Cisco BPX 8600 Series Installation and Configuration

Release 9.3.10
July 2001

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-7811603=
Text Part Number: 78-111603-01 Rev. D0

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco BPX 8600 Series Installation and Configuration, Release 9.3.10

Cisco Reader Comment Card

General Information

1 Years of networking experience ______ Years of experience with Cisco products ______

2 I have these network types: □ LAN □ Backbone □ WAN
□ Other:

3 I have these Cisco products: □ Switches □ Routers
□ Other: Specify model(s)

4 I perform these types of tasks: □ H/W Install and/or Maintenance □ S/W Config
□ Network Management □ Other:

5 I use these types of documentation: □ H/W Install □ H/W Config □ S/W Config
□ Command Reference □ Quick Reference □ Release Notes □ Online Help
□ Other:

6 I access this information through: ____% Cisco Connection Online (CCO) ____% CD-ROM
____% Printed docs ____% Other:

7 Which method do you prefer?

8 I use the following three product features the most:

Document Information

Document Title: Cisco BPX 8600 Series Installation and Configuration

Part Number: 78-11603-01 Rev. D0 S/W Release (if applicable): 9.3.10

On a scale of 1–5 (5 being the best) please let us know how we rate in the following areas:

_____ The document was written at my technical level of understanding.

_____ The information was accurate.

_____ The document was complete.

_____ The information I wanted was easy to find.

_____ The information was well organized.

_____ The information I found was useful to my job.

Please comment on our lowest score(s):

Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

City State/Province ZIP/Postal Code

Country Phone ( ) Extension

Fax ( ) E-mail

Can we contact you further concerning our documentation? □ Yes □ No

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**.

CONTENTS

PART 2 **Installation**

CHAPTER 6 **Installation Overview** 6-1

CHAPTER 23

CHAPTER 29

CHAPTER 30

PART 6

BPX Specifications

CHAPTER 31

TABLES

FIGURES

Preface

This manual is the primary Cisco guide to installing and configuring the BPX 8600 Series wide-area switches. It provides:

- Description and specifications of the switch hardware, chassis, cards, cables, and peripherals
- Description of WAN switch software
- Procedures for the installation of the switch, cards, cables, control terminals
- Procedures for initial startup.
- Procedures for configuring the BPX cards
- Procedures for configuring lines and trunks
- Procedures for provisioning (making ocnnections to your network).

The 8600 series of Broadband Packet Exchange switches include:

- BPX 8620 wide-area switch
- BPX 8650 IP + ATM switch
- BPX 8680 universal service switch
- BPX 8680-IP (BPX+MGX8800+7204LSC)

Instructions for configuring MPLS on BPX switches, see the *Cisco MPLS Controller Software Configuration Guide*.

Instructions for configuring PNNI on BPX switches, see the *Cisco SES PNNI Controller Software Configuration Guide.*

All terms are defined in the Glossary.

Refer to current Release Notes for additional supported features.

Documentation CD-ROM

Cisco documentation and additional literature are available in the CD-ROM package that ships with your product. Because the Documentation CD-ROM is updated monthly, it might be more current than printed documentation.

To order additional copies of the Documentation CD-ROM, contact your local sales representative or call Cisco 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
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.

Audience

This publication is intended for those installing the BPX 8600 series broadband network switches. Installers should be familiar with electronic circuity and electrical wiring practices and should have experience as an electronic or electromechanical technician.

It is also intended for the network administrator performing initial BPX configuration. Both the installers and the network administrator should be familiar with BPX network operation. Administrators should be familiar with LAN and WAN protocols and current networking technologies such as Frame Relay and ATM.

Cisco WAN Switching Product Name Change

The Cisco WAN Switching products were once known by older names.

Old Name	New Name
Any switch in the BPX switch family (Cisco BPX® 8620 broadband switch and Cisco BPX® 8650 broadband switch)	A Cisco BPX® 8600 series broadband switch
The BPX Service Node switch	The Cisco BPX® 8620 broadband switch
The BPX switch as a Label Switch Controller	The Cisco BPX® 8650 broadband switch
The AXIS shelf	The Cisco MGX™ 8220 edge concentrator
Any switch in the IGX switch family (IGX 8, IGX 16, and IGX 32 wide-area switches)	The Cisco IGX™ 8400 series multiband switch
The IGX 8 switch	The Cisco IGX™ 8410 multiband switch
The IGX 16 switch	The Cisco IGX™ 8430 multiband switch.
Cisco StrataView Plus®	Cisco WAN Manager® (CWM)

Related Documentation

The following Cisco publications contain additional information related to the operation of the BPX switch and associated equipment in a Cisco WAN switching network:

Cisco BPX 8600 Series Installation and Configuration DOC-7810674=	Provides a general description and technical details of the BPX broadband switch.
Cisco IGX 8400 Series Reference DOC-7810706=	Provides a general description and technical details of the IGX multiband switch.
Update to the Cisco IGX 8400 Series Reference Guide DOC-7811029=	Provides update information about new features in the 9.3.10 Switch Software release that apply to the IGX 8400 switch. Use this update document in conjunction with the Cisco IGX 8400 Series Reference, 9.3.05 Switch Software release documentation on the IGX 8400 switch.
Cisco IGX 8400 Installation and Configuration DOC-7810722=	Provides installation instructions for the IGX multiband switch.
Update to the Cisco WAN Switching Command Reference Guide DOC-7810703=	Provides update information about new features contained in the 9.3.10 Switch Software release that apply to both BPX and IGX switches documented in the WAN Switching Command Reference. Use this update document in conjunction with *Cisco WAN Switching Command Reference, Release 9.3.05*.
Cisco WAN Switching Command Reference DOC-7811457=	Provides detailed information on the general command line interface commands.
Cisco WAN Switching SuperUser Command Reference DOC-7810702=	Provides detailed information on the command line interface commands requiring SuperUser access authorization.
Cisco MPLS Installation and Configuration DOC-7810672=	Provides information on a method for forwarding packets through a network.
WAN CiscoView for the IGX 8400 Switches DOC-7810669=	Provides instructions for using WAN CiscoView for the IGX 8400.
WAN CiscoView for the BPX 8600 Switches DOC-7810670=	Provides instructions for using WAN CiscoView for the BPX 8600.
Cisco WAN Manager Installation Guide for Solaris, Release 10 DOC-7810308=	Provides procedures for installing Release 10 of the Cisco WAN Manager (CWM) network management system on Solaris systems.
Cisco WAN Manager User's Guide, Release 10 DOC-7810658=	Provides procedures for using Release 10 of the Cisco WAN Manager (CWM) network management system.

Cisco WAN Manager SNMP Proxy Agent Guide DOC-7810786=	Provides information about the Cisco WAN Manager Simple Network Management Protocol (SNMP) Service Agent components and capabilities.
Cisco WAN Manager Database Interface Guide DOC-7810785=	Provides the information to gain direct access to the Cisco WAN Manager Informix OnLine database that is used to store information about the elements within your network.

Conventions

Command descriptions use these conventions:

- Commands and keywords are in **boldface**.
- Arguments for which you supply values are in *italics*.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and 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 *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

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

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. (To see translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment.)**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.**

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel ette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Timesaver Means *the described action saves time*. You can save time with this action.

PART 1

The BPX Switch

CHAPTER 1

The BPX Switch: Functional Overview

This chapter introduces the BPX 8600 Series broadband switches and describes the main networking functions:

- The BPX 8600 Series
- New with Release 9.3
- Discontinued
- BPX Switch Operation
- Traffic and Congestion Management
- Network Management
- Switch Software Description
- Network Synchronization
- Switch Availability

Also, refer to the *Cisco WAN Switching Command Reference* publications.

Refer to Release Notes for additional supported features.

The BPX 8600 Series

Cisco BPX 8600 series wide-area switches offer a variety of service interfaces for data, video, and voice traffic, and support numerous connectivity options to address a broad range of diverse needs. Network interface options include broadband (T3/E3 to OC-12/STM-4) and narrowband (64 Kbps to n x T1/E1) via leased lines or public ATM services. Additionally, the BPX switch provides a cost-effective solution by offering a wide range of port densities via the MGX 8220 and MGX 8800 edge concentrators. Proven in the world's largest networks, the Cisco BPX 8620, 8650, and 8680 help you to anticipate and meet market demands while eliminating technology risk.

The Cisco BPX® 8600 series wide-area switches are standards-based high-capacity broadband ATM switches that provide backbone ATM switching, IP+ATM services including Multiprotocol Label Switching (MPLS) with trunk and CPU hot standby redundancy. The BPX 8600 series deliver a wide range of other user services (see Figure 1-1).

The BPX 8600 Series includes:

- BPX 8620 wide-area switch
- BPX 8650 IP+ATM switch

- BPX 8680 universal service node
- BPX 8680-IP (BPX + MGX 8850 + 7204 LSC)

BPX 8620

The Cisco BPX 8620 switch is a scalable, standards-compliant unit, fully compatible with:

- Cisco MGX™ 8800 series wide-area edge switch
- Cisco MGX 8220 edge concentrator
- Cisco IGX™ 8400 series wide-area switch
- Cisco Service Expansion Shelf

The BPX multishelf architecture integrates both IP and ATM services, thereby enabling you to deploy the industry's widest range of value-added services. This architecture offer low-cost entry points for small sites up to unprecedented port density and scalability for the very largest sites. Finally, it supports both broadband services and narrowband services within a single platform.

The architecture supports both the broadband BPX switch and up to 16 edge concentrator shelves. This scalability results in full utilization of broadband trunks and allows the BPX switch to be expanded incrementally to handle an almost unlimited number of subscribers.

The edge concentrators terminate traffic from a variety of interfaces, such as IP, Frame Relay, ATM, and circuit emulation, and adapt non-ATM traffic into ATM cells. This traffic is aggregated and sent to the BPX switch where it is switched on high-speed ATM links. This aggregation on a single platform maximizes the density of broadband and narrowband ports. High-density aggregation of low-speed services also optimizes the efficiency of the high-speed switching matrix and broadband card slots.

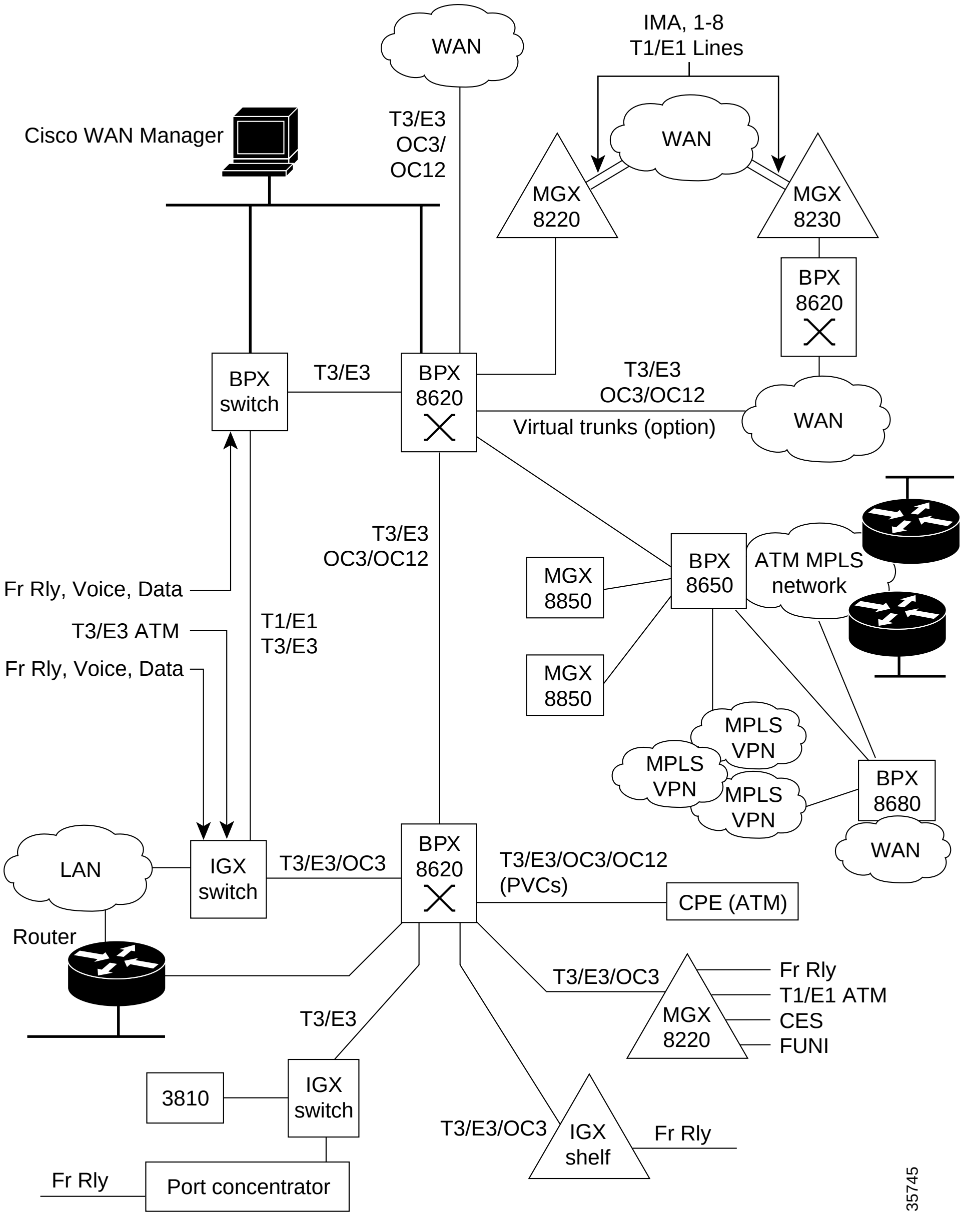
The multishelf view is a "logical" view. Physically, the edge concentrator shelves may be co-located with the BPX switch or they may be located remotely. The connection between a shelf and the BPX switch is a high-speed, optionally redundant ATM link.

The BPX switch consists of the BPX shelf with fifteen card slots that may be co-located with the MGX 8220 or MGX 8800 and Service Expansion Shelf (SES) as required.

Three of the slots on the BPX switch shelf are reserved for common equipment cards. The other twelve are general purpose slots used for network interface cards or service interface cards. The cards are provided in sets, consisting of a front card and its associated back card.

The BPX shelf can be mounted in a rack enclosure that provides mounting for a co-located SES and the MGX 8220 or MGX 8800 interface shelves.

Figure 1-1 BPX Switch General Configuration Example



BPX 8650

The BPX® 8650 is an IP+ATM switch that provides ATM-based broadband services and integrates Cisco IOS® software via Cisco 7200 series routers to deliver Multiprotocol Label Switching (MPLS) services.

The BPX 8650 provides these core Internet requirements:

- scalability
- advanced IP services

- Layer 2 virtual circuit switching advantages
- Layer 2/Layer 3 interoperability

The BPX 8650 supports:

- Premium IP services
  The Internet, intranets, extranets, and IP VPNs, are now available over an ATM infrastructure
- Value-added services, such as content hosting, voice over IP, and video, as well as data-managed services
- ATM Services
  Standards-based ATM interfaces offer broadband and narrowband interconnection for routers, ATM LANs, and other ATM access devices
- The ATM Forum's available bit rate (Abr) virtual source/virtual destination (VS/VD) traffic management capabilities
- Constant bit rate (Cbr)
- Variable bit rate real-time (Vbr-RT)
- Vbr nonreal-time (Vbr-NRT)
- Unspecified bit rate (Ubr)

BPX 8680

The BPX 8680 universal service switch is a scalable IP+ATM WAN edge switch that combines the benefits of Cisco IOS® IP with the extensive queuing, buffering, scalability, and quality-of-service (QoS) capabilities provided by the BPX 8600 and MGX 8800 series platforms.

The BPX 8680 switch incorporates a modular, multishelf architecture that scales from small sites to very large sites and enables service providers to meet the rapidly growing demand for IP applications while cost-effectively delivering today's services.

The BPX 8680 consists of one or more MGX 8850s connected as feeders to a BPX 8620. Designed for very large installations, the BPX 8680 can scale to 16,000 DS1s by adding up to 16 MGX 8850 concentrator shelves while still being managed as a single node.

BPX 8680-IP

The BPX 8680-IP scalable Layer 2/Layer 3 WAN solution integrating the proven multiservice switching technology of the Cisco BPX 8650 switch with the flexibility and scalability of the Cisco MGX 8850. The MGX 8850 switch serves as an edge concentrator to the BPX 8650, which employs the BPX 8600 series switch modular, multishelf architecture to enable scalability. The BPX 8650 switch includes a Cisco 7204 label switch controller (LSC) and supports multiprotocol label switching (MPLS) for New World integrated infrastructures.

New with Release 9.3

With Release 9.3.0, the BPX switch software supports a number of new features:

- Priority Bumping
  This feature allows connections for both BPX and IGX that are classified as more important (via COS value) to bump existing connections that are of lesser importance when there are insufficient resources (such as bandwidth) to route these important connections due to trunk failures in the network. You turn on priority bumping, change parameters, and view the statistics by using the command **cnfbpparm**. This feature cannot be turned on until all nodes are upgraded to 9.3.

  For procedures on using Priority Bumping, see “Optimizing Traffic Routing and Bandwidth” in the *Cisco WAN Switching Command Reference*.
- UXM ATM Forum IMA-Compliant Ports
  This feature addresses the need for IMA line support between the IGX and either a router, LS 1010, or an edge device to complete end-to-end interoperability.You can now bundle multiple physical lines into a logical line to enlarge the traffic bandwidth to support high-speed ATM without upgrading your access line to higher speed service such as T3/E3 line. By grouping a number of T1/E1 lines with inverse multiplexing of the data flow (ATM Forum IMA protocols) into the group of T1/E1 lines, the group of lines can be treated as a logical high-bandwidth line to solve the narrow bandwidth problem with the advantage of availability and cost-effectiveness.
- BXM to BXM-E Upgrades
  It is now possible to gracefully “hitlessly” upgrade an active legacy BXM configured in 16K mode to an enhanced BXM-E (DX, EX) configured in 32K mode. You can scale up your networks with the 32K BXM-E on either the port or trunk or a combination of both without any down time and without any service interruption. This feature also supports BXM-E on APS.
- Separate Software Abort Table
  Previously, the BPX and IGX switch software logged both critical and non-critical errors into the Software Error Table. Due to the limited number of entries in the table (12), critical errors (aborts) could be overwritten by non-critical errors, making it hard to determine the cause of faults. The separate Software Abort Table contains only the critical abort faults and retrieved Abort information for reporting and debugging purposes. After an upgrade, old aborts that are stored in the Software Error Table will not be migrated to the new Software Abort Table. Only new aborts will be logged into the Abort table.
- Upgrade Protection
  This enhancement provides additional protection against running loadrev/runrev and doing upgrades during the time that statistics collection is enabled. This enhancement will warn and automatically disable statistics collection: “**Warning: Statistics collection will be automatically disabled**.”
- VSI MIB Support
  Enables the BPX software to track specific information about a VSI controller (such as type, capability, resource usage, and so on). In order for the network management system to find out about them, they need to query the controller directly via SNMP. This enhancement is to provide via SNMP MIB the capability to query the BPX switch for VSI controllers attached to that switch and associated information. This allows for easier discovery of BPX-attached VSI controllers by external SNMP-capable applications (including Cisco WAN Manager).
- Support for <50 cps for Connections on the BXM and UXM Cards.
  With policing turned off this will be supported on all interface types. However, with policing on, the minimum rate will be lowered from 12 to 6 cps only for the T3/E3 and T1/E1 interfaces.

- Enhanced Shaping of the Control Traffic
  This feature limits the maximum bandwidth guaranteed by the high priority Qbins so that the control traffic does not flood the trunk and overtake the bandwidth allocated for user traffic.
- Support for Three VSI Partitions
  The BXM now supports Three VSI partitions.
- Soft and Dynamic VSI Partitioning
  In Release 9.3.10, BPX switch software provides Soft Partitioning and Dynamic Partitioning of its resources to support smooth introduction of another VSI controller into an existing BPX network already configured with an existing VSI controller, easier tuning of switch resources, and the migration of AutoRoute to PNNI. Soft partitioning allows a pool of resources to be used by multiple AR and VSI controllers. Dynamic partitioning allows you alter the switch configuration without deleting and then re-adding it. Now resources allocated to the VSI slave or VSI partition can be reduced and redistributed between different VSI partitions. This feature facilitates the introduction of MPLS into PNNI networks, and MPLS and PNNI or third-party controllers into existing AutoRoute networks.
- Qbin Statistics Reporting to Cisco WAN Manager
  In Release 9.3.10, BPX switch software can now collect, display, and propagate to Cisco WAN Manager the Summary and Interval Statistics of egress Qbin numbers 10 through 15 on IGX UXM trunks and Qbin numbers 1 through 15 on BPX BXM and IGX UXM ports. The newly added statistics are similar to those existing on BPX trunk Qbins 1 through 9. These statistics are helpful for monitoring system performance when using PNNI or MPLS controllers on virtual switch interfaces.
- 800 Board Level Revision Number
  The board level revision number (also known as the Manufacturing 800 number) provides the maximum information possible about a given card, which assists in troubleshooting. This enables Cisco Customer Service to remotely identify the board level revision number without physically removing the card from the slot. This project provides the capability to identify the board level revision number via command line interface, Cisco WAN Manager, or CiscoView.
- ILMI Neighbor Discovery
  In Release 9.3.10, the ILMI Neighbor Discovery feature enables a network management system such as Cisco WAN Manager to discover other external ATM devices, such as Cisco routers, connected to the BXM card.
- Virtual Ports
  In Release 9.3.10, multiple virtual ports are supported on each BXM card interface. Virtual ports on BPX switches provide both virtual port traffic shaping and connection traffic shaping on a QOS basis.

Discontinued

These older hardware components and technologies will be supported for five years from the time they are discontinued:

- The BNI-155 card
- All ASI cards
- The BCC-3 card
- The BCC-3-32 card
- The IPX switch

- The Extended Services Processor (ESP)
  However, PNNI is available on the BPX via the Service Expansion Shelf (SES) PNNI. For a brief description, see Service Expansion Shelf PNNI, page 2-8.
- VSI 1.0
- The FastPAD

BPX Switch Operation

With the BCC-4 card, the BPX switch employs a non-blocking crosspoint switch matrix for cell switching that can operate at up to 19.2 Gbps peak. The switch matrix can establish up to 20 million point-to-point connections per second between ports.

The BXM cards support egress at up to 1600 Mbps and ingress at up to 800 Mbps. The enhanced egress rate enhance operations such as multicast.

Access to and from the crosspoint switch matrix on the BCC is through multiport network and user access cards. It is designed to easily meet current requirements with scalability to higher capacity for future growth.

A BPX switch shelf is a self-contained chassis that may be rack-mounted in a standard 19-inch rack or open enclosure.

All control functions, switching matrix, backplane connections, and power supplies are redundant, and non-disruptive diagnostics continuously monitor system operation to detect any system or transmission failure. Hot-standby hardware and alternate routing capability combine to provide maximum system availability.

The BPX Switch with MGX 8220 Shelves

Many network locations have increasing bandwidth requirements due to emerging applications and the confluence of voice, data, and video digital communications. To meet these requirements, you can overlay your existing narrowband networks with a backbone of BPX switches to utilize the high-speed connectivity of the BPX switch operating at up to 19.2 Gbps with its T3/E3/OC-3/OC-12 network and service interfaces.

The BPX switch service interfaces include BXM ports on the BPX switch and service ports on MGX 8220 shelves. The MGX 8220 shelves may be co-located in the same cabinet as the BPX switch, providing economical port concentration for T1/E1 Frame Relay, T1/E1 ATM, CES, and FUNI connections.

Multiprotocol Label Switching

The BPX 8650 MPLS switch combines a BPX switch with a separate MPLS controller (Cisco Series 7200 router). By integrating the switching and routing functions, MPLS combines the reachability, scalability, and flexibility provided by the router function with the traffic engineering optimizing capabilities of the switch.

Multiprotocol Label Switching (MPLS) is a high-performance method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply simple labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS integrates the performance and traffic management capabilities of Data Link Layer 2 with the scalability and flexibility of Network Layer 3 routing. It is applicable to networks using any Layer 2 switching, but has particular advantages when applied to ATM networks. It integrates IP routing with ATM switching to offer scalable IP-over-ATM networks.

In contrast to label switching, conventional Layer 3 IP routing is based on the exchange of network reachability information. As a packet traverses the network, each router extracts all the information relevant to forwarding from the Layer 3 header. This information is then used as an index for a routing table lookup to determine the packet's next hop. This is repeated at each router across a network. At each hop in the network, the optimal forwarding of a packet must be again determined.

The information in IP packets, such as IP Precedence information and information on Virtual Private Network membership, is usually not considered when forwarding packets. Thus, to get maximum forwarding performance, typically only the destination address is considered. However, because other fields could be relevant, a complex header analysis must be done at each router that the packet meets.

The main concept of MPLS is to include a *label* on each packet.

Packets or cells are assigned short, fixed length labels. Switching entities perform table lookups based on these simple labels to determine where data should be forwarded.

The label summarizes essential information about routing the packet:

- Destination
- Precedence
- Virtual Private Network membership
- Quality of Service (QoS) information from RSVP
- The route for the packet, as chosen by traffic engineering (TE)

With Label Switching the complete analysis of the Layer 3 header is performed only once: at the edge label switch router (LSR) which is located at each edge of the network. At this location, the Layer 3 header is mapped into a fixed length label, called a label.

At each router across the network, only the label need be examined in the incoming cell or packet in order to send the cell or packet on its way across the network. At the other end of the network, an edge LSR swaps the label out for the appropriate header data linked to that label.

A key result of this arrangement is that forwarding decisions based on some or all of these different sources of information can be achieved by means of a single table lookup from a fixed-length label. For this reason, label switching makes it feasible for routers and switches to make forwarding decisions based upon multiple destination addresses.

Label switching integrates switching and routing functions, combining the reachability information provided by the router function, plus the traffic engineering benefits achieved by the optimizing capabilities of switches.

For multiservice networks, the BPX 8650 switch provides ATM, Frame Relay, and IP Internet service all on a single platform in a highly scalable way. Support of all these services on a common platform provides operational cost savings and simplifies provisioning for multiservice providers.

Cisco's MPLS solution is described in detail in the *Cisco MPLS Controller Software Configuration Guide*.

Private Network to Network Interface (PNNI)

Private Network to Network Interface (PNNI) is a link-state routing protocol that provides standards-based dynamic ATM routing with QoS support as defined by the ATM Forum. PNNI supports aggregation for private ATM addresses and links between switches, and can scale the network and its performance by configuring PNNI peer groups and hierarchical levels.

A key feature of the PNNI hierarchy mechanism is its ability to automatically configure itself in networks in which the address structure reflects the topology. It is responsive to changes in network resources and availability.

PNNI is available on the BPX switch when an optional Cisco Service Expansion Shelf (SES) PNNI is installed. This controller is connected locally to a BPX 8600 series switch to provide PNNI signaling and routing for the establishment of ATM and Frame Relay switched virtual circuits (SVCs) and Soft Permanent Virtual Circuits (SPVCs) over a BPX 8600 wide area network. The network created with BPX SES PNNI nodes also supports traditional ATM and Frame Relay permanent virtual circuits (PVCs) in a separately partitioned AutoRoute network.

ATM SVCs are ATM connections that are established and maintained by a standardized signaling mechanism between ATM CPE (ATM end systems) across a Cisco WAN switching network. ATM SVCs are set up in accordance with user demand and removed when calls are completed, thus freeing up network resources.

BPX SES PNNI node resources, such as port virtual path identifier (VPI) range and bandwidth and trunk bandwidth, are partitioned between SVCs/SVPCs and PVCs. Resource partitioning provides a firewall between PVCs and SVCs/SVPs so that problems with CPE or large bursts do not affect the robustness and availability of PVC services. Bursty data for either PVCs or SVCs/SPVCs can always use any unused link bandwidth, regardless of partitioning.

For a brief description of the SES PNNI, see Service Expansion Shelf PNNI, page 2-8. Refer to the *Cisco SES PNNI Controller Software Configuration Guide* for detailed information abut the SES.

For further information about PNNI and the SES, refer to the *Cisco SES PNNI Controller Software Configuration Guide.*

Virtual Private Networks

This section is a brief description of the BPX switch's support for Virtual Private Networks (VPN). For additional information, refer to *the Cisco MPLS Controller Software Configuration Guide*.

Conventional VPNs that use dedicated lease lines or Frame Relay Private Virtual Circuits (PVC) and a meshed network (Figure 1-2) provide many advantages, but typically have been limited in efficiency and flexibility.

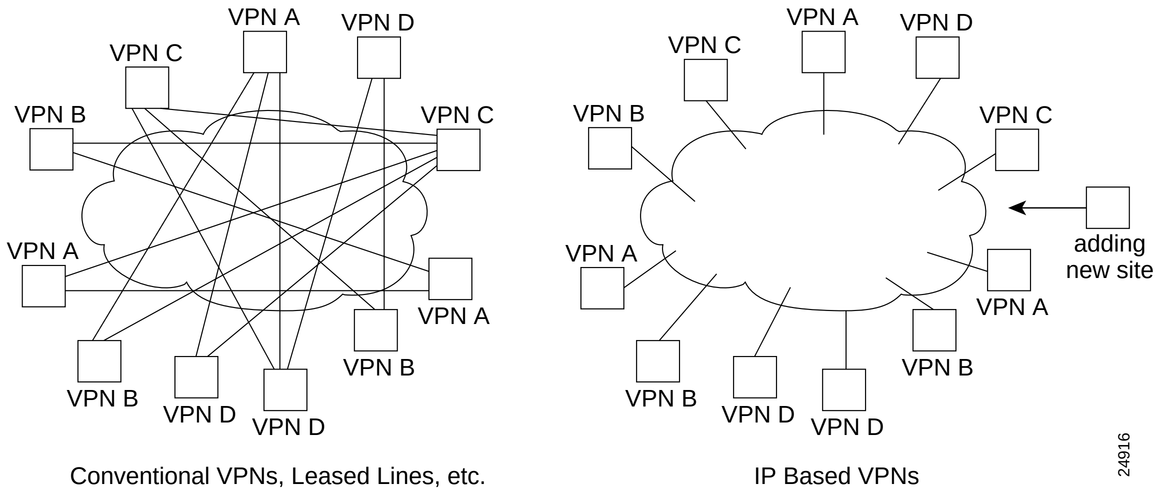
Instead of using dedicated leased lines or Frame Relay PVCs, and so on, for a VPN, an IP virtual private network uses the open connectionless architecture of the Internet for transporting data as shown in Figure 1-2.

An IP virtual private network offers these benefits:

- Scalability
  - Avoids VC mesh configuration
  - Easy to add a new site since IP is connectionless
  - Service provider handles router service management

- Efficiency
  - Rapid provisioning for networks
  - Supports any-to-any intranets

Figure 1-2 IP VPN Service Example



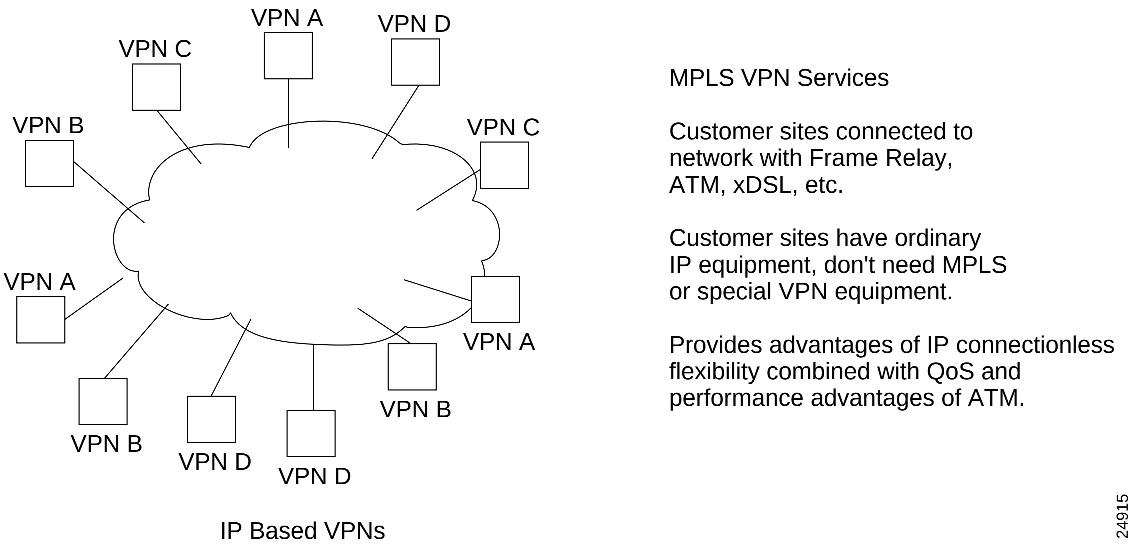
MPLS Virtual Private Networks

MPLS virtual private networks combine the advantages of IP flexibility and connectionless operation with the QoS and performance features of ATM (Figure 1-3).

The MPLS VPNs provide the same benefits as a plain IP Virtual Network plus:

- Scaling and Configuration
  - Existing BGP techniques can be used to scale route distribution
  - Each edge router needs only the information for the VPNs it supports
  - No VPN knowledge in core
  - No need for separate VC mesh per VPN
- Highly Scalability
- Ease of using new sites
  Configure one site on one edge router or switch and network automatically does the rest.
- Traffic Separation in MPLS
  Each packet has a label identifying the destination VPN and customer site, providing the same level of privacy as Frame Relay.
- Flexible Service Grouping
  A single structure can support multiple services, such as voice VPNs, extranets, intranets, Internet, multiple VPNs.

Figure 1-3 MPLS VPNs Example


VPN A
VPN D
VPN C
VPN B
VPN C
VPN A
VPN A
VPN B
VPN B
VPN D
VPN D
IP Based VPNs
MPLS VPN Services
Customer sites connected to network with Frame Relay, ATM, xDSL, etc.
Customer sites have ordinary IP equipment, don't need MPLS or special VPN equipment.
Provides advantages of IP connectionless flexibility combined with QoS and performance advantages of ATM.
24915

Frame Relay to ATM Interworking

Interworking lets you retain your existing services and migrate to the higher bandwidth capabilities provided by BPX switch networks, as your needs expand. 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 (see Figure 1-4)
  - Performed by the BTM card on the IGX switch
  - Performed by the FRSM card on the MGX 8220
- Service Interworking (see Figure 1-5)
  - Supported by the FRSM card on the MGX 8220
  - Supported by the UFM cards on the IGX switch

Network Interworking

Part A of Figure 1-4 shows typical Frame Relay to network interworking. In this example, a Frame Relay connection is transported across an ATM network, and the interworking function is performed by both ends of the ATM network.

These are typical configurations:

- IGX switch Frame Relay (shelf/feeder) to IGX switch Frame Relay (either routing node or shelf/feeder).
- MGX 8220 Frame Relay to MGX 8220 Frame Relay.
- MGX 8220 Frame Relay to IGX switch Frame Relay (either routing node or shelf/feeder).

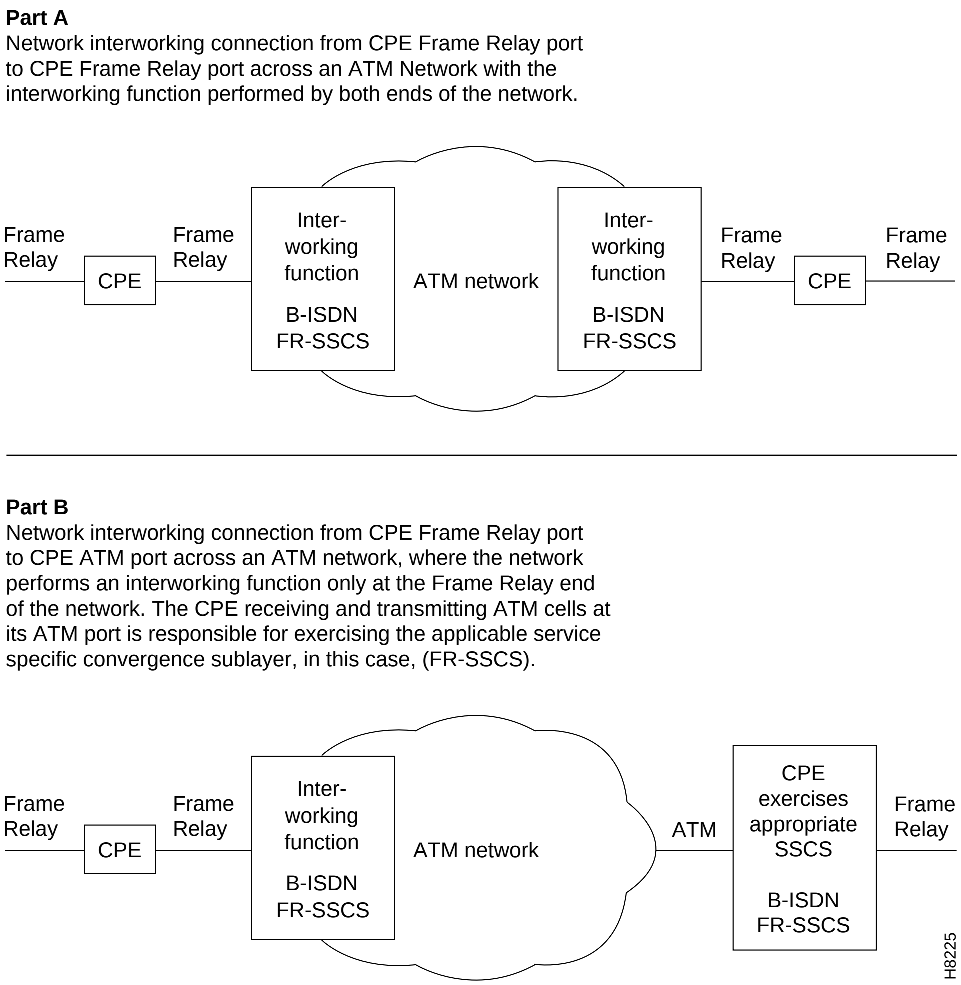
Part B of Figure 1-4 shows a form of network interworking where the interworking function is performed by only one end of the ATM network, and the CPE connected to the other end of the network must itself perform the appropriate service-specific convergence sublayer function.

These are sample configurations:

- IGX switch Frame Relay (either routing node or shelf/feeder) to BPX switch or to MGX 8220 ATM port.
- MGX 8220 Frame Relay to BPX switch or MGX 8220 ATM port.

Network Interworking is supported by the FRM, UFM-C, and UFM-U on the IGX switch, and the FRSM on the MGX 8220. The Frame Relay Service Specific Convergence Sublayer (FR-SSCS) of AAL5 is used to provide protocol conversion and mapping.

Figure 1-4 Frame Relay to ATM Network Interworking



Part A
Network interworking connection from CPE Frame Relay port to CPE Frame Relay port across an ATM Network with the interworking function performed by both ends of the network.

Part B
Network interworking connection from CPE Frame Relay port to CPE ATM port across an ATM network, where the network performs an interworking function only at the Frame Relay end of the network. The CPE receiving and transmitting ATM cells at its ATM port is responsible for exercising the applicable service specific convergence sublayer, in this case, (FR-SSCS).

Service Interworking

Figure 1-5 shows a typical example of Service Interworking. Service Interworking is supported by the FRSM on the MGX 8220 and the UFM-C and UFM-U on the IGX switch. Translation between the Frame Relay and ATM protocols is performed in accordance with RFC 1490 and RFC 1483.

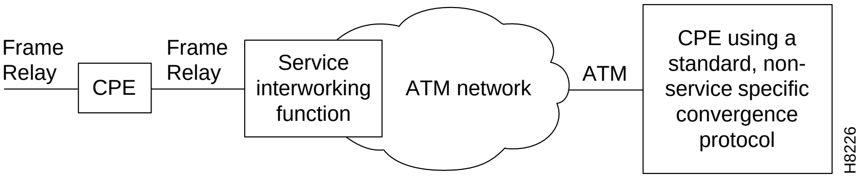
Unlike Network Interworking, in a Service Interworking connection between an ATM port and a Frame Relay port, the ATM device does not need to be aware that it is connected to an interworking function.

The Frame Relay service user does not implement any ATM specific procedures. Also, the ATM service user does not need to provide any Frame Relay specific functions. All translational (mapping functions) are performed by the intermediate interworking function.

This is a typical configuration for service interworking:

- MGX 8220 Frame Relay (FRSM card) to BPX switch or MGX 8220 ATM port.
- IGX switch Frame Relay (FRM-U or FRM-C) to BPX switch or MGX 8220 ATM port.

Figure 1-5 Frame Relay to ATM Service Interworking


Frame Relay
CPE
Frame Relay
Service interworking function
ATM network
ATM
CPE using a standard, non-service specific convergence protocol
H8226

Tiered Networks

Networks may be configured as:

- **Flat**
  All nodes perform routing and communicate fully with one another, or
- **Tiered**
  Interface shelves are connected to routing hubs, where the interface shelves are configured as nonrouting nodes.

By allowing CPE connections to connect to a nonrouting node (interface shelf), a tiered network is able to grow in size beyond that which would be possible with only routing nodes comprising the network.

Starting with Release 8.5, tiered networks support both BPX switch routing hubs and IGX switch routing hubs. Voice and data connections originating and terminating on IGX switch interface shelves (feeders) are routed across the routing network via their associated IGX switch routing hubs.

Tiered networks support multiservice connections, including Frame Relay, circuit data, voice, and ATM. By allowing the customer's equipment to connect to a nonrouting node (interface shelf), a tiered network is able to grow in size beyond that which would be possible with only routing nodes.

Intermediate routing nodes must be IGX switches. IGX switch interface shelves are the only interface shelves that can be connected to an IGX switch routing hub. With this addition, a tiered network provides a multiservice capability (Frame Relay, circuit data, voice, and ATM).

Routing Hubs and Interface Shelves

In a tiered network, interface shelves at the access layer (edge) of the network are connected to routing nodes via feeder trunks (Figure 1-6).

- **Routing hubs**
  Those routing nodes with attached interface shelves are referred to as routing hubs.
- **Interface shelves**
  The interface shelves, sometimes referred to as feeders, are nonrouting nodes.

The routing hubs route the interface shelf connections across the core layer of the network.The interface shelves do not need to maintain network topology nor connection routing information. This task is left to their routing hubs.

This architecture provides an expanded network consisting of a number of nonrouting nodes (interface shelves) at the edge of the network that are connected to the network by their routing hubs.

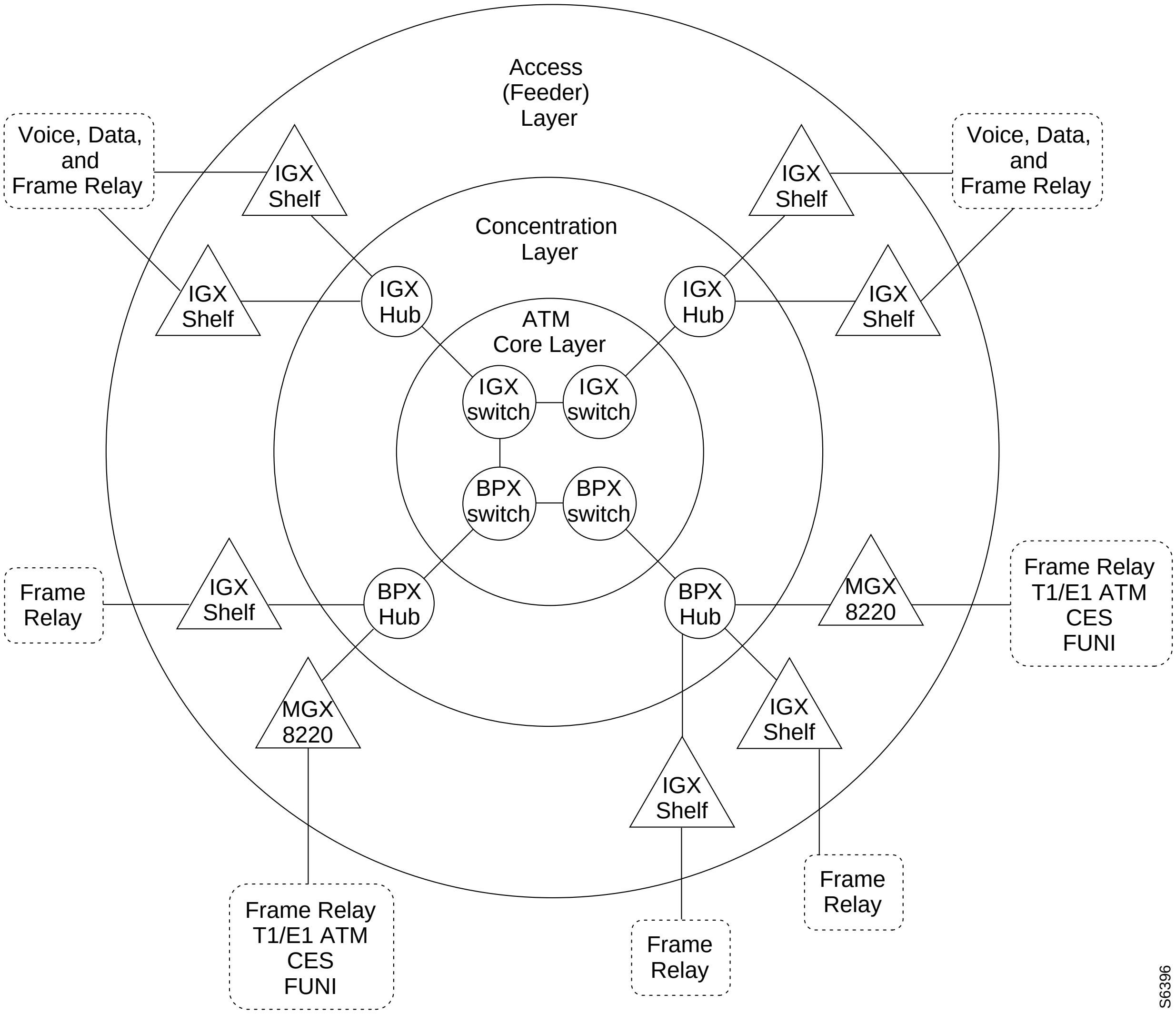
BPX Switch Routing Hubs

T1/E1 Frame Relay connections originating at IGX switch interface shelves and T1/E1 Frame Relay, T1/E1 ATM, CES, and FUNI connections originating at MGX 8220 interface shelves are routed across the routing network via their associated BPX switch routing hubs.

These requirements apply to BPX switch routing hubs and their associated interface shelves:

- Only one feeder trunk is supported between a routing hub and interface shelf.
- No direct trunking between interface shelves is supported.
- No routing trunk is supported between the routing network and interface shelves.
- The feeder trunks between BPX switch hubs and IGX switch interface shelves are either T3 or E3.
- The feeder trunks between BPX switch hubs and MGX 8220 interface shelves are T3, E3, or OC-3-C/STM-1.
- Frame Relay connection management to an IGX switch interface shelf is provided by Cisco WAN Manager.
- Frame Relay and ATM connection management to an MGX 8220 interface shelf is provided by Cisco WAN Manager.
- Telnet is supported to an interface shelf; the **vt** command is not.
- Frame Relay connections originating at IGX switch interfaces shelves connected to IGX switch routing hubs may also be routed across BPX switch intermediate nodes.
- Remote printing by the interface shelf via a print command from the routing network is not supported.

Figure 1-6 Tiered Network with BPX Switch and IGX Switch Routing Hubs



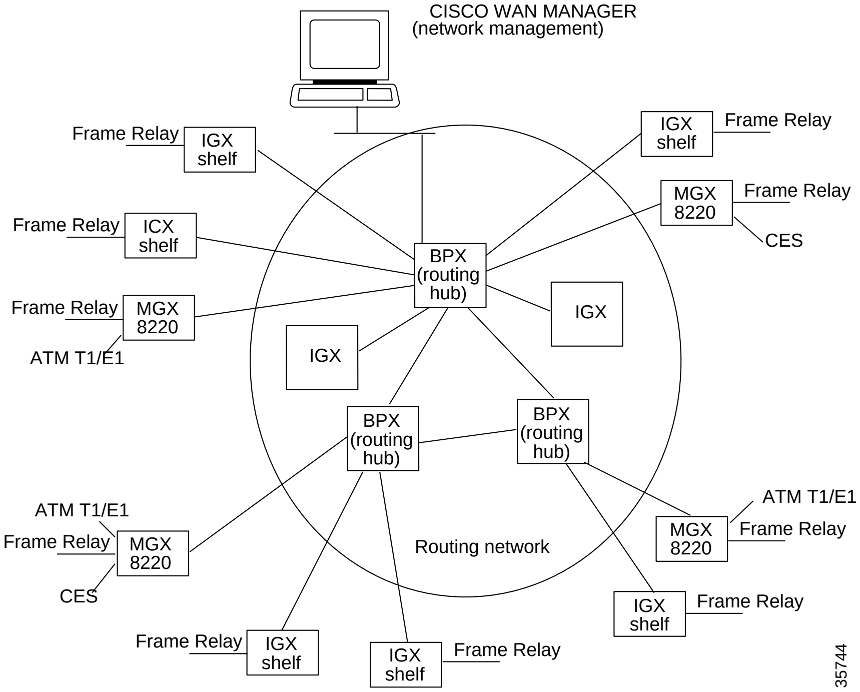
BPX Routing Hubs in a Tiered Network

Tiered networks with BPX routing hubs have the capability of adding interface shelves/feeders (nonrouting nodes) to an IGX/BPX routing network (Figure 1-7). Interface shelves allow the network to support additional connections without adding additional routing nodes.

The MGX 8220 or MGX 8800 and IGX 8400 nodes configured as interface shelves are connected to BPX routing hubs.

The MGX 8220 and MGX 8800 support frame T1/E1, X.21 and HSSI Frame Relay, ATM T1/E1, and CES, and are designed to support additional interfaces in the future.

Figure 1-7 Tiered Network with BPX Routing Hubs



Tiered Network Implementation

These requirements apply to BPX routing hubs and their associated interface shelves:

- MGX 8220 Release 4 level is required on all MGX 8220 interface shelves.
- Only one feeder trunk is supported between a routing hub and interface shelf.
- No direct trunking between interface shelves is supported.
- No routing trunk is supported between the routing network and interface shelves.
- The feeder trunks between BPX hubs and IGX interface shelves may be T3, E3, or OC-3 (since Release 9.2.30).
- The feeder trunks between BPX hubs and MGX 8220 or MGX 8800 interface shelves are T3, E3, or OC-3-C/STM-1.
- Frame Relay and ATM connection management to an MGX 8220 or MGX 8800 interface shelf is provide by Cisco WAN Manager
- Telnet is supported to an interface shelf; the **vt** command is not.
- Remote printing by the interface shelf via a print command from the routing network is not supported.

Tier Network Definitions

Annex G
A bidirectional protocol, defined in Recommendation Q.2931. It is used for monitoring the status of connections across a UNI interface. Tiered Networks use the Annex G protocol to pass connection status information between a hub node and attached interface shelf.

BPX Routing Hub
A BPX node in the routing network that has attached interface shelves. Also referred to as a hub node or BPX hub.

MGX 8220 Interface Shelf
A standards-based service interface shelf that connects to a BPX routing hub, aggregates and concentrates traffic, and performs ATM adaptation for transport over broadband ATM networks.

MGX 8800 Interface Shelf
A standards-based service interface shelf that connects to a BPX routing hub, aggregates and concentrates traffic, and performs ATM adaptation for transport over broadband ATM networks.

IGX Interface Shelf
A special configuration of an IGX switch that is connected as a shelf to an IGX routing hub. An IGX interface shelf is sometimes referred to as an IGX A/F or feeder. The IGX interface shelf does not perform routing functions nor keep track of network topology.

IGX Routing Hub
An IGX node in the routing network that has attached IGX interface shelves. Also referred to as a hub node or IGX hub.

Feeder Trunk
Refers to a trunk that interconnects an interface shelf with the routing network via a BPX routing hub. A feeder trunk is sometimes referred to as an interface shelf trunk.

IGX/AF
Another name for the IGX interface shelf.

Routing Network
The portion of the tiered network that performs automatic routing between connection endpoints.

VPI
Virtual Path Identifier.

VCI
Virtual Connection Identifier.

Upgrades

Converting an IGX node to an interface shelf requires reconfiguring connections on the node because no upgrade path is provided in changing a routing node to an interface shelf.

A BPX node, acting as a Hub Node, is not restricted from providing any other feature normally available on BPX nodes. A BPX Hub supports up to 16 interface shelves.

Connections within tiered networks consist of distinct segments within each tier. A routing segment traverses the routing network, and an interface shelf segment provides connectivity to the interface shelf end-point. Each of these segments are added, configured and deleted independently of the other segments.

Use the Cisco WAN Manager Connection Manager to configure and control these individual segments as a single end-to-end connection.

Interface shelves are attached to the routing network via a BPX routing hub using a BXM trunk (T3/E3 or OC-3) or BNI trunk (T3/E3). The connection segments within the routing network are terminated on the BNI feeder trunks.

All Frame Relay connection types that can terminate on the BPX are supported on the BNI feeder trunk (Vbr, Cbr, Abr, and ATF types). No check is made by the routing network to validate whether the connection segment type being added to a BNI feeder trunk is actually supported by the attached interface shelf.

Co-locating Routing Hubs and Interface Shelves
The trunk between an interface shelf and the routing network is a single point of failure, therefore, the interface shelves should be co-located with their associated hub node. Card level redundancy is supported by the Y-Cable redundancy for the BXM, BNI, AIT, and BTM.

Network Management

Communication between CPE devices and the routing network is provided in accordance with Annex G of Recommendation Q.2931. This is a bidirectional protocol for monitoring the status of connections across a UNI interface. (Note: the feeder trunk uses the STI cell format to provide the ForeSight rate controlled congestion management feature.)

Communication includes the real-time notification of the addition or deletion of a connection segment and the ability to pass the availability (active state) or unavailability (inactive state) of the connections crossing this interface.

A proprietary extension to the Annex G protocol is implemented that supports the exchange of node information between an interface shelf and the routing network. This information is used to support the IP Relay feature and the Robust Update feature used by network management.

Network Management access to the interface shelves is through the IP Relay mechanism supported by the SNMP and TFTP projects or by direct attachment to the interface shelf. The IP Relay mechanism relays traffic from the routing network to the attached interface shelves. No IP Relay support is provided from the interface shelves into the routing network.

The BPX routing hub is the source of the network clock for its associated feeder nodes. Feeders synchronize their time and date to match their routing hub.

Robust Object and Alarm Updates are sent to a network manager that has subscribed to the Robust Updates feature. Object Updates are generated whenever an interface shelf is added or removed from the hub node and when the interface shelf name or IP Address is modified on the interface shelf. Alarm Updates are generated whenever the alarm state of the interface shelf changes between Unreachable, Major, Minor, and OK alarm states.

An interface shelf is displayed as a unique icon in the Cisco WAN Manager topology displays. The colors of the icon and connecting trunks indicate the alarm state of each.

Channel statistics are supported by FRP, FRM, ASI, and MGX 8220 endpoints. BNIs, AITs, and BTMs do not support channel statistics. Trunk Statistics are supported for the feeder trunk and are identical to the existing BNI trunk statistics.

- Preferred Routing
  Preferred routing within the routing network can be used on all connections. Priority bumping is supported within the routing network, but not in the interface shelves. All other connection features such as conditioning, **rrtcon, upcon, dncon**, and so on, are also supported.

- Local and Remote Loopbacks
Connection local and remote loopbacks are managed at the user interface of the FRP endpoint routing node or interface shelf. Remote loopbacks are not supported for DAX connections. The command **addlocrmtlp** supports remote loopbacks at FRP DAX endpoints.
- **Tstcon** and **Testdly**
Tstcon is supported at the FRP endpoints in a non-integrated fashion and is limited to a pass/fail loopback test. Fault isolation is not performed. This is the same limitation imposed on interdomain connections. Intermediate endpoints at the AIT and BNI cards do not support the **tstcon** feature. **Tstdelay** is also supported for the FRP and ASI in a non-integrated fashion similar to that of the **tstcon** command.

Inverse Multiplexing ATM

Where greater bandwidths are not needed, the Inverse Multiplexing ATM (IMA) feature provides a low-cost trunk between two BPX switches.

The IMA feature allows BPX switches to be connected to one another over any of the eight T1 or E1 trunks provided by an IMATM module on an MGX 8220 shelf. A BNI or BXM port on each BPX switch is directly connected to an IMATM module in an MGX 8220 by a T3 or E3 trunk. The IMATM modules are then linked together by any of the eight T1 or E1 trunks.

Refer to the *Cisco MGX 8220 Reference* and the *Cisco WAN Switching Command Reference* publications for further information.

Virtual Trunking

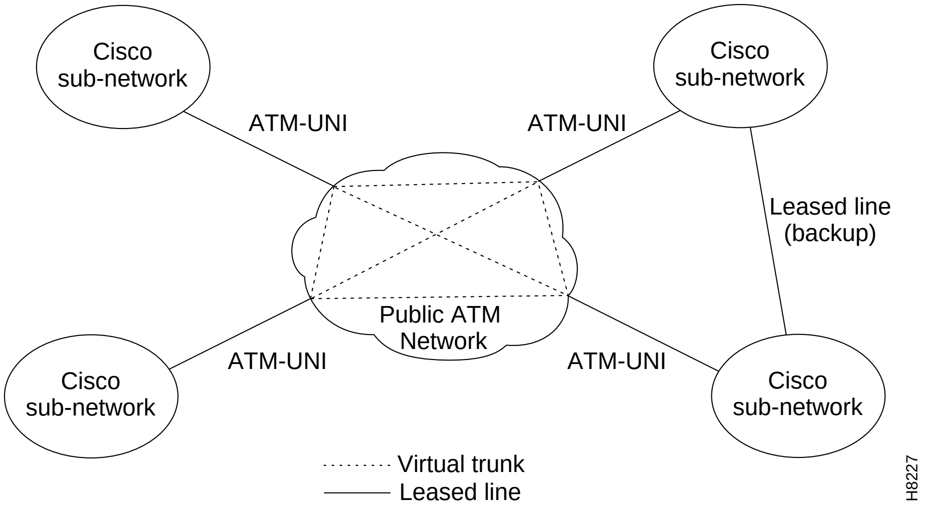
Virtual trunking provides the ability to define multiple trunks within a single physical trunk port interface. Virtual trunking benefits include the following:

- Reduced cost by configuring the virtual trunks supplied by the public carrier for as much bandwidth as needed instead of at full T3, E3, or OC-3 bandwidths.
- Utilization of the full mesh capability of the public carrier to reduce the number of leased lines needed between nodes in the Cisco WAN switching networks.
- Choice of keeping existing leased lines between nodes, but using virtual trunks for backup.
- Ability to connect BNI or BXM trunk interfaces to a public network using standard ATM UNI cell format.
- Virtual trunking can be provisioned via either a Public ATM Cloud or a Cisco WAN switching ATM cloud.

A virtual trunk may be defined as a “trunk over a public ATM service.” The trunk really doesn’t exist as a physical line in the network. Rather, an additional level of reference, called a **virtual trunk number**, is used to differentiate the virtual trunks found within a physical trunk port.

Figure 1-8 shows four Cisco WAN switching networks, each connected to a Public ATM Network via a physical line. The Public ATM Network is shown linking all four of these subnetworks to every other one with a full meshed network of virtual trunks. In this example, each physical line is configured with three virtual trunks.

Figure 1-8 Virtual Trunking Example



Traffic and Congestion Management

The BPX switch provides ATM standard traffic and congestion management per ATM Forum TM 4.0 using BXM cards.

The Traffic Control functions include:

- Usage Parameter Control (UPC)
- Traffic Shaping
- Connection Management Control
- Selective Cell Discarding
- Explicit Forward Congestion Indication (EFCI)
- Priority Bumping

In addition to these standard functions, the BPX switch provides advanced traffic and congestion management features including:

- Support for the full range of ATM service types per ATM Forum TM 4.0 by the BXM-T3/E3, BXM-155, and BXM-622 cards on the BPX Service Node.
- Advanced CoS Management (formerly Fairshare and Opticlass features) Class of Service management delivers the required QoS to all applications.
  - The BPX provides per virtual circuit (VC) queuing and per-VC-scheduling provided by rate controlled servers and multiple class-of-service queuing at network ingress.
  - On egress, up to 16 queues with independent service algorithms for each trunk in the network.
- Automatic Routing Management (formerly AutoRoute feature), end-to-end connection management that automatically selects the optimum connection path based upon the state of the network and assures fast automatic alternate routing in the event of intermediate trunk or node failures.
- Cost-Based Routing Management

- Abr Standard with VSVD; congestion control using RM cells and supported by BXM cards on the BPX Switch.
- Optimized Bandwidth Management (formerly ForeSight), an end-to-end closed loop rate based congestion control algorithm that dynamically adjusts the service rate of VC queues based on network congestion feedback.
- Dynamic Buffer Management, Cisco's Frame Relay and ATM service modules are equipped with large buffers and a dynamic buffer management technique for allocating and scaling the buffers on a per VC basis to traffic entering or leaving a node. The switch dynamically assigns buffers to individual virtual circuits based on the amount of traffic present and service level agreements. The large queues readily accommodate large bursts of traffic into the node.
- PNNI, a standards-based routing protocol for ATM and Frame Relay SVCs.
- Early and partial packet discard for AAL5 connections.

Advanced CoS Management

Advanced Class of Service (CoS) management provides per-VC queueing and per-VC scheduling. CoS management provides fairness between connections and firewalls between connections. Firewalls prevent a single non-compliant connection from affecting the QoS of compliant connections. The non-compliant connection simply overflows its own buffer.

The cells received by a port are not automatically transmitted by that port out to the network trunks at the port access rate. Each VC is assigned its own ingress queue that buffers the connection at the entry to the network. With Abr with VSVD or with Optimized Bandwidth Management (ForeSight), the service rate can be adjusted up and down depending on network congestion.

Network queues buffer the data at the trunk interfaces throughout the network according to the connection's Class of Service. Service classes are defined by standards-based QoS. Classes can consist of the five service classes defined in the ATM standards as well as multiple sub-classes to each of these classes. Classes can range from constant bit rate services with minimal cell delay variation to variable bit rates with less stringent cell delay.

When cells are received from the network for transmission out a port, egress queues at that port provide additional buffering based on the Service Class of the connection.

CoS management provides an effective means of managing the Quality of Service defined for various types of traffic. It permits network operators to segregate traffic to provide more control over the way that network capacity is divided among users. This is especially important when there are multiple user services on one network. The BPX switch provides separate queues for each traffic class.

Rather than limiting the user to the five broad classes of service defined by the ATM standards committees, CoS management can provide up to 16 classes of service (service subclasses) that you can further define and assign to connections. Some of the COS parameters that may be assigned include:

- Minimum bandwidth guarantee per subclass to assure that one type of traffic will not be preempted by another.
- Maximum bandwidth ceiling to limit the percentage of the total network bandwidth that any one class can utilize.
- Queue depths to limit the delay.
- Discard threshold per subclass.

These class of service parameters are based on the standards-based Quality of Service parameters and are software programmable by the user.

Automatic Routing Management

With Automatic Routing Management (formerly referred to as AutoRoute), connections in Cisco WAN switching networks are added if there is sufficient bandwidth across the network and are automatically routed when they are added.

You need enter only the endpoints of the connection at one end of the connection and the IGX switch and BPX switch software automatically set up a route based on a sophisticated routing algorithm. This feature is called Automatic Routing Management. It is a standard feature on the IGX and BPX switches.

System software automatically sets up the most direct route after considering the network topology and status, the amount of spare bandwidth on each trunk, as well as any routing restrictions entered by the user (for example, avoid satellite links). This avoids having to manually enter a routing table at each node in the network. Automatic Routing Management simplifies adding connections, speeds rerouting around network failures, and provides higher connection reliability.

Cost-Based Routing Management

You can selectively enable cost-based route selection as the route selection per node. With this feature, a trunk cost is assigned to each trunk (physical and virtual) in the network. The routing algorithm then chooses the lowest-cost route to the destination node. The lowest cost routes are stored in a cache to reduce the computation time for on-demand routing.

Cost-based routing can be enabled or disabled at anytime. There can be a mixture of cost-based and hop-based nodes in a network.

The “Cost-Based Connection Routing” section on page 1-36, contains more detailed information about cost-based AutoRoute.

Priority Bumping

Priority bumping allows BPX and IGX switch connections classified as more important (via COS value) to “bump” (that is, set aside) existing connections of lesser importance. While the Automatic Routing Management feature is capable of automatically redirecting all failed connections onto other paths, priority bumping lets you prioritize and sustain more important connections when network resources are diminished to a point that all connections cannot be sustained. Network resources are reclaimed for the more important connections by bumping (derouting) the traffic on less important connections.

Priority bumping is triggered by insufficient resources (such as bandwidth), resulting from any number events, including changes to the network made by using the commands **addcon**, **upcon**, **cnfcon**, **cnnfcos**, **cnfpref**, **cnftrk**, and **deltrk**. Other triggers include trunk line/card failure, node failure, and communication failure. The most prominent event is a trunk failure.

For information on setting up Priority Bumping, see “Specifying Priority Bumping” in Chapter 10 of the *Cisco WAN Switching Command Reference.*

Concurrent Routing

Overview

The Concurrent Routing feature is introduced in Switching Software Release 9.3.30 for the BPX and IGX platforms. Concurrent Routing (CR) allows multiple routing requests to be processed simultaneously on a node. For example, a node can initiate (master) one or more routes while simultaneously accepting other routes that pass through it (via) or terminate at it (slave).

If CR is not enabled on a node, routing requests received while a connection is being routed will be rejected or “blocked”. As a result, only one bundle at a time can be routed on a node if CR isn’t enabled This “blocking” algorithm underutilizes the switch’s computational power. Blocked routing is illustrated in Figure 1-9 below.

CR allows the switch’s processor to be more effectively utilized by allowing multiple routes to be in progress concurrently. The result is better overall reroute performance. CR is illustrated in Figure 1-10 below.

Figure 1-9 , Blocked Routing

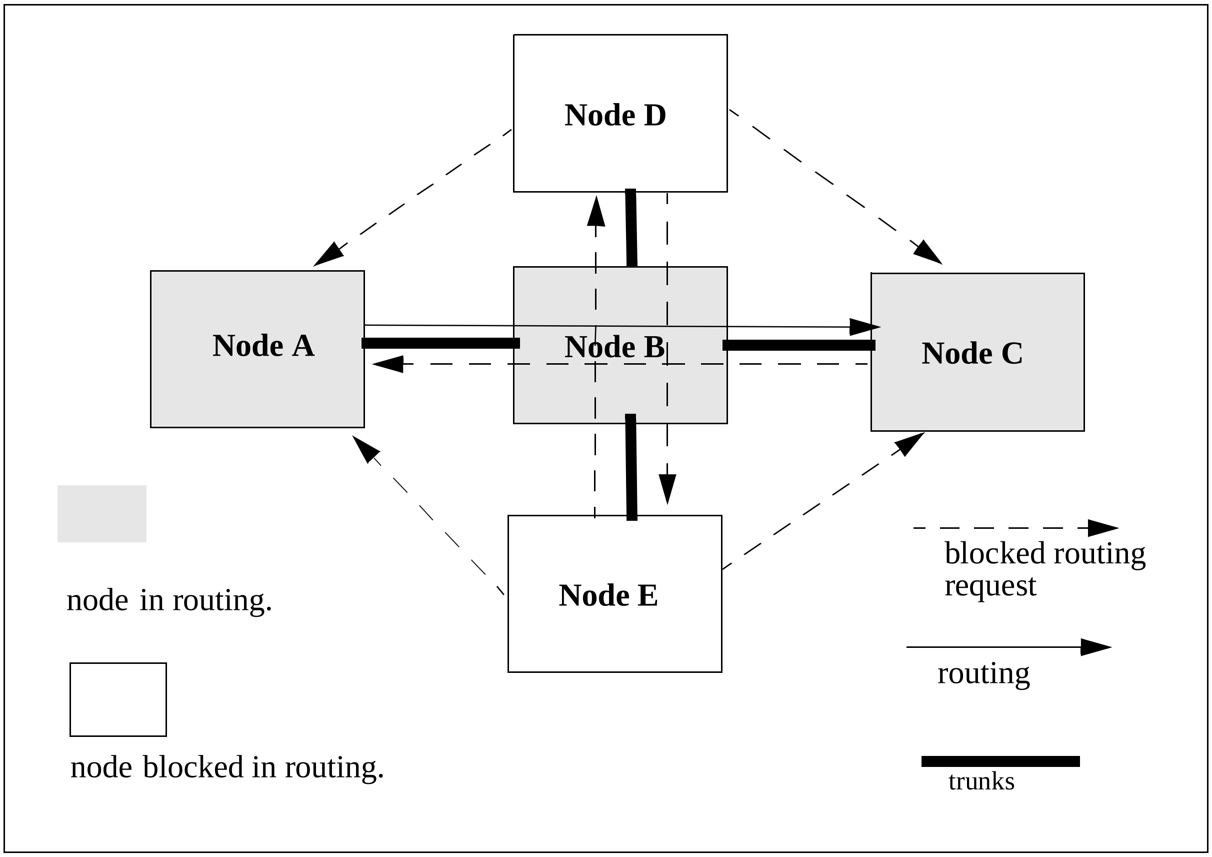
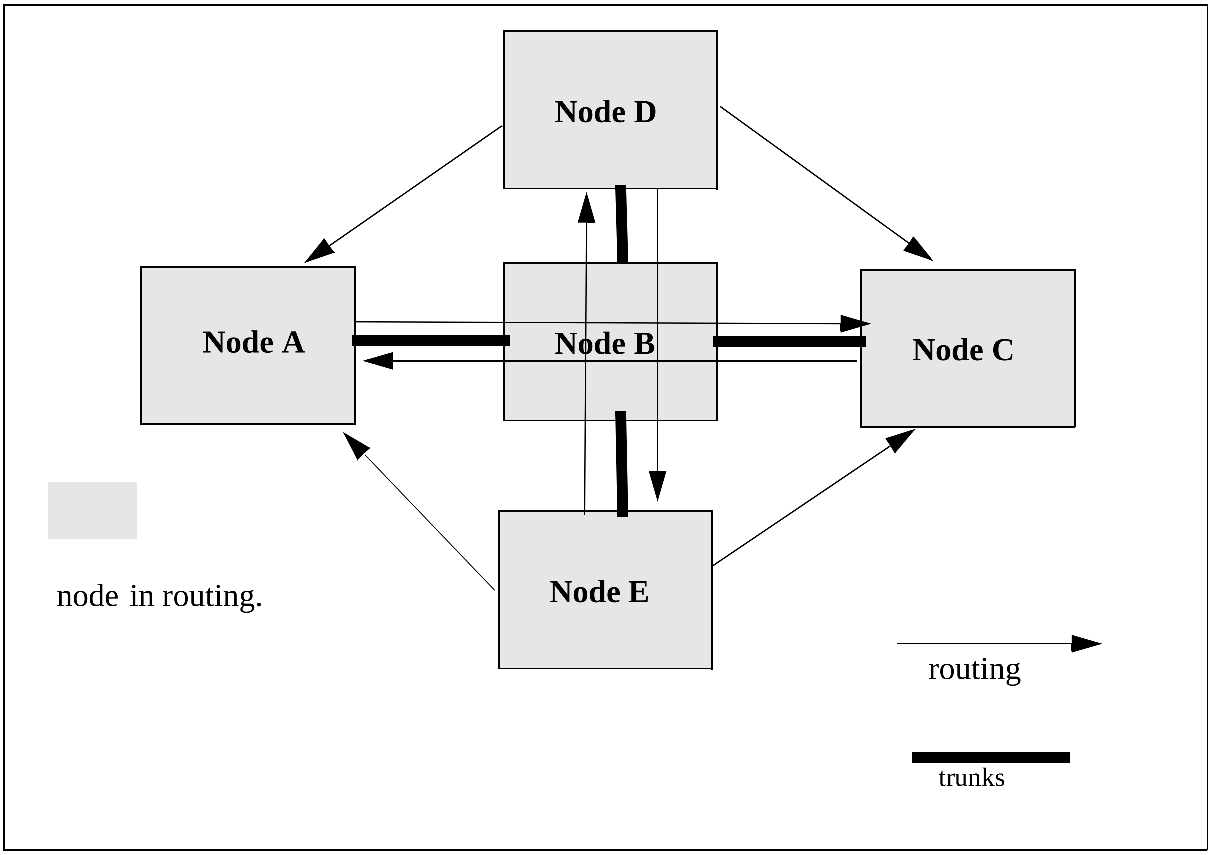


Figure 1-10 Concurrent Routing



Performance improvement will not be realized for individual or topologically disjoint reroutes. The key performance metric that will be improved by CR is network settling time. Network settling time is defined by the longest settling time for any single node, assuming all of the nodes start routing at the same time. The number of nodes and connections in the network, network topology and other configurable routing parameters all effect network settling time.

Features

The CR Feature provides the following functions:

- Allows a node to initiate multiple simultaneous route requests.
- Allows multiple route requests to be accepted and serviced by a node without blocking.
- Allows the degree of route concurrency to be configurable on a node-by-node basis, allowing the user to tailor the application of the CR enhancement to a specific network topology.
- Implements a CPU throttling mechanism, wherein route concurrency is limited if CPU usage becomes too high.
- New statistics on CPU-based route throttling.
- A mechanism for automatically measuring nodal settling time and maintaining a history of settling time measurements.

Benefits

- CR reduces network settling time.
- CR increases network traffic flow per unit of time.
- CR increases network availability.

Note The extent to which CR reduces network settling time will vary with network topology, traffic conditions and the number of CR enabled nodes in the network.

Restrictions

Network Upgrade to SWSW Release 9.3.30

CR cannot be enabled until all of the nodes in a network have been upgraded to SWSW release 9.3.30. Once all of the nodes in a network have been upgraded to SWSW release 9.3.30, CR can be enabled on any node in that network. It is not necessary for CR to be enabled on every node in a network for CR to take place on those nodes that are CR enabled.

Concurrency Limit

The maximum number of concurrent routes that can be configured on a node is 8. Allowing more than 8 concurrent routes would have diminishing returns, because processor utilization would become excessive. A node will continue to master new route requests (provided route candidates exist), or serve as a via or slave for new routes, unless doing so would exceed the route concurrency level that is configured on the node.

CPU Throttling

CR has the potential to dramatically reduce CPU idle time. To preserve enough CPU time for users to interact effectively with a node, even during periods of extensive rerouting, a mechanism has been implemented to limit (throttle) route concurrency. When CPU utilization exceeds a defined threshold (throttle level), new route activity is temporarily suspended to preserve node responsiveness. Throttling continues until CPU utilization drops below a second threshold (resume level), which is less than or equal to the throttle level. Allowing the resume level to be less than the throttle level provides for a hysteresis mechanism to avoid oscillation around the throttling point. The default CPU throttling values for master, via and slave routes are set at 80% of CPU capacity for throttling and 60% of CPU capacity to resume new route activity. Separate throttle and resume points can be set for master, via, and slave routes to allow tailoring of route behavior, however, these settings can only be changed with Cisco-level commands.

Path Blocking

If a node masters two or more routes that share the same via and slave nodes, these routes will have overlaping paths. Due to messaging protocol limitations, a node is only able to master concurrent routes that do not have overlaping paths. The Path Blocking algorithm checks each master route candidate that a node might initiate to see if it overlaps with another active route mastered by that node. If there will be any overlaping, the candidate is rejected and candidate selection continues. Path Blocking is node specific, but the degree to which it will limit concurrent master routes on a node is a function of network topology. If a node is only serving as a via and/or a slave, it cannot be path blocked.

Priority Bumping

Priority Bumping (PB) is a computationally-intensive process which allows switch connections classified as more important (based on CoS value) to “bump” connections of lesser importance. CR may be restricted if the PB feature is enabled on a network. Both PB and CR are processor intensive. To avoid excessive processor utilization, no new route requests will be initiated or accepted on the nodes an active PB route traverses, until it has completed.

Blocking By Nodes That Are Not CR Enabled

The CR feature does not alter the AutoRoute messaging protocol. AutoRouting is enabled by default on nodes that are not CR enabled. When Auto Routing is enabled on a node a backoff mechanism may be triggered to prevent excessive collisions. When the backoff mechanism is triggered the node will be temporarily unavaliable as a candidate for CR. This mechanism is conceptually similar to the Path Blocking algorithm described above.

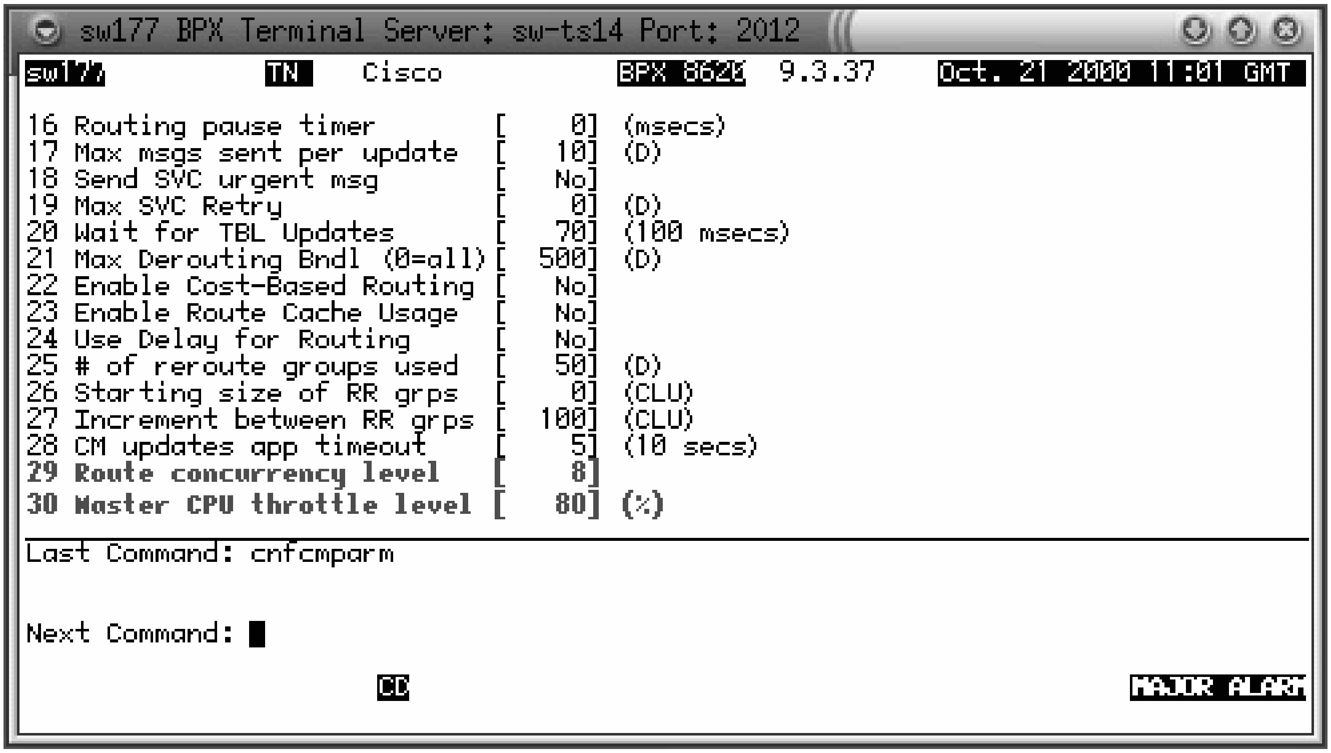
Configuration

Once all of the nodes on a network have been upgraded to Release 9.3.30, CR can be enabled on any node by using the **cnfcmparm** command to set the route concurrency level to an integer value greater than 1 but no greater than 8. Once CR has been enabled on a node, it operates automatically. CR can be turned off on a node by specifying a concurrency level of 1. See table 1-1 and example 1-1 below.

