1 (201)

Service Category                  Tag1 (201)
Qbin                              11
UPC Enable                        NONE
Scaling Class                     Scaled 1st
CAC Treatment                     LCN
VC Max Threshold                  61440            (cells)
VC Dscd Selection                 EPD
VC CLP High                       100              (% of Vc MAX Threshold)
VC EPD                            40               (% of Vc MAX Threshold)




Last Command: dspsct 1 Tag2


Next Command:
```

Example 12

dspsct 1 VbrRt1

Description

Displays the service classes in the service template 3, which is a service class template for use with a PNNI controller.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  18:09 PST

         Service Template: ATMF1 (2)     Service Type:   VbrRt1 (101)

Service Category                   VbrRt (101)
Qbin                               11
UPC Enable                         GCRA_1_2
UPC CLP Selection                  CLP01_CLP01
Policing Action 1                  DISCARD
Policing Action 2                  DISCARD
Sustained Cell Rate                100              (% of PCR)
Maximum Burst Size                 1024             (cells)
Scaling Class                      Scaled 3rd
CAC Treatment                      CAC4
VC Max Threshold                   1280             (cells)
VC Dscd Selection                  Hysteresis
VC CLP High                        80               (% of Vc MAX Threshold)

This Command: dspsct 2 VbrRt1


Continue?
```

Example 13

dspsct 1 VbrRt1

Description

Displays the service classes in the service template 3, which is a service class template for use with a PNNI controller.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  18:11 PST

         Service Template: ATMF1 (2)     Service Type:   Cbr1 (100)

Service Category                   Cbr (100)
Qbin                               10
UPC Enable                         GCRA_1
UPC CLP Selection                  CLP01
Policing Action 1                  DISCARD
Scaling Class                      Scaled 4th
CAC Treatment                      CAC4
VC Max Threshold                   160               (cells)
VC Dscd Selection                  Hysteresis
VC CLP High                        80                (% of Vc MAX Threshold)
VC CLP Low                         35                (% of Vc MAX Threshold)
Cell Delay Variation Tolerance     250000


Last Command: dspsct 2 Cbr1


Next Command:
```

dspvsiif

You can use the **dspvsiif** command to display a service class template assigned to an interface (VI). You can also display a summary of the resources allocated to the VSI partition on a given interface. Multiple users are allowed to use the **dspvsiif** at one time.

Example

After using **cnfvsiif** command to assign a selected service class template to an interface, you can use the **dspvsiif** command to display the type of service template assigned to an interface (VI). It has the following syntax:

```
dspvsiif <slot.port.vtrk>
```

Full Name

Display a service class template assigned to an interface.

Syntax

dspvsiif <slot.port.vtrk> <tmplt_id>

Related Commands

cnfrsrc, dsprsrc, cnfqbin, dspqbin

Attributes

Privilege	Jobs	Log	Node	Lock
1–6	Yes	Yes	IGX, BPX	Yes

Example 1

dspvsiif 13.1.1

Description

Display the service class template ID assigned to an interface configured on slot 13, port 1, virtual trunk of 1. In this case, service class template 2 has been assigned to this interface.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:39 PST

Virtual Trunk :13.1.1

Service Class Template ID:2









Last Command:dspvsiif 13.1.1
```

Example 2

dspvsiif 11.1 2

Description

Display a service class template assigned to an interface.

System Response

```
sw53           TN    StrataCom       BPX 8600  9.2.30 Date/Time Not Set

Port: 11.1

Service Class Template ID: 2


VSI Partitions
                channels              bw             vpi
Part   E/D   min   max      min   max      start end   ilmi
 1      E     1000  4000     10000 40000    240   249   Off
 2      E     2000  4000     20000 40000    250   255   On





Last Command: dspvsiif 11.1 2


Next Command:
```

dspvsipartcnf

Use this command to display VSI partition characteristics. It displays information about only VSI ILMI functionality. This command displays:

- whether VSI ILMI is enabled for a given partition
- the LCN used for the sessions (only for trunk interfaces)
- the type of IP address downloaded to the BXM card for topology discovery purposes

If no partition is specified, this command displays the above information about all the VSI partitions and also the Sys_Id downloaded to the BXM card for ILMI functionality.

Full Name

Display VSI partition characteristics.

Syntax

dspvsipartcnf <slot.port.[vtrk]> [partition_id]

Table 17-29 dspvsipartcnf–Parameters

Parameter	Description
slot.port.[vtrk]	Slot, port (and virtual port if applicable) of the interface.
partition_id	Partition ID corresponding to the VSI partition. This parameter is optional and if not specified, this command will display information about all VSI partitions.

Related Commands

cnfrsrc, **cnfvsipart, cnfport, cnftrk**

Attributes

Privilege	Jobs	Log	Node	Lock
1–2	Yes	No	BPX	Yes

dspvsipartinfo

Use the **dspvsipartinfo** command to display VSI statistics for a particular active partition on an interface. You can use the **dspvsipartinfo** command on only one partition at a time, to get VSI statistics on an interface (can be a port or virtual trunk). You can optionally specify an interval in seconds, which will display VSI statistics for the specified active partition every *x* seconds. The command shows you some of the same parameters that display on the **cnfrsrc** screen, such as Min LCNs and Max LCNs, Used LCNs and Available LCNs, and Min BW, Max BW, and Used BW.

The command **dspvsipartinfo** also displays a line that provides slave redundancy status. It tells you whether the standby card is in synch with the active card. You must have cards in Y-redundancy configuration for this line to display.

Multiple users may use the **dspvsipartinfo** command at the same time.

Job mode is not allowed.

Full Name

Display VSI statistics per partition.

Syntax

dspvsipartinfo <interface>.<partition>[<interval>]

<interface>	the slot.port.[vtrk] of the interface being monitored.
<partition>	partition id for which information is to be displayed.
<interval>	the refresh interval for displaying data. Range:1–60 seconds. Default: 1 second.

Related Commands

cnfrsrc, dsprsrc, cnfvsiif, dspvsiif

Attributes

Privilege	Jobs	Log	Node	Lock	Multiple Users
1–6	No	No	BPX	Yes	Yes

Information Displayed

Parameter	Description
Min BW	Configured minimum bandwidth for this partition (for reference only).
Max BW	Configured maximum bandwidth for this partition (for reference only).
Used BW	Bandwidth currently used by connections on this partition.

Parameter	Description
Available BW	Bandwidth currently available to connections on this partition. This is determined based on the minimum and maximum bandwidth configured for the partition and the bandwidth currently available in the common pool.
Min Lcns	Configured minimum LCNs for this partition (for reference only).
Max Lcns	Configured maximum LCNs for this partition (for reference only).
Used Lcns	Number of LCNs currently used by connections in this partition.
Available Lcns	Number of LCNs available to this partition. This is determined based on the minimum and maximum LCNs configured for the partition and the LCNs currently available in the common pool.

Example 1

dspvsipartinfo 3.1 1 10

Description

Display VSI statistics for slot 3, port 1 for interface configured on partition ID 1, at an interval of every 10 seconds.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.1G    June 9 1999  17:32 PST

            VSI Resources Status for trunk  3.1 Partition 1

Min Lcns       : 0          Min BW (cps)     : 0
Max Lcns       : 20         Max BW (cps)     : 0
Used Lcns      :            Used BW (cps)    :
Available Lcns :            Available BW(cps):



Next Command: dspvsipartinfo 3.1 1
```

Example 2

dspvsipartinfo 11.1 2 10

Description

Display VSI statistics for port 1 for interface configured on partition ID 2, at an interval of every 10 seconds.

```
sw53 TN StrataCom BPX 8600  9.2.10  Jan. 10 1999 14:31 GMT


            VSI Resource Status for port 11.1 Partition 2

Min Lcns         1000        Min BW (cps)       20000
Max Lcns         4000        Max BW (cps)       40000
Used Lcns        500         Used BW (cps)      20000
Available Lcns:: 1000        Available BW(cps)   10000



This Command: dspvsipartinfo 11.1 2 10


Hit DEL key to quit:
```

Example 3

dspvsipartinfo 4.1 1

Description

Display VSI statistics for slot 4, port 1 for interface configured on partition ID 1.

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.L3    May  10 1999 14:58 PST

            VSI Resources Status for trunk  4.1 Partition 1          Snapshot

Min Lcns       :20         Min BW (cps)      :2000
Max Lcns       :30         Max BW (cps)      :3000
Used Lcns      :           Used BW (cps)     :
Available Lcns :            Available BW(cps):




Last Command:dspvsipartinfo 4.1 1
```

dspvsich

The **dspvsich** command is a debug command that displays VSI logical connections. These VSI logical connections are also sometimes referred to as management LCNs (1–6, 9–15). The **dspvsich** command displays the LCN number, type of channel (for example, interslave, master-slave, or intershelf); the destination slot, and destination LCN.

(Note that you must have debug level privileges to use this command, that is, either Service or StrataCom level privileges. Check with the TAC for assistance in accessing these commands.)

In this release, this command displays the control_VPI and control_VCI_start of the particular controller.

Full Name

Display VSI logical connections

Syntax

dspvsich <slot>

Description

Display the VSI channels (or LCNs) on the specified slot.

Related Commands

cnfqbin

Attributes

Privilege	Jobs	Log	Node	Lock
Service Level	No	No	BPX	No

Example

```
dspqbin 13.1
```

Description

Display the current qbin configuration on the OC-3 trunk on port 1 of slot 13 on the BPX to support MPLS (Multiprotocol Label Switching).

Example

dspvsich 4

Description

Display VSI management channels (or LCNs) on slot 4

System Response

```
sw237          TN    StrataCom       BPX 8620  9.2.a3    June 16 1999 05:10 PST

                             VSI lcns for Slot 4

     lcn             type         dest_slot   dest_lcn    vpi      vci
    272       slave-end msvc        13         546         -        -
    16365     control-port msvc     local      -           1        23
    16364     control-port msvc     3          16365       1        22
    16374     control-port msvc     13         8173        1        32
    16349     interslave            3          16350       -        -
    16359     interslave            13         8158        -        -



Last Command: dspvsich 4
```

Table 17-30 dspvsich—Parameters

Parameter	Description
slot.port	Specifies the BXM card slot and port number.
Qbin ID	Specifies the ID number of the Qbin available for use by the LSC (MPLS Controller) for VSI. The range is 0 to 255. 0 is the default. Always use 10 in 9.1.