Table 1-1

CLI command	Parameter	Description
cnfcmparm	Routing concurrency level	This is a nodal parameter. It specifies the amount total number of routes that can be simultaneously in progress on the node.

Example 1-1



```
sw177 BPX Terminal Server: sw-ts14 Port: 2012
sw177          TN    Cisco          BPX 8620  9.3.37    Oct. 21 2000 11:01 GMT

16 Routing pause timer        [     0] (msecs)
17 Max msgs sent per update   [    10] (D)
18 Send SVC urgent msg        [    No]
19 Max SVC Retry              [     0] (D)
20 Wait for TBL Updates       [    70] (100 msecs)
21 Max Derouting Bndl  (0=all)[   500] (D)
22 Enable Cost-Based Routing  [    No]
23 Enable Route Cache Usage   [    No]
24 Use Delay for Routing      [    No]
25 # of reroute groups used   [    50] (D)
26 Starting size of RR grps   [     0] (CLU)
27 Increment between RR grps  [   100] (CLU)
28 CM updates app timeout     [     5] (10 secs)
29 Route concurrency level    [     8]
30 Master CPU throttle level  [    80] (%)

Last Command: cnfcmparm


Next Command:

                      CD                                          MAJOR ALARM
```

Routing Statistics

The **dsprrst** command continues to be used to display routing statistics in SWSW release 9.3.30, however, when CR is enabled, the semantics of some statististics are altered slightly.

Three new statistics have been added to the display to show the number of times CPU throttling/resumption has occurred for master, via, and slave routes, respectively. These statistics will be shown on the first page of reroute statistics as shown in the example below.

Note that the CR performance gain is not reflected in the basic **dsprrst** display. The basic statistics show the CPU real-time performance, whereas CR enhances routing concurrency in the network. To correct this deficiency, a new option to the **dsprrst** command is added to display nodal settling time measurements. A settling time measurement is initiated whenever candidate selection successfully locates a candidate for routing. The settling time measurement ends when candidate selection fails to find a candidate to route and no routes are currently active. In addition to the start and end time of the measurement, the following statistics are kept:

- Number of route bundles routed during measurement
- Number of connections routed during measurement
- Total real-time spent on all successful routing threads

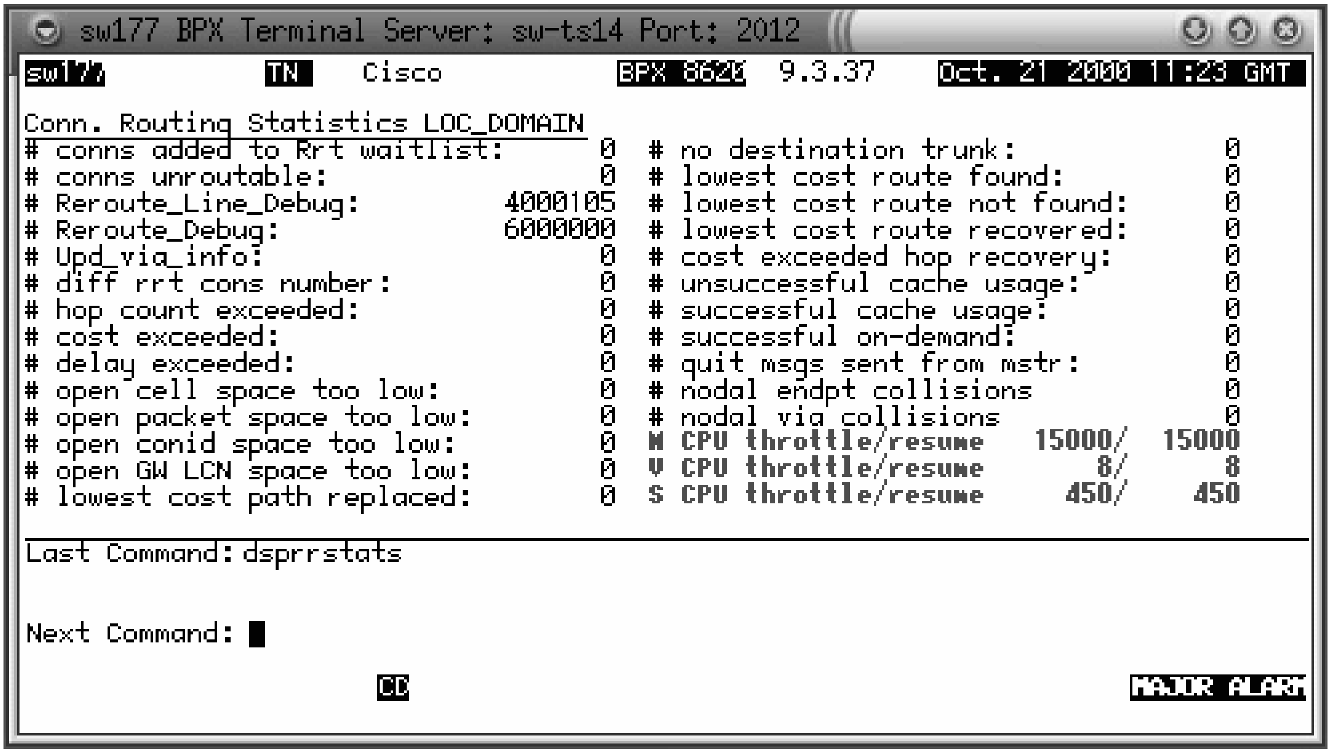
These statistics allow the following quantities to be derived:

- Average bundle size during measurement

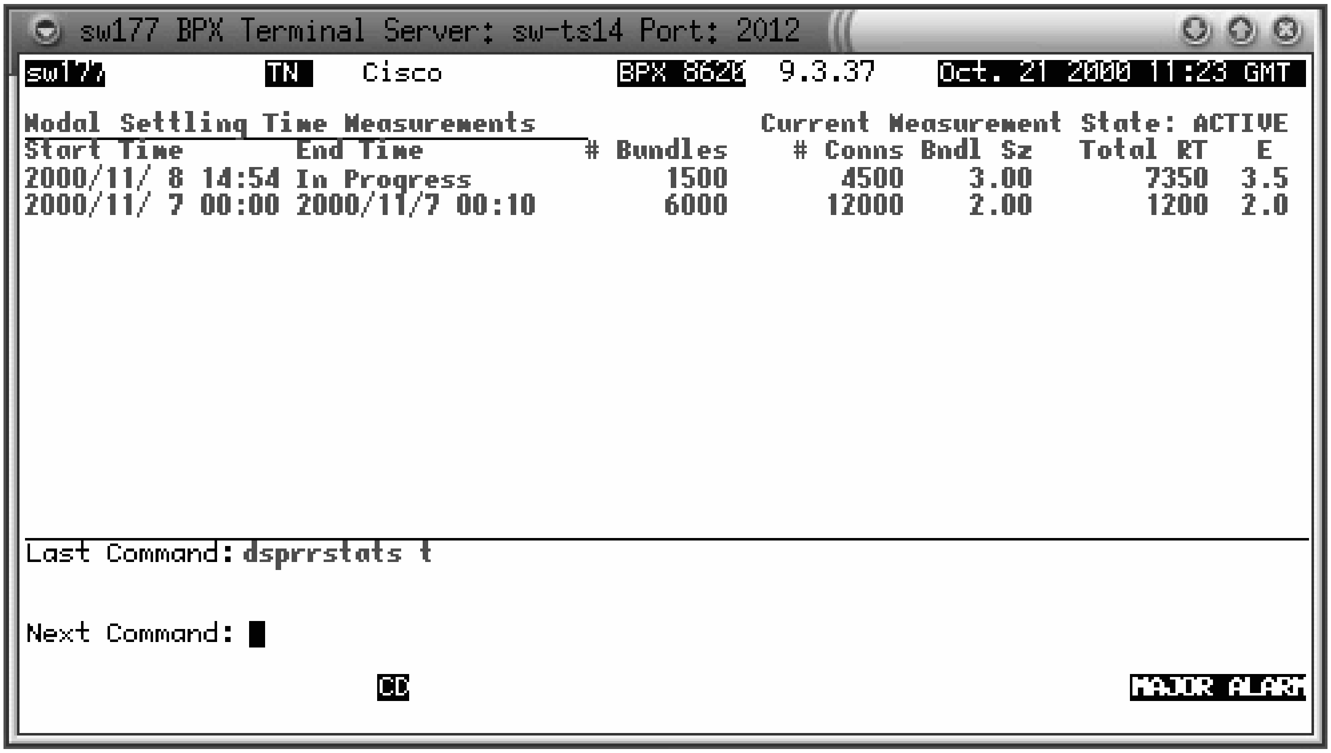
- Effective concurrency, defined as:

$$\varepsilon = \frac{\text{total realtime spent processing routing threads}}{\text{node settling time}}$$

At any time, the last 10 settling time measurements (including the active measurement, if any) are displayed using the new option. Nodal settling time history is cleared whenever reroute statistics are cleared. This new screen is shown in the second example, below.



```
sw177          TN    Cisco          BPX 8620  9.3.37     Oct. 21 2000 11:23 GMT

Conn. Routing Statistics LOC_DOMAIN
# conns added to Rrt waitlist:          0  # no destination trunk:            0
# conns unroutable:                     0  # lowest cost route found:         0
# Reroute_Line_Debug:             4000105  # lowest cost route not found:     0
# Reroute_Debug:                  6000000  # lowest cost route recovered:     0
# Upd_via_info:                         0  # cost exceeded hop recovery:      0
# diff rrt cons number:                 0  # unsuccessful cache usage:        0
# hop count exceeded:                   0  # successful cache usage:          0
# cost exceeded:                        0  # successful on-demand:            0
# delay exceeded:                       0  # quit msgs sent from mstr:        0
# open cell space too low:              0  # nodal endpt collisions           0
# open packet space too low:            0  # nodal via collisions             0
# open conid space too low:             0  W CPU throttle/resume    15000/  15000
# open GW LCN space too low:            0  V CPU throttle/resume        8/      8
# lowest cost path replaced:            0  S CPU throttle/resume      450/    450

Last Command: dsprrstats


Next Command:

                         CD                                         MAJOR ALARM
```



```
sw177          TN    Cisco          BPX 8620  9.3.37    Oct. 21 2000 11:23 GMT

Modal Settling Time Measurements               Current Measurement State: ACTIVE
Start Time       End Time          # Bundles     # Conns Bndl Sz   Total RT   E
2000/11/ 8 14:54 In Progress            1500        4500    3.00       7350  3.5
2000/11/ 7 00:00 2000/11/7 00:10        6000       12000    2.00       1200  2.0











Last Command: dsprrstats t


Next Command:

                          CD                                         MAJOR ALARM
```

Abr Standard with VSVD Congestion Control

The BPX/IGX switch networks provide a choice of two dynamic rate based congestion control methods, Abr with VSVD and Optimized Bandwidth Management (ForeSight). This section describes Standard Abr with VSVD.

Note Abr with VSVD is an optional feature that must be purchased and enabled on a single node for the entire network.

When an ATM connection is configured between BXM cards for Standard Abr with VSVD per ATM Forum TM 4.0, Resource Management (RM) cells are used to carry congestion control feedback information back to the connection's source from the connection's destination.

The Abr sources periodically interleave RM cells into the data they are transmitting. These RM cells are called forward RM cells because they travel in the same direction as the data. At the destination these cells are turned around and sent back to the source as backward RM cells.

The RM cells contain fields to increase or decrease the rate (the CI and NI fields) or set it at a particular value (the explicit rate ER field). The intervening switches may adjust these fields according to network conditions. When the source receives an RM cell, it must adjust its rate in response to the setting of these fields.

When spare capacity exists with the network, Abr with VSVD permits the extra bandwidth to be allocated to active virtual circuits.

Optimized Bandwidth Management (ForeSight) Congestion Control

The BPX/IGX switch networks provide a choice of two dynamic rate-based congestion control methods, Abr with VSVD and Cisco's Optimized Bandwidth Management (ForeSight). This section describes Optimized Bandwidth Management (ForeSight).

Note Optimized Bandwidth Management (ForeSight) is an optional feature that must be purchased and enabled on a single node for the entire network.

Optimized Bandwidth Management (ForeSight) may be used for congestion control across BPX/IGX switches for connections that have one or both endpoints terminating on cards other than BXM. The ForeSight feature is a dynamic closed-loop, rate-based congestion management feature that yields bandwidth savings compared to non-ForeSight equipped trunks when transmitting bursty data across cell-based networks.

ForeSight permits users to burst above their committed information rate for extended periods of time when there is unused network bandwidth available. This enables users to maximize the use of network bandwidth while offering superior congestion avoidance by actively monitoring the state of shared trunks carrying Frame Relay traffic within the network.

ForeSight monitors each path in the forward direction to detect any point where congestion may occur and returns the information back to the entry to the network. When spare capacity exists with the network, ForeSight permits the extra bandwidth to be allocated to active virtual circuits. Each PVC is treated fairly by allocating the extra bandwidth based on each PVC's committed bandwidth parameter.

If the network reaches full utilization, ForeSight detects this and quickly acts to reduce the extra bandwidth allocated to the active PVCs. ForeSight reacts quickly to network loading in order to prevent dropped packets. Periodically, each node automatically measures the delay experienced along a Frame Relay PVC. This delay factor is used in calculating the ForeSight algorithm.

With basic Frame Relay service, only a single rate parameter can be specified for each PVC. With ForeSight, the virtual circuit rate can be specified based on a minimum, maximum, and initial transmission rate for more flexibility in defining the Frame Relay circuits.

ForeSight provides effective congestion management for PVC's traversing broadband ATM as well. ForeSight operates at the cell-relay level that lies below the Frame Relay services provided by the IGX switch. With the queue sizes utilized in the BPX switch, the bandwidth savings is approximately the same as experienced with lower speed trunks. When the cost of these lines is considered, the savings offered by ForeSight can be significant.

Network Management

BPX switches provide one high-speed and two low-speed data interfaces for data collection and network management:

- **High-speed interface**
  An Ethernet 802.3 LAN interface port is provided for communicating with a Cisco WAN Manager NMS workstation. TCP/IP provides the transport and network layer, Logical Link Control 1 is the protocol across the Ethernet port.
- **Low-speed interfaces**
  Two RS-232 ports are provided: one for a network printer and the second for either a modem connection or a connection to an external control terminal. These low-speed interfaces are the same as provided by the IGX switch.

Each BPX switch can be configured to use optional low-speed modems for inward access by the Cisco Technical Response Team for network troubleshooting assistance or to autodial Customer Service to report alarms remotely. If desired, another option is remote monitoring or control of customer premise equipment through a window on the Cisco WAN Manager workstation.

A Cisco WAN Manager NMS workstation connects via the Ethernet to the LAN port on the BPX and provides network management via SNMP. Statistics are collected by Cisco WAN Manager using the TFTP protocol.

You can also use the Cisco WAN Manager's Connection Manager to manage:

- Frame Relay connections on IGX switch shelves
- Frame Relay and ATM connections on MGX 8220 shelves
- MGX 8220 shelf configuration.

Network Management software includes these applications:

- Cisco WAN Manager (formerly StrataView Plus)
  A single unified management platform utilizing HP OpenView® to manage BPX, IGX, and SES devices.
- StrataSphere BILLder
  Monitors traffic flow over a network and captures data per standard or customized billing periods and formats.
- StrataSphere Modeler
  Network modeling tool used for preliminary design of new networks and for analysis and modification studies of existing networks.
- StrataSphere Adaptor
  Exports network modeling information to external third-party modeling systems.
- SNMP Service Agent
  A service agent that provides an interface for automated provisioning and fault management to customers or Operations Support Systems (OSS).

For further information on network management, refer to the *Cisco WAN Manager Operations* publication.

Cisco WAN Manager

Cisco WAN Manager is a single unified management platform utilizing HP OpenView® to manage BPX, IGX, and SES devices. It provides a standards-based multiprotocol management architecture. Regardless of the size or configuration of your network, Cisco WAN Manager collects extensive service statistics, tracks resource performance, and provides powerful remote diagnostic and control functions for WAN maintenance.

Online help screens, graphical displays, and easy command line mnemonics make Cisco WAN Manager user-friendly. Plentiful hard disk storage is provided to allow accumulating time of day statistics on many network parameters simultaneously. The data is accumulated by the node's controller card and transmitted to the Cisco WAN Manager workstation where it is stored, processed, and displayed on a large color monitor.

Cisco WAN Manager connects to the network over an Ethernet LAN connection. With Ethernet, you can establish Cisco WAN Manager connectivity to remote nodes via Frame Relay over TCP/IP to the LAN connector on the local node, or via in-band ILMI.

Cisco WAN Manager provides in-band management of network elements via SNMP agent interfaces and MIBs embedded in each node and interface shelf. The SNMP agent allows a user to manage a StrataCom network or sub-network from any SNMP-based integrated network management system (INMS).

- Connection Management
  The Cisco WAN Manager Connection Manager enables you to perform connection provisioning such as adding, configuring, and deleting Frame Relay, ATM, and Frame Relay-to-ATM interworking connections.
- Network Topology
  A map of the network is generated at system installation to graphically display all nodes, trunks, circuit lines, and access devices in the network. Various colors are used to indicate the status of each network item. You can zoom in to display specific network details while a small overview map remains displayed as a locator. The Network Topology can also display other connected ATM devices that support the ILMI 4.0 Neighbor Discovery procedure.
- Network Performance
  Statistics are collected and temporarily stored by each node in the network and released to Cisco WAN Manager when you enable polling, and in accordance with your configuration for specific information within reports. Cisco WAN Manager then stores statistics in a relational database; you retrieve and view these statistics by invoking a statistics display window from the Cisco WAN Manager GUI. From data gathered throughout the network, you can quickly view the operational integrity and deployment of installed network devices and communication media by activating and invoking statistics displays.
- Equipment Management
  The Cisco WAN Manager Equipment Manager provides the ability to perform equipment management functions such as adding lines and ports on a Cisco MGX 8220 edge concentrator shelf.
- Alarm Reporting/Event Log
  Cisco WAN Manager displays major and minor alarm status on its topology screen for all nodes in a network. It also provides an event log with configurable filtering of the log events by node name, start time, end time, alarm type, and user-specified search string.
- Software Updates
  System software and software updates are supplied on magnetic tape or floppy disk. You can then load the system software files onto the Cisco WAN Manager workstation where they can be downloaded to a buffer memory in each node in the network in a background mode without disturbing network operation. When the loading is complete for all nodes, you issue a command to switch all nodes over to the new software. The previous software is preserved and can be recalled at any time.
- Backup
  You can obtain all network configuration files from the network and store them on the Cisco WAN Manager workstation for backup purposes. In the event of a system update or a node failure, you can download the configuration files to one or all nodes for immediate system restoration.

Network Interfaces

Network interfaces connect the BPX switch to other BPX or IGX switches to form a wide-area network. The BPX switch provides these trunk interfaces:

- T3
- E3

- OC-3/STM-1
- OC-12/STM-4

The T3 physical interface utilizes DS3 C-bit parity and the 53-byte ATM physical layer cell relay transmission using the Physical Layer Convergence Protocol.

The E3 physical interface uses G.804 for cell delineation and HDB3 line coding.

The BXM-622 cards support these physical interfaces:

- SMF
- SMFLR

The BPX switch supports network interfaces up to 622 Mbps and provides the architecture to support higher broadband network interfaces as the need arises.

Optional redundancy is on a one-to-one basis. The physical interface can operate either in a normal or looped clock mode. As an option, the node synchronization can be obtained from the DS3 extracted clock for any selected network trunk.

Service Interfaces

Service interfaces connect ATM customer equipment to the BPX switch. ATM User-to-Network Interfaces (UNI) and ATM Network-to-Network Interfaces (NNI) terminate on the ATM Service Interface (ASI) cards and on BXM T3/E3, OC-3, and OC-12 cards configured for as service interfaces (UNI access mode).

The BXM T3/E3 card supports the standard T3/E3 interfaces.

The BXM-155 cards support SMF, SMFLR, and MMF physical interfaces.

The BXM-622 cards support SMF and SMFLR physical interfaces.

The BXM cards support cell relay connections that are compliant with both the physical layer and ATM layer standards.

The MGX 8220 interfaces to a BNI or BXM card on the BPX, via a T3, E3, or OC-3 interface. The MGX 8220 provides a concentrator for T1 or E1 Frame Relay and ATM connections to the BPX switch with the ability to apply Optimized Bandwidth Management (ForeSight) across a connection from end-to-end. The MGX 8220 also supports CES and FUNI (Frame-based UNI over ATM) connections.

Statistical Alarms and Network Statistics

The BPX Switch system manager can configure alarm thresholds for all statistical type error conditions. Thresholds are configurable for conditions such as frame errors, out of frame, bipolar errors, dropped cells, and cell header errors. When an alarm threshold is exceeded, the NMS screen displays an alarm message.

Graphical displays of collected statistics information, a feature of the Cisco WAN Manager NMS, are a useful tool for monitoring network usage. Statistics collected on network operation fall into four general categories:

- Node statistics
- Network trunk statistics
- Network Service, line statistics
- Network Service, port statistics

These statistics are collected in real-time throughout the network and forwarded to the WAN Manager workstation for logging and display. The link from the node to the Cisco WAN Manager workstation uses a protocol to acknowledge receipt of each statistics data packet.

Refer to the *Cisco WAN Manager Operations publication*, for more details on statistics and statistical alarms.

Node Synchronization

A BPX service switch network provides network-wide, intelligent clock synchronization. It uses a fault-tolerant network synchronization architecture recommended for Integrated Services Digital Network (ISDN). The BPX switch internal clock operates as a Stratum 3 clock per ANSI T1.101.

Because the BPX switch is designed to be part of a larger communications network, it is capable of synchronizing to higher-level network clocks as well as providing synchronization to lower-level devices. You can configure any network access input to synchronize the node. Any external T1 or E1 input can also be configured to synchronize network timing.

A clock output allows synchronizing an adjacent IGX switch or other network device to the BPX switch and the network. In nodes equipped with optional redundancy, the standby hardware is locked to the active hardware to minimize system disruption during system switchovers.

You can configure the BPX Service Node to select clock from these sources:

- External (T1/E1)
- Line (DS3/E3)
- Internal

Switch Software Description

The Cisco WAN switching cell relay system software shares most core system software, as well as a library of applications, between platforms. System software provides basic management and control capabilities to each node.

BPX node system software manages its own configuration, fault-isolation, failure recovery, and other resources. Because no remote resources are involved, this ensures rapid response to local problems. This distributed network control, rather than centralized control, provides increased reliability.

Software among multiple nodes cooperates to perform network-wide functions such as trunk and connection management. This multiprocessor approach ensures rapid response with no single point of failure. System software applications provide advanced features that you can install and configure as required.

Some of the many software features are:

- Automatic routing of connections (Automatic Routing Management feature).
- Various Classes of Service that may be assigned to each connection type (Advanced CoS Management).
- Bandwidth reservation on a time-of-day basis.
- Detection and control of network congestion with Abr with VSVD or Optimized Bandwidth Management (ForeSight) algorithms.
- Automatic self-testing of each component of the node.

- Automatic collecting and reporting of many network-wide statistics, such as trunk loading, connection usage, and trunk error rates, as you specify.

The system software, configuration database, and the firmware that controls the operation of each card type is resident in programmable memory and can be stored off-line in the Cisco WAN Manager NMS for immediate backup if necessary. This software and firmware is easily updated remotely from a central site or from Customer Service, which reduces the likelihood of early obsolescence.

Connections and Connection Routing

The routing software supports the establishment, removal and rerouting of end-to-end channel connections. There are three routing modes:

- Automatic Routing
  The system software computes the best route for a connection.
- Manual Routing
  You can specify the route for a connection.
- Alternate Routing
  The system software automatically reroutes a failed connection.

The system software uses these criteria when it establishes an automatic route for a connection:

- Selects the most direct route between two nodes.
- Selects unloaded lines that can handle the increased traffic of additional connections.
- Takes into consideration user-configured connection restrictions (for example whether or not the connection is restricted to terrestrial lines or can include satellite hops or routes configured for route diversity).

When a node reroutes a connection, it uses these criteria and also looks at the priority that has been assigned and any user-configured routing restrictions. The node analyzes trunk loading to determine the number of cells or packets the network can successfully deliver. Within these loading limits, the node can calculate the maximum combination allowed on a network trunk of each type of connection: synchronous data, ATM traffic, Frame Relay data, multimedia data, voice, and compressed voice.

Network-wide T3, E3, OC-3, or OC-12 connections are supported between BPX switches terminating ATM user devices on the BPX switch UNI ports. These connections are routed using the virtual path and/or virtual circuit addressing fields in the ATM cell header.

Narrowband connections can be routed over high-speed ATM backbone networks built on BPX broadband switches. FastPacket addresses are translated into ATM cell addresses that are then used to route the connections between BPX switches, and to ATM networks with mixed vendor ATM switches. Routing algorithms select broadband links only, avoiding narrowband nodes that could create a choke point.

Connection Routing Groups

The rerouting mechanism ensures that connections are presorted in order of cell loading when they are added. Each routing group contains connections with loading in a particular range. The group containing the connections with the largest cell loadings is rerouted first, and subsequent groups are then rerouted on down to the last group that contains connections with the smallest cell loadings.

There are three configurable parameters for configuring the rerouting groups:

- Total number of rerouting groups

- Starting load size of first group
- Load size range of each group

You configure the three routing group parameters by using the **cnfcmparm** command.

For example, there might be 10 groups, with the starting load size of the first group at 50, and the incremental load size of each succeeding group being 10 cells. Then group 0 would contain all connections requiring 0–59 cell load units, group 1 would contain all connections requiring from 60–69 cell load units, on up through group 9 which would contain all connections requiring 140 or more cell load units.

Table 1-2 Routing Group Configuration Example

Routing Group	Connection Cell Loading
0	0–59
1	60–69
2	70–79
3	80–89
4	90–99
5	101–109
6	110–119
7	120–129
8	130–139
9	140 and up

Cost-Based Connection Routing

In standard AutoRoute, the path with the fewest number of hops to the destination node is chosen as the best route. Cost-based route selection uses an administrative trunk cost routing metric. The path with the lowest total trunk cost is chosen as the best route.

Cost-based route selection is based on Dijkstra’s Shortest Path Algorithm, which is widely used in network routing environments. You can use cost-based route selection (that is, cost-based AutoRoute) to give preference to slower privately owned trunks over faster public trunks that charge based on usage time. This gives network operators more control over the usability of their network trunks, while providing a more standard algorithm for route selection.

Major Features of Cost-Based AutoRoute

Here is a short description of the major functional elements of Cost-Based Route Selection.

- **Enabling Cost-Based Route Selection.**
  You enable cost-based route selection at any time. This feature does not require special password access. The default algorithm is the hop-based algorithm.
- **Configuring Trunk Cost**
  You assign a trunk cost to each trunk (physical and virtual) in the network. One cost is assigned per trunk; no separate costs are used for different connection or service types. The valid range of trunk costs is 1 (lowest cost) to 50 (highest cost). A trunk has a default cost of 10 upon activation. The cost of a trunk can be changed before or after the trunk has been added to the network topology.

The cost can also be changed after connections have been routed over the trunk. Such a change does not initiate automatic connection rerouting, nor does it cause any outage to the routed connections. If the new trunk cost causes the allowable route cost for any connections to be exceeded, the connections must be manually rerouted to avoid the trunk. This avoids large-scale simultaneous network-wide rerouting and gives you control over the connection reroute outage.

- **Cache vs. On-Demand Routing**
  In previous releases, Hop-Based Route Selection always requires on-demand routing. On-demand routing initiates an end-to-end route search for every connection. Due to the computation time required for Dijkstra's algorithm in cost-based route selection, a route cache is used to reduce the need for on-demand routing.

  This cache contains lowest cost routes as they are selected. Subsequent routing cycles use these existing routes if the routing criteria are met. Otherwise on-demand routing is initiated. This caching greatly benefits environments where routing criteria is very similar among connections.

  Enabling cost-based route selection automatically enables cache usage. Enabling Hop-Based Route Selection automatically disables cache usage. Cache usage can also be independently enabled or disabled for both types of route selection.
- **On-Demand Lowest Cost Route Determination**
  On-demand routing chooses the current lowest cost route to the destination node. This lowest cost route is bounded by the maximum route length of 10 hops. If more than one route of similar cost and distance is available, the route with most available resources is chosen. No route grooming occurs after the initial routing. A connection does not automatically reroute if its route cost changes over time. A connection also does not automatically reroute if a lower cost route becomes available after the initial routing. However, a forced reroute or a preferred route can be used to move the connection to a lower cost route.
- **Delay-Sensitive Routes**
  Delay-sensitive IGX connection types (Voice and Non-Timestamped Data) may be configured to use the worst case queueing delay per trunk, rather than the configured trunk cost, in the lowest-cost route determination. The trunk delay acts as the cost attribute in the Dijkstra algorithm. The default mode for the delay sensitive connections is to use the trunk cost. All other connection types always use the trunk cost in the route determination.

  AutoRoute does not use the worst case end-to-end queueing delay in route selection for delay sensitive BPX connection types (ATM Cbr). Cost-based route selection does not change this.
- **Cost Cap**
  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). You can change the cost cap 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 you more control over the connection reroute outage.
- **Hop-Based Route Selection**
  Since Release 9.0, AutoRoute uses Hop-Based Route Selection. The cost of all trunks is set to the default cost (10). The cost cap of all connections is set to the maximum allowable cost (100). All other new cost-based routing parameters are set to regular default values.

- **AutoRoute Interoperability**
  Because AutoRoute is source-based, nodes can interoperate using different route selection algorithms. The originating node computes the full end-to-end route based on its own knowledge of the network topology. The route is then passed to the subsequent nodes on the route. This source routing allows a mix of Cost-Based and Hop-Based Route Selection to run in a network.

Cost-Based AutoRoute Commands

You use these switch software Command Line Interface (CLI) commands for cost-based route selection:

- **cnfcmparm**
  Enables cost-based route selection. This is a SuperUser command to configure all AutoRoute parameters. By default cost-based route selection is disabled. Enabling or disabling cost-based route selection can be done at any time. Each connection routing cycle uses whichever algorithm is enabled when the cycle begins. The configuration is node-based, not network-based, which allows each node to have its own route selection algorithm.

  Enabling cost-based route selection automatically enables cache usage. Disabling cost-based route selection automatically disables cache usage. Cache usage may also be independently enabled or disabled.
- **cnftrk**
  Configures the administrative cost for a trunk. Both physical and virtual trunks have the cost attribute. Each trunk has a cost ranging from 1 (lowest) to 50 (highest). The default cost is 10 upon trunk activation.

  The cost can be configured from either end of the trunk. The cost can be changed before or after the trunk has been added to the network. The cost can also be changed 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. This knowledge is required for successful source-based routing.
- **cnfrtcost**
  Configures the cost cap for a connection. This command is valid only at the node where the connection is added.
- **cnfsysparm**
  Configures the delay cost cap for all delay sensitive connections in the network.
- **dspcon**
  Displays the maximum and current costs for a connection route.
- **dspload**
  Displays the administrative cost and queue delay for a network trunk.
- **dsprts**
  Displays the current costs for all connection routes.
- **dsptrkcnf**
  Displays the configured cost of a trunk.

The *Cisco WAN Switching Command Reference* contains detailed information about the use of BPX switch commands.

Network Synchronization

Cisco WAN switching cell relay networks use a fault-tolerant network synchronization method of the type recommended for Integrated Services Digital Network (ISDN). You can select any circuit line, trunk, or an external clock input to provide a primary network clock. Any line can be configured as a secondary clock source in the event that the primary clock source fails.

All nodes are equipped with a redundant, high-stability internal oscillator that meets Stratum 3 (BPX) or Stratum 4 requirements. Each node keeps a map of the network's clocking hierarchy. The network clock source is automatically switched in the event of failure of a clock source.

There is less likelihood of a loss of data resulting from re-frames that occur during a clock switchover or other momentary disruption of network clocking with cell-based networks than there is with traditional TDM networks. Data is held in buffers and packets are not sent until a trunk has regained frame synchronism to prevent loss of data.

Virtual Trunk Clock Source Synchronization

The increasing use of Virtual Trunks in Wide Area Networks has led to the development of the Virtual Trunk Clock Source Synchronization feature (VTCSS) in SWSW release 9.3.30. VTCSS operates transparently making network synchronization to a single ATM service provider clock source possible.(1)

When a virtual trunk port (VTP) is configured as a network clock source in pre-9.3.30 SWSW releases, the first virtual trunk (VT) interfaced on that VTP becomes the clock source by default. If the first VT fails, the clock source is automatically switched to the next available clock source (2) exclusive of the VTP that the failed VT was interfaced with.

With the VTCSS feature, if the first VT on a clock configured VTP fails, the clock source is switched to the next VT interfaced on that VTP. If the second VT fails the clock source is switched to the next VT interfaced on the same VTP and so on. As a result, the clock source remains associated with the physical interface (clock configured VTP) as long as there are one or more active VTs interfaced on it.(3)

The VTCSS feature is here is no configuration

1. May not allow all nodes in the network to synch. to the same clock source...may just allow a network to achieve a higher degree of clock synchronization than was previously possible.

2.As defined by the network system software.

3. If one VT on a VTP is configured: pass synch = yes, that VTP can’t be a clock source in the first place. Do I need to mention that in the scope of this doc?

4. Do I need to mention the debug on/off flag, or is this beyond the scope of the BPX Installation & Configuration Guide?

as the clock source., even though the physical interface of the Virtual interface is active and there are other active VT’s available to switch to.

In Wide Area Networks, the clock synchronization from a public ATM service provider helps to have glitch free, data transfer between the IGX/BPX and the service provider, if we can derive the clock out of the VT's successfully. Therefore if the physical interface can derive the clock from the ATM cloud, irrespective of any Virtual Interface failures, the nodes in a network can achieve a higher degree of clock synchronization.

This feature enables the association of the Virtual trunk clock source with the physical interface and therefore enables the use of Virtual Trunks as clock sources for all of the virtual interfaces available on the trunk port.

This project is aimed at associating the network clock source with the physical interface, rather than the virtual interface, since the physical interface is the one which drives/derives the clock. Therefore, if a VT fails, the clock source should not be switched to another physical interface or internal clock source, if there is another healthy (clock configurable) active interface up and running. This implies that if at least one virtual trunk interface is up without any failure, the physical interface will still be a sustainable clock source. So irrespective of the virtual trunk failure, the clock source should always be associated with the physical interface port, where the virtual trunk is activated.

Background and Justification

The requirement of supporting the Virtual Trunk clocking, arises from the marketing requirement of network synchronization using a single clock source of public ATM service provider, irrespective of single VT failures in a multiple VT scenario. The present switch software implementation associates the VT clock source with the first logical trunk interface (VI), and therefore a failure of the first VT interface, will cause a switching of the clock source to the next available interface. This project is aimed at allowing the network clock source to be always associated with the physical interface, since the physical interface is the one which drives/derives the clock.

Configuration

The clock synchronization from a public ATM service provider helps to have a glitch free, data transfer between the IGX/BPX and the service provider, if we can derive the clock out of the VT's successfully. Therefore, if the physical interface can derive the clock from the ATM cloud, irrespective of the Virtual Interface failures, the nodes in a network can achieve a higher degree of clock synchronization. There is no special configuration required with the addition of this feature

Overview

The VT clock source synchronization will allow the network to synchronize and provide stable clocking for all nodes throughout the attached nodes in the cloud.

The summary of functions which will be implemented in Release 9.3 for the support of enhanced VT clocking includes:

1. When a VT port is configured for clock source, the first virtual trunk interface on the trunk port will be internally marked as the clock source. Unlike the current implementation, if the first interface on the trunk port fails, or becomes unusable as clock source, the node will search for the next active virtual interface (which will be usable as a clock source) and mark that interface as the clock source. Therefore this VT search mechanism, allows the clock source of the node to be associated with the physical trunk port rather than virtual interface.

2. The clock selection mechanism, within the same trunk port(slot.port) will be transparent to the user. An event will be generated to indicate the switching of the clock source from one VI to another on the same trunk port, if the debug flag on/off3 is enabled. This debug flag will be defaulted to 'disabled'.This event log is confined only to the local node and can be enabled through a debug on/off flag. The present clock switch event logs (local and remote node) will be modified, to remove the virtual interface number.

3. There is no switching of the interface clock occurs, if a clock source VT fails, and there is another active (OK state) interface available on the same interface port and therefore the interface clock source is not failed. However, the new selected VI has to be suitable for configuring as a clock source. With this implementation, the permanent association of the clock source to the first virtual interface of the VT port will be removed and a selection criteria will be applied to associate the clock source to the next available virtual interface on the trunk port.

4. When one VT (the first interface) on the trunk port, configured for the clock source fails, the selection algorithm will look for one clock source configurable virtual interface on the same trunk port. The clock switch to the next source occurs only if there were no clock configurable VIs detected. The suitability of an interface to be a clock source is determined by the clock test.

5. When a virtual trunk, which is configured as a clock source is deleted/deactivated from the node, the clock switch (to the next available source) occurs only if the physical trunk port containing the VT has no other usable virtual trunks.

6. If all of the Virtual Trunks on a trunk port are failed, even though the physical interface may be configurable as clock source, the clock selection criteria will not select the trunk port, for the clock source, since there are no more usable logical trunks available.

7. If the VT port is configured as a clock source, the clock routing/selection algorithm will be triggered at the highest number node only if all the virtual interfaces of a virtual trunk port are not clock source configurable. The current implementation triggers the selection, when a trunk status change occurs only on the first VI of the VT port, independent of the logical trunk number.

8. The clock source switch will occur only if all the VIs on a VT port are failed (the trunk port is now not a sustainable clock) and the message to the trunk card will be issued to de-configure the clock. This is because there is no need to send in the configuration message to the card as long as trunk port is not changing. Therefore between logical trunk selections on the same port, the clock switch will not happen to the next source (or internal, if no source is available).

9. The VT search occurs only on the local node and the VT search is transparent to the other nodes in the n/w, including highest numbered node. If the VT search does not find one suitable clock then the node may trigger a network wide selection or routing as appropriate, depending on the clock routing topology.

The association of the Virtual trunk clock source to the physical interface allows the use of Virtual Trunks as clock source for all of the virtual interfaces available on the trunk port, since the physical interface is the one which drives/derives the clock. Therefore if a VT, configured as a clock source fails, the clock source should not be switched to another physical interface or internal clock source, unless there is no clock configurable active interface up and running. So irrespective of the virtual trunk failure, the clock source should always be associated with the physical interface port, where the virtual trunk is activated.

Feature Summary:

This feature provides an indirect association of the clock source to the physical trunk port rather than the individual virtual interfaces of a virtual trunk port. A clock switch from a configured clock source occurs when a failure is detected by the clock test (diagnostics) running in the back ground. The clocks will be selected in the order of their configuration and the routing of the clock occurs through the topology table defined or derived by the highest number node in the network.The details of the clock synchronization is given in the following section (5.3.1).

A Virtual trunk port can be configured for a clock source, if that physical trunk port (all of the VIs) does not pass the clock sync to route the clock through the other nodes in the network. The default configuration for the VT's for the clock routing is (pass sync) No, where as the non-virtual trunks are always defaulted as clock routing trunks(pass sync = yes). A trunk can be configured as a clock source, only if it is not a clock routing trunk (pass sync = no) and therefore the VT ports that are configured for clock sources cannot route the clock through. Also, the configuration of a virtual trunk, as clock routing as yes or no (pass sync) will affect all the VI's on the trunk port, since the clock routing attribute is a characteristic of the physical interface.

For the software implementation, the default association of clock source internally to the first VI on the trunk port, when the clock source is configured on the port will continue in the same way as now. Therefore if we first configure a VT port, for clock, the first virtual trunk will be selected for our internal reference, which helps us in implementing the local clock switching, transparently to the user. The logical trunk association is for the implementation reference, since a logical trunk is the way of connecting the trunk port interface in switch software.

The use of the trunk port as clock source with all of the VTs in failed state, may not be a real customer scenario and therefore such a configuration is not supported. Also the current switch software implementation of virtual trunks does not provide an accurate status for the detection of the physical interface failures, when all the virtual interfaces are failed.The failure of a clock source can be due to some of the alarm conditions and is determined by the clock diagnostics.

Features:

The VT clocking feature allows the mapping of clock source to one of the suitable logical trunk out of all of the active VIs of a VT port. The following additional features will be provided, if a VT port is configured for clock source:

The event log will indicate the clock switch to the physical interface (slot.port) as in the case of a regular trunk.

If all the VIs fail on physical trunk port, even though this would be configurable as a clock source, the interface will be taken out of service and removed from the list of selectable sources.

The VI failure and clock switching within the same interface port will be transparent to the other nodes in the network.

All of the VIs in a trunk port can trigger the nw clock selection depending on the topology

A debug flag can turn on the event logging, whenever a clock switch occurs between the VIs of a trunk port. The default value for this flag is 'Disabled'

The normal trunk failures continue to cause clock source switches as they do currently and there is no effect on regular trunks (non-virtual trunks) with the introduction of this feature.

If the first virtual interface is failed, at a time when the clock source is configured at a node, the node will behave in the same as currently, and the clock source will be marked for the first interface. Because of the failure the clock source will not be switched to the new configured interface, but when the clock diagnostics reports the failure, the VT search will look for the next interface on the port and attach the source.

When the first interface comes back up, the interface will not be switched back, unless there is a failure and no alternate VI is available.

The VT search occurs in the cyclic order starting at the current interface and runs through max VI's. In IGX the maximum number of Virtual Interfaces is 15 and in BPX the maximum number of VIs is 31 on a trunk port.

No impact on the Release 9.3 Virtual Ports feature, with the introduction of this feature

Limitations:

The following is a known limitation of the VT clock sources:

Even though the VTs can be configured to pass the clock sync (pass sync = yes), and therefore route the clock through Virtual Trunks (through the cloud), the stability of the clock is determined by the entry and exit points in the cloud. This is a current system limitation.

Functional Description and Feature Usage:

The clock source selection algorithm will be modified to indirectly map the clock source to the active physical interface rather than the first virtual interface, by a logical assignment of the VIs to the clock source, according to the VI failure. The behavior of the present UI configuration for the cnfclksrc command will not be changed, it continues to take the virtual trunk port interface, in the slot.port format. The feature will be provided for both IGX and BPX virtual trunks.Following the clock source failure and recovery detection, the clock source will get re-attached, but without sending any message to the card to de-configure and later re-configure. Therefore NO switching to internal source and back will occur between clock switches within the same port. Since the re-attachment is within the same trunk port in the case of VT, the logical trunk interface is referred only for the fault detection, since switch software always require a reference by logical trunk.

Switch Availability

Cisco WAN hardware and software components are designed to provide a switch availability in excess of 99.99 percent. Network availability will be impacted by link failure, which has a higher probability of occurrence than equipment failure.

Because of this, Cisco WAN network switches are designed so that connections are automatically rerouted around network trunk failures, often before users detect a problem. System faults are detected and corrective action taken often before they become service affecting. This section describes some of the features that contribute to network availability.

Node Redundancy

System availability is a primary requirement with the BPX switch. The designed availability factor of a BPX switch is (99.99 percent) based on a node equipped with optional redundancy and a network designed with alternate routing available. The system software, as well as firmware for each individual system module, incorporates various diagnostic and self-test routines to monitor the node for proper operation and availability of backup hardware.

For protection against hardware failure, a BPX switch shelf can be equipped with the following redundancy options:

- Redundant common control modules
- Redundant crosspoint switch matrixes
- Redundant high-speed data and control lines
- Redundant power supplies
- Redundant high-speed network interface cards
- Redundant service interface cards

If redundancy is provided for a BPX switch, when a hardware failure occurs, a hot-standby module is automatically switched into service, replacing the failed module. All cards are hot-pluggable, so replacing a failed card in a redundant system can be performed without disrupting service.

Since the power supplies share the power load, redundant supplies are not idle. All power supplies are active; if one fails, then the others pick up its load. The power supply subsystem is sized so that if any one supply fails, the node will continue to be supplied with adequate power to maintain normal operation of the node. The node monitors each power supply voltage output and measures cabinet temperature to be displayed on the NMS terminal or other system terminal.

Node Alarms

Each BPX switch shelf within the network runs continuous background diagnostics to verify the proper operation of all active and standby cards, backplane control, data, and clock lines, cabinet temperature, and power supplies. These background tests are transparent to normal network operation.

Each card in the node has front-panel LEDs to indicate active, failed, or standby status.

Each power supply has green LEDs to indicate proper voltage input and output.

An Alarm, Status, and Monitor card collects all the node hardware status conditions and reports it using front panel LED indicators and alarm closures. Indicators are provided for major alarm, minor alarm, ACO, power supply status, and alarm history. Alarm relay contact closures for major and minor alarms are available from each node through a 15-pin D-type connector for forwarding to a site alarm system.

BPX switches are completely compatible with the network status and alarm display provided by the Cisco WAN Manager NMS workstation. In addition to providing network management capabilities, it displays major and minor alarm status on its topology screen for all nodes in a network.

The Cisco WAN Manager NMS also provides a maintenance log capability with configurable filtering of the maintenance log output by node name, start time, end time, alarm type, and user-specified search string.

CHAPTER 2

BPX Switch Physical Overview

This chapter describes the physical components of the BPX switch:

- BPX Switch Enclosure
- Card Shelf Configuration
- BPX Switch Major Hardware Component Groups
- Service Expansion Shelf PNNI
- Optional Peripherals

The BPX switch is supplied as a stand-alone assembly. It may be utilized as a stand-alone ATM switch, or it may be integrated at customer sites with one or more multiband IGX switches, MGX 8220 or MGX 8800 shelves, SES PNNI shelves and other access devices to provide network access to broadband backbone network links for narrowband traffic. Cisco and CPE service interface equipment can also be co-located with the BPX switch and connect to its ATM service interfaces.

BPX Switch Enclosure

The BPX switch enclosure is a self-contained chassis which may be rack mounted in any standard 19-inch rack or enclosure with adequate ventilation. It contains a single shelf that provides fifteen slots for vertically mounting the BPX switch cards front and rear.

At the front of the enclosure (see Figure 2-1) are 15 slots for mounting the BPX switch front cards. Once inserted, the cards are locked in place by the air intake grille at the bottom of the enclosure.

To remove or insert cards, a mechanical latch on the air intake grille must be released by using a screwdriver and the grille must be tilted forward in order.

At the rear of the enclosure (illustrated in Figure 2-2) is another series of card slots for mounting the rear plug-in cards. These are held in place with two thumbscrews, top and bottom. A mid-plane, located between the two sets of plug-in cards, is used for interconnect and is visible only when the cards are removed.

Warning **To provide proper cooling, it is essential that blank faceplates be installed in all unused slots. Failure to do so will degrade node cooling and circuit card damage will result. The blank faceplates also provide RFI shielding.**

Figure 2-1 BPX Switch Exterior Front View

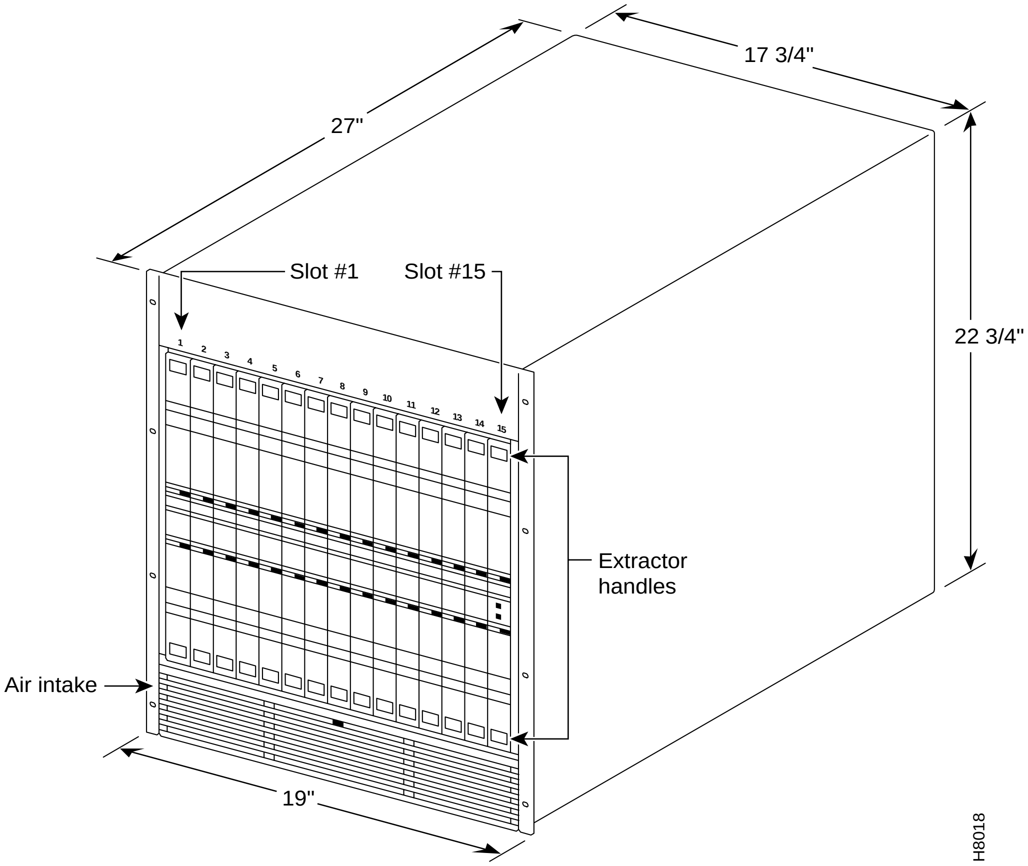
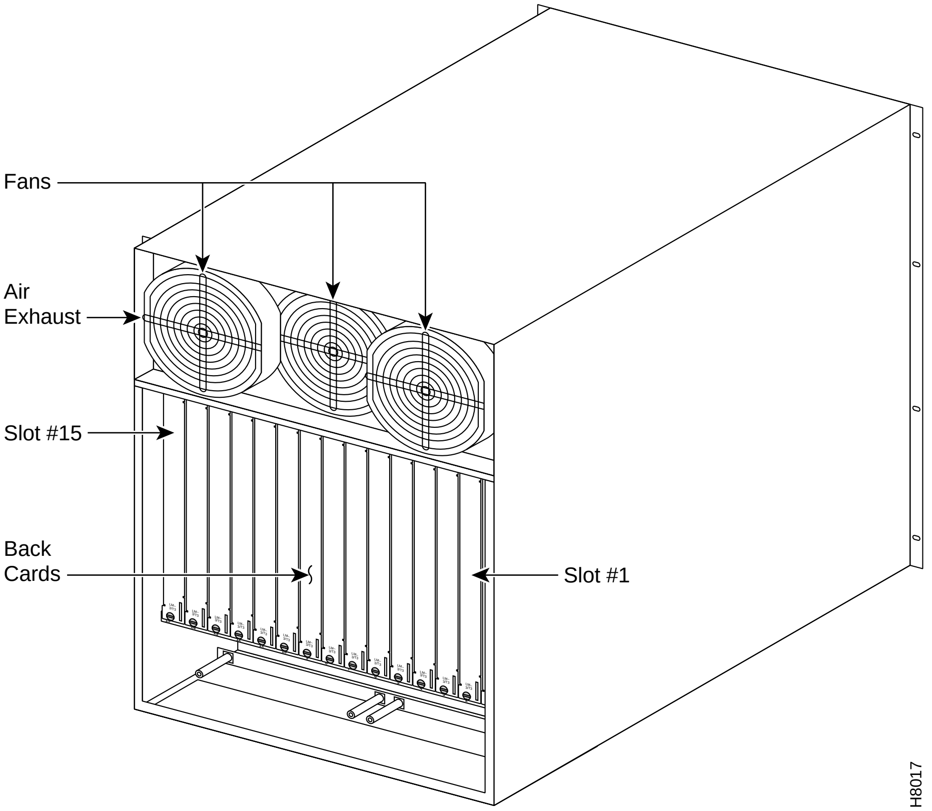


Figure 2-2 BPX Switch Exterior Rear View



Node Cooling

A fan assembly with three six-inch 48 VDC fans is mounted on a tray at the rear of the BPX switch shelf (see Figure 2-2). Air for cooling the cards is drawn through an air intake grille located at the bottom in the front of the enclosure. Air passes up between the vertically-mounted cards and exhausts at the top, rear of the chassis.

All unused slots in the front are filled with blank faceplates to properly channel airflow.

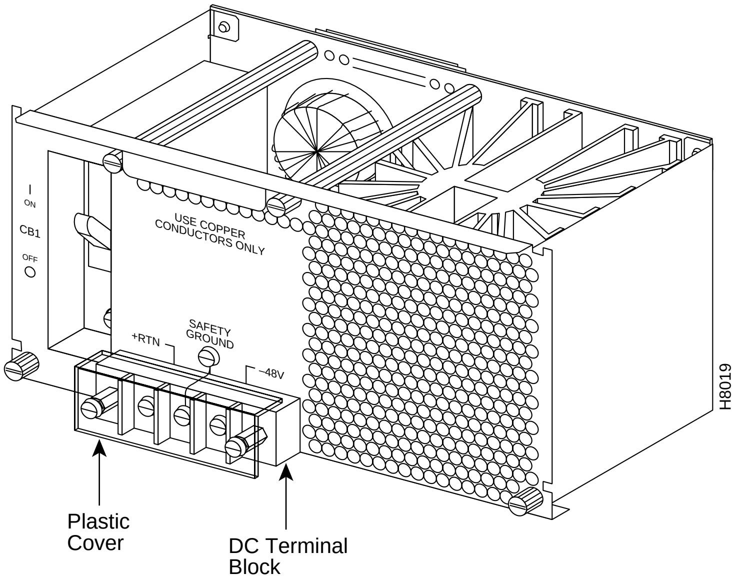
Node DC Powering

The primary power for a BPX switch node is -48 VDC which is bused across the backplane for use by all card slots. DC-to-DC converters on each card convert the -48V to lower voltages for use by the card.

The -48 VDC input connects directly to the DC Power Entry Module (PEM). The DC Power Entry Module (see Figure 2-3) provides a circuit breaker and line filter for the DC input.

Nodes may be equipped with either a single PEM or dual PEMs for redundancy. PEMs are mounted at the back of the node below the backplane. A conduit hookup box or an insulated cover plate is provided for terminating conduit or wire at the DC power input. It is recommended that the source of DC for the node be redundant and separately fused.

Figure 2-3 DC Power Entry Module Shown with Conduit Box Removed

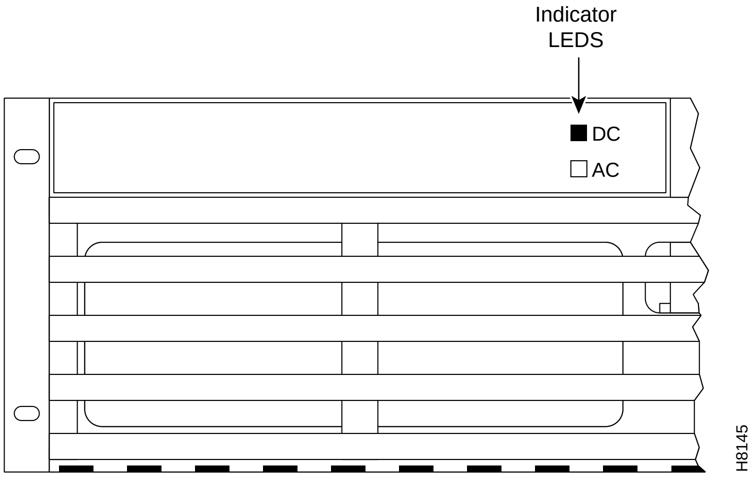


Optional AC Power Supply Assembly

For applications requiring operation from an AC power source, an optional AC Power Supply Assembly and shelf is available. It provides a source of –48 VDC from 208/240 VAC input. A shelf, separate from the BPX switch shelf, houses one or two AC Power Supplies and mounts directly below the node cabinet. This provides a secure enclosure for the power supply assemblies (supplies cannot be removed without the use of tools).

Two of these supplies are usually operated in parallel for fail-safe redundant operation. The front of the AC Power Supplies for the BPX switch includes two green LEDs to indicate correct range of the AC input and the DC output for each individual supply (see Figure 2-4).

Figure 2-4 AC Power Supply Assembly Front View



Card Shelf Configuration

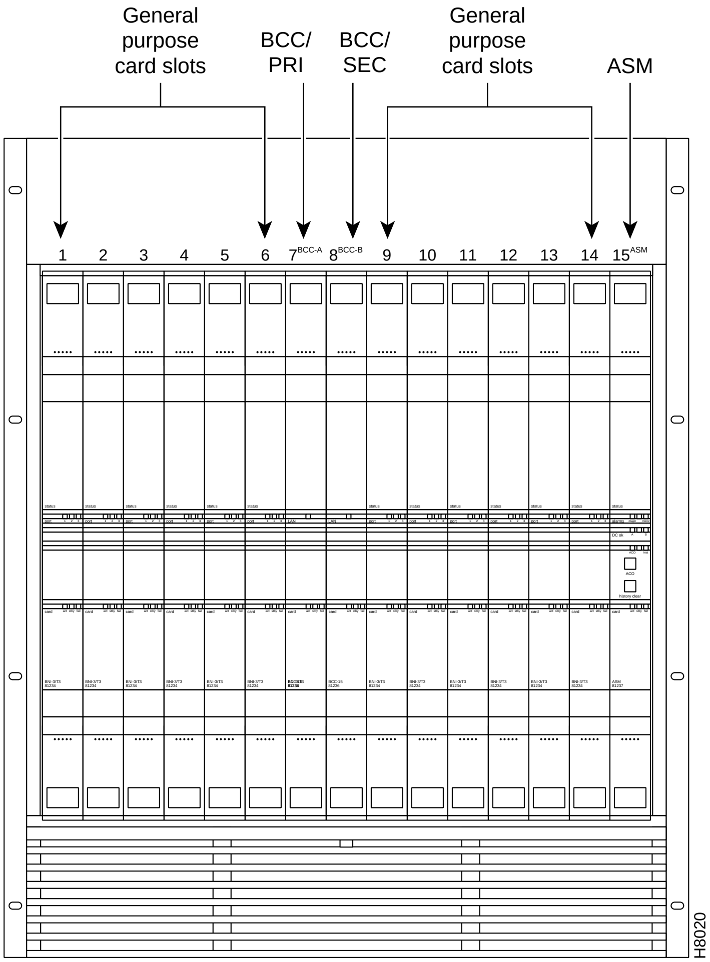
There are fifteen vertical slots in the front of the BPX switch enclosure to hold plug-in cards (see Figure 2-5).

The middle two slots, slots number 7 and number 8, are used for the primary and secondary Broadband Controller Cards (BCC).

The right-most slot, number 15, is used to hold the single Alarm/Status Monitor Card.

The other twelve slots, number 1 through number 6 and number 8 through number 14, can be used for the Network Interface and Service Interface cards.

Figure 2-5 BPX Switch Card Shelf Front View



BPX Switch Major Hardware Component Groups

There are four major groups of hardware components in the BPX switch:

- Common Core Components
- Network Interface Components

- Service Interface Components
- Power Supply Components

Table 2-1 lists these groups and their components along with a brief description of each.

For a detailed description of these components, see:

Table 2-1 BPX Switch Plug-In Card Summary

Card	Card Name	Where
BPX-	**Common Core Component Group**	
BPX-BCC-32	Broadband Controller Card, operates with versions of System Software Release 7.0 and above, and requires 32 Mbyte RAM for 8.1 and later software. For redundancy configuration, installed as a pair of BCC-32s. (System operation equivalent to BCC-3.)	Front
BPX-BCC-bc	Back card (also known as LM-BCC) used only with the BCC-32.	Back
BPX-BCC-3-64	Broadband Controller Card, enhanced BCC-3. Note: BCC-3-64 or BCC-4 required to support VSI and MPLS.	
BPX-BCC-4	Broadband Controller Card, operates with 8.4 software and above. For redundancy configuration, installed as a pair of BCC-4s. Provides 64 Mbyte of RAM and above. Supports up to 19.2 Gbps performance of BXM cards. Note: BCC-3-64 or BCC-4 required to support VSI and MPLS	Front
BPX-BCC-3-bc	Back card (also known as LM-BCC) used with BCC-4.	Back
BPX-ASM	Alarm/Status Monitor Card.	Front
BPX-ASM-BC	Line Module - Alarm/Status Monitor.	Back
	Network Interface Component Group	
BPX-BXM-T3-8 BPX-BXM-E3-8 BP:X-BXM-T3-12 BPX-BXM-E3-12	T3/E3 card with 8 or 12 ports. Card is configured for use in either network interface or service access (UNI) mode and with either a T3 or E3 interface.	Front
BPX-T3/E3-BC	Backcard for use with a BXM-T3/E3-8 or BXM-T3/E3-12	Back
BPX-BXM-155-4 BPX-BXM-155-8	BXM OC-3 cards with 4 or 8 OC-3/STM-1ports, respectively. Card is configured for use in either network interface or service access (UNI) mode.	Front
BPX-MMF-155-4-BC BPX-SMF-155-4-BC BPX-SMFLR-155-4-BC	Backcards for BXM-155-4.	Back
BPX-MMF-155-8-BC BPX-SMF-155-8-BC BPX-SMFLR-155-8-BC	Backcards for BXM-155-8.	Back
BPX-BXM-622 BPX-BXM-622-2	OC-12 card with 1or 2 OC-12/STM-4 ports. Card is configured for use in either network interface or service access (UNI) mode.	Front
BPX-BME	Used for multicast connections. Used with SMF-622-2 backcard with port 1 looped to port 2, transmit to receive, and receive to transmit.	
BPX-SMF-622 BPX-SMFLR-622 BPX-XLR-622-BC	Backcards for BXM-622. The XLR card supports a 1500nm interface	Back

Table 2-1 BPX Switch Plug-In Card Summary (continued)

<table>
<tr><th>Card</th><th>Card Name</th><th>Where</th></tr>
<tr><td>BPX-SMF-622-2-BC
BPX-SMFLR-622-2-BC
BPX-SMFLR-622-2-BC</td><td>Backcards for BXM-622-2 and BME (BME typically would use SMF-622-2).</td><td>Back</td></tr>
<tr><td>BPX-BME</td><td>Used for multicast connections. Used with SMF-622-2 backcard with port 1 looped to port 2, transmit to receive, and receive to transmit.</td><td>Back</td></tr>
<tr><td>BPX-BNI-3-T3</td><td>Broadband Network Interface Card (with 3 T3 Ports).</td><td>Front</td></tr>
<tr><td>BPX-T3-BC</td><td>Line Module, used with BNI-T3 for 3 physical T3 ports. (Configured for 3 ports)</td><td>Back</td></tr>
<tr><td>BPX-BNI-3-E3</td><td>Broadband Network Interface Card (with 3 E3 Ports).</td><td>Front</td></tr>
<tr><td>BPX-E3-BC</td><td>Line Module, used with BNI-E3 for 3 physical E3 ports. (Configured for 3 ports).</td><td>Back</td></tr>
<tr><td></td><td><b>APS Backcards and APS Redundant Backplane</b></td><td></td></tr>
<tr><td colspan="3">The APS 1+1 feature requires two BXM front cards, an APS redundant frame assembly, and two redundant type BXM backcards. The types of redundant backcard and backplane sets 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.</td></tr>
<tr><td colspan="3">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</td></tr>
<tr><td></td><td><b>Service Interface Component Group</b></td><td></td></tr>
<tr><td>BPX-E3-BC</td><td>Line Module, used with BNI-E3 for 2 physical E3 ports. (Configured for 2 ports)</td><td>Back</td></tr>
<tr><td></td><td><b>Power Supply Group</b></td><td></td></tr>
<tr><td></td><td>48 Volt DC Power Supply</td><td></td></tr>
<tr><td></td><td>Optional AC Power Supply</td><td></td></tr>
</table>

Service Expansion Shelf PNNI

The Cisco BPX SES PNNI Controller is an optional Service Expansion Shelf (SES) controller connected directly to a BPX 8600 series switch to provide Private Network to Network Interface (PNNI) signaling and routing for the establishment of ATM switched virtual circuits (SVCs) and Soft Permanent Virtual Circuits (SPVCs) over a BPX 8600 wide area network. However, the SES can be used in several WAN switching applications and is not limited to function only as a BPX SES PNNI Controller

Every BPX 8600 series switch that deploys PNNI signaling and routing is collocated and attached to a BPX SES PNNI Controller. The BPX SES PNNI Controller uses Cisco's Virtual Switch Interface (VSI) protocol to control the BPX switch for its networking application.

The BPX SES PNNI Controller is a 7-slot chassis that contains two Processor Switch Modules (PXMs) that run the PNNI and SVC software. One of the PXMs serves as the active processor, while the other serves as the standby. The PNNI controller is mounted directly atop the BPX switch and cabled to it through either the OC-3 ATM interface (Figure 1-3) or the DS3 interfaces (Figure 1-4).

For instructions on installing a Service Expansion Shelf in a BPX 8620 rack and initially powering up, see *Cisco Service Expansion Shelf (SES) Hardware Installation Guide*. To configure an SES PNNI for a BPX 8620, see the *Cisco SES PNNI Controller Software Configuration Guide*.

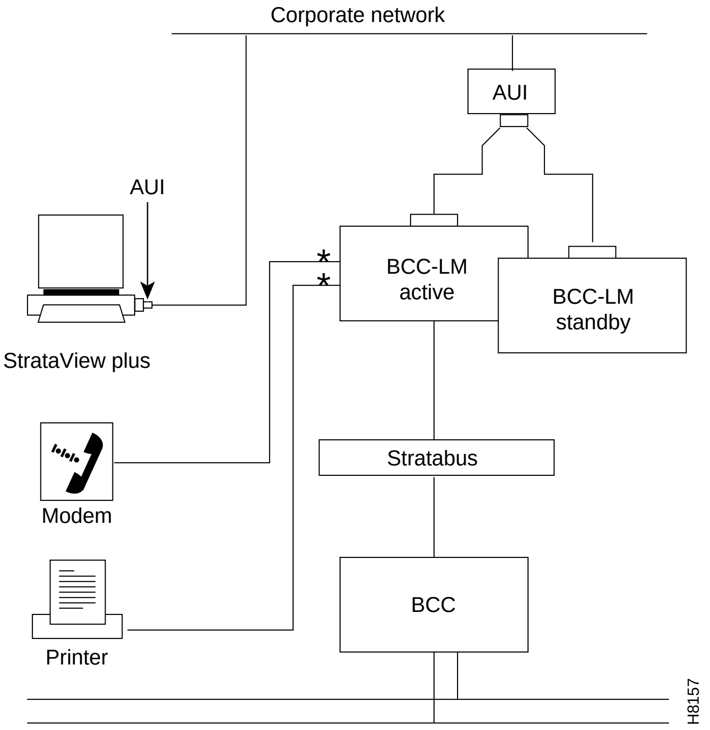
Optional Peripherals

At least one node in the network (or network domain if a structured network) must include a Cisco WAN Manager network management station (see Figure 2-6).

A Y-cable may be used to connect the LAN ports on the primary and secondary BCC Line Modules, through an AUI to the LAN network, because only one BCC is active at a time.

The serial Control port may be connected to a dial-in modem for remote service support or other dial-up network management access. The serial Auxiliary Port can be used for incoming and outgoing data as well as the Autodial feature to report alarms to Cisco TAC.

Figure 2-6 Optional Peripherals Connected to BPX Switch



Two ports on BCC-LM can be used to connect up to two (2) of the peripherals shown.

CHAPTER 3

BPX Switch Common Core Components

This chapter describes the BPX Switch's common core hardware components:

- Broadband Controller Card (BCCs)
- 19.2 Gbps Operation with the BCC-4V
- Alarm/Status Monitor Card
- BPX Switch StrataBus 9.6 and 19.2 Gbps Backplanes

The BPX switch Common Core group includes the components shown in Figure 3-1:

- Broadband Controller Cards:
  - BCC-4 backcard
  - or BCC-32 and associated BCC15-BC backcard

Note The BCC-4 is required for VSI and MPLS features operation

- Alarm/Status Monitor (ASM), a Line Module for the ASM card (LM-ASM).
- StrataBus backplane.

The BCC-4V provides a 16 x 32 crosspoint switch architecture to extend the BPX peak switching capability from 9.6 up to 19.2 Gbps peak. The BCC-4V also provides 4 MBytes of BRAM and 128 MBytes of DRAM.

The functions of the common core components include:

- ATM cell switching.
- Internal node communication.
- Remote node communication.
- Node synchronization.
- Network management communications (Ethernet), local management (RS-232).
- Alarm and status monitoring functions.

Broadband Controller Card (BCCs)

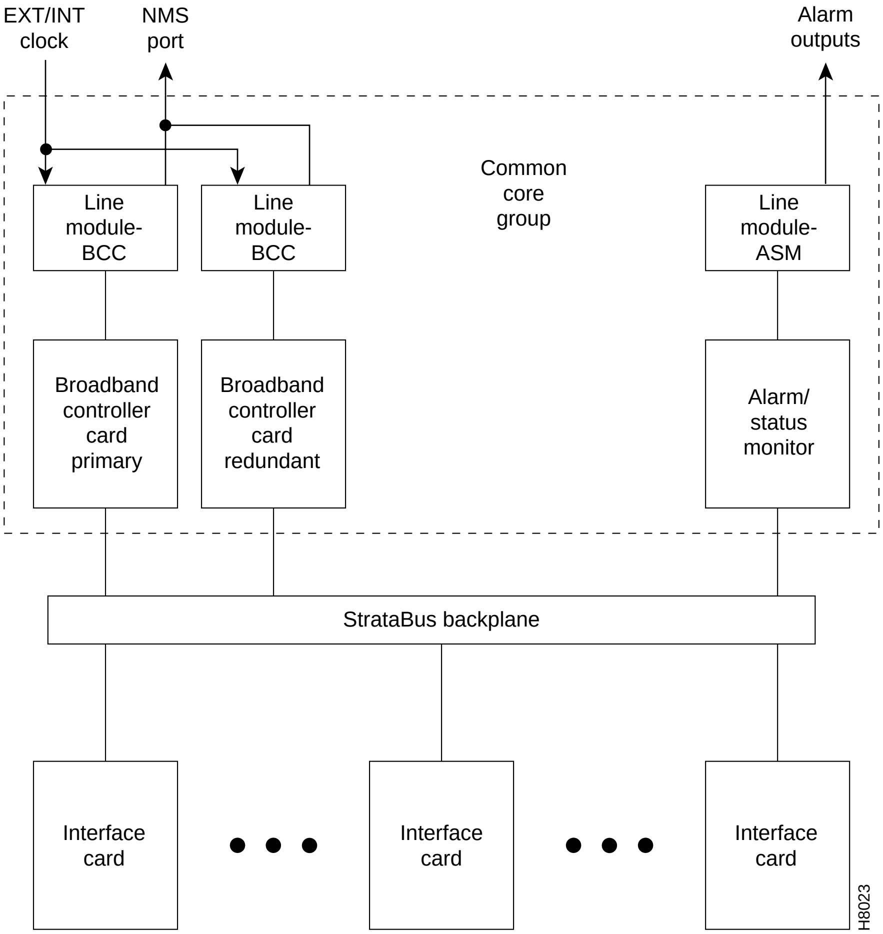
The Broadband Controller Card is a microprocessor-based system controller and is used to control the overall operation of the BPX switch. The controller card is a front card that is usually equipped as a redundant pair.

Slots number 7 and number 8 are reserved for the primary and secondary (standby) broadband controller cards. Each broadband controller front card requires a corresponding back card.

- For non-redundant nodes, a single BCC is used in front slot number 7 with its appropriate backcard.
- For redundant nodes, a pair of BCCs of matching type, are used in front slot numbers 7 and 8.

Note The three types of BCCs with their proper backcards may be operated together temporarily for maintenance purposes, for example, replacing a failed controller card. Throughout a network, individual BPX switches may have either a single BCC-4V controller card or a pair of the identical type of BCC.

Figure 3-1 Common Core Group Block Diagram



The term BCC is used in this manual to refer to the functional operation of the Broadband Controller Card. When a difference in operation does occur, the specific type of BCC is specified.

The BCC-4V provides a 16 x 32 cross-point architecture that increases the peak switching capacity of the BPX switch to 19.2 Gbps, with a sustained non-blocking throughput of 9.6 Gbps.

Features

The Broadband Controller Card performs these major system functions:

- Runs the system software for controlling, configuring, diagnosing, and monitoring the BPX switch.
- Contains the crosspoint switch matrix operating at 800 Mbps per serial link or up to 1600 Mbps (BCC-4V).
- Contains the arbiter which controls the polling each high-speed data port and grants the access to the switch matrix for each port with data to transfer.
- Generates Stratum 3 system clocking and can synchronize it to either a selected trunk or an external clock input.
- Communicates configuration and control information to all other cards in the same node over the backplane communication bus.
- Communicates with all other nodes in the network.
- Provides a communications processor for an Ethernet LAN port plus two low-speed data ports. The BCC15-BC provides the physical interface for the BCC-32.
  The BCC-3-BC provides the physical interface for the BCC-3-32M, BCC-3-64M, and BCC-4V.

Each Broadband Controller Card includes the following:

- 68EC040 processor operating at 33 MHz.
- 32 Mb or 64 MB option for BCC-4.
- 4 Mb of Flash EEPROM for downloading system software.
- 512 Kbytes of BRAM for storing configuration data.
- EPROM for firmware routines.
- 68302 Utility processor.
- SAR engine processor operating at 33 MHz.
- Communication bus interface.
- HDLC processor for the LAN connection interface.
- Two RS-232 serial port interfaces.

Functional Description

The BPX switch is a space switch. It employs a crosspoint switch for individual data lines to and from each port. The switching fabric in each BPX switch consists of three elements for the BCCs (see Figure 3-2):

- Central Arbiter on each BCC.
- Crosspoint Switch.
  - 16 X 32 Crosspoint Switching Matrix on each BCC (2 X [12 X 12]) used for BCC-4V.
- Serial Interface and LAN Interface Modules on each BCC and on each Function Module.

The arbiter polls each card to see if it has data to transmit. It then configures the crosspoint switching matrix to make the connection between the two cards. Each connection is unidirectional and has a capacity of 800 Mbps (616.7 Mbps for cell traffic plus the frame overhead).

Only one connection at a time is allowed to an individual card.

Each card contains a Switch Interface Module (SIM) which merely provides a standardized interface between the card and the data lines and polling buses. The SIM responds to queries from the BCC indicating whether it has data ready to transmit.

With the BPX switch equipped with two BCCs, the cell switching is completely redundant in that there are always two arbiters, two crosspoint switches, two completely independent data buses, and two independent polling buses.

The BCC incorporates non-volatile flash EEPROM which permits new software releases to be downloaded over the network and battery-backup RAM (BRAM) for storing user system configuration data. These memory features maintain system software and configuration data even during power failures, eliminating the need to download software or reconfigure after the power returns.

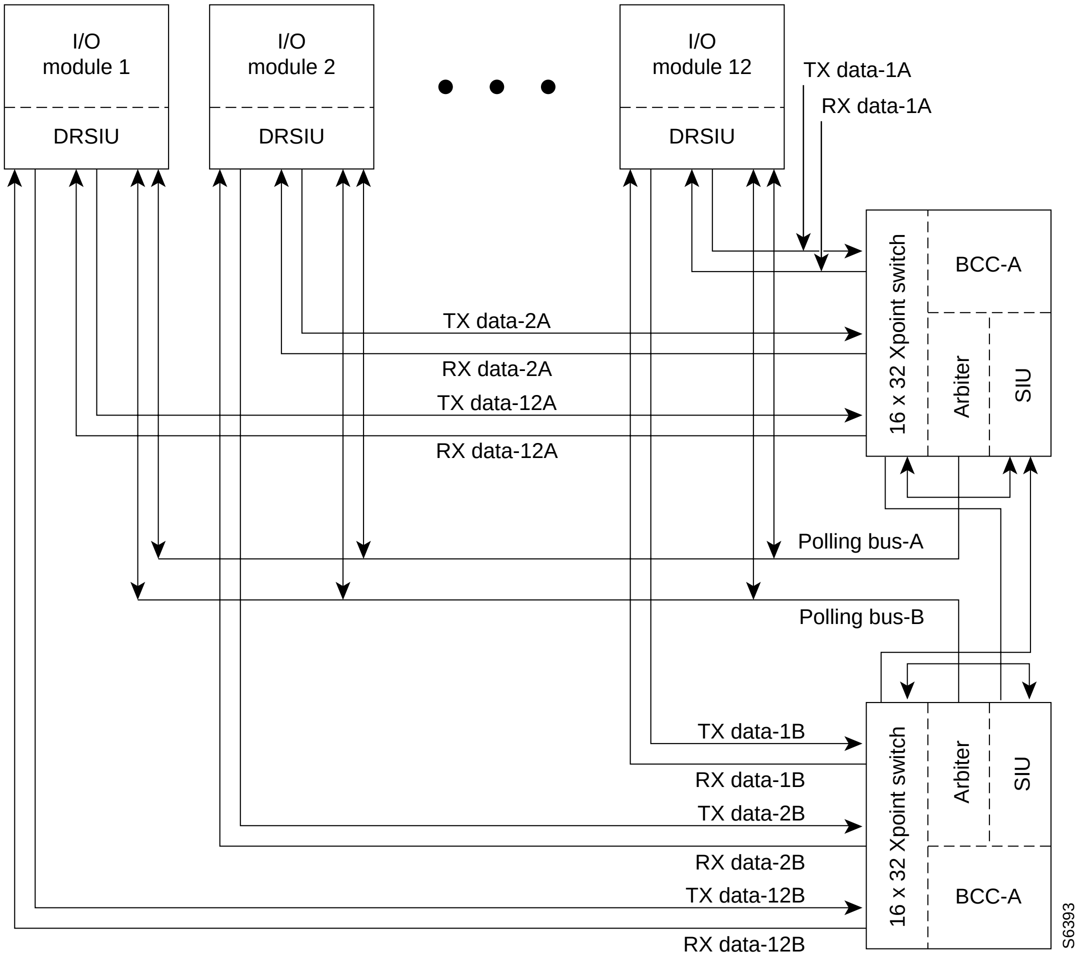
The BPX switch cell switching is not synchronized to any external clocks; it runs at its own rate. No switch fabric clocks are used to derive synchronization nor are these signals synchronized to any external sources.

Node clocking is generated by the BCC. Because the BPX switch resides as an element in a telecommunications network, it is capable of synchronizing to higher-stratum clocking devices in the network and providing synchronization to lower stratum devices. The BCC can be synchronized to any one of three different sources under software control:

- An internal, high-stability oscillator.
- Derived clock from a BNI module.
- An external clock source connected directly to the BPX.

The BCC clock circuits provide clocking signals to every other card slot. If a function card needs to synchronize its physical interface to the BPX switch clock, it can use this timing signal to derive the proper reference frequency. These reference frequencies include DS1, E1, DS3, and E3.