.

dspyred

Displays information for Y-cable pairings. A single slot can be specified, or all pairings are displayed when no slot is specified. Slot numbers appearing in high intensity indicate active card status. Front card, back card, and channel configuration conflicts appear in reverse video. A conflict occurs when the port interfaces are different for corresponding ports in a redundant slot pair. The output display contains the following information:

- First column (Slot) designates the slot of the displayed card.
- Second column (Slot Type) designates its status, Pri (primary) or Sec (secondary).
- Third column (Other Slot) designates the slot number of the associated Y-redundant card.
- Fourth column (Front Card) designates the type of card in the front slot.
- Fifth column (Back Card) designates the type of card in the back slot.

Remaining columns (Channel Configuration) describe the channel configurations when appropriate.

Full Name

Display Y-cable redundancy

Syntax

dspyred [slot]

Related Commands

addyred, **delyred**, **prtyred**

Attributes

Privilege	Jobs	Log	Node	Lock
1–4	No	No	IGX, BPX	No

Example 1

```
dspyred
```

Description

Display Y-redundancy for all cards.

System Response

```
beta           TRM   YourID:1        IGX 8420    9.2    Aug. 15 1998 14:28 MST

     Slot Other Front  Back   Channel Configuration
Slot Type Slot  Card   Card     1    2    3    4    5    6    7    8
25   Pri  26    SDP    RS232   DCE  DCE  DCE  DCE
26   Sec  25    SDP    RS232   DCE  DCE  DCE  DCE









Last Command: dspyred


Next Command:
```

CHAPTER 18

Miscellaneous Features

This chapter provides information on the following features in this release:

- Feature Mismatching
- High Priority Login Feature (Hi-Pri)
- VP (Virtual Path) Tunnelling through a Public ATM Cloud (for IGX-UXM Cards)

Feature Mismatching

This section describes how each feature supports feature mismatch situations in Release 9.2 IGX/BPX switch software. Refer to the 9.2 release notes for up-to-date information on feature support, and software, hardware, and firmware requirements.

Introduction

This section provides some general guidelines for feature mismatching on the IGX and BPX in Release 9.2. These features perform feature mismatching functions:

- VSI 2.0
- Virtual trunking
- On Card LMI/ILMI
- APS (Automatic Protection Switching)
- FBTC with policing for BXM cards that support PPD on policing
- Multiple VSI Partitions

The following areas in switch software support feature mismatching:

- The command line interface will block you from enabling the feature if it is not supported by the logical card.
- Inserting cards/mismatch checking. The card will be mismatched only if the feature has been enabled and the inserted card does not support this feature.
- **addyred** command mismatch checking. If the primary card is active, the **addyred** command will not allow you to configure Y-redundancy if the secondary card does not support this feature. If the feature is not enabled, and the primary and secondary cards do not support the same feature sets, you will be warned that the capability will not function.

Configuration Commands that Perform Feature Mismatch Verification

All configuration commands that enable Release 9.2 features support mismatch verification. For example:

- **uptrk**: verifies virtual trunking support
- **cnfrsrc/addshelf**: verifies VSI 2.0 support
- **addapsln**: verifies APS support
- **cnfport**: verifies LMI/ILMI support
- **cnfoamlpbk**: verifies OAM Loopback support
- **dspcd:** verifies PPD on policing (PPDPolic) support

Feature mismatching provides customers a graceful migration path to Release 9.2 features. Switch software Release 9.1 and previous releases of switch software will mismatch cards if the capabilities in the logical card database do not match exactly the capabilities of the physical card. Such a restriction would not allow customers to gracefully migrate their BXM/UXM cards.

In this release, the feature mismatching capability will not mismatch cards unless the actual feature has been enabled on the card. This allows for a graceful card migration from an older release.

Switch software provides an upgrade path for each of the Release 9.2 features. Table 18-1 below describes the various scenarios while running Release 9.2 switch software and various versions of Release 9.1 and Release 9.2 firmware. Table 18-1 also describes the process of upgrading firmware in a scenario where a single active card and Y-cable is in use.

Table 18-1 Upgrading Firmware when Single Active Card and Y-Cable Are in Use

Configuration/Features	VSI	VT	LMI/ILMI	APS	OAM
Single Active Card Configuration: if the firmware is upgraded from 9.1 to 9.2, no mismatch will occur.	N.A. See Note 1 below table.)	OK	OK	OK	OK
Single Active Card Configuration: if the firmware is downgraded from 9.2 to 9.1, mismatch will occur if the 9.2 feature has been configured.	MM (if VSI is configured)	MM (if VT is configured)	MM (if Card based LMI is configured)	MM (if APS is configured)	MM (if OAM is configured)
Y-cable configuration with the Primary Card running 9.1 firmware and the Secondary Card running 9.2 firmware: the Primary Card will mismatch if the 9.2 feature has been configured.	Primary-MM (Primary Card mismatch if VSI Configured)	Primary-MM (Primary Card mismatch if VT feature is configured)	Primary MM (Primary Card mismatch if Card based ILMI is configured)	Primary MM (Primary Card mismatch if APS is configured)	Primary MM (Primary Card mismatch if AOM is configured)
Y-Cable configuration with the Primary Card and the Secondary Card running 9.2 firmware: no mismatch will occur and the 9.2 features are available to be configured.	OK	OK	OK	OK	OK

Configuration/Features	VSI	VT	LMI/ILMI	APS	OAM
Y-cable configuration with the Primary Card running 9.2 firmware and the Secondary Card running 9.1 firmware: the Secondary Card will mismatch if the 9.2 feature has been configured	Secondary-MM (Secondary Card mismatch if VSI Configured)	Secondary-MM (Secondary Card mismatch if VT feature is configured)	Secondary MM (Secondary Card mismatch if Card based ILMI is configured)	Secondary MM (Secondary Card mismatch if APS is configured)	Secondary MM (Secondary Card mismatch if OAM is configured)

Note VSI 1.0 is supported in Release 9.1 switch software and Release 9.1 BXM firmware. In Release 9.2, VSI 1.0 will not be supported in switch software. You must upgrade firmware before switch software can support VSI 2.0. (Refer to 9.2 Release Notes for firmware and hardware requirements to use VSI 2.0 and VSI 2.2.) Release 9.2 switch software will mismatch BXM cards that have VSI 1.0 supported when the VSI feature is configured.

Note If BXM cards are configured for Y-cable redundancy and the cards do not support the same feature sets, if the feature is not enabled, the cards will not mismatch. If you attempt to enable the Y-cable redundancy feature, it will be blocked at the command line interface.

Multiple VSI Partitions

Support for up to two partitions requires BPX switch software 9.2.3 and Firmware Ez. The card uses a flag in the capability message to report multiple partition capability. Firmware releases that do not support multiple partitions set this flag. The multiple partitions capability is treated as a card attribute and added to the attribute list.

Use of a partition with ID higher than 1 requires support for multiple VSI partitions in both switch software and BXM firmware, even if this is the only partition active on a the card.

In a y-red pair configuration, the multiple partition capability will be determined by the minimum of the two cards. A card with no multiple partition capabilities will mismatch if any of the interfaces has an active partition with an ID higher than 1. Attempts to enable a partition with an ID higher than 1 in a logical card that does not support multiple partitions will be blocked.

Table 18-2 shows mismatch conditions if the number of channels changes.

Table 18-2 Mismatch Conditions if Number of Channels Changes

Configurations	Mismatch
Replacing the current active card with a card with more channels: card will not mismatch, although the additional channels are NOT available to the user.	No
Replacing the current active card with a card with fewer channels: the inserted card will mismatch.	Yes
Active or standby Y-cable configuration with both the primary and secondary card supporting the same number of channels as defined in the logical database: no mismatch.	No

Table 18-2 Mismatch Conditions if Number of Channels Changes (Continued)

Configurations	Mismatch
Active Y-cable configuration with the Secondary Card supporting fewer channels than defined in the logical card (primary card) database: the secondary card will mismatch.	Secondary card mismatch
Active Y-cable configuration with the primary card supporting less channels than the logical card database: the primary card will mismatch.	Primary card mismatch
Active Y-cable configuration with the primary or secondary cards (or both) supporting more channels then the logical card DB: neither card will mismatch although the additional channels are NOT available to the user.	No mismatch
Standby Y-cable configuration with the primary or secondary cards supporting different number of channels: card will mismatch.	Mismatch

Functional Description of Feature Mismatch Checking

The following sections describe some of the behavior related to feature mismatching in this release.

Card Insertion/Mismatch Checking

The BXM and UXM card insertion/mismatch checking verifies that the inserted card supports all features currently available to the user. For Feature Mismatching, the following verification is performed:

- When a single card is inserted, if the physical card does not support the specific feature, and the feature has been enabled, the card will mismatch.
- When a single card is inserted, if the feature is not enabled, and the physical card supports the new feature, the logical card database should be updated to reflect this feature.
- During Y-cable mismatch, if the feature is enabled and if the inserted primary or secondary card does not support this feature, the card will mismatch.
- During Y-cable mismatch, if the feature is not enabled and if the inserted primary or secondary card does not support the feature, the logical card database will be updated to reflect this.
- During Y-cable mismatch, if the feature is disabled, and if both the inserted primary and secondary cards both support this feature, the logical database will be updated to reflect this.

UI Commands and Enabling Feature Mismatch

When a feature is enabled, a verification is made to assure that the hardware and firmware supports this feature. That is, during feature configuration, switch software performs a check to determine if the feature is supported by the BXM or UXM card. For example, if you are trying to add APS on a specific line (with **addapsln**) and the BXM card does not support this feature, a warning message is displayed and the addition is not completed.

The **dspcd** command gives you mismatch information for the specified card.

If the feature is not available, a warning message is displayed and the feature will not be enabled.

addyred/delyred Mismatch Checking

During addyred’s mismatch checking, the following verifications are done:

- A verification is done to ensure that both the primary and secondary cards support features that are activated. For example, if on the primary card, the APS feature has been configured, and on the secondary card this feature is not available, you will be blocked from using the **addyred** command.
- If the feature is not enabled, and the secondary card does not support similar feature sets, switch software updates its logical database to reflect this.
- Following a **delyred** command execution, the logical card’s database is updated to reflect the primary card’s capabilities.

The **addyred** commands (**addyred, delyred, dspyred, prtyred, switchyred**) will verify feature support on both the primary and secondary cards.

Things Related to Feature Mismatch Checking to Be Aware of

Following are some things to be aware of related to feature mismatch:

- Consider a situation where a user replace an active BXM card running Release 9.1 firmware with an Enhanced BXM card running Release 9.2 firmware (active card). The BXM-E (enhanced card) has more channels (channels scheduler). However, in this situation, the additional channels on the Enhanced BXM card cannot be used. To benefit from the additional channels provided on the Enhanced BXM card, you must put this card in a standby mode.
- Mismatches are reported when an old BXM card is replaced with a new BXM card that has different port group or channel levels (MLCS), even though the old BXM card and the new BXM card have identical channel numbers.

High Priority Login Feature

The High Priority (Hi-Pri) login feature provides a solution to ensure that network floods do not cause outages to occur.

Introduction

The network flooding control feature is an enhancement to switch software that prevents network traffic floods from aborting the processor card and thus keeps the user traffic flowing. Other improvements are included as part of this enhancement to provide additional resilience to the software to ensure that other overload conditions are also handled.

This network flooding control enhancement provides a quick response to outages to networks recently. This enhancement is meant to ensure that multiple node failures no longer occur due to overload conditions that were created in these networks.

Problem Description for which Network Flooding Control Enhancement Provides a Solution

A problem occurred that resulted in a flood of network messages being sent to most of the network. The problem was caused by a combination of things on the BPX. A firmware bug caused a standby BXM to loop real traffic back to the bus. An active BXM card in a Y-cable hot standby pair had its firmware upgraded. In doing so, a card switchover occurred which correctly put the card in a standby state but caused all traffic to loop back towards the bus without being blocked. Software had programmed the networking channels on the card so that traffic destined to leave the card would be sent back to the active card. The BPX crosspoint architecture allows standby cards to loop their traffic back to themselves as well as send it to the true destination. The BXM normally rejects cells not destined for the slot they are in except in the case of a hot standby. As a result of these steps, a loop was formed where traffic would loop continuously on the standby card but would also be sent to the active card for transmission out the trunks. This caused a very high rate of duplicate network messages to many nodes downstream from the trunks on this BXM card.

This network traffic flooding resulted in overloading the processor cards at multiple nodes. This overload exhausted critical resources within the processor cards which caused the nodes to abort. The resulting aborts caused CC switchovers but then these processor cards aborted as well. The second abort resulted in derouting all connections at each node.

One factor prolonging the outage was the difficulty in locating and disabling the source of the traffic flood. Aborts continued to occur as the flooding continued. The user interface at each node was unavailable as the nodes serviced the overload of traffic and aborted. This made isolation of the flood difficult. (Physically removing trunk cards at nodes ultimately isolated the source of the flood.)

An additional factor that prolonged the outage was the inability of the routing mechanism to quickly route so many connections at once. The ineffectiveness of the single threaded routing and its backoff collision mechanism led to an unacceptably slow rate of routing (and restoring the user traffic flow). (Manual intervention to shut off routing at key nodes reduced the collision rate and allowed the routing mechanism to efficiently restore all connections.)

This network flooding control enhancement is meant to solve the above problem with the following requirements:

- must be 8.4 compatible
- must keep user traffic flowing if possible
- network communication is secondary to user traffic
- prevent the problem from affecting multiple nodes if possible

Note that the BXM firmware is expected to be upgraded (carefully) to "W" or beyond to prevent the known flood from reoccurring.

Terminology

CC:Control Card is the processor card that controls the BPX or IGX nodes. This card runs the AutoRoute networking software.

Configuring the High Priority Login Mode Feature

You do not need to configure anything to get the functionality of the network flooding control feature enhancement or the high priority login feature.

Overview

A selected set of features are added to the 8.4 system software to improve the reliability of the software and ensure that network traffic floods do not cause user traffic interruption. The changes are limited in scope to provide a quick fix, minimize the risk of this fix, and to provide compatibility with other 8.4 releases.

Function of High Priority Login Feature

The major changes are to prevent similar flooding loopbacks and to prevent the processor card CPU from aborting in the presence of network floods. The secondary changes are to provide a high priority console login to allow you to view and correct flooding problems, and build tolerance into the communication between nodes and between hubs and feeders to allow user traffic to continue flowing when this communication breaks down.

Using the High Priority Login Feature

A flood of network traffic can lead to a node becoming unreachable from other nodes in the network. The high priority login feature allows you to log in at the console port and execute a small set of commands. You log in as follows:

Enter User ID: **StrataCom**

Password:********

Next Command: **hipri**

At this point you may detect excessive network messages using the **nwstats** command or see excessive network handler processing using the **dspprf** command.

To lessen the CPU use of the network handler task and allow lower priority tasks to execute, you can use the **cnfnhparm** command to decrease the loop count before the network handler task suspends processing.

If the source of the traffic flood cannot be quickly located and shut off, you can disable LMI error detection using the **addfdrlp** command on the hub and at all connected feeders. After the network returns to its normal state, you can re-enable LMI at the hub and feeder nodes using the **delfdrlp** command. You can see the loopback state of the feeder trunk LMI using the **dspnode** command.

Functional Description

The following subsections describe the individual features in detail.

Software Loop Prevention

The network channel programming on the BPX now blocks trunk channels that loop incoming traffic back to the same trunk. This eliminates the possibility that undetected hardware loopbacks create a flood of traffic on the trunk.

For each node in the network there exists one channel on each BPX trunk to receive control traffic for that node and forward it to the one trunk that transmits the traffic for that node. To avoid looping back traffic that unexpectedly arrives on the transmit trunk, a CLP object was set for that channel. On BNI cards the firmware interpreted this to turn off the receive part of the channel. The BXM firmware does not have this functionality. The software now sets the receive VPI/VCI to 0/0. This has the same effect on BXM firmware as the CLP object had on BNI firmware (the receive part of the channel is turned off). The BXM firmware does not sink cells with VPI/VCI equal to 0/0.

Note This change first went into effect in Release 8.4.20.

Duplicate Coerced Message Dumping

The network message handler checks for receiving duplicate network messages without sequence numbers (coerced messages) within a small amount of time. If duplicates are detected, they are quickly discarded without acknowledgment. Duplicates are considered coerced messages received within 1 second of each other. This has the effect of limiting the remaining flow to other parts of the software to 1 coerced message per second. Floods of network messages that use sequence numbers appear as messages with duplicate sequence numbers. Duplicate messages are already handled efficiently. The **nwstats** screen shows “Dropped flooding msgs”.

Network Message Read Limit

A configurable limit is added to the network handler to control the number of cells that may be read from the SAR receive queue before giving up the CPU to lower priority tasks. This has the effect of limiting the amount of CPU usage by this high priority task even when floods of network traffic are present. The command and its syntax for controlling this feature are defined below.

cnfnhparm <parm> <value>

whereparm is 1

value is from 0 to 1200 cells per loop [default = 1200]

The setting of this parameter to a low number may lead to the dropping of network traffic, possibly resulting in comm breaks, comm fails, or background test failures.

High Priority Console Login

A special high priority console user login is created to allow you to log in and execute some commands on the node even during periods of node congestion. The console login executes as high priority before the user logs in. When you log in as “StrataCom” and the first command typed is the new command is **hipri**, then the user task stays in high priority mode. If the user logs in using another account or uses “StrataCom” but does not use the **hipri** command first, then the user task reverts to the normal (lower) priority. The following error message is displayed when the **hipri** command is used by a non-Cisco login.

— “Incorrect privilege group”

The following error message is displayed when **hipri** is not the first command immediately after login.

— “Allowed only immediately after login”

The following error message is displayed when you try to use command but not from the control port.

— “Allowed only through Control Port”

The high priority user task executes above all tasks but the resource handler. This allows this feature to execute even in cases of network message flooding, connection routing, extreme CommBus usage, etc.

Notification is given when high priority mode is in use by the “High Priority!” string on the **dsplog** screen. A sample screen is shown in Example 4 under the “dsplog” section on page 14-92.

Only a subset of the user commands is allowed to run during a high priority login. Due to the high priority of this task, some commands may not work correctly or may affect other features in the system. For that reason, the list of commands is limited and are blocked at the command line. The user receives the following message when an invalid command is attempted from high priority:

— “Not allowed with High Priority Login”

Table 18-3 lists the commands allowed in high priority mode for the StrataCom user level:

Table 18-3 High Priority Mode StrataCom User Level Commands

addfdrlp	**bye**	**cbstats**	**cbtrace**	**ccb**	**cnw**
cnfnhparm	**dcb**	**dcct**	**delfdrlp**	**dlcon**	**dm**
dncd	**dspalms**	**dnib**	**dnw**	**dspalms**	**dspcd**
dspcderrs	**dspcds**	**dsplog**	**dspnds**	**dspnode**	
dspnw	**dspprf**	**dspprfhist**	**dspqs**	**dspsust**	**dspswlog**
dsptrkerrs	**dsptrks**	**dsptrkstats**	**dsptrkutl**	**dspusertask**	**dspusertasks**
dvc	**help or “?”**	**killuser**	**logoutuser**	**nwstats**	**nwtrace**
off1	**off2**	**off3**	**on1**	**on2**	**on3**
pm	**resetcd**	**resetsys**	**runrev**	**stopjob**	**switchcc**
vt	**“.” (history)**				

ARP Table Expansion

The ARP cache table size has been increased to provide more efficient management of IP to Ethernet (MAC) addresses and prevent processor overloads from excessive ARP messages.

Address Resolution Protocol (ARP) is used by IP hosts on an Ethernet LAN to determine the Ethernet (MAC) addresses of fellow hosts. This protocol will, using Ethernet broadcast packets, allow for mapping an IP address to an Ethernet address. To assist in maintaining the mappings, an ARP cache is usually resident on each IP host. By eavesdropping on ARP messages, each IP host can build its ARP cache quickly and efficiently.

When large numbers of IP hosts are resident on the same physical Ethernet, lots of ARP broadcast messages can be normal. Each new translation of IP address to Ethernet address is placed in a local ARP cache entry on the BPX node. Previously, this ARP cache had a size limit of four entries. In situations where a large number of ARP translations exist on the Ethernet, bumping of ARP cache entries to make room for new entries is necessary. In fact, a sort of thrashing in the ARP cache can occur.