Figure 3-2 BCC4V Block Diagram



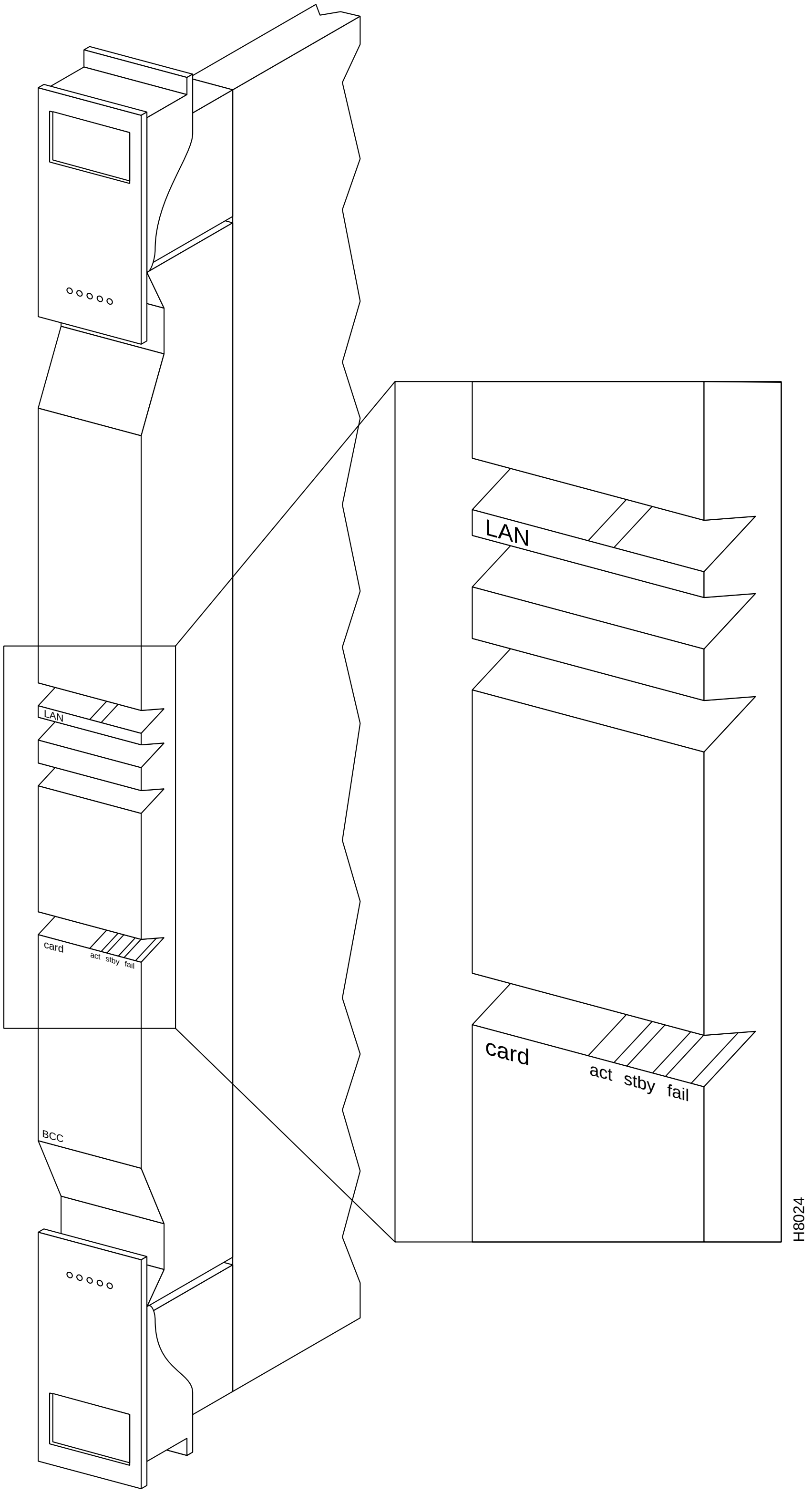
Front Panel Description

The BCC front panel has four Led, three card status LEDs, and a LAN LED. (See Figure 3-3 and Table 3-1.)

Table 3-1 BCC Front Panel Indicators

Number	Indicator	Function
1	LAN	Indicates there is data activity over the Ethernet LAN port.
2	card - act	Card active LED indicates this BCC is online and actively controlling the node.
3	card - stby	Card standby LED indicates this BCC is offline but is ready to take over control of the node at a moments notice.
4	card - fail	Card fail LED indicates this BCC has failed the internal self-test routine and needs to be reset or replaced.

Figure 3-3 BCC Front Panel



The BCC runs self-tests continuously on internal functions in the background and if a failure is detected, the **fail** LED is lighted. If the BCC is configured as a redundant pair, the off-line BCC is indicated by the lighted **stby** LED. The **stby** LED also flashes when a software download or standby update is in progress. The LAN LED indicates activity on the Ethernet port.

19.2 Gbps Operation with the BCC-4V

To operate the BPX switch at up to a 19.2 Gbps peak throughput, these components are required:

- A 19.2 Gbps backplane
- BCC-4V or later controller cards
- One or more BXM cards
- Release 8.4.00 or later switch software
- A backplane NOVRAM that is programmed to identify the backplane as a 19.2 Gbps backplane.

Switch software does not allow node operation at 19.2 Gpbs unless it can read the backplane NOVRAM to verify that the backplane is a 19.2 Gbps backplane.

The 19.2 backplane can be visually identified by the small white card slot fan fuses at the bottom rear of the backplane. These fan fuses are approximately 1/4 inch high and 1/8 inch wide. The 9.6 Gbps backplane does not have these fuses.

If the BPX switch is a late model, then a 19.2 Gbps backplane is installed. You can be verify this by running the **despond** command which will display “Word #2 =0001” if the backplane NOVRAM has been programmed. If anything else is displayed, visually check the backplane for the fuses.

If the backplane is a 19.2 Gbps backplane, but the backplane NOVRAM has not been set to display Word #2 =0001, then you may use the **cnfbpnv** command to program the NOVRAM:

Step 1 Enter **cnfbpnv**. The interface responds:

```
Are you sure this is a new backplane (y/n).
```

Step 2 Enter **y**

Step 3 Confirm that the change has been made by entering **dspbpnv** to confirm the response:

```
Word #2 =0001
```

Note If the change does not take place, it will be necessary to change the backplane NOVRAM. Contact Cisco Customer Service.

Step 4 Enter **switchcc** to make switch software recognize the change.

If the backplane is not a 19.2 Gbps backplane, contact Customer Customer Service.

Back Cards for the BCC-4V

The backcards for the Broadband Controller Card serve as an interface between the BPX switch and the BPX switch network management system.

For the BCC-4V, the backcard is the BCC-3-BC. (These backcards are also known as the BCC backcards).

The BCC-4V provides important features such as support for up to 19.2 Mbps peak operation with BXM cards. Both BCCs in a node should be of the same type.

The backcard provides these interfaces:

- An 802.3 AIU (Ethernet) interface for connecting the node to a CWM NMS.
- A serial RS-232 Control Port for connecting to a VT100-compatible terminal or modem.
- A serial RS-232 Auxiliary Port for connecting to an external printer.
- External clock inputs at T1 or E1 rates, output at 8 kHz.

The face plate connectors are described in Table 3-2 and Table 3-3 and shown in Figure 3-4. The BCC15-BC is shown on the left and the BCC-3-BCC is shown on the right.

For specifications on cabling, refer to Chapter 31, BPX Switch Cabling Summary.

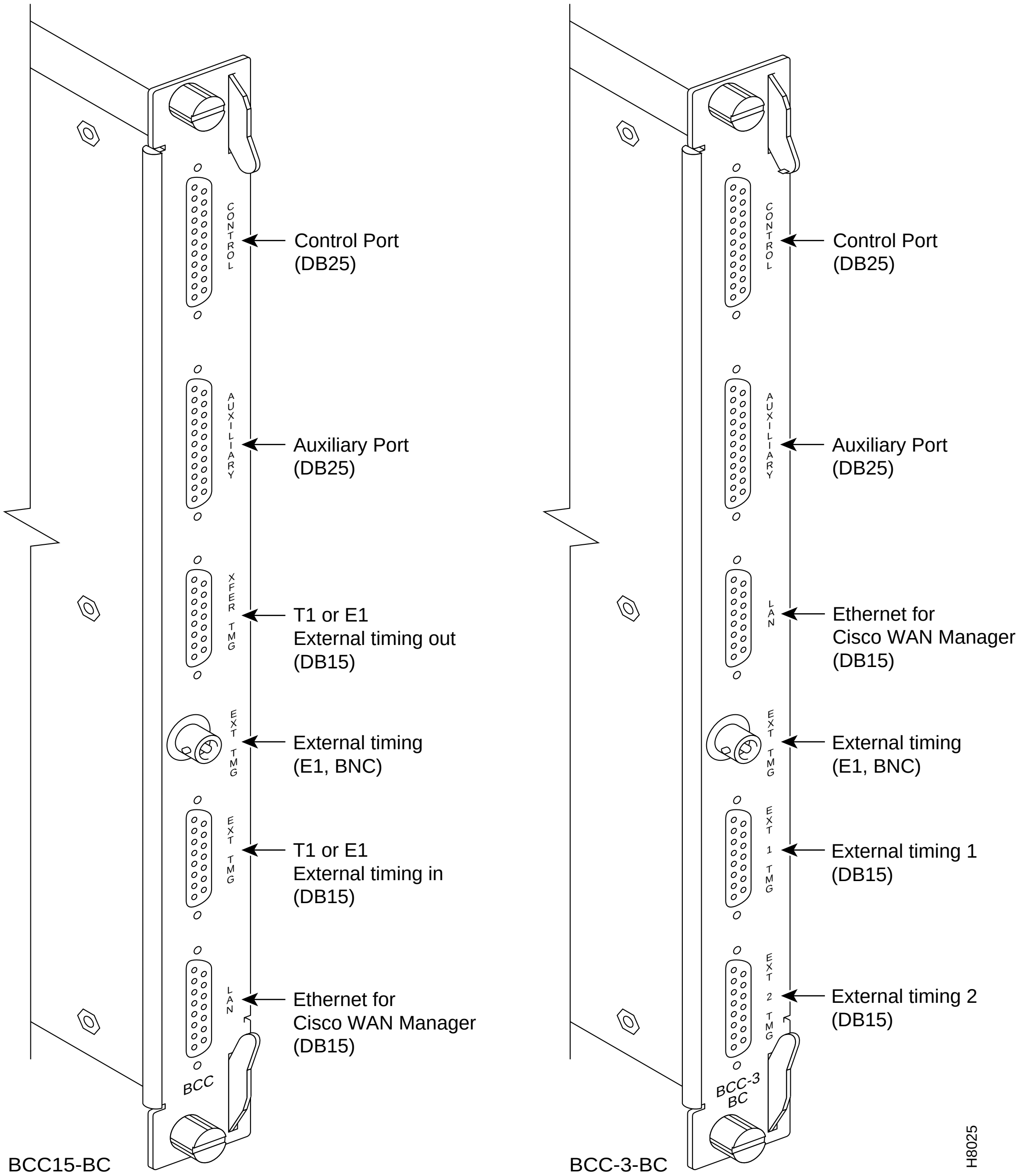
Table 3-2 BCC15-BC Backcard for BCC-32, Connectors

Connector	Function
CONTROL	A DB25 connector for a VT100 or equivalent terminal for a basic terminal connection enabling you to use the command line interface commands. You can also connect to a dial-in modem for remote service support or other network management dial-up access. This is a bidirectional RS232 communications port. It is not used for CWM Network Management; the LAN connector is used for CWM Network Management.
AUXILIARY	A DB25 connector for a system printer. This is a one-way, RS232 outgoing port.
XFER TMG	DB15 connector that supplies an 8-kHz timing signal (RS422 type output that is synchronized to the BPX switch system clock.)
EXT TMG	A 75-ohm BNC connection for clock input. An E1 source with 75 ohm impedance typically uses this connector. If the shield on the cable needs grounding, slide the BCC back card out and jumped connector JP1 across its two pins.
EXT TMG	DB15 connector for a primary and optional redundant external source of system clock. A T1 source with 100 ohm impedance or an E1 source with 100/120 ohm impedance typically use this connector.
LAN	A DB15 Ethernet LAN connection for connecting to a CWM NMS. You can also connect a terminal (or NMS other than CWM) to the BPX switch LAN port via Ethernet. However, only the CWM NMS provides full management configuration and statistics capabilities via SNMP and TFTP.

Table 3-3 BCC-3-BC Back Card for BCC-4V

Connector	Function
CONTROL	A DB25 connector for a VT100 or equivalent terminal for a basic terminal connection using command line interface commands. You can also connect to a dial-in modem for remote service support or other network management dial-up access. This is a bidirectional RS232 communications port. This is not used for CWM Network Management; the LAN connector is used for CWM Network Management.
AUXILIARY	A DB25 connector for a system printer. This is a one-way, RS232 outgoing port.
LAN	A DB15 Ethernet LAN connection for connecting to a CWM NMS. A terminal or NMS other than CWM can also be connected to the BPX switch LAN port via Ethernet. However, only the CWM NMS provides full management configuration and statistics capabilities via SNMP and TFTP.
EXT TMG	A 75-ohm BNC connection for clock input. An E1 source with 75 ohm impedance typically uses this connector. If the shield on the cable needs grounding, slide the BCC back card out and jumper connector JP1 across its two pins.
EXT 1 TMG	DB15 connector for a primary and optional redundant external source of system clock. A T1 source with 100 ohm impedance or an E1 source with 100/120 ohm impedance typically use this connector.
EXT 2 TMG	Provides for an external clock source redundant to the EXT 1 TMG source.

Figure 3-4 BCC15-BC and BCC-3-BC Backcard Face Plate Connectors



Another function of the line module back card is to provide two low-speed, serial communications ports, as described in Table 3-3:

CONTROL port
A bidirectional port for connecting the BPX switch to a local terminal or to a modem for a remote terminal dial-in connection.

AUXILIARY port
An output only port, typically used to connect to a printer dedicated to printing logs.

The Cisco WAN Manager NMS is connected to the LAN port on the BCC backcards. When control is provided via an Ethernet interface, you configure the node IP address by using the **cnflan** command for the BPX switch. For redundancy, also configure the LAN ports on both BCC back cards, each connected to an AUI adapter.

The LAN port of the primary Broadband Control Card is active. If the secondary Broadband Control Card becomes primary (active), then its LAN port becomes active. The Cisco WAN Manager workstation will automatically try to restore communications over the LAN and will interface with the newly active Broadband Controller Card.

For small networks, one Cisco WAN Manager workstation is adequate to collect statistics and provide network management. For larger networks additional Cisco WAN Manager workstations may be required. Refer to the *Cisco WAN Manager Operations Guide*.

Alarm/Status Monitor Card

The Alarm/Status Monitor (ASM) card is a front card. Only one is required per node and it is installed in slot 15 of the BPX switch. It is used in conjunction with an associated back card, the Line Module for the ASM (LM-ASM) card.

The ASM and LM-ASM cards are non-critical cards used for monitoring the operation of the node and not directly involved in system operation. Therefore, there is no provision or requirement for card redundancy.

Features

The ASM card provides a number of support functions for the BPX switch:

- Telco compatible alarm indicators, controls, and relay outputs.
- Node power monitoring (including provision for optional external power supplies).
- Monitoring of shelf cooling fans.
- Monitoring of shelf ambient temperature.
- Sensing for the presence of other cards that are installed in the BPX switch.

Functional Description

BPX switch system software commands the ASM card to activate the major and minor alarm indicators and relays.

There are four significant circuits controlled by the ASM processor:

- Alarm
  The alarm monitor controls the operation of the front panel alarm LEDs and ACO and history push buttons as well as the alarm relays that provide dry contact closures for alarm outputs to customer connections.
- Power supply monitor
  The power supply monitor circuit monitors the status of the -48V input to the shelf on each of the two power buses, A and B. The status of both the A bus and B power bus is displayed on the ASM front panel.

- Fan and temperature monitor
  Each of the three cooling fans is monitored by the fan monitor circuit which forwards a warning to the BPX switch system software if any fan falls below a preset RPM. Cabinet internal temperature is also monitored by the ASM which sends the temperature to the system software to be displayed on the NMS terminal. The range that can be displayed is 0 degrees to 60 degrees Centigrade.
- Card detection.

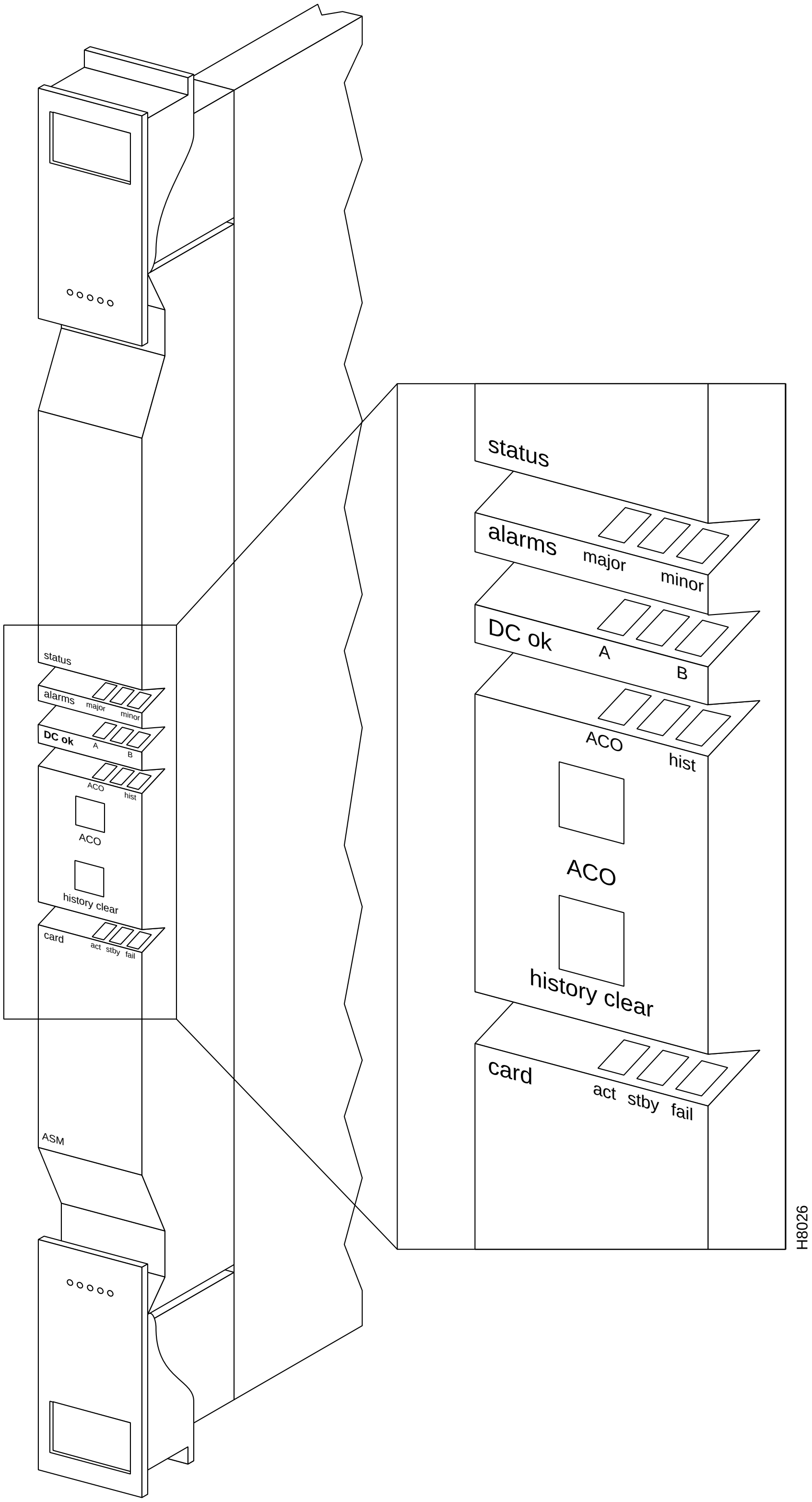
Front Panel Description

The front panel displays the status of the node and any major or minor alarms that might be present. Figure 3-5 illustrates the front panel of the ASM card. Each front panel feature is described in Table 3-4.

Table 3-4 ASM Front Panel Controls and Indicators

Number	Controls/Indicator	Function
1	alarms LEDs	A red major alarm and a yellow minor alarm indicator to display the status of the local node. In general, a major alarm is affects service whereas a minor alarm is a failure that does not affect service.
2	dc LEDs	Two green LEDs display the status of the two DC power busses on the Stratabus backplane. ON indicates voltage within tolerance. OFF indicates an out-of-tolerance voltage.
3	ACO/hist LEDs	ACO LED (yellow) lights when you press the front panel ACO pushbutton. History LED (green) indicates an alarm has been detected by the ASM at some time in the past but might not be clear at present time.
4	ACO switch	When operated, releases the audible alarm relay.
5	history clear switch	Extinguishes the history LED if the alarm condition has cleared. If the alarm is still present when the history clear switch is thrown, the history LED will stay lit.
6	card status LEDs	Active (green) indicates the card is online and clear of alarms. Standby (yellow) indicates the card is offline. Fault (red) indicates a card failure is detected by the card self-test diagnostics.

Figure 3-5 ASM Front Panel Controls and Indicators



Line Module for the Alarm/Status Monitor Card

The Line Module for the Alarm/Status Monitor Card (LM-ASM) is a back card to the ASM card. It provides a simple connector panel for interfacing to your alarm system. It is not required for system and ASM operation.

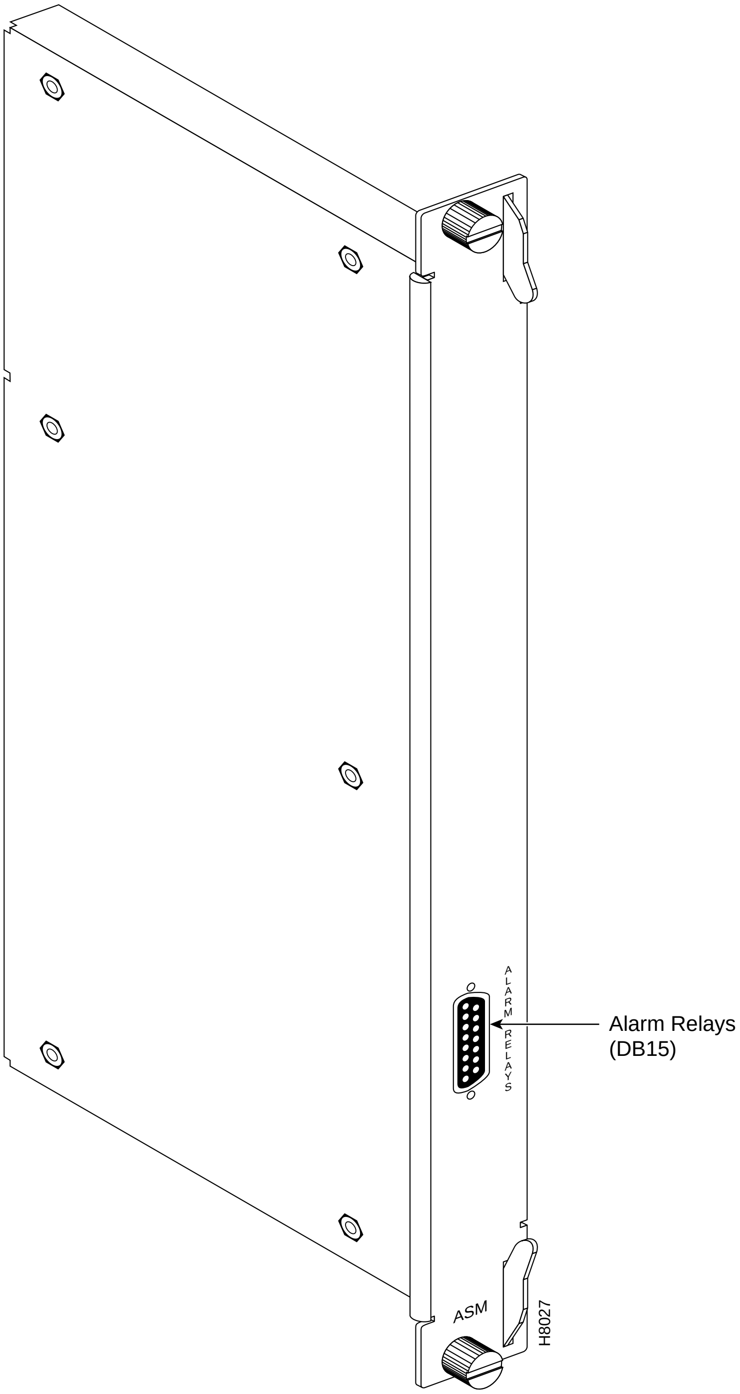
The LM-ASM backcard must be installed in back slot number 15.

Figure 3-6 illustrates the face plate of the LM-ASM which contains a single subminiature connector (see Table 3-5). The Alarm Relay connector provides dry-closure (no voltage) relay contact outputs.

Table 3-5 LM-ASM Face Plate Connectors

Number	Connector/Indicator	Function
1	ALARM RELAYS	A DB15 connector for alarm relay outputs. Refer to Chapter 3 or Appendix C for pinouts.

Figure 3-6 LMI-ASM Face Plate



BPX Switch StrataBus 9.6 and 19.2 Gbps Backplanes

The BPX switch may be equipped with a backplane that supports either a 9.6 or up to 19.2 Gbps operation. The 19.2 Gbps backplane can physically be identified by the card slot fuses on the bottom rear of the backplane. All BPX switch modules are interconnected by the BPX switch StrataBus backplane physically located between the front card slots and the back card slots.

Although the ATM data paths between the switching fabric and the interface modules are individual data connections, there are also a number of system bus paths for controlling the operation of the BPX switch. The StrataBus backplane, in addition to the 15 card connectors, contains these signal paths:

- ATM crosspoint wiring
  Individual paths to carry ATM trunk data between both the network interface and service interface modules and the crosspoint switching fabric.
- Polling bus
  To carry enable signals between the BCC and all network interface modules.
- Communications bus
  For internal communications between the BCC and all other cards in the node.
- Clock bus
  To carry timing signals between the BCC and all other system cards.
- Control bus
  Enables either the A-bus wiring or B-bus wiring.

All StrataBus wiring is completely duplicated and the two sets of bus wiring operate independently to provide complete redundancy. Either the A-side wiring or B-side wiring is enabled at any particular time by signals on the Control bus.

CHAPTER 4

BNI (Trunk) Cards

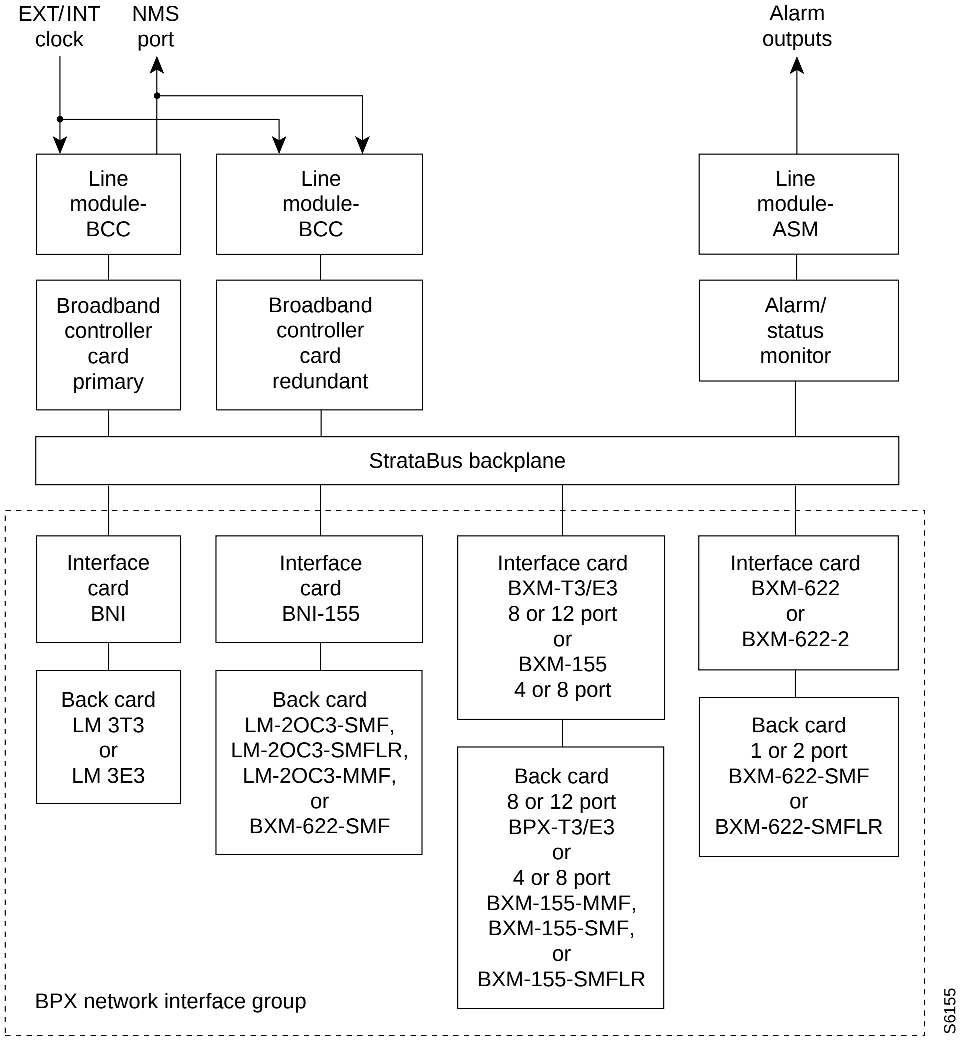
This chapter describes the Broadband Network Interface (BNI) card and associated backcards:

- BPX Switch Network Interface Group
- Broadband Network Interface Cards (BNI-T3 and BNI-E3)
- T3 and E3 Line Modules (LM-3T3 and LM-3E3)
- OC-3, Line Modules (SMF, SMFLR, & MMF)
- Y-Cabling of BNI Backcard, SMF-2-BC

BPX Switch Network Interface Group

The BPX switch network interface group of cards provides the interface between the BPX switch and the ATM network (see Figure 4-1).

Figure 4-1 BPX Switch Network Interface Group


EXT/INT clock
NMS port
Alarm outputs
Line module-BCC
Line module-BCC
Line module-ASM
Broadband controller card primary
Broadband controller card redundant
Alarm/ status monitor
StrataBus backplane
Interface card BNI
Interface card BNI-155
Interface card BXM-T3/E3 8 or 12 port or BXM-155 4 or 8 port
Interface card BXM-622 or BXM-622-2
Back card LM 3T3 or LM 3E3
Back card LM-2OC3-SMF, LM-2OC3-SMFLR, LM-2OC3-MMF, or BXM-622-SMF
Back card 8 or 12 port BPX-T3/E3 or 4 or 8 port BXM-155-MMF, BXM-155-SMF, or BXM-155-SMFLR
Back card 1 or 2 port BXM-622-SMF or BXM-622-SMFLR
BPX network interface group
S6155

Broadband Network Interface Cards (BNI-T3 and BNI-E3)

The BNI-T3 and BNI-E3 interface the BPX switch with ATM T3 and E3 broadband trunks, respectively. These ATM trunks may connect to either:

- another BPX,
- an MGX 8220; or
- an MGX 8800

The BNI-3T3 back card provides three DS3 interfaces on one card. The BNI-E3 back card provides three E3 interface ports. The BNI back card types are very similar, differing only in the electrical interface and framing.

Any of the 12 general purpose slots may be used to hold these cards. Each BNI operates as a pair with a corresponding Line Module back card.

Features

The BNI card features include:

- BNI-T3 provides three broadband data ports operating at 44.736 Mbps.
  BNI-E3 provides three broadband data ports operating at 34.368 Mbps.
- BNI T3 trunks can transmit up to 96,000 cells per second.
  BNI E3 trunks can transmit up to 80,000 cells per second.
- BNI-T3 utilizes the Switched Megabit Data Service (SMDS) Physical Layer Convergence Protocol (PLCP).
- BNI-E3 utilizes the CCITT G.804 framing format.
- T3 and E3 provide up to 32 class-based queues for each port.
- 24,000 cell transmit buffer per port.
- 800 Mbps backplane speed.
- Two-stage priority scheme for serving cells.
- Synchronize the electrical interface to either the line or the BPX switch system timing.
- Recover timing from the line for synchronizing the BPX switch timing.
- Accumulates trunk statistics for T3, E3, and OC-3.
- Optional 1:1 card redundancy using Y-cable configuration for BNI T3 and E3.

Functional Description

The BNI T3 and E3 cards are functionally alike except for the two different electrical interfaces. Refer to illustrating the main functional blocks in the BNI-3T3 card.

The DS3 port interface on the BNI-T3 card is the DS3 Function Block, a Physical Layer Protocol Processor (PLPP) custom semiconductor device, which implements the functions required by the DS3 PLCP as defined in various AT&T™ technical advisories. This VLSI device operates as a complete DS3 transmitter/receiver. Each BNI-3T3 has three of these devices, one for each of the DS3 ports on the card.

In the **transmit** direction (from the BPX switching matrix towards the transmission facility, referred to as *egress*), the BNI performs these functions:

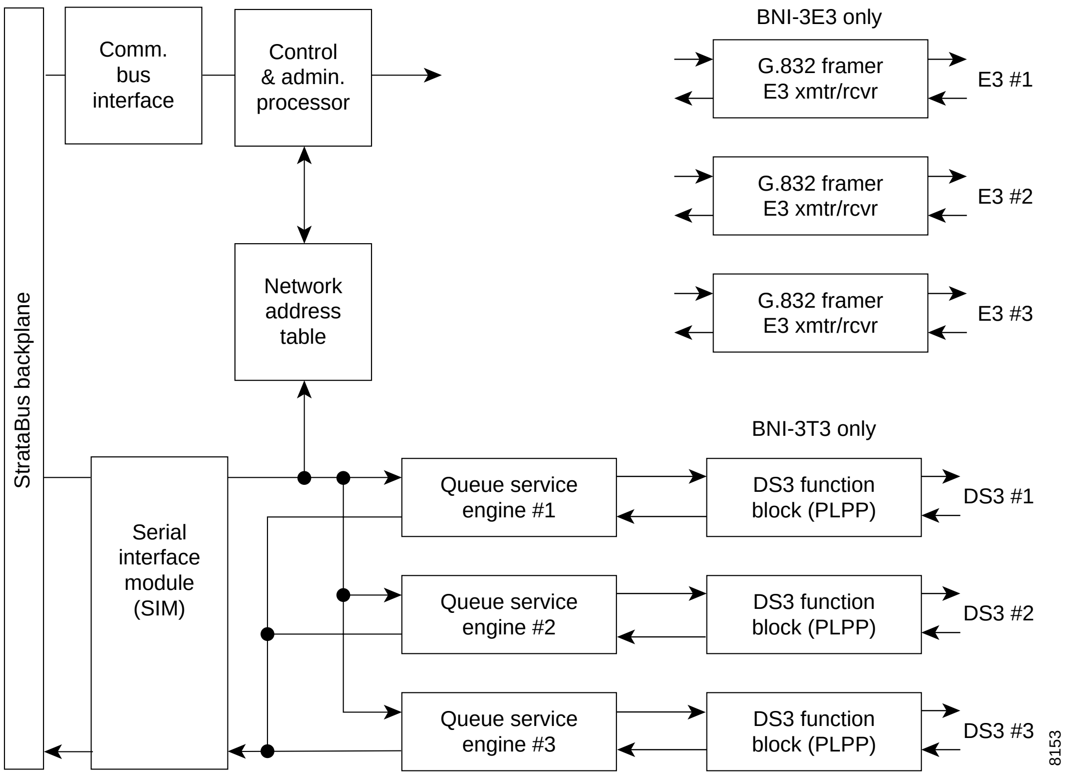
- Software controlled line buildout to match up to 900 feet (275 meters) of ABAM cable.
- Receives incoming cells from the switch matrix on the BCC.
- Queues and serves the cells based on the class-of-service algorithm.
- Sets congestion indication (EFCN) in cell header when necessary.
- Adds frame sync pattern and PLCP or G.804 overhead and transmits cells onto the T3 or E3 trunk.

In the **receive** direction (from the transmission facility towards the BPX switching matrix, sometimes referred to as *ingress*), the BNI performs these functions:

- Receives incoming ATM cells from the DS3 transmission facility, stripping the framing and overhead from the received bit stream.
- Determines the address of the incoming cells by scanning the Virtual Path Identifier (VPI)/Virtual Circuit Identifier (VCI) in the cell header.
- Queues the cells for transmission through the switch matrix.

- Extracts receive timing from the input framing and makes it available for node timing. Line can operate in looped timing mode.
- Recovers clock and data from the bipolar B3ZS (T3) or HDB3 (E3) line signal and converts data to unipolar.

Figure 4-2 Simplified BNI-T3, BNI-E3 Block Diagram


StrataBus backplane
Comm. bus interface
Control & admin. processor
Network address table
Serial interface module (SIM)
BNI-3E3 only
G.832 framer E3 xmtr/rcvr
E3 #1
G.832 framer E3 xmtr/rcvr
E3 #2
G.832 framer E3 xmtr/rcvr
E3 #3
BNI-3T3 only
Queue service engine #1
DS3 function block (PLPP)
DS3 #1
Queue service engine #2
DS3 function block (PLPP)
DS3 #2
Queue service engine #3
DS3 function block (PLPP)
DS3 #3
8153

Some of the functions performed by the PLPP in the BNI-3T3 include:

- PLPP—Receiver Side
  - Provides frame sync for either the M23 or C-bit parity frame format.
  - Provides alarm detection and accumulates B3ZS code violations, framing errors, parity errors, C-bit parity errors, and far end bit error (FEBE) events.
  - Detects far end alarm channel codes, yellow alarm, and loss of frame.
  - Provides optional cell descrambling, header check sequence (HCS) error detection, and cell filtering.
  - Small receive FIFO buffer for incoming cells.
- PLPP—Transmitter Side
  - Inserts proper frame bit sequence into outgoing bit stream.
  - Inserts proper alarm codes to be transmitted to the far end.
  - Provides optional ATM cell scrambling, HCS generation and insertion, and programmable null cell generation.
  - Small transmit FIFO for outgoing cells.

In the BNI-3E3 the PLPP is replaced by a G.804 framer. The E3 framer obtains end-to-end synchronization on the Frame Alignment bytes. And a E3 transmitter/receiver replaces the DS3 transmitter/receiver for the BNI-3E3.

Another major BNI function is queuing of the ATM cells waiting to be transmitted to the network trunk. This is controlled by the Queue Service Engine. There are 32 queues for each of the three ports to support 32 classes of service, each with its programmable parameters such as minimum bandwidth, maximum bandwidth, and priority. Queue depth is constantly monitored to provide congestion notification (EFCN) status. The Queue Service Engine also implements a discard mechanism for the cells tagged with Cell Loss Priority.

The destination of each cell is contained in the Virtual Path Identifier/Virtual Circuit Identifier VPI/VCI) field of the cell header. This is translated to a Logical Connection Number via table lookup in the Network Address Table. Both terminating and through connections can coexist on a port.

A Serial Interface Module (SIM) provides cell interface to the StrataBus backplane. This operates at 800 Mbps. It provides a serial-to-parallel conversion of the data and loopback and pseudo-random bit generation for test purposes.

Both BNI-T3 and BNI-E3 cards support two clock modes that are selected by the system operator through software control. Normal clocking uses receive clock from the network or user device for incoming data and supplies transmit clock for outgoing data. The clock obtained can be used to synchronize the node if desired. Loop timing uses receive clock from the network for the incoming data and turns that same clock around for timing the transmit data to the network or connecting CSU.

Bandwidth Control

The transmit bandwidth can be throttled down for certain applications. For example, when interfacing with an older IPX switch E3 ATM Trunk Card, the trunk transmit rate is limited to 40,000 cells/second. If a T2 trunk adapter is used, the trunk transmit rate is limited to 14,000 cells/second.

Loopbacks and Diagnostics

There are two types of self-tests that may be performed:

- A non-disruptive self test
  This is automatically performed on a routine basis.
- A more complete, disruptive test
  This may be initiated manually when a card failure is suspected. If the card self-test detects a failure, the card status LEDs displays an indication of the failure type.

Loopback paths are provided:

- A digital card loopback path
  This is used by the node for self-test. It loops the data at the serial DS3 or E3 interface back toward the node.
- A digital line loopback
  This loops the data at the electrical transmitter/receiver at the card output.

Internally, the PLPP circuit in the BNI-T3 has several loopbacks for use by diagnostic routines. These loopbacks loop the signal in both directions, toward the StrataBus as well as toward the output. Therefore, they can be used to support both near-end and far-end maintenance loopback testing:

- A digital loopback at the DS3 or E3 transmitter/receiver
  This checks both the transmit and receive signal paths in the near-end BNI card.

- A digital loopback capability on the BNI-3T3 to the PLPP processor
  This is used for the internal self test to basically check the operation of the signal processor.

When a trunk has been assigned to a BNI card but is not yet activated (upped), it is put in a loopback mode and a diagnostic test is continuously performed. This loopback is disruptive so it cannot be performed on a card that has an active trunk. This diagnostic test checks the data path through the BNI out to the BCC, through the switch matrix, and back to the BNI.

Active trunks are constantly checked by the Communications Fail test routine which is part of system software.

Front Panel Indicators

The lower section of the BNI front panel (see Figure 4-3) has a three-section, multicolored LED to indicate the card status. The card status LED is color-coded as indicated in Table 4-1.

At the upper portion of the front panel, there is a three-section multicolored LED to indicate the status of the three ports on the BNI. Types of failures are indicated by various combinations of the card status indicators as indicated in Table 4-2.

Table 4-1 BNI Front Panel Status Indicators

Status	LED color	Status Description
Port	off	Trunk is inactive and not carrying data.
	green	Trunk is actively carrying data.
	yellow	Trunk is in remote alarm.
	red	Trunk is in local alarm.
Card	green (act)	Card is on-line and one or more trunks on the card have been upped. If off, card may be operational but is not carrying traffic.
	yellow (stby)	The card is offline and in standby mode (for redundant card pairs). It might not have any upped trunks. If blinking, indicates card firmware or configuration data is being updated.
	red (fail)	Card failure; the card has failed self-test and/or is in a reset mode.

Figure 4-3 BNI-3T3 Front Panel (BNI-3E3 appears the same except for name)

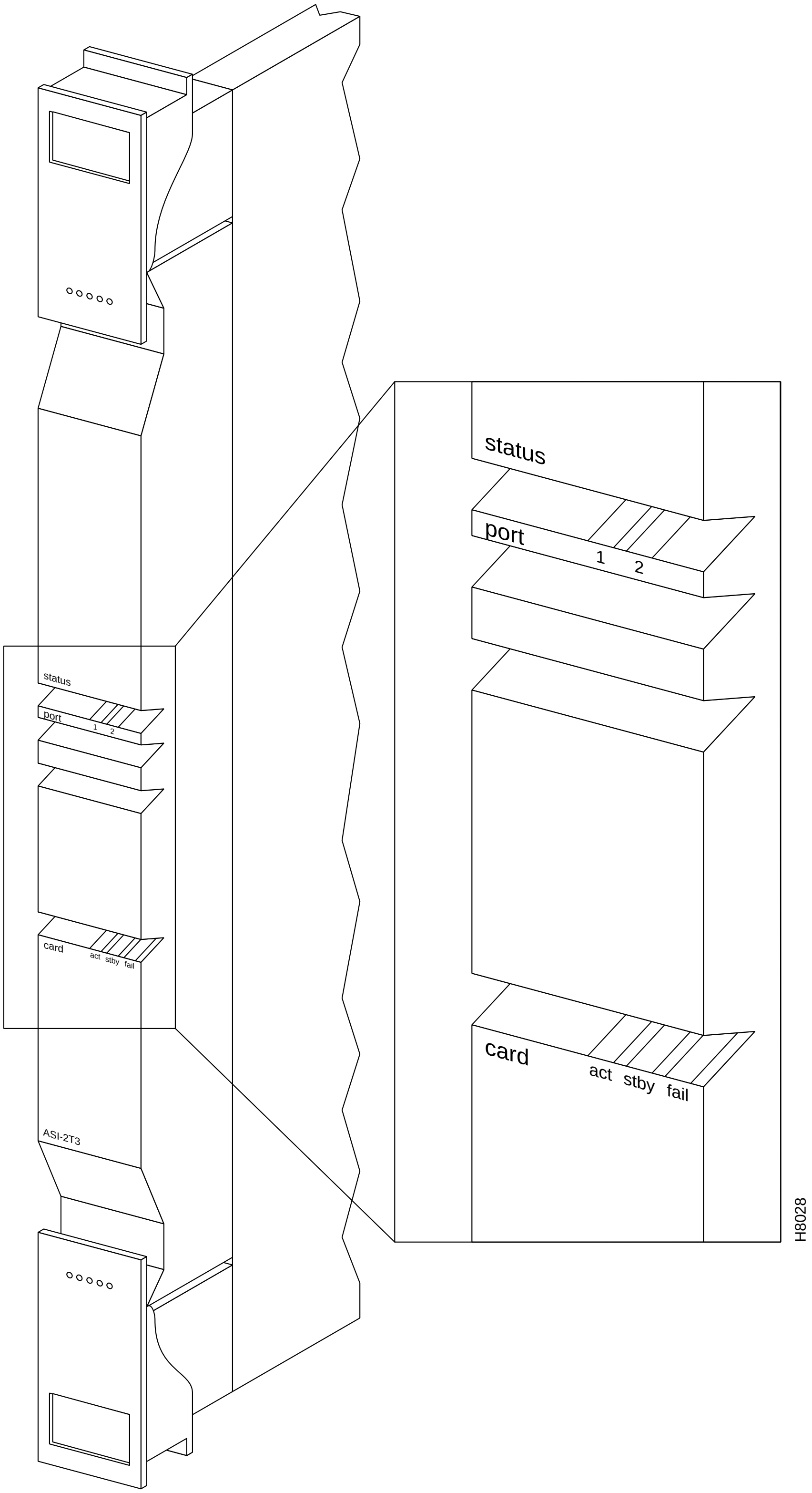


Table 4-2 BNI Front Panel Card Failure Indications

act	stby	fail	Failure Description
on	off	on	Non-fatal error detected; the card is still active.
off	on	on	Non-fatal error detected; the card is in standby mode.
off	blinking	on	Fatal error detected; the card is in a reboot mode.
on	on	on	The card failed boot load and operation is halted.

T3 and E3 Line Modules (LM-3T3 and LM-3E3)

The Line Modules for the BNI-T3 and BNI-E3 front cards are back cards used to provide a physical interface to the transmission facility. The LM-3T3 is used with the BNI-T3. The LM-3E3 with the BNI-3E3.

The Line Module connects to the BNI through the StrataBus midplane. You can make two adjacent cards of the same type redundant by using a Y-cable at the port connectors. All three ports on a card must be configured the same.

Refer to Figure 4-4, Figure 4-5, and Table 4-3 which describe the faceplate connectors of the LM-3T3 and LM-3E3. There are no controls or indicators.

The LM-3T3 and LM-3E3 provides these features:

- BNC connectors for 75-ohm unbalanced signal connections to the transmit and receive of each of the three ports.
- Transformer isolation from the trunk lines.
- Metallic relays for line loopback when in standby mode.

A final node loopback is at the end of the LM-3T3 or LM-3E3 card. This is a metallic loopback path that uses a relay contact closure. It is a near-end loopback path only; the signal is looped at the final output stage back to circuits in the node receive side. It is operated only when the corresponding front card is in standby.

Table 4-3 LM-3T3 and LM-3E3 Connectors

No	Connector	Function
1	PORT 1 RX - TX	BNC connectors for the transmit and receive T3/E3 signal to/from ATM trunk 1.
2	PORT 2 RX - TX	BNC connectors for the transmit and receive T3/E3 signal to/from ATM trunk 2.
3	PORT 3 RX - TX	BNC connectors for the transmit and receive T3/E3 signal to/from ATM trunk 3.

Figure 4-4 LM-3T3 Face Plate, Typical

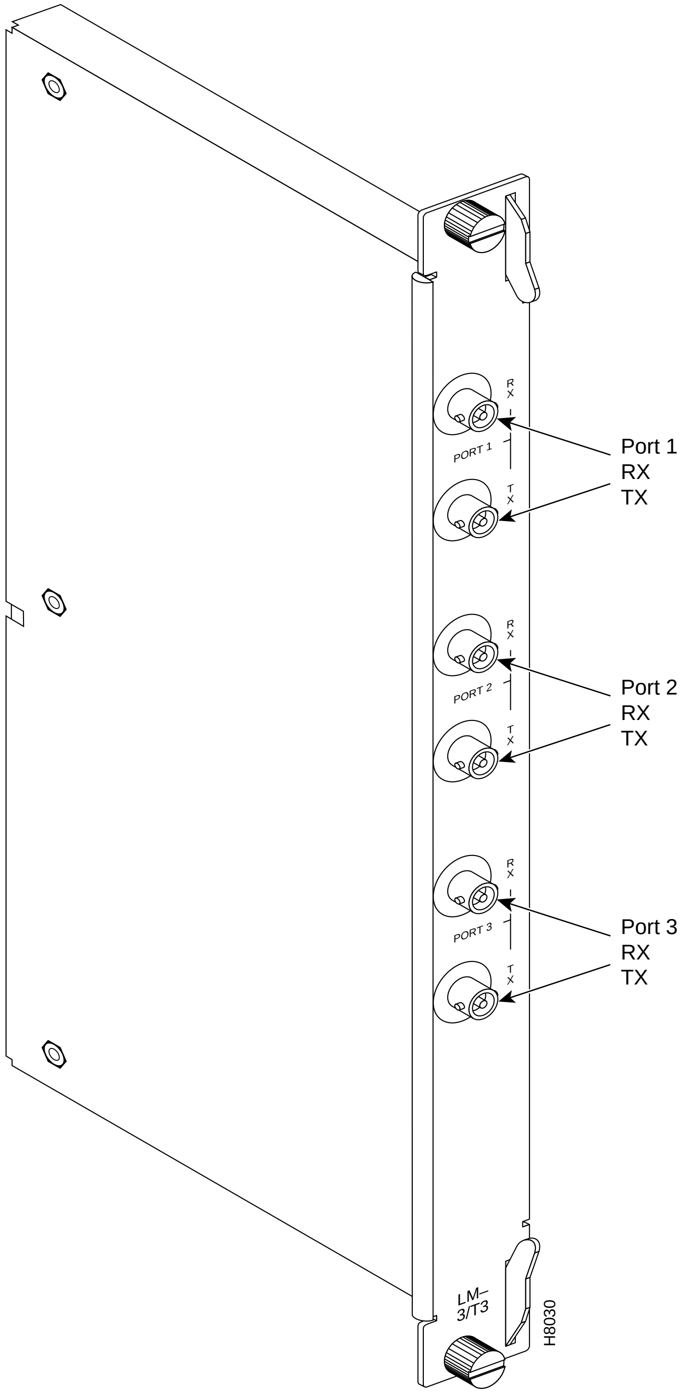
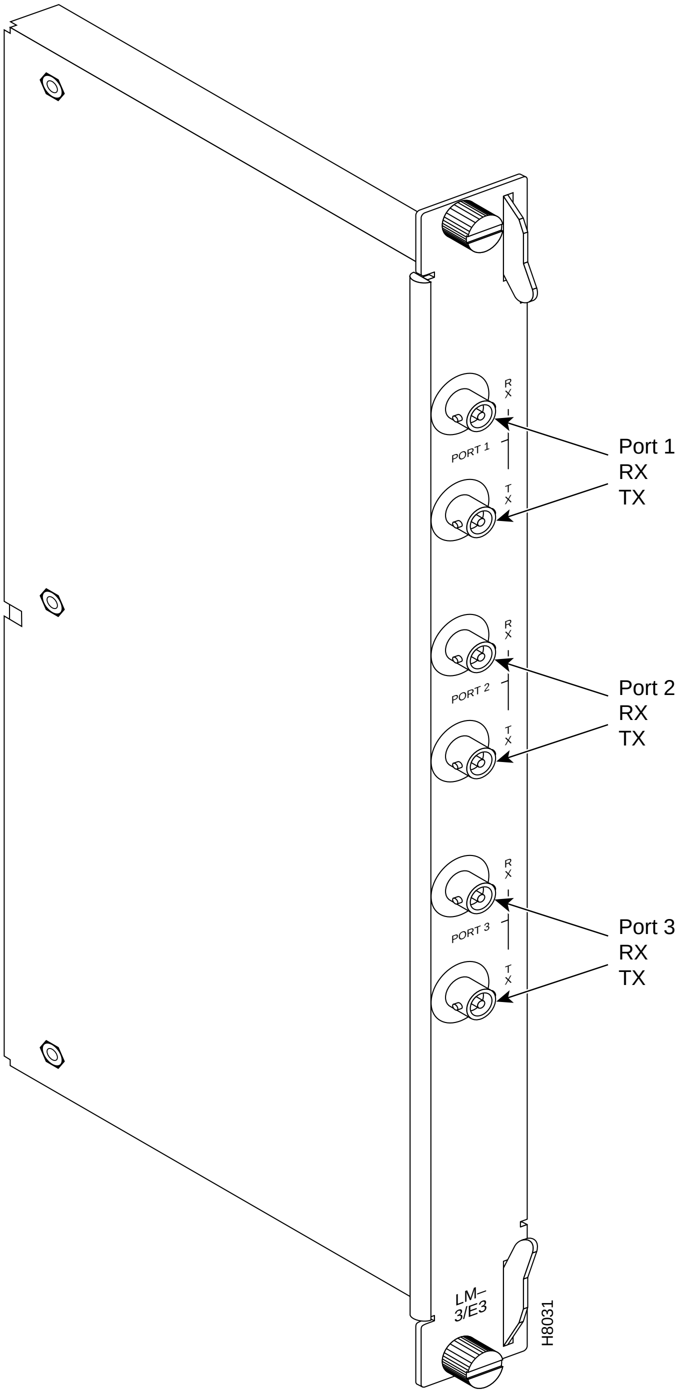


Figure 4-5 LM-3E3 Face Plate, Typical



OC-3, Line Modules (SMF, SMFLR, & MMF)

The Line Modules for the OC-3 BNI cards are back cards provide a physical interface to the transmission facility. There are three types:

- Single-mode fiber intermediate range
- Single-mode fiber long range
- Multimode fiber backcard

The Line Modules connect to the BNI through the StrataBus midplane.

For connector information, refer to Figure 4-6 and Table 4-4 for the LM-OC-3-SMF and to Figure 4-7 and Table 4-5 for the LM-OC-3-MMF.

The LM-OC-3-SMFLR uses the same type of connectors as the LM-OC-3-SMF.

Table 4-4 LM-OC-3-SMF and LM-OC-3-SMFLR Connectors

No	Connector	Function
1	PORT	FC-PC connectors for the transmit and receive OC-3 signal to/from ATM trunk 1.
2	PORT	FC-PC connectors for the transmit and receive OC-3 signal to/from ATM trunk 2.

Table 4-5 LM-OC-3-MMF Connectors

No	Connector	Function
1	PORT	Duplex SC connectors for the transmit and receive OC-3 signal to/from ATM trunk 1.
2	PORT	Duplex SC connectors for the transmit and receive OC-3 signal to/from ATM trunk 2.

Figure 4-6 LM-2OC-3-SMF Face Plate

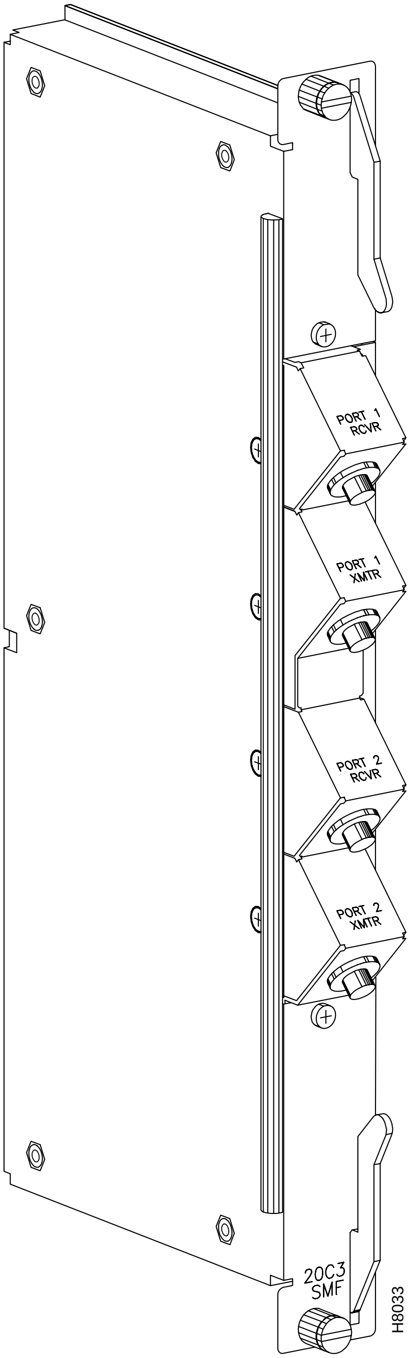
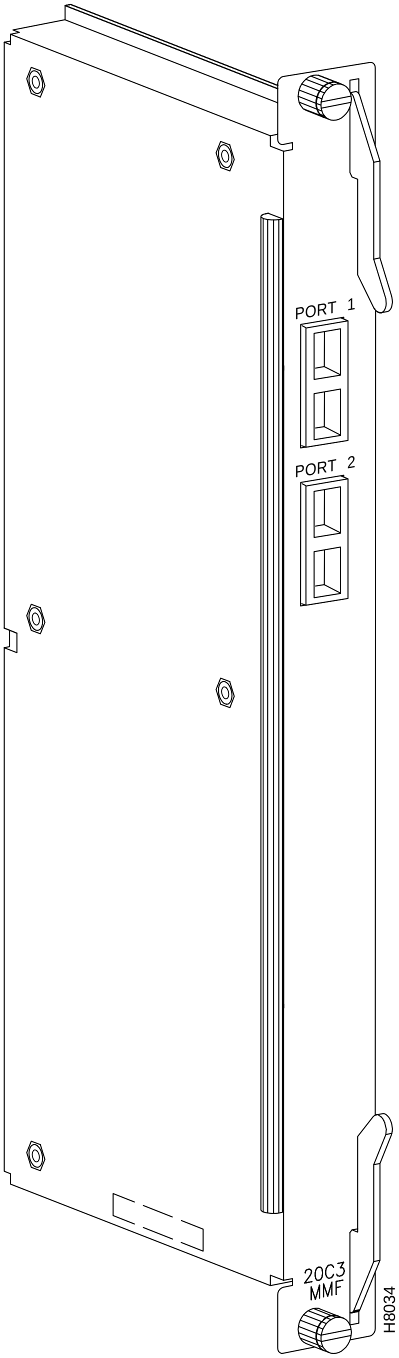


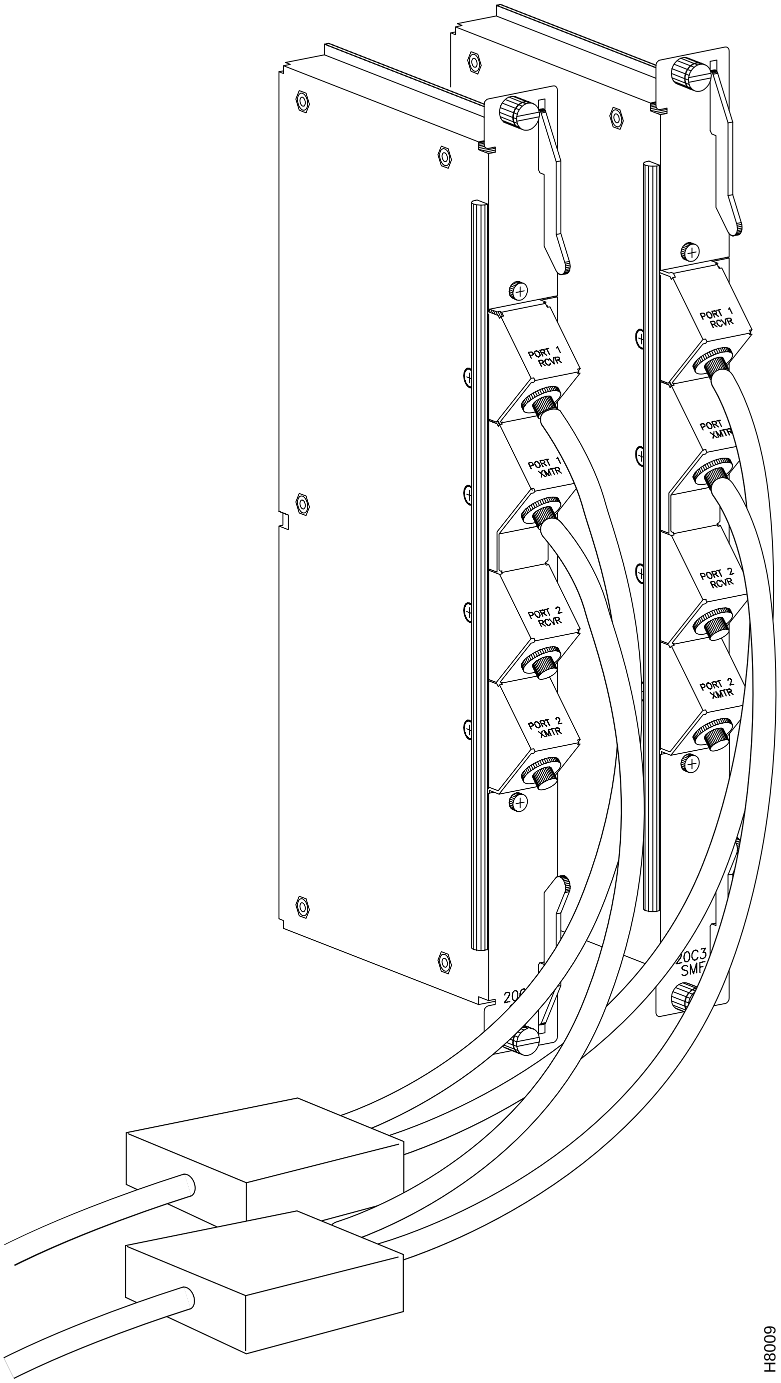
Figure 4-7 LM-2OC-3-MMF Face Plate



Y-Cabling of BNI Backcard, SMF-2-BC

The LM-OC-3-SMF (Model SMF-2-BC) backcards may be Y-cabled for redundancy by using the Y-Cable splitter shown in Figure 4-8. You must configure the cards for Y-Cable redundancy by using the **addyred** command.

Figure 4-8 Y-Cable (Model SMFY), LC-OC-3-SMF (Model SMF-2-BC)



CHAPTER 5

BXM Card Sets: T3/E3, 155, and 622

This chapter describes the physical BXM card sets, their major circuit functionality, and technical specifications:

- Overview: BXM Cards
- BXM Capabilities
- Enhanced BXM
- BXM Front Card Indicators
- BXM Backcard Connectors
- Automatic Protection Switching Redundancy
- BXM Functional Description
- Fault Management and Statistics
- Technical Specifications

The BXM set includes these cards:

- BXM T3/E3
- BXM-155
- BXM-622

The BXM cards may be upgraded to Enhanced BXM. Enhanced BXM cards improve upon the current BXM cards by delivering even more cost-effective ATM switching and traffic management. The Enhanced BXM cards support up to 12 ATM interfaces per card at speeds from T3/E3 to OC-12/STM-4.

The BXM cards may be configured for either:

- Trunk mode
  In Trunk mode, BXM cards provide BPX network interfaces.
- Service mode.
  In service (port UNI) mode, BXM cards provide service access to customer premise equipment.

The BXM cards support Multiple Protocol Label Switching (MPLS). For information on MPLS, refer to *The MPLS Controller Software Configuration Guide*.

Partitions for the BXM can be allocated between either:

- SVCs and PVCs, or
- Label switching virtual circuits (LVCs) and PVCs.

The BXM card supports dynamic resource partitioning to support the conversion of PVCs to soft permanent virtual circuits (SPVCs). This feature is described in *Cisco SES PNNI Controller Software Configuration Guide*.

Overview: BXM Cards

A BXM card set, using Application Specific Integrated Circuit (ASIC) technology, provides high speed ATM connectivity, flexibility, and scalability. The card set is comprised of a front card that provides the processing, management, and switching of ATM traffic and a back card that provides the physical interface for the card set.

An example of a BPX switch network provisioned with BXM-622 cards is shown in Figure 5-1.

The BXM card group includes:

- BXM-T3/E3
  Available in 8 or 12 port versions with T3/E3 interfaces.
- BXM-155
  Available in 4 or 8 port versions with OC-3/STM-1 interfaces.
- BXM-622
  Available in 1 or 2 port versions with OC-12/STM-4 interfaces.

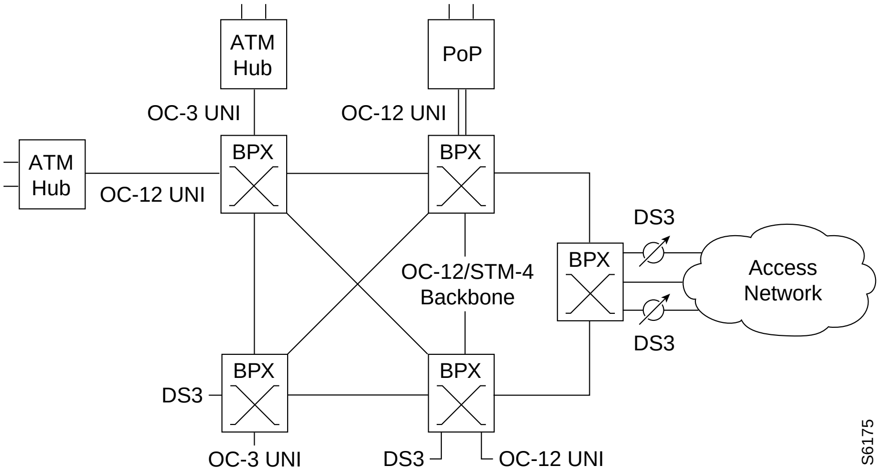
BXM cards may be configured to support either trunk (network) or port (service access) interfaces.

BXM cards are compliant with ATM UNI 3.1 and Traffic Management 4.0 including Abr VSVD and provide the capacity to meet the needs of emerging bandwidth driven applications.

For additional information on ATM Connections, refer to *Chapter 21, Configuring ATM Connections*.

The enhanced BXM-E card (version DX or EX) supports a higher connection density (32K) than either the legacy BXM or regular BXM-E cards. Both DX and EX versions have the same connection density, providing you with the ability to upgrade networks with the high connection density BXM-Es on trunk side, port side, or a combination of trunks and ports. You can smoothly upgrade BXM cards to BXM-E capabilities; see “Upgrade BXM to BXM-E Cards” in Appendix A, “Upgrade Information”

Figure 5-1 A BPX Switch Network with BXM Cards



The BXM cards are designed to support all these service classes:

- Constant Bit Rate (Cbr)
- Real time and no-real time Variable Bit Rate (rt-Vbr and nrt-Vbr)
- Available Bit Rate (Abr) with VSVD
- Available Bit Rate (Abr) without VSVD
- Abr with VSVD supports explicit rate marking and congestion indication (CI) control.
- Abr using Foresight
- Unspecified Bit Rate (Ubr).

All software and administration firmware for the BXM card is downloadable from the BCC and is operated by the BXM on-board sub-system processor.

A BXM card set consists of a front and back card:

- The BXM T3/E3 is available with a universal BPX-T3/E3 backcard in 8 or 12 port versions.
- The BXM-OC-3 is available with 4 or 8 port multi-mode fiber (MMF), single mode fiber (SMF), or single mode fiber long reach (SMFLR) back cards.
- The BXM-OC-12 is available with 1 or 2 port SMF or SMFLR back cards.

Any of the 12 general purpose slots can be used for the BXM cards. The same backcards are used whether the BXM ports are configured as trunks or lines. Table 5-1 and Table 5-2 list the available front and back card options for the BXM-T3/E3, BXM-155, and BXM-622.

Table 5-1 BXM T3/E3, BXM-155, and BXM 622 Front Card Options

Front Card Model Number	No. of Ports	Cell Buffer (ingress/egress)	Connections per card	Back Cards
T3/E3 (45 Mbps/34 Mbps)				
BXM-T3-8	8	100K/130K	16K	BPX-T3/E3-BC
BXM-E3-8	8	100K/130K	16K	BPX-T3/E3-BC
BXM-T3-12	12	100K/230K	16K	BPX-T3/E3-BC
BXM-E3-12	12	100K/230K	16K	BPX-T3/E3-BC
OC-3/STM-1 (155.52 Mbps)				
BXM-155-8	8	230K/230K	16K	MMF-155-8 SMF-155-8 SMFLR-155-8
BXM-155-4	4	100K/230K	16K	MMF-155-4 SMF-155-4 SMFLR-155-4
OC-12/STM-4 (622.08 Mbps)				
BXM-622-2	2	230K/230K	16K	SMF-622-2 SMFLR-622-2 SMFXLR-622-2
BXM-622	1	130K/230K	16K	SMF-622 SMFLR-622 SMFXLR-622

*The BXM cards can be configured for either, but not both, trunk or service access (UNI) on a card by card basis. Once a card is so configured, all ports are either trunk or service interfaces until the card is reconfigured.

**The BPX-T3/E3-BC universal backcard supports 8 or 12 ports.

Table 5-2 BXM-T3/E3, BXM-155, and BXM-622 Back Cards

Back Card Model Number	No. of Ports	Description	Optical Range (less than or equal to)
T3/E3 (45 Mbps/34 Mbps)			
BPX-T3/E3-BC	8/12	Universal T3/E3 backcard for 8 or 12 port card configurations	n/a
OC-3/STM-1 (155.520 Mbps)			
MMF-155-8	8	Multi-Mode Fiber	2km
MMF-155-4	4	Multi-Mode Fiber	2km
SMF-155-8	8	Single-Mode Fiber	20km
SMF-155-4	4	Single-Mode Fiber	20km
SMFLR-155-8	8	Single-Mode Fiber Long Reach	40km
SMFLR-155-4	4	Single-Mode Fiber Long Reach	40km
OC-12/STM-4 (622.08 Mbps)			
SMF-622-2	2	Single-Mode Fiber	20km
SMF-622	1	Single-Mode Fiber	20km
SMFLR-622-2	2	Single-Mode Fiber Long Range	40km
SMFLR-622	1	Single-Mode Fiber Long Range	40km

BXM Capabilities

Here are some of the major features of the BXM cards:

- Virtual Path (VP) as well as Virtual Circuit (VC) connections.
- Support both PVC and SVC connections.
- Connections supported per card:
  - 16,000 to 32,000 connections per card depending on configuration.
- BXM, T3/E3 ATM with 8 or 12 ports, either T3 at a 44.736 Mbps rate, or E3 at a 34.368 rate.
- BXM, OC-3/STM-1 ATM: four or eight ports, with each port operating at a 155.52 Mbps rate, 353,208 cells per second (full OC-3 rate).
- BXM, OC-12/STM-4 ATM: one or two ports, with each port operating at a 622.08 Mbps rate, 1,412,830 cells per second (full OC-12 rate).
- Selective Cell Discard.
- Up to 228,300 cell ingress (receive) buffers depending on card configuration.
- Up to 228,300 cell egress (transmit) buffers depending on card configuration.
- Cbr, Vbr, Abr, and Ubr service classes.

- For MFJ firmware and above, channel statistics level 0 is no longer supported for BXM-155-4, BXM-155-8, BXM-622, BXM-622-2, BXM-T3-12, BXM-T3-8, BXM-E3-8, and BXM-E3-12 models. However, it is still supported for all the other models (BXM-155-8DX, BXM-155-8D, BXM-155-4DX, BXM-155-4D, BXM-622-2DX, BXM-622-2D, BXM-622-DX, BXM-T3-12EX, BXM-T3-12E, BXM-T3-8E, BXM-E3-12EX, BXM-E3-12E, and BXM-E3-8E).
- ATM cell structure and format per ATM Forum UNI v3.1.
- Loopback support.
- 1:1 card redundancy using Y-cable configuration.
- A BXM card may be configured for either network or port (access) operation.

ATM Layer

- UNI port option conforming to ATM Forum UNI v3.1 specification.
- ATM cell structure and format supported per ATM UNI v3.1 and ITU I.361.
- Header Error Correction (HEC) field calculation and processing supported per ITU I.432.
- Usage Parameter Control using single and dual leaky bucket algorithm, as applicable, to control admission to the network per ATM Forum 4.0 Traffic Management.
- Provides up to 16 CoS's with the following configurable parameters:
  - Minimum service rate
  - Maximum queue depth
  - Frame discard enable
  - Cell Loss Priority (CLP) High and Low thresholds
  - Service priority level
  - Explicit Forward Congestion Indication (EFCI) threshold
- Per VC Queuing
- Support for Ubr CoS with Early Packet Discard
- Failure alarm monitoring per T1.64b
- ATM layer OAM functionality
- Congestion control mechanisms
  - Abr with Virtual Source Virtual Destination (VSVD)
  - Abr with Explicit Rate (ER) stamping/EFCI tagging
  - Abr with ForeSight
- Self-test and diagnostic facility.

Service Types

The BXM cards support the full range of ATM service types per ATM Forum TM 4.0.

Cbr Service:

- Usage Parameter Control (UPC) and Admission Control
- UPC: Ingress rate monitoring and discarding per I.371 for:

  - Peak Cell Rate (PCR)
  - Cell Transfer Delay Variation (CTDV)

Vbr Service:

- Usage Parameter Control (UPC) and Admission Control
- UPC: Ingress rate monitoring and cell tagging per ITU-T I.371 for:
  - Sustained Cell Rate (SCR)
  - Peak Cell Rate (PCR)
  - Burst Tolerance (BT)
- CLP tagging, enabled or disabled on a per VC basis at the Ingress side

Abr Service:

- Based on Virtual Source Virtual Destination (VSVD) per ATM Forum TM4.0
- VSVD
  - VSVDs provide Resource Management (RM) cell generation and termination to support congestion control loops
  - A virtual connection queue (VCQ) is assigned to a VC in the ingress direction
  - VCQ configurable parameters
  - CLP Hi and Lo thresholds

    Maximum queue depth

    Reserved queue depth

    Congestion threshold
- Abr congestion control

  Based on Explicit rate stamping/EFCI cell tagging and ingress rate monitoring per ITU-T I.371
  - Abr with Virtual Source Virtual Destination (VSVD)
  - Abr with Explicit Rate (ER) stamping/EFCI tagging
  - Abr with ForeSight

Ubr Service:

- Based on UPC and admission control including EPD
- Based on Explicit Rate Marking/EFCI cell tagging and ingress rate monitoring per ITU-T I.371

Minimum SCR and PCR

The minimum Sustainable Cell Rate (SCR) and Peak Cell Rate (PCR) of a connection supported by the BXM and UXM cards, including enhanced modes, was 50 cells per second (cps) or 19.2 Kbps. These values were set to maintain a policing accuracy with 1% when policing is performed on a BXM or UXM card. Because of this limitation, it was impossible to offer and differentiate connection services on a UXM or BXM at speeds less than 19.2 Kbps (50 cps).

In Release 9.3.0, the switch software supports connections with policing enabled and with SCR and PCR values as low as 12 cps on the BPX switch, with certain card limitations.

Use the **dspcd** command to determine if this feature is supported on a given slot.

Use the **addcon** command to set the minimum SCR and PCR values.

If these values are less than the minimum values supported on a given card, the command line interface will not allow you to set them until you have disabled policing. (A prompt will let you know about this limitation.)

Please refer to Table 5-1 for a list of cards that are supported by this feature and their performance specifications.

Table 5-3 Supported Cards and Performance Specifications

Card Name	Card Types	Minimum SCR and PCR, UPC/NPC Values
IGX-UXM	T1/E1	6 cps
IGX-UXM	IMA	6 cps
IGX-IUX	T3/E3	12 cps
IGX-UXM	OC3/STM-1	50 cps
BPX-BXM	T3/E3	12 cps
BPX-BXM	OC3/STM-1	50 cps
BPX-BXM	OC12/STM-4	50 cps
Note: The policing accuracy is always within 1%. The maximum SCR and PCR policing values are the same as the line rate.		

Policing must be disabled to support 6 cps and above for all BXM/UXM interface types.

Virtual Interfaces

- VPI/VCI used to identify virtual connection
- Support for up to 32 virtual interfaces per card, each with 16 CoS queues
- Virtual Interface parameters
  - Physical port (trunk or access)
  - Peak Service Rate (PSR)
  - Minimum Service Rate (MSR)
  - Maximum resource allocation

Virtual Ports

Virtual ports support hierarchical egress traffic shaping at more than one level on a single UNI port, combining virtual path traffic shaping and associated virtual connections. This feature allows one or more Virtual Ports per Physical Port interface.

A maximum of 31 virtual ports are available per BXM card. Each port supports all Automatic Routing Management traffic types currently supported by physical ports. Up to 255 virtual ports are supported per BPX node (with BCC-4-128) and 144 ports (with BCC-3-64).

Enhanced BXM

The Enhanced BXM cards improve the current BXM cards by delivering even more cost-effective ATM switching and traffic management. The Enhanced BXM cards come in EX and DX versions, both including these key feature enhancements:

- **Support a greater cell storage capacity and a greater number of connections**
  - The cell memory has been increased on the Enhanced BXM cards to support even greater cell buffering to maximize bandwidth efficiency and cell/frame throughput in wide area networks.
  - Enhanced BXM cards support up to 12 ATM interfaces per card at speeds from T3/E3 to OC-12/STM-4.
  - The ACP processor memory is quadrupled
    ACP Processor memory is 64 Mbyte and the flash memory is doubled to 4 Mbyte on all Enhanced BXM cards to allow more headroom for feature addition and enhancement in the future.

  With a more powerful processor and more VC configuration memory in ATM cell switching subsystem, the EX and DX versions of Enhanced BXM cards meet the ever increasing demand for greater number of connections per interface. For each PVC terminating on the card, Enhanced BXM supports a full range of stats for usage-based billing at cell and frame levels, cell policing, EFCI marking, Abr RM cells, and OAM cells. Supporting a greater number of connections per interface translates to supporting a greater user density more cost effectively.

  This table provides detailed information about the number of connections and cell buffer size supported on different types of Enhanced BXM card:

Table 5-4 Enhanced BXM Cards

Model Number	Physical Interface	Number of Ports per Card	Ingress Cell Buffer (cells)	Egress Cell Buffer (cells)	Maximum Number of Connections per Card
BPX-BXM-155-8DX	OC-3c/STM-1	8	512K	512K	32K
BPX-BXM-155-8D	OC-3c/STM-1	8	256K	256K	16K
BPX-BXM-155-4DX	OC-3c/STM-1	4	256K	256K	32K
BPX-BXM-155-4D	OC-3c/STM-1	4	128K	256K	16K
BPX-BXM-622-2DX	OC-12c/STM-4	2	512K	512K	32K
BPX-BXM-622-2D	OC-12c/STM-4	2	256K	256K	16K
BPX-BXM-622-DX	OC-12c/STM-4	1	256K	256K	32K
BPX-BXM-E3-12EX	E3	12	256K	512K	32K
BPX-BXM-E3-12E	E3	12	128K	256K	16K
BPX-BXM-E3-8E	E3	8	128K	128K	16K
BPX-BXM-T3-12EX	T3	12	256K	512K	32K
BPX-BXM-T3-12E	T3	12	128K	256K	16K
BPX-BXM-T3-8E	T3	8	128K	128K	16K

- Support an improved traffic shaping granularity for each virtual interface (VI) to allow any desired shaping rate.

On regular BXM cards, the VI traffic shaping rate is limited to OC-12/n, where n is an integer. On the Enhanced BXM cards, the VI traffic shaping rate can be any desired shaping rate with a precision of 9-bit mantissa and 4-bit exponent.

- Provide Abr support for connections with non-AAL5 traffic

  On the current BXM cards, the Abr support is limited to connections with AAL5 traffic. These connections allow early packet discard to be applied to avoid queue congestion and thus maintain RM cell flow. The Enhanced BXM cards extend the Abr support to connections with non-AAL5 traffic also. The Enhanced BXM cards minimize the problem of RM cell discard when RM cells are injected into a congested VC by reserving room for 8 RM cells even when the VC begins to drop data cells. The RM cell reserve can be globally configured for VSVD and non-VSVD connections.

- Support unidirectional ForeSight connections

  On the current BXM cards, the ForeSight Abr (Cisco's pre-standard Abr implementation) support is limited to bi-directional connections only. The current BXM cards also support ATM Forum standard Abr for both bi-directional and unidirectional connections. The Enhanced BXM cards will extend the ForeSight Abr support to include unidirectional connections also.

- Support interworking of the port Abr segment controlled with ATM Forum Abr algorithm and the network Abr segment controlled with ForeSight Abr algorithm.