Increasing the table size to 16 entries improves the performance of the processor when more than 4 physical devices are on the same LAN segment. ARP broadcasts are minimized as are updates to the ARP cache. This is expected to address the large number of Cisco WAN Manager workstations that a node can support.

Comm Fail Tolerance

The trunk keep-alive mechanism, also known as the Comm Fail test, allows you to select whether or not connections are derouted on keep-alive time-outs. Previously when the Comm Fail test failed, all connections on the trunk were derouted affecting user traffic. This test runs in addition to the physical line alarm mechanism.

In the event of a network flood, the network handler will inevitably end up dropping numerous network messages. Among these will be messages for the Comm Break and Comm Fail tests, leading to a failure of the tests and the declaration of comm breaks with other nodes and comm fails on its trunks.

To provide more tolerance to a flood of network messages, the Comm Fail test functions so that the default for physical trunks is to leave connections routed in spite of a failure detected by the Comm Fail test. Network alarms and log events are still generated for Comm Fail failures, but connections are not derouted.

In the case of virtual trunks, the Comm Fail test may be the only indication that a virtual trunk crossing an ATM cloud is not passing traffic. For this reason, virtual trunks must continue to de-route connections on Comm Fail failures.

Control of whether Comm Fail test failures cause deroutes on physical trunks is provided by the **confounders** command. A new parameter *Reroute on Comm Fail* indicates whether connections should be derouted on failures. If enabled, a Comm Fail test failure on any local trunk results in all nodes rerouting the connections they own that are currently on that trunk. If this is not enabled, a Comm Fail test failure will not result in the rerouting of the connections. A comm fail on a virtual trunk will always result in the rerouting of all the connections on the trunk, regardless of the setting of the enable flag.

Regardless of the Reroute on Comm Fail parameter setting, a trunk that fails the Comm Fail test is still declared as failed. Route-op still runs and will consider this trunk unusable for network traffic. Network clock routing also considers the trunk unusable for clocking and builds a route around this trunk. These operations continue to work as in releases previous to Release 9.2.

The syntax of this command is shown below.

cnfnodeparm 38 [Y | N]

where:Y = deroute conns when any local physical trunk fails the Comm Fail test

N = don’t deroute connections on a local physical trunk Comm Fail test failure

N = default)

LMI Failure Prevention–Manual

A manual command is added to IGX and AXIS feeder software to allow control over the endpoint connection status. If the BPX cannot communicate LMI messages with its feeders, then the LMI status at the feeders must be maintained to keep the connections “active” to their external devices.

If the BPX hub is flooded with network messages, then LMI/ILMI communication with its feeders may be interrupted. LMI normally runs a keep-alive between the hub node and feeder node. If the keep-alive fails, then the other end changes the status of all connections to "failed". If the outage is only due to a network message flood, then it is desirable to override this mechanism to keep the connection status as "active".

The BPX and IGX software now has the **addfdrlp** and **delfdrlp** commands. On the BPX hub with attached feeders, the **delfdrlp** command clears any communication failures on the specified feeder and sends messages to the remote nodes (the routing nodes for the other end of the feeder connections) informing them of this clearing. In addition, the BPX no longer sends any status updates to the feeder yet it continues to acknowledge any feeder LMI messages received. The **dspnode** command indicates loopbacks on feeders.

The syntax for **addfdrlp** is shown below.

addfdrlp <slot>.<port>

where: slot is the slot number for the feeder trunk

port is the port number for the feeder trunk

The following error messages may be displayed.

"Shelf has not been added on this trunk."

"Feeder loop is already added"

The BPX command **delfdrlp** restores the BPX's feeder LMI protocol to the normal state and triggers an update of connection status towards the feeder.

The syntax for **delfdrlp** is shown below.

delfdrlp <slot>.<port>

where: slot is the slot number for the feeder trunk

port is the port number for the feeder trunk

The following error messages may be displayed.

"Shelf has not been added on this trunk."

"Feeder loop is not added"

The following log messages occurs as a result of using the feeder loopback commands.

Major	IPX/AF shelf on TRK 10.2: Major Alarm
Info	IPX/AF shelf on TRK 10.2: Cleared

On the IPX/IGX feeder, the ***"addfdrlp"*** command clears any communication failure on the feeder to the routing node (hub). It also, clears any ingress (coming from the routing node) A-bit failures. In addition, the feeder does not send the routing nodes any status updates but continues to acknowledge any routing node LMI messages received.

The syntax for ***"addfdrlp"*** is shown below:

addfdrlp <slot>.<port>

where: slot is the slot number for the feeder trunk

port is the port number for the feeder trunk

The following error messages may be displayed.

— Shelf has not been added on this trunk

— Feeder loop is already added

The IGX command **delfdrlp** restores the routing node's LMI protocol to the normal state and triggers an update of connection status toward the routing node.

The syntax for **delfdrlp** is shown below:

delfdrlp <slot>.<port>

where: slot is the slot number for the feeder trunk

port is the port number for the feeder trunk

The following error messages can be displayed:

— Shelf has not been added on this trunk

— Feeder loop is not added

The implementation of the LMI disabling feature is manual in this release.

cnfnodeparm Screen

Figure 18-1 shows a sample **cnfnodeparm** screen. More than one screen is needed to show all the parameters for this command.

Figure 18-1 cnfnodeparm Screen

```
sw45           TN    SuperUser       BPX 8620    9.2 Aug. 27 1998 18:26 PDT

31 TFTP Write Retries      [    3] (D)
32 SNMP Event logging      [    Y] (Y/N)
33 Job Lock Timeout        [   60] (D)
34 Max Via LCONs           [50000] (D)
35 Max Blind Segment Size  [ 3570] (D)
36 Max XmtMemBlks per NIB  [ 3000] (D)
37 Max Stby Update Q Sz (%)[   33] (D)
38 Stat Config Proc Cnt    [ 1000] (D)
39 Stat Config Proc Delay  [ 2000] (D)
40 Enable Degraded Mode    [N]     (Y/N)
41 Trk Cell Rtng Restrict  [N]     (Y/N)
42 Enable Feeder Alert     [N]     (Y/N)
43 Reroute on Comm Fail    [N]     (Y/N)
44 Auto Switch on Degrade  [Y]     (Y/N)
45 Max Degraded Aborts     [100]   (D)
46 Max Htls Rebuilt Count  [100]   (D)
47 Htls Counter Reset Time [1000]  (D)
48 Send Abit Early         [Y]     (Y/N)
49 Abit Timer Multiplier M [2]     (D)
50 Abit Timer Granularity M [3]    (0)
51 FBTC with PPD Policing  [   N]  (Y/N)


This Command: cnfnodeparm


Enter parameter index:
```

dspnode Screen

Figure 18-2 shows a sample dspnode screen.

Figure 18-2 dspnode Screen

```
-----------------------------------------------------------------------
sw237          TN    StrataCom       BPX 8620  9.2.3    June 16 1999 05:06 PST

                   BPX 8620 Interface Shelf Information

Trunk    Name      Type          Part Id   Ctrl Id       CntrlVC        Alarm
                                                     VPI   VCIRange
 4.1     VSI       VSI              1         1        1    20 - 34      OK
13.2     SIMFDR0   AXIS             1         2        0    40 - 54      OK




Last Command: dspnode
```

Virtual Trunking through a Public ATM Cloud using VP (Virtual Path) Tunnelling on IGX-UXM Cards

VP Tunnelling provides the ability to encapsulate a VP connection into a VC connection (VCC) using gateway functions on the UXM module on the IGX nodes, making it possible to use a public ATM PVC service (VCC service).

The Cisco IGX is Cisco's multiservice enterprise WAN switch using ATM technology that consolidates different traffic types. Virtual Trunking enables IGXs to be connected to a VP service offered by a public ATM network, where each virtual trunk uses a corresponding VP. In certain situations, carriers may offer only a VC service to subscribers, which may be more economical than a VP service to carry virtual trunks. The flexible architecture of the IGX facilitates use of virtual trunking over a permanent virtual circuit (PVC) service, thus providing customers with an option to use the public ATM VP or VC service. A virtual trunk using a VP can be encapsulated into a VC connection (VCC) offered by the public network using advanced gateway functions on the IGX, such as simple gateway and cell forwarding gateway.

This section describes virtual trunking over a PVC service (VCC) solution on the IGX using UXM cards, and how to implement VP tunnelling connections on the IGX.

Introduction

Multiservice wide-area networks are deployed by enterprise customers to consolidate voice, video and data traffic. Traditionally, leased lines are used to connect the multiservice switches in an enterprise backbone. With the widespread availability of public ATM services, customers now have a cost-effective option of interconnecting multiple sites.

Asynchronous Transfer Mode (ATM) is the preferred technology in the WAN for implementing a multiservice backbone due to its bandwidth efficiency, superior performance and guaranteed quality of service (QOS) offering. Compared with time-division multiplexing (TDM), using ATM in the WAN companies can realize 30 to 50 percent total network savings. Cisco's IGX multiservice WAN switches use ATM's superior capabilities to combine bursty or constant-rate data, voice and video onto one enterprise backbone.

The IGX multiservice ATM backbone can be connected using leased lines or the increasing world-wide availability of public ATM services. Using public networks to interconnect IGXs can be more economically attractive than leased lines to achieve scaling of the network and guaranteed QOS delivery.

Virtual trunking (VT) and traffic shaping functionality is an important product differentiator on the IGX in enabling key customer applications over public ATM networks. The Virtual Trunking feature maximizes the use of a single physical ATM interface to connect to several destinations using a public ATM service. For specific information on virtual trunking, and how to set it up in your network, see the “Overview of Virtual Trunking” section on page 4-4.

The prevalent type of service offered to subscribers by public ATM Service Providers for trunking different locations is a Virtual Path connection (VPC), independent of the Virtual Circuits (VC) carried by the VP. In certain situations, the service provider may be unable to offer VP service to its customers, but instead provides a VC service. In such cases, the IGX provides a solution to its customers by enabling virtual trunking over a public ATM PVC service.

This section addresses the scenario when a public ATM carrier provides a PVC service, and describes the virtual trunking implementation on the IGX using this PVC service. A virtual trunk uses a VP connection that is encapsulated into a VC connection using gateway functions on the UXM module, making it possible to use the public ATM PVC service (VCC).

Virtual Trunking through Public ATM Service using UXM Cards

After the explosive successful growth of Frame Relay services in the WAN, customers requiring higher bandwidth and guaranteed QOS agreements for multiservice integration are universally adopting ATM services. To meet the increasing demand for ATM services, carriers and service providers are exploiting the inherent powerful nature of ATM technology and its advanced traffic engineering capabilities to offer cost-effective public ATM services.

Customers deploying IGXs to form a multi-service WAN backbone have an alternate economical means of connection using public ATM service compared with leased lines. The use of public ATM service facilitates speedy provisioning of service level agreements (SLA) and scalable bandwidth levels.

On the other hand, sharing the same public ATM network between different subscribers may raise some security concerns in the minds of customers who wish to control privacy of their networks. It is also mandatory for the customer premise equipment to perform shaping on the traffic entering the public ATM network to conform to the SLA specified parameters. The ingress side of the public ATM network performs traffic policing to ensure that the customer maintains the service level agreements and discards any non-conformant traffic. Public ATM switches reserve adequate bandwidth needed to fulfill the service level agreements, and traffic policing ensures that network-wide congestion is not caused by misbehaving user traffic.

The predominant type of service offered by carriers is the VP service, which is used to trunk different locations. Although in certain cases when the carrier ATM edge switch may be unable to offer a VP service, a less expensive VC service option is provided to customers.

Performing Virtual Trunking through a Public ATM Cloud by Tunnelling a VP through a VC Service

The virtual trunking feature in this release enables IGXs to be connected through a VP service offered by the public ATM network, where each virtual trunk uses a corresponding VP. In some situations, carriers may offer only a VC service to subscribers, which may be more economical than a VP service, to carry virtual trunks. The IGX's flexible architecture facilitates use of virtual trunking over a permanent virtual (PVC) service, thus providing customers with an option to use a public ATM VP or VC service. A virtual trunk using a VP can be encapsulated into a VC connection (a VCC) offered by the public network using advanced gateway functions on the IGX such as simple gateway and cell forwarding gateway.

The Virtual Path tunneling connections for the UXM card give you the ability to encapsulate a virtual path connection (VPC) inside a virtual circuit connection (VCC). This feature provides a solution an application that uses the public ATM network but does not support Virtual Path connections. To create an IGX network using a public ATM network, the UXM virtual trunk feature is required along with the ability to tunnel the virtual trunk traffic across the cloud using Virtual Circuit Connections (VCCs) provided by the ATM cloud.

The virtual trunking feature introduces the capability to provide connectivity for a hybrid network consisting of Cisco nodes through a public ATM cloud. This feature is intended for providing connectivity to an ATM cloud through IGX nodes. The connections at the cloud's access points can be an ATM UNI or ATM NNI interface.

Purpose of VP Tunnelling

The purpose for virtual path tunneling on UXM cards is to provide the capability to provide the virtual trunking feature set, even when the network cloud doesn't support virtual path connectivity. This way Cisco IGXs can be introduced into a public ATM network supporting ATM-UNI or ATM-NNI interfaces, by using Virtual Circuit Connections (VCCs) provided by the ATM cloud.

This chapter describes how virtual path tunneling connections over UXM virtual trunks on IGX nodes work. You can configure multiple interfaces on a UXM card as either port(s) or trunk(s), so that a single UXM card can have both tunneling connections (on ports) and virtual trunks (on trunks). Part of the VP tunnelling setup involves configuring DAX connections (connections local to the node) on the IGX UXM card.

Environment Requirements

The virtual path tunneling feature requires the following components, along with the UXM virtual trunking feature. (The Ports and Trunks feature allows you to use this feature with a single UXM interface card along with 9.2.10 switch software.)

- UXM—T3/E3/T1/E1/OC-3/IMA
- Release 9.2.10 IGX switch software—a subrelease of 9.2.00
- ATM cloud: any public or private ATM network supporting Virtual Circuit Connections across ATM UNI/NNI interfaces
- UXM Firmware revision that supports virtual trunking.

If upgrading from Release 9.1, you must upgrade the firmware first, the upgrade the switch software. See the 9.2 release notes for current system and environment requirements for VP Tunnelling feature.

Compatibility

The UXM virtual trunking and VP tunneling features require 9.2.10 switch software. Virtual trunks support requires new UXM firmware. (Refer to the 9.2 Release Notes for information.) The new firmware revisions are backward-compatible with earlier versions of the software, but the Release 9.2 software is not compatible with 9.1 UXM firmware, therefore a UXM firmware upgrade is required for networks running Release 9.2, so that you can use the virtual trunking feature.

Even though network interoperability is supported between Release 9.2 software and 9.1 or 8.5 or 8.4 software, in a network of hybrid releases, you cannot add UXM virtual trunks.

Overview of Configuration of VP Tunnelling

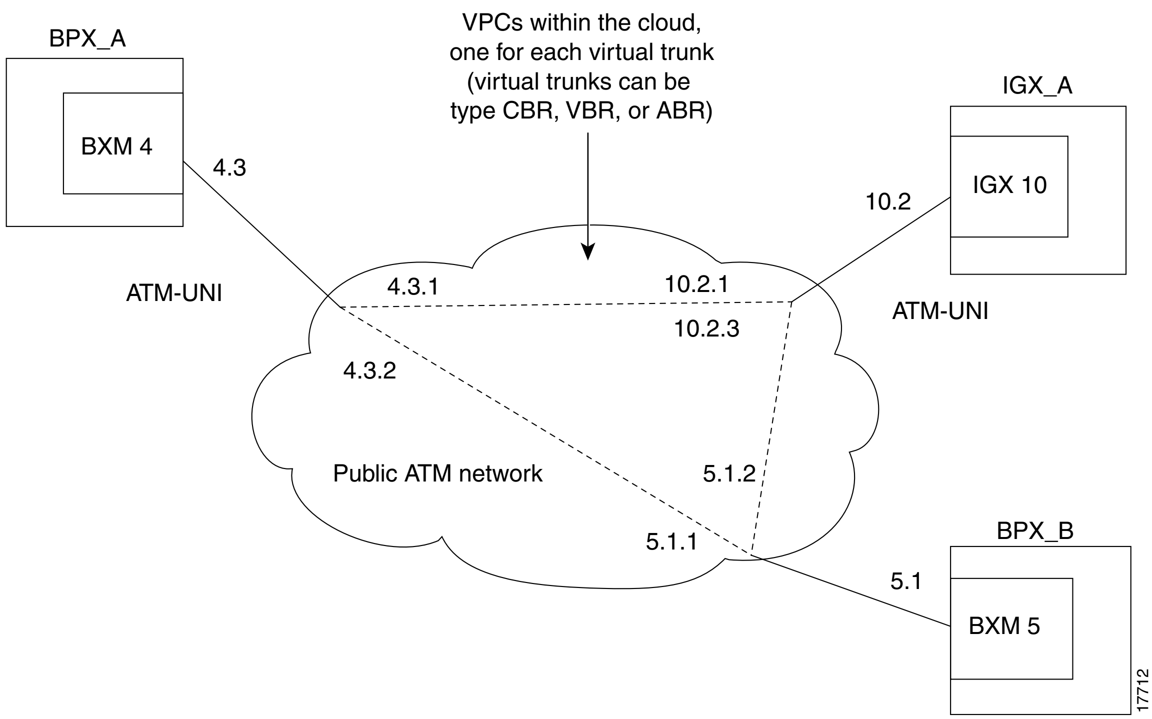
This section provides a brief description of how to set up VP tunnelling. Refer to later sections for step by step procedures.

You set up the Virtual Path Tunneling connection by configuring three UXM ports, one of which you configure as a virtual trunk port, and the other two as line ports. (For information on how to configure a virtual trunk port, refer to the "Setting up a BXM or UXM Virtual Trunk through an ATM Cloud" section on page 4-12.) A physical back-to-back cabling is provided between the virtual trunk port and one of the other line ports. The third port functions as the entry point to the ATM cloud, feeding the VCC provided by the cloud. The ATM cloud provider will provision this VC connection. You add the tunneling DAX connection between the line ports by using the virtual trunk port side as the

VP side and the line port (the port at the cloud entry point) as the VC side. After provisioning a similar tunneling connection at the other end of the cloud (VCC), the virtual trunk is added between the virtual trunk ports at both ends of the connections.

If the ATM cloud is comprised of Cisco nodes (BPX or IGX): for a BPX, the access points are ASI or BXM ports; for an IGX, the access points are UXM ports. If the private ATM cloud consists entirely of Cisco nodes, the Virtual Trunking feature can be used without the tunneling connections, because a cloud consisting of Cisco nodes already supports Virtual Path Connections (VPCs). See Figure 18-3 for an illustration of virtual trunks across a public ATM network. For more information on virtual trunking, and how to set it up in your network, refer to "Overview of Virtual Trunking" section on page 4-4.

Figure 18-3 Virtual Trunks across a Public ATM Network



Overview of VP Tunnelling

This section provides an overview of VP tunnelling and virtual trunking and a description of the setup requirements.

The virtual trunking feature introduces the concept of defining multiple trunks within a single trunk port interface. In the past, trunking has been associated with the physical existence of a trunk card and port. The virtual trunking capability is now extended to UXM trunk cards in Release 9.2 along with the ability to configure ports and trunks on the same interface card. Virtual trunking allows you to define an additional level of trunking within the port resources. This "many-to-one" virtual trunk to port relationship produces a "fanout" trunk capability.

The Virtual Path tunneling solution requires two additional UXM ports (which may not reside on the same card), one of which is connected to the public ATM network, while the other is connected to the virtual trunk port. In addition, a new connection type is supported to allow the virtual path connection (VPC) to tunnel over the public ATM network. This new connection must be used in pair, that is, at both ends of the virtual trunk that attaches to the ATM public cloud.

Figure 18-4 shows how an IGX network is connected over a public ATM cloud. Each virtual trunk is connected using a virtual path connection (VPC) across the public ATM cloud. This is how virtual trunks are connected to an ATM cloud that provides a virtual path connection (VPC).