  The Enhanced BXM cards will provide coupling between the port Abr segment with ATM Forum Abr algorithm and the network Abr segment with ForeSight Abr algorithm.

The Enhanced BXM cards include features that can be enabled by future firmware and switch software:

- Separate frame discard CLP0 and frame discard CLP1 thresholds for each Class-of-Service (CoS) queue

  The Enhanced BXM cards support separate frame discard CLP0 and frame discard CLP1 thresholds for each CoS queue. This feature enables preferential treatment for conforming traffic within CIR (frames with CLP=1 start-of-frame cell) compared to non-conforming traffic (frames with CLP=0 start-of-frame cell) when applying early packet discard (EPD).

- Merging of multiple frame-based VCs onto a single frame-based VC with future software upgrade

  The Enhanced BXM card hardware will support VC merge to facilitate label switching with simple software upgrade. With VC merge, the Enhanced BXM cards allow the BPX to aggregate multiple incoming frame based VCs with the same destination address into a single outgoing frame-based VC. Cells from different VCIs going to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

  Where VC merge occurs, several incoming labels indicated by VCIs are mapped to one single outgoing label. This sharing of labels reduces the total number of virtual circuits required for label switching. Without VC merge, each source-destination prefix pair consumes one label VC on each interface along the path. VC merge reduces the label space shortage by sharing labels for different flows with the same destination.

60K LCN Support for VSI on Enhanced BXM Cards

Overview

Definitions

BPX:Broadband Packet Exchange is a WAN Business Unit's high-end ATM switch. BPX is a carrier-quality switch, with trunk and CPU hot standby redundancy.

BXM:Broadband Switch Module (BXM) are ATM cards for the BPX switch which use the Monarch chipset. Various different port configurations are supported by the BXM card: 8xDS3, 12xDX3, 4xOC3, 8xOC3, 1xOC12 or 2xOC12.

CLI:Command Line Interface

LCN:Each interface card in a BPX has a certain number of Logical Connection Number. A Logical Connection Number is used for each cross connect leg through the card in question.

VSIVirtual Switch Interface

Introduction

The enhanced BXM-E cards, model DX and EX support a higher number of LCNs (60K) than the legacy BXM or BXM-E model D and E. However, current SWSW caps the maximum number of LCNs that it can support to 32k; this means the total number of LCNs used by Autoroute connections and VSI connections cannot exceed the capped number of LCNs.

This project provides the BPX with the capability to support up to 60K LCNs for VSI connections while the maximum supported Autoroute LCNs remains unchanged at 32K.

Except otherwise stated, hereunder the term "legacy BXM" is used to stand for both legacy BXM and BXM-E model D or E, and the term "BXM-E" is used to represent DX or EX version of BXM-E which implies it supports 60K LCNs.

This document describes the feature content to support 60K LCN for VSI connections, and support hitless scaling from an active BXM-E configured in low VSI LCN density mode (32K) to higher VSI LCN density (60K) mode.

Purpose

The purpose of this project is to provides the customer with the ability to scale up their networks with the higher LCN density BXM-Es on trunk side, or port side, or a combination of ports and trunks. This high LCN density is only used for VSI connections.

Functional Description

Overview

This project is to provide the customer with the ability to scale up their VSI networks with the high connection density of BXM-Es on trunk side, or port side, or a combination of ports and trunks. This higher connection density is only used for VSI connections. It only requires the changes in SWSW, no firmware change is needed.

Currently, Autoroute and VSI connections share the same up boundary of LCN. When the BXM card comes up, it reports through 0X50 message about the "Number of Channels" and "Max Scheduler Channels". The Max Scheduler Channels is dependent on the BXM card type, e.g. regular BXM-E is 32K and enhanced BXM-E is 60K. The "Number of Channels" is dependent on the card type and

Channel Statistics Level. The up boundary of combined Autoroute/VSI LCN is capped from "Number of Channels" in the current SWSW. All reserved 64 management channels are located at the top of this LCN space. Table 1 shows relationship for Enhanced BXM-E card about Channel Statistics Level, reported Number of Channels, Up boundary of LCN in current SWSW and the Management channel range.

Relationship of Channel Statistics Level, reported Number of Channels and Up boundary of LCN in current SWSW for Enhanced BXM-E card

Channel Stats LevelNumber of Channels ReportedUp Boundary of LCN for AR+VSI in Current SWSW Management Channel Range

316K16K-64(16K-63) to 16K

232K32K-64(32K-63) to 32K

160K32K-64(32K-63) to 32K

060K32K-64(32K-63) to 32K

The management channels described in the table include:

1 APS channel,

12 LMI/ILMI channels,

12 IP relay channels,

15 VSI_IS channels

15 VSI_CVC channels

This project, via the execution of the cnfcdparm command as briefly described before, will move the management channels to the up end of 60K if the channel stats level is 0 or 1, change the up boundary of LCN for Autoroute and let VSI application use up to (60K-64) LCNs. Table 2 show the new channel relationship:

New channel relationship after this project in implemented

Channel Stats LevelNumber of Channels ReportedMax LCN for AutorouteMax LCN for VSI Management Channel Range

316K16K-6416K-64(16K-63) to 16K

232K32K-6432K-64(32K-63) to 32K

160K32K60K-64(60K-63) to 60K

060K32K60K-64(60K-63) to 60K

The new feature does not affect service. No existing Autoroute and VSI connections are required to be deleted and added later on. No Autoroute and VSI traffic is disrupted when the user is deploying this feature.

The existing CLI command cnfcdparm is modified to support this feature. It is straightforward to execute this command. The successful execution of this command will configure the VSI LCNs to 60K and reprogram the management channels accordingly.

Features/Benefits

Functions

The following is the highlights of the features provided by this project:

Provides the capability to support 60K VSI LCNs on BXM-E cards while giving the option for the user to keep the previous 32K LCNs configuration.

Provides the hitless upgrading from an active BXM-E configured in 32K LCN mode to 60K VSI LCN mode.

Provides the capability to tell if a BXM-E card is already scaled up to support 60K VSI LCN.

RESTRICTIONS

Scope and Inter-dependencies

Scope

This feature will be available on the BPX 9.3.30 SWSW revision, the BXM-E card must support 60K LCNs.

Environment

This feature will require:

BPX Switch Software Release 9.3.30 which is targeted for Q2’01

BXM-E model EX or DX hardware with firmware revision supporting VSI.

BCC-4 controller card.

Usage

MPLS or PNNI user who wants to increase the number of VSI LCNs for a BXM-E slot to 60K need to upgrade their Switch Software to this release.

User who currently has legacy BXM cards need to upgrade those to BXM-E cards (model EX or DX) following the procedure for “Hitless Upgrade of BXM to BXM-E” [3]. This procedure is documented in release 9.3.00 which applies to this release and onward. The result of this upgrade is that the maximum number of LCNs will still be capped at 32K.

The user can use the CLI command cnfcdparm <slot> 2 Y to scale up the VSI LCN to 60K for the <slot>. If the <slot> has been scaled up to support 60K VSI LCN and the BXM-E card in the <slot> is in Standby status, the user can scale that slot back to support 32K LCN by using CLI command cnfcdparm <slot> 2 N.

Compatibility

This feature is to allow an easy way to configure the VSI LCN to 60 K for BXM-E card. There is no issue of incompatibility whatsoever in this project. However, this project introduces new scenarios of mismatch for BXM cards:

When a BXM-E slot, which has been configured to support 60K VSI LCN, is replaced by another card with lower channel density, mismatch will be declared.

When BXM-E cards are configured as y-redundancy or 1+1 APS, these Y-red pairs have been configured for 60K VSI LCN support, if one card of Y-red pairs is replaced by another card with lower channel density, mismatch will be declared.

Limits

Even though the BXM-E card can support up to 60K channels (LCNs), the maximum number of LCNs for Autoroute connections supported per BXM-E card is still capped at 32 K.

Since current BXM-E firmware does not support VSI partition shrinking, after VSI LCN expanding, the configured VSI connections will be kept at previous LCN space, and all additional LCNs will be forcefully allocated to the valid partitions on the card using the rules described in section 5.3.

After BXM-E slot is configured to support 60K LCN for VSI, customer cannot hitlessly reconfigure the card back to support previous 32K LCN. This is to protect the existing Autoroute and VSI connections which may have used the extra LCNs beyond previous LCN spaces. Please refer to Table 1 and 2. The only way to scale back is to down all lines and trunks on that BXM-E card first then use cnfcdparm to configure the slot back to support 32K LCNs.

END OF NEW FEATURE

BXM Front Card Indicators

The BXM front panel has a three-section, multicolored “card” LED to indicate the card status. The card status LED is color-coded as indicated in Table 5-5. A three-section multi-colored “port” LED indicates the status of the ports.

A two-port BXM-622 is shown in Figure 5-2. An 8-port BXM-155 front card is shown in Figure 5-3. A 12-port BXM-T3/E3 is shown in Figure 5-4.

Types of failures are indicated by various combinations of the card status indicators as described in Table 5-6.

Table 5-5 BXM Front Panel Status Indicators

Status	LED color	Status Description
port	off	Trunk/line is inactive and not carrying data.
	green	Trunk/line is actively carrying data.
	yellow	Trunk/line is in remote alarm.
	red	Trunk/line is in local alarm.
card	green (act)	Card is on-line and one or more trunks/lines on the card have been upped. If off, card may be operational but is not carrying traffic.
	yellow (stby)	Card is off-line and in standby mode (for redundant card pairs). May not have any upped trunks/lines. If blinking, indicates card firmware or configuration data is being updated.
	red (fail)	Card failure; card has failed self-test and/or is in a reset mode.

Table 5-6 BXM Front Panel Card Failure Indicators

act	stby	fail	Failure Description
on	off	on	Non-fatal error detected; card is still active.
off	on	on	Non-fatal error detected; card is in standby mode.
off	blinking	on	Fatal error detected; card is in a reboot mode.
on	on	on	Card failed boot load and operation is halted.

Figure 5-2 BXM-622 Front Panel, Two-Port Card Shown

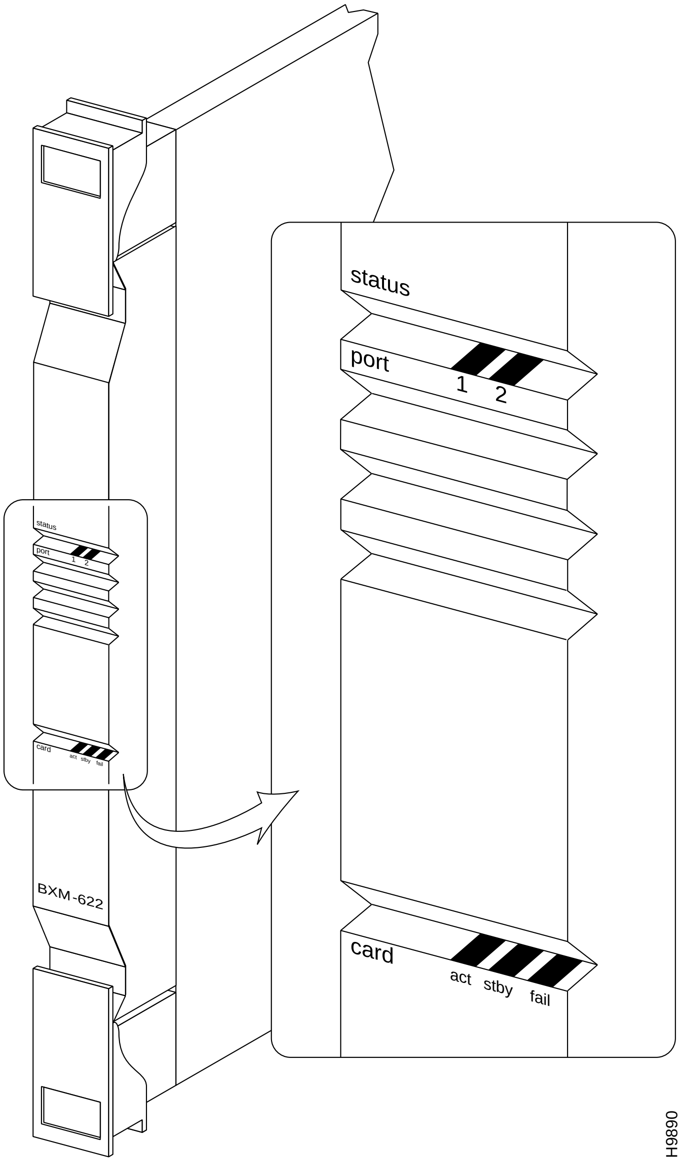


Figure 5-3 BXM-155 Front Panel, Eight-Port Card Shown

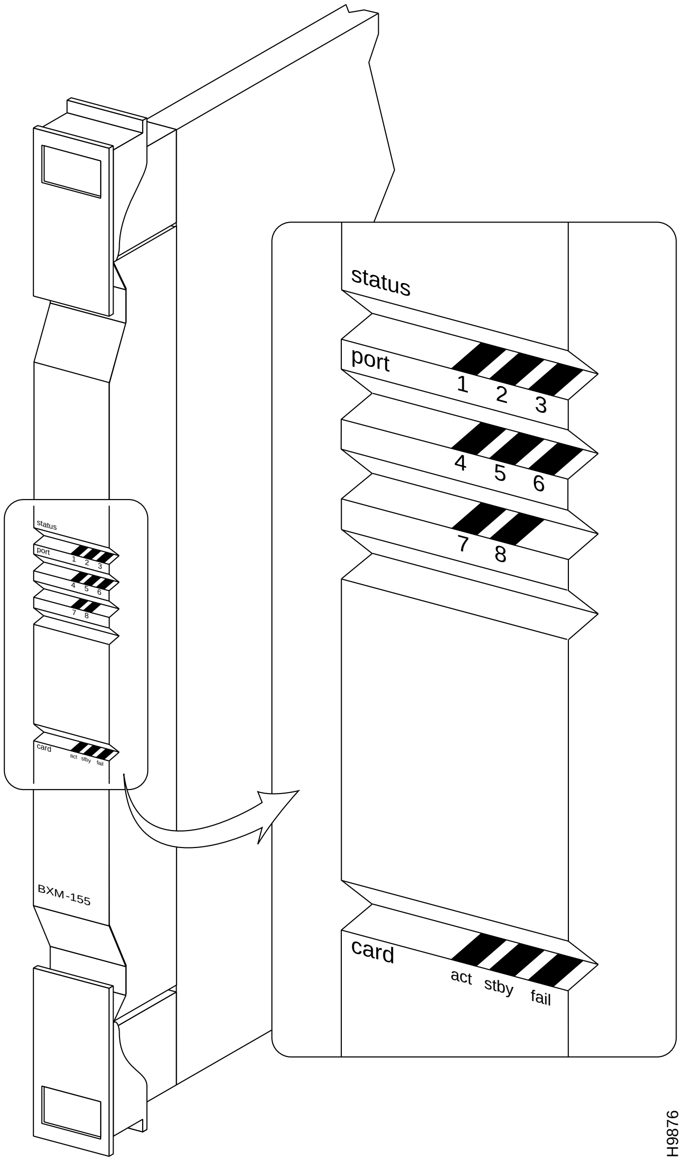
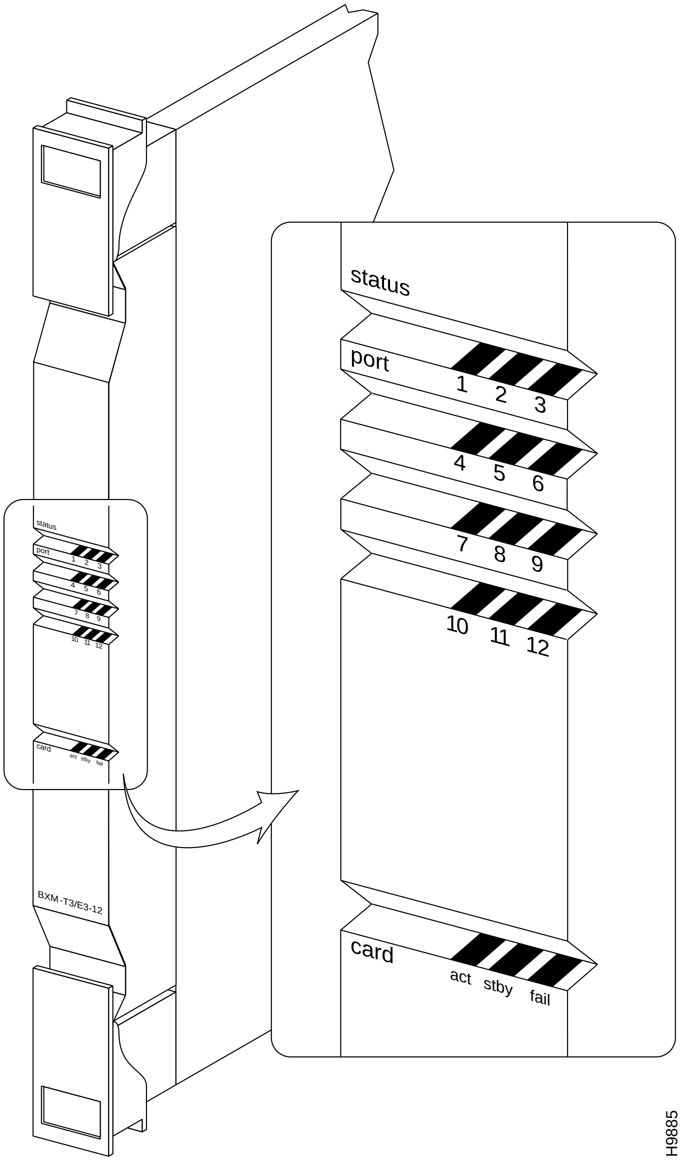


Figure 5-4 BXM-T3/E3 Front Panel, 12-Port Card Shown



BXM Backcard Connectors

The BXM backcards connect to the BXM front cards through the StrataBus midplane.

The BXM-622 is available in one or two port versions in either a single-mode fiber intermediate range (SMF) or a single-mode fiber long range (SMFLR) backcard. Connector information is listed in Table 5-7. A 2-port SMF card is shown in Figure 5-5.

Table 5-7 BXM-622 Backcards

No.	Connector	Function
1 or 2	PORT	Two FC connectors per port, one each for the transmit and receive signal.

The BXM-155 is available in four or eight port versions in a choice of multimode fiber (MMF), single-mode fiber intermediate range (SMF), or single-mode fiber long range (SMFLR) backcards. Connector information is listed in Table 5-8 and an 8-port SMF card is shown in Figure 5-6.

Table 5-8 BXM-155 Backcards

No.	Connector	Function
4 or 8	PORT	One SC connector per port, accommodates both the transmit and receive signals.

The BXM-STM1-4 is available in a four-port version that provides an electrical interface where the longer line lengths provided by the BXM optical backcards are not required. Connector information is listed in Table 5-9 and the backcard is shown in Figure 5-7.

Table 5-9 BXM-STM1-EL4 Backcard

No.	Connector	Function
4	PORT	Two SMB connectors per port, one each for the transmit and receive signals.

The BXM-T3/E3 is available in eight or twelve port versions. Connector information is listed in Table 5-10 and a 12-port T3/E3 card is shown in Figure 5-8.

Table 5-10 BXM-T3/E3 Backcards

No.	Connector	Function
8 or 12	PORT	Two SMB connectors per port, one each for the transmit and receive signals.

For SONET APS, card redundancy is provided by the use of two standard BXM front cards and two special backcards. The special backcards are the:

- SMF-155-4R or
- SMF-155-8R,
- SMF LR-4R or
- SMF LR-8R,
- SMF-622-1R or
- SMF-622-2R, or
- SMFLR-1R or
- SMFLR-2R.

The two backcards are connected together by a BPX Redundant Backplane which mates with the BPX Midplane. The connectors are the same as those for the standard backcards. An APS backcard is shown in (Figure 5-10, and the BPX Redundant Backplane is shown in (Figure 5-11).

Figure 5-5 SMF-622-2, SMFLR-622-2, and SMFXLR-622-2 Back Card

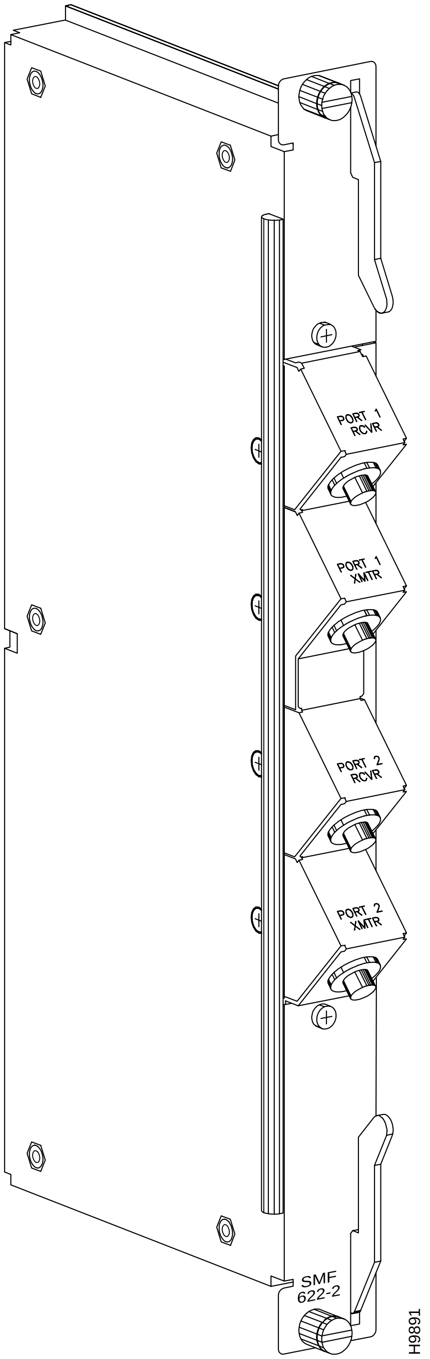


Figure 5-6 BXM-155-8 Port Backcard, MMF, SMF, or SMFLR

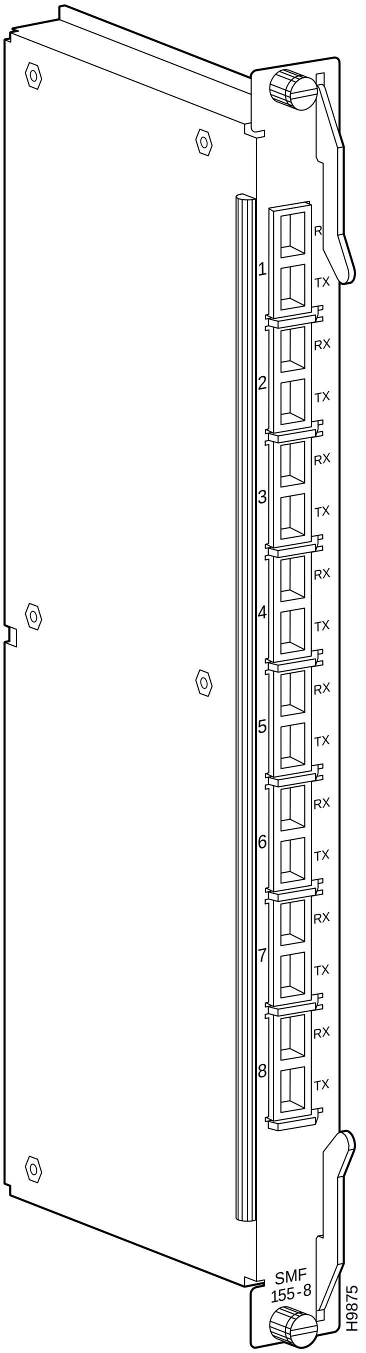


Figure 5-7 BPX-STM1-EL-4 Back Card

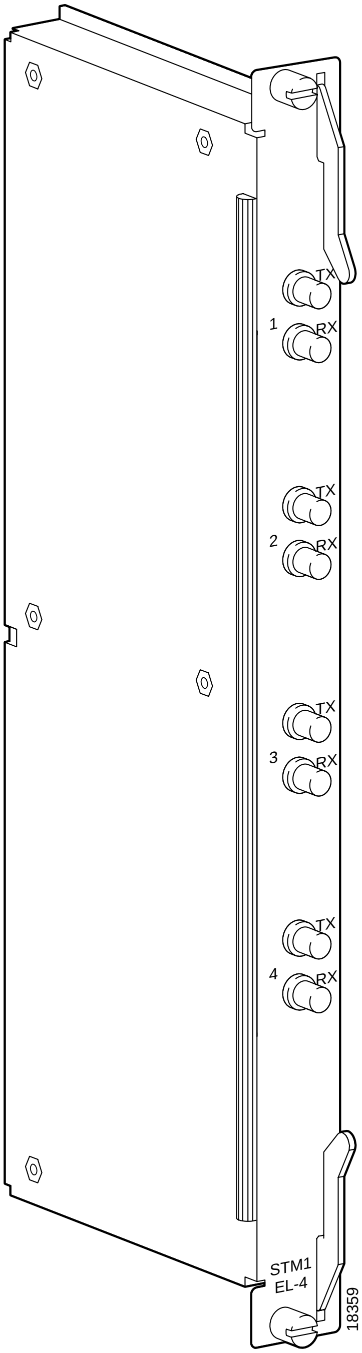
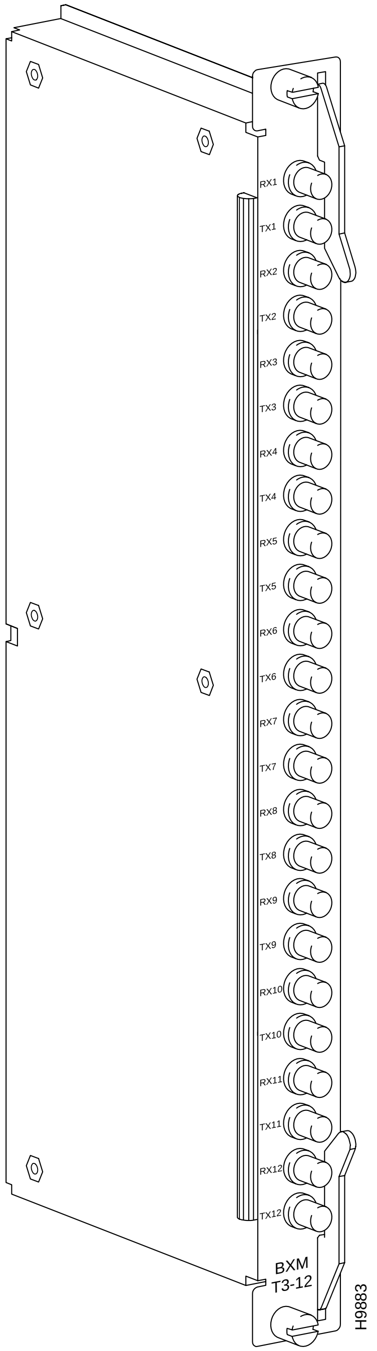


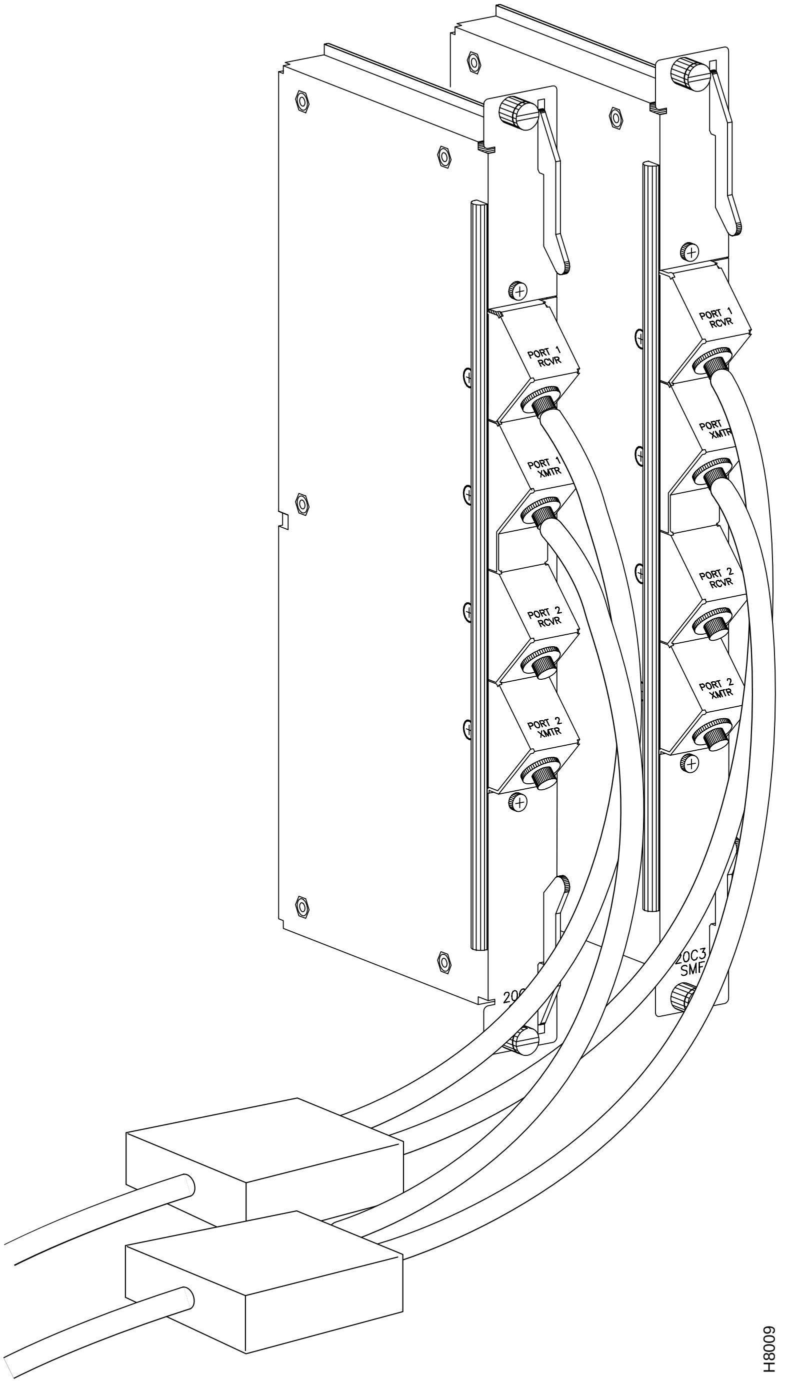
Figure 5-8 BPX-T3/E3 Back Card, 12-Port Option Shown



Y-Cabling of SMF-622 Series Backcards

You can Y-cable the SMF-622 series backcards for redundancy by using the Y-Cable splitter shown in Figure 5-9. To configure the cards for Y-Cable redundancy, use the **addyred** command.

Figure 5-9 Y-Cabling of SMF-622 Series Backcards



Automatic Protection Switching Redundancy

Automatic Protection Switching (APS) provides a standards-based line-redundancy for BXM OC-3 and OC-12 cards. The BXM OC-3 and BXM OC-12 cards support the SONET APS 1+1 and APS 1:1 standards for line redundancy. Line redundancy is provided by switching from the working line to the protection line.

The APS protocols supported by the BXM are listed in Table 5-11:

Table 5-11 BXM Sonet APS

APS 1+1	The APS 1+1 redundancy provides card and line redundancy, using the same numbered ports on adjacent BXM backcards.
APS 1:1	The APS 1:1 redundancy provides line redundancy, using adjacent lines on the same BXM backcard.

APS 1:1 redundancy provides line redundancy only and is supported with the standard BXM OC-3 and OC-12 front and back cards.

APS 1+1 redundancy provides both card and line redundancy. It uses the standard BXM OC-3 and OC-12 front cards, but uses a special APS Redundant Frame Assembly and APS Redundant backcards.

A backcard is shown in (Figure 5-10). The APS Redundant Frame Assembly is shown in (Figure 5-11). Two redundant backcards are connected together by the APS Redundant Frame Assembly. The APS Redundant Frame Assembly with associated APS redundant backcards is inserted as a unit in two appropriate backcard slots.

Refer to *Chapter 25, Configuring SONET Automatic Protection System*, for additional information.

Figure 5-10 BXM SMF-155-8R Backcard

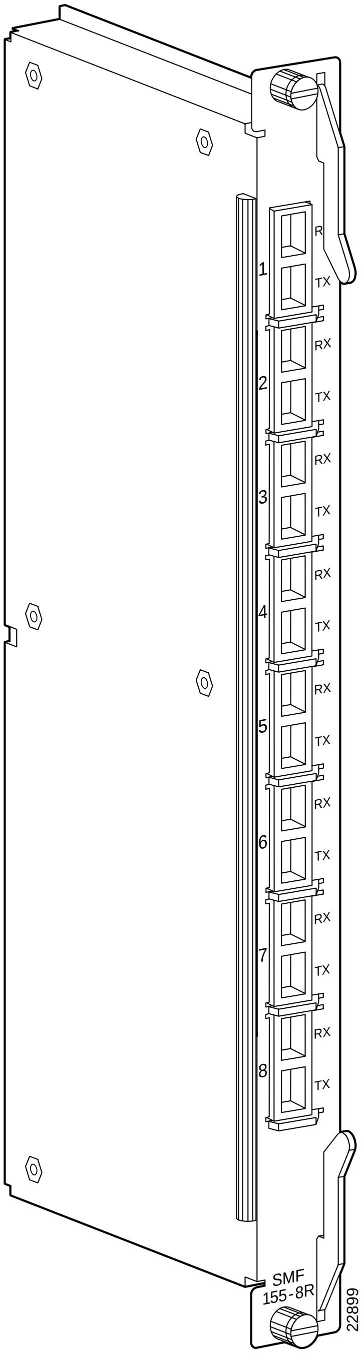
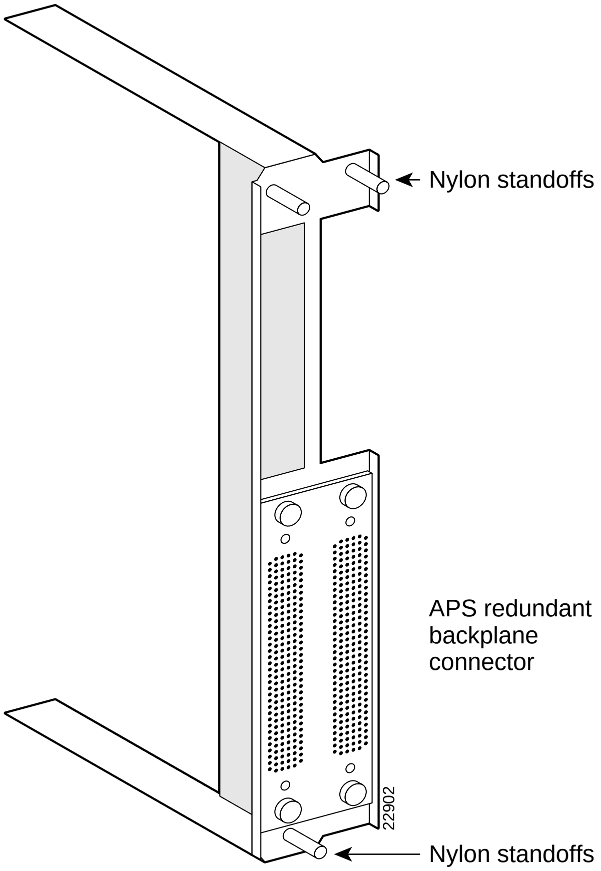


Figure 5-11 BXM APS Redundant Frame Assembly



BXM Functional Description

This functional description provides an overview of BXM operation.

Operation in Port (UNI) Mode

This section is an overview of operation when the BXM card's ports are configured in port (access) mode for connection to customer equipment.

The ingress flow of ATM cells from CPE into a BXM port when the card is configured for port (access) operation is shown in Figure 5-12.

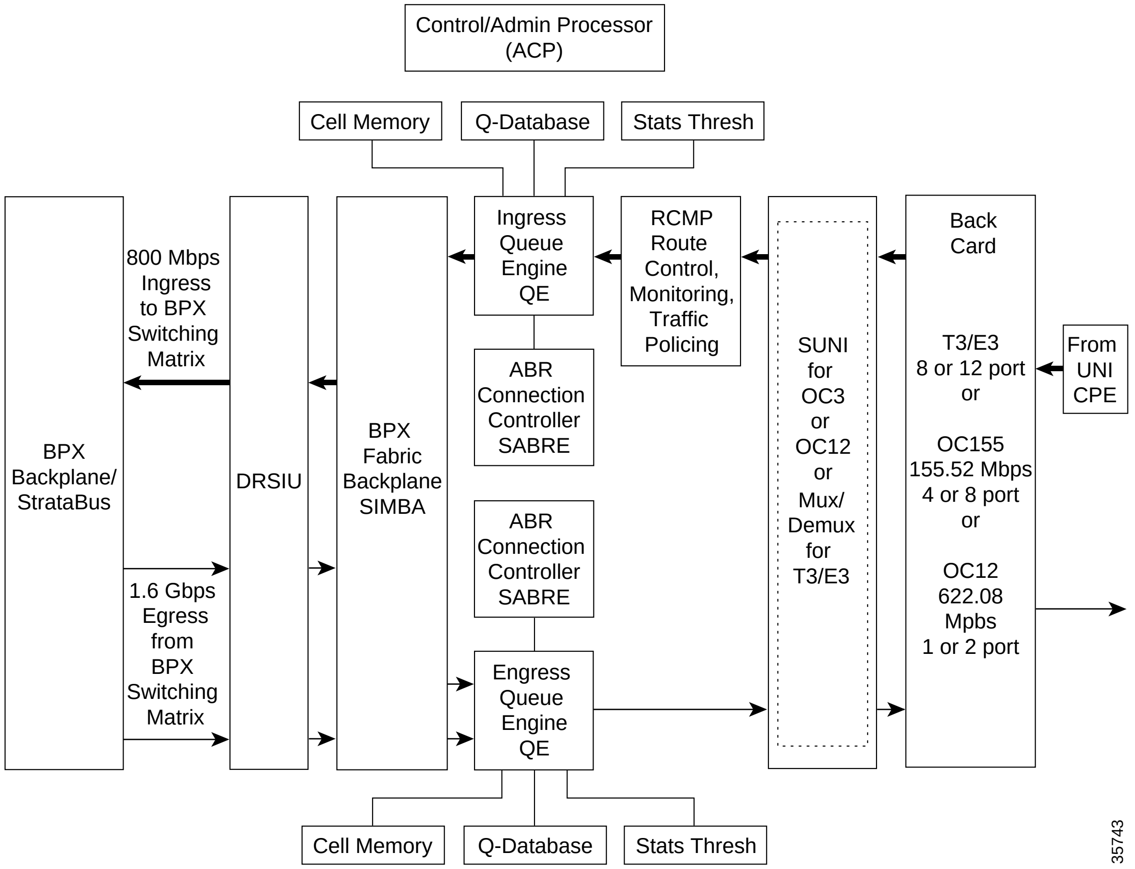
ATM cells from the customer premise equipment are:

- Processed at the physical interface level by the SUNI (OC-3/OC-12) or Mux/Demux (T3/E3),
- Served out via the BPX Backplane to the BPX crosspoint switch in an order of priority based on their connection type
- Policed per individual VC by the RCMP and
- Routed to applicable ingress queues

For Abr cells, additional functions are performed by the SABRE Abr connection controller, including: VSVD, Foresight, and virtual connection queueing.

Figure 5-12 BXM Port (Access UNI) Ingress Operation

SABRE	Scheduling and ABR Engine	SUNI	SONET/SDH UNI ASIC
SIMBA	Serial I/F and Multicast Buffer ASIC	ACP	Sub-system Processor
RCMP	Routing Ctl, Monitoring, & Policing ASIC	ASIC	Application Specific Integrated Ckt
DRSIU	Dual Receiver Serial I/F Unit		


Control/Admin Processor (ACP)
Cell Memory
Q-Database
Stats Thresh
BPX Backplane/ StrataBus
800 Mbps Ingress to BPX Switching Matrix
1.6 Gbps Egress from BPX Switching Matrix
DRSIU
BPX Fabric Backplane SIMBA
Ingress Queue Engine QE
ABR Connection Controller SABRE
ABR Connection Controller SABRE
Engress Queue Engine QE
RCMP Route Control, Monitoring, Traffic Policing
SUNI for OC3 or OC12 or Mux/ Demux for T3/E3
Back Card
T3/E3 8 or 12 port or
OC155 155.52 Mbps 4 or 8 port or
OC12 622.08 Mpbs 1 or 2 port
From UNI CPE
Cell Memory
Q-Database
Stats Thresh
35743

The egress flow of ATM cells out of the BXM when the card is configured for port (access) operation is shown in Figure 5-13.

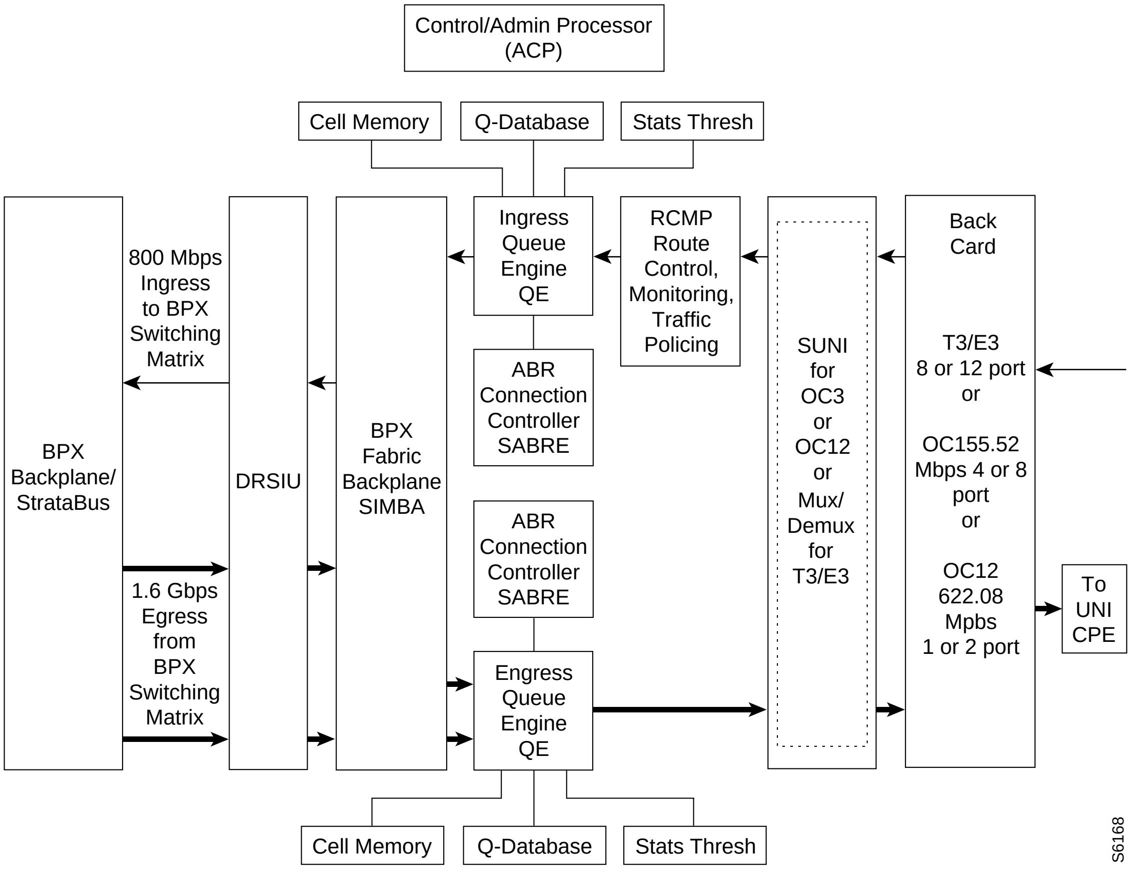
ATM cells are:

1. Routed to the BXM-622 via the BPX Backplane/Stratabus from the BPX crosspoint switch,
2. Applied to the DRSIU,
3. To an egress queue per class of service, and
4. Served out to the SUNI (OC-3/OC-12) or Mux/Demux (T3/E3)
5. Which processes the ATM cells into frames,
6. Processes the cells from the ATM layer to the physical, and
7. On out to customer premise equipment connected to the ports on the BXM backcard.

For Abr cells, additional functions are performed by the SABRE Abr connection controller, including: VSVD, Foresight, and virtual connection queueing.

Figure 5-13 BXM Port (Access, UNI) Egress Operation

SABRE	Scheduling and ABR Engine	SUNI	SONET/SDH UNI ASIC
SIMBA	Serial I/F and Multicast Buffer ASIC	ACP	Sub-system Processor
RCMP	Routing Ctl, Monitoring, & Policing ASIC	ASIC	Application Specific Integrated Ckt
DRSIU	Dual Receiver Serial I/F Unit		


Control/Admin Processor (ACP)
Cell Memory
Q-Database
Stats Thresh
BPX Backplane/ StrataBus
800 Mbps Ingress to BPX Switching Matrix
1.6 Gbps Egress from BPX Switching Matrix
DRSIU
BPX Fabric Backplane SIMBA
Ingress Queue Engine QE
ABR Connection Controller SABRE
ABR Connection Controller SABRE
Engress Queue Engine QE
RCMP Route Control, Monitoring, Traffic Policing
SUNI for OC3 or OC12 or Mux/ Demux for T3/E3
Back Card
T3/E3 8 or 12 port or
OC155.52 Mbps 4 or 8 port or
OC12 622.08 Mpbs 1 or 2 port
To UNI CPE
Cell Memory
Q-Database
Stats Thresh
S6168

Operation in Trunk Mode

This section is an overview of the operation of the BXM when the card is configured in the trunk mode for connection to another node or network.

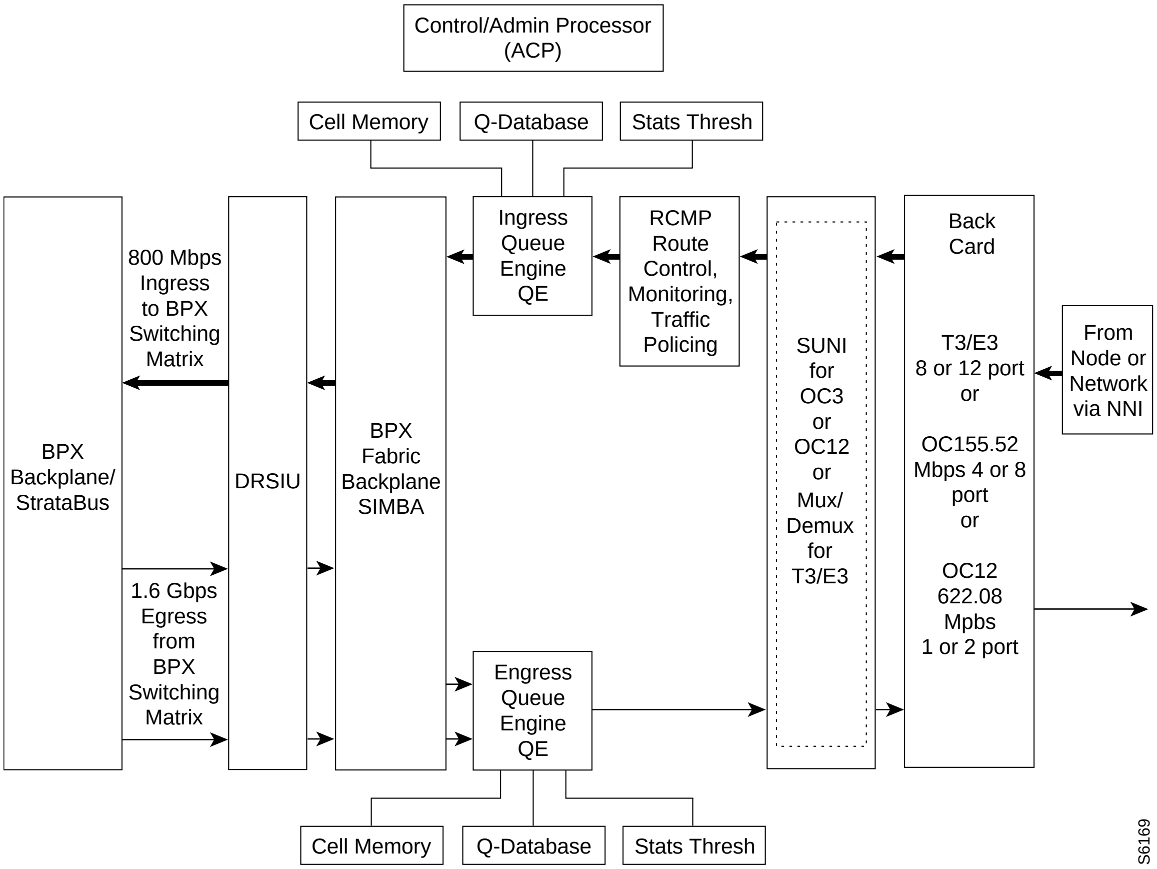
The ingress flow of ATM cells into the BXM when the card is configured for trunk operation is shown in Figure 5-14.

On ingress, ATM cells from a node or network are:

1. Processed at the physical interface level by the SUNI (OC-3/OC-12) or Demux/Mux (T3/E3)
2. Routed to applicable ingress slot queues
3. Served out to the BPX crosspoint switch via the BPX Backplane.

Figure 5-14 BXM Trunk Ingress Operation

SABRE	Scheduling and ABR Engine	SUNI	SONET/SDH UNI ASIC
SIMBA	Serial I/F and Multicast Buffer ASIC	ACP	Sub-system Processor
RCMP	Routing Ctl, Monitoring, & Policing ASIC	ASIC	Application Specific Integrated Ckt
DRSIU	Dual Receiver Serial I/F Unit		


Control/Admin Processor (ACP)
Cell Memory
Q-Database
Stats Thresh
BPX Backplane/ StrataBus
800 Mbps Ingress to BPX Switching Matrix
1.6 Gbps Egress from BPX Switching Matrix
DRSIU
BPX Fabric Backplane SIMBA
Ingress Queue Engine QE
RCMP Route Control, Monitoring, Traffic Policing
SUNI for OC3 or OC12 or Mux/ Demux for T3/E3
Back Card
T3/E3 8 or 12 port or
OC155.52 Mbps 4 or 8 port or
OC12 622.08 Mpbs 1 or 2 port
From Node or Network via NNI
Engress Queue Engine QE
Cell Memory
Q-Database
Stats Thresh
S6169

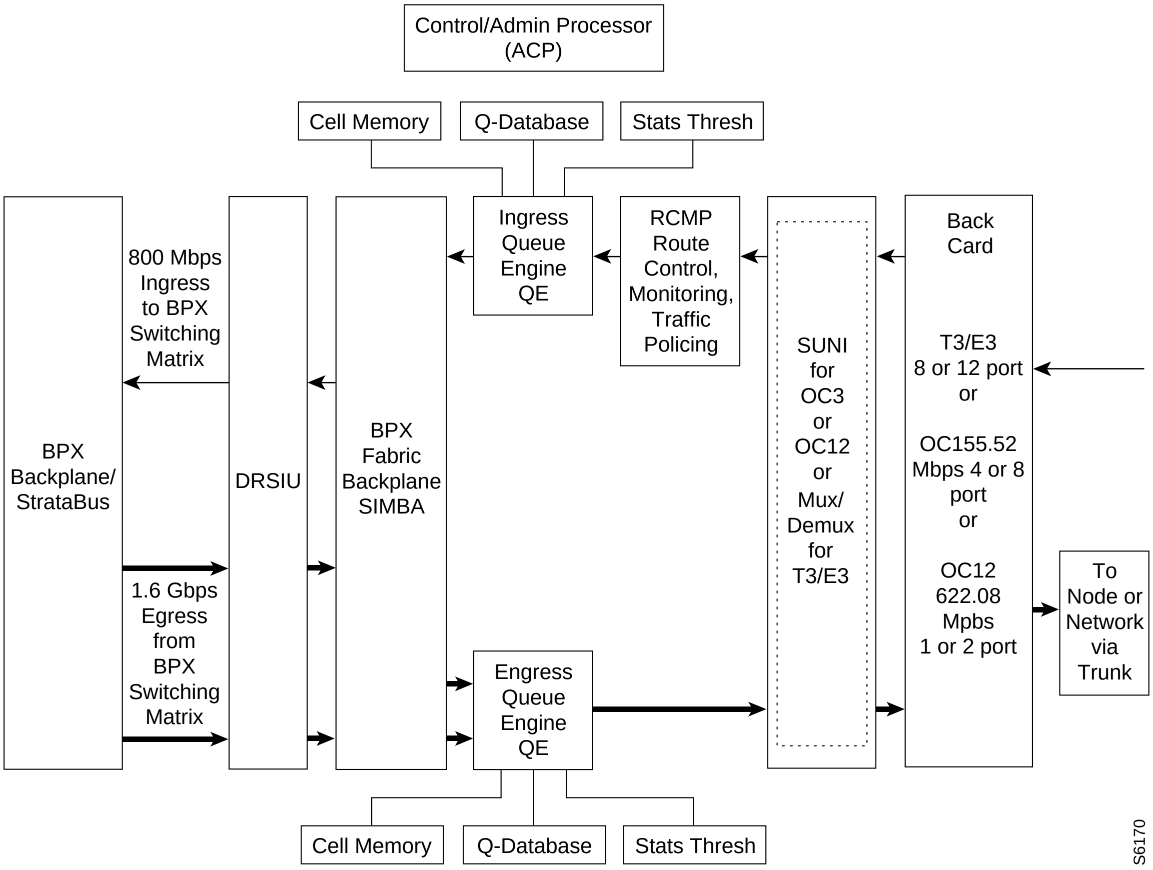
The egress flow of ATM cells out of the BXM when the card is configured for trunk operation is shown in Figure 5-15.

In egress, ATM cells are:

1. Routed to the BXM from the BPX crosspoint switch,
2. Applied to the DRSIU,
3. To an egress queue per class of service, and
4. Served out to the SUNI (OC-3/OC-12) or Demux/Mux (T3/E3).
5. The SUNI or Demux/Mux, as applicable, processes the ATM cells into frames,
6. Processing the cells from the ATM layer to the physical and
7. On out to the backcard trunk interface connecting to another node or network.

Figure 5-15 BXM Trunk Egress Operation

SABRE	Scheduling and ABR Engine	SUNI	SONET/SDH UNI ASIC
SIMBA	Serial I/F and Multicast Buffer ASIC	ACP	Sub-system Processor
RCMP	Routing Ctl, Monitoring, & Policing ASIC	ASIC	Application Specific Integrated Ckt
DRSIU	Dual Receiver Serial I/F Unit		


Control/Admin Processor (ACP)
Cell Memory
Q-Database
Stats Thresh
BPX Backplane/ StrataBus
800 Mbps Ingress to BPX Switching Matrix
1.6 Gbps Egress from BPX Switching Matrix
DRSIU
BPX Fabric Backplane SIMBA
Ingress Queue Engine QE
RCMP Route Control, Monitoring, Traffic Policing
SUNI for OC3 or OC12 or Mux/ Demux for T3/E3
Back Card
T3/E3 8 or 12 port or
OC155.52 Mbps 4 or 8 port or
OC12 622.08 Mpbs 1 or 2 port
To Node or Network via Trunk
Engress Queue Engine QE
Cell Memory
Q-Database
Stats Thresh
S6170

Detailed Description of Port (UNI) and Trunk Modes

This section is a summary of the principal functions performed by the major functional circuits of the BXM.

DRSIU

The DRSIU provides a total egress capacity from the BPX switch fabric of 1.6 Gbps.

SONET/SDH UNI (SUNI)

The SUNI ASIC implements the BXM physical processing for OC-3 and OC-12 interfaces. The SUNI provides SONET/SDH header processing, framing, ATM layer mapping and processing functions for OC-12/STM-4 (622.08 Mbps) or OC-3/STM1 (155.52 Mbps).

For ingress traffic, the BXM physical interface:

1. Receives incoming SONET/SDH frames,
2. Extracts ATM cell payloads, and
3. Processes section, line, and path overhead.

For egress traffic ATM cells are processed into SONET/SDH frames.

Alarms and statistics are collected at each level: section, line, and path.

DeMux/Mux

The Demux/Mux and associated circuits implement the BXM physical layer processing for T3/E3 interfaces, processing functions for T3 at a 44.736 Mbps rate or E3 at a 34.368 rate. It provides:

- header processing
- framing
- ATM layer mapping

RCMP

Usage Parameter Control (UPC) is provided by the RCMP. Each arriving ATM cell header is processed and identified on a per VC basis. The policing function utilizes a leaky bucket algorithm.

In addition to UPC and traffic policing, the RCMP provides route monitoring and also terminates OAM flows to provide performance monitoring on an end-to-end per VC/VP basis.

Traffic policing and UPC functionality is in accordance with the GCRA as specified by ATM Forum's UNI 3.1 using dual leaky buckets.

- Leaky Bucket 1 utilizes:
  - Peak Cell Rate (PCR)
  - Cell Delay Variation Tolerance: CDVT
- Leaky Bucket 2 utilizes:
  - Sustainable Cell Rate (SCR)
  - Maximum Burst Size (MBS)

In addition, two selective cell discard thresholds are supported for all queues for discard of CLP=1 cells should congestion occur.

SABRE

The Scheduling and Abr Engine (SABRE) includes both VSVD and Foresight dynamic traffic transfer rate control and other functions:

- ATM Forum Traffic Management 4.0 compliant Abr Virtual Source/Virtual Destination (VSVD).
- Terminates Abr flows for VSVD and Foresight control loops.

- Performs explicit rate (ER) and EFCI tagging if enabled.
- Supports Foresight congestion control and manages the designated service classes on a per VC basis with OAM processing.
- Supports OAM flows for internal loopback diagnostic self-tests and performance monitoring.
- Provides service queue decisions to the Ingress and Egress Queue Engines for per VC queues for Abr VCs.

Ingress and Egress Queue Engines

The overall function of the queue engines is to manage the bandwidth of trunks or ports (UNI) via management of the ingress and egress queues.

In addition to the Abr VS queues, the ingress queues include 15 slot servers, one for each of 14 possible BPX destination slots, plus 1 for multicast operation. Each of the 15 slot servers contains 16 Qbins, supporting 16 classes of service per slot server.

In addition to the Abr VS queues, the egress queues include 32 Virtual Interfaces (VIs). Each of the 32 VIs supports 16 qbins.

SIMBA

This serial interface and multicast buffer ASIC provides:

- ATM cell header translation.
- Directs ATM cells to the Egress Queue Engine with a 2 x OC-12c throughput capacity.
- Implements the multicast function in the egress direction, providing up to 4000 multicast connections.
- Translates standard OAM flows and Foresight cells.
- Optimizes backplane bandwidth by means of a polling mechanism.

ACP Subsystem Processor

The ACP performs these localized functions:

- Initializes BXM at power up
- Manages local connection databases
- Collects card, port, and connection statistics
- Manages OAM operation
- Controls alarm indicators (active, standby, fail)

All basic configuration data on the card is copied to the battery backup memory (BRAM) on the card so that in the event of a power outage, the card will retain its main configuration.

Fault Management and Statistics

Port (UNI) Mode

Compliant to Bellcore GR-253-CORE

Alarms:

- Loss Of Signal (LOS)
- Loss Of Pointer (LOP)
- Loss Of Frame (LOF)
- Loss Of Cell delineation (LOC)
- Alarm Indication Signal (AIS)
- Remote Defect Indication (RDI)
- Alarm Integration Up/down Count

Performance Monitoring:

- Performance monitoring provided for Line, Section, and Path
- Bit Interleaved Parity (BIP) error detection
- Far End Block Error (FEBE) count
- Unavailable Seconds (UAS)
- Errored Seconds (ES)
- Severely Errored Seconds (SES)
- Header Error Checksum (HCS) monitoring

Statistics:

- ATM statistics collected on a per VC basis
  - Two modes of statistics collection:

    Basic: collection of 4 statistics per VC per direction

    Enhanced: collection of 12 statistics per VC per direction

OAM

- Loopback support
- Generation and detection of AIS and RDI OAM cells
- Termination and processing of OAM cells

Trunk Mode

Compliant to Bellcore GR-253-CORE

Alarms:

- Loss Of Signal (LOS)
- Loss Of Pointer (LOP)
- Loss Of Frame (LOF)
- Loss Of Cell delineation (LOC)
- Alarm Indication Signal (AIS)
- Remote Defect Indication (RDI)
- Alarm Integration Up/down Count

Performance Monitoring:

- Performance monitoring provided for Line, Section and Path
- Bit Interleaved Parity (BIP) error detection
- Far End Block Error (FEBE) count
- Unavailable Seconds (UAS)
- Errored Seconds (ES)
- Severely Errored Seconds (SES)
- Header Error Checksum (HCS) monitoring

Statistics:

Process Monitoring for ATM Header Cell Processing

- Cells discarded due to Header Errors (LCN mismatch)

Miscellaneous ATM Layer Statistics

- Number of cell arrivals from port
- Number of cell arrivals with CLP = 1
- Number of cells transmitted to port
- Number of cells transmitted with CLP = 1

Technical Specifications

Physical Layer

- Trunk or port (access) interface mode.
- Compliant to SONET standards.
  - *Bellcore GR-253-CORE, TR-TSY-000020
  - *ANSI T1.105, T1E1.2/93-020RA

- Compliant to SDH standards.
  - *ITU-T G.707, G.708 and G.709
  - *ITU-T G.957, G.958
- 1:1 BXM redundancy supported using ‘Y’ redundancy.
- Fiber optic interface characteristics are listed in Table 5-12 and Table 5-13.

Table 5-12 Fiber Optic Characteristics OC-12

Back card	Source 1310 nm	Tx Power (dBm) Min	Max	Rx Power (dBm) Min	Max	Connection Type	Range (km)
SMF (IR)	Laser 1310 nm	-15	-8	-28	-8	FC	20
SMF (LR)	Laser 1310 nm	-3	+2	-28	-8	FC	40
SMF (E)	Laser 1550 nm	-3	+2	-28	-8	FC	40 plus

Table 5-13 Fiber Optic Characteristics OC-3

Back card	Source	Tx Power (dBm) Min	Max	Rx Power (dBm) Min	Max	Connection Type	Range (km)
MMF	LED	-22	-15	-31	-10	SC	2
SMF (IR)	Laser (Class 1)	-15	-8	-34	-10	SC	20
SMF (LR)	Laser (Class 1)	-5	0	-34	-10	SC	40

General Information

- Card dimensions: 19”(H) x 1.1”(W) x 27”(D)
- Weight: 6 lb (2.7kg)
- Power -48 V DC at 85 W
- EMI/ESD: FCC Part 15, Bellcore GR1089-CORE
- IEC 801-2, EN55022
- Safety: EN 60950, UL 1950
- Bellcore NEBS:Level 3 compliant
- Optical Safety:
  - Intermediate Reach IEC 825-1 (Class 1)
  - Long Reach IEC 825-1 (Class 36)

PART 2

Installation

CHAPTER 6

Installation Overview

This chapter is an overview of the configuration procedures in this manual:

- Summary: Installation Procedure
- Installation Sequence Flow
- Configuration: Lines, Trunks, and Connection

The installation tasks introduced here are explained in detail in subsequent chapters.

For a description of the commands used to initially set up a BPX switch, refer to the *Cisco WAN Switch Command Reference* and *Cisco WAN Switch SuperUser Command Reference*.

For additional information on network management and the graphical user interface recommended for configuring and provisioning, refer to the *Cisco WAN Manager* manual.

Summary: Installation Procedure

Step 1 Safety

Step 2 Site Preparation

Step 3 Unpacking

Step 4 Installing shelf in cabinet or rack

Step 5 Installing a Cisco 7200 or 7500 router on a BPX 8650

Step 6 Optional Cable Management Tray

Step 7 Verifying 9.6 or 19.2 Gbps Backplane

Step 8 Upgrading to BCC-4 Cards

Step 9 Installing APS Redundant Frame Assembly and Backcards

Step 10 Making T3 or E3 Connections

Step 11 Making a BXM OC3 or OC12 Connection

Step 12 Making a BXM T3/E3 Connection

Step 13 Setting up the BME OC-12 Port Loop

Step 14 Alarm Output Connections

Step 15 Attaching Peripherals

Step 16 LAN Connection for the Network Management Station

Step 17 Connecting a Network Printer to the BPX Switch

Step 18 Connecting Modems

Step 19 Making External Clock Connections

Step 20 Initial Power-Up of the BPX Switch

Step 21 Provisioning the BPX Switch (making connections)

Installation Sequence Flow

Here is the sequence of operations that you should follow during the installation of the BPX switch:

- *Chapter 7, Preliminary Steps Before Installing*: Follow these preliminary setup instructions for the mechanical installation of a BPX switch shelf. Depending on the type of rack or cabinet, the you are then directed to either:
  - *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers* with rear rail setback at 19.86 inches; or
  - *Chapter 9, Installation in Customer Cabinet* that is 19 inches wide with a rear rail setback of 30 inches.
  - Otherwise, the installation is non-standard and requires that you contact Cisco Customer Service.

The BPX switch shelves are either AC or DC powered. At the completion of the cabinet installation procedures you are directed to the appropriate power setup and connection chapter:

- *Chapter 10, Installing the DC Shelf*, or
- *Chapter 11, Installing the AC Shelf*.

An optional cable management tray and BXM T3/E3 cable management brackets are available for use with T3/E3 BXM cards. The brackets are designed for cards set up as non-redundant (single cables rather than Y-cabling). The tray is designed primarily for use in a mid-mount open-rack configuration. Instructions for installing the optional tray are provided in:

- *Chapter 12, Installing the T3/E3 Cable Management Tray*

The remaining installation procedures are the same for every installation. You will proceed to the initial setup and configuration procedures in:

- *Chapter 13, Installing the BPX Switch Cards*
- *Chapter 14, Connecting Cables*
- *Chapter 15, Connecting Temporary Terminal and Attaching Peripherals*
- *Chapter 16, Checking and Powering-Up*

Following the completion of these installation procedures, you should set-up a network management workstation so that you can use the CiscoView and Cisco WAN Manager graphical user interfaces to provision the BPX equipment with network connections.

Overview and network configuration procedures are in *Part 3, Initial Configuration and Network Management*.

When you have connected and configured the network management terminal and software, you are ready to configure the BPX switch. Configuration procedures are provided in *Part 4, Configuring Connections*.

Configuration: Lines, Trunks, and Connection

In many cases, you can add and configure lines and trunks by using the Cisco WAN Manager, which provides a graphical interface that is most convenient for configuring connections. In certain other cases, however (and particularly during the initial setup before you have configured network management) you will need to use the command line interface (CLI).

For example, to add an ATM connection, you might use the following CLI command:

addcon local_addr node remote_addr traffic type ...extended parameters

Other initial configuration must be performed by using the command line interface:

- Configure node name
- Configure time zone
- Configure date and time
- Configure node number

For additional information about the CLI and complete details on all its commands, refer to the *Cisco WAN Switching Command Reference*.

CHAPTER 7

Preliminary Steps Before Installing

Before proceeding with the installation of the BPX switch, follow these preliminary steps to ensure safety and reliability:

- Site Preparation
- Parts Checklist
- Safety Requirements
- Mechanical Installation

Warning **Installation should be performed by authorized personnel only.**

Site Preparation

These site preparations are required.

- **Location**
  The BPX switch may be installed only in a RESTRICTED ACCESS LOCATION.
- **Space**
  Each BPX switch shelf requires floor space 22 inches (55.9 cm) wide and 80 inches (203.2 cm) deep to provide sufficient clearance around the cabinet to allow access to the front and back.
- **Power**
  An AC or DC power source must be available within 6 feet (2 m.) of the rear of the BPX switch shelf. A maximum configuration for an AC-powered BPX switch might require up to 2333 VA (13 A at 180 VAC, 10 A at 230 VAC). A maximum configuration for a DC powered BPX switch might require up to 1680 Watts (40 A at –42 VDC, 35 A at -48 VDC).
- **Uninterruptible Power Source**
  Please consult Cisco Engineering if a portable uninterruptible power source (UPS) will be used to power the BPX 8600 Series System. Do not use an UPS or power source with a Ferro-Resonant transformer. For UPS, Cisco Systems recommends only low output impedance UPS capable of providing the necessary fault current required to trip the protection devices.
- **Cooling**
  The site must be capable of maintaining an ambient temperature of 40°C maximum (recommended range 20°C to 30°C) while the system is operating. A fully loaded BPX switch may dissipate up to 7200 BTUs. It is extremely important that the BPX switch is positioned to assure an unrestricted air flow through the enclosure.

- **Weight**
  A fully loaded, AC-version, BPX switch can weigh up to 213 pounds (97 Kgs). A fully-loaded DC-version BPX switch can weigh up to 163 pounds (74 Kgs).

Parts Checklist

Before proceeding, go through this parts checklist to verify that all the parts you ordered are present, and that they are all in good condition. If there is anything missing or damaged, report it to your Cisco Order Administration representative.

Plug-in cards may be shipped installed or under separate cover. The exact number of cards will vary from site to site, depending on the selected configuration.

The BPX switch is shipped with all unused slots covered by backplane inserts that prevent radio frequency emissions from the equipment. The unit must not be operated with any unused slots left uncovered.

Refer to this list to check the number and type of cards shipped against the number and type of card you ordered. Check that:

If a DC version, it has the correct number of Power Entry modules.

If an AC version, it has the correct number of power supplies (1 or 2).

For non- redundant configuration, there should be one Broadband Controller Card. This can be a BCC-4v, BCC-3-32M, BCC-3-64M, or a BCC-32 depending on system configuration

For a non-redundant configuration, there should be one Broadband Controller backcard. For a BCC-4V or BCC-3-32M, or BCC-3-64M front card, a BCC-3-BC backcard must be used. For a BCC-32 front card, a BCC15-BC backcard must be used.

For a redundant configuration, there should be two Broadband Controller Cards. These can be two BCC-4Vs, BCC-3-32Ms, or BCC-64Ms, or two BCC-32s.

For a redundant configuration, there should be two Broadband Controller backcards. For BCC-4V, BCC-3-32M, or BCC-3-64M front cards, these must be BCC-3-BC backcards. For BCC-32 front cards, these must be BCC15-BC backcards.

One ASM card.

One LM-ASM card.

Correct number of BXM cards.

Correct number of BNI cards.

Correct number of BME cards.

One line module backcard for each BXM, as applicable (such as, BPX-T3/E3-BC, MMF-155-4, SMF-155-4, SMFLR-155-4, MMF-155-8, SMF-155-8, SMFLR-155-8, SMF-622, SMFLR-622, SMF-622-2, or SMFLR-622-2),
or STM-1 backcard,
or SONET APS backcards (such as, SMF-155-4R, SMF-155-8R, SMF-622-1R, SMF-622-2R, SMF-LF-155-4R, SMF-LF-155-8R, SMF-LF-622-1R, and SMF-LR-622-2R,

One line module backcard, SMF-622-2 for each BME.

One line module backcard (such as, BPX-T3-BC, BPX-E3-BC, MMF-2-BC, SMF-2-BC, or SMFLR-2-BC) for each BNI, as applicable.

All cables specified in the order.

Note An inventory of the installed cards is taped to the BPX switch. The inventory states each card's serial number, revision number, and slot number (serial and revision numbers are also found on the component side of each card).

Safety Requirements

This section details safety information for system planners, installers, and maintenance personnel.

The mechanical design of the BPX switch prevents any access to exposed voltages without the use of tools. When installed properly, all front and rear cards are mechanically held captive.

Warning **For protection against shock hazard, verify that all power cords or cables are disconnected before servicing the unit (there may be more than one power cable). The highest voltage that may be present in the node when powered up is 264 VAC (AC systems) or 56 VDC (DC systems).**

CEPT Requirements

All apparatus (such as, 48 VDC power supplies) connected to the BPX switch must comply with BS6301 or EN60950.

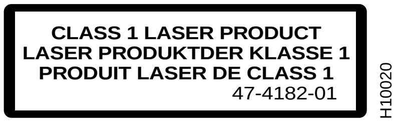
EMI Requirements

Compliance with emission regulations depends upon adherence to the installation steps in this manual, including installation of faceplates for all slots and the use of shielded cables between systems.

Laser Safety Guidelines

The optical ports contain an information label as shown in Figure 7-1.

Figure 7-1 Laser Information Label



Warning **Invisible laser radiation may be emitted from the optical ports of the single-mode or multimode products when no fiber cable is connected. Avoid exposure and do not look into open apertures. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment).**

Warning **Class 1 laser product. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment).**

Warning **Laser radiation when open. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment).**

Maintaining Safety with Electricity

You must install your BPX switch in accordance with national and local electrical codes.

United States: National Fire Protection Agency (NFPA) 70, United States National Electrical Code.

Canada: Canadian Electrical Code, C22.1, part 1.

Other countries: International Electrotechnical Commission (IEC) 364, part 1 through part 7.

The BPX switch operates safely when it is used in accordance with its marked electrical ratings and product usage restrictions.

Basic Guidelines

Follow these basic guidelines when working with any electrical equipment:

- Locate the emergency power-OFF switch for the room in which you are working before beginning any procedures requiring access to the interior of the BPX chassis.
- Disconnect all power and external cables before removing or installing a chassis.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, frayed power cords and missing safety grounds.
- Never work alone when potentially hazardous conditions exist.
- Never assume that power has been disconnected from a circuit; always check.
- Never perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never install equipment that appears damaged.

Any list of guidelines might not address all potentially hazardous situations in your working environment so be alert and exercise good judgment at all times.

These safety guidelines will help to ensure your safety and protect the equipment:

- Keep the chassis area clear and dust-free before, during, and after installation.
- Keep tools away from walk areas where you and others could fall over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the equipment.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Never attempt to lift an object that might be too heavy for you to lift alone.
- Always power OFF all power supplies and unplug all power cables before opening, installing, or removing a chassis.

Power and Grounding

Step 1 In order for the BPX switch to function safely and correctly, along with peripheral equipment, use only the power cords, cables, and connectors specified for the attached peripheral equipment, and make sure they are in good condition.

Step 2 Certain BPX switches are supplied with two power feeds (cords). Before commencing installation or maintenance inside the cabinet, be sure both power feeds are disconnected from their respective sources.

Step 3 Ensure that the BPX switch frame is attached to an isolated ground connection (connection attached directly to ground through an uninterrupted line).

Step 4 A conduit hookup box is factory-installed on each DC Power Entry Module for sites requiring wiring to be enclosed in conduit. A plastic terminal block cover is also provided for installations that do not require conduit hookup. Install one or the other as protection for the DC input.

Step 5 For an AC system, verify that the node is powered from a dedicated AC branch circuit. The circuit shall be protected by a dedicated 2-pole circuit breaker sized such that the rated current and the trip delay is higher and longer than the BPX switch circuit breaker. A dedicated 20A, 2-pole AC circuit breaker with a long trip delay is recommended for installation.

Note The BPX switch uses a 15A (or in newer models a 20-A), 2-pole AC circuit breaker with a medium trip delay on each AC input. The circuit breaker manufacture is either Carlingswitch (p/n CA2-B0-34-615-121-C) or Heinemann (part number AM2-A3-A-0015-02E).

Step 6 For a DC system, verify that the node is powered from a dedicated DC branch circuit. The circuit shall be protected by a dedicated circuit breaker sized such that the rated current and the trip delay is higher and longer than the BPX switch circuit breaker. A dedicated 50A, 1-pole DC circuit breaker with a long trip delay is recommended for installation.

Note The BPX switch uses a 50A, 1-pole DC circuit breaker with medium trip delay on the -48V input. The circuit breaker manufacture is Heinemann (part number AM1S-B3-A-0050-02-H).

Step 7 An insulated grounding conductor should be installed as part of the branch circuit that supplies the unit. This grounding conductor is identical in size to the grounded and ungrounded branch circuit supply conductors, but is green with yellow stripes.

Mechanical Installation

Caution If the BPX switch is to be mounted in an enclosed cabinet, ensure that a free flow of air in and out of the enclosure is provided. Contact Customer Service for further information.

Horizontal Positioning

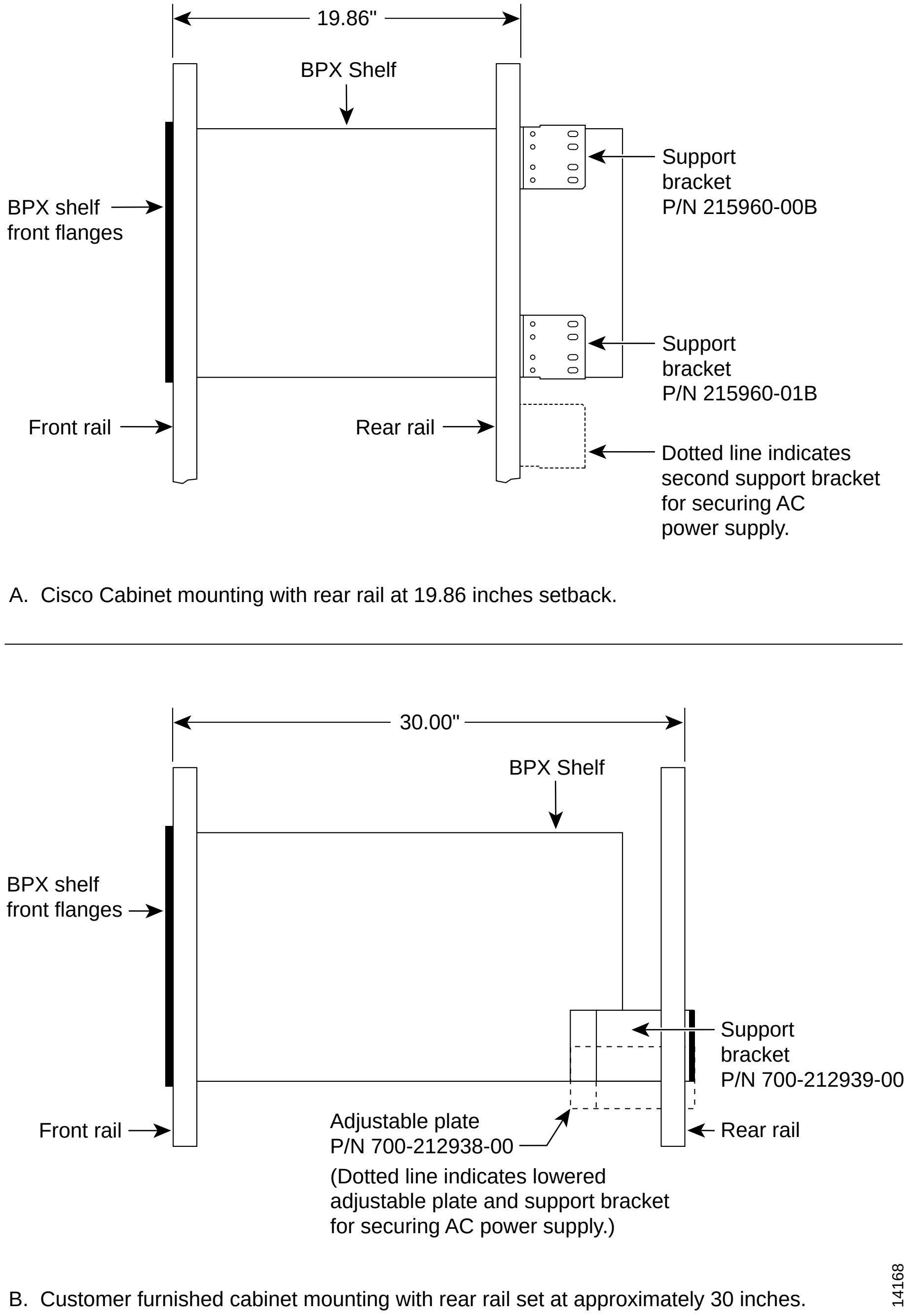
BPX switch shelves are designed to be mounted to two sets of vertical mounting rails in either a Cisco cabinet or a standard 19-inch equipment rack with unrestricted front to rear air flow. When installed in a Cisco cabinet (see Figure 7-2), the front flanges of the BPX switch are secured to the front rails of the Cisco cabinet. In factory installations, rear support is provided by rear mounting rails in the cabinet at a setback of 19.86 inches. As an option, a rear set of rails located at a setback of approximately 30 inches may be used for rear support.