Figure 18-4 Virtual Trunk with Public ATM Cloud (with Virtual Path provided by the Cloud)

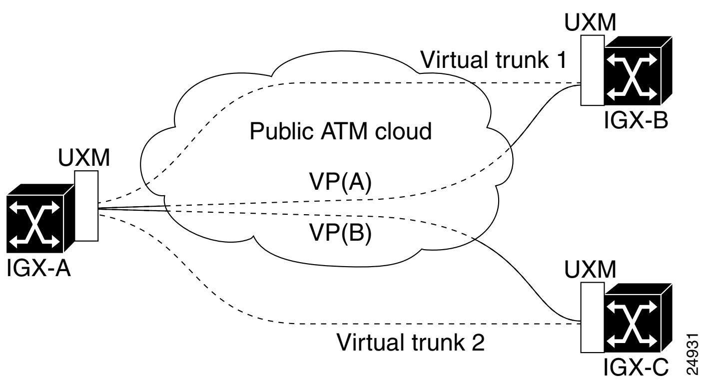


Figure 18-5 illustrates the solution that lets you configure a virtual trunk over a public ATM VC connection (VCC) service.

The **addcon** command lets you add the virtual path tunneling connection between UXM ports. Similar to the case of virtual trunking, where the virtual path connection should be added before adding the virtual trunks, the Virtual Circuit Connection within the cloud and the tunneling DAX-connection between the two UXM ports have to be provisioned before adding the virtual trunking path between the UXM trunk ports. The connectivity between the UXM virtual trunk side (virtual trunk port) and the Virtual Path side of the port has to be of the same interface type, since they are connected back to back to each other.

An IGX network is connected using a virtual path connection, as shown in Figure 18-4, where virtual trunks are added between IGX-A and IGX-B/IGX-C. However, a special configuration is implemented at each node to provide tunneling of a virtual path connection over the public ATM cloud, as shown in Figure 18-5. The configuration details at each node is given in Figure 18-6. See Figure 18-7 for an illustration of two additional possible configuration combinations within the same IGX node.

Note The three ports shown in Figure 18-6 do not necessarily need to be in the same order, nor on the same card.

Figure 18-5 Virtual Trunk with VP Tunnelling (with VCC Provided by the Cloud)

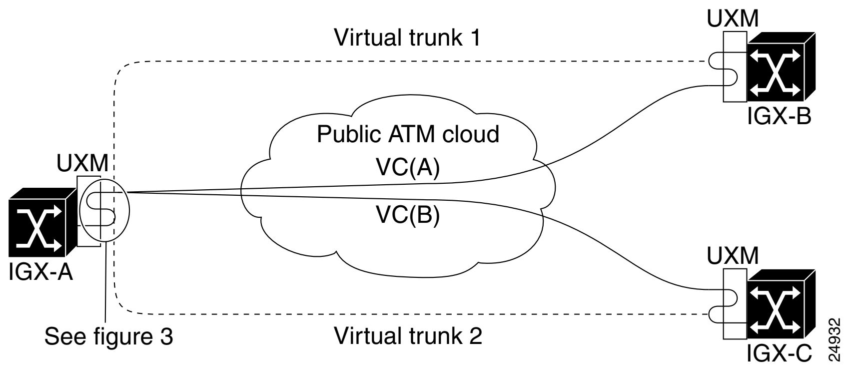


Figure 18-6 Description of Cabling at each IGX Node

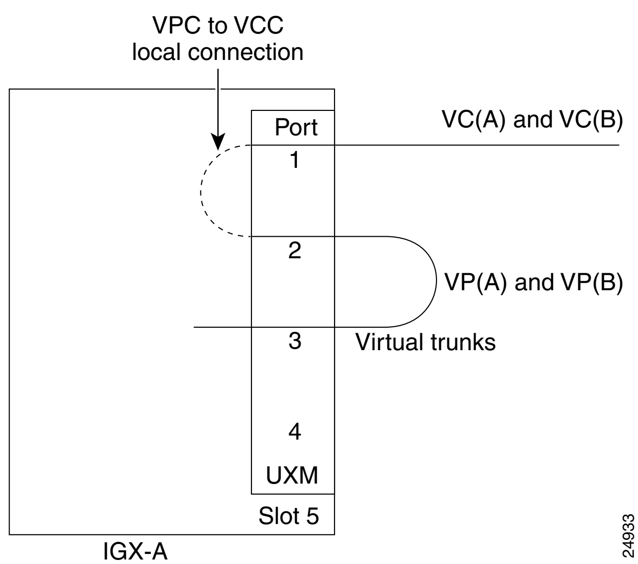
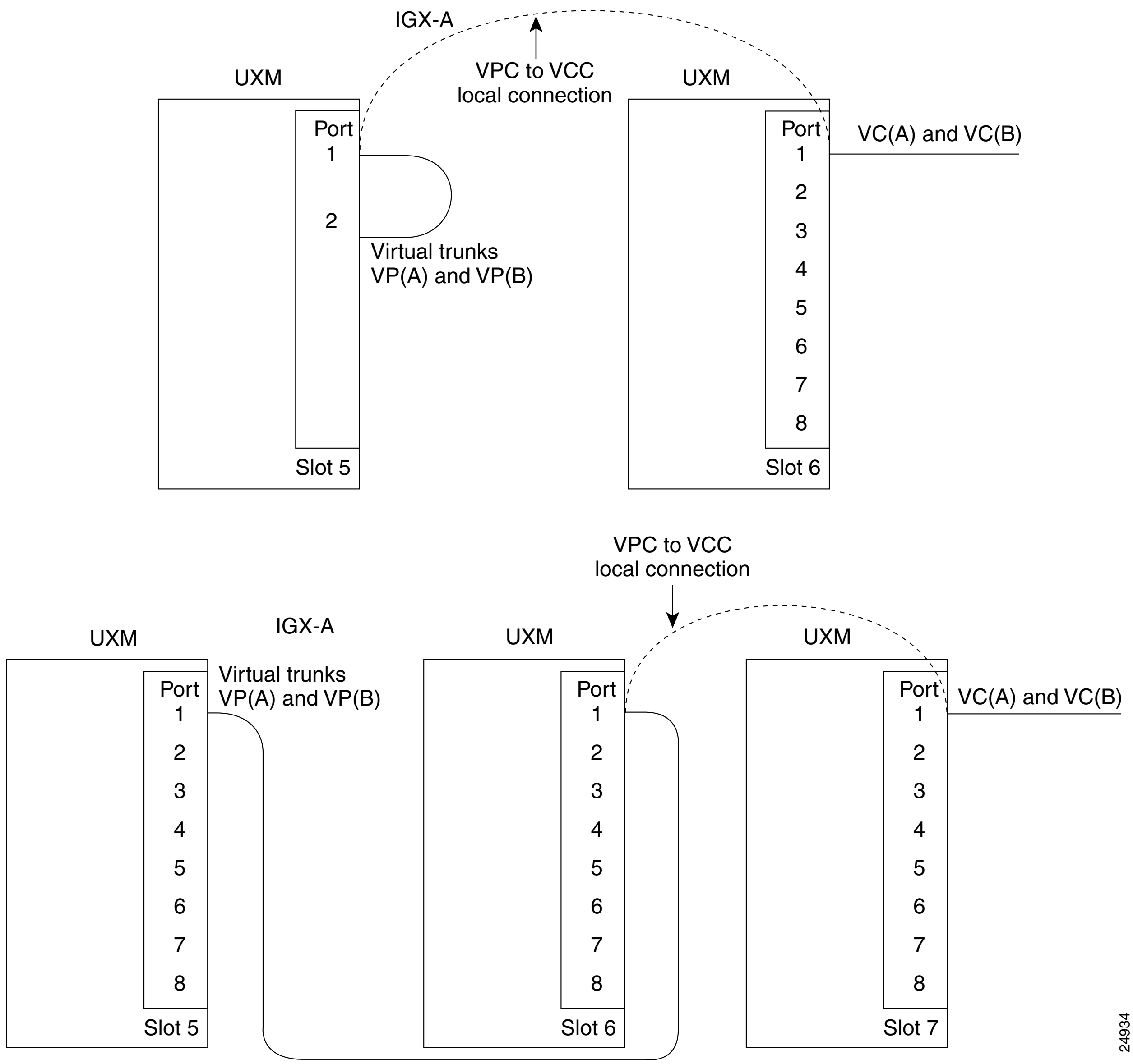


Figure 18-7 Two Additional Possible Combinations within the Same Node



How to Use the VP Tunnelling Feature and Redundancy Support

Note Support of the VP tunnelling connection to use IGX virtual trunking across VCCs (virtual circuit connections) is limited in its use to within a single IGX node. Therefore, you cannot add tunnelling connections between nodes.

You will be prompted with appropriate error messages if you attempt to add non-DAX (non-local) tunneling connections. Only DAX connections are allowed for VP Tunnelling.

You can add VP tunneling connections between cards residing in the same node, not necessarily on the same slot. Therefore, you can configure this tunneling connection to span across a maximum of three slots, with one trunk port on one slot (as the virtual trunk port), and the other two ports on two different slots as line ports. (See Figure 18-7, the second part of the figure.) You must configure it this way for the interface requirements to be met for connecting a trunk port to a line port back to back. Figure 18-6 shows a VP tunnelling configuration setup with all three ports on the same card, as just described.

Figure 18-7 describes the other two possible combinations within the same node. The first example shows how you can configure a virtual path DAX-connection on one UXM module, creating a VPC to VCC local connection to a port on a UXM module on the same node. This VCC then goes out on the network to the public ATM cloud, with the Virtual Path encapsulated, or "tunnelled", within it. (A DAX connection is connection that is local to the node.)

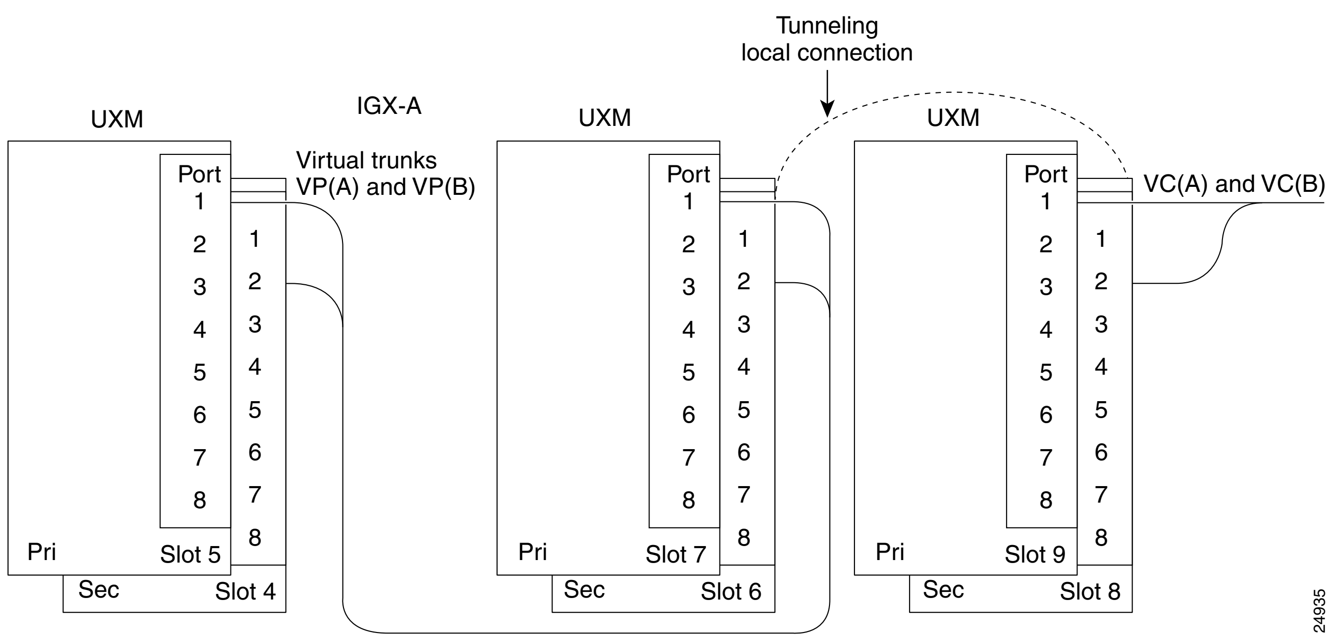
The second example shows a tunneling connection configuration spanning across a maximum of three slots, with one trunk port on one slot (as the virtual trunk port) and the other two ports on two different slots as line ports, if the interface requirements are met for connecting trunk port to line port back to back.

Note As you configure the VP tunnelling connections in the nodes, you can display all the VP tunnelling connections on a particular node by using the **dspcons -tun** command.

Configuring VP Tunnelling Connections on an IGX Node with Y-Redundancy

Y-cable redundancy is also supported with the VP Tunnelling feature. Therefore, each card can have its own Y-redundant pair. In the case where all three ports reside on different cards, each card must be configured with Y-redundancy. The Y-cable setup can be configured as shown in Figure 18-8.

Figure 18-8 Configuration of VP Tunnelling Connections in an IGX and Y-Redundancy



VP Tunnelling Feature Summary

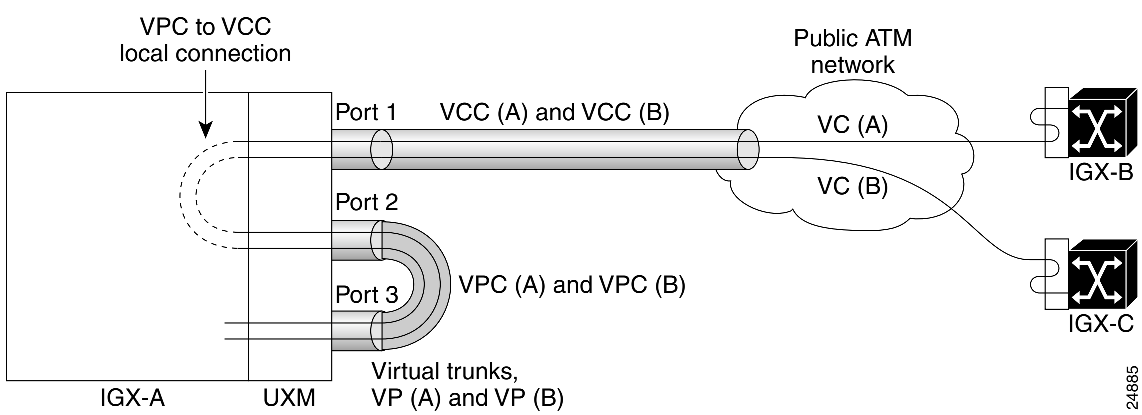
Following are some important feature details that you should know about before configuring VP tunnelling into your network:

- The VCC (Virtual Circuit Connection) should be provided by the cloud administrator. In this example, the VCC (ATM-UNI or NNI) is between port 1 (of IGX A) and port 1 (of IGX B). The ATM-UNI ports (UXM port 1, in this example) will be feeding these VCs, which are provided by the cloud from either end.
- The physical interface at the cloud entry point should match that of the VC side of the tunnelling connection, so that the line port interface can be activated. You can add the virtual trunk between trunk end points, regardless of the interface type, such as T1/E1/T3/E3/OC-3.
- The VP Tunneling feature assumes that the UXM virtual trunking features are available in Release 9.2 switch software. Because the Ports and Trunks feature is also available with Release 9.2, a single UXM card with multiple port interfaces can be used to implement this feature. In addition, you can use this feature where three ports are available across three different UXM cards on the same node.
- In this example, trunk port 3 will be configured as a virtual trunk on each of the IGXs. (Port 3 is physically cabled to port 2.) After provisioning the VP tunneling connections, you add the virtual trunk with the specific VPI, configured on the virtual trunk interface.
- The DAX connections within the IGX node at the entry points to the cloud will be provided by the tunnelling connection. This connection type can be the ATM connection types supported by UXM virtual trunks, that is, ABR, CBR, UBR and VBR. This connection type has to be the same as the VCC connection type provisioned within the cloud.

Setting up the VPC to VCC Tunnelling Connection on the UXM

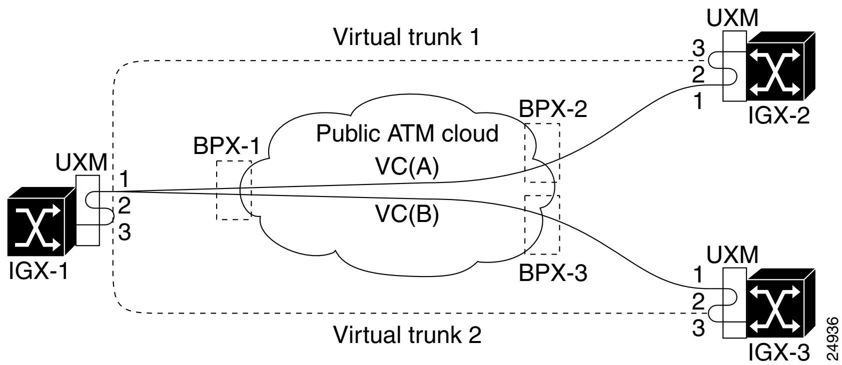
At each IGX node accessing the public ATM network, implement the setup on the UXM module identified below and as shown in Figure 18-9.

Figure 18-9 IGX-UXM Setup and Configuration



At each IGX node that interfaces to the cloud, you must perform the similar setup described in the steps below. The following example is illustrated with a private ATM cloud containing BPX nodes with ASI interfaces. See Figure 18-10 for an illustration of VP tunnelling connections within the BPX cloud.

Figure 18-10 VP Tunnelling Connections within a BPX Cloud



Step 1 Port 3 is used for virtual trunks. (Port 3 is only used for this example—you can configure any port for virtual trunking.) Normally, to use the virtual trunk feature, this port is connected to a public ATM network that supports virtual path connections.

Step 2 Use a cable to connect port 3 to another port (port 2) on the same UXM card, or another UXM card.

The interface type much match so that the line port can be activated on port 2.

Step 3 Connect port 1 to the public ATM cloud. As shown in the example above in Figure 18-10, connect BPX-1 (ASI/BXM) at the cloud to IGX-1 (UXM port 1), with the matching interface types. Repeat the steps for IGX2-BPX2 and IGX3-BPX3 pair. For illustration purposes, assume that the UXMs on all the IGXs are in slot 5, and that the ASIs at the BPXs are in slot 10.

Step 4 Provision the VC within the ATM cloud. If the cloud is comprised of Cisco nodes (such as BPXs), you can provision the VC connection at BPX1 with the **addcon** command, where there is connectivity available between BPX-1 and BPX-2.

```
addcon 10.1.1.200 BPX-2 10.1.1.200 CBR
```

This connection is referred to as VC(a) within the cloud. The bandwidth required for this connection cannot exceed the maximum configurable bandwidth for the UXM virtual trunk.

Similarly provision the VC(b) connection with another **addcon** command at BPX-1; for example:

```
addcon 10.1.1.300 BPX-3 10.1.1.200 CBR ...
```

The connection just added is referred to as VC(b) within the cloud.

Step 5 Add a local connection between port 2 to port 1 for VP(a) to VC(a), and VP(b) to VC(b). In this example, port 2 is referred as the VP side of the connection, and port 1 is referred to as the VC side of the connection. This new connection will provide an encapsulation function. In this example, the **addcon** command syntax will look like the following:

```
addcon 5.2.1.*  IGX-1 5.1.1.200 CBR ....
```

```
addcon 5.2.3.*  IGX-1 5.1.1.300 CBR ....
```

You must select the VPI/VCI at the VC side so that it will match up with the VPI/VCI provisioned at the cloud. Also, the VPI at the VP side of the tunneling connection should be selected so that it will match with the VPI configured on the virtual trunk at port 3. Add similar connections at the other ends of the provisioned VC—at IGX-2 and IGX-3.

Step 6 After the VP tunnelling connection is established at both ends, you can add the virtual trunk between the trunk ports 3 as shown in the following sub-steps.

Note The VPI selected at port 2 should match the VPI of the trunk port activated at port 3.

```
uptrk 5.3.10
```

to activate the virtual trunk.

```
cnftrk 5.3.10
```

to configure the VPI on this virtual trunk, to be the VPI used for adding the tunneling connection at the VP side. In this example, 1 is the VPI selected for the trunk between IGX-1 and IGX-2. You can configure and activate another trunk, for example (5.3.15), for the VPI value of 3 corresponding to VC(b).

```
addtrk 5.3.10
```

This **addtrk** command adds the virtual trunk between IGX-1 and IGX-2 (if IGX-2 had similar tunneling connections to that of IGX-1, and is physically attached to BPX-2 at the cloud entry point). Similarly, the virtual trunk 5.3.15 can be added between IGX-1 and IGX-3 (VPI=3).