BPX switch shelves can also be mid-mounted to an open T-Rail type rack (see Figure 7-3) with unrestricted front to rear air flow. To facilitate this type of installation, brackets may be fastened to the BPX switch shelf at a 5 or 10 inch setback for supporting the front of the BPX switch shelf. Additional rear mounting support is also recommended. Contact Customer Service for further information.

Vertical Positioning

For recommended typical equipment configurations in a Cisco cabinet, refer to *Chapter 2, BPX Switch Physical Overview*.

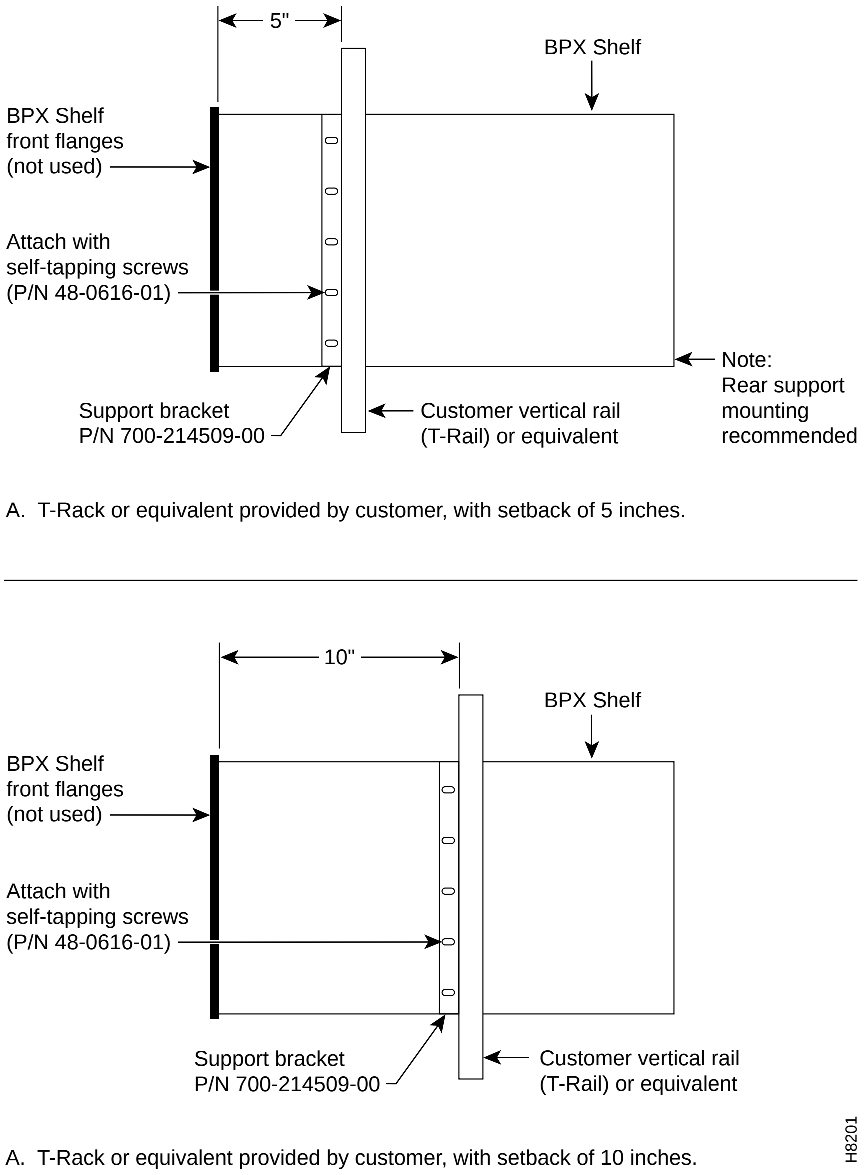
Figure 7-2 Cabinet Mounting Options for the BPX Shelf


19.86"
BPX Shelf
BPX shelf front flanges
Support bracket P/N 215960-00B
Support bracket P/N 215960-01B
Front rail
Rear rail
Dotted line indicates second support bracket for securing AC power supply.
30.00"
BPX Shelf
BPX shelf front flanges
Support bracket P/N 700-212939-00
Front rail
Adjustable plate P/N 700-212938-00
(Dotted line indicates lowered adjustable plate and support bracket for securing AC power supply.)
Rear rail
14168

A. Cisco Cabinet mounting with rear rail at 19.86 inches setback.

B. Customer furnished cabinet mounting with rear rail set at approximately 30 inches.

Figure 7-3 BPX Shelf and T-Rail (Open Rack) or Equivalent Mounting Options



A. T-Rack or equivalent provided by customer, with setback of 5 inches.

A. T-Rack or equivalent provided by customer, with setback of 10 inches.

Installing a BPX Switch Shelf, Preliminary Steps

The BPX switch shelf is designed for mounting in a standard 19-inch (48.25 cm) equipment rack such as the standard Cisco cabinet. A minimum width between rails of 17.750 inches (44.45 cm) is required (see Figure 7-4 and Figure 7-5).

Mounting flanges are permanently attached to the front edge of the BPX switch shelf.

Note It is recommended that you use a lifting device to assist in mounting the shelf with all plug-in cards installed. This procedure eliminates the possibility of damaging the card contacts during removal and reinstallation. However, if no lifting device is available, it is possible to temporarily remove the plug-in cards to lessen the weight. Great care should be taken with removing and reinstalling cards.

There are two types of BPX switch shelves with special installation requirements:

- **AC powered**
  If you install an AC-powered BPX switch shelf, you must also install an AC Power Supply Tray directly below it.
- **DC powered**
  The DC Powered BPX switch Shelf contains factory-installed DC power entry modules (PEMs) within the shelf itself.

Temporary support brackets and a spacer bar are furnished to ease installation by supporting the BPX shelf as you slide it into a cabinet.

Note Installation in a non-Cisco cabinet or T-Rail type rack is similar to installation in a Cisco cabinet. Contact Customer Service for recommended rear support details.

These instructions apply to a BPX switch shelf installation in a Cisco cabinet, which has rear rails at 19.86 inches (50.5 cm) or in a customer supplied standard 19-inch (48.25 cm) equipment rack with rear rails at a 30 inch (76.2 cm) setback.

The recommended stacking order, from the bottom, up, is:

1. BPX on the bottom
2. Next, the 7204 Label Switch Controller (if ordered)
3. Next, the MGX (8250 or 8230) on top

Gap between the shelves is designed to be .060" minimum to allow clearance for replacement.

The first of the two following procdures is the recommended method for installing the BPX shelf and other shelves in a Cisco cabinet: by leaving in the cards and using a lifting device to raise the fully loaded unit into position. The second procedure describes removing all cards for situations where no lifting device is available.

To install the fully loaded BPX switch shelf in a Cisco cabinet by means of a lifting device:

Step 1 Position the shipping container and pallet facing the front of chassis. Remove the foam strips on the sides, front and rear.

Step 2 Slide the BPX onto the lifting device platform.

Step 3 Decide where the BPX switch is to be located. The top of the spacer bracket should be temporarily installed in the rack 22.75" (57.8 cm.) below the location selected for the top of the BPX switch chassis.

Step 4 Install the temporary support brackets and spacer bar (shipped with the unit). Use two mounting screws to attach each temporary support bracket and two screws to attach the temporary spacer bar to the rack.

Note It is recommended that all BPX switches use a set of vertical support rails to provide additional support for the rear of the chassis. In the Cisco cabinet these are located at a 19.86 inch setback from the front in factory installations.

Step 5 If you are installing the BPX switch shelf in a Cisco cabinet and using factory installed rear rails located at a 19.86 inch setback from the front, then see the installation instructions in *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers* , for instructions.

Step 6 If you are installing the BPX switch shelf in a customer-supplied cabinet using rear rail mounting support brackets located at a setback of approximately 30 inches from the front, then see the installation instructions in *Chapter 9, Installation in Customer Cabinet*.

To install the BPX switch shelf in a Cisco cabinet without use of a lifting device:

Step 1 Position the shipping container and pallet facing the front of chassis. Remove the foam strips on the sides, front and rear.

Step 2 Remove the card retaining bracket from the front of the chassis by unscrewing the four Phillips screws. This bracket is used to retain the boards during shipping.

Step 3 Remove the Air Intake Grill and all front and rear cards from the shelf and temporarily set them aside as follows:

a. Locate the small access hole in the top center of the front Air Intake Grille below the card slots (see Figure 7-6 for location).

b. Insert a small slotted blade screwdriver (0.20/0.25 inch blade width) into the access hole until it stops (approximately 1 inch).

c. Carefully rotate the screwdriver approximately a quarter turn in either direction. The top of the Air Intake Grille should spring out.

d. Remove Air Intake Grille.

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the strap lead to the cabinet.

e. To remove the cards, rotate the extractor handles at the top and bottom of each card to release the card and slide it out.

Step 4 Decide where the BPX switch is to be located. Refer to Figure 7-2 through Figure 7-5 for typical mounting dimensions. The top of the spacer bracket should be temporarily installed in the rack 22.75" (57.8 cm) below the location selected for the top of the BPX switch chassis.

Step 5 Install the temporary support brackets and spacer bar (shipped with the unit). Use two mounting screws to attach each temporary support bracket and two screws to attach the temporary spacer bar to the rack (see Figure 7-7 and Figure 7-8).

Note It is recommended that all BPX switches use a set of vertical support rails to provide additional support for the rear of the chassis. In the Cisco cabinet these are located at a 19.86 inch setback from the front in factory installations.

Step 6 If you are installing the BPX switch shelf in a Cisco cabinet and using factory installed rear rails located at a 19.86 inch setback from the front, then see the installation instructions in *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers* , for instructions.

Step 7 If you are installing the BPX switch shelf in a customer-supplied cabinet using rear rail mounting support brackets located at a setback of approximately 30 inches from the front, then see the installation instructions in *Chapter 9, Installation in Customer Cabinet*.

Figure 7-4 Rack Mounting Dimensions, DC Powered Shelf

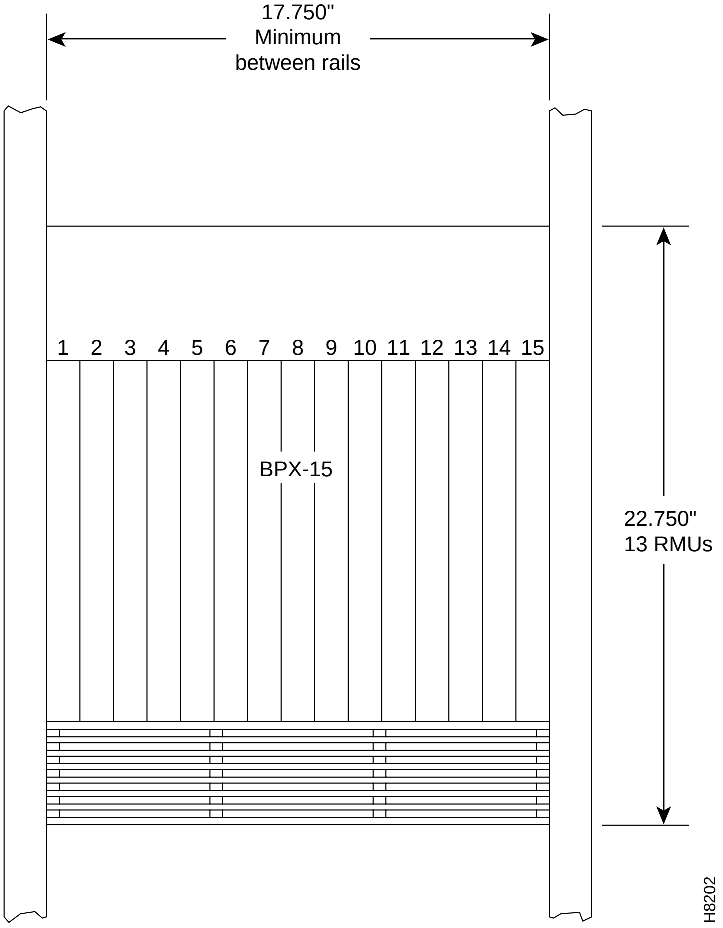


Figure 7-5 Rack Mounting Dimensions, AC Powered Shelf

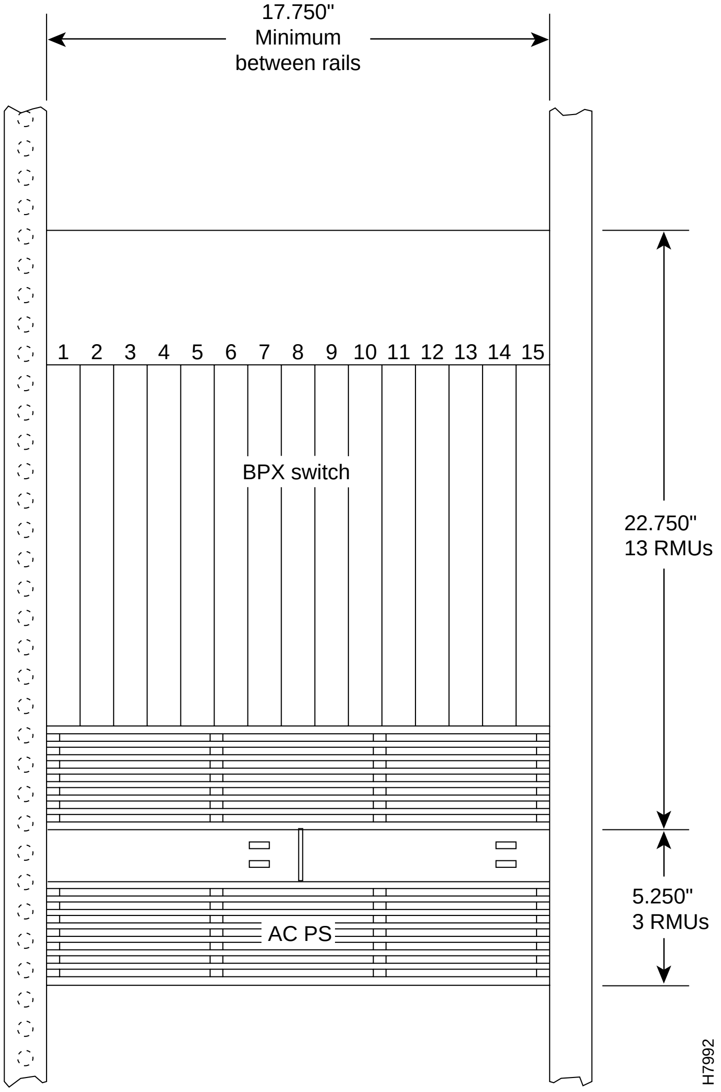


Figure 7-6 Removing an Air Intake Grille

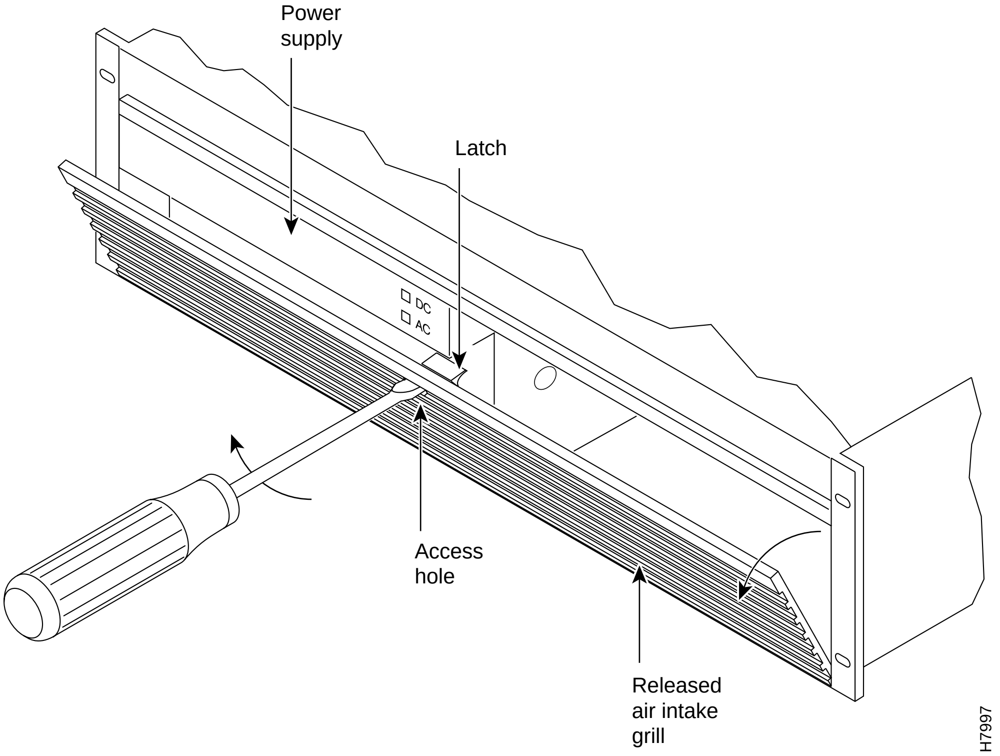


Figure 7-7 Temporary Spacer Bar and Support Brackets Installation

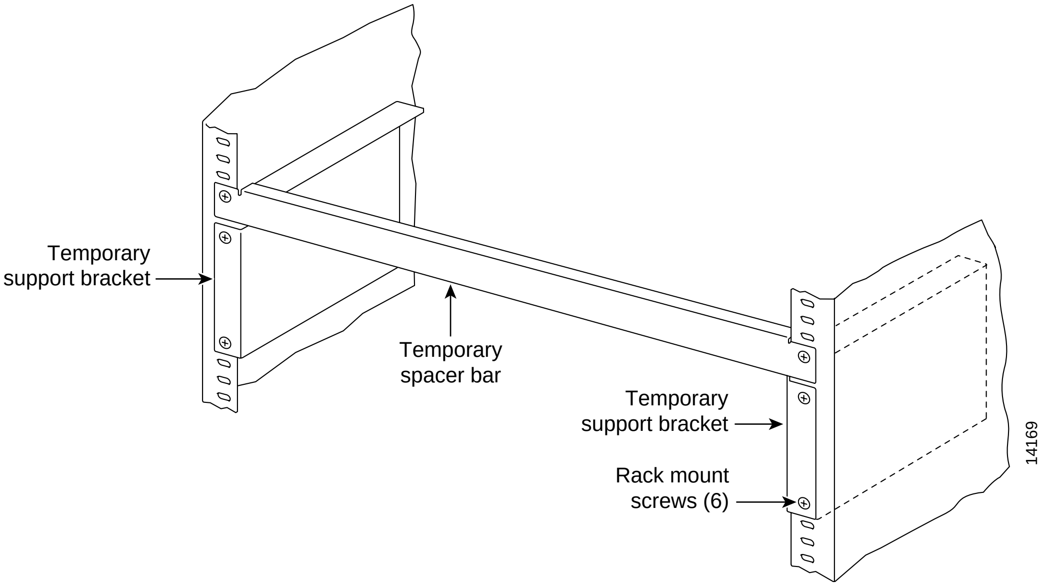
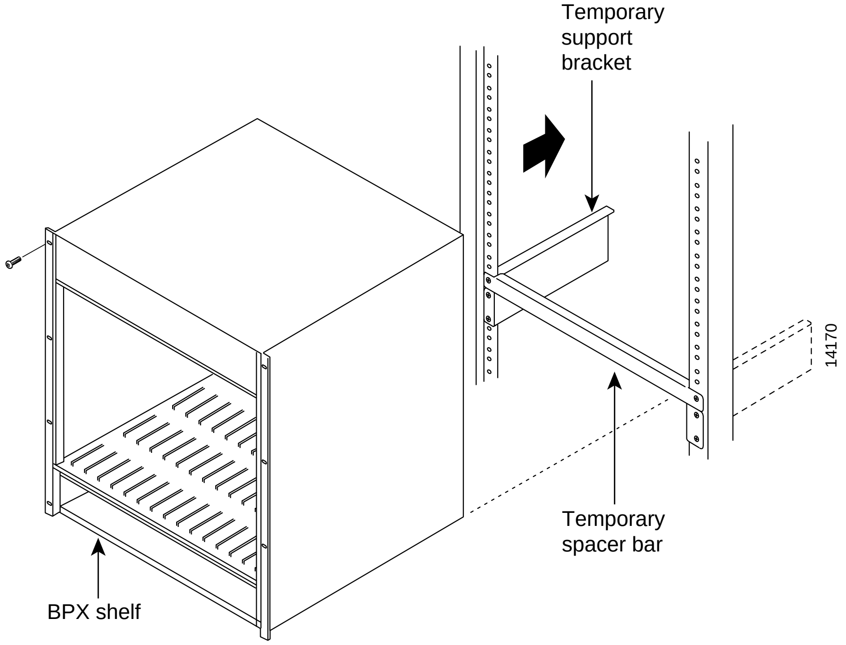


Figure 7-8 BPX Switch Shelf Aligned with Temporary Support Brackets and Bar



CHAPTER 8

Installation with Cisco Cabinets including 7000 Series Routers

This chapter provides these installation procedures:

- Installing a BPX Switch in a Cisco Cabinet
- Installing a 7200 or 7500 Router in a BPX 8650 Cabinet or Rack

Before proceeding with this chapter, complete the procedures and safety checks in:

- *Chapter 7, Preliminary Steps Before Installing*

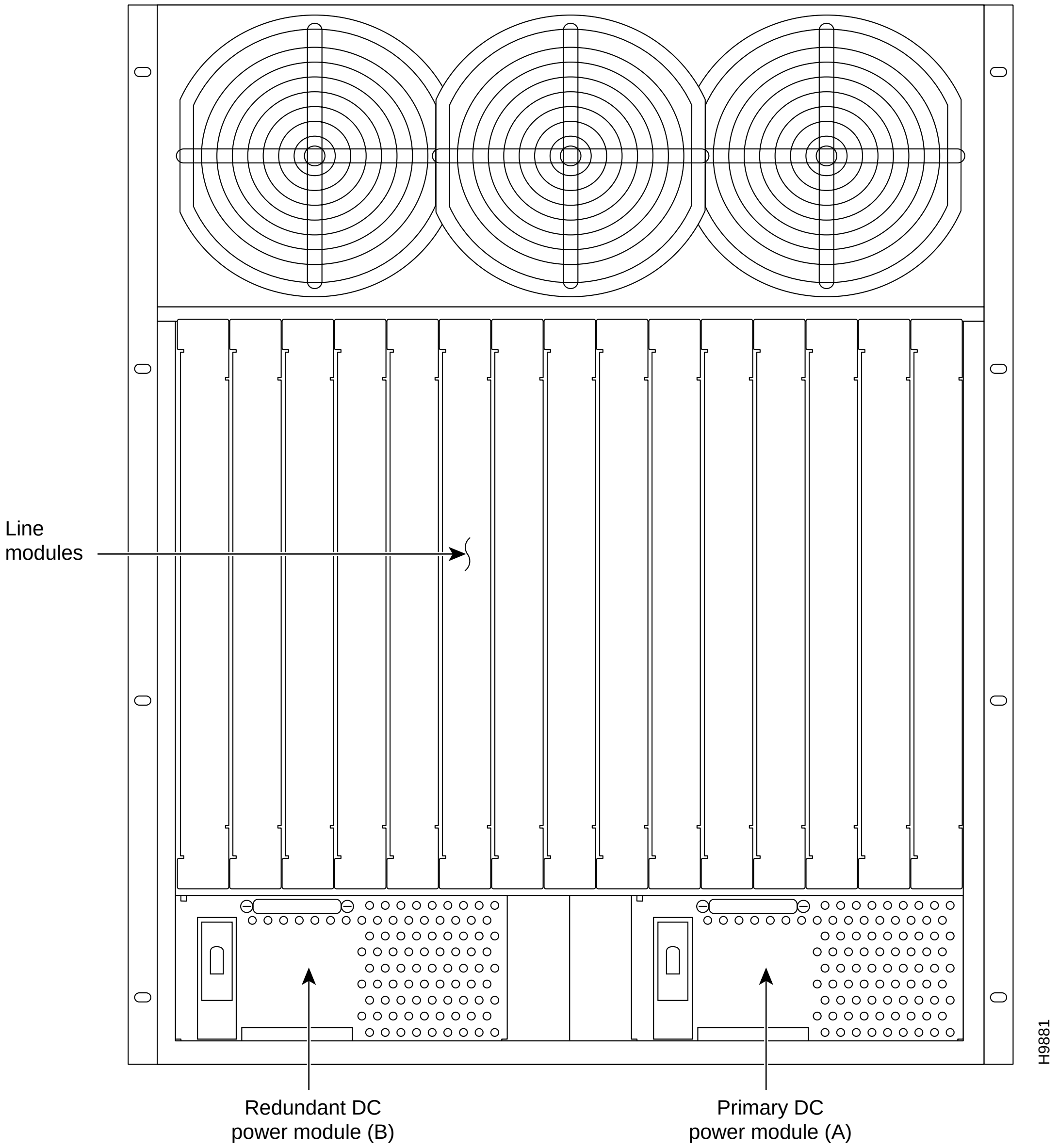
Installing a BPX Switch in a Cisco Cabinet

Follow the steps in this procedure to install a BPX switch shelf in a Cisco cabinet, using the factory-installed rear rails located at a 19.86 inch (50.5 cm) setback from the front mounting flanges.

If the BPX switch shelf is DC-powered:
The DC Power Entry Modules are factory-installed in the lower portion of the rear of the BPX switch shelf (see Figure 8-1). Locate the DC Power Entry Modules and make sure they are equipped as ordered.

If the BPX switch shelf is AC-powered:
You will also need to install an AC Power Tray below it.

Figure 8-1 Location of DC Power Entry Module(s), Cabinet Rear View



Preliminary Procedure:

Follow these steps to install either an AC- or DC-powered BPX switch shelf, referring to Figure 8-2 and Figure 8-3 and to either Figure 8-4 for DC powered systems or Figure 8-5 for AC powered systems:

Step 1 With one person on each side of the BPX shelf, slide the BPX from lifting device shelf and rest it on the temporary space bar and temporary support brackets.

Step 2 Slide the BPX switch shelf into the cabinet over the temporary support bar and brackets and into place over the flanges of the brackets previously attached to the rear rails of the cabinet.

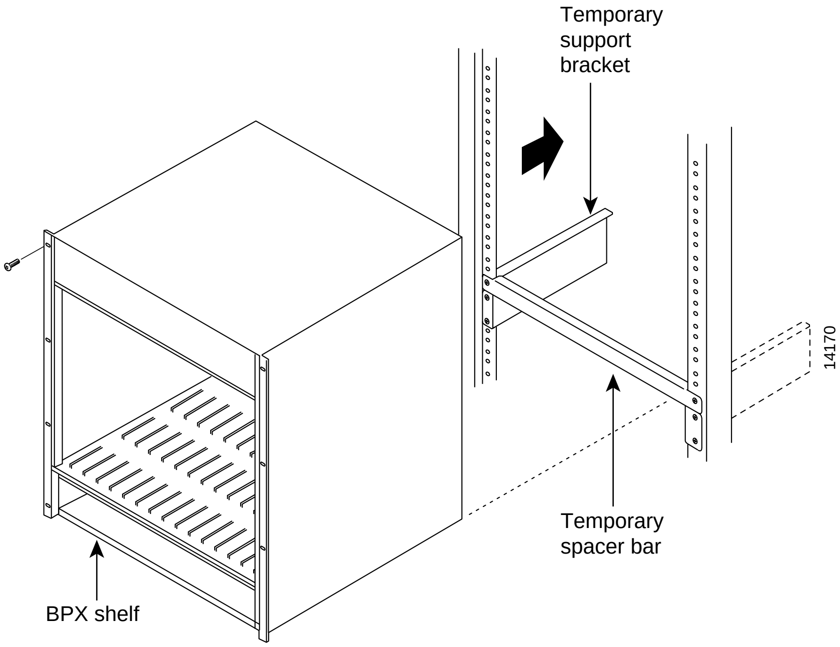
Step 3 Locate the rear support brackets (P/N 215960-00B and 215960-01B) in the miscellaneous parts kit.

Step 4 Secure one support bracket to the back of each of the two rear rails located at 19.86 inches from the front flange of the Cisco cabinet. Use two #10-32 machine screws and flat washers per bracket. The flange on each bracket faces down and inward to support the bottom of the BPX shelf.

Note European installations may use a size M6 metric screw.

Warning **An empty BPX switch shelf weighs 75 pounds (34 Kgs.) and requires a 2 or 3 persons to lift and move it into position. Use of a lifting device is recommended.**

Figure 8-2 BPX Shelf Aligned with Temporary Support Brackets and Bar



Step 5 Attach the BPX switch shelf to the cabinet front rail by using 8 # 10-32 screws.

Step 6 An extra set of support brackets may be mounted to the rear rails at the top back of the shelf. These brackets will prevent any upward movement of the shelf.

Note If another device is installed above the BPX shelf, you can use the extra set of support brackets at the top of that device, rather than at the top of the BPX shelf.

Step 7 Remove the temporary support brackets and spacer bar.

Step 8 If this is a DC-powered shelf, proceed to *Chapter 10, Installing the DC Shelf*.

Step 9 If this is an AC-powered shelf, proceed to *Chapter 11, Installing the AC Shelf*.

Figure 8-3 BPX Shelf with Rear Rail Mounting at Setback of 19.86 inches

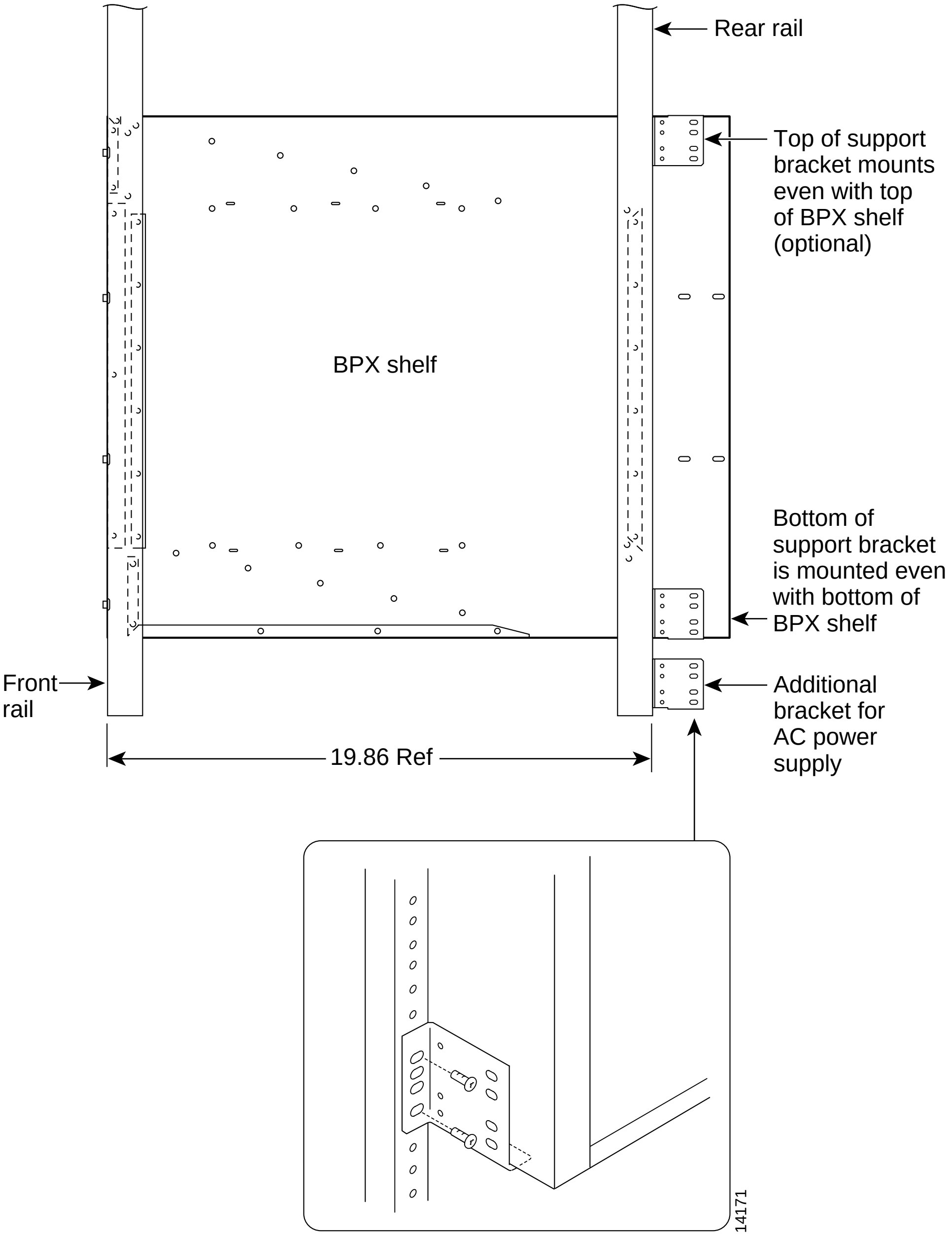

Rear rail
Top of support bracket mounts even with top of BPX shelf (optional)
BPX shelf
Bottom of support bracket is mounted even with bottom of BPX shelf
Front rail
Additional bracket for AC power supply
19.86 Ref
14171

Figure 8-4 Rear Mounting Brackets, with 19.86 Inch Rear Rail Setback (DC Systems)

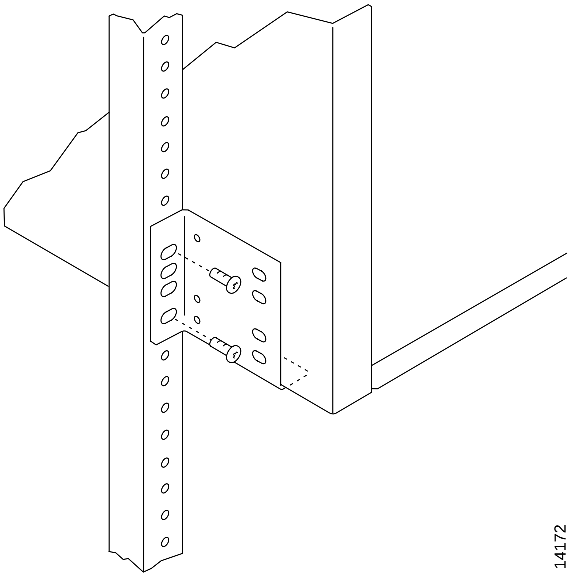
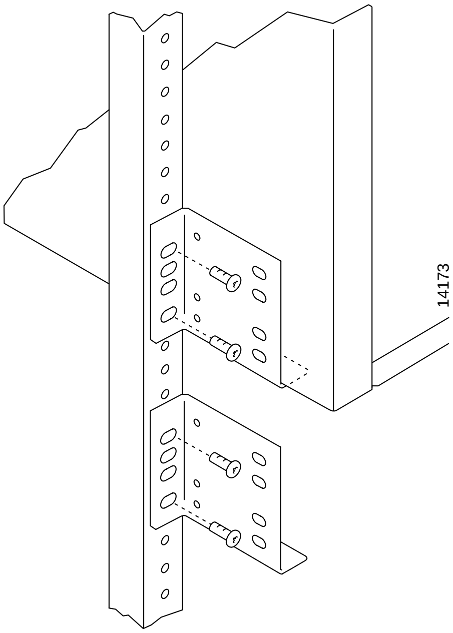


Figure 8-5 Rear Mounting Brackets, 19.86 Inch Rear Rail Setback (AC-Systems)



Installing a 7200 or 7500 Router in a BPX 8650 Cabinet or Rack

This procedure applies to the installation of a 7200 or 7500 Router Label Switch Controller assembly in a Cisco cabinet as part of a BPX 8650 installation. A hardware kit is provided with the router and router enclosure that contains support brackets and other required hardware.

Step 1 Assemble the router into the router enclosure:

a. Place the router into the router enclosure as shown (see Figure 8-6) with the power connector side of the router toward the hinged front door of the router enclosure.

b. Install the power cord along the top left side of the router and router enclosure.

c. Mount the front hinged door to the router enclosure by spreading the sides of the router enclosure slightly so that the holes in each side of the cover engage the pins at the front of the router enclosure.

Note To open the router enclosure door, use the tabs on top of the door. If these are not accessible because another device is installed on top of the router, use a screwdriver in the access cutouts to gently pry open the door.

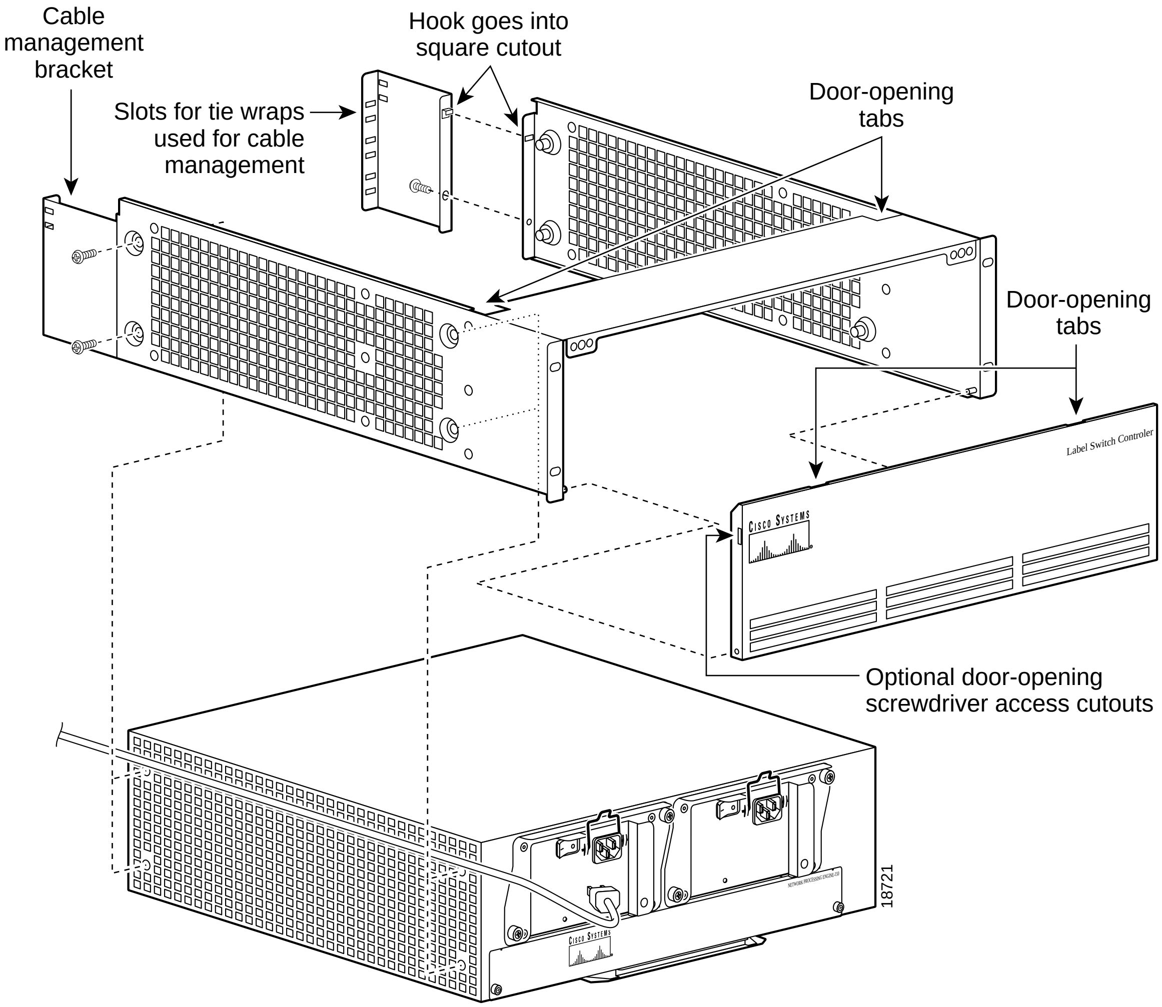
d. Secure the router to the router enclosure by using four screws on each side.

e. You can attach cable management brackets now or later, as desired. The upper end of each bracket hooks into the square cutouts shown in Figure 8-6 and the bottom of each bracket is secured with screws.

Step 2 To install the router assembly in a BPX 8650 cabinet, a 19-inch open rack, or a 23-inch open rack, choose the applicable procedure:

- To install the router assembly in a BPX 8650 cabinet, proceed to "Installing Router Assembly in a Cisco Cabinet" section on page 8-7
- To install the assembly in a 19-inch open rack, proceed to "Installing the Router Enclosure Assembly in a 19-inch Open Rack" section on page 8-9
- To install the assembly in a 23-inch open rack, proceed to "Installing the Router Enclosure Assembly in a 23-inch Open Rack" section on page 8-10

Figure 8-6 Assembly of Router in Router Enclosure


Cable management bracket
Hook goes into square cutout
Slots for tie wraps used for cable management
Door-opening tabs
Door-opening tabs
Label Switch Controler
Cisco Systems
Optional door-opening screwdriver access cutouts
18721

Installing Router Assembly in a Cisco Cabinet

Install the router enclosure assembly in BPX 8650 cabinet (see Figure 8-7):

Step 1 Slide the router enclosure assembly into the cabinet on top of the BPX shelf.

Step 2 Attach the two support brackets from the hardware kit, one to each vertical rail at the back of the cabinet as shown using two screws to secure each. The support brackets have a horizontal flange that supports the router enclosure assembly.

Step 3 Secure the front of the router assembly to the cabinet rails with two screws on each side.

Step 4 Secure the router enclosure assembly to the cabinet with mounting screws.

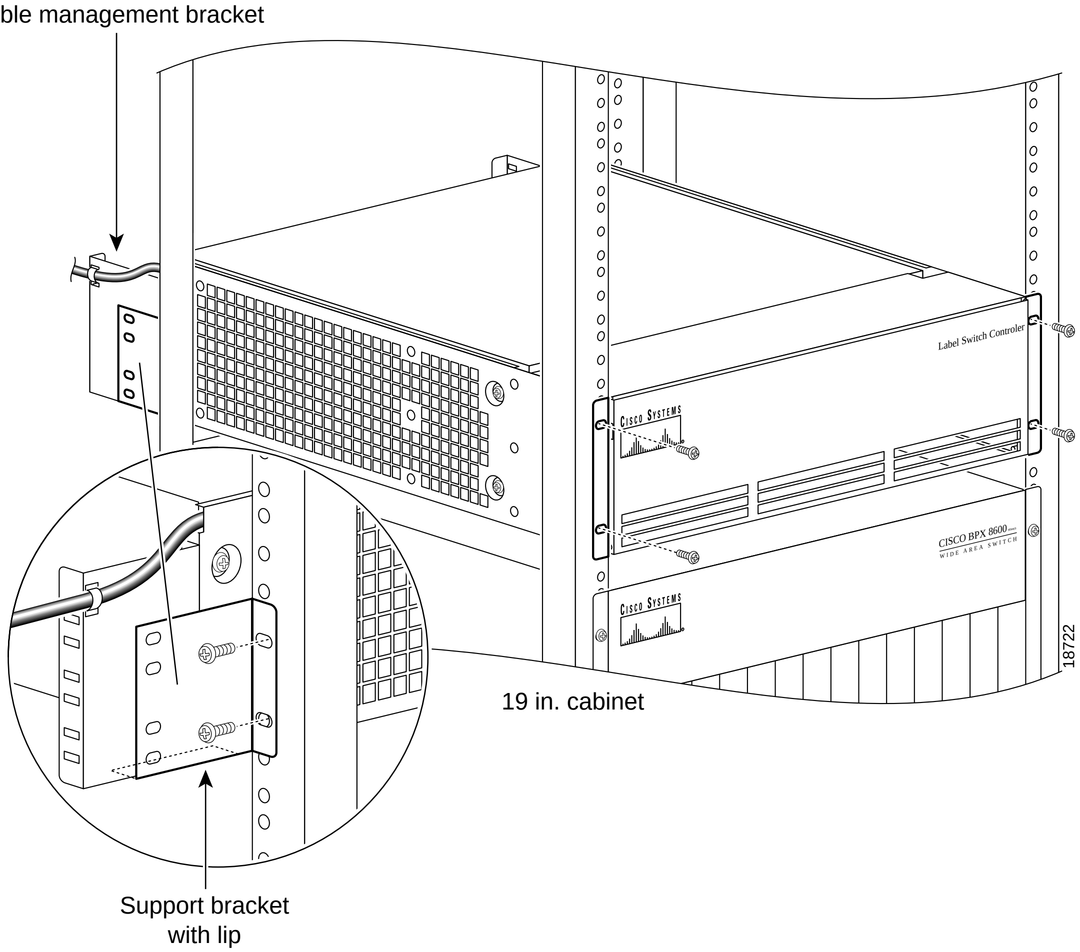
Step 5 Connect the power cord to router connector receptacle at the front of the cabinet, and close the router enclosure assembly door.

Step 6 Use the tie wraps provided in the hardware kit to secure power cord to a Cable Management Bracket.

Step 7 If this is a DC-powered shelf, proceed to *Chapter 10, Installing the DC Shelf*.

Step 8 If this is an AC-powered shelf, proceed to *Chapter 11, Installing the AC Shelf*.

Figure 8-7 Installing the Router Enclosure Assembly in the Cisco BPX 7650 Cabinet



Installing Router Assembly in a 19-Inch Open Rack

Install the router enclosure assembly in BPX 8650 cabinet (see Figure 8-8):

Step 1 Slide the router enclosure assembly into the cabinet on top of the BPX shelf.

Step 2 Attach the two support brackets (for 19-inch open rack mounting) from the hardware kit, one to each side of the router enclosure assembly, using two securing screws for each bracket.

Step 3 Secure the front of the router assembly to rack with two screws on each side.

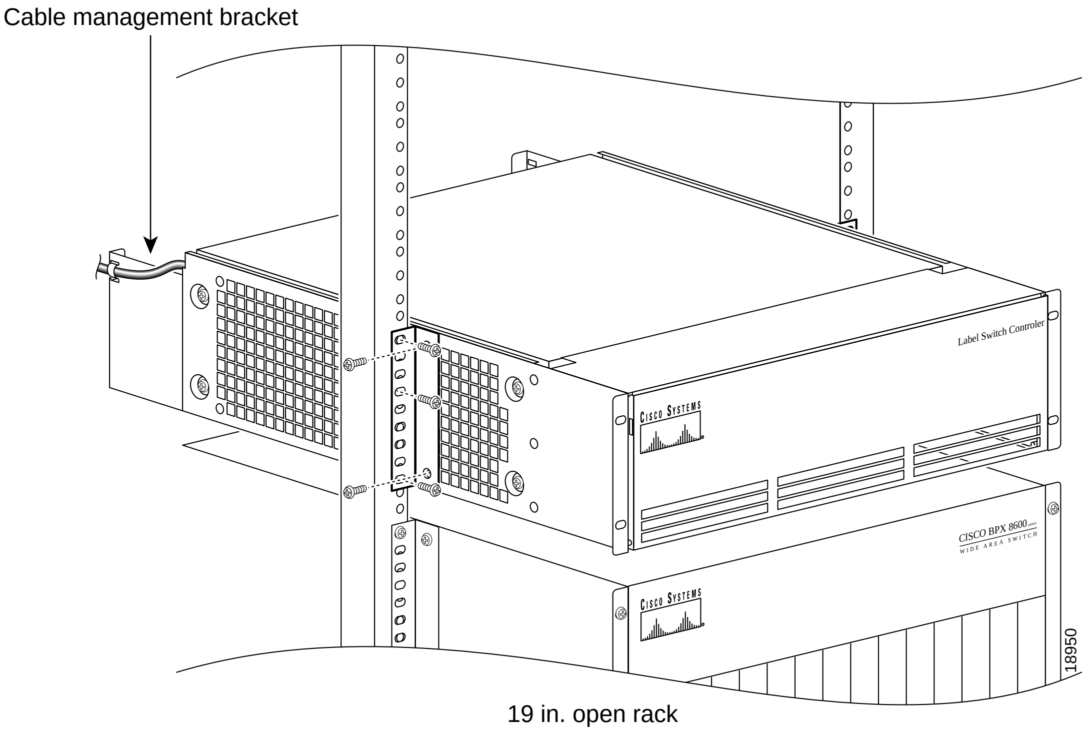
Step 4 Connect the power cord to the router connector receptacle at the front of the cabinet, and close the router enclosure assembly door.

Step 5 Use the tie wraps provided in the hardware kit to secure power cord to a Cable Management Bracket.

Step 6 If this is a DC-powered shelf, proceed to *Chapter 10, Installing the DC Shelf*.

Step 7 If this is an AC-powered shelf, proceed to *Chapter 11, Installing the AC Shelf*.

Figure 8-8 Installing the Router Enclosure Assembly in a 19-inch Open Rack



Installing Router Assembly in a 23-Inch Open Rack

Install the router enclosure assembly in BPX 8650 cabinet (see Figure 8-9):

Step 1 Slide the router enclosure assembly into the cabinet on top of the BPX shelf.

Step 2 Attach the two support brackets (for 23-inch open rack mounting) from the hardware kit, one to each side of the router enclosure assembly, using five securing screws for each bracket.

Step 3 Slide the router enclosure assembly into the cabinet on top of the BPX shelf.

Step 4 Secure the front of router assembly to the rack with three screws on each side.

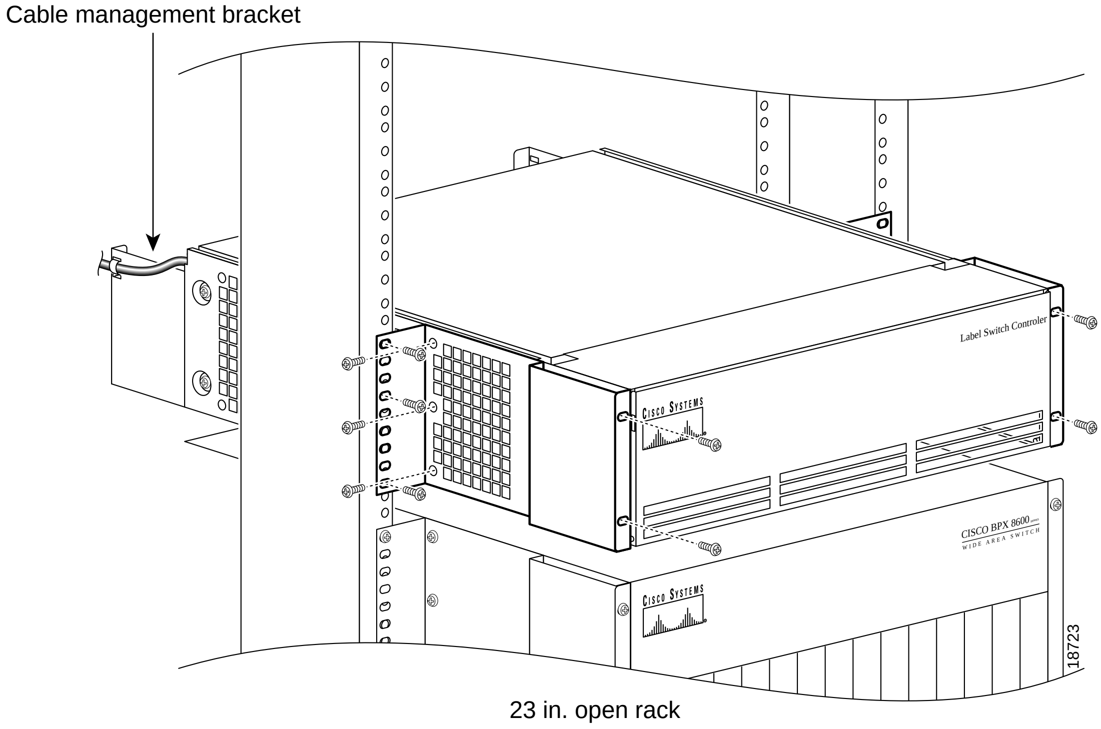
Step 5 Connect the power cord to the router connector receptacle at the front of the cabinet, and close the router enclosure assembly door.

Step 6 Use the tie wraps provided in the hardware kit to secure the power cord to a Cable Management Bracket.

Step 7 If this is a DC-powered shelf, proceed to *Chapter 10, Installing the DC Shelf*.

Step 8 If this is an AC-powered shelf, proceed to *Chapter 11, Installing the AC Shelf*.

Figure 8-9 Installing the Router Enclosure Assembly in a 23-inch Open Rack



CHAPTER 9

Installation in Customer Cabinet

This chapter provides installation steps for the mechanical placement of a BPX switch shelf in a standard 19-inch customer-supplied equipment cabinet or rack with a rear rail setback at 30 inches.

Before proceeding to this chapter, complete the procedures in:

- *Chapter 7, Preliminary Steps Before Installing*

Installing a BPX Switch, Rear Rail Setback at 30-Inch

This procedure applies to a BPX switch shelf to be installed in a customer-supplied cabinet with rear vertical rails located at a setback of approximately 30 inches from the front.

If the BPX switch shelf is DC powered, the DC Power Entry Modules are factory-installed in the lower portion of the rear of the BPX switch shelf itself. Locate the DC Power Entry Module(s) and make sure it/they are equipped as ordered.

If the BPX switch shelf is AC powered, you will also need to install an AC Power Assembly below it.

Preliminary Procedure

Proceed as follows to install the BPX switch shelf, referring to Figure 9-1 through Figure 9-3, and to either Figure 9-4 for DC-powered systems or Figure 9-5 for AC-powered systems. Figure 9-2 shows the location of the rear-located third rails in a customer supplied cabinet and of the corresponding adjustable plates and support brackets on the BPX switch shelf.

Step 1 With one person on each side of the BPX switch shelf, slide the BPX from lifting device and rest it on the temporary space bar and temporary support brackets. positioning the slots at the rear of the pallet tray over the locating tabs on the spacer bracket (see Figure 9-1).

Step 2 Slide the BPX switch shelf into the cabinet over the temporary support bar and brackets and into place over the flanges of the brackets previously attached to the rear rails of the cabinet.

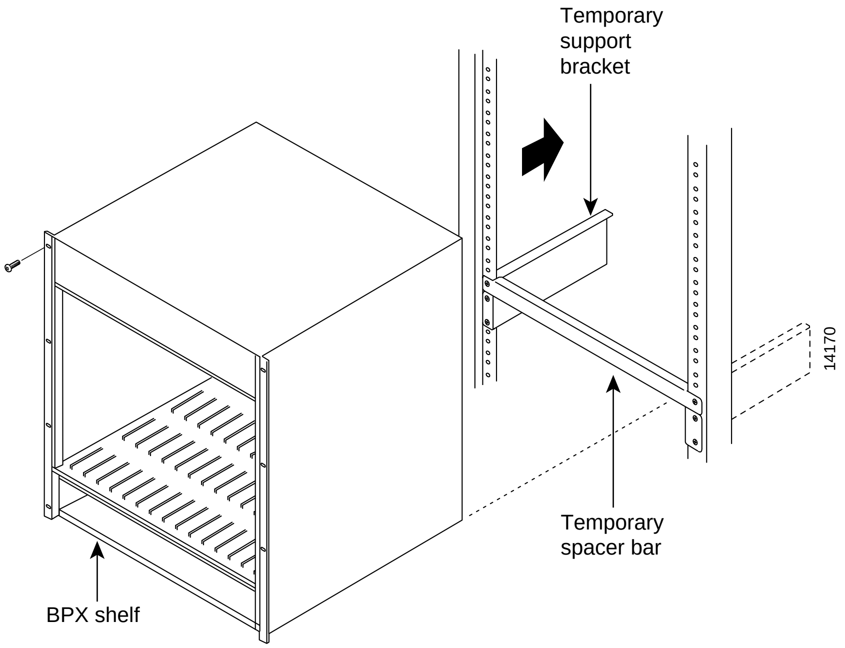
Step 3 Secure the BPX switch shelf to the front rail using 8 each #10-32 screws.

Note European installations may use a size M6 metric screw.

Step 4 Locate the rear support brackets (P/N 215960-00B and 215960-01B) in the miscellaneous parts kit.

Step 5 Position the adjustable plates with the tabs in the three punchouts facing up as shown in Figure 9-3.

Figure 9-1 BPX Switch Aligned with Temporary Support Brackets and Spacer Bar



Step 6 Align the top and bottom holes in the adjustable plates with corresponding holes in the side panel of the BPX switch shelf. (The bottom of the plates should be approximately aligned with the bottom of a DC-powered BPX switch shelf. They should be extended below the bottom of an AC-powered BPX switch shelf so that the AC Power Supplies can be secured to the shelf.)

Step 7 Secure one each adjustable plate to each side of the BPX switch shelf, using (2) each #10-32 machine screws and flat washers.

Step 8 Attach a rear support bracket to each one of the adjustable plates with 2 each #10-32 screws and washers. **Do not tighten yet.**

Step 9 Secure the support brackets to the rear located vertical rails using 2 each #10-32 screws. You might have to lift the BPX switch shelf slightly to align the holes in the bracket to the holes in the rack.

Step 10 Tighten the screws attaching the support bracket to the adjustable plate.

Step 11 Slide a cable strap over each of the three tabs on the support brackets.

Step 12 Remove the temporary support bracket and spacer bracket from the front of the cabinet.

Step 13 If this is a DC-powered shelf, proceed to *Chapter 10, Installing the DC Shelf*.

Step 14 If this is an AC-powered shelf, proceed to *Chapter 11, Installing the AC Shelf*.

Figure 9-2 BPX Switch with Rear Rail Mounting at Setback of 30 Inches

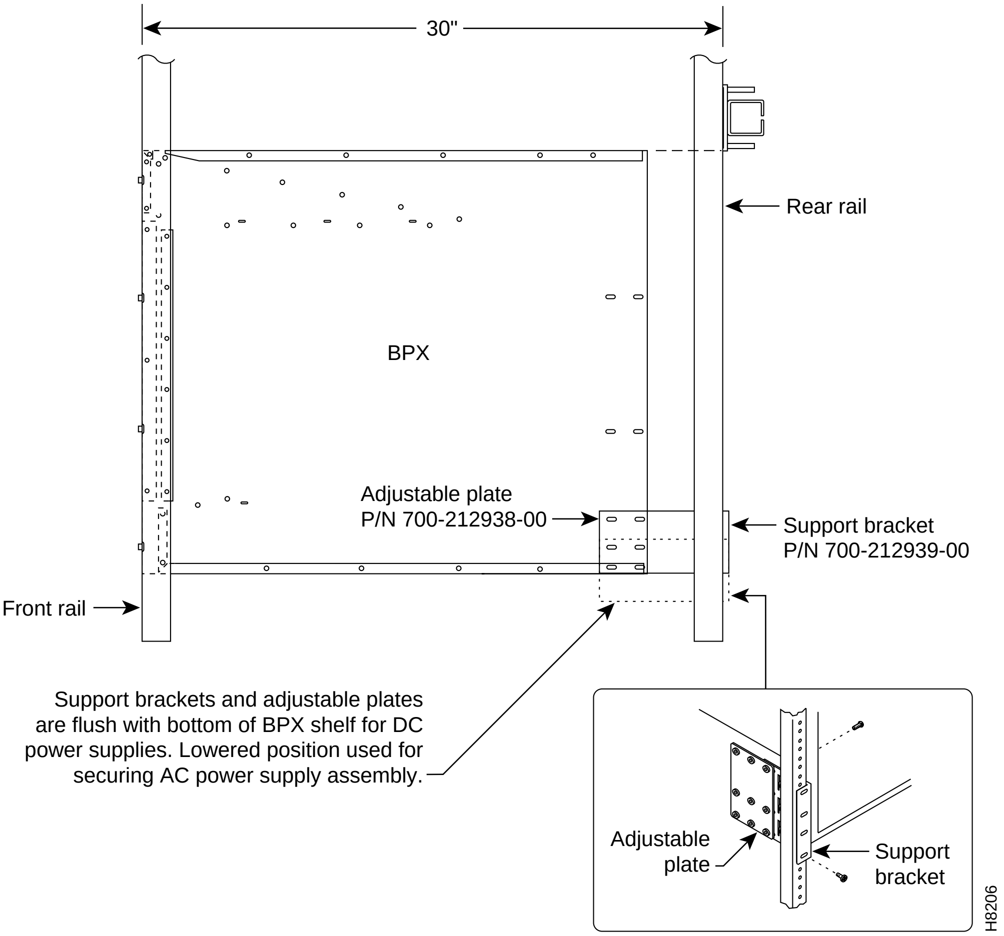

30"
Rear rail
BPX
Adjustable plate
P/N 700-212938-00
Support bracket
P/N 700-212939-00
Front rail
Support brackets and adjustable plates are flush with bottom of BPX shelf for DC power supplies. Lowered position used for securing AC power supply assembly.
Adjustable plate
Support bracket
H8206

Figure 9-3 Rear Mounting Brackets, Detail

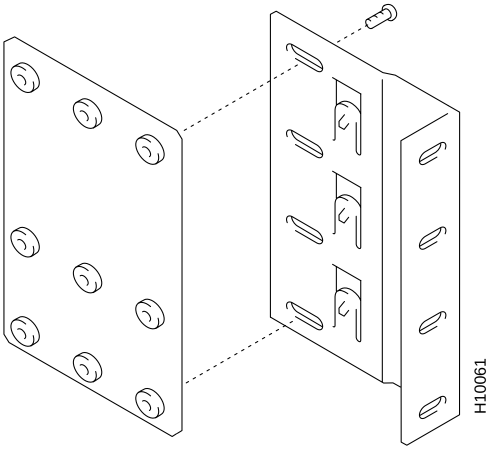


Figure 9-4 Rear Mounting Brackets, with 30 Inch Rear Rail Setback (DC Systems)

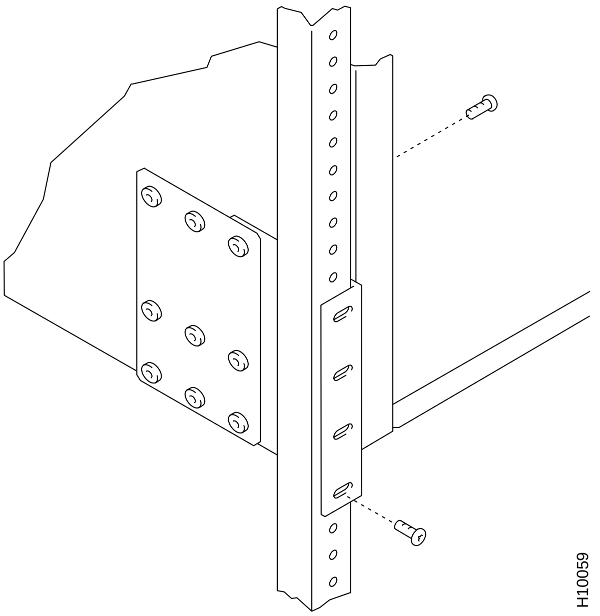
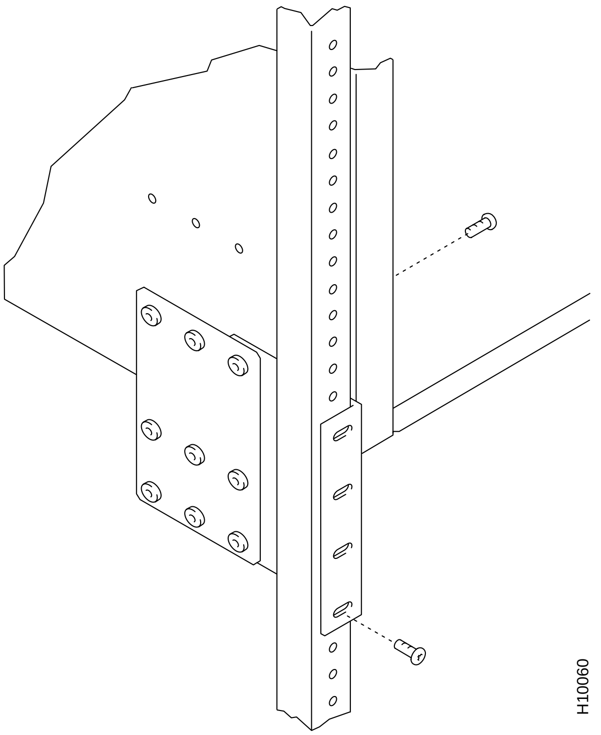


Figure 9-5 Rear Mounting Brackets, 30 Inch Rear Rail Setback (AC-Powered Systems)



CHAPTER 10

Installing the DC Shelf

This chapter explains how to connect the DC power supply to the BPX switch:

- DC Power Input Connections
- Card Slot Fuses
- Fan Power Fuses

Before proceeding in this chapter, complete the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or
- *Chapter 9, Installation in Customer Cabinet*

Preparing for DC Power Installation

Before beginning:

- Verify that you have all necessry DC power cables.
- Verify that you have all cabinet earthing cabling and ground points.
- Dedicated grounds are installed to the switch.
  (Suitable crimps can be obtained from RS Components at http://rswww.com with product codes of 531-021 for a 10mm 2 cable and 119-160 for a 6mm 2 cable.)
- Confirm that power is from isolated supplies.
- Verify that -48 VDC, 50 amp dual feeds are connected to the switch from the power distribution unit.
- Inspect all power and ground connections. Check for voltage and polarity.

DC Power Input Connections

There are two ways to configure a DC-powered BPX switch:

- Single DC Power Entry Module, single power feed
- Dual DC Power Entry Module, dual power feed

Connect wiring from a -48 VDC power source to one or two DC Power Entry Modules (see Figure 10-1). This wiring is provided by the installer.

A metallic conduit box that meets all electrical codes for attaching electrical conduit is factory-installed Figure 10-2. A simple plastic cover is also enclosed for customers who do not require conduit protection for the input power leads Figure 10-3. Use conduit if required by local electrical code.

Only a source that complies with the safety extra low voltage (SELV) requirements in UL1950, CSA C22.2 No. 950, EN60950 may be connected to a BPX switch DC system.

To make DC power connections to the BPX switch:

Step 1 Locate the conduit terminating box, one for each Power Entry Module. (See Figure 10-2.) Remove the two cover screws and lift off the cover. If conduit is required, proceed to
step 2. If conduit is not required, proceed to step 3.

Step 2 Determine which knockout to remove (rear or bottom). Remove knockout and install conduit fitting.

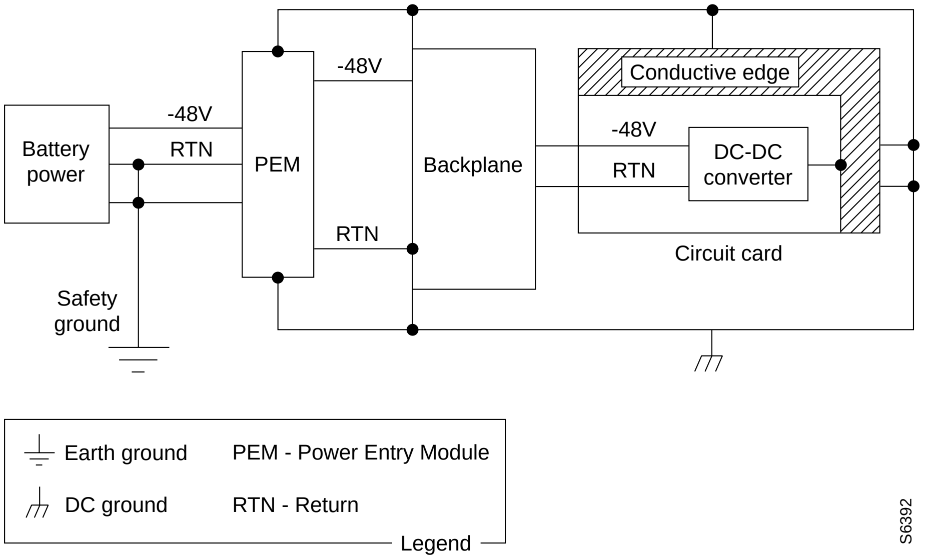
Step 3 If conduit is not required, remove the conduit box by removing the two screws, one above the terminal block and one below it.

Step 4 Run three wires from the DC terminal block to a source of 48 VDC.
Use 8 AWG wire (or metric equivalent for E1 systems).
Use a #10 screw ring lug designed for 8 AWG wire (90° lug if using conduit box) to terminate the wires.

Caution Ensure that the polarity of the DC input wiring is correct! Connections with reversed polarity may damage the equipment.

Warning **Remember that this is a positive ground system.
Connect the positive lead to the +RTN terminal.
Connect the negative lead to the –48V terminal.
Connect the earth ground to the middle terminal labeled SAFETY GROUND.
(See Figure 10-1, Figure 10-2 and Figure 10-3.)
For personnel safety, the green/yellow wire must be connected to safety (earth) ground at both the equipment and at the supply side of the DC wiring.**

Figure 10-1 DC Power



Step 5 Terminate the DC input wiring to a DC source capable of supplying at least 50 amperes. A 50A DC circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring. Be sure to connect the ground wire/conduit to a solid office (earth) ground.

Note Primary overcurrent protection is provided by the building circuit breaker. In North America, this breaker should protect against excess currents, short circuits, and earth faults in accordance with NEC ANSI NFPA 70/CEC.

Step 6 If the system is equipped with dual power feed, repeat steps 1 through 6 for the second power feed.

Step 7 Either replace the cover on the conduit terminating box(es) or attach the plastic cover plate(s) to the terminal block with screws into the two terminal block standoffs. (See Figure 10-2 and Figure 10-3.)

Step 8 Proceed to *Chapter 13, Installing the BPX Switch Cards*.

Figure 10-2 DC Power Connections—With Conduit Box

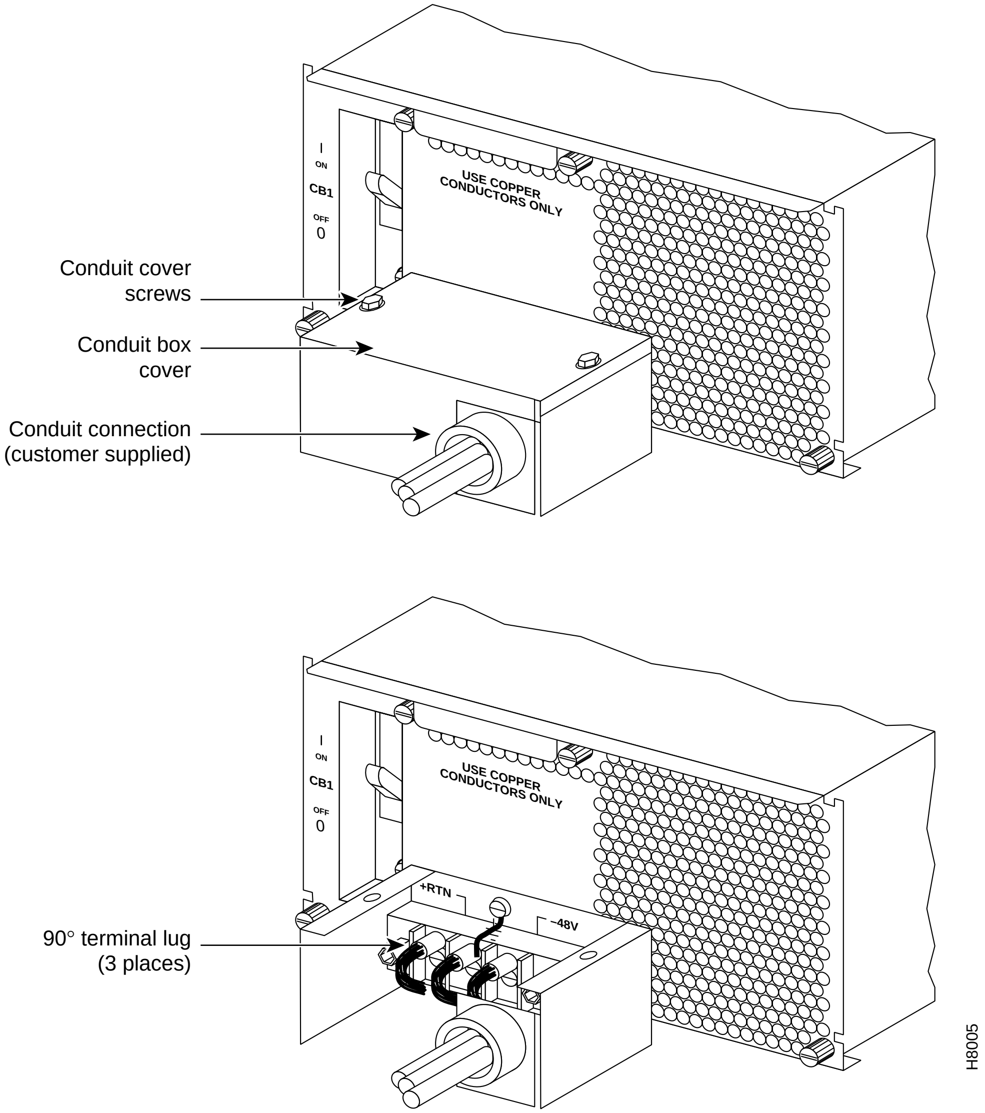
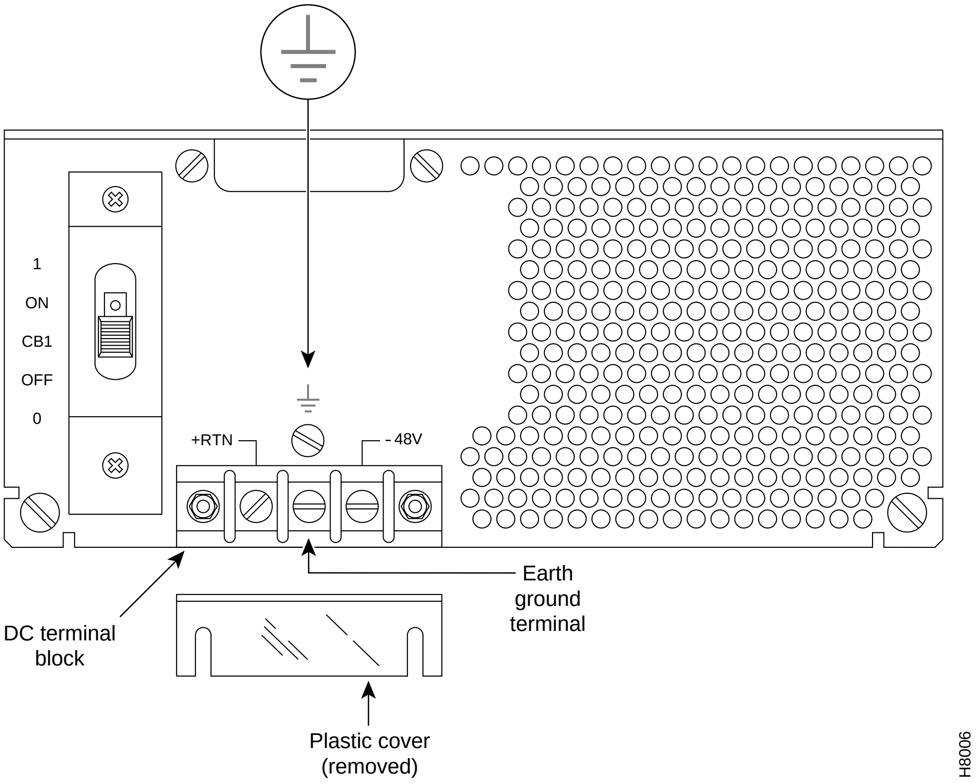


Figure 10-3 DC Power Connections—Without Conduit Box



Card Slot Fuses

Fuses for each card slot are installed to the backplane of the BPX switch to protect against catastrophic backplane damage in the event of a shorted connector power pin. Backplane fuses should rarely, if ever, need replacement. The card slot fuses are designated F4 through F18, corresponding to card slot numbers 1 through 15, respectively.

See *Chapter 29, Replacing Parts,* for instructions on replacement of these fuses. Contact Cisco Customer Service for assistance regarding their replacement.

Caution For continued protection against risk of fire, replace only with the same type and rating of fuse. Fuses should be replaced only after all power to the BPX switch has been turned off.

Fan Power Fuses

Fan fuses are located on the backplane of the BPX switch to protect against catastrophic backplane damage in the event of a shorted fan cable. Backplane fuses should rarely, if ever, need replacement. The fuses are designated F1 through F3, corresponding to fans 1 through 3.

Caution See *Chapter 29, Replacing Parts,* for instructions on replacement of these fuses, and contact Cisco Customer Service for assistance regarding their replacement.

Warning **For continued protection against risk of fire, replace only with the same type and rating of fuse. Replace fuses only after all power to the BPX switch has been turned off.**

CHAPTER 11

Installing the AC Shelf

This chapter provides procedures for:

- Installing an AC Power Supply Tray
- Installing an AC Power Supply
- AC Power Input Connections
- Card Slot Fuses
- Fan Power Fuses

Before proceeding to this chapter, complete the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or
- *Chapter 9, Installation in Customer Cabinet*

Installing an AC Power Supply Tray

The AC Power Supply Assembly is shipped separately and must be mounted directly below the BPX switch shelf. It consists of a Power Supply Tray and one or two AC power supplies. The power supplies are shipped separately from the AC Power Supply Tray.

Install power supplies **after** the BPX switch shelf is mounted in place.

All AC-powered systems are required to use a set of rear support brackets to provide additional support for the rear of the Power Supply Tray.

To install the AC Power Supply Tray:

Step 1 Use two screws to attach each of two temporary support brackets and a temporary spacer bar to the rack (see Figure 11-1 and Figure 11-2).

Step 2 Locate the small access hole in the top center of the front Air Intake Grille on the Power Supply Tray (see Figure 11-3).

Step 3 Insert a slotted blade screwdriver (0.20/0.25 inch blade width) into the access hole until it stops (approximately 1 inch).

Step 4 Carefully rotate the screwdriver approximately a quarter turn in either direction. The top of the Air Intake Grille should spring out.

Step 5 Remove the Air Intake Grille.

Figure 11-1 Temporary Spacer Bracket and Support Bracket Installation

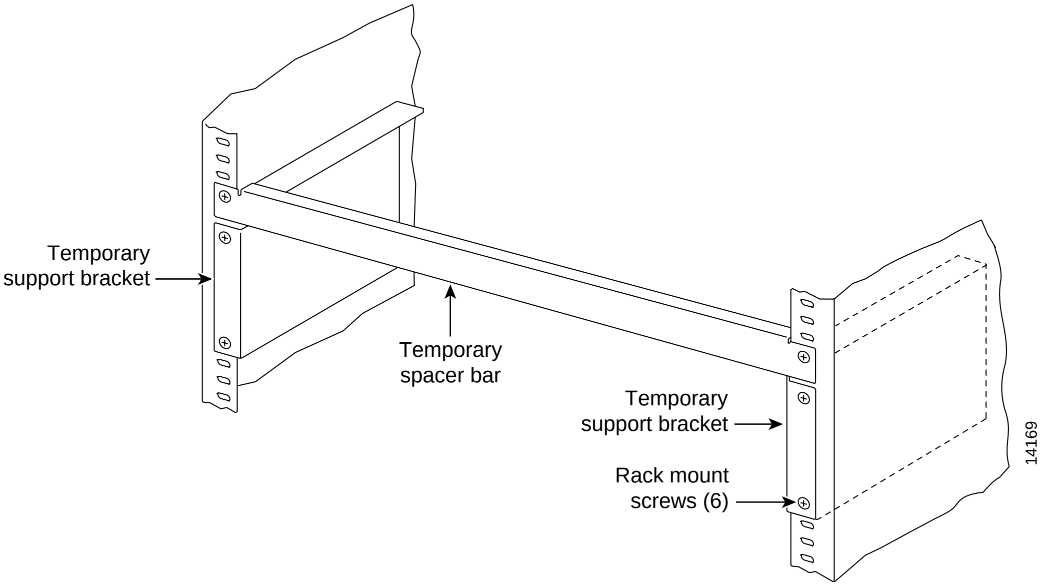


Figure 11-2 Power Supply Tray aligned with Temporary Support Brackets and Bar

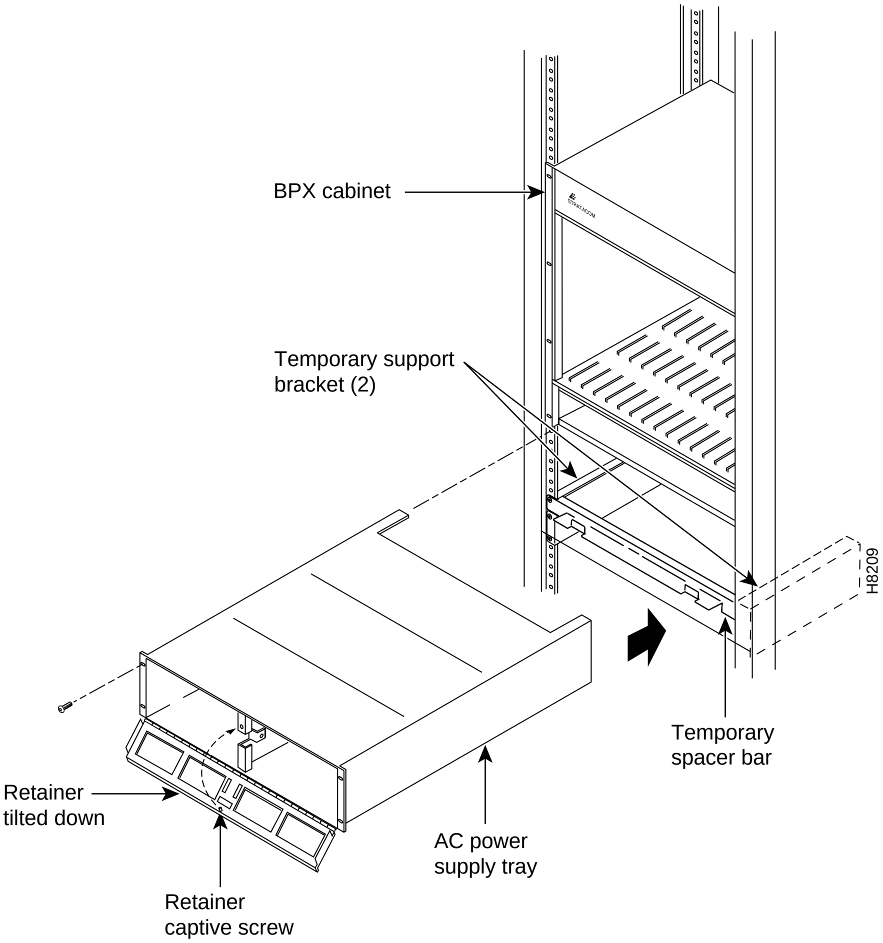
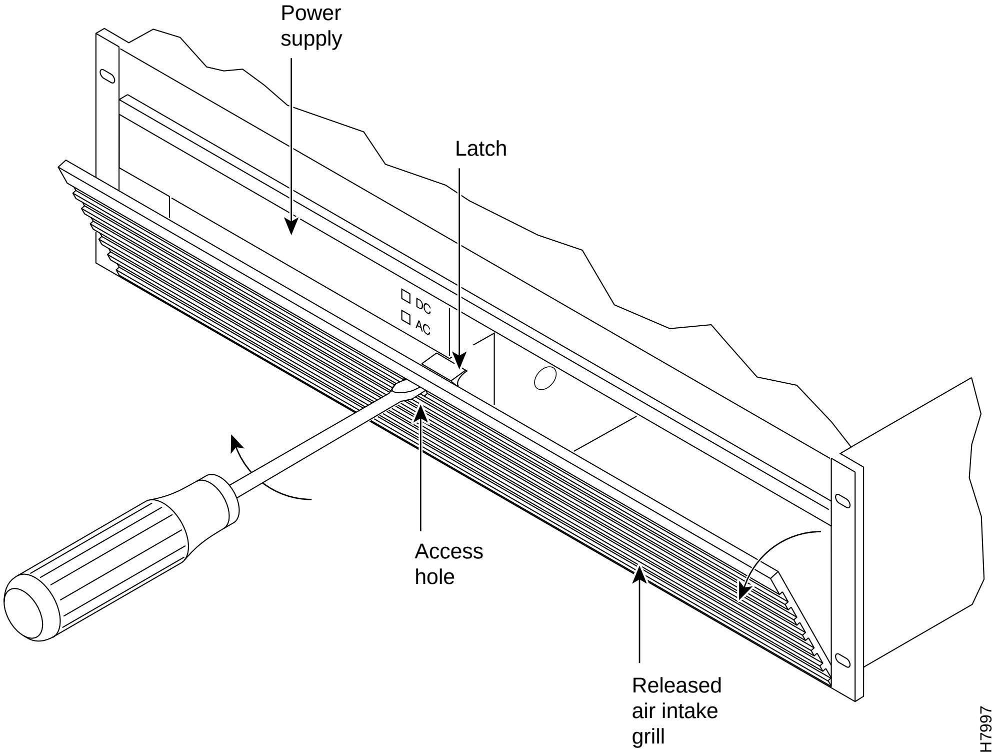


Figure 11-3 Removing an Air Intake Grille



Step 6 Slide the Power Supply Tray in the rack between the BPX switch shelf and the temporary support brackets and spacer bar (see Figure 11-2). If cables are attached, take care to avoid damaging them.

Step 7 Install screws and washers to loosely secure power supply assembly to the front of the BPX switch shelf. Align the front flanges of the Power Supply Tray with the flanges on the BPX switch shelf and tighten screws. Allow approximately 1/16” clearance between the BPX switch shelf and the Power Supply Tray to provide sufficient clearance for inserting power supplies.

Step 8 Secure the Power Supply Tray to the rear support bracket (plate) using one #10-32 screw and flat washer on each side. Use the lower hole in the brackets. Figure 11-4 shows the setup for a configuration with the vertical rails at a 30 inch setback.

For a configuration with vertical rails at a 19.86 inch rail setback, attach one #10-32 screw and flat washer to the single bracket on each side. Use the lower hole in the brackets. Figure 11-5 shows the bracket configuration only; the power supply tray position is the same as shown for in Figure 11-4.

Figure 11-4 Securing AC Power Supply Tray, 30-Inch Rail Setback

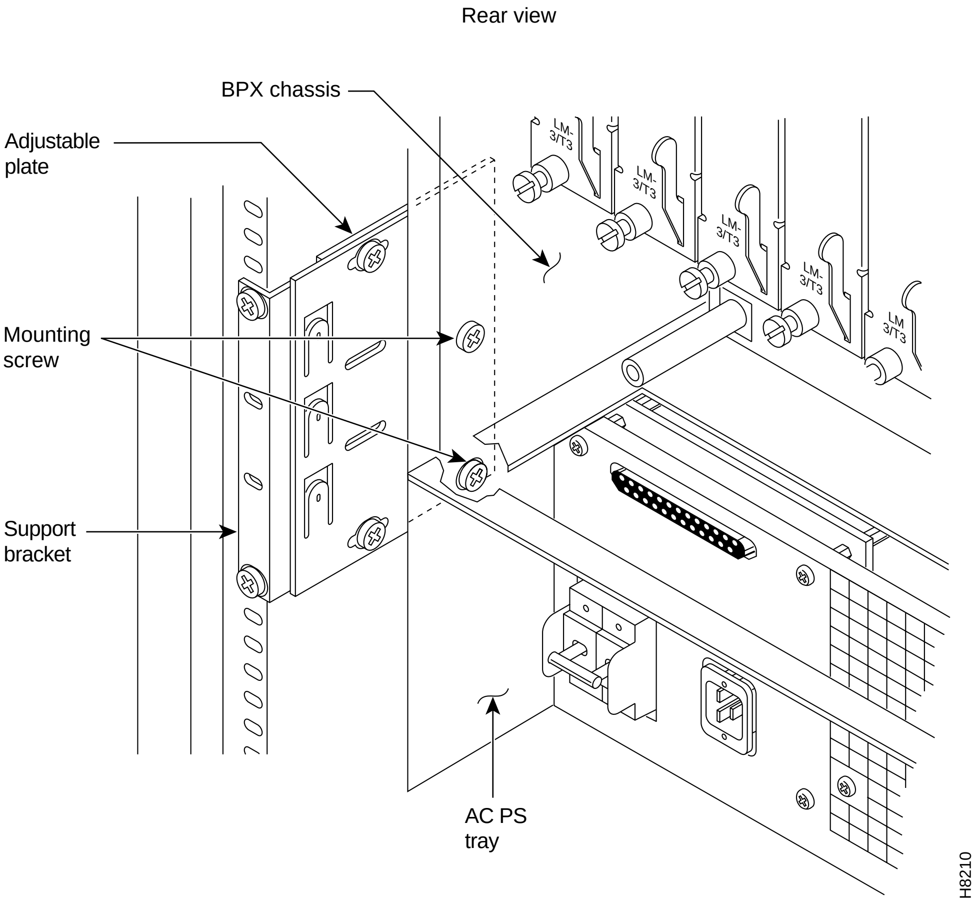
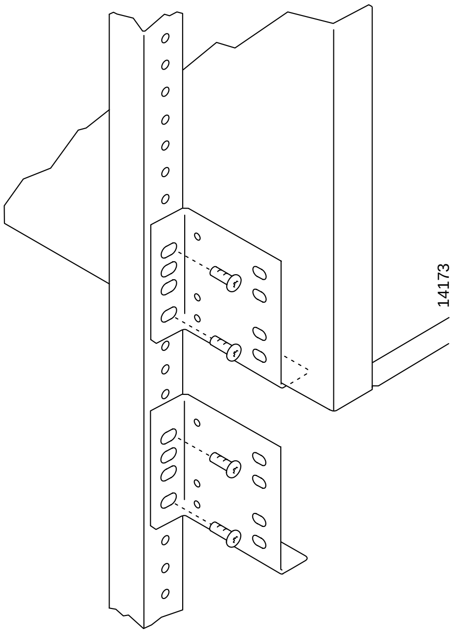


Figure 11-5 Securing an AC Power Supply Tray, 19.86 inch Rear Rail Setback

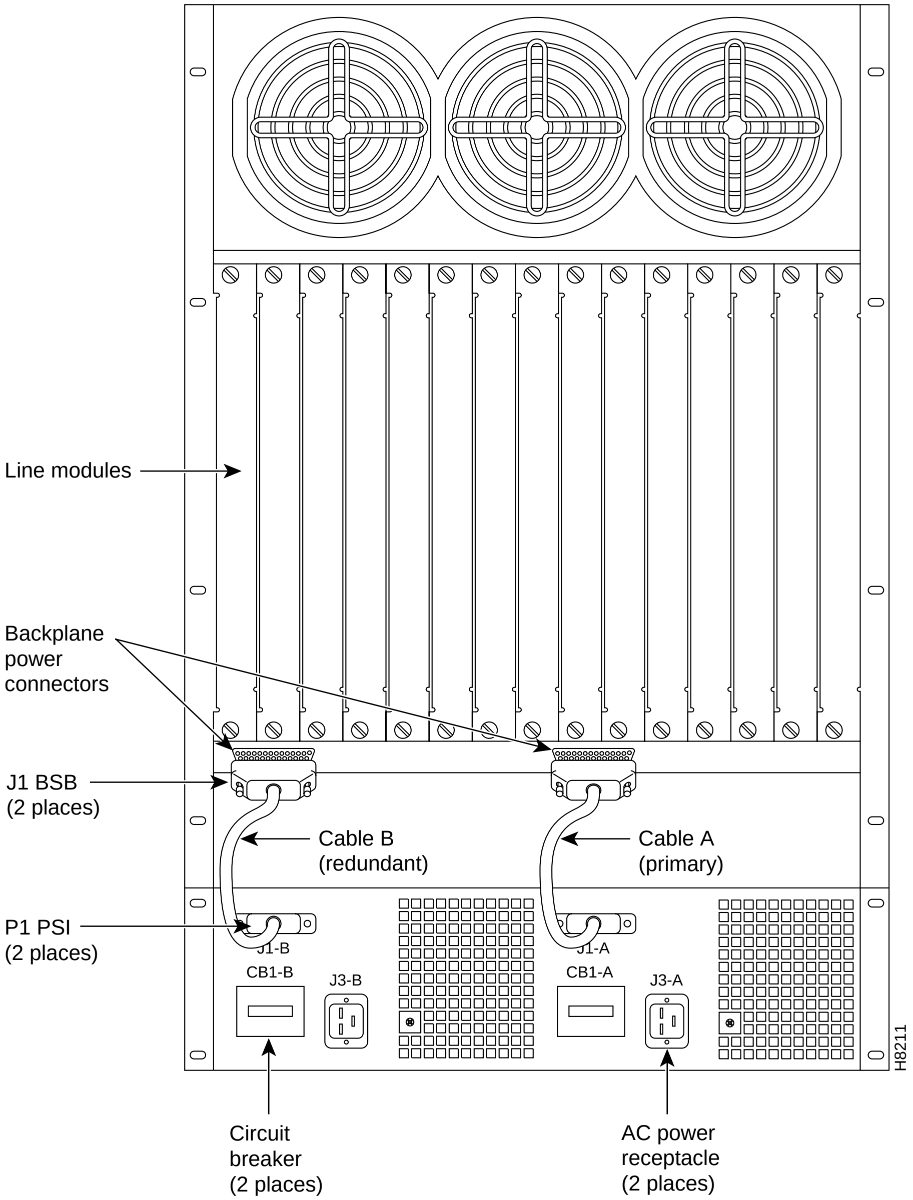


Step 9 Connect and secure a power supply interconnect cable (Cable A in Figure 11-6) between the primary AC Power Supply and the BPX switch backplane power connector.

Step 10 Connect and secure a second power supply interconnect cable (Cable B in Figure 11-6) between the redundant AC Power Supply and the BPX switch backplane power connector.

Step 11 Remove the temporary support bracket and spacer bracket from the front of the cabinet

Figure 11-6 AC Power Supply Tray with Redundant AC Inputs (view from rear)



Installing an AC Power Supply

The AC Power Supply is an assembly consisting of:

- an AC-DC converter
- cooling fan
- LED bezel
- mounting frame

The AC Power Supply must be installed and removed as an integral unit. There may be one or two AC Power Supplies depending on node configuration. They are housed in the Power Supply Tray.

To install an AC Power Supply in the Power Supply Tray:

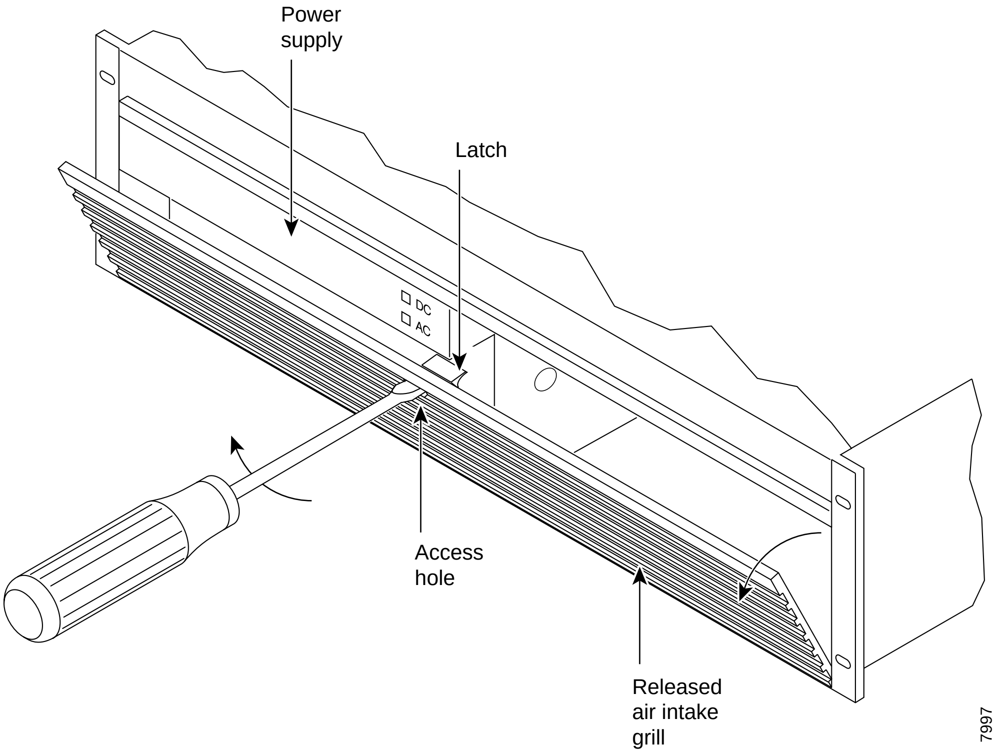
Step 1 First install the Power Supply Tray in a rack (see “Installing an AC Power Supply Tray” section).

Step 2 Set the circuit breakers at the rear of the Power Supply Tray to OFF.

Note When replacing an AC power supply, the circuit breaker at the rear of the Power Supply Tray may be left ON as the power supplies are hot pluggable.

Step 3 If not already removed, remove the Power Supply Tray front Air Intake Grille. Locate the small access hole in the top, center of the front Air Intake Grille for the Power Supply Tray (see Figure 11-7).

Figure 11-7 Removing an Air Intake Grille

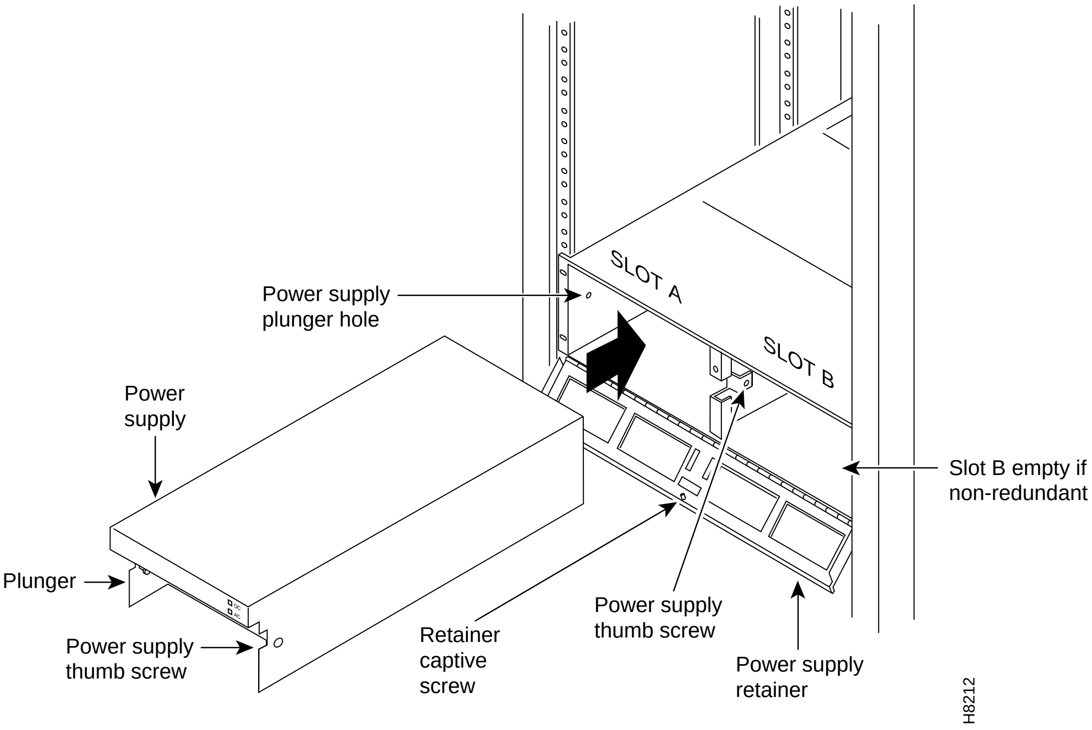


Step 4 Insert a small slotted blade screwdriver (0.20/0.25 inch blade width) into the access hole until it stops, approximately 1 inch (2.5 cm).

Step 5 Carefully rotate the screwdriver approximately a quarter turn in either direction. The top of the Air Intake Grille should spring out.

Step 6 Loosen the captive screw in the center of the power supply retainer and rotate the hinged retainer frame down (see Figure 11-8).

Figure 11-8 AC Power Supply Installation



Step 7 Align the power supply in the PS-A slots at the bottom of the Power Supply Tray and gently slide it in part way (see Figure 11-8).

Step 8 Continue to slide the power supply in until it mates with the rear connector.

Step 9 When the power supply is completely seated in its connector, the pin plunger on the left side of the supply will engage with a hole in the tray. If not, push firmly on the front edge until the power supply assembly seats in the connector.

Step 10 Screw the right-hand thumbscrew in finger tight.

Step 11 When a second power supply is provided, install it in the PS-B slot in the same manner after removing the Blank Panel from Slot B.

Step 12 Rotate the power supply retainer up and tighten the center captive screw.

Step 13 Install the Air Intake Grille. Press on the top center until the latch snaps into place.

AC Power Input Connections

There are three configurations of the AC-powered BPX switch cabinet:

- Single power supply, single AC power feed
- Dual power supplies, single AC power feed
- Dual power supplies, dual AC power feed

An 8–foot (3-meter) power cord is supplied with each AC Power Supply Assembly.

To make AC power connections to the BPX switch:

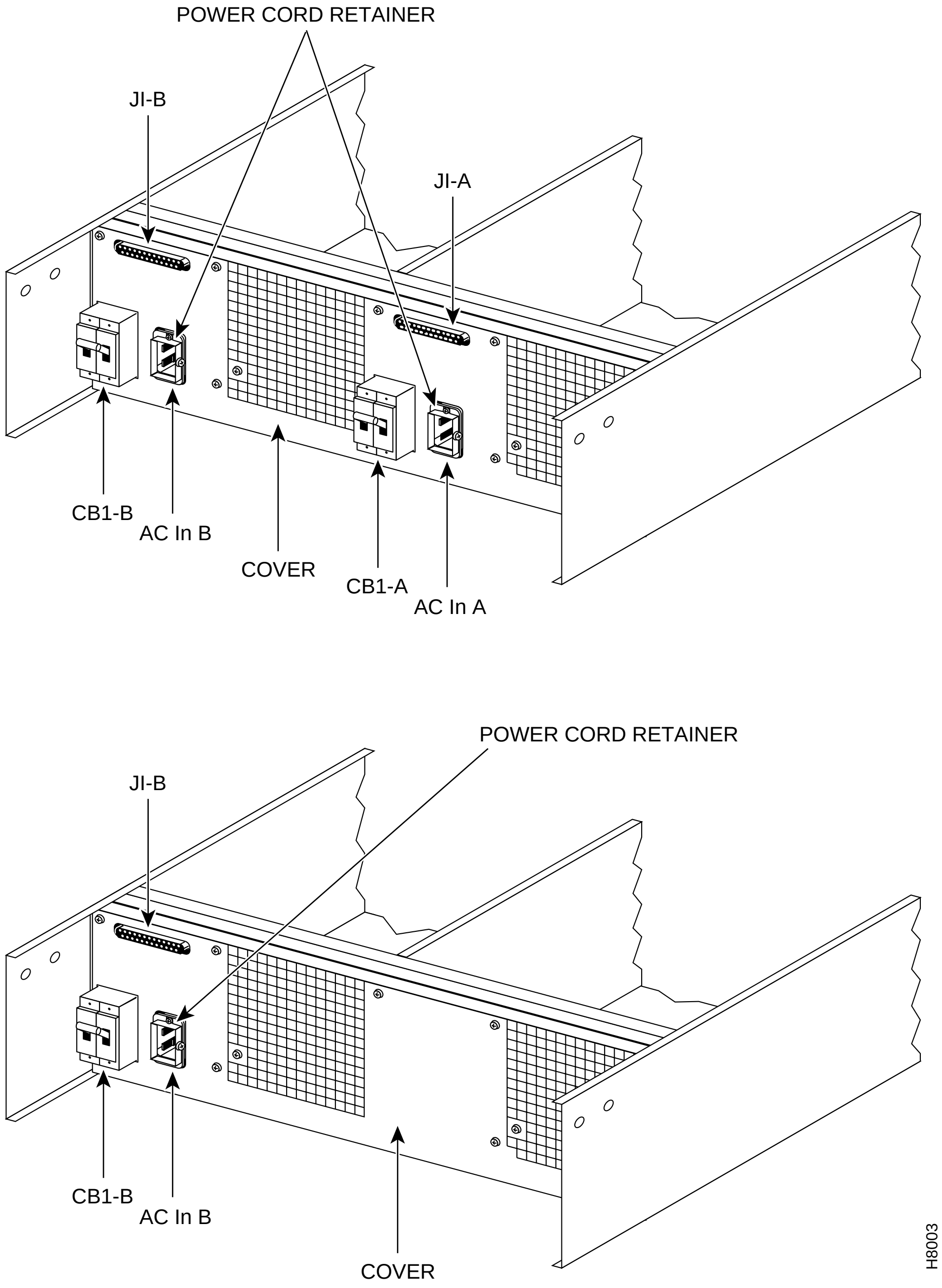
Step 1 Plug the power cords into the applicable IEC connectors as shown in Figure 11-9 and tighten the cord retainers. A separate power cord connects to each of one or two IEC connectors depending on the version of power supply shelf provided.

Step 2 Plug the BPX switch cord into a 220 to 240 VAC single-phase wall outlet capable of supplying 20 A. The building circuit should be protected with a 20 A circuit breaker.

Note The BPX switch circuit breaker is 20 A to provide improved system availability for installations with a single line cord and (N+1) power supplies.

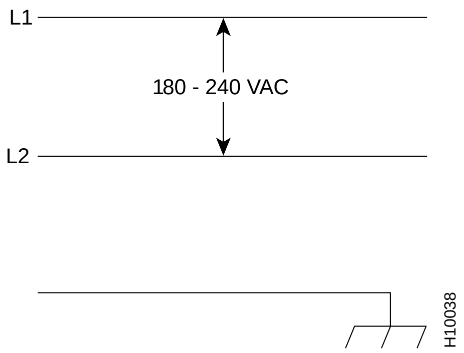
Step 3 For the dual power feed version, plug each power cord into receptacles on separate building circuits to provide protection against a power feed failure. Each building circuit should be protected with a 20 A circuit breaker.

Figure 11-9 AC Power Supply Connections (Dual and Single Versions Shown)



Step 4 The ground (green/yellow) wire of the AC power cord provides the safety ground to the BPX switch via the grounding prong on the three-prong connectors. Make sure the building AC receptacle is also properly grounded (see Figure 11-10).

Figure 11-10 AC Power



Step 5 As applicable, provide a convenience AC outlet strip, with at least four outlets, near the BPX switch to power optional modems, CSU, or DSUs, test equipment, and so on. There is no accessory AC outlet supplied on the BPX switch. This outlet strip should be connected to a source of AC voltage normal for the region (such as, 115 VAC for domestic US use).

Step 6 Proceed to *Chapter 13, Installing the BPX Switch Cards*.

Card Slot Fuses

Fuses for each card slot on the backplane of the BPX switch protect against catastrophic backplane damage in the event of a shorted connector power pin. The card slot fuses are designated F4 through F18, corresponding to card slot numbers 1 through 15, respectively.

Backplane fuses should rarely, if ever, need replacement.

See *Chapter 29, Replacing Parts*, for instructions on replacement of these fuses, and contact Customer Service for assistance regarding their replacement.

Caution For continued protection against risk of fire, replace only with the same type and rating of fuse. Fuses should be replaced only after all power to the BPX switch has been turned off.

Fan Power Fuses

Fan fuses are located on the backplane of the BPX switch to protect against catastrophic backplane damage in the event of a shorted fan cable. Backplane fuses should rarely, if ever, need replacement. The fuses are designated F1 through F3, corresponding to fans 1 through 3.

Caution See *Chapter 29, Replacing Parts*, for instructions on replacement of these fuses, and contact Customer Service for assistance regarding their replacement.

Caution For continued protection against risk of fire, replace only with the same type and rating of fuse. Replace fuses only after all power to the BPX switch has been turned off.

CHAPTER 12

Installing the T3/E3 Cable Management Tray

This chapter provides instructions for the installation of the optional cable management tray that you can use to route cables in an open-rack, non-redundant configuration:

- Installation of Cable Management Tray
- Raising Tray for Access to PEMs
- Installing BXM T3/E3 Cable Bracket
- Connecting Cables to BXM T3/E3 Cards
- Routing Cables from Cards through Cable Management Tray
- Tray Raised with Cables in Place

You will need to obtain the optional cable management tray kit and one each BXM T3/E3 cable bracket kit for each BXM T3/E3 card.

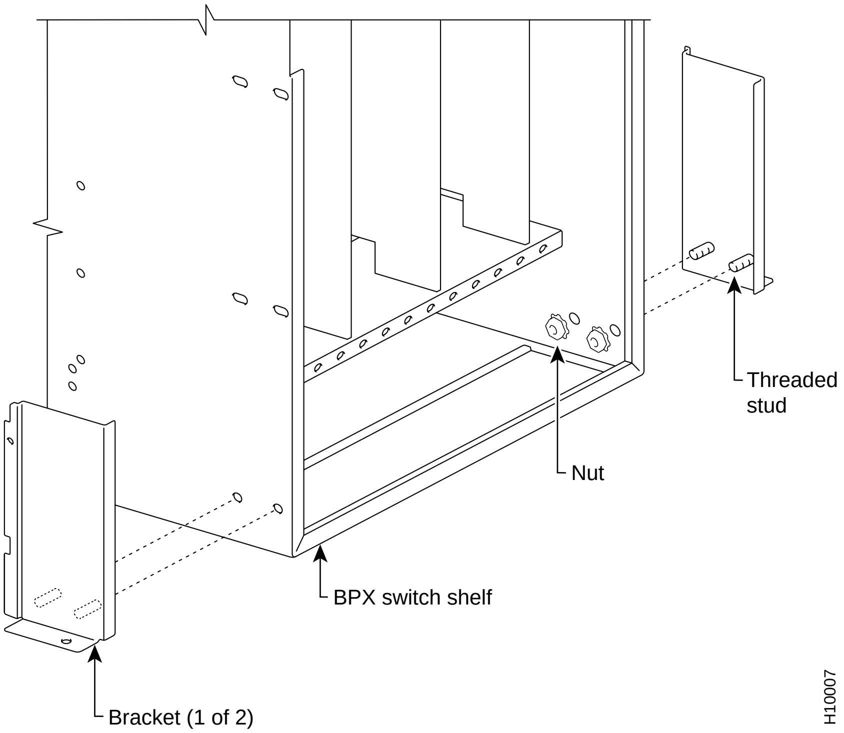
Installation of Cable Management Tray

Installing Tray Brackets

Step 1 Obtain brackets and associated hardware from the kit.

Step 2 Install left and right brackets, using two nuts to secure each bracket, Figure 12-1.

Figure 12-1 Installation of Cable Management Tray Brackets



Installing Tray

Step 1 Using two hands to hold the cable management tray, slide it over the brackets Figure 12-2.

Step 2 Lower the tray into the lower rest position Figure 12-3.

Figure 12-2 Sliding Cable Management Tray over Brackets

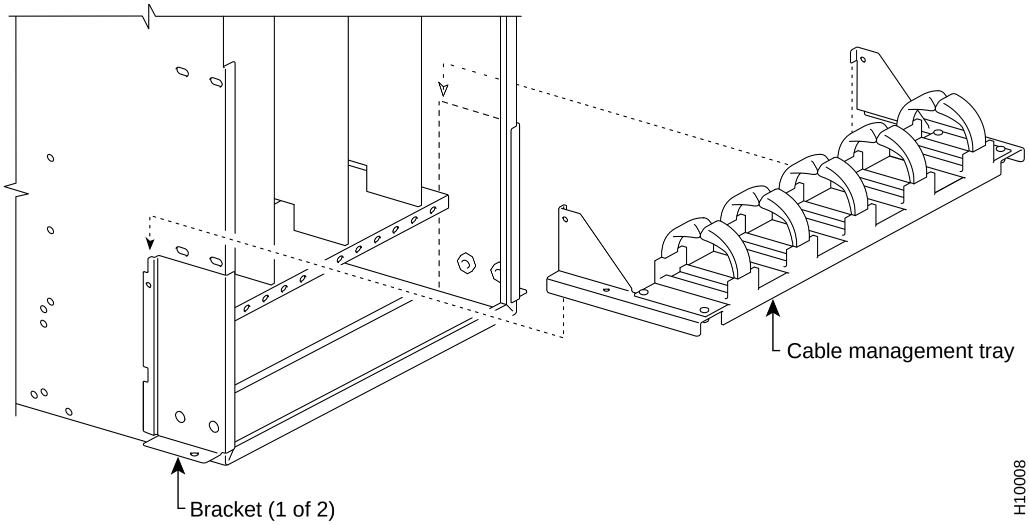
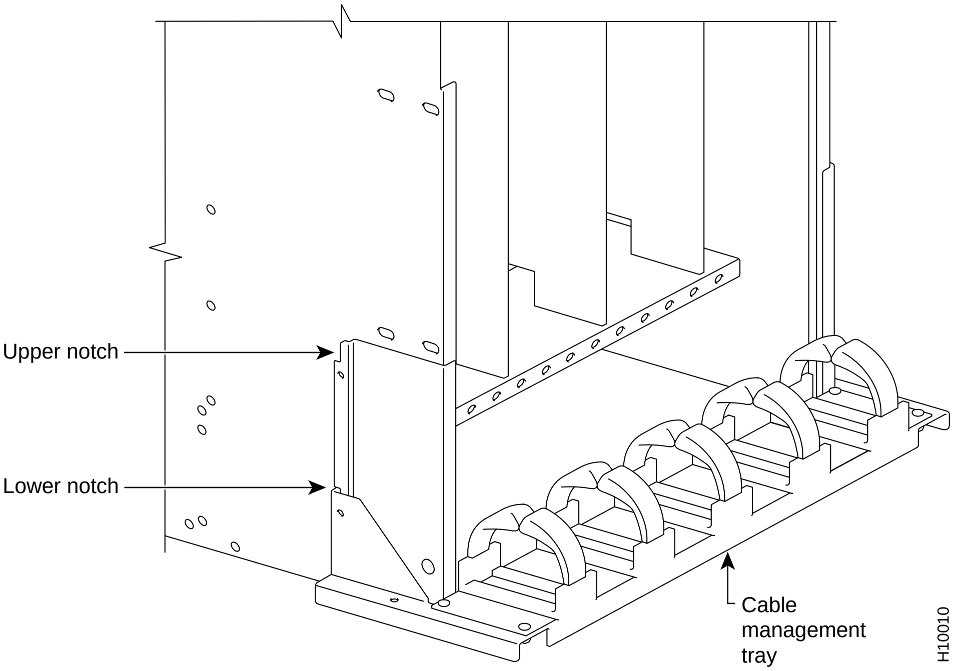


Figure 12-3 Cable Management Tray in Lowered Home Position



Raising Tray for Access to PEMs

You should raise the tray only when necessary to access the Power Entry Modules (PEMs), typically for replacement or to install a second PEM. Figure 12-4 shows the tray in the raised position.

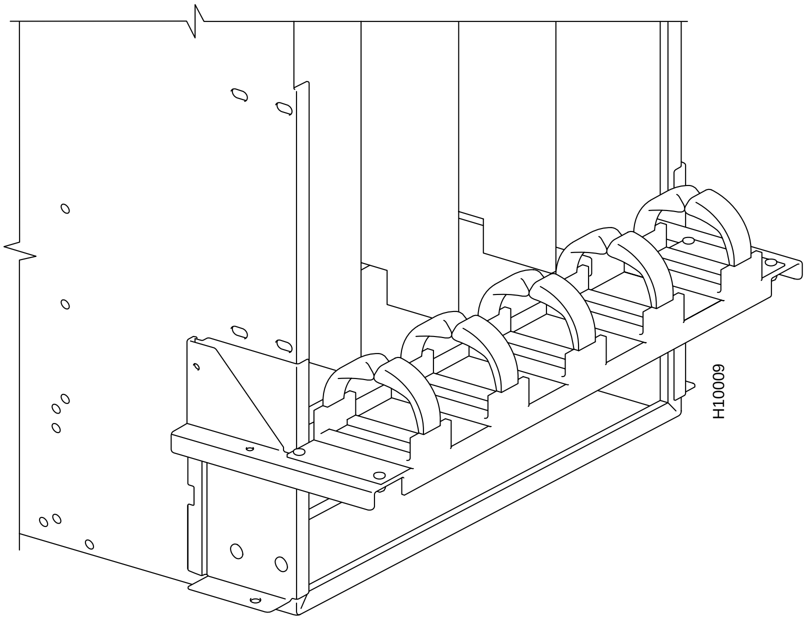
To raise the tray to provide access to the PEMs:

Step 1 Remove the securing screws as necessary.

Step 2 With two hands, pull the tray towards yourself and up.

Step 3 Raise the tray to the upper position and lower it onto the upper slots.

Figure 12-4 Cable Management Tray in Raised Position



Installing BXM T3/E3 Cable Bracket

To attach the BXM T3/E3 cable bracket to each BXM T3/E3 card as shown in Figure 12-5:

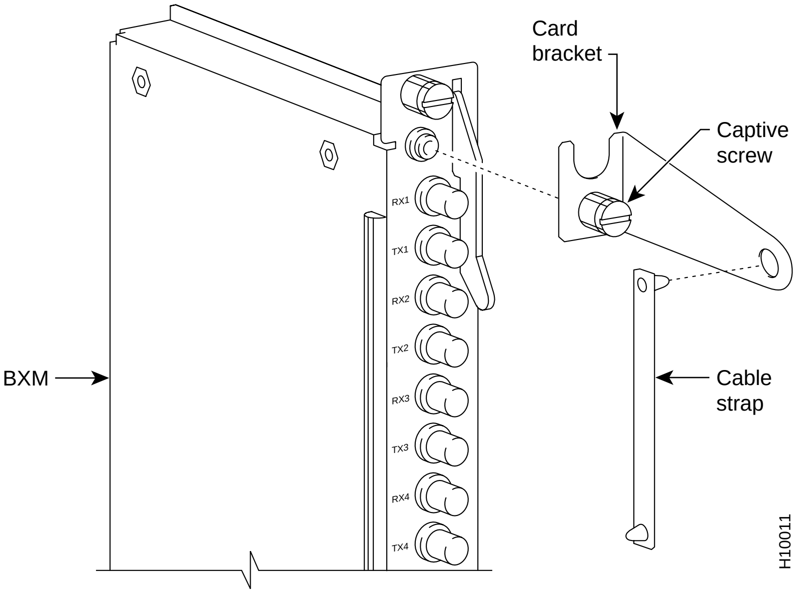
Step 1 Remove the bracket from the kit.

Step 2 Place the bracket in position as shown.

Step 3 Screw in and tighten the captive screw.

Step 4 Insert one end of the cable tie through the hole in the bracket.

Figure 12-5 Installing BXM T3/E3 Cable Bracket



Connecting Cables to BXM T3/E3 Cards

To route the cables as shown in Figure 12-6 and Figure 12-7:

Step 1 Connect the cables to the card by pushing on the SMB connector locking sleeves as you push the cable connectors on to the card connectors.

Step 2 Dress the cables upward to provide a service loop.

Step 3 Bundle the cables by using cable ties.

Step 4 Wrap the cable strap around the cables and secure them to the cable management bracket.

Note To disconnect cables from a card, pull on the cable connector locking sleeve as you pull the cable connector away from the card connector.

Figure 12-6 Connecting Cables to T3/E3 Card

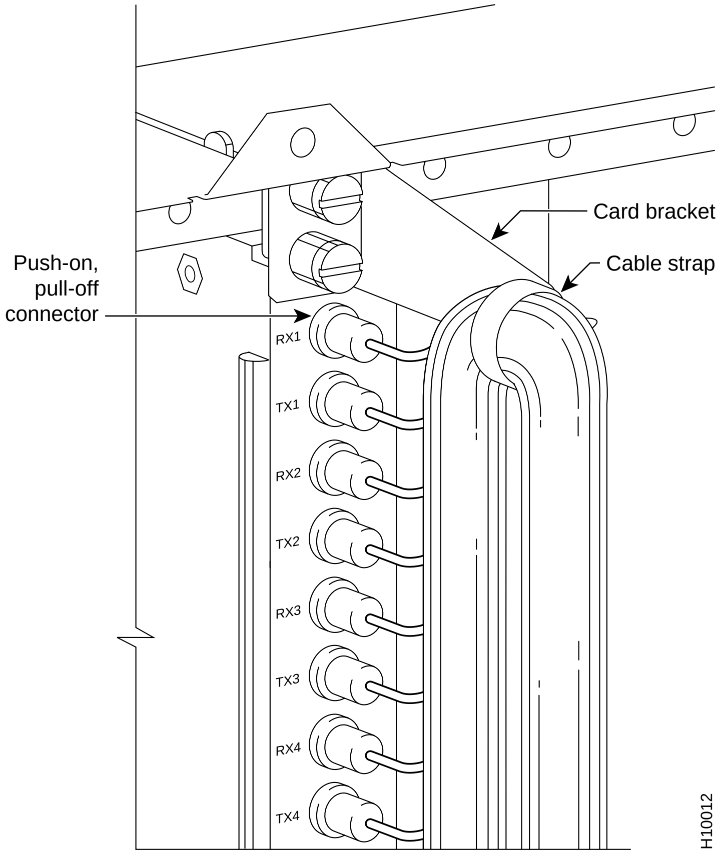
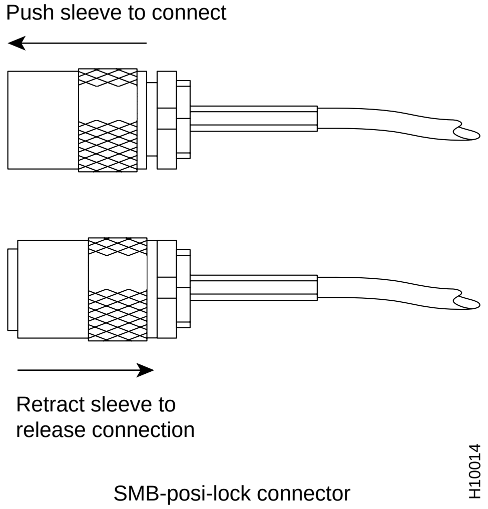


Figure 12-7 T3/E3 SMB Connector Detail



Routing Cables from Cards through Cable Management Tray

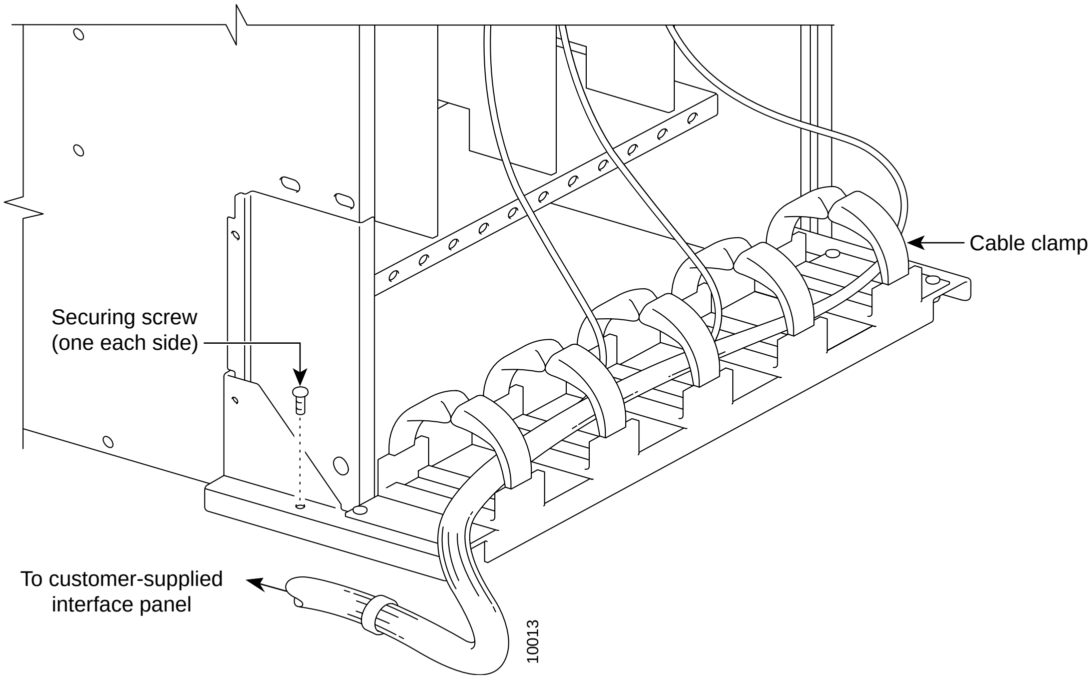
To route cables as shown in Figure 12-8:

Step 1 Verify that the cable management tray is in the lowered home position.

Step 2 Route cables from the cards through the cable clamps on the cable management tray.

Step 3 Secure the cable management tray to the cable tray brackets by inserting and tightening securing screw, one to each bracket.

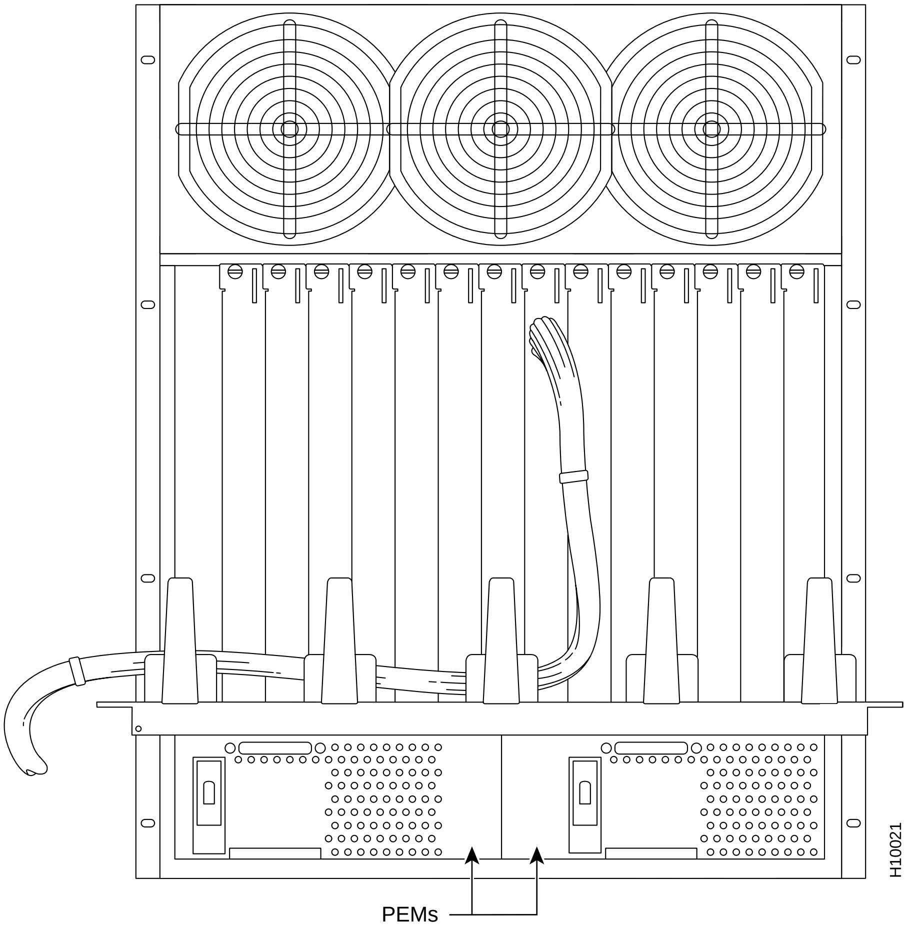
Figure 12-8 Cables Routed through Cable Management Tray in Lowered Position



Tray Raised with Cables in Place

Figure 12-9 shows how to raise the cable management tray with cables in place, to provide access to the Power Entry Modules (PEMs).

Figure 12-9 Tray Raised with Cables in Place



CHAPTER 13

Installing the BPX Switch Cards

This chapter explains how to install the BPX switch cards, check for a 9.6 or 19.2 Gbps backplane, connect line and trunk cables, connect peripherals, connect to a network management station, initial power up, and initial configuration:

- Installing the Cards
- Verifying 9.6 or 19.2 Gbps Backplane
- Upgrading to BCC-4 Cards
- Specifying Card Redundancy
- Installation of APS Redundant Frame Assembly and Backcards

Before proceeding to this chapter, you should first complete the procedures in either:

- *Chapter 10, Installing the DC Shelf;* or
- *Chapter 11, Installing the AC Shelf*

  and
- *Chapter 12, Installing the T3/E3 Cable Management Tray*

and before that, the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or
- *Chapter 9, Installation in Customer Cabinet*

Installing the Cards

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the strap lead to the cabinet, or use the wrist strap that is connected to the cabinet.

The card shelf in the BPX switch has card slots numbered from 1 to 15, as viewed from left to right from the front of the cabinet. Front and rear views of the BPX switch card shelf are shown in Figure 13-1 and Figure 13-2, respectively.

Here is a summary of the card installation rules for the BPX switch:

Non-Redundant Nodes:

- Use either a Broadband Controller Card:
  BCC-4V
  BCC-3-32M
  BCC-3-64M, or
  BCC-32
  in front slot number 7.
- With a
  BCC-4V
  BCC-3-32M, or
  BCC-3-64M front card,
  use a BCC-3-BC backcard in back slot number 7,
  OR:
- With a BCC-32 front card, use a BCC15-BC in back slot number 7.

Redundant Nodes:

- Use two Broadband Controller Cards, a pair of:
  BCC-4Vs,
  BCC-3-32Ms,
  BCC-3-64Ms, or
  BCC-32s
  in front slot numbers 7 and 8.
- With:
  BCC-4V,
  BCC-3-32M, or
  BCC-3-64M front cards
  use BCC-3-BC backcards in back slot numbers 7 and 8,
  OR:
- With BCC-32 front cards, use BCC15-BC backcards in back slot numbers 7 and 8.

Note In some cases, it may be possible to operate two of the three types of BCCs with their proper backcards temporarily for maintenance purposes, that is, replacing a failed controller card. Contact Customer Service for assistance.

- Place the ASM card in front slot number 15.
- Place the LM -ASM card in back slot number 15.
- Place the cards BNI-3T3 or BNI-3E3 in any other front slot than 7, 8, or 15.
- Place the cards LM -3T3, LM-3E3, 2OC3-SMF, 2OC3-MMF in all back slots with a BNI in the corresponding front slot.

Figure 13-1 BPX Shelf (front view)

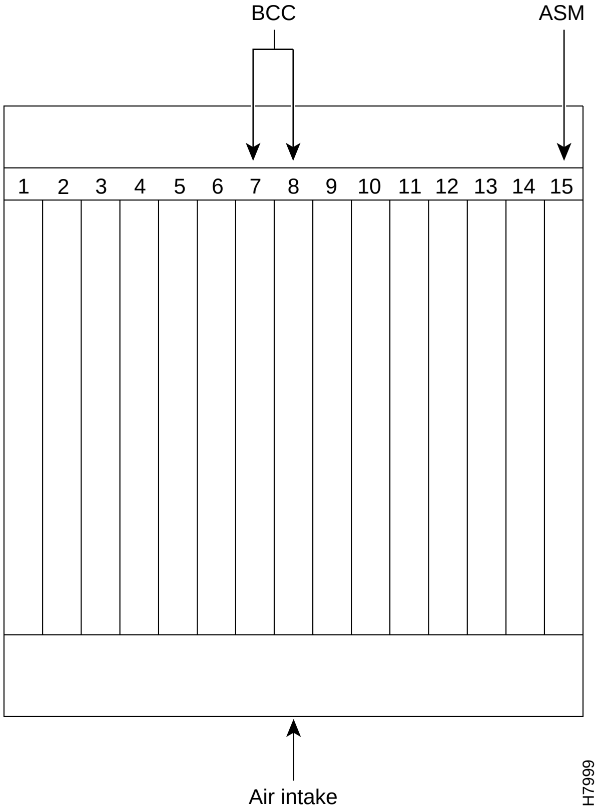
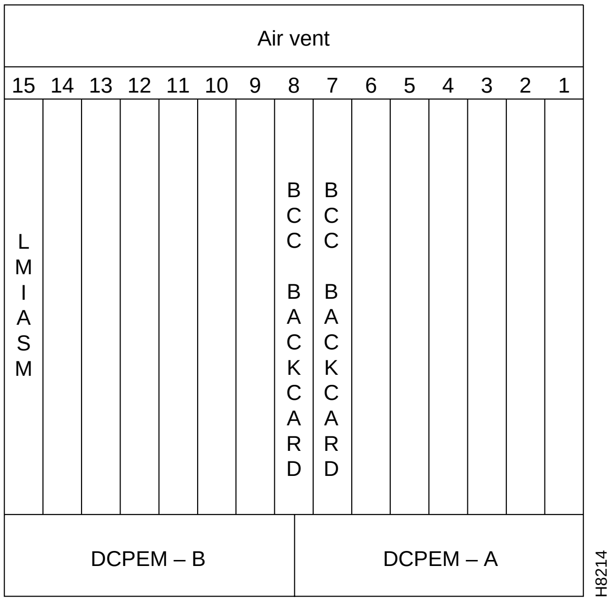


Figure 13-2 BPX Shelf (rear view, DC shelf shown)



Installing Front Cards

Before following the front card installation procedure, carefully note and perform each of the following cautionary steps:

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the strap lead to the cabinet, or use the wrist strap that is connected to the cabinet.

Caution You must use Blank Front Card and Rear Face Plates to fill/cover empty card slots to eliminate Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI) and to ensure correct air flow through the card cage.

Systems may be shipped with empty shelves, with filler cards or with plug-in cards installed. If filler cards are installed in each slot, then you must replace some of them may with functional cards. The front cards are held captive mechanically by the Air Intake Grille and can not be removed until the lower Air Intake Grille is released.

Caution Do not attempt to remove a front card from the BPX switch cabinet until the Air Intake Grille is released and lowered or the Air Intake Grille and/or card extractors may be damaged.

Caution Before any card is installed, always examine the chassis backplane and card cage guides for any signs of loose or misplaced EMI gasketing. Examine the backplane connectors for bent or damaged connection or pre-power pins.

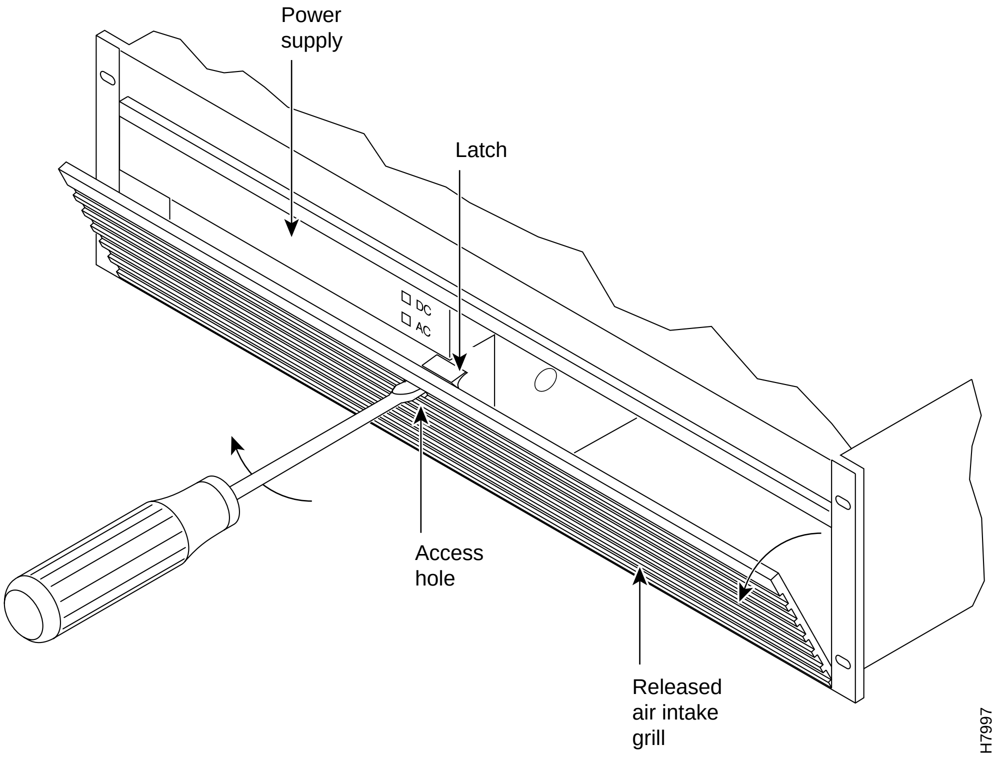
To remove or to install a front card:

Step 1 Turn off all power to the BPX switch.

Note It is a good idea to **turn off power** when initially installing cards. When replacing cards on an operating BPX switch, it is not necessary to turn off power because the cards are hot pluggable.

Step 2 Locate the small access hole in the top center of the front Air Intake Grille below the card slots (see Figure 13-3 for location).

Figure 13-3 Removing an Air Intake Grille



Step 3 Insert a small slotted blade screwdriver (0.20/0.25 inch blade width) into the access hole until it stops (approximately 1 inch).

Step 4 Carefully rotate the screwdriver approximately a quarter turn in either direction. The top of the Air Intake Grille should spring out.

Step 5 Remove Air Intake Grille.

Step 6 To remove a card, rotate the extractor handles at the top and bottom of the card to release the card and slide it out.

Step 7 To insert a new card, position the rear card guides over the appropriate slots at the top and bottom of the card cage.

Step 8 Gently slide the card in all the way to the rear of the slot and seat the board by fully seating both extractor handles. The handles should snap back to a vertical position when seated.

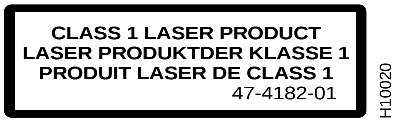
Note The card should slide in with slight friction on the adjacent board’s EMI gaskets. Investigate any binding. Do not use excessive force.

Installing Back Cards

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the strap lead to the cabinet, or use the wrist strap that is connected to the cabinet.

The optical ports contain an information label as shown in Figure 13-4.

Figure 13-4 Laser Information Label



CLASS 1 LASER PRODUCT
LASER PRODUKTDER KLASSE 1
PRODUIT LASER DE CLASS 1
47-4182-01

Warning **Invisible radiation may be emitted from the optical ports of the single-mode or multi-mode products when no fiber cable is connected. Avoid exposure and do not look into open apertures. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment.)**

Warning **Class 1 laser product. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment.)**

Warning **Laser radiation when open. (For translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment.)**

To install back cards:

Step 1 Locate the card slot for the card to remove or install.

Step 2 For existing installations, remove any cables that may be attached and label them so they may be replaced in the same location.

Step 3 Loosen the captive mounting screws on both top and bottom of the line module faceplate by using a slotted blade screwdriver (see Figure 13-5).

Step 4 Lift the extractor handles at the top and bottom, and slide out the line module.

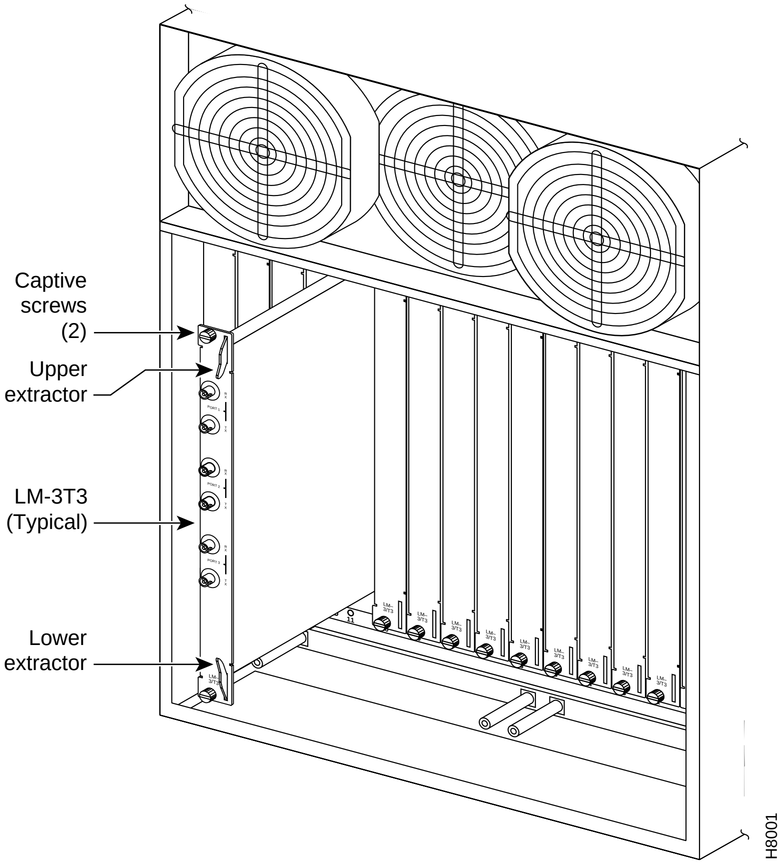
Step 5 To re-insert the line module, locate the corner edges of the card into the appropriate guide slots at the top and bottom of the card cage. Gently slide the card in all the way to the rear of the slot and push to seat the card in the connector.

Note The card should slide in easily. Investigate any binding.
Do not use excessive force.

Step 6 Screw in the captive screws.

Step 7 Replace any cables that may have been removed in step 2.

Figure 13-5 Installing a Back Card



Verifying 9.6 or 19.2 Gbps Backplane

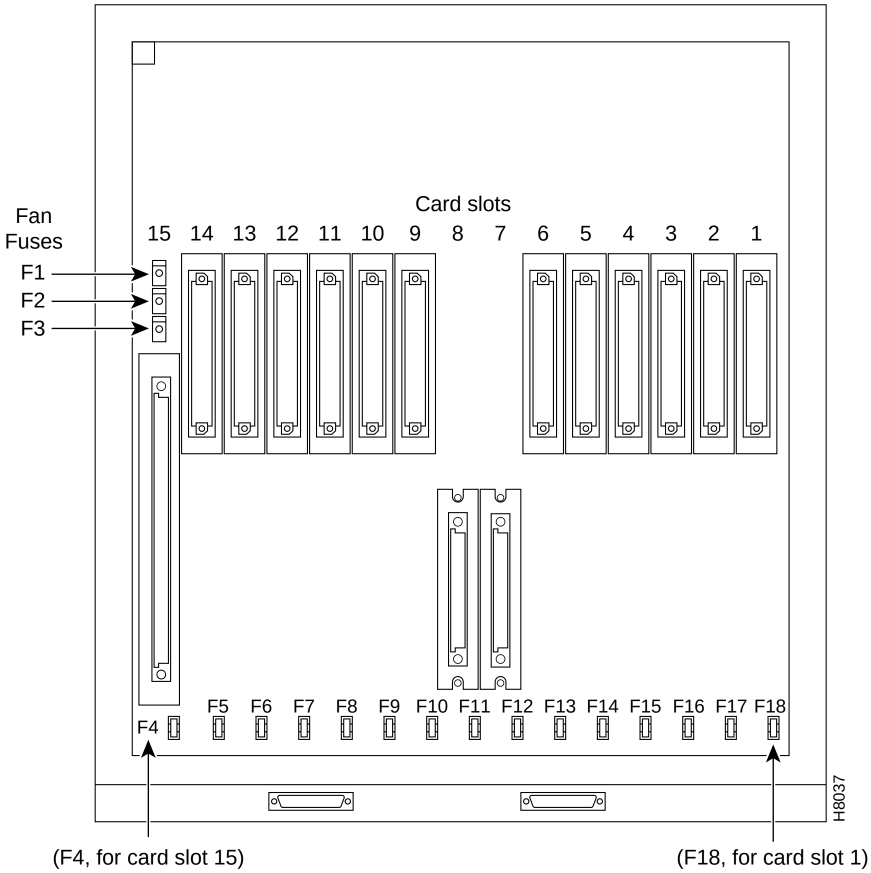
Operation of the BPX Switch at 19.2 Gbps entails these requirements:

- A 19.2 Gbps backplane.
- BCC-4 or later controller cards.
- One or more BXM cards.
- Release 8.4.18 or later switch software.
- A backplane NOVRAM that is programmed to identify the backplane as a 19.2 Gbps backplane.

  Switch software will not allow node operation at 19.2 Gpbs unless it can read the backplane NOVRAM to verify that the backplane is a 19.2 Gbps backplane.

You can visually identify the 19.2 backplane by the small white card slot fan fuses at the bottom rear of the backplane. These fan fuses are approximately 1/4 inch high and 1/8 inch wide. The 9.6 Gbps backplane does not have these fuses.

Figure 13-6 Card slot and fan fuses, identifying the 19.2 Gpbs backplane



If the BPX Switch is a late model, then a 19.2 Gbps backplane is installed. You can verify this by running the **dspbpnv** command which will display “Word #2 =0001” if the backplane NOVRAM has been programmed. If anything else is displayed, you’ll have to visually check the backplane for the fuses.

If the backplane is a 19.2 Gbps backplane, but the backplane NOVRAM has not been set to display Word #2 =0001, then you can use the **cnfbpnv** command to program the NOVRAM.

To use the **cnfbpnv** command to program the NOVRAM:

Step 1 Enter **cnfbpnv**. The response is:

```
Are you sure this is a new backplane (y/n).
```

Step 2 Enter **y**

Step 3 Confirm that the change has been made by entering **dspbpnv** to confirm the response:

```
Word #2 =0001
```

Note If for some reason the change does not take place, it will be necessary to change the backplane NOVRAM. Contact customer service.

Step 4 Enter **switchcc** so that the change will be recognized by the switch software.

If the backplane is not a 19.2 Gbps backplane, then it will be necessary to install a 19.2 Gbps backplane to obtain 19.2 Gbps operation. Contact Cisco Customer Service.

Upgrading to BCC-4 Cards

BCC-4 cards support 19.2 Gbps performance of the BXM cards.

Note that BCC-4 cards requires that the backplane be either a 9.6 or 19.2 Gbps backplane. Refer to the previous section, Verifying 9.6 or 19.2 Gbps Backplane, page 13-7.

To upgrade to BCC-4 cards:

Step 1 Remove the current standby BCC front and back card.

Note If the control card being replaced is a BCC-3, the BCC-3 backcard (BCC-3-bc) can be used as it is used with both the BCC-3 and BCC-4 front cards.

Step 2 Replace with new BCC-4 front and back cards.

Step 3 Wait for the standby updates on the newly installed standby BCC-4 to complete.

Step 4 Issue a **switchcc** command to utilize the newly installed BCC-4.

Step 5 Verify that the network is stable.

Step 6 Remove the current standby BCC front and back card.

Step 7 Replace with new BCC-4 front and back cards that are identical to the current active BCC-4.

Step 8 Wait for the standby updates on the newly installed standby BCC-4 to complete.

Step 9 The BCC-4 physical upgrade is now complete.

After step 2, the node will contain a mix of an old type BCC and the new type BCC-4. This condition is permitted only while the standby updates to the new BCC are in progress, which will take less than one hour.

You should keep the time during which this mixture of BCC types exists to a minimum by immediately replacing the second old type BCC with the matching BCC of the new type.

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.

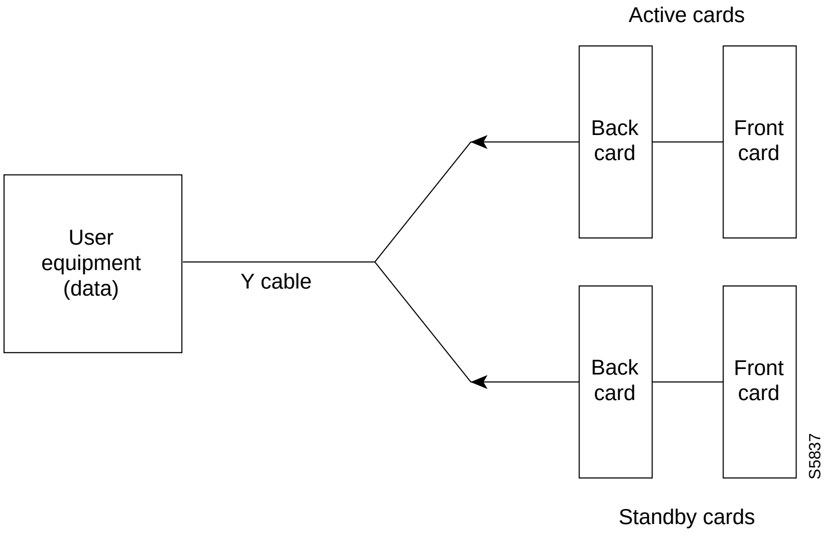
BPX card sets may consist of the following:

- 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 SMF 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.
- Most service cards on the IGX and BPX nodes support Y-cable redundancy, with the exception of MMF back cards which do not support Y-redundancy
- Most trunk cards support trunk redundancy. See *Chapter 9, Installation in Customer Cabinet*, for a description.

Figure 13-7 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.

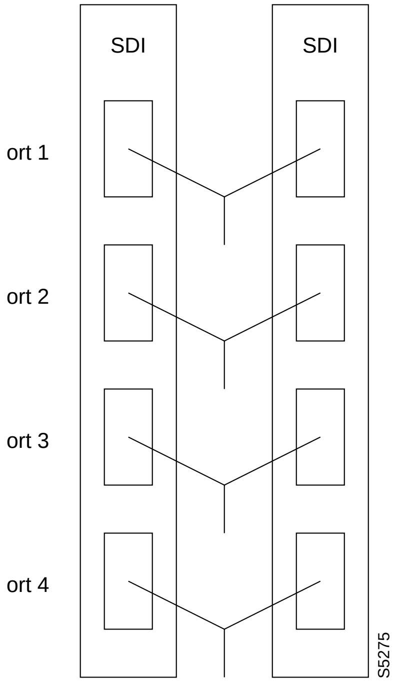
Figure 13-7 Y-Cable Connection



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 13-8 illustrates the cabling for a multiport card set.

Figure 13-8 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.

BPX mismatch types:

- feature mismatch
- back card mismatch
- front card mismatch

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 in the *Cisco WAN Switching Command Reference* for details.

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

Installation of APS Redundant Frame Assembly and Backcards

The procedures in this section provide installation instructions for the SONET Automatic Protection System (APS) Redundant Frame Assemblies and backcards. These may be used to provide line and card redundancy for BXM OC-3 and OC-12 cards.

The APS protocols supported by the BXM are listed in Table 13-1 and shown in Figure 13-9 and Figure 13-10.

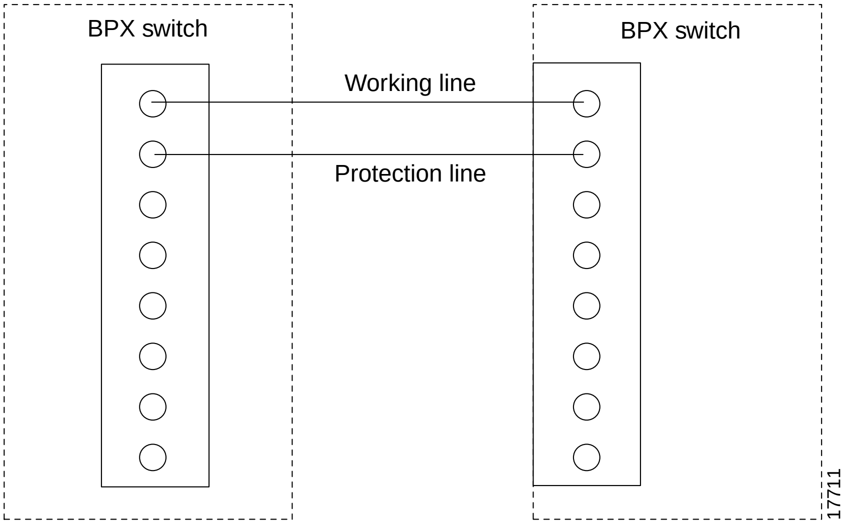
Table 13-1 BXM SONET APS

APS 1:1	The APS 1:1 redundancy provides line redundancy, using adjacent lines on the same BXM backcard.
APS 1+1	The APS 1+1 redundancy provides card and line redundancy, using the same numbered ports on adjacent BXM backcards.

APS 1:1 Redundancy Installation

APS 1:1 redundancy provides line redundancy only and is supported with the standard BXM OC-3 and OC-12 front and back cards.

Figure 13-9 APS 1:1 Redundancy



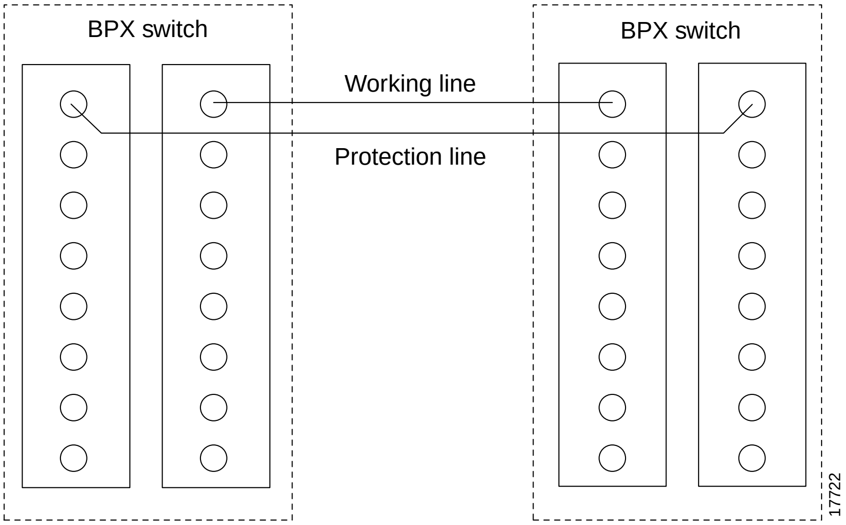
APS 1+1 Redundancy Installation

APS 1+1 redundancy provides both card and line redundancy. It uses the standard BXM OC-3 and OC-12 front cards but requires a special APS Redundant Backplane and APS Redundant backcards.

With previous card cages, because of the positioning of mechanical dividers, the APS card pairs could be inserted only in slots 2 through 5 and 10 through 13. The mechanical dividers are located at slots 1 and 2, 5 and 6, 9 and 10, and 13 and 14.

With current card cages, this limitation is removed so that the APS card pairs 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).

Figure 13-10 APS 1+1 Redundancy



To install APS Redundant Frame Assembly and backcards:

Step 1 If not already in place in the APS Redundant Frame Assembly, slide the two APS backcards into the APS Redundant Frame Assembly.

Warning **Nylon standoffs on the APS Redundant Frame Assembly must be in place to prevent shorting against -48 VDC pins and ground pins on the BPX Midplane.**

Step 2 Verify that nylon standoffs are securely installed on APS Redundant Frame Assembly (see Figure 13-11).

Step 3 Carefully slide APS Redundancy Frame Assembly and APS cards into selected side-by-side slots at the back of the BPX shelf (see Figure 13-12). Slide the APS Redundancy Frame Assembly and cards into the BPX shelf until snug against the BPX midplane (see Figure 13-13).

Step 4 Going back and forth between the screws, gradually tighten retaining screws at top and bottom of the APS backcards until all are secure.

Figure 13-11 APS Redundant Frame Assembly

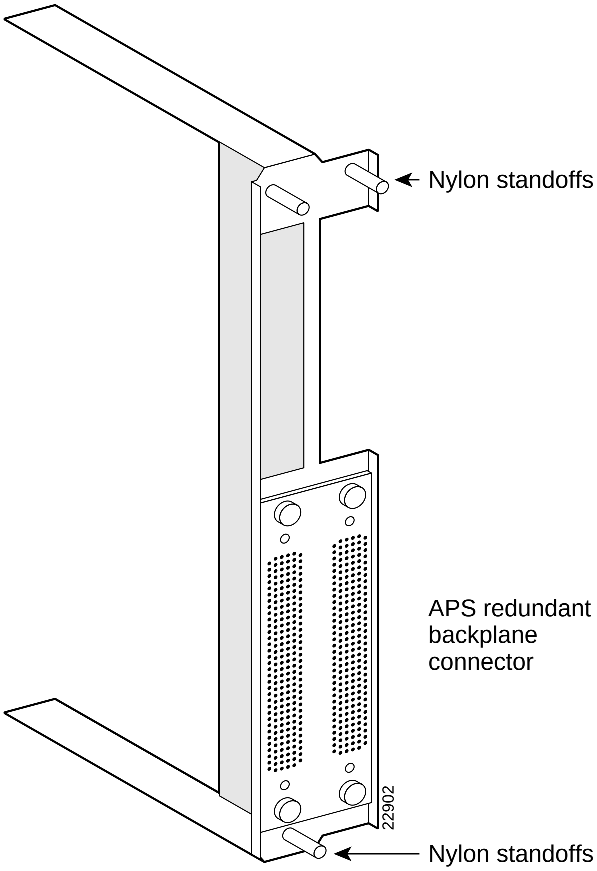


Figure 13-12 BPX Shelf, Rear View

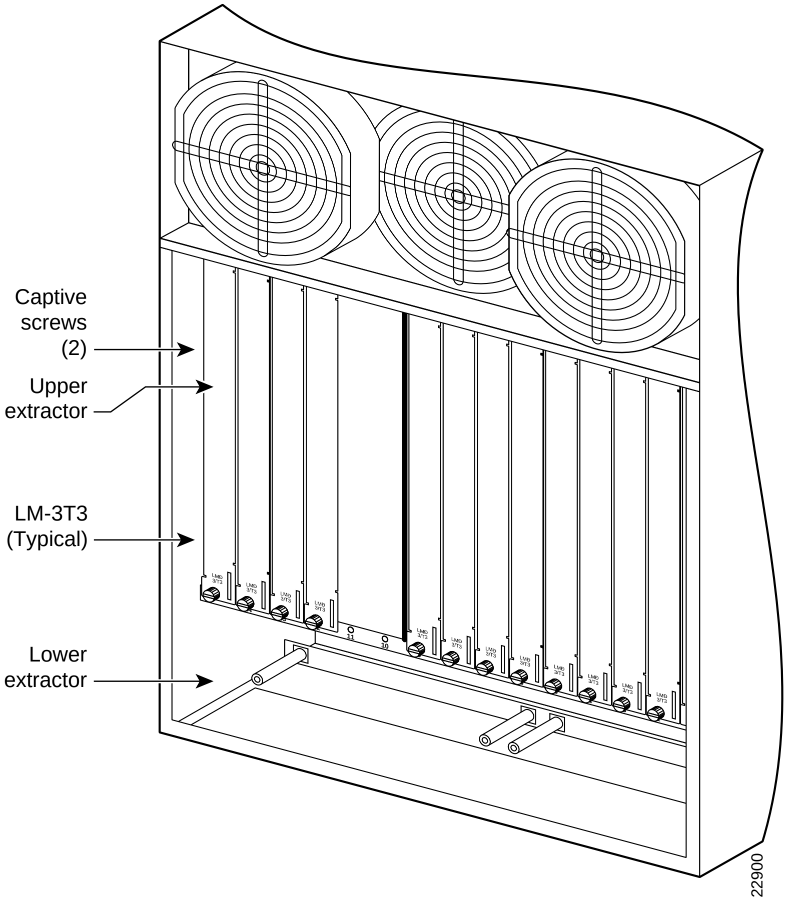
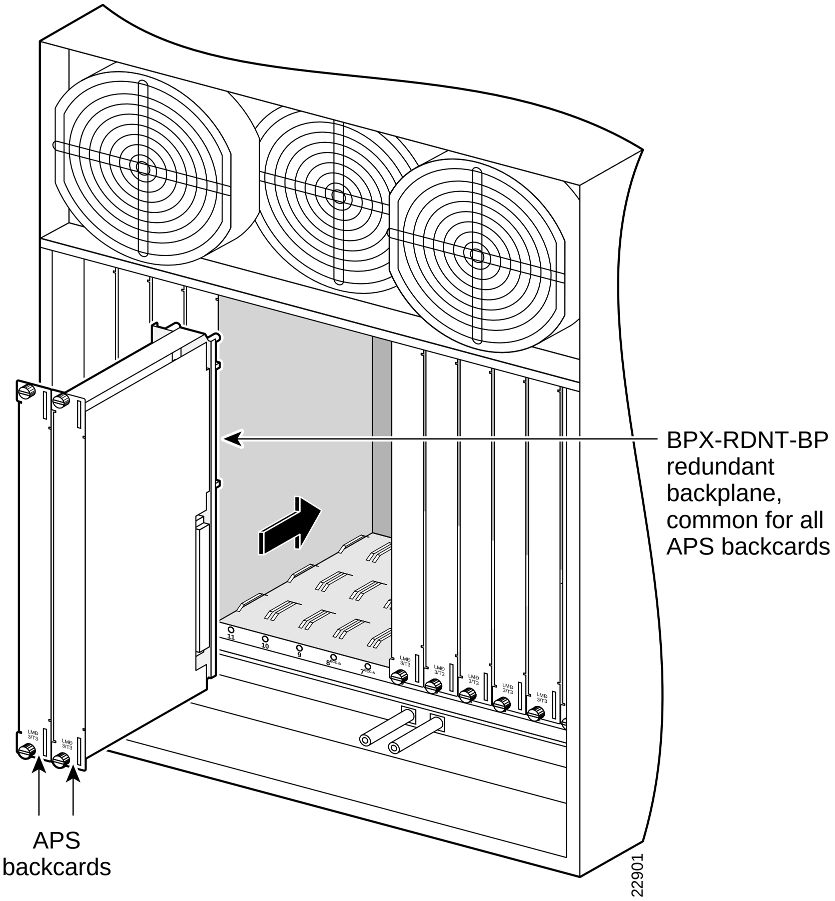


Figure 13-13 Installing APS Redundant Frame Assembly and Backcards into Place


BPX-RDNT-BP redundant backplane, common for all APS backcards
11
10
9
8
7
APS backcards
22901

CHAPTER 14

Connecting Cables

This chapter explains how to connect trunk and circuit line cables:

- Making T3 or E3 Connections
- Making a BXM OC-3 or OC-12 Connection
- Making a BXM T3/E3 Connection
- Setting up the BME OC-12 Port Loop
- Alarm Output Connections

Before proceeding to this chapter, you should first complete the procedures in:

- *Chapter 13, Installing the BPX Switch Cards*

and before that, the procedures in either:

- *Chapter 10, Installing the DC Shelf*
- *Chapter 11, Installing the AC Shelf*

  and

- *Chapter 12, Installing the T3/E3 Cable Management Tray*

and before that, the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or

- *Chapter 9, Installation in Customer Cabinet*

Making T3 or E3 Connections

Each LM-3T3 and LM-3E3 line module (BNI backcard) provides three ports with a BNC connector each for the XMT trunk output and for the RCV trunk input.