You can display the trunks at IGX-1 between IGX-2/IGX-3 by using a **dsptrks** command as follows:

```
5.3.10          E3/19              Clear-OK              IGX-2/5.3.10

5.3.15          E3/19              Clear-OK               IGX-3/5.3.5
```

The required connections for the above setup at IGX-2 will be:

```
addcon 5.1.1.200 IGX-2 5.2.1.* CBR ......and cnftrk 5.3.10 to VPI = 1
```

and similarly at IGX-3:

addcon 5.1.1.300 IGX-3 5.2.3.* CBR ......and cnftrk 5.3.5 to VPI = 3

Step 7 The back to back cabled ports (Virtual Trunk port and one of the other line ports) should be running the same port interface protocol (UNI or NNI or no protocol). However, this protocol does not need to be the same as the protocol running on the port at the VC side of the tunneling connection.

Step 8 Enable ILMI on port 1 and port 2. These ILMI status changes will be propagated between the VC attached to the cloud and the VP used by the virtual trunk.

Step 9 The VC failure on the cloud has to be propagated to the line ports, so that the endpoints on the IGX side can be conditioned.

Some Things to be Aware of

The following are known limitations of this feature:

1. Because UXM hardware does not support local switching, twice the amount of UBU is required because cells must visit the bus twice. If necessary, an additional IGX node may be required to implemented VP tunneling.

This limit is imposed in case the system runs out of UBU on a single IGX node. Normally, traffic is contacting the MUXBUS once in one direction (that is, in on one port and out on another port). With this VP tunneling, traffic is contacting the MUXBUS twice. An additional visit on the MUXBUS is for the traffic coming in on the port connected to the virtual trunk port through cable, and going out on another port attaching to the public ATM cloud. Thus, additional UBU is required for this second visit on the MUXBUS.

If the system runs out of UBU on a single IGX node, an additional IGX may be required to implement the wrap around, that is, to connect the virtual trunking cable to a port on another IGX. However, this configuration is not supported by the current implementation of VP tunneling.

2 This VP tunneling connection is limited to a local connection only. This VP tunnelling connection is not allowed over any trunk.

3 Clock source must be derived from either the cloud or a external clock source. Clock source cannot be passed over the cloud. This is a known limitation of virtual trunks.

4 There may be a delay of trunk failure detection in case physical failure (for example, LOS) occurs on the port connected to the cloud. Normally, physical failure automatically triggers virtual trunk failure. In our case, the failure is propagated to virtual trunk using ILMI status changes.

5 Note that the Traffic Shaping option may be required on the UXM port connected to the ATM network cloud to maintain the CDV (Cell Delay Variation) of the VC traffic going through the cloud.

6 Additional bandwidth is necessary to be subscribed from the public ATM network for virtual circuit connection as compared to virtual path connection. The efficiency of this solution is approximately at 50%.

This configuration requires that congestion cannot occur at the port attached to the public ATM network. For example, if the port speed attached to the public ATM network is *x* cells/second, then the sum of the virtual trunk's transmit rate terminated on this port should not exceed *x*/2 cells/second. If congestion occurs at this port, node unreachability may occur. This is because the same queue is being used for this local connection, which contains both networking traffic and user traffic. If traffic is dropped due to congestion, network traffic may be dropped causing node unreachability in the network.

Impact of VP Tunnelling on Performance

There should be no performance impact except for trunk failure due to LOS as described in Item 4 in the "Some Things to be Aware of" section on page 18-24.

UXM trunks use more than one Virtual Interface (Virtual Interface) per physical port: each of these virtual interfaces aggregates a group of traffic-type based queues. On a physical port supporting multiple virtual trunks, one VI is used to support each virtual trunk. The maximum number of virtual trunks per card equals the number of VIs. This is 15 for UXM cards, which can support a maximum of 8000 LCNs. If there are active ports on a UXM card, the number of virtual trunks/interfaces will be reduced accordingly, so that the total number of virtual trunks that can be active is 15.

Two ends of a virtual trunk can have different port interfaces. For example, a virtual trunk supported by a UXM-OC-3 on one end can be supported by a BXM-T3 at the other end. BNI virtual trunks are incompatible with UXM and BXM virtual trunks. UXM and BXM virtual trunks are compatible with each other. The incompatibility is due to the cell formats used by BNI (StrataCom Trunk Interface, or "STI") as opposed to standard ATM cell formats used by BXM/UXM. Virtual trunks support ATM-UNI or ATM-NNI interfaces, and the VPIs that can be used are limited to 1–255 for UNI and 1–4095 for NNI virtual trunks.

Command Line Interface

The **addcon** command allows you to add a tunnelling DAX connection. Adding a connection supports one end of the connection as the VP connection, and the other end as a VC connection between different port interfaces of the same card or different cards. You reference the virtual trunk port as <*slot*>.<*port*>.<*vtrk*>. You can configure bandwidth parameters when adding a connection with the **addcon** command, and upping a connection and downing a connection. The following screens show some of these display changes. All the commands that support the UXM connections are available for VP tunneling connections also. You add the tunneling connection by using the **add-on** command; for example:

addcon slot.port.vpi.vci <nodename> otherend_slot.otherend_port.vpi.* <atm_class>

with either end as the VPI or VCI side. If a tunnelling connection is attempted between nodes or non-UXM cards, you will be prompted with error messages.

Following are the **dspcons** and and **dspcon** screens, showing the added connections:

System Response

```
sw224          TRM   StrataCom       IGX 8420  9.2.a5    Mar. 5 1999  11:10 PST

 Local          Remote      Remote
 Channel        NodeName    Channel         State  Type     Compress   Code COS
 12.1.1.100     sw224       12.2.1.*        Ok     cbr
 12.2.1.*       sw224       12.1.1.100      Ok     cbr




Last Command: dspcons
```

System Response

```
sw224          TRM   StrataCom       IGX 8420  9.2.a5    Mar. 5 1999  11:10 PST
Conn:  12.2.1.*          sw224       12.1.1.100         cbr      Status:OK
   PCR(0+1)     % Util    CDVT(0+1)     Policing
   1000/1000   100/100   10000/10000     4/4

Pri: L  Test-RTD: 0 msec
Path:   Route information not applicable for local connections


sw224     UXM:   OK                   sw224     UXM:   OK
          Line 12.2 : OK                        Line 12.1 : OK
          OAM Cell RX: Clear                    NNI:   OK
          NNI:   OK

This Command: dspcon 12.2.1.*
```

External Interfaces/Cisco WAN Manager

All the statistics supported on a UXM connection will also be supported on the UXM tunneling connections. Event logging, alarm notifications through a Robust message, and TFTP statistics collection are enhanced to support the virtual path tunneling connection. Upon VC connection failure reported from the cloud, the information is propagated to each virtual trunk using the ILMI protocol.

Common Control—The standby updates handle these new types of connections.

SNMP—Provisioning of the VP tunneling connection is supported by SNMP (Cisco WAN Manager). This includes changes to:

— atmEndptDesc

— atmOtherEndptDesc in AtmEndptEntry

Parsing routines to enable VP tunnelling connections are different from previous releases of switch software to be added through SNMP. The MIB has not changed (to support the tunnelling connections).

Table 18-4 MIB Objects Supported for VP Tunneling

MIB Objects Supported	Description of MIB Object	Ranges/Values
atmEndptDesc	String describing this end-point. Contains information about the domain, nodename, slot, port, vpi, and vci for the endpoint. For example, D1.Node1.12.1.100.200, is a valid description. Domain and nodename need not be given but slot, port, and nodename need not be given but slot, port, VPI, and VCI values must exist; 12.1.100.200 is valid. A virtual path connection endpoint of the form 12.1.100.* is also valid. A virtual path tunnelling DAX connection, with one endpoint as VP and other as VC, of the form 12.1.100.*. Node 1.12.2.100.200 is a valid description. For a basis port, the last 4 bits of the VPI must be between 3 and 14.	<*string*>

Table 18-4 MIB Objects Supported for VP Tunneling

MIB Objects Supported	Description of MIB Object	Ranges/Values
atmOtherEndptDesc	String describing the remote PVC endpoint. Contains information about the domain, nodename, slot, port, vpi, and vci for the end-point. For example, D2.Node2,10.100.200 is valid description. Nodename, slot, port, VPI and VCI values must exist. A virtual path connection endpoint of the form D2.Node2.10.1.100.* is also valid. A virtual path tunneling DAX connection, with one endpoint as VC and other as VP of the form 12.1.100.100 Node 1.12.2.100.* is a valid description. For a basis port, the last 4 bits of the VPI must be between 3 and 14.	<*string*>

Command List

Click on a page number to go to a command definition.

Command	Page
cnfcos	10-9
cnfdate	13-5
cnfdch	7-23
cnfdchtp	7-23
cnfdclk (Data)	7-32
cnffwswinit	13-6
cnfdclk (FastPAD)	16-27
cnfoamlpbk	14-61
cnffrcls	8-26
cnffrcon	9-45
cnffrcport (Fr Rly - PCS)	8-32
cnffrport (Fr Rly)	9-47
cnffrport (FastPAD)	16-29
cnfftcport (FastPAD)	16-35
cnffwswinit	13-6
cnffunc	3-41
cnfict (Data)	7-36
cnfict (Fr Rly)	8-46
cnfict (FastPAD)	16-40
cnfleadmon	14-52
cnfln	5-8
cnflnalm	14-57
cnflnpass	6-22
cnfmode	8-51
cnfname	3-46
cnfoamlpbk	14-61
cnfport	9-47
cnfportq	9-54

Command	Page
dspusers	13-24
dspusertask	13-33
dspusertasks	13-36
dspvsich	17-128
dspvsiif	17-119
dspvsipartcnf	17-122
dspvsipartinfo	17-123
dspyred	3-104
editjob	12-19
help or ?	2-5
prtcdred	3-106
prtchcnf (Voice)	6-55
prtchcnf (Data)	7-57
prtchcnf (Fr Rly)	9-107
prtchcnf (FastPAD)	16-75
prtchdlcnf	6-56
prtclnerrs	14-139
prtcons (Voice)	6-57
prtcons (Data)	7-58
prtcons (Fr Rly)	9-107
prtcons (FastPAD)	16-76
prtict (Data)	7-60
prtict (Fr Rly)	8-124
prtict (FastPAD)	16-77
prtjob	12-21
prtjobs	12-22
prtlnerrs	14-141
prtlns	5-31