Each LM-2T3 and LM-2E3 line module provides two ports with a BNC connector each for the XMT line output and for the RCV line input.

To make the T3/E3 connections to each port:

Step 1 Bring each cable through the opening at the bottom of the cabinet at the back and route them up the side.

Step 2 The BPX switch has velcro tie-downs inside the cabinet to hold cabling in place. Pull the tie-downs apart as applicable, place the routed cable in position, wrap the ties around the cable and remake the loops by pressing the two sections together.

Step 3 Connect the cables to the BNC connectors on the LM-3T3 or LM-3E3 line modules.
Remember, the RCV is an input to the BPX switch and XMT is an output from the BPX switch. The ports are numbered from top to bottom as indicated in Figure 14-1.

Note Maximum distance from a BPX switch to a DSX3 cross connect point is approximately 450 feet (150 meters).

Step 4 Record which slot and port number you are using for each trunk or line. You'll need this information later when configuring the network.

Step 5 If optional Y-cable redundancy is desired, locate a 3-way BNC Y-cable adapter for each port to be so equipped. As an alternative to the Y-cable, use a BNC “T” and two short, equal-length BNC-BNC cables.

Step 6 For card redundancy, make sure there are two appropriate line modules equipped in adjacent slots.

Step 7 Connect two legs of the Y-cable to the XMT T3 or E3 connectors on the same port on each of the two line modules (see Figure 14-2). Do the same with the two RCV T3 or E3 connectors.

Step 8 Connect the third leg of the XMT and RCV Y-cable adapters to the XMT and RCV trunk cable.

Figure 14-1 Connecting T3 Cables to BPX LM-T3 (BNI T3 backcard)

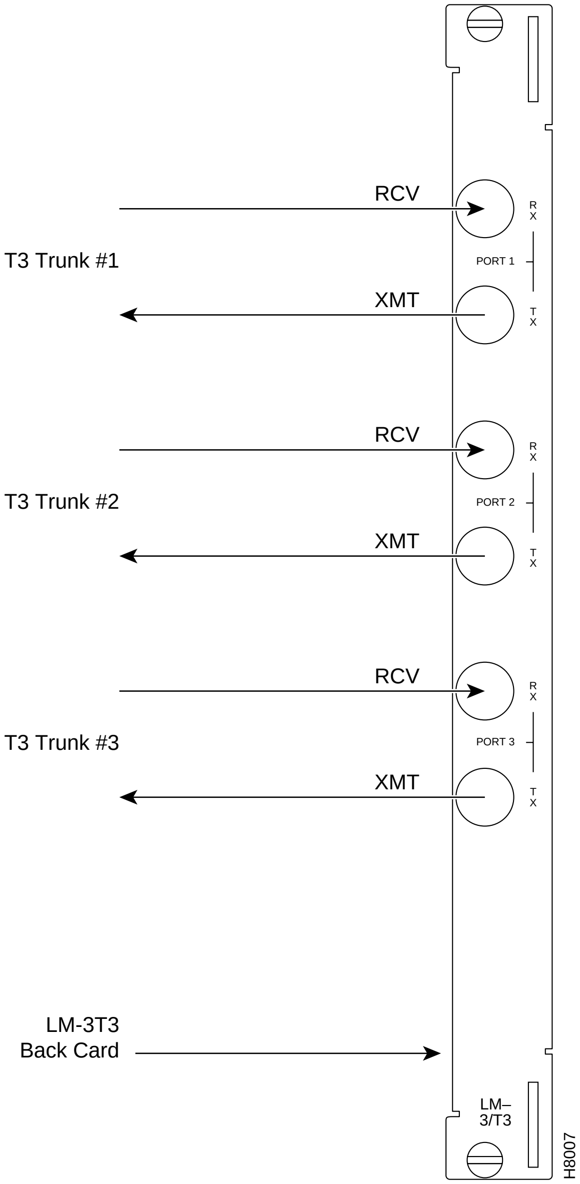
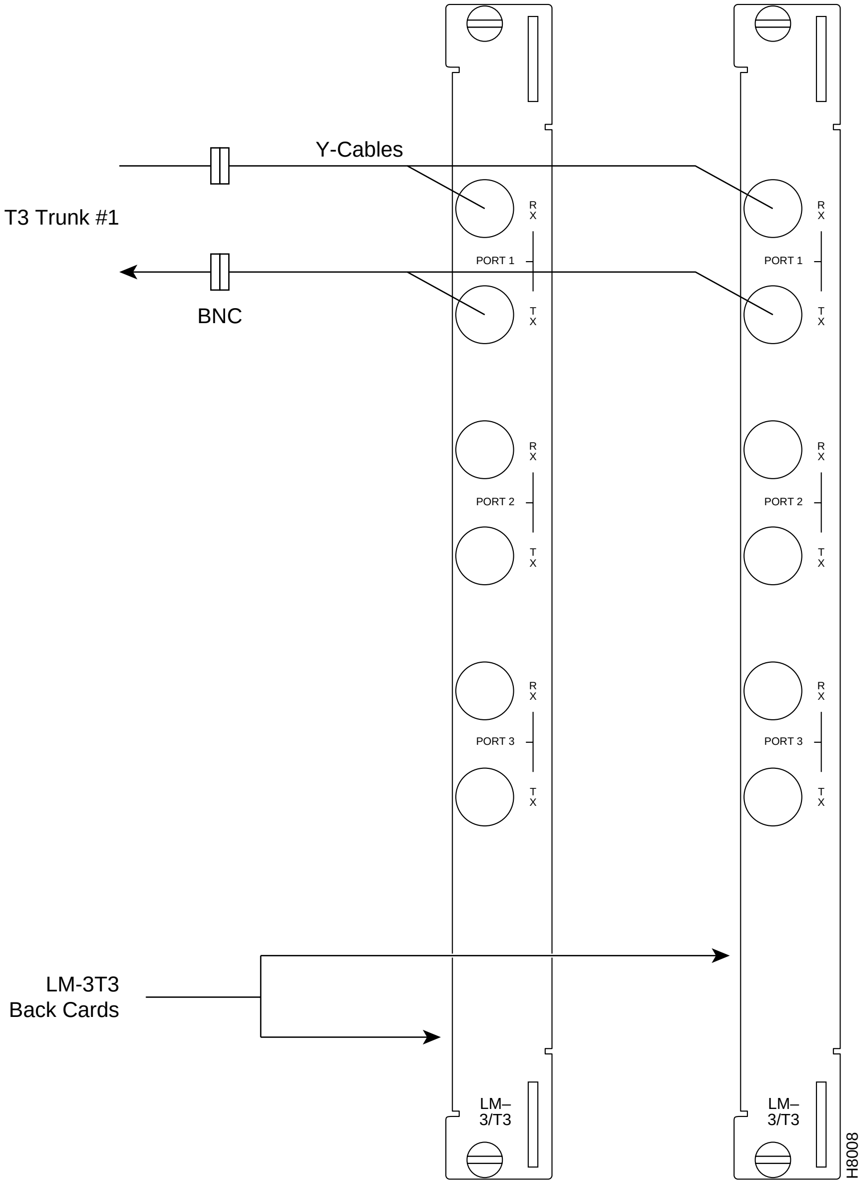


Figure 14-2 Connecting Y-Cable Adapters to a T3 Port



Making a BXM OC-3 or OC-12 Connection

Each OC-3 or OC-12 line module provides ports with both a transmit and receiver connector for each port. This procedure applies to OC-3 and OC-12 backcards, except that Y-Cabling redundancy is supported only for the SMF cards.

To make BXM OC-3 or OC-12 connections:

Step 1 At the back of the cabinet, route each cable up the inside of the cabinet, as applicable.

Step 2 The Cisco cabinet has tie-downs inside the cabinet to hold cabling in place. If using a Cisco cabinet, pull the tie downs apart as applicable, place the routed cable in position, wrap the ties around the cable and remake the loops by pressing the two sections together.

Step 3 Connect the cables to the applicable connectors on the line modules.
Remember, the RCV is an input to the BPX switch and XMT is an output from the BPX switch. The ports are numbered from top to bottom.

Step 4 Record which slot and port number you are using for each trunk or line. You'll need this information later when configuring the network.

Step 5 A Y-Cable redundancy connection for the SMF-2-BC backcard is shown in Figure 14-3.

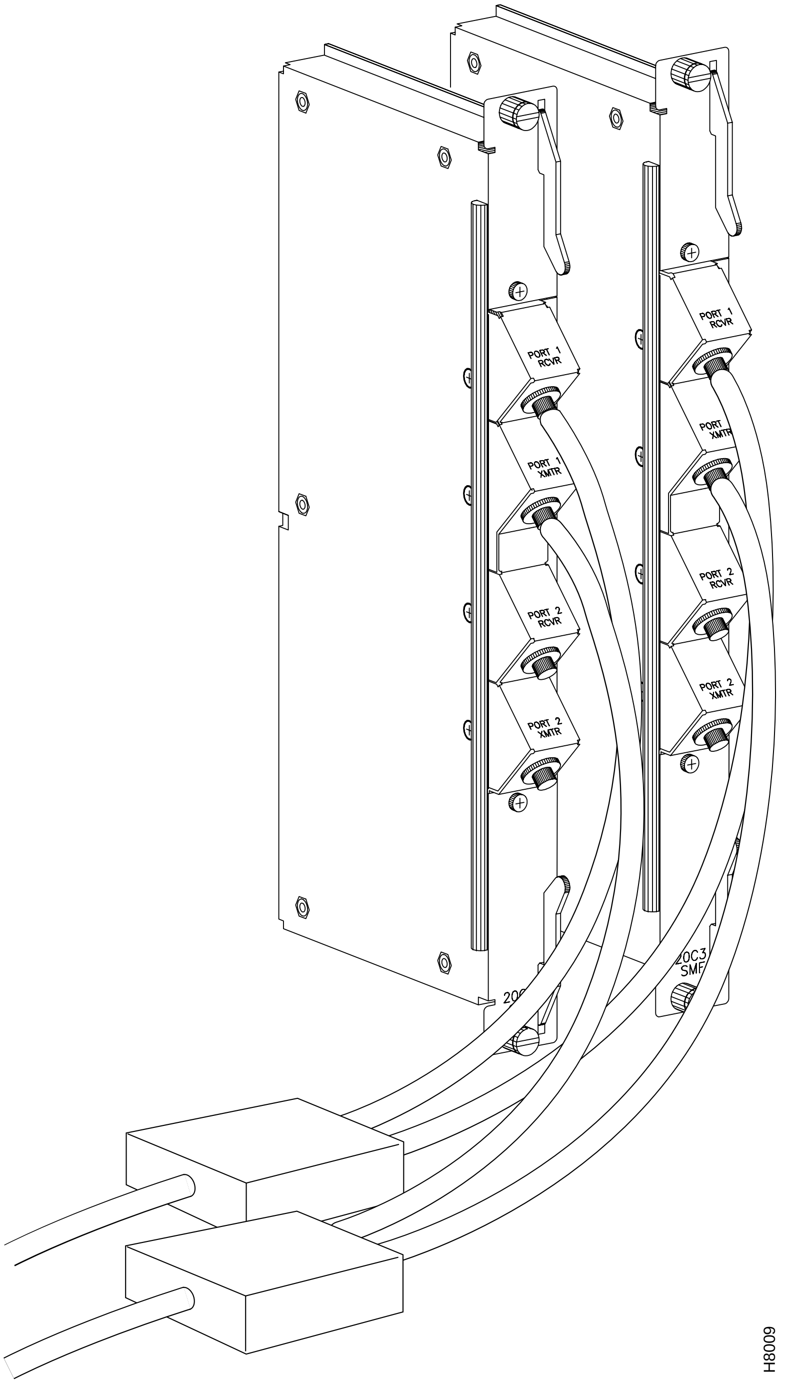
Step 6 For card redundancy, make sure there are two appropriate line modules equipped in adjacent slots.

Step 7 Connect two legs of the Y-cable to the XMT connectors on the same port on each of the two line modules (see Figure 14-3). Do the same with the two RCV connectors.

Note: Y-redundancy is supported on these cards:

- SMF-155-8-BC
- SMFLR-155-8-BC
- SMF-155-4-BC
- SMFLR-155-4-BC
- SMF-622-2-BC
- SMFLR-622-2-BC
- SMF-622-BC
- SMFLR-622-BC
- BPX-XLR-622-BC
- BPX-XLR-622-2-BC
- BPX-STM1-EL-4-BC

Figure 14-3 Connecting Y-Cables to an OC-3-SMF Backcard



Making a BXM T3/E3 Connection

Each T3/E3 line module provides ports with both a transmit and receiver connector for each port. The backcards can provide 4, 8, or 12 ports.

Figure 14-4 shows a typical T3/E3 cable connector that connects to the BXM T3/E3 cards.

Y-Cabling redundancy is supported on the BXM T3/E3 cards. An example of a Y-cable is shown in Figure 14-5.

To make a BXM T3/E3 connection:

Step 1 At the back of the cabinet, route each cable up the inside of the cabinet, as applicable. If Y-cables are used, the Y-cable connects to the corresponding connectors on adjacent cards.

Step 2 The Cisco cabinet has velcro tie-downs inside the cabinet to hold cabling in place. If using a Cisco cabinet, pull the tie downs apart as applicable, place the routed cable in position, wrap the ties around the cable and remake the loops by pressing the two sections together.

Step 3 Connect the cables to the applicable connectors on the T3/E3 line modules.
Remember, the RCV is an input to the BPX switch and XMT is an output from the BPX switch. The ports are numbered from top to bottom.

Step 4 For an open rack configuration in which Y-redundancy is not being used, an optional cable management tray is available. This is helpful for routing cables when a number of DS3/T3 cards are installed resulting a large number of cables to handle. Refer to *Chapter 12, Installing the T3/E3 Cable Management Tray*.

Figure 14-4 BXM T3/E3 Cable Connector Detail

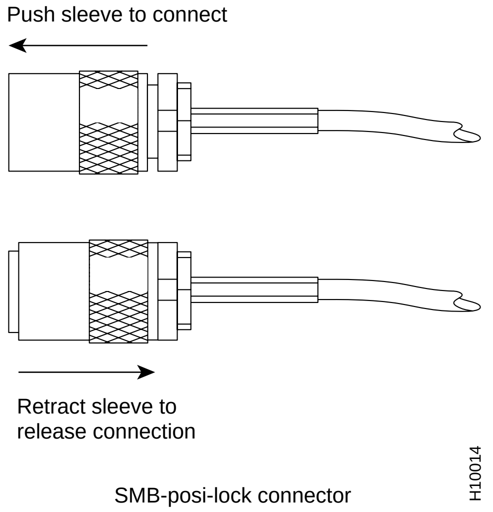
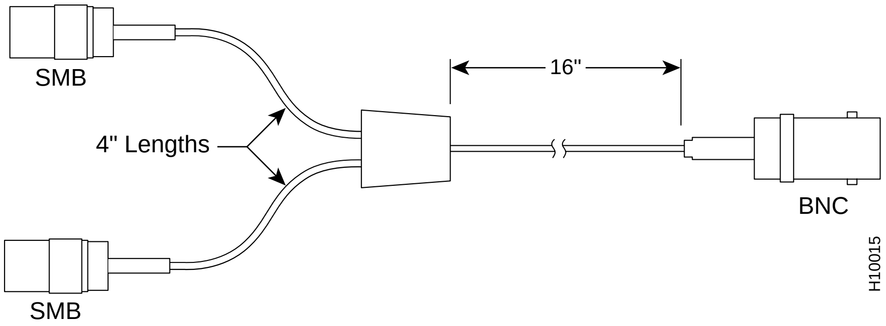


Figure 14-5 Y-Cable for BXM T3/E3 Cards



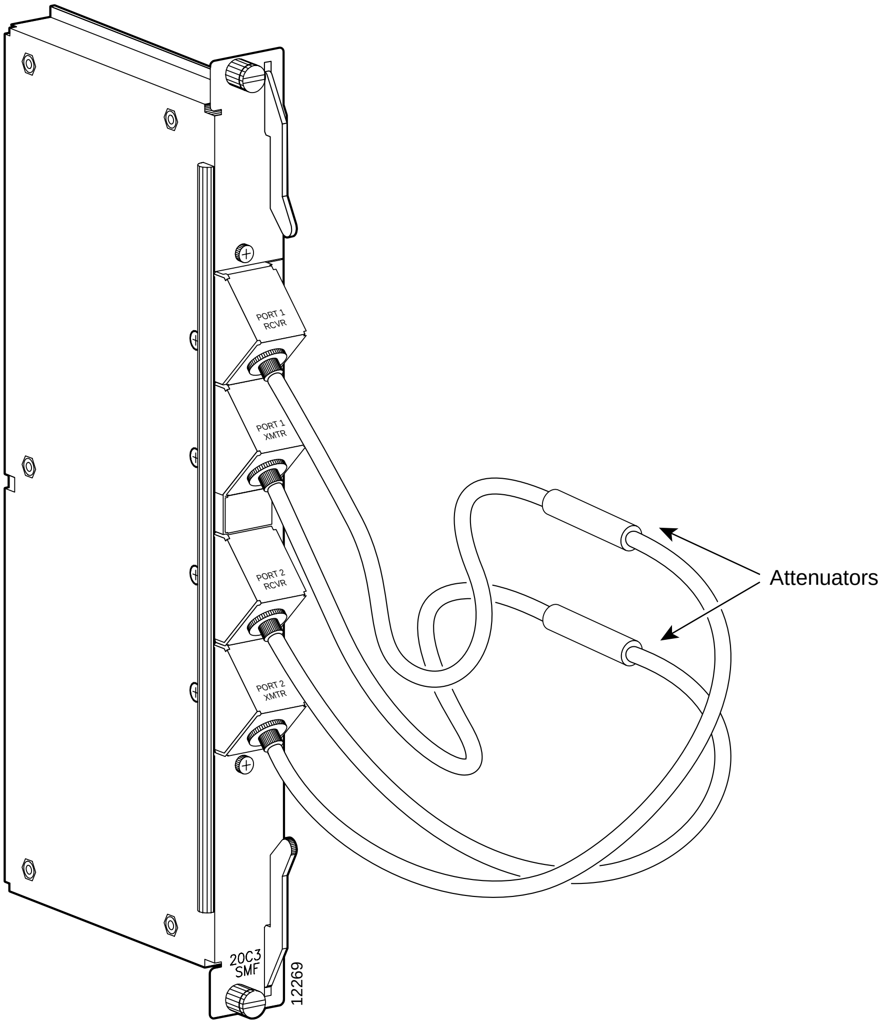
Setting up the BME OC-12 Port Loop

To set up the two ports on the OC-12 backcard for the BME multicast card, connect both:

- the transmit of port 1 to the receive of port 2
- the receive to port 1 to the transmit of port 2

Thus you have looped the two ports together. This is shown in Figure 14-6.

Figure 14-6 Looping Ports 1 and 2 for BME on OC-12 Backcard

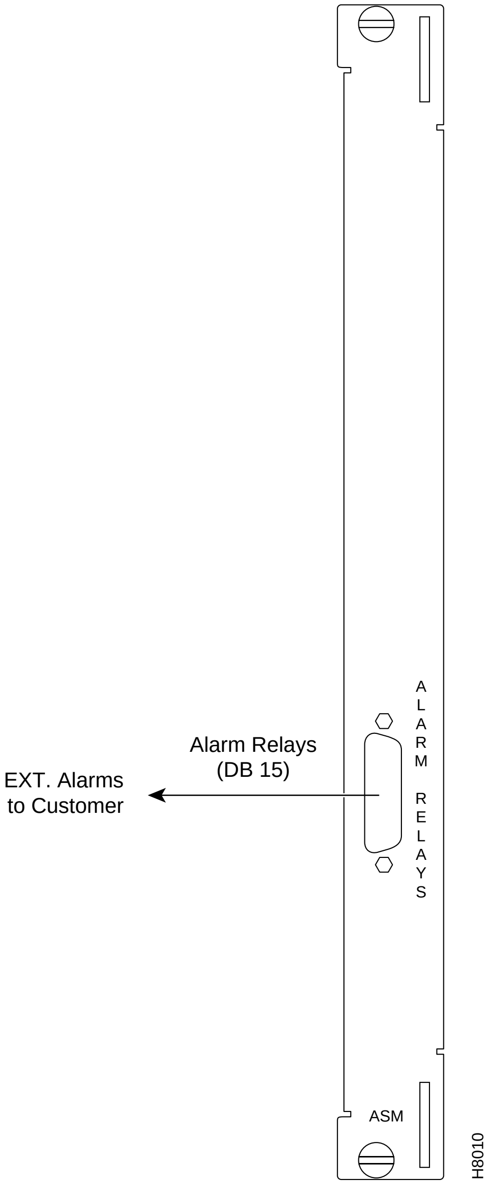


Alarm Output Connections

Dry contact relay closures are available for forwarding BPX switch alarms to a user office alarm system. Separate visual and audible alarm outputs are available for both major as well as minor alarm outputs.

These outputs are available from a DB15 connector on the LM-ASM faceplate (see Figure 14-7). Refer to *Chapter 31, BPX Switch Cabling Summary*, for a list of the pinouts for this connector. Use switchboard cable for running these connections.

Figure 14-7 Alarm Output Connector



CHAPTER 15

Connecting Temporary Terminal and Attaching Peripherals

This chapter explains how to set-up a temporary terminal or network management station for initial power-up, and how to attach other peripherals:

- Temporarily Connecting a Terminal or NMS to the Control Port
- Connecting a Network Printer to the BPX Switch
- Connecting Dial-In and Dial-Out Modems
- Making External Clock Connections

A network must have at least one connection to a control terminal or Cisco WAN Manager network management workstation. You use the Cisco WAN Manager network management workstation to configure and maintain all nodes in a network and report network statistical data.

A network printer may be connected to the AUXILIARY port if you wish to print.

If you want to have Cisco Customer Service perform remote troubleshooting, you must attach a dial-in modem to the network. See Connecting Dial-In and Dial-Out Modems, page 15-10.

Before proceeding to this chapter, you should first complete the procedures in:

- *Chapter 14, Connecting Cables*
- *Chapter 13, Installing the BPX Switch Cards*

and before that, the procedures in either:

- *Chapter 10, Installing the DC Shelf*
- *Chapter 11, Installing the AC Shelf*

  and

- *Chapter 12, Installing the T3/E3 Cable Management Tray*

and before that, the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or

- *Chapter 9, Installation in Customer Cabinet*

Before attempting to attach equipment to the BPX switch, read the manufacturer’s literature to ensure that you have made the equipment ready for attachment.

For additional information, refer to these sources:

- For the pin assignments for the BPX switch control terminal port, see *Chapter 31, BPX Switch Cabling Summary*.
- For instructions on using the switch commands, refer to the *Cisco WAN Switching Command Reference*.
- For instructions on using the Cisco WAN Manager workstation, refer to the *Cisco WAN Manager Operations Manual*.

Temporarily Connecting a Terminal or NMS to the Control Port

You will need to connect a basic VT-100 type terminal (or PC or workstation, including a Cisco WAN Manager workstation) to the BPX's CONTROL port for use in entering commands to bring up a new node. This temporary or local control is especially useful during installation, initial power-up, and configuration.

To support the Cisco WAN Manager workstation, the BPX switch's LM-BCC back card offers these ports for attaching peripherals:

- An RS-232 serial data port labeled CONTROL port
- An RS-232 serial data port labeled AUXILIARY port
- An Ethernet port labeled LAN

A Cisco WAN Manager workstation is recommended for managing a network containing the IGX and BPX switches. Refer to the *Cisco WAN Manager Operation Manual* and *Cisco WAN Manager Installation Manual* for setup instructions and specifications for the Cisco WAN Manager network management system, which is required to provide network alarm, control, and statistics monitoring.

Note For network management, a Cisco WAN Manager workstation must be connected to the LAN port of one or more network nodes, typically BPX switches because of their processing power, to provide network management.
It is not connected to the Control Port during normal operation.

Refer to Table 15-1 for configuration data for the BPX CONTROL port.

Table 15-1 Control Port Parameters for Local Control (pc or workstation)

Parameter	Setting
BPX switch Port Used:	Serial CONTROL port, located on a BCC back card, is used to interface to a local terminal.
Code:	Standard 7 or 8-bit ASCII; 1 or 2 stop-bits; even, odd or no parity.
Interface:	RS-232 DCE.
Data Rate:	All standard asynchronous data rates from 300 to 19200 bps, independently software-selectable.
Supported Terminals:	Any terminal compatible with DEC VT-100.
Cable Required:	Straight-through RS-232 cable.

The BPX Control and Auxiliary ports are pinned as RS-232/V.24 DCE ports. When connecting a terminal, PC, or other device pinned as RS-232/V.24 DTE to the Control or Auxiliary port, you may use a straight-through cable. However, to connect a modem to the Control or Auxiliary ports, you must use a null-modem cable.

In these procedures:

- The term BCC refers to the BCC-4V, BCC-3-32M, BCC-3-64M, or BCC-32
- The BCC-4V, BCC-3-32M, and BCC-3-64M require BCC-3-BC backcards
- The BCC-32 requires the BCC15-BC backcard

To attach a terminal to the BPX switch:

Step 1 From the back of the cabinet, run the control terminal RS-232/V.24 cable through the opening at the bottom and up to the LM-BCC card in back slot 7.

Step 2 **For nodes with a single BCC:** Locate the CONTROL port connector on the LM-BCC in slot 7. Attach the RS-232/V.24 cable as shown in Figure 15-1, then proceed to Step 5.

Step 3 **For nodes with redundant BCCs:** A single cable is sufficient for temporarily connecting to the CONTROL port of the active BCC during initial node configuration. However, if you want to monitor the switchover function of the BCCs via the CONTROL port without swapping the cable from the CONTROL port of one BCC to the CONTROL port of the other, you can use a Y-cable.
Connect one leg of the Y-cable to the CONTROL port connector on the backcard in slot 7 and the other leg to the slot 8 CONTROL port connector.

Step 4 Attach a RS-232/V.24 cable to the remaining leg of the Y-cable as shown in Figure 15-2.

Step 5 Fasten the cable connector to the CONTROL port connector with the captive screws on the connector hood.

Step 6 Plug the control terminal (or Cisco WAN Manager) power cord into the appropriate wall receptacle (115 VAC or 240 VAC) and switch it on.

Step 7 If connecting to a Cisco WAN Manager workstation, set the port function for VT100/StrataView by using the **cnftermfunc** command. If using a “dumb” terminal, select VT100 only (# 5).

Step 8 Make sure that the CONTROL port and the terminal or workstation are set to the same baud rate and check the other communication parameters by using the **cnfterm** command.

Step 9 When you have completed the initial node configuration, remove the connections to the CONTROL Ports. Network Management connections are described in the next section.

Note When a node is powered up, it enters “boot mode” which has a default speed of 9600 bps. If the node’s control port has been previously configured to 19,200, the first messages will appear garbled because the terminal is at 19,200 bps, but the control port (in “boot mode”) is temporarily at 9,600 bps. When the “transition to online” occurs, then the speeds will match and the terminal display will be readable.

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:
```

Figure 15-1 Temporary Connections to Bring up a New Node, LM-BCC Backcard Shown

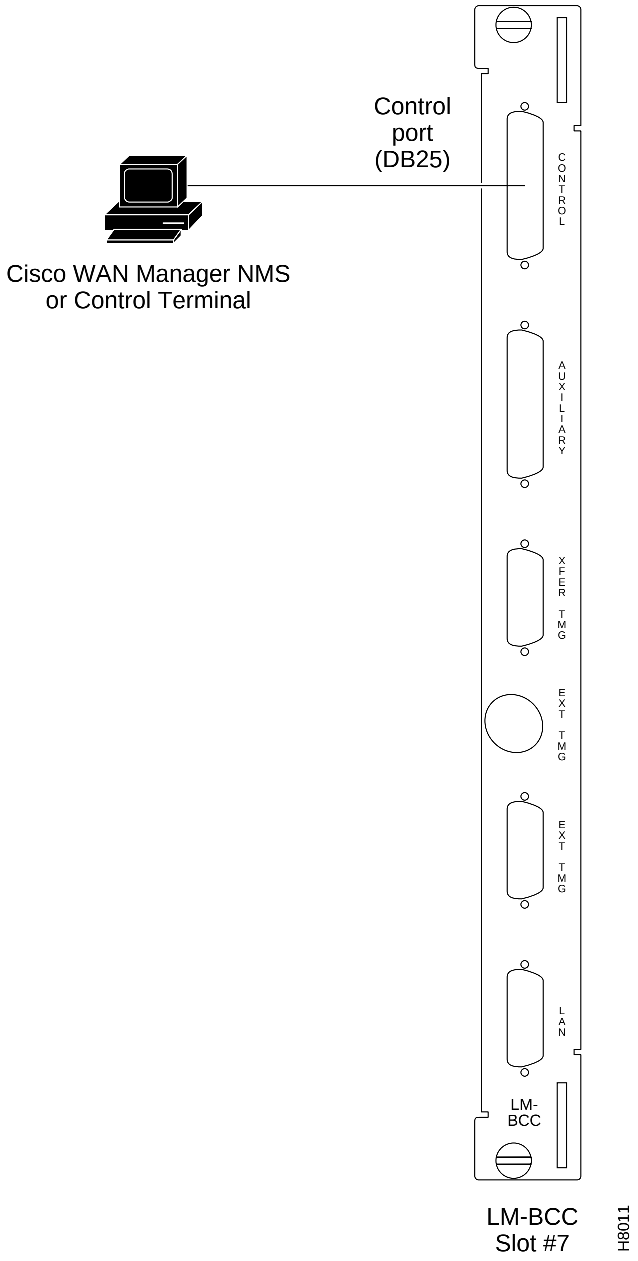
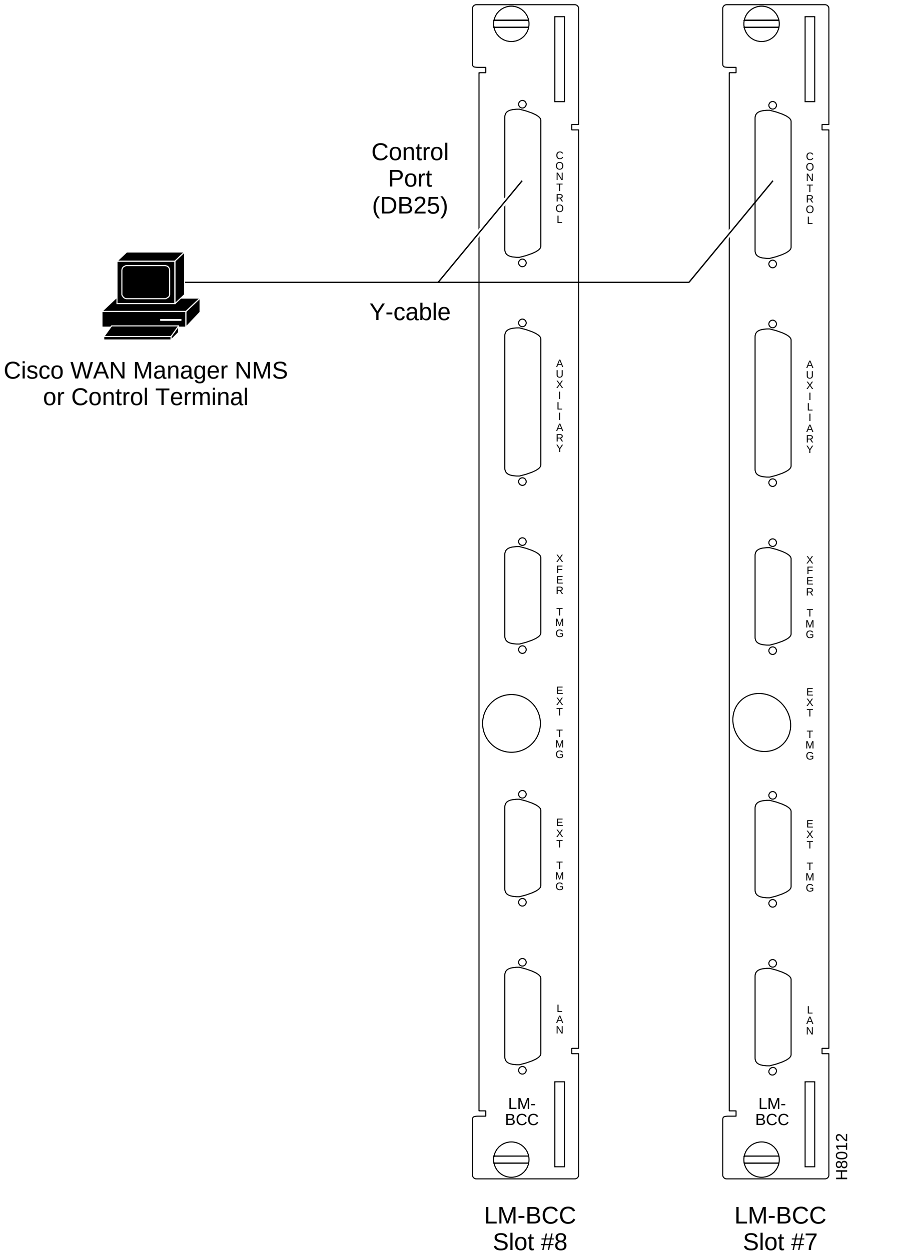


Figure 15-2 Temporary Connections to Bring up a New Node, LM-BCCs Shown



Connecting a Network Printer to the BPX Switch

In most systems, the network printer will be connected to a serial port on the Cisco WAN Manager NMS terminal server. The maintenance log and all statistics data will reside on the Cisco WAN Manager.

However, it is possible to connect a printer to a node and use various BPX switch software print commands to print locally. This may be helpful during the initial network installation phase.

Auxiliary Port Parameters for Okidata 184 Local Printer

The optional local maintenance printer for the BPX switch is the Okidata Model 184 dot matrix printer. You may connect this printer to any node.

Refer to Table 15-2 and Table 15-3 for printer configuration requirements. Note that the Okidata Model 184 is not the same printer that may be provided with the Cisco StrataView Plus NMS terminal but in addition to it.

Table 15-2 Auxiliary Port Parameters for Okidata 184 Printer

Parameter	Setting
BPX switch Port Used:	Serial AUXILIARY port, located on the LM-BCC card, is used for the maintenance printer
Code:	Standard 8-bit ASCII; 8 data bits, 1 stop-bit, odd parity
Interface:	RS-232 DCE
Data Rate:	9600 baud
Supported Printer:	Okidata 184
Cable Required:	Straight-through RS-232 cable

DIP Switch Settings for Okidata 184

DIP Switch A is an 8-section DIP switch located on the printer’s main circuit board.

To access the configuration switches, slide back the switch cover at the top, rear of the printer case. Set Switch A as indicated in Table 15-3.

Table 15-3 Switch A Settings—Okidata 184 Printer

Switch A	Setting	Description
1	Off	ASCII with non-slashed zero
2	Off	ASCII with non-slashed zero
3	Off	ASCII with non-slashed zero
4	Off	11-inch paper length
5	On	11-inch paper length
6	Off	No Auto Line Feed.
7	On	8-bit data.
8	Off	Enables front panel.

The High Speed Serial Interface DIP Switch consists of two DIP switches, SW1 and SW2, located on a serial-board attached to the printer's main board.

Set switches 1 and 2 as indicated in Table 15-4 and Table 15-5.

Table 15-4 Switch 1 Settings—Okidata 184 Printer

Switch 1	Setting	Description
1	On	Odd parity
2	On	No parity
3	On	8 data bits
4	On	Ready/busy protocol
5	On	Test select circuit
6	On	Print mode
7	On	Busy line selection
8	On	DTR pin 2 enabled

Table 15-5 Switch 2 Settings—Okidata 184 Printer

Switch 2	Setting	Description
1	Off	Transmission
2	On	Speed = 9600 baud
3	On	Speed = 9600 baud
4	On	DSR active
5	On	Buffer = 32 bytes
6	On	Timing = 200 ms
7	On	Space after power on
8	Don't care	Not used

For the pin assignments for the AUXILIARY port on the BPX switch and the recommended RS-232/V.24 cable pinout and printer DIP switch settings, see *Chapter 31, BPX Switch Cabling Summary*.

Procedure to Attach a Local Printer

To attach the printer to the BPX switch:

Step 1 Check the printer RS-232/V.24 cabling pinout, and if required adjust the DIP switches to the settings indicated for the type of printer to be connected to the BPX switch.

Step 2 **For nodes with single BCC:** Connect the RS-232/V.24 printer cable to the AUXILIARY port on the LM-BCC back card (see Figure 15-3). Go to Step 4.

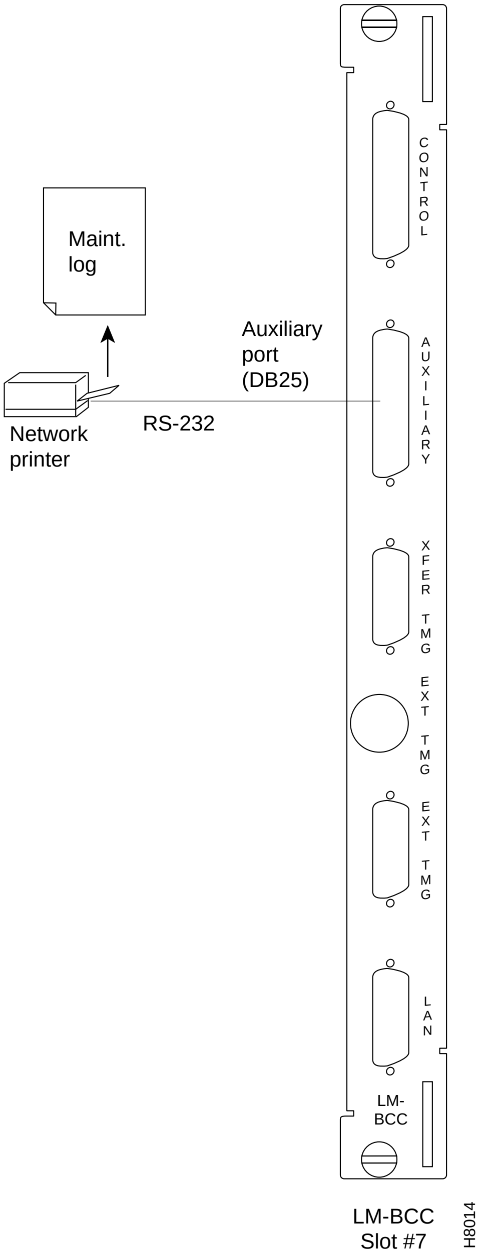
Step 3 **For nodes with redundant BCCs:** A Y-cable is required for this application. Connect one leg of the Y-cable to the AUXILIARY port connector on the LM-BCC in slot 7. Connect the other leg to the AUXILIARY port connector on the LM-BCC in slot 8.

Step 4 Plug the printer power cord into the appropriate AC outlet (115 VAC or 240 VAC).

Step 5 Set the port function for printer by using the **cnftermfunc** command.

Step 6 Make sure the control port and the printer are set to the same baud rate and check the other communication parameters by using the **cnfterm** command.

Figure 15-3 Connections to a Network Printer, LM-BCC Shown



Connecting Dial-In and Dial-Out Modems

Cisco Customer Service uses modems to remotely diagnose and correct customer problems with installed BPX switches. You will need to connect a modem to each BPX switch to provide remote access.

The modem currently recommended for use with the BPX switch is the Codex Model V.34R. You must use an auto-answer modem

A dial-in connection to a BPX switch RS-232 from customer service via a modem uses the CONTROL port of the BPX switch. This port is bi-directional transmit and receive.

A dial-out connection from a BPX switch via a modem to Cisco Customer Service uses the AUXILIARY port of the BPX switch.

These modems connect to a standard telephone line wall jack. The modem connections require special cables and setup procedures.

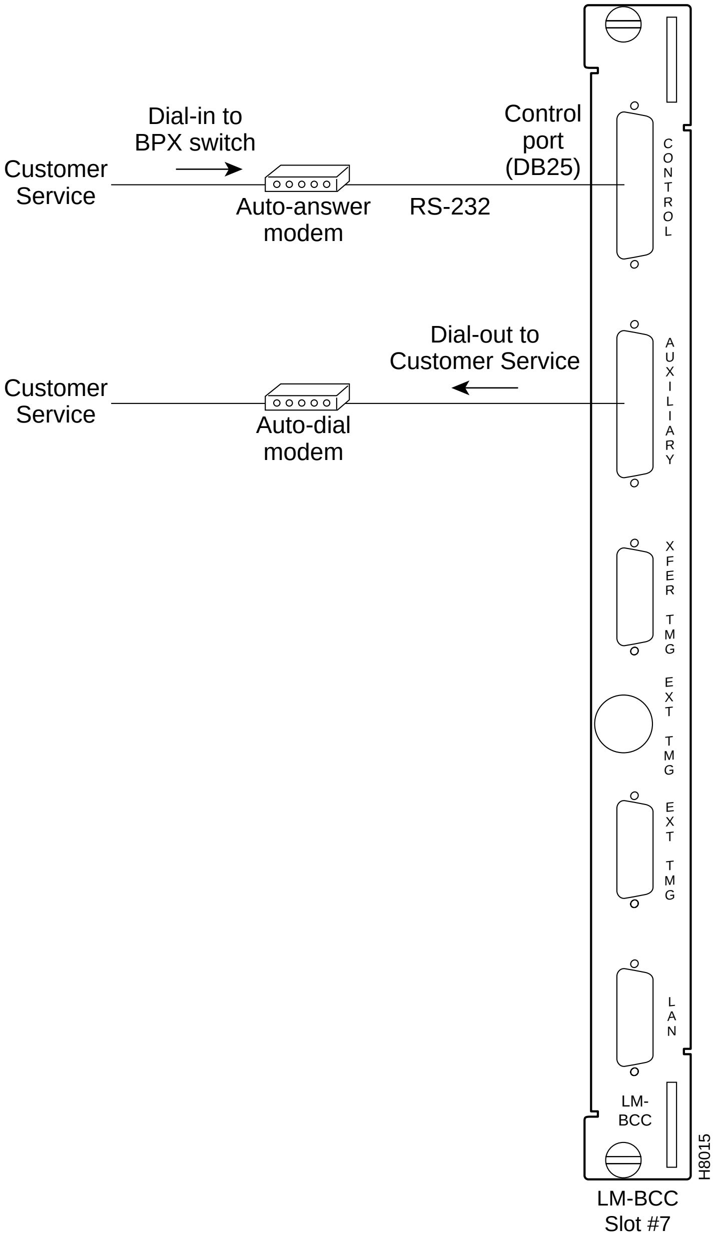
If the BPX switch is equipped with redundant BCCs, you must use an RS-232 Y-cable for these connections.

See Table 15-6 for modem interface requirements.

Table 15-6 Modem Interface Requirements

Parameter	Requirement
BPX switch Port Used:	CONTROL port on BCC back card is used for auto-answer modem setup. AUXILIARY port on a BCC back card is used for auto-dial modem setup.
Code:	Standard 8-bit ASCII, 1 stop-bit, no parity
Interface:	RS-232 DCE
Cable to modem:	Null modem cable: CONTROL or AUXILIARY port to modem (DCE to DCE)
Phone Lines:	Dedicated, dial-up business telephone line for Customer Service-to-BPX switch modem
Data Rate:	All standard asynchronous data rates from 300 to 19200 bps, independently software-selectable
Supported Modems:	Motorola V.34R 28.8 baud modem with or without talk/data button

Figure 15-4 Connecting Modems to the BPX Switch, LM-BCC Shown



Motorola V.34R BPX Switch Dial-In Configuration

BPX Switch Auto-Answer (Dial-In to BPX switch)

This setup procedure allows Cisco Customer Service to dial in to your BPX switch to provide support and troubleshooting:

Step 1 Using the **cnfterm** command, set the BPX CONTROL port speed to 9600 bps.

Step 2 Using the **cnftermfunc** command, set the terminal type to VT100/StrataView.

Step 3 To program the modem, temporarily attach a terminal to the modem using a straight through RS-232 cable (DTE to DCE). The modem EIA port will automatically match the 9600 bps setting of the terminal.

Step 4 Enter the commands listed in Table 15-7 to set up the modem for proper operation.

Note Consult the manual supplied with your modem for specifics concerning the modem configuration. Call Cisco Customer Service for latest modem configuration information.

Step 5 Disconnect the terminal and the straight-through cable from the BPX CONTROL port.

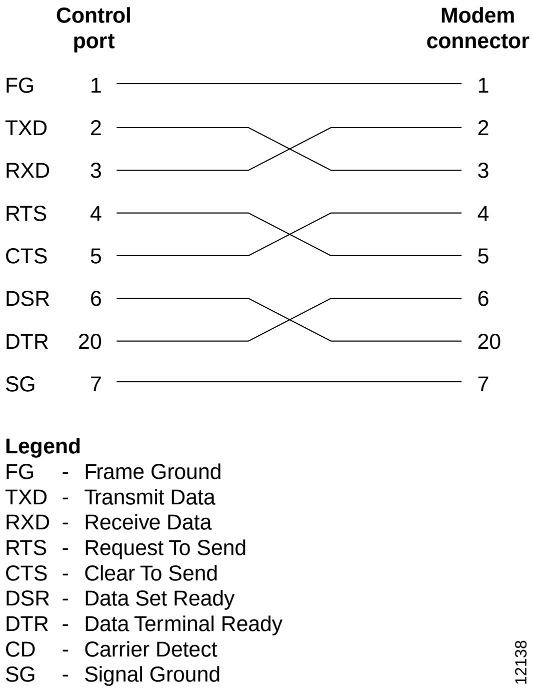
Step 6 Connect the modem to the BPX CONTROL port by using null-modem cables Figure 15-5. A null modem cable is used because the connection is essentially a DCE to DCE rather than a DTE to DCE connection.

Step 7 Ask Cisco Customer Service to assist in testing the operation of the modem setup.

Table 15-7 V.34R Modem Configuration for Auto-Answer (Dial-in to BPX)

Step	Command	Function
1.	AT & F	Reset to factory default
2	ATL1	Set modem loudness, modem speaker at low volume
3.	ATSØ=1	Enables Auto-Answer Mode on modem (answer on first ring)
4	AT\N3	Enables automatic MNP error correction
5	AT%C	Disables data compression
6.	AT\QØ	Disables XON/XOFF flow control
7.	AT&S1	Sets DSR to normal
8.	ATEØ	Disables local character echo. Modem will not echo what you type.
9.	ATQ1	Disables result codes. (Modem will appear “dead”, will stop responding “OK” to commands.)
10.	AT&W	Saves current configuration settings in non-volatile memory. (Writes and stores to configuration location 1.)

Figure 15-5 Dial-Modem Cabling for Auto Answer (Dial-In to BPX)



Auto-Dial to Customer Service

This setup procedure enables your BPX to dial up Cisco Customer Service.

Step 1 Using the **cnfterm** command, set the BPX AUXILIARY port speed to 9600 bps. Enable XON/XOFF flow control.

Step 2 Using the **cnftermfunc** command, select option 7, "Autodial Modem" Enter the customer service-designated Network ID and the customer service modem phone number.

Step 3 Attach a 9600 bps terminal to the modem by using a straight-through cable. The modem EIA port will automatically match the 9600 bps setting of the terminal.

Step 4 Enter the commands listed in either Table 15-8 (V.34R modem without talk/data pushbutton) or Table 15-9 (V.34R modem with talk/data pushbutton), to set up the modem for proper operation.

Note Consult the manual supplied with your modem for specifics concerning the modem configuration. Call customer service for latest modem configuration information.

Step 5 Disconnect the terminal and the straight-through cable from the CONTROL port.

Step 6 Connect the modem to the AUX port by using a null modem cable Figure 15-6.

Step 7 Ask Cisco Customer Service to assist in testing the operation of the modem setup.

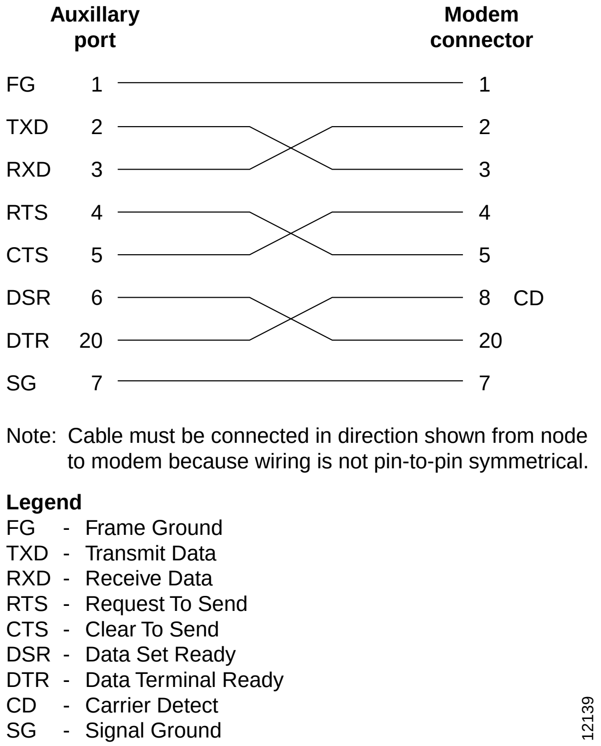
*Table 15-8 V.34R Auto-Dial Configuration (dial-out to customer service)**

Step	Command	Function
These configuration commands are for a V.34R modem that does not have a talk/data pushbutton.		
1.	AT&F	Initializes factory defaults.
2.	ATL1	Modem speaker at minimum volume.
3.	AT*SM3	Enables automatic MNP error correction.
4	AT*DC0	Disables data compression.
5.	AT*SC1	Enables DTE speed conversion.
6.	AT*FL1	Enables XON/XOFF flow control.
7.	AT*SI1	Enables 5-minute inactivity disconnect.
8.	AT&C1	DCD controlled by modem.
9.	AT&D2	Modem disconnects when toggles DTR.
10.	AT&V	Verify entries.
11.	AT&W	Saves current settings to non-volatile memory.

Table 15-9 V.34R with talk/data, Auto-Dial Configuration (dial-out to customer service)

Step	Command	Function
These configuration commands are for a V.34R modem that has a talk/data pushbutton.		
1.	AT&F	Initializes factory defaults.
2.	ATL1	Modem speaker at minimum volume.
3	AT\N3	To enable MNP error correction.
4	AT%C	To disable data compression.
5	AT\J	Enables DTE speed conversion.
6	AT\Q1	Enables flow control.
7	AT\T3	Enables 3-minute inactivity timer.
8.	AT&C1	DCD controlled by modem.
9.	AT&D2	Modem disconnects when toggles DTR.
10.	AT&V	Verify entries. *(shows current configuration)*.
11.	AT&W	Saves current settings to non-volatile memory.

Figure 15-6 Dial Modem Cabling for Auto Dial (dial-out to customer service)



Note: Cable must be connected in direction shown from node to modem because wiring is not pin-to-pin symmetrical.

Legend

FG	-	Frame Ground
TXD	-	Transmit Data
RXD	-	Receive Data
RTS	-	Request To Send
CTS	-	Clear To Send
DSR	-	Data Set Ready
DTR	-	Data Terminal Ready
CD	-	Carrier Detect
SG	-	Signal Ground

Making External Clock Connections

If you want to synchronize the BPX switch to some other external equipment or a local digital central office, you can use one of two connectors on an BCC15-BC or BPX-BCC-3-BC backcard to accept a clock input.

You can use a DB15 connector labeled EXT TMG to connect a balanced T1 or E1 signal, synchronized from some higher-level source to the BPX switch. If an unbalanced 75-ohm E1 signal is available as the timing source, a BNC EXT TMG connector is also provided.

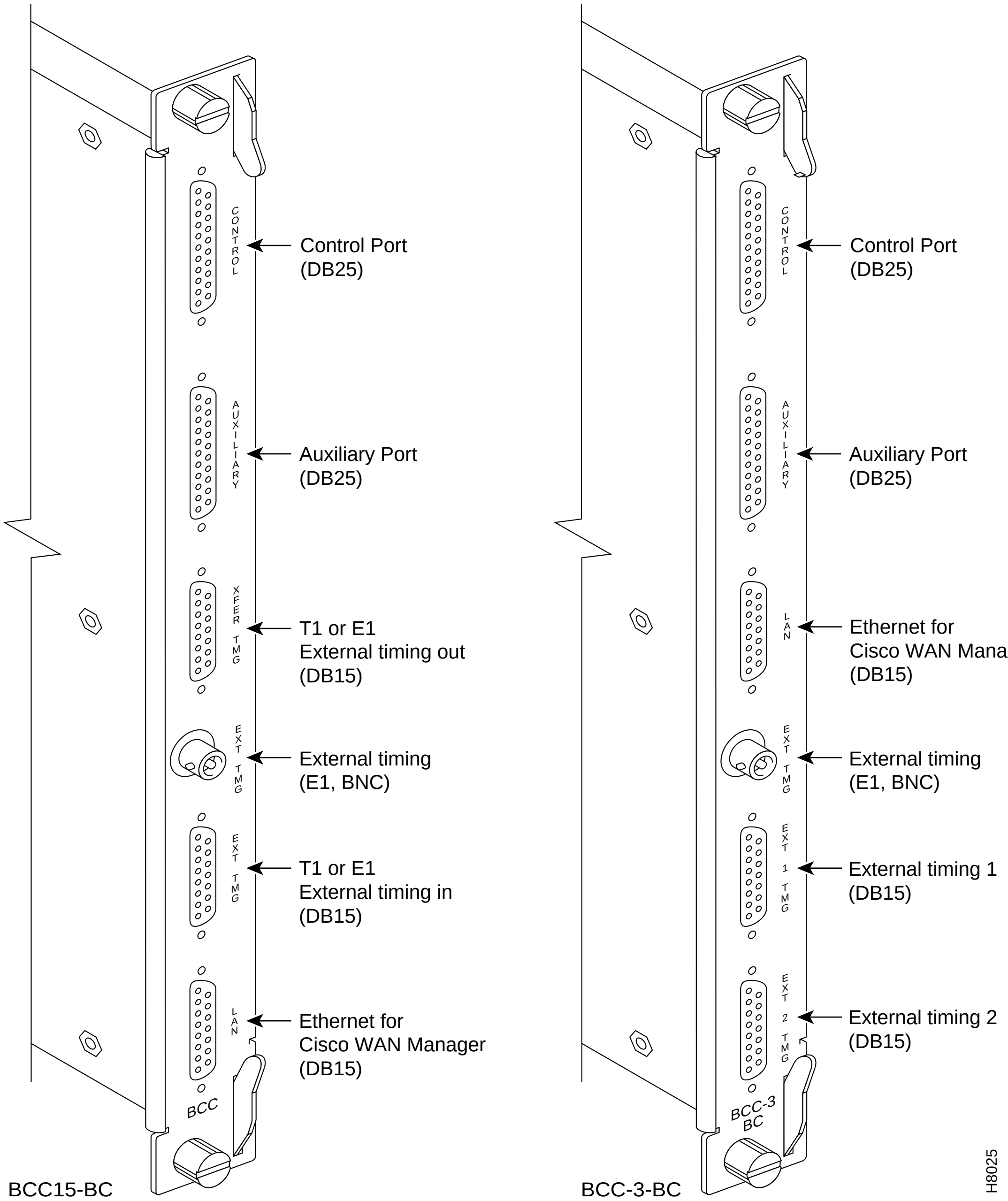
For a BCC-3-BC backcard (backcard for BCC-3-32M, BCC-3-64M, or BCC-4V), you can use a DB15 connector labeled EXT 1 TMG to connect a balanced T1 or E1 signal, synchronized from some higher-level source to the BPX switch.

The EXT 2 TMG connector provides a redundant connector to EXT 1 TMG. A T1 source with 100 ohm impedance or an E1 source with 100/120 ohm impedance typically uses this connector. If an unbalanced 75-ohm E1 signal is available as the timing source, a BNC EXT TMG connector is also provided.

The BPX switch can use these inputs rather than its internal Stratum 3 clock source.

Note Contact Cisco Customer Service for information on setting up either a 75-ohm or 120-ohm clock interface on the BCC backcard.

Figure 15-7 External Clock Source Connections to Backcards for BCCs



.

CHAPTER 16

Checking and Powering-Up

This chapter explains how to check that you are ready and then perform the initial power up.

Before proceeding to this chapter, you should first complete the procedures in:

- Chapter 15, Connecting Temporary Terminal and Attaching Peripherals
- *Chapter 14, Connecting Cables*
- *Chapter 13, Installing the BPX Switch Cards*

and before that, the procedures in either:

- *Chapter 10, Installing the DC Shelf*
- *Chapter 11, Installing the AC Shelf*

  and
- *Chapter 12, Installing the T3/E3 Cable Management Tray*

and before that, the procedures in either:

- *Chapter 8, Installation with Cisco Cabinets including 7000 Series Routers*

  or
- *Chapter 9, Installation in Customer Cabinet*

Before operating the BPX switch, verify that the following procedures have been performed:

Step 1 The BPX switch is connected to an appropriate power source with an isolated ground connection, according to the procedures in *Chapter 10, Installing the DC Shelf* or *Chapter 11, Installing the AC Shelf*, as applicable.

Step 2 The BPX switch power cord is plugged into an appropriate power outlet.

Step 3 The full complement of cards for the specific node are mounted in the correct slots, correctly seated, and locked in place.

Step 4 The T3 or E3 connections are attached appropriately.

Step 5 A control terminal (or Cisco WAN Manager Work Station) is connected to the CONTROL port on the LM-BCC in back slot 7/8, and the terminal's power cord plugged into the appropriate voltage wall outlet.

Step 6 If desired, a printer is connected to the AUXILIARY port on the LM-BCC in back slot 7/8 and the printer power cord is plugged into the appropriate power outlet.

Step 7 If desired, modems are connected to the CONTROL port or AUXILIARY port, as applicable, on the LM-BCC in back slot 7/8, and the modem power cords plugged into the appropriate power wall outlet.

Having completed the preceding checklist, proceed to power up the BPX switch:

Step 1 From the back of the BPX switch, turn the power switches to the ON position.

Step 2 From the front of the BPX switch, observe the cards go through initial diagnostic self-tests.

- The AC power supply's –48V indicator is on.
- The standby BCCs red "FAIL" light flashes until self-testing and configuration updates are completed. The other BCC becomes active immediately, but also performs self-testing and configuration updating. The entire process may take several minutes to complete.
- The remaining cards show "FAIL" for a few seconds, then become active or standby.
- The ASM DC LEDs are both green, indicating that the DC voltages on the two DC power busses are within tolerance.
- There may be alarms showing on the ASM, BXMs, BMEs, and BNIs.
  Alarms may be present on ATM trunk connectors that have not been physically connected to their associated lines.

Note New nodes will not have any configured trunks, lines or ports therefore all cards should be in Standby mode except for one BCC which should be Active.

BPX Switch Startup Diagnostic

The BPX switch software provides a group of diagnostic tests to be run on the system's hardware at power-up. The startup diagnostic either passes or fails the BCC(s) tests. The test result is displayed on the screen of a control terminal connected to the CONTROL port on the backcard in slot 7 of the BPX. A successful power up results in a pass message.

Note On power-up, the BCC in slot 7 is always the active BCC.

If a BCC fails the power-up diagnostic, it will not boot. If that happens, perform this procedure:

Step 1 Remove the failed BCC from its slot.

Step 2 Reseat the BCC in the same slot.

Step 3 Wait for the power-up diagnostic to run.

Step 4 If the BCC fails the power-up diagnostics a second time, replace it with another BCC that is known to have passed the test.

Once the software has successfully booted up, the display (a terminal connected to the CONTROL port or an NMS workstation connected via a telnet session to the LAN port) shows the software online screen as in the following example.

At this point, you may login as a user to the node.

Sample display:

```
pubsbpx1       TN    No User         BPX 15    9.2      Nov.  21 1998       14:15 PST












Enter User ID:
```

Provisioning the BPX Switch

Provisioning is the general term for configuring ports, lines, trunks, and adding connections to the BPX Switch.

Up to this point, you have used the command line interface (CLI) to perform the installation and power-up. You could use the CLI to perform provisioning also.

However, that is an exacting and time-consuming approach for most general provisioning tasks. It is recommended that you use Cisco Network Management, that is, the Cisco WAN Manager Workstation and Cisco's graphical WAN Manager and CiscoView applications to configure ports, lines, trunks and visually interconnect the BPX to your network topology.

For set-up and configuration procedures for Cisco Network Management, see *Chapter 20, Configuring Network Management*.

For configuration procedures for the BPX switch, proceed to *Chapter 17, Initial BPX 8600 Node Configuration*.

You might also need to refer to the following Cisco manuals:

- *Cisco WAN Manager Operations*
- *Cisco MPLS Controller Software Configuration Guide*
- *Cisco SES PNNI Controller Software Configuration Guide*.
- *Cisco WAN Switching Command Reference*
- *Cisco WAN Switching SuperUser Command Reference*

PART 3

Initial Configuration and Network Management

CHAPTER 17

Initial BPX 8600 Node Configuration

This chapter guides you through the initial node configuration that must be done before you can set up network management, which will enable you to use Cisco WAN Manager workstation to configure network connections

- Summary of Configuration Procedures
- Initial Node Configuration Summary
- Command Sequences for Setting Up Nodes
- Summary of Commands

Before proceeding with this chapter, make sure you have completed all procedures in Part Two, Installation. It is assumed that the BPX chassis is mounted, BPX cards are installed, cables connected, temporary terminal or network management station is connected, peripherals connected, and the BPX node is powered up.

You are now ready to do:

- Initially configure the node
  - Configure node name
  - Configure node number
  - Configure LAN IP address and subnet mask
  - Configure time zone
  - Configure network IP relay addresses
- Configure trunks (adding the new node to the network)
- Configure lines and ports (enabling and configuring user ports)
- Add and Configure Connections

Summary of Configuration Procedures

This section summarizes the configuration steps as an overview to the procedures in the following chapters.

For a description of the commands used to operate a BPX switch, refer to the *Cisco WAN Switch Command Reference*.

For node installation and operation, refer to the applicable reference publications: *Cisco IGX 8400 Series Reference* and Cisco *MGX 8220 Reference.*

Initial Node Configuration Summary

This section is an overview of adding nodes and trunks by using the command line interface.

As a minimum, you should configure the nodes, as applicable, by using:

- name (**cnfname**)
- date (**cnfdate**)
- time (**cnftime**)
- timezone (**cnftmzn**)
- trunks upped (**uptrk**)
- trunks added (**addtrk** or **addshelf**)

You may add connections now or later, after configuring the nodes for operation with the Cisco WAN Manager NMS manager.

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.

Here are the basic tasks to configure a BPX switch:

1. Set up the node.
    a. Configure the node name (**cnfname**)
    Before you can add a node to the network, you must assign it 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. This new name will be distributed automatically to other nodes in the network. For example, to assign the node the name of alpha, enter:

    ```
    cnfname alpha
    ```

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

    ```
    cnftmzn GMT
    ```

    c. Configure date (**cnfdate**)
    d. Configure time (**cnftime**)
    e. Configure the LAN interface (**cnflan**)
    f. Configure the auxiliary or terminal ports to support any necessary external devices such as a local printer, an autodial modem, or an external multiplexer attached to the unit (**cnfprt**, **cnfterm**, **cnftermfunc**)
2. Set up the trunks to other routing nodes.
    Verify that the correct cards are in both the local and remote nodes (**dspcds**).
    a. Up the trunks at each node (**uptrk**).
    b. Configure any parameters required for the trunk at each node (**cnftrk**).
    c. Add the trunks at each node (**addtrk**).
    d. Set up Y redundancy if desired (**addyred**).

3. If you are using an IGX Interface Shelf, configure it as a shelf.
    a. Up the trunk from the AIT/BTM to the BPX switch by using (**uptrk**). Shelf trunks for the IGX must be upped on both the BPX routing switch and the shelf before the shelf can be joined to the Routing Network.
    b. Contact Cisco Customer Service to configure the IGX shelf option.
    c. At the BPX switch, add the IGX switch as a shelf to the BPX (**addshelf**).
4. Adding the MGX 8220 or MGX 8800 Shelf.
    a. At the BPX switch, add the MGX as a shelf to the BPX switch (**addshelf**).
5. Set up ATM service lines and ports.
    a. Activate the line (**upln**).
    b. Configure the line (**cnfln**).
    c. Activate the ports (**upport**).
    d. Configure the ports (**cnfport**).
6. Set up ATM connections.
    a. Add connections (**addcon**).
    b. Configure a connection type (**cnfcontyp**).
7. Set up ATM to Frame Relay (ATF) connections.
    a. Add the connections (**addcon**).
    b. Configure connection classes (**cnfcls**).
    c. Configure connection groups (**addcongrp**).
8. Set up Interface Shelf Frame Relay Connections in Tiered Networks.
    a. Refer to the *Cisco WAN Manager Operations* publication.
    b. Frame Relay connections terminated at an MGX 8220 or MGX 8800 Shelf. You add and manage these by using the Cisco WAN Manager Connection Manager via the SNMP protocol. All connections are treated as end-to-end.
    c. ATM connections terminated at an MGX 8220 or MGX 8800 Shelf. You add and manage these by using the Cisco WAN Manager Connection Manager via the SNMP protocol. All connections are treated as end-to-end.

The “**dspnode**” screen displayed at the “shlf3igx” node shows that it is connected to the BPX switch via AIT trunk 8.

```
shlf3IGX          TN    edgar       IGX 8     9.3 June 20 2000 09:24 PDT

                        BPX Switching Shelf Information

Trunk    Name      Type      Alarm
   8     hubone    BPX       MAJ









Last Command: dspnode


Next Command:
```

Command Sequences for Setting Up Nodes

Follow the illustrated command sequences to perform these node-related tasks:

- Set up a node. See in Figure 17-1
- View information about the presence of the cards and system power. See Figure 17-2.
- Configure an interface for a control terminal that is connected to the node. See Figure 17-3.
- Remove a node from a network. See Figure 17-4.
- Add an interface shelf. See Figure 17-5.

Figure 17-1 Setting Up Nodes

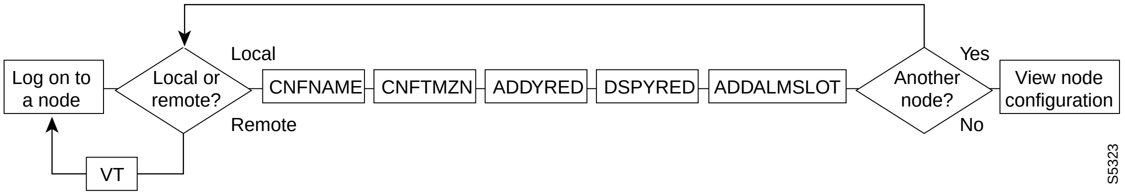


Figure 17-2 Viewing the Node Configuration

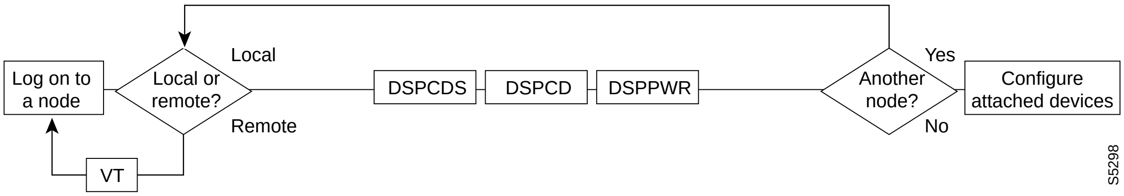


Figure 17-3 Configuring the Node Interface for a Local Control Terminal

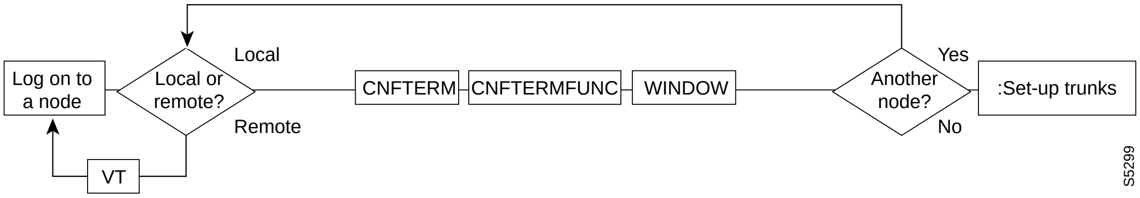


Figure 17-4 Removing a Node From the Network

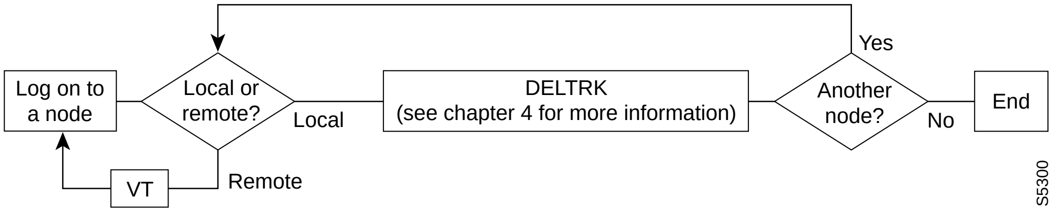
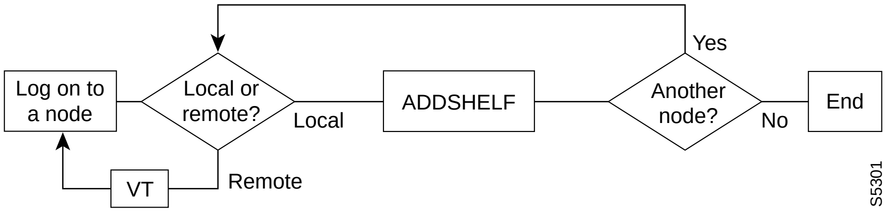


Figure 17-5 Add an Interface Shelf to the Network



Summary of Commands

Table 17-1 Here are the names and brief descriptions of each node command:

Table 17-1 Commands for Setting Up a Node

Name	Description
addalmslot	Add an alarm slot
addcdred	Add card redundancy for SONET APS 1+1 across two BXM cards
addctrlr	Add a PNNI VSI controller to a BPX node through an AAL5 interface shelf
addshelf	Add a trunk between an IGX or BPX core switch shelf and an interface shelf
addyred	Add Y-cable redundancy
cnfasm	Configure ASM card
cnfdate	Configure date
cnffunc	Configure system function
cnfname	Configure node name
cnfprt	Configure printing functions

Table 17-1 Commands for Setting Up a Node (continued)

Name	Description
cnfterm	Configure terminal port
cnftime	Configure time
cnftmzn	Configure time zone
delalmslot	Delete alarm slot
delshelf	Delete a trunk between a IGX/BPX core switch shelf and interface shelf
delcdred	Delete Y-cable redundancy (disables card redundancy (for SONET Automatic Protection Switching feature)
delyred	Delete Y-cable redundancy
dspasm	Display ASM card configuration
dspcd	Display card
dspcds	Display cards
dsplancnf	Display LAN configuration
dspctrlrs	Display all PNNI VSI controllers on a BPX node
dsplmistats	Display LMI Statistics
dspnds	Display nodes
dspnode	Display summary information about interface shelves
dsptermcnf	Display terminal configuration
dsptermfunc	Display terminal port configuration
dspprtcnf	Display print configuration
dsppwr	Display power
dspcdred	Display Y-cable redundancy (displays card redundancy for SONET Automatic Protection Switching)
dspyred	Display Y-cable redundancy
prtcdred	Print card redundancy (prints Y cable redundancy for SONET Automatic Protection Switching)
prtyred	Print Y-cable redundancy
upcd	Up card
window	Window to external device

CHAPTER 18

Configuring Trunks and Adding Interface Shelves

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

This chapter describes:

- Configuring Trunks
- Adding an Interface Shelf

Before proceeding to this chapter, you should first complete the procedures in:

- Part 2, Installation
- *Chapter 17, Initial BPX 8600 Node Configuration*

For details on virtual trunking, see:

- *Chapter 23, Configuring BXM Virtual Switch Interface*
- *Chapter 24, Configuring BXM Virtual Trunks*

Configuring Trunks

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 18-1 shows the communication technology for each node type, card combination, and line type.

Table 18-1 Supported Card Types

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

Table 18-1 Supported Card Types (continued)

Node Type	Front Card	Back Card	Line Types	Technology
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 (see the “Initial BPX 8600 Node Configuration” chapter.) Also, the front and back cards that support the proposed line type and communication technology must reside in the slot intended for the trunk.

You can configure port, routing trunk, and feeder trunk interfaces simultaneously on a slot containing a BXM 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 cards, you do not need to upgrade the firmware.

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 18-2 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

To set up a trunk:

Step 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. For details on virtual trunking, see *Chapter 24, Configuring BXM Virtual Trunks*.

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.

Step 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 18-1. (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 respecify 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.

Step 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 need only add one end of the trunk.

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 platforms, 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:

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:

- Statistical reserve
- Trunk Partitions SVC/PVC
- Maximum PVC Channels

For example, any increase to Statistical reserve would cause a reroute of all connections on the trunk. Any changes you make to these parameters will cause reroutes to PVCs on the trunk only if resources are no longer available to support the current connection load

Note that MPLS partitions will not be affected by trunk/line reconfiguration, because label 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. 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.

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:

- an IGX node configured as an interface shelf
- an MGX 8850 node configured as an interface shelf
- an MGX 8220 interface shelf
- an MGX 8800 interface shelf
- a Service Expansions Shelf (SES) with PNNI

For instructions on installing a Service Expansion Shelf in a BPX 8620 rack and initially powering up, see *Cisco Service Expansion Shelf (SES) Hardware Installation Guide*. To configure an SES PNNI for a BPX 8620, see the *Cisco SES PNNI Controller Software Configuration Guide*.

Because tiered network capability is a purchased option, personnel in the Technical Assistance Center (TAC) must first configure a node to serve as an interface shelf. Then 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 Figure3-7 for an illustration of the command sequence for setting up an interface shelf. (Note that **addshelf** and **addtrk** are mutually exclusive commands.)

To delete a feeder shelf, use **delshelf**.

To view conditions on a feeder trunk, use **dspnode**.

Table 18-3 show designations for various devices that can be used as interface shelves. To display these designations, use the display commands **dspnw** and **dspnode**. The **dspnode** command identifies the hub and feeder nodes and shows the alarm status.

Table 18-3 Interface Shelf Designations

Device Serving as Shelf	Designation
MGX 8220	AXIS
MGX 8850	AAL5
SES (Service Expansion Shelf)	AAL5
IGX	AGX/AF

CHAPTER 19

Configuring Circuit Lines and Ports

A circuit line is the physical wire that carries data, voice, Frame Relay, or ATM traffic between a BPX node (or IGX node) and customer premises equipment (CPE). Each piece of customer premises equipment is attached to a node through a circuit line.

A circuit line is connected to a physical interface on a switch backcard. Each physical line interface is represented by a unique software configuration called a *port* or *logical interface* for that line. A port is the logical interface between the BPX network and a single ATM device attached by a line. There is one port for each active line.

ATM ports are provided on ASI and BXM cards.

Before you can add connections on the circuit line, you must create a port or a virtual port on the line.

This chapter describes:

- Setting Up a Circuit Line
- Setting Up Ports and Virtual Ports
- Local Management Interface and Integrated Local Management Interface
- ILMI Neighbor Discovery

Setting Up a Circuit Line

ATM connections require an active line.

Before you can activate and configure a *circuit line* on a card, you must first establish or “up” a card by using the **upcd** command.

Use the **cnfln** to configure circuit lines. The switch software prompts for the parameters appropriate for the card type it detects. For details on each circuit line command, see the *Cisco WAN Switching Command Reference*. Note: Line commands are the same as “circuit line” commands.

To establish (or “up”) an active line:

Step 1 Make sure the card must be in either the active or standby state

Step 2 Use **upln** to activate a circuit line in a slot that contains the appropriate circuit line card set.

Step 3 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.

To down a line:

Step 1 Remove all connections on a line by using **delcon** or **delcongrp**).

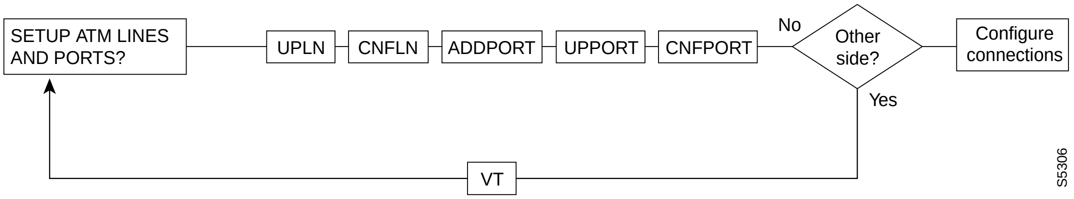
Step 2 **Use dnln** to down the line. A downed line is inactive, so no signals or statistics are generated.

Flow Diagram for ATM Line Setup

The command sequence for setting up lines for ATM is shown in Figure 19-1

A yes/no decision branch for “Other Side?” and the **vt** command in the sequence indicates command sequences on local and far nodes.

Figure 19-1 Setting Up ATM Lines



Line Commands

Table 19-1 Here are the names and descriptions for each line command:

Table 19-1 Line Commands

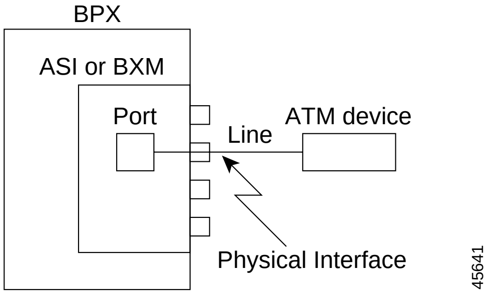
Name	Description
cnfln	Configure line (same as cnfcln)
cnfrsrc	Configure resources
dnln	Down line (same as dncln). A downed line is inactive, so no signals or statistics are generated. You must remove all connections on a line (delcon or delcongrp) before you down the line by using dnln.
dsplncnf	Display line configuration (same as dspclncnf). Displays the configuration of a specified circuit line.
dsplns	Displays the circuit line configuration and alarm status for the node (same as dspclns)
prtlns	Prints the circuit line configuration and circuit line alarm status for the node (same as prtclns)
upln	Up line (same as upcln)

Setting Up Ports and Virtual Ports

Once you have set up a circuit line, you are ready for the next step in adding connections: to create a port or one or more virtual ports for the line.

A port is the unique logical interface between the BPX network and a single attached ATM device.

Figure 19-2 Ports and Lines



Once you have activated a line by using the **upln** command, to set up a port or virtual port:

Step 1 Add a port by using the **addport X.Y[.Z]** command, where X is the slot, Y is the port, and Z is an optional virtual port number**.**

Step 2 Activate the port by using the **upport X.Y[.Z]** command, where X is the slot, Y is the port, and Z is an optional virtual port number**.**

Step 3 Use the **cnfport** command to establish the characteristics for the port.

Note When adding a connection to a virtual port on a BXM card, the virtual port number is not required. The slot, port, and VPI will map to the supporting virtual port.

Note In Release 9.3.0, if a slot-port combination for a BXM card has been brought up as a port (**upport X.X**), that slot-port cannot have virtual ports activated unless the port is first deleted (**delport X.X**). The opposite also applies; once a virtual port is configured, it cannot be used as a port until all virtual ports are deleted (**delport X.X**).

Virtual Ports

Virtual ports are logical interfaces like virtual trunks, trunks, and ports. (A maximum of 31 logical entities are available on a BXM card.)

Virtual ports is an optional feature that must be configured by Cisco on the BPX.

One or more virtual ports may function on a single port connected to CPE devices, directly or through an ATM cloud. Although virtual ports, like ports, can connect directly to CPEs, they are generally used to connect indirectly.

Traffic shaping has previously been supported on ports and on connections. Virtual ports on BPX switches provide hierarchical traffic shaping, which means both virtual port traffic shaping and connection traffic shaping.

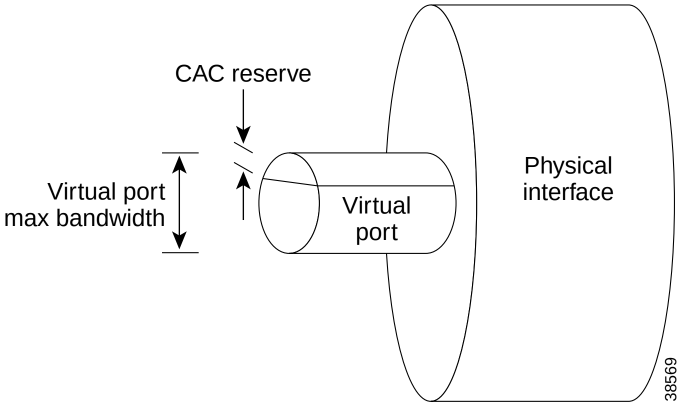
A virtual port may carry multiple PVCs or PVPs. VI traffic shaping capability is provided per virtual port. Additionally, connection traffic shaping is available on a QOS basis. While virtual port shaping is always ON, you can turn connection traffic shaping ON or OFF by using the **cnfportq** command.

Each virtual port supports all Automatic Routing Management (AutoRoute) traffic types that are currently supported by ports.

To set the maximum bandwidth available for use on that virtual port, use the Bandwidth parameter of the command **cnfport** (see Figure 19-3). This parameter is similar to the Bandwidth parameter used for ports. However, while the Bandwidth parameter is configurable on a virtual port, on a port, this parameter is not configurable; it is automatically set to the line speed.

You can configure a virtual port's bandwidth to the full port bandwidth or a subset thereof. However, the bandwidth sum of all virtual ports on a port cannot exceed the port's total bandwidth.

Figure 19-3 Port Bandwidth



Virtual Port Examples

This section describes two of many possible examples of virtual port configurations.

- **Type I** Virtual Ports can have PVP or PVC connections terminating on it.
All traffic through this Virtual Port is constrained to the Virtual Port's configured bandwidth (Virtual Port shaping). Moreover, if connection shaping is enabled (per QOS), each connection will be constrained to its PCR and be given a fair chance to transmit by using WFQ (Weighted Fair Queuing).
- **Type II** Virtual Ports have PVC connections all with the same VPI terminating on it.
As with the type I Virtual Port above, all traffic through this port is constrained to the Virtual Port's configured bandwidth. If connection shaping is enabled, each connection will be constrained to its PCR and undergo WFQ.

The BPX switch software does not distinguish between the two types of virtual ports.

Depending on the interface type, UNI or NNI, the maximum number of PVPs will be 255 or 4095 respectively. The maximum number of VCIs is 65535.

Local Management Interface and Integrated Local Management Interface

Local Management Interface (LMI) is a protocol that lets you monitor the status of permanent virtual connections between two communication devices.

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

LMI and ILMI functions for the BXM card support virtual UNIs, feeder and virtual trunk ports, a total of 256 sessions on different interfaces (ports, trunks, virtual UNIs) per BXM.

For ILMI information, refer to Table 19-2

.

Table 19-2 ILMI Parameters

Parameter	Description
VPI.VCI	VPI.VCI for ILMI signaling channel equal 0.16 as default
Polling Enabled	Keep-alive polling
Trap Enabled	VCC change of state traps
Polling Interval	Time between GetRequest polls
Error Threshold	Number of failed entries before ILMI link failure is declared.
Event Threshold	Number of successful polls before ILMI link failure is cancelled.

For the LMI information, refer to Table 19-3

.

Table 19-3 LMI Parameters

Parameter	Description
VPI.VCI	VPI.VCI for LMI signaling channel equal 0.31
Polling Enable	Keep-alive polling
T393	Status Enquiry timeout value
T394	Update Status timeout value
T396	Status Enquiry polling timer
N394	Status Enquiry retry count
N395	Update Status retry count

Early Abit Notification with Configurable Timer on LMI/ILMI Interface

The time required 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 customer premise equipment if a connection is derouted and fails to transport user data after a specified time interval. However, it is also desirable not to send out Abit = 0, then Abit =1 when a connection is derouted and rerouted quickly. Such notifications might prematurely trigger the CPE backup facilities, causing instabilities in an otherwise stable system.

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.

The time period is configurable. The configurable time gives you the flexibility to synchronize the operation of the primary network and backup utilities, such as dialed backup over the ISDN or PSTN network.

Configuring Early Abit Notification

You configure the timer delay period by setting **cnfnodeparm** parameters. You want to choose timer settings that give you the flexibility to synchronize the operation of the primary network and backup utilities, such as dialed backup over the ISDN or PSTN network.

Be aware of these guidelines when using the Early Abit feature:

- When you 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.
- 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).
- If the **cnfnodeparm** parameter *Abit Timer Multiplier M* 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).
- 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.

Recommended Settings

You should be aware of the dynamic relation between the two timer parameters:

- **Abit Timer Granularity N**
  The time period is referred to as N, which defines the granularity of the timers. You specify N by the value of the **cnfnodeparm** Abit Timer Granularity N parameter.
  The default value for N is 3 sec.
- **Parameter X**
  The time to wait before Abit = 0 is sent out if the connection is in a derouted state.
  X, is set to be M*N
- **Abit Timer Multiplier M**
  M can be configured to be from 0 to 100. Default value for M (Abit Timer Multiplier M parameter) is 0, meaning Abit = 0 is sent out on deroute.

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.

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.

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 that 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.

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.

Behavior with Previous Releases

Early Abit Notification on ILMI/LMI Using Configurable Timer is supported on both the BPX and IGX platforms. 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.

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.

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.

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 was 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.

Performance Considerations

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.

There are two factors in performance:

- **System performance**
  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**
  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.

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, the estimated time to reroute all 12K connections increases no more than 5 percent.

Note that on 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.

ILMI Neighbor Discovery

The ILMI Neighbor Discovery feature, available only with the BXM card, enables a network management system such as Cisco WAN Manager or CiscoWorks 2000 to discover other attached ATM devices such as Cisco ATM routers or switches, provided that those devices also support ILMI Neighbor Discovery.

The ILMI Neighbor Discovery feature is supported only on a BXM port, but not on a virtual port.

Configuring the BPX for ILMI Neighbor Discovery

To enable ILMI Neighbor Discovery on the BXM card, use the **cnfport** command to set the BXM card parameters shown in ILMI Neighbor Discovery ParametersTable 19-4.

Table 19-4 ILMI Neighbor Discovery Parameters

Parameters	Value
Protocol	ILMI
Protocol by Card	Yes
NebrDisc Enabled	Yes
ILMI Polling Enabled	Yes

Use the **cnfport** command to enable ILMI Neighbor Discovery:

```
sw143          TN    Cisco        BPX 8620  9.3.10    Aug. 9 2000  16:23 GMT

Port:     4.3       [ACTIVE  ]                Bandwidth/AR BW: 353208/353208
Interface:          LM-BXM                    CAC Override:    Enabled
VPI Range:             0 -  255               CAC Reserve:      0
Type:               UNI                       %Util Use:       Disabled
Shift:              SHIFT ON HCF (Normal Operation)
SIG Queue Depth:    640                       Port Load:        0 %

Protocol:           ILMI                      Protocol by Card: Yes
NbrDisc Enabled:    Yes
   VPI.VCI:                            0.16      Addr Reg Enab:  Y
   ILMI Polling Enabled:               Y
   Trap Enabled:                       Y
   T491 Polling Interval:             30
   N491 Error Threshold:               3
   N492 Event Threshold:               4         ILMI Reset Flag:Y

Last Command: cnfport 4.3 353208 N H I 0 16 Y Y Y 30 3 4 Y N 0 N Y Y
```

Publishing the BXM Interface Information

When ILMI Neighbor Discover is enabled on a BXM port, the BPX and the attached ATM device exchange their management IP addresses and other interface information with each other via the ILMI protocol.

The exchanged information consists of:

- atmfMyIfName: physical interface name
- atmfMyIfIdentifier: Interface identifier
- atmfMyIpNmAddress: Management IP Address, either the LAN IP or network IP.
- atmfMySysIdentifier: System Identifier, a 6-byte string read from the BPX NOVRAM, or if not available, the default value is "000001".

Meaning of the NebrDiscEnable Parameter

Table 19-5 NebrDisc Enabled Parameter

Value	Meaning
No	The BPX will NOT publish its interface information to its neighbor. However, the BPX still queries for its neighbor information and if the neighbor's interface information is available, it will make the information available to CWM or any NMS applications requesting it. If there is a desire to keep the BPX interface information secure, set this parameter to No.
Yes	The BPX will provide its interface information to its neighbor if queried.

Note If the port is also controlled by a PNNI controller, disabling Neighbor Discovery has no effect.

Configuring the ILMI Management IP address

The Management IP address is used by the NMS application to access the BPX or the ATM device. Depending on your network set up, you can configure the BPX to send either the LAN IP address or Network IP address as part of the neighbor information exchange with the attached ATM device.

To select LAN IP or NETW IP, use the **cnfnodeparm** command with option #56 Dnld LanIP or NwIP.

Enter 0 for LAN IP address, or 1 for Network IP address. The default is the network IP address for BPX.

```
sw143          TN    Cisco       BPX 8620  9.3.10    Aug. 9 2000  16:25 GMT

31 TFTP Write Retries     [    3] (D)   46 Max Htls Rebuild Count [ 100] (D)
32 SNMP Event logging     [    Y] (Y/N) 47 Htls Counter Reset Time[1000] (D)
33 Job Lock Timeout       [   60] (D)   48 Send Abit early        [   N] (Y/N)
34 Max Via LCONs          [50000] (D)   49 Abit Tmr Multiplier  M [   0] (D)
35 Max Blind Segment Size [ 3570] (D)   50 Abit Tmr Granularity N [   3] (D)
36 Max XmtMemBlks per NIB [ 3000] (D)   51 FBTC with PPDPolicing  [   N] (Y/N)
37 Max Mem on Stby Q (%)  [   33] (D)   52 CommBrk Hop Weight     [  25] (D)
38 Stat Config Proc Cnt   [ 1000] (D)   53 CB Fail Penalty Hops   [   2] (D)
39 Stat Config Proc Delay [ 2000] (D)   54 Auto BXM upgrade       [   Y] (Y/N)
40 Enable Degraded Mode   [    Y] (Y/N) 55 LCN reprgrm batch cnt  [ 100] (D)
41 Trk Cell Rtng Restrict [    Y] (Y/N) 56 Dnld LanIP or NwIP     [   1](Lan/Nw)
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)

This Command: cnfnodeparm 56


Enter 0 (LanIP) or 1 (NwIP):
```

Displaying Neighbors

You can use the **dspnebdisc** command to display all the neighbor's information discovered by the BPX via the ILMI Neighbor Discovery procedure.

```
sw143          TN    Cisco       BPX 8620  9.3.10    Aug. 9 2000 17:02 GMT
 Port Neighbor Discovery
Port     Enable State    NbrIpAddress     NbrIfName
4.1      No     ACTIVE   N/A              N/A
4.3      Yes    ACTIVE   172.29.9.205     ATM1/0
4.4      No     ACTIVE   172.29.9.206     ATM3/0
11.1     Yes    ACTIVE   172.29.9.207     ATM1/0
```

CHAPTER 20

Configuring Network Management

A permanent network management station (NMS) enables you to use Cisco's network management software, including CiscoView and Cisco WAN Manager. For many configuring and provisioning tasks, you may find the graphical interface more convenient than the command line interface.

During the initial setup of the BPX node, you temporarily connected a terminal or Cisco WAN Manager workstation to the CONTROL port, as required for initial power-up. However, this temporary CONTROL port connection is not used in normal operation. This chapter explains how to connect a permanent network management station to the LAN port

(Of course, you can always access the BPX switch through a local control port over an RS-232 or Ethernet TCP/IP link. You use an administration screen from a control terminal or from the Cisco WAN Manager Network Management Station (NMS) to issue BPX switch commands.)

To connect a permanent network management station, you must configure both the nodes and the Cisco WAN Manager workstation.

This chapter covers these initial procedures for setting up a permanent network management station:Configuring the BPX Switch LAN and IP Relay

- LAN Connection for the Network Management Station
- Configuring the BPX Switch LAN and IP Relay
- Configuring the LAN Port
- Controlling External Devices

For remote control terminal access, you can use a Virtual Terminal (**vt**) command provided that the node has been configured with a name and at least one trunk to the network has been established.

When an IGX is configured as an Interface Shelf, it cannot be reached by the **vt** command. For this reason, you must configure Frame Relay end-to-end connections from the Cisco WAN Manager via the Connection Manager over an in-band LAN connection.

However, Telnet can be used to access an interface shelf (such as an IGX shelf, MGX 8220, or MGX 8800 shelf) if a Cisco WAN Manager workstation is not available to provide in-band management.

You can monitor, manage, and troubleshoot the BPX switch by using the Cisco WAN Manager Network Management Station. You issue commands to a BPX switch through the Node Administration window.

You use Cisco WAN Manager's Connection Manager to provision and perform end-to-end configuration management for Frame Relay connections in both tiered and non-tiered networks.You can display and monitor the network's topology, monitor alarms, events, and statistics. Refer to the *Cisco WAN Manager Operations* manual.

For an overview of BPX network management software, including WAN Manager, see *Network Management*, in *Chapter 1, The BPX Switch: Functional Overview*.

For details about using the command line interface (CLI) to perform initial NMS setup, refer to the *Cisco WAN Switch Command Reference.*

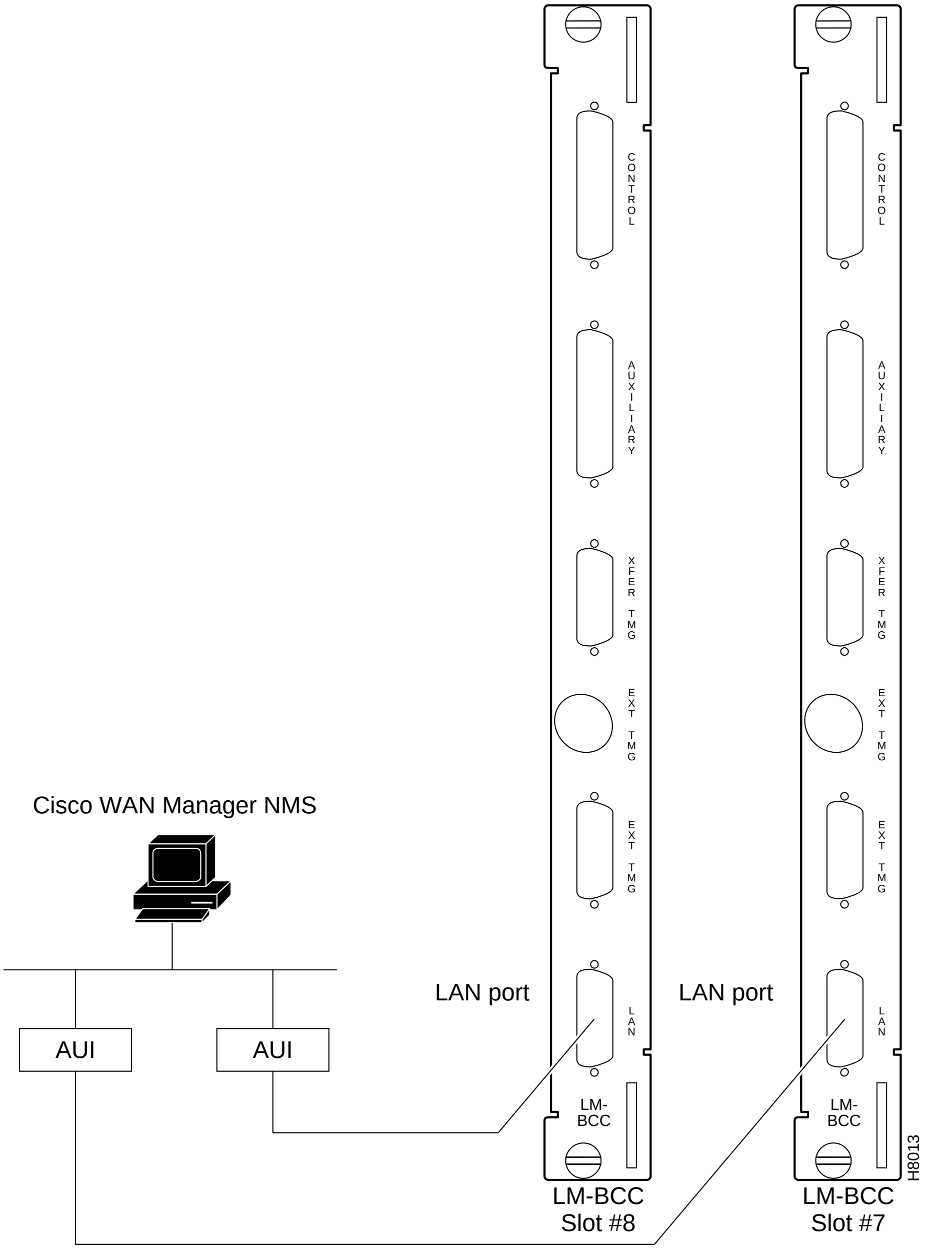
LAN Connection for the Network Management Station

You connect the Cisco WAN Manager Network Management Station to an Ethernet port (LAN port) on a node in the network. The LAN port provides the capacity necessary for network management traffic and network statistics collection. See Figure 20-1 illustrating this connection.

For access to the node using an Internet connection, you must use the **cnflan** command to enter:

- Internet Protocol (IP) address
- IP subnet mask
- TCP service port
- Gateway IP address

Figure 20-1 LAN Connections to BCC Backcards, LM-BCCs Shown



Configuring the BPX Switch LAN and IP Relay

In setting up network management for a network, you must configure both the Cisco WAN Manager workstation and network nodes.

Cisco WAN Manager communicates over a standard physical LAN network to a gateway node or nodes, but you must setup a separate in-band IP relay network for all nodes via a gateway node for SNMP and TFTP in-band communication over the node trunks.

During the configuration of BPX switch interfaces, you must make sure that these parameters are set consistent with your local area network (Ethernet LAN):

- The BPX switch IP address
- SNMP parameters
- Network IP address

Use these BPX switch commands to set the parameters:

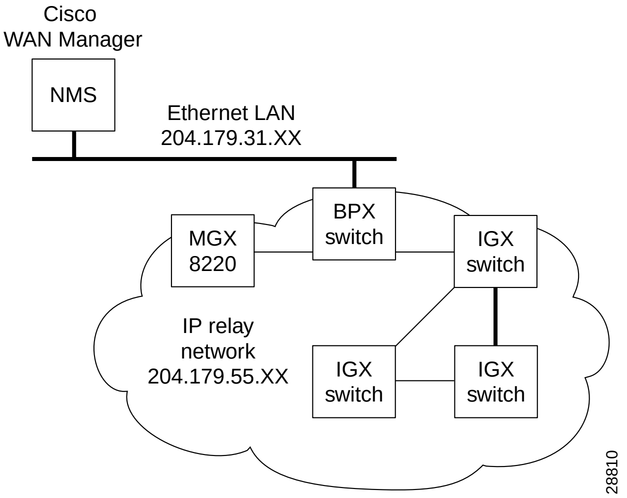
- **cnflan**
  This is a SuperUser command that must be used to configure the BPX switch BCC LAN port IP address and subnet mask. This command is necessary only for nodes or shelves in which the LAN port is actually connected to a physical Ethernet LAN as shown in Figure 20-2.
- **cnfsnmp**
  This command configures the SNMP Get and Set community strings for the BPX switch:
  - Get Community String = public
  - Set Community String = private
  - Trap Community String = public
- **cnfnwip**
  This is a Superuser command to configure the virtual IP network (IP relay) among BPX switches.
- **cnfstatmast**
  This command is used to define the IP address for routing messages to and from the Statistics Manager in CiscoView.

On BPX and IGX switches, use these commands to configure the nodes for operation with Cisco WAN Manager:

- **cnflan (**This command is necessary only for nodes or shelves in which the LAN port is actually connected to a physical Ethernet LAN as shown in Figure 20-2.)
- **cnfnwip**
- **cnfstatmast**
- **cnfsnm**

The use of these commands is covered in the *Cisco WAN Switching Command Reference* or the *Cisco WAN Switching SuperUser Command Reference*. SuperUser commands may be used only by authorized personnel with great care.

Figure 20-2 Cisco WAN Manager Physical LAN and IP Relay Network



Configuring the Cisco WAN Manager Workstation

Step 1 Contact your System Administrator to obtain IP addresses.
Note: For the workstation to use /etc/hosts, it must not be able to access the NIS directory even though it may be linked to other LANs besides its own local network.

Step 2 Enter physical IP addresses and physical LAN node names (with a letter “p”, for example, such as “nw1bpx1p”, to differentiate from IP relay name) in /etc/hosts and also enter IP relay addresses with actual configured node names (“nw1bpx1”, for example).

```
beacon% more /etc/hosts
#
# Sun Host Database
#
# If the NIS is running, this file is only consulted when booting
#
127.0.0.1       localhost
#
204.179.61.121  beacon loghost

# node physical ethernet LAN addresses

204.179.61.104 nw1bpx1p
204.179.61.71 nw1axi1p

# node ip relay addresses

204.179.55.101 nw1ipx1
204.179.55.102 nw1ipx2
204.179.55.103 nw1ipx3
204.179.55.123 nw1igx1
204.179.55.111 nw1bpx1
204.179.55.105 nw1axi1
```

If the workstation is connected to the corporate network for access to hosts on another network, add any IP addresses and associated names of the hosts that you may want to connect to your workstation, because the NIS is disabled.

Step 3 Enter the name or IP address of the gateway node in config.sv, using physical LAN name, such as, “nw1bpx1p”.
Note: normally a BPX switch is used for the gateway node because of its greater processing power.

0|Network1|nw1bpx1p|9600|0|7|6|0|30|1024|9.1|

or

0|Network1|204.179.61.104|9600|0|7|6|0|30|1024|9.1|

Step 4 Enter IP Relay subnet mask in /etc/rc2.d/S72inetsvc file:

```
vi /etc/rc2.d/S72inetsvc
/usr/sbin/route add “224.0.0.0 ...................{this is already there
# route add for Cisco WAN Manager
route add net 204.179.55.0 204.179.61.104 1
```

Note The **routeAdd** command sets up the route for all nodes in the 204.179.55.0 IP relay subnetwork. In this example, the name “nw1bpx1p” is the name in the /etc/hosts table associated with the physical LAN port IP of 204.179.61.104 on the gateway node, such as, “nw1bpx1”. In steps 2 and 3, either the name “nw1bpx1p” or the IP of “204.179.61.104” can be entered.

Configuring the LAN Port

Note Configure the LAN parameters of the nodes before connecting them to a LAN.

Refer to the *Cisco WAN Manager Operations* for instructions on configuring the Cisco WAN Manager workstation. Refer to the *Cisco WAN Switching Command Reference* for command definitions.

Step 1 Contact your System Administrator to obtain IP addresses for your workstation and for the BPX/IGX switches you are going to configure. Also, access to the NIS directories should be disabled so that the workstation will consult the /etc/hosts table for IP LAN relay addresses.

Normally, the System Administrator will provide the IP addresses for the workstation and node.

The addresses shown are just examples. Use the addresses obtained from your System Administrator. (This example is for a workstation named “hedgehog” at address 192.187.207.200. It also assumes that the BPX or IGX switch LAN port for node sanfran has been assigned an IP address of 192.187.210.30 and a host name of sanfran. Your own host name and addresses will be different.)

```
192.187.207.200  hedgehog
192.187.210.30  sanfran
```

Note If an NIS is being used (such as, corporate network), you will need to contact the system administrator.

Note 5120 is used for the LAN ports on all BPX switch ports.

Step 2 Configure the LAN port on the BPX switch by using a dumb terminal or an RS-232 connection via the workstation (using the **vt** command, as applicable) to enter the appropriate **cnflan** parameters.

The **cnflan** command configures the node's communication parameters so that the node can communicate with a Cisco WAN Manager terminal over an Ethernet LAN using the TCP/IP protocol. The parameters contain address information about the Ethernet TCP/IP network that is used to connect the Cisco WAN Manager station to an IGX or BPX switch. The values used must conform to those of the network and should be supplied by the Ethernet network administrator.

The **cnflan** command has these parameters:

- **Active IP Address** is the Internet Protocol address of the node used in the TCP/IP protocol.
- **IP Subnet Mask** is a 32-bit mask. The default for a Class C LAN network is 255.255.255.0. (Other than C Class masks may be used.)
- **IP Service Port** is the BPX/IGX switch LAN port number entered in the **/etc/service** file on the workstation. It is 5120 for all BPX/IGX switches.
- **Default Gateway IP Address** is the Internet gateway address. This is the gateway that traffic is routed through if the BPX or IGX switch and workstation are on different networks. If they are on the same network, the gateway is not used. The default "none" is displayed in this case. (Note: If a gateway IP is entered and later you want to remove it, enter 255.255.255.255 opposite the "IP Subnet Mask" prompt and 192.0.0.0 opposite the "Default Gateway IP Address" prompt and "none" will again be displayed. The node will reset itself if you do this.)

A **cnflan** screen is shown in the following example for the LAN setup shown in Figure 20-3.

An IP address of 192.187.210.30 has been entered as the active IP address for the node. The IP Subnet mask is entered as 255.255.255.0 for a Class C LAN network.

The TCP service port is entered as 5120.

Because the workstation and node are on different networks in this example, a gateway address of 192.187.207.1 (the address of the node serving as a gateway for Cisco WAN Manager, in this example), has been entered. You must obtain this gateway address from your System Administrator. If the workstation and node are both on the same network, no gateway address is needed.

The "Maximum LAN Transmit Unit" and "Ethernet Address" parameters are not configurable by the **cnflan** command.

The "Ethernet Address" is a hardware address that is different for every node controller card, such as, BCC.

Example: Configuring a Control Port (Gateway Router Example)

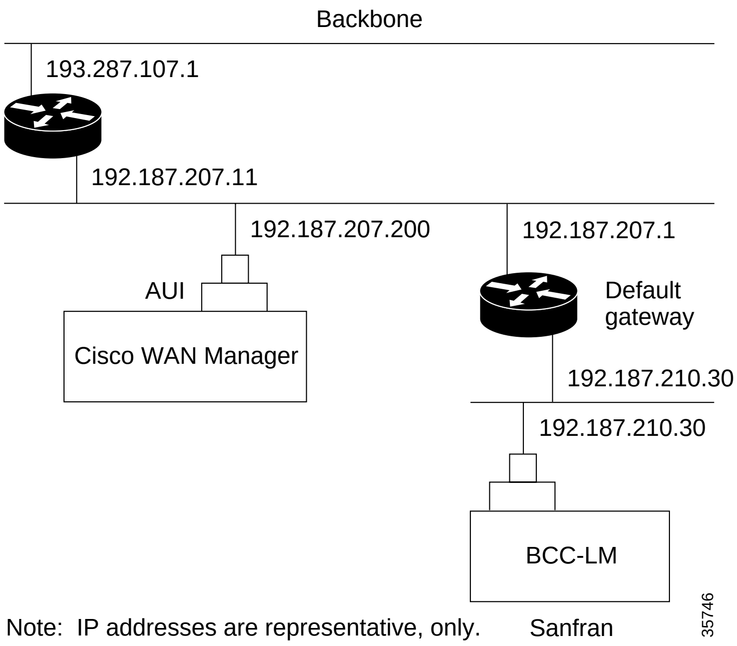
```
beta       TN    YourID.1       BPX 15    9.3 July 3 2000 02:16 PST

Active IP Address:                     192.187.210.30
IP Subnet Mask:                        255.255.255.0
IP Service Port:                       5120
Default Gateway IP Address:            192.187.207.1
Maximum LAN Transmit Unit:             1500
Ethernet Address:                      00.C0.43.00.00.20


Type      State
TCP       UNAVAIL
UDP       READY
Telnet    READY

This Command: cnflan

Enter IP Address:
```

Step 3 Connect the Cisco WAN Manager workstation and the BPX switch to a LAN network. The LAN port on the BPX switch provides a DB-15 connector that can be connected to a Y-cable which in turn is connected to an AUI.

Step 4 To test that a LAN connection to the BPX switch LAN port is okay, for example, for a host name of “sanfran” entered in the **config.sv** file, you would enter the following at the Cisco WAN Manager workstation:

```
ping sanfran
```

Figure 20-3 Cisco WAN Manager LAN Connection via Gateway Router to a BPX Switch



Step 5 An IP Relay address must be configured for each node. The following example shows an example of using the **cnfnwip** command to configure the IP Relay address for a node.

Also, at the workstation, the /etc/hosts table and routing must be set up for each node in the network. This enables network management using SNMP and statistics collection using TFTP via inband ILMI.

Assuming an isolated network for the nodes, the workstation must be isolated from the NIS reference pages so that the Cisco WAN Manager workstation consults the /etc/hosts table. Refer to the *Cisco WAN Manager Operations* manual.

Example of the display using **cnfnwip** to configure IP Relay address (required for each node):

```
beta     TN     YourID        BPX 15   9.3 July 3 2000 02:11 PST

Active Network IP Address:             192.187.57.10
Active Network IP Subnet Mask:         255.255.255.192




This Command: cnfnwip


Enter active network IP address:
```

Step 6 Once the workstation and BPX switch interface have been set up, you can start Cisco WAN Manager. The following example shows the **dsplan** screen after you've started Cisco WAN Manager and the communication sockets are active.

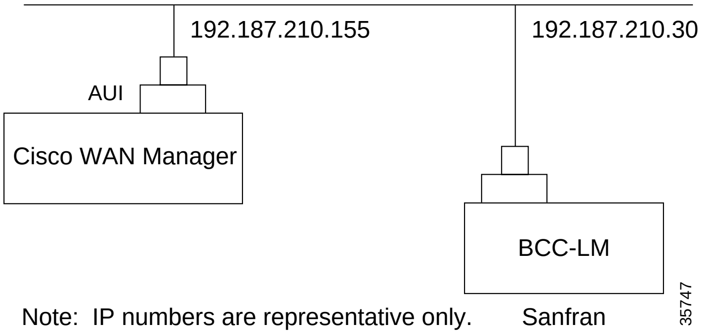
"Sockets" is the BSD Unix name for connections between processes, typically used in network communication.

Example of **dsplan** after Cisco WAN Manager has been started:

```
beta       TN    YourID.1       BPX 15    9.3 July 3 1998  02:16 PST


Active IP Address:                     192.187.210.30
IP Subnet Mask:                        255.255.255.0
IP Service Port:                       5120
Default Gateway IP Address:            192.187.207.1
Maximum LAN Transmit Unit:             1500
Ethernet Address:                      00.C0.43.00.00.20


Control Socket - Ready

Open Socket Descriptor - 2


Last Command: dsplan

Next Command:
```

Figure 20-4 shows an example of a Cisco WAN Manager workstation LAN connection to a BPX switch on a network with no gateway router, nor connection to another LAN. This type of LAN connection could also be connected through a "Hub" which is essentially a signal splitter (passive or active).

Figure 20-4 Cisco WAN Manager LAN Connection to a BPX Switch (no gateway)



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:

Step 1 First, check the port and the port function with **cnfterm** and **cnftermfunc**.

Step 2 Next, determine whether the external window device is cabled to a node's Control Terminal (EIA/TIA-232) port or Aux Port (EIA/TIA-232) port.

Step 3 Use the Virtual Terminal (**vt**) command to access the node cabled to the device.

Step 4 Invoke the **window** command. The format for the **window** command is:

```
window [a | c]
```

Step 5 Enter an **a** if the external device is attached to the node's Aux Port or
Enter **c** if the device is attached to the node's Control Terminal port. The default for this parameter is Aux Port.

Step 6 To establish a **window** session with an external device attached to a node's Control Terminal port, enter:

```
window c
```

Step 7 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

Step 8 Enter an escape sequence.

Escape sequences are one to eight characters in length. You configure escape sequences by using 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.

PART 4

Configuring Connections

CHAPTER 21

Configuring ATM Connections

This chapter explains how to establish ATM connection services by adding ATM connections between ATM service interface ports in the network using ATM standard UNI 3.1 and Traffic Management 4.0:

- ATM Connection Services
- Setting Up an ATM Connection
- Traffic Management Overview
- ATM Connection Requirements
- ATM Connection Flow
- rt-Vbr and nrt-Vbr Connections
- ATM Connection Configuration
- Traffic Policing Examples
- ATM Command List

ATM Connection Services

You establish ATM connection services by adding ATM connections between ATM service interface ports in the network.

- on the BPX switch through cards configured for port (service access) operation:
  - BXM-T3/E3
  - BXM-155 (OC-3)
  - BXM-622 (OC-12) cards
- or on the MGX 8220 through the AUSM card for the MGX 8220

Frame relay to ATM network interworking connections are supported between either BXM cards to:

- the IGX
- the MGX 8220
- the MGX 8800
- or to FRSM cards on the MGX 8220

Figure 21-1 depicts ATM connections over a BPX switch network, via BXM-T3/E3, BXM-155, BXM-622, as well as over MGX 8220 switches. It also shows Frame Relay to ATM interworking connections over the MGX 8220 and IGX shelves.

For further information on the MGX 8220, refer to the *Cisco MGX 8220 Reference*.

For further information on the MGX 8800, refer to the *Cisco MGX 8800 Reference*.

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.

Note As of Release 9.3.0, for BPX ports: **upln** no longer automatically configures a port. You can verify that the line has been activated by using the **dsplns** command. (See Chapter 5, “BXM Card Sets: T3/E3, 155, and 622,” for descriptions of **upln** and **dsplns**.)

Step 2 For BPX ATM, add an ATM port by using the **addport X.Y[.Z]** command, where X is the slot, Y is the port, and Z is the optional virtual port number**.**

Step 3 Use the **cnfport** command to establish the characteristics for the ATM port.

Step 4 Activate the ATM port with the **upport X.X[.X]** command, where X is the slot, Y is the port, and Z is the optional BXM card virtual port of the ATM card set.

Step 5 If a suitable class is already configured, note its number and use this class when adding the ATM connection by using the **addcon** command. (The **dspcls** command displays the parameters for each connection class. The **cnfcls** command allows you to modify an individual class.)

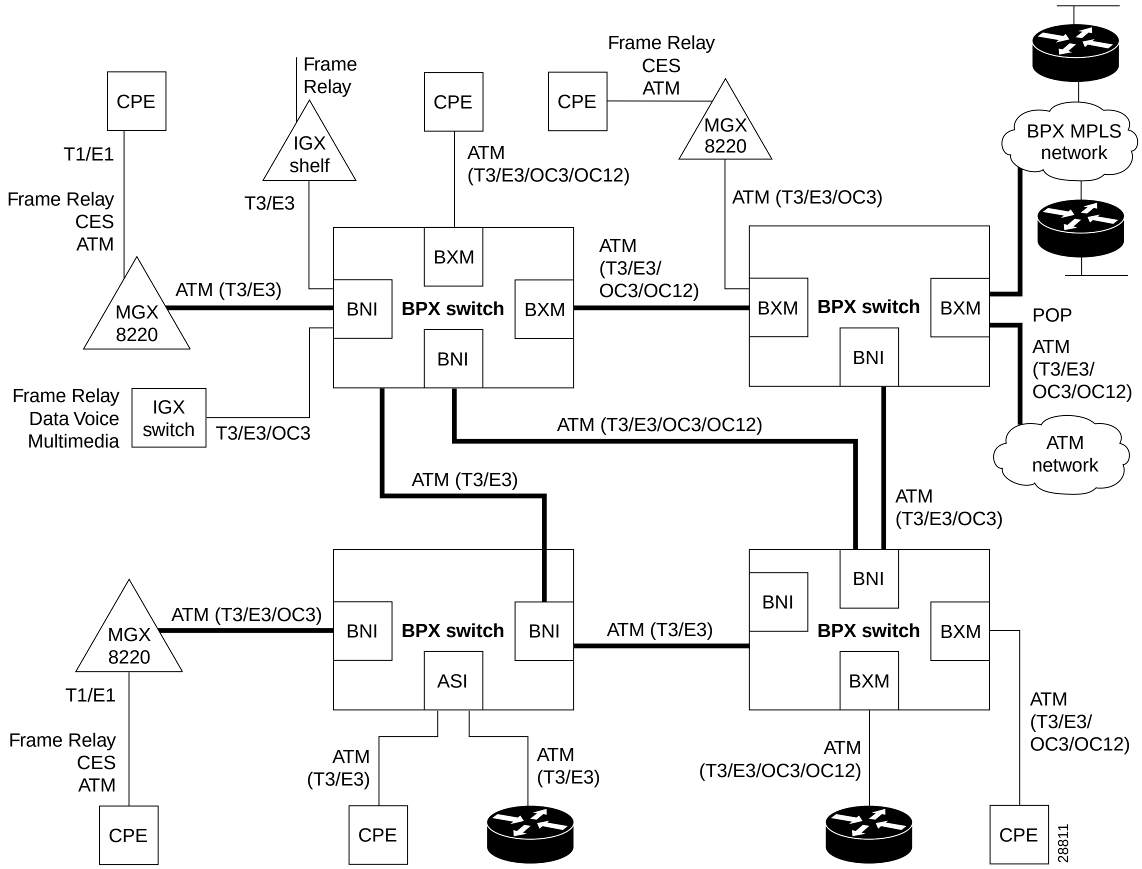
Step 6 Use the **vt** command to log in to the node at the remote end of the proposed ATM connection.

Step 7 At the remote node, use the **upln**, **addport**, **upport,** and **cnfport** commands, as listed in Steps 1 through 4, to activate and configure the remote port.

Note Use the **addcon** command at one end of the connection to activate the ATM connection.

Note In Release 9.3.0, if a slot-port combination for a BXM card has been brought up as a port (**upport X.X**), that slot-port cannot have virtual ports activated unless the port is first deleted (**delport X.X**). The opposite also applies; once a virtual port is configured, it cannot be used as a port until all virtual ports are deleted (**delport X.X**).

Figure 21-1 ATM Connections over a BPX Switch Network



Traffic Management Overview

The ATM Forum Traffic Management 4.0 Specification defines five basic traffic classes:

- Cbr (Constant Bit Rate)
- rt-Vbr (Real-Time Variable Bit Rate)
- nrt-Vbr (Non-Real Time Variable Bit Rate)
- Ubr (Unspecified Bit Rate)
- Abr (Available Bit Rate)

Table 21-1 summarizes the major attributes of each of the traffic management classes:

Table 21-1 Standard ATM Traffic Classes

Attribute	Cbr	rt-Vbr	nrt-Vbr	Ubr	Abr
Traffic Parameters					
PCR & CDVT	x	x	x	x	x
SCR & MBS		x	x		

Table 21-1 Standard ATM Traffic Classes (continued)

Attribute	Cbr	rt-Vbr	nrt-Vbr	Ubr	Abr
MCR					x
QoS Parameters					
Pk-to-Pk CDV	x	x			
Max CTD	x	x			
CLR	x	x	x		nw specific
Other Attributes					
Congestion Control Feedback					x

Traffic parameters are defined as:

- Peak Cell Rate (PCR) in cells per second
  The maximum rate at which a connection can transmit.
- Cell Delay Variation Tolerance (CDVT) in usec
  Establishes the time scale over which the PCR is policed. This is set to allow for jitter (CDV) that is introduced for example, by upstream nodes.
- Maximum Burst Size in cells (MBS)
  The maximum number of cells that may burst at the PCR but still be compliant. This is used to determine the Burst Tolerance (BT) which controls the time scale over which the Sustained Cell Rate (SCR) is policed.
- Minimum Cell Rate (MCR) in cells per second
  The minimum cell rated contracted for delivery by the network.

QoS (Quality of Service) parameters are defined as:

- Cell Delay Variation (CDV)
  A measure of the cell jitter introduced by network elements.
- Maximum Cell Transfer Delay (Max CTD)
  The maximum delay incurred by a cell (including propagation and buffering delays.)
- Cell Loss Ratio (CLR)
  The percentage of transmitted cells that are lost.

Congestion Control Feedback:

- With Abr, provides a means to control flow based on congestion measurement.

Standard Available Bit Rate

Standard Abr uses RM (Resource Management) cells to carry feedback information back to the connection's source from the connection's destination.

Abr sources periodically interleave RM cells into the data they are transmitting. These RM cells are called forward RM cells because they travel in the same direction as the data. At the destination these cells are turned around and sent back to the source as Backward RM cells.

The RM cells contain fields to increase or decrease the rate (the CI and NI fields) or set it at a particular value (the explicit rate ER field). The intervening switches may adjust these fields according to network conditions. When the source receives an RM cell it must adjust its rate in response to the setting of these fields.

VSVD Description

Abr sources and destinations are linked via bi-directional connections, and each connection termination point is both a source and a destination; a source for data that it is transmitting, and a destination for data that it is receiving. The forward direction is defined as from source to destination, and the backward direction is defined as from destination to source.

Figure 21-2 shows the data cell flow in the forward direction from a source to its destination along with its associated control loop. The control loop consists of two RM cell flows, one in the forward direction (from source to destination) and the other in the backward direction (from destination to source).

The data cell flow in the backward direction from destination to source is not shown, nor are the associated RM cell flows. However, these flows are just the opposite of that shown in the diagram for forward data cell flows.

A source generates forward RM cells which are turned around by the destination and returned to the source as backward RM-cells. These backward RM-cells may carry feedback information from the network elements and/or the destination back to the source.

The parameter Nrm is defined as the maximum number of cells a source may send for each forward RM cell, that is, one RM cell must be sent for every Nrm-1 data cells. Also, in the absence of Nrm-1 data cells, as an upper bound on the time between forward RM cells for an active source, an RM cell must be sent at least once every Trm msecs.

BXM Connections

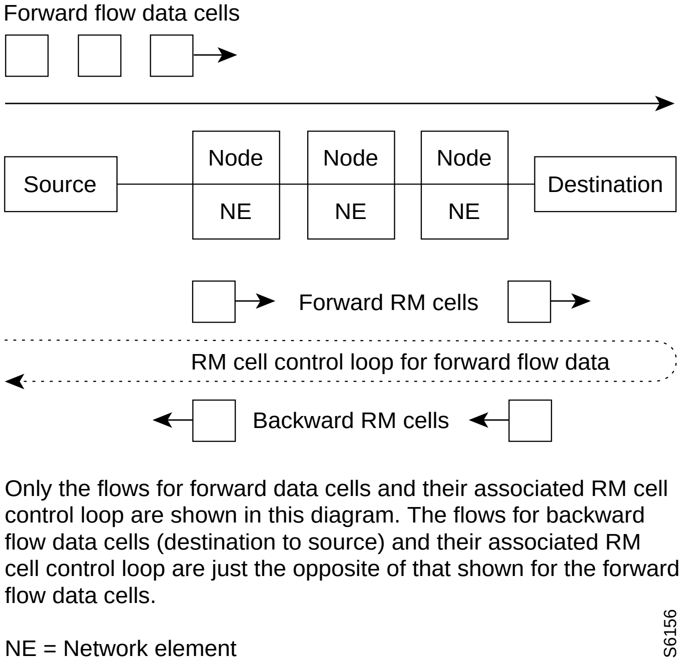
The BXM-T3/E3, BXM-155, and BXM-622 cards support ATM Traffic Management 4.0.

The BXM cards are designed to support all the following service classes:

- Constant Bit Rate (Cbr)
- real time Variable Bit Rate (rt-Vbr)
- non-real time Variable Bit Rate (nrt-Vbr)
- Available Bit Rate (Abr with VSVD
- Abr without VSVD, and Abr using ForeSight)
- Unspecified Bit Rate (Ubr)

Abr with VSVD supports explicit rate marking and Congestion Indication (CI) control.

Figure 21-2 Abr VSVD Flow Control Diagram


Forward flow data cells
Source
Node
NE
Node
NE
Node
NE
Destination
Forward RM cells
RM cell control loop for forward flow data
Backward RM cells
Only the flows for forward data cells and their associated RM cell control loop are shown in this diagram. The flows for backward flow data cells (destination to source) and their associated RM cell control loop are just the opposite of that shown for the forward flow data cells.
NE = Network element
S6156

ForeSight Congestion Control

The ForeSight feature is a proprietary dynamic closed-loop, rate-based, congestion management feature that yields bandwidth savings compared to non-ForeSight equipped trunks when transmitting bursty data across cell-based networks.

ForeSight may be used for congestion control across BPX and IGX switches for connections that have one or both end points terminating on BXM cards. The BXM cards also support the VSVD congestion control mechanism as specified in the ATM Traffic Management 4.0 standards.

ATM Connection Requirements

Two connection addressing modes are supported:

- You may enter a unique VPI/VCI address in which case the BPX switch functions as a virtual circuit switch.
- You may enter only a VPI address in which case all circuits are switched to the same destination port and the BPX switch functions as a virtual path switch in this case.

The full ATM address range for VPI and VCI is supported.Virtual Path Connections are identified by an * in the VCI field. Virtual Circuit Connections specify both the VPI and VCI fields.

The VPI and VCI fields have significance only to the local BPX switch, and are translated by tables in the BPX switch to route the connection. Connections are automatically routed by the Automatic Routing Management feature once the connection endpoints are specified.

You can add ATM connections by using either the Cisco WAN Manager Connection Manager or a node's command line interface (CLI). Typically, the Cisco WAN Manager Connection Manager is the preferred method because it has an easy to use GUI interface. The CLI may be the method of choice in some special cases or during initial node setup for local nodes.

Overview of Procedure to add ATM Connections

In general, to add ATM connections:

Step 1 Configure the access port and access service lines connecting to the customer premise equipment.

Step 2 Configure the trunks across the network appropriately for the type of connection.

Step 3 Use the **addcon** command to add a connection, first specifying the service type and then the appropriate parameters for the connection.

For example, when configuring a BXM for CPE connections:

Step 1 Configure the BXM for port mode,

Step 2 Up a line by using the **upln** command

Step 3 Configure the line by using the **cnfln** command.

Step 4 Configure the associated port by using the **cnfport** command

Step 5 Up the associated port by using the **upport** command.

Step 6 Then add the ATM connections by using the **addcon** command.

Connection Routing

ATM connections for a BXM card are identified by these numbers:

- slot number (in the BPX switch shelf where the BXM is located)
- port number (one of the ATM ports on the BXM)
- Virtual Path Identifier (VPI)
- Virtual Circuit Identifier (VCI) – (* for virtual path connections)

The slot and port are related to the BPX switch hardware.

Virtual path connections (VPCs) are identified by a "*" for the VCI field.

Virtual circuit connections (VCCs) are identified by both a VPI and VCI field.

Connections added to the network are automatically routed once the end points are specified. This Automatic Routing Management feature is standard with all BPX and IGX switches. The network automatically detects trunk failures and routes connections around the failures.

addcon Command Syntax

Enter the following parameters for the BXM **addcon** command. Depending upon the connection type, you are prompted for the appropriate parameters as shown:

```
addcon local_addr  node  remote_addr   traffic_type/class number....extended parameters

EXAMPLES

addcon 2.2.11.11 pubsbpx1 2.3.12.12 3

addcon 2.3.22.22 pubsbpx1 2.2.24.24 abrstd 50/50 100/100 50/50 25000/* e e e d 50/50 * 3
* 80/* 35/* 20/* 50/* * 100 128 16 32 0 *
```

Field	Value	Description
local/remote_addr	slot.port.vpi.vci	desired VCC or VPI connection identifier
node		slave end of connection
traffic_type/connection class		Type of traffic, chosen from service type (nrt/rt-Vbr, Cbr, Ubr, ABRSTD, ABRFST, ATFR, ATFST, ATFT, ATFTFST, ATFX, ATFXFST) or connection class. For example, for rt-Vbr, connection class 3 for a new node running Release 9.2.20. **Note** For a new node running 9.2.20 or later, the rt-Vbr connection class number is 3. An upgraded node retains 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 using the cnfcls/cnfatmcls command.
extended parameters		Additional traffic management and performance parameters associated with some of the ATM connection types, for example ABRSTD with VSVD enabled and default extended parameters disabled.

Note The range of VPIs and VCIs reserved for PVC traffic and SVC traffic is configurable using the **cnfport** command. While adding connections, the system checks the entered VPI/VPC against the range reserved for SVC traffic. If there is a conflict, the **addcon** command fails with the message “VPI/VCI on selected port is reserved at local/remote end”.

addcon Example

The following example shows the initial steps in adding a connection with the **addcon** command, and the **addcon** prompt requesting the user to enter the ATM type of service.

```
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:
```

Instead of entering a class of service, you 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. You can modify the class of service templates as required by using the **cnfcls/cnfatmcls** command and displaying them by 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 will not have the rt-Vbr connection class 3. However, you can configure the connection classes to any service and parameters you want by using the cnfcls/cnfatmcls command.

An example of a **cnfcls/cnfatmcls** command and response is shown in the following example:

```
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):
```

ATM Connection Flow

ATM Connection Flow through the BPX

The BPX supports the standard ATM service types, Cbr, rt-Vbr, nrt-Vbr, Abr, and Ubr. When adding a connection by using the **addcon** command, you select these service types by entering one of the CLI service type entries shown in Table 21-2 when prompted:

Table 21-2 Standard ATM Type and addcon

CLI Service Type Entries	Connection Description
Cbr	cell bit rate
rt-Vbr	real time Vbr
nrt-Vbr	non real time Vbr
Ubr	unspecified bit rate
ABRSTD	Abr per forum standard, with option to enable VSVD congestion control.
ABRFST	Abr with Cisco ForeSight congestion control.

The BPX also supports ATM to Frame Relay Network Interworking and Service Interworking connections. When adding a connection by using the **addcon** command, you select these service types by entering one of the CLI service type entries shown in Table 21-3 when prompted:

Table 21-3 ATM to Frame Relay Network and Service Interworking

CLI Service Type Entries for addcon Command	Connection Description
ATFR	ATM to Frame Relay Network Interworking
ATFST	Same as ATFR with ForeSight
ATFT	ATM to Frame Relay Transparent Service Interworking
ATFTFST	Same as ATFT with ForeSight
ATFX	ATM to Frame Relay Translational Service Interworking
ATFXFST	Same as ATFX with ForeSight

Advanced CoS Management

Advanced CoS management provides per-VC queueing and per-VC scheduling. CoS management provides fairness between connections and firewalls between connections. Firewalls prevent a single non-compliant connection from affecting the QoS of compliant connections. The non-compliant connection simply overflows its own buffer.

The cells received by a port are not automatically transmitted by that port out to the network trunks at the port access rate. Each VC is assigned its own ingress queue that buffers the connection at the entry to the network. With Abr with VSVD or with Optimized Bandwidth Management (ForeSight), the service rate can be adjusted up and down depending on network congestion.

Network queues buffer the data at the trunk interfaces throughout the network according to the connection’s class of service. Service Classes are defined by standards-based QoS. Service Classes can consist of the five service classes defined in the ATM standards as well as multiple sub-classes to each of these classes. Service Classes can range from constant bit rate services with minimal cell delay variation to variable bit rates with less stringent cell delay.

When cells are received from the network for transmission out a port, egress queues at that port provide additional buffering based on the Service Class of the connection.

CoS Management provides an effective means of managing the quality of service defined for various types of traffic. It permits network operators to segregate traffic to provide more control over the way that network capacity is divided among users. This is especially important when there are multiple user services on one network.

Rather than limiting the user to the five broad classes of service defined by the ATM standards committees, CoS management can provide up to 16 classes of service (service subclasses) that can be further defined by the user and assigned to connections. Some of the CoS parameters that may be assigned include:

- Minimum bandwidth guarantee per subclass to assure that one type of traffic will not be preempted by another
- Maximum bandwidth ceiling to limit the percentage of the total network bandwidth that any one class can utilize
- Queue depths to limit the delay
- Discard threshold per subclass

These class of service parameters are based on the standards-based Quality of Service parameters and are software programmable by the user. The BPX switch provides separate queues for each traffic class.

Connection Flow Example

The example shown in Figure 21-3 shows the general ATM connection flow through BXM cards in BPX switches. The **cnfport, cnfportq, cnfln, cnftrk, and cnftrkparm** commands are used to configure resources affecting the traffic flow of a connection. Examples are described in *Traffic Shaping for Cbr, rt-Vbr, nrt-Vbr, and Ubr*, page 21-13.

Ingress from CPE 1 to BXM 3

ATM cells from CPE 1 that are applied to BXM 3, Figure 21-3, are processed at the physical level, policed per individual VC based on ATM header payload type, and routed to the applicable one of 15 per card slot servers, each of which contains 16 CoS service queues, including ATM service types Cbr, rt-Vbr, nrt-Vbr, Abr, and Ubr.

ATM cells undergoing traffic shaping, for example, Abr cells are applied to traffic shaping queues before going to one of the 15 per card slot servers. ATM cells applied to the traffic shaping queues receive additional processing, including congestion control by means of VSVD or ForeSight and virtual connection queuing.

Cells are served out from the slot servers via the BPX backplane to the BCC crosspoint switch. The cells are served out on a fair basis with priority based on class of service, time in queue, bandwidth requirements, and so on.

Note For a description of traffic shaping on Cbr, rt-Vbr, nrt-Vbr, and Ubr connections, refer to the section later in this chapter, *Traffic Shaping for Cbr, rt-Vbr, nrt-Vbr, and Ubr,* page 21-13.

Egress to Network via BXM 10

In this example, ATM cells destined for BPX 2 are applied via the BCC crosspoint switch and BPX backplane to BXM 10 and out to the network. The cells are served out to the network via the appropriate trunk Qbin , Cbr, rt-Vbr, nrt-Vbr, Abr, or Ubr.

Ingress from Network via BXM 5

ATM cells from the network that are applied to BXM 5 in BPX 2 are processed at the physical level and routed to one of 15 per card slot servers, each of which contains 16 CoS service queues, including ATM service types Cbr, rt-Vbr, nrt-Vbr, Abr, and Ubr.

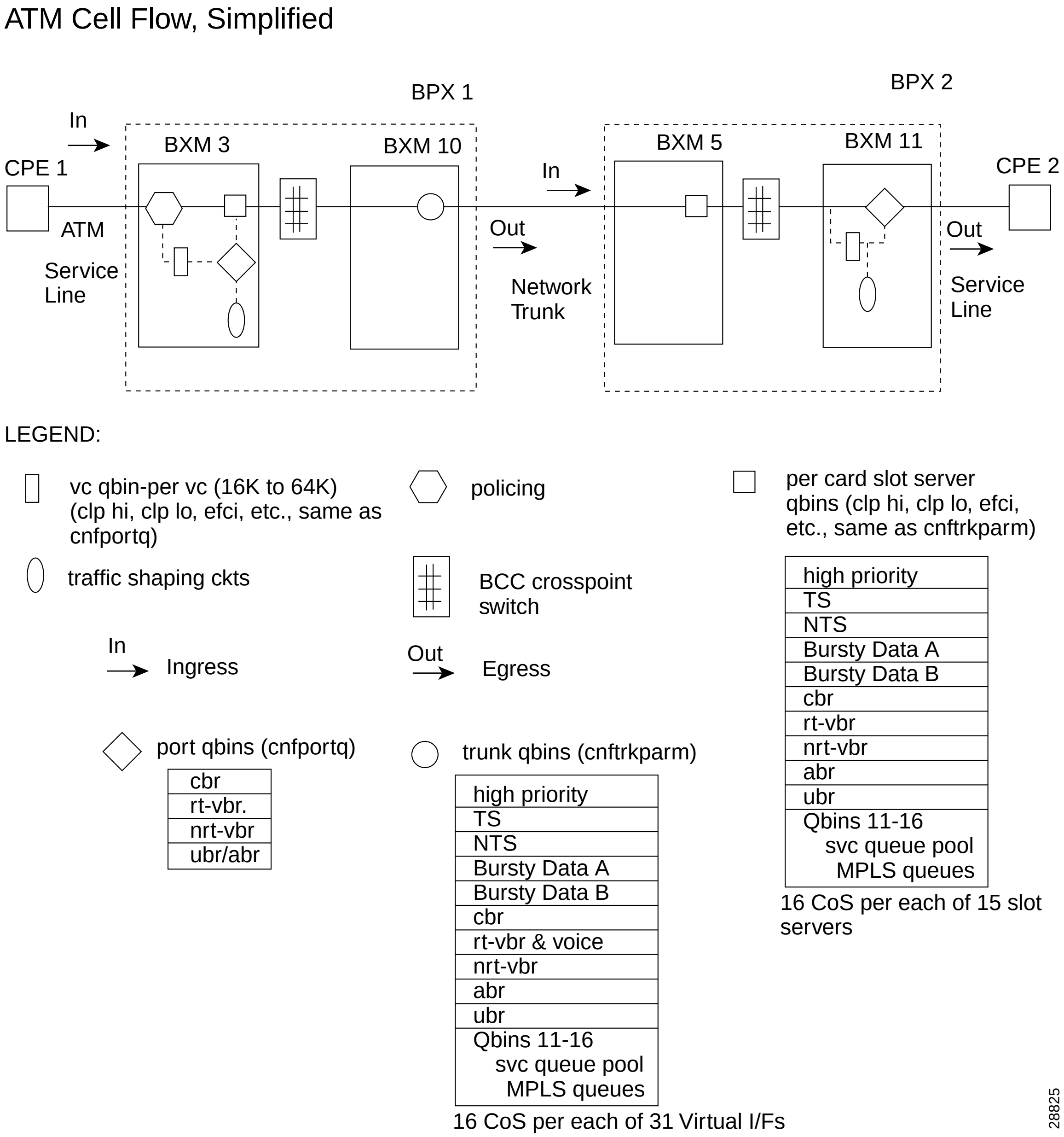
Cells are served out from the slot servers via the BPX backplane to the BCC crosspoint switch. The cells are served out on a fair basis with priority based on class of service, time in queue, bandwidth requirements, etc.

Egress from BXM 11 to CPE 2

In this example, ATM cells destined for CPE 2 are applied via the BCC crosspoint switch and BPX backplane to BXM 11 and out to CPE 2. The cells are served out to CPE 2 via the appropriate port Qbin, Cbr, rt-Vbr, nrt-Vbr, or Abr/Ubr.

ATM cells undergoing traffic shaping, for example Abr cells are applied to traffic shaping queues before going to one of the 15 per card slot servers. ATM cells applied to the traffic shaping queues receive additional processing, including congestion control by means of VSVD or ForeSight and virtual connection queuing.

Figure 21-3 ATM Connection Flow via BPX Switches



cbr
rt-vbr.
nrt-vbr
ubr/abr

high priority
TS
NTS
Bursty Data A
Bursty Data B
cbr
rt-vbr & voice
nrt-vbr
abr
ubr
Qbins 11-16 svc queue pool MPLS queues

high priority
TS
NTS
Bursty Data A
Bursty Data B
cbr
rt-vbr
nrt-vbr
abr
ubr
Qbins 11-16 svc queue pool MPLS queues

Traffic Shaping for Cbr, rt-Vbr, nrt-Vbr, and Ubr

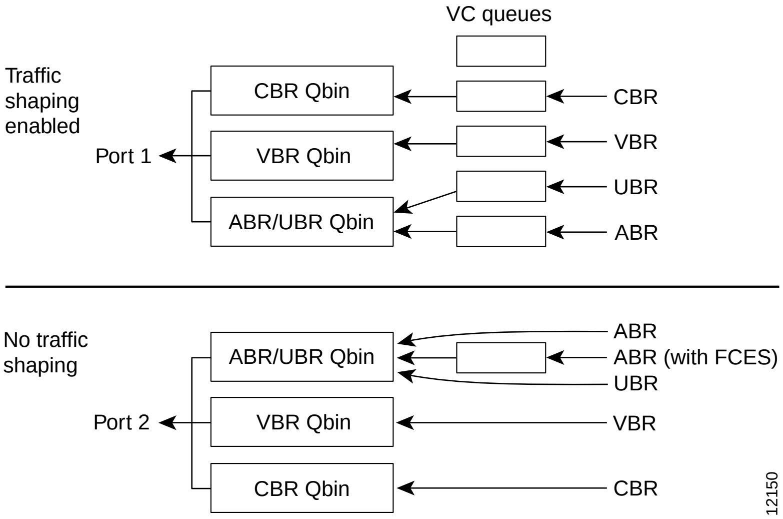
With the introduction of traffic shaping for Cbr, Vbr, and Ubr, you have the option to provide traffic shaping for these connections types on the BXM. Previously, only Abr utilized traffic shaping. Traffic shaping involves passing Cbr, Vbr, or Ubr traffic streams through VC queues for scheduled rate shaping.

Traffic shaping is performed on a per port basis. When traffic shaping is enabled, all traffic exiting the port (out to the network) is subject to VC scheduling based on the parameters you configure for the connection.

Figure 21-4 shows an example of traffic shaping. In this example, port 1 is configured to perform traffic shaping.

Note that all the ATM cells regardless of class of service pass through the VC queues before leaving the card when traffic shaping is enabled. In the example, port 2 is not configured for traffic shaping, and only the Abr traffic with FCES (flow control external segment) passes through the VC queues.

Figure 21-4 Traffic Shaping Example



Traffic Shaping Rates

Traffic shaping rates are listed in Table 21-4.

Table 21-4 Traffic Shaping Rates

Service Type	MCR	PCR
Cbr	PCR	PCR
rt-Vbr and nrt-Vbr	SCR * %Util	PCR
Ubr	0	PCR
Abr	MCR * %Util	PCR

Configuration

Traffic shaping is disabled by default.

Use the **cnfport** and **cnfln** command to enable and disable the function on a per port basis.

Use the **cnftrk** command to enable traffic shaping on trunks.

No connections should be enabled on the port prior to changing the port traffic shaping parameter. If there are existing connections when the port 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.

See the following examples of the **cnfln**, **cnfport**, and **cnftrk** commands:

Example of **cnfln**:

```
pubsbpx1       TN    silves    BPX 8620  9.3 Aug. 1 2000 14:41 PDT

LN   2.2 Config    OC3     [353208cps]     BXM slot:     2
Loop clock:            No                  Idle code:             7F hex

Line framing:          --
     coding:           --
     CRC:              --
     recv impedance:   --
     E1 signalling:    --
     encoding:         --                       cable type:       --
     T1 signalling:    --                       length:           --
                                           HCS Masking:           Yes
                                           Payload Scramble:      Yes
     56KBS Bit Pos:    --                  Frame Scramble:        Yes
     pct fast modem:   --                  Cell Framing:          STS-3C
                                           VC Shaping:            No

Last Command: cnfln 2.2

Next Command:
```

Example of **cnfport**:

```
pubsbpx1       TN    silves       BPX 8620  9.3 Aug. 1 2000 15:12 PDT

Port:       2.2     [ACTIVE  ]
Interface:          LM-BXM                     CAC Override:     Enabled
Type:               UNI                        %Util Use:        Disabled
Shift:              NO SHIFT (Virtual Trunk Operation)
SIG Queue Depth:    640                        Port Load:        28 %

Protocol:           NONE                       Protocol by Card: No





Last Command: cnfport 2.2


Next Command:
```

Example of **cnftrk**:

```
pubsbpx1       TN    silves       BPX 8620  9.3 Aug. 1 2000 14:43 PDT

TRK  2.4 Config    OC3     [353207cps]     BXM slot:     2
Transmit Rate:         353208              Line framing:          STS-3C
Protocol By The Card:  No                       coding:           --
VC Shaping:            No                       CRC:              --
Hdr Type NNI:          Yes                      recv impedance:   --
Statistical Reserve:   1000    cps              cable type:       --
Idle code:             7F hex                         length:     --
Connection Channels:   256                 Pass sync:             No
Traffic:V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR, T-VBR  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                  Virtual Trunk Type:    --
Link type:             Terrestrial         Virtual Trunk VPI:     --
Routing Cost:          10                  Deroute delay time:    0 seconds

This Command: cnftrk 2.4


Transmit Rate [ 1-353208 ]:
```

rt-Vbr and nrt-Vbr Connections

Vbr (variable bit rate) connections may be classified as either:

- **real time (rt-Vbr)**
  This 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).
- **non-real time (nrt-Vbr)**
  This 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.

When configuring a rt-Vbr connection, the trunk cell routing restriction prompt does not display, because rt-Vbr connection routing is automatically restricted to ATM trunks.

With Release 9.2.20 and later, you specify rt-Vbr and nrt-Vbr connections separately when adding a connection by using the **addcon** command. To do this, enter either **rt-vbr** or **nrt-vbr** to select the rt-Vbr or nrt-Vbr connection class, respectively. Each connection is assigned the applicable associated default parameters for its type of service.

For rt-Vbr an additional queue, referred to as the rt-Vbr queue, is used at a BXM port. At BXM or BNI trunks, voice and rt-Vbr traffic share a queue, referred to as the rt-Vbr queue.

The rt-Vbr and nrt-Vbr service queues are configured differently from each other at both port ingress and port egress queues. The rt-Vbr typically uses smaller queues for low delay, whereas the nrt-Vbr queues are typically larger in size for more efficient bandwidth sharing with other non-real time service types.

The rt-Vbr connections are configured per class 3 service parameters. The nrt-Vbr connections are configured per class 2 service parameters.

You can configure the connection classes to whatever service and parameters you want by:

- Using the **cnfcls** and **cnfatmcls** commands.
- Or, you can enter the parameters individually for each connection by specifying ‘yes’ to the extended parameters prompt of the **addcon** command.

For a new node running software release 9.2.20 or later, the rt-Vbr connection class number is 3. However, an upgraded node will retain existing connection classes. Therefore, it won’t have the rt-Vbr connection class 3.

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.

Example of **cnfcls** 3, for rt-Vbr:

```
pubsbpx1       TN    silves:1        BPX 8620  9.2.20 July 16 2000 10:42 PDT

                        ATM Connection Classes
Class:  3                                                         Type: rt-VBR
   PCR(0+1)     % Util       CDVT(0+1)       AAL5 FBTC        SCR
 4000/4000     100/100      10000/10000          n        4000/4000

    MBS         Policing
 1000/1000           3

       Description: "Default rt-VBR 4000 "







This Command: cnfcls atm 3


Enter class type (rt-VBR, nrt-VBR, CBR, UBR, ABRSTD, ABRFST, ATFR, ATFST, ATFT,
ATFTFST, ATFX, ATFXFST):
```

Example of cnfcls2, for nrt-Vbr

```
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):
```

Connection Criteria

- Default utilization for voice traffic is 100 percent.
- For rt-Vbr connections, all nodes must be running at least Release 9.2.20. The user interface will block the addition of rt-Vbr connections in a network running pre-9.2.20 SWSW.
- BXM 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
- On the IGX switch, only UXM trunks support rt-Vbr queues.
- 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 be routed over only ATM trunks; rt-Vbr traffic should not be routed over FastPacket trunks.)
- With release 9.3, rt-vbr is supported on 2- and 3-segment connections, but only on IGX feeders and UXM endpoints. For example: 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).

Configuring Connection Policing

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:

- PCR
- %util

- CDVT
- FBTC flag
- SCR
- MBS
- Policing Type

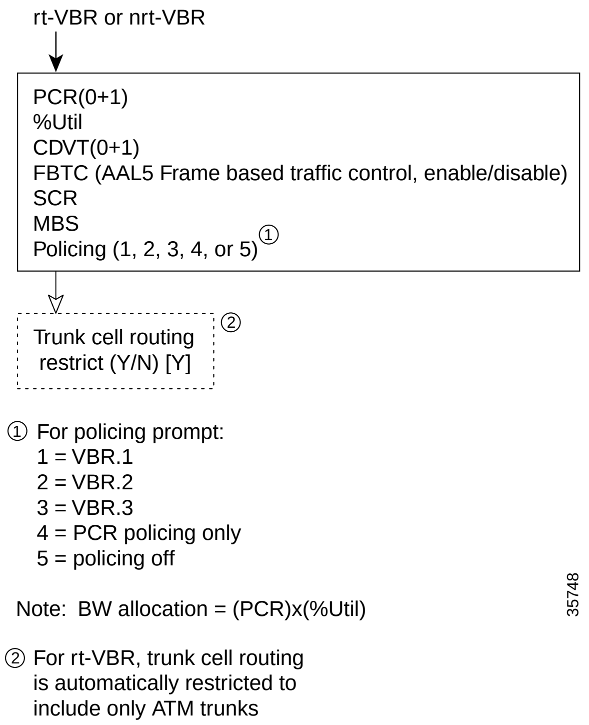
There is no change in CDVT usage and the previous policing system.

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.

To modify the values of a connection class, use the commands **cnfcls** and **cnfatmcl**.

To display these values, use the commands **dspcls** and **dspatmcls**.

Figure 21-5 rt-Vbr and nrt-Vbr Connection Prompt Sequence


rt-VBR or nrt-VBR
PCR(0+1)
%Util
CDVT(0+1)
FBTC (AAL5 Frame based traffic control, enable/disable)
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
Trunk cell routing restrict (Y/N) [Y] ②
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
Note: BW allocation = (PCR)x(%Util)
② For rt-VBR, trunk cell routing is automatically restricted to include only ATM trunks
35748

Configuring Resources

Qbin values on both ports and trunks used by rt-Vbr connections and nrt-Vbr connections can be configured separately.

Trunk Queues for rt-Vbr and nrt-Vbr

A rt-Vbr connection uses the rt-Vbr queue on a trunk. It shares this queue with voice traffic. The rt-Vbr and voice traffic shares the default or user configured parameters for the rt-Vbr queue. These parameters are queue depth, queue CLP high and CLP low thresholds, EFCI threshold, and queue priority.

A nrt-Vbr connection uses the nrt-Vbr queue on a trunk. The configurable parameters are queue depth, queue CLP high and CLP low thresholds, EFCI threshold, and queue priority.

You can configure the Qbin values separately for rt-Vbr and nrt-Vbr classes on trunks by using the **cnftrkparm** command.

- For rt-Vbr, the **cnftrkparm** command configures Q-depth rt-Vbr and Max Age rt-Vbr.
- For nrt-Vbr, the **cnftrkparm** command configures Q-depth nrt-Vbr, Low CLP nrt-Vbr, and High CLP nrt-Vbr.

This example shows the **cnftrkparm** screen and the parameters that can be configured for the various service type queues:

```
pubsbpx1       TN    silves:1        BPX 8620  9.2.2G    July 16 1999 10:50 PDT




TRK 2.4 Parameters
 1 Q Depth - rt-VBR    [  885] (Dec)    15 Q Depth   - CBR     [  600] (Dec)
 2 Q Depth - Non-TS    [ 1324] (Dec)    16 Q Depth   - nrt-VBR [ 5000] (Dec)
 3 Q Depth - TS        [ 1000] (Dec)    17 Q Depth   - ABR     [20000] (Dec)
 4 Q Depth - BData A   [10000] (Dec)    18 Low  CLP  - CBR     [  60] (%)
 5 Q Depth - BData B   [10000] (Dec)    19 High CLP  - CBR     [  80] (%)
 6 Q Depth - High Pri  [ 1000] (Dec)    20 Low  CLP  - nrt-VBR [  60] (%)
 7 Max Age - rt-VBR    [   20] (Dec)    21 High CLP  - nrt-VBR [  80] (%)
 8 Red Alm - I/O (Dec) [  2500 /  10000]22 Low CLP/EPD-ABR     [  60] (%)
 9 Yel Alm - I/O (Dec) [  2500 /  10000]23 High CLP  - ABR     [  80] (%)
10 Low  CLP - BData A  [ 100] (%)       24 EFCN      - ABR     [  20] (%)
11 High CLP - BData A  [ 100] (%)       25 SVC Queue Pool Size [    0] (Dec)
12 Low  CLP - BData B  [  25] (%)
13 High CLP - BData B  [  75] (%)
14 EFCN     - BData B  [  30] (Dec)

This Command: cnftrkparm 2.4
```

Port Queues for rt-Vbr and nrt-Vbr

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 by using the **cnfportq** command.

The following example shows he configuration parameters available for a port queue.

Port Queue Parameters, **cnfportq**

```
pubsbpx1       TN    silves:1        BPX 8620  9.3 July 16 2000 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
```

Related Switch Software Commands

These commands are related to the process of adding and monitoring ATM connections:

- addcon
- dspload
- cnfcls
- cnfatmcls
- cnfcls
- cnfcon
- cnftrkparms
- dsptrkcnf
- dspatmcls
- dspcls
- dsconcls
- dspconcnf
- dspcon
- dspcons
- dlcon
- dcct
- dvcparms
- dvc
- cnfpre
- dsptrkcnf
- dspload
- chklm
- dsplm
- updates
- upport
- dspportq
- cnfportq
- dspblkfuncs
- dspchstats
- dspportstats
- dsptrkstats
- dsptrkerrs.

For additional information on CLI command usage, refer to the *Cisco WAN Switching Command Reference* and *Cisco WAN Switching SuperUser Command Reference*.

ATM Connection Configuration

These figures and tables describe the parameters used to configure ATM connections:

- Table 21-5, Traffic Policing Definitions
  - This table describes the policing options that may be selected for ATM connection types: Cbr, Ubr, rt-Vbr. and nrt-Vbr. The policing options for Abr are the same as for Vbr.
- Table 21-6, Connection Parameters with Default Settings and Ranges
  - This table specifies the ATM connection parameter ranges and defaults. Not all the parameters are used for every connection type. When adding connections, you are prompted for the applicable parameters, as specified in the prompt sequence diagrams included in Figure 21-6 through Figure 21-11.
- Table 21-7, Connection Parameter Descriptions
  - This table defines the connection parameters listed in Table 21-6.

The following figures list the connection parameters in the same sequence as they are entered when a connection is added:

- Figure 21-6, Cbr Connection Prompt Sequence
- Figure 21-7, rt-Vbr and nrt-Vbr Connection Prompt Sequence
- Figure 21-8, Abr Standard Connection Prompt Sequence

This figure shows the VSVD network segment and external segment options available when Abr Standard or Abr ForeSight is selected. ForeSight congestion control is useful when both ends of a connection do not terminate on BXM cards. At present, FCES (Flow Control External Segment) as shown in Figure 21-9 is not available for Abr with ForeSight.

- Figure 21-9, Meaning of VSVD and Flow Connection External Segments

These figures list the connection parameters in the same sequence as you would enter them when adding a connection:

- Figure 21-10, Abr ForeSight Connection Prompt Sequence
- Figure 21-11, Ubr Connection Prompt Sequence
- Figure 21-14, ATFR Connection Prompt Sequence
- Figure 21-15, ATFST Connection Prompt Sequence
- Figure 21-16, ATFT Connection Prompt Sequence
- Figure 21-17, ATFTFST Connection Prompt Sequence
- Figure 21-18, ATFX Connection Prompt Sequence
- Figure 21-19, ATFXFST Connection Prompt Sequence

Note With DAX connections, the trunk cell routing restriction prompt is not displayed since there is no trunking involved.

Table 21-5 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 21-6 Connection Parameters with Default Settings and Ranges

Parameter with [Default Setting]	BXM T3/E3, OC-3 & OC-12 Range
PCR(0+1)[50/50]	50–T3/E3 cells/sec 50–OC3 50–OC12
%Util [100/100] for Ubr [1/1]	0–100%
MCR[50/50]	cells per sec 6–T3/E3OC3/0C12

FBTC (AAL5 Frame Base Traffic Control):
for rt/nrt-Vbr [disable]
for Abr/Ubr [enable]
for Path connection [disable]
	enable/disable
	With the BXM, FBTC means packet discard on queueing only.

CDVT(0+1):
for Cbr [10000/10000],
others [250000/250000]
	0–5,000,000 usec

VSVD[disable]	enable/disable
FCES (Flow Control External Segment) [disable]	enable/disable
Default Extended Parameters[enable]	enable/disable
CLP Setting[enable]	enable/disable
SCR [50/50]	cells per sec 50–T3/E3OC3/OC12
MBS [1000/1000]	1–5,000,000 cells
Policing[3] For Cbr: [4]	1–Vbr.1 2–Vbr.2 3–Vbr.3 4–PCR policing only 5–off
ICR: max[MCR, PCR/10]	MCR–PCR cells per sec
ADTF[1000]	62–8000 msec
Trm[100]	ABRSTD: 1–100 msec ABRFST: 3–255 msec
VC QDepth [16000/16000] For ATFR/ATFST [1366/1366]	0–61440 cells
CLP Hi [80/80]	1–100%

Table 21-6 Connection Parameters with Default Settings and Ranges (continued)

Parameter with [Default Setting]	BXM T3/E3, OC-3 & OC-12 Range
CLP Lo/EPD [35/35]	1–100%
EFCI [30/30] For ATFR/ATFST [100/100]	1–100%
RIF: For ForeSight: max[PCR/128, 10] For Abr STD[128]	If ForeSight, then in absolute (0–PCR) If Abr then 2^n (1–32768)
RDF: For ForeSight [93] For Abr STD [16]	If ForeSight, then % (0%–100%) If Abr then 2^n (1–32768)
Nrm[32], BXM only	2–256 cells
FRTT[0], BXM only	0–16700 msec
TBE[1,048,320], BXM only	0–1,048,320 cells (different max range from TM spec. but limited by firmware for CRM (4095 only) where CRM=TBE/Nrm)
IBS[1/1]	0–24000 cells
Trunk cell routing restrict (Y/N) [Y]	Y/N

Table 21-7 Connection Parameter Descriptions

Parameter	Description
PCR	Peak cell rate: The cell rate which the source may never exceed
%Util	% Utilization; bandwidth allocation for: rt/nrt-Vbr, Cbr, Ubr it’s PCR*%Util, for Abr it’s MCR*%Util
MCR	Minimum Cell Rate: A minimum cell rate committed for delivery by network
CDVT	Cell Delay Variation Tolerance: Controls time scale over which the PCR is policed

Table 21-7 Connection Parameter Descriptions (continued)

Parameter	Description
FBTC (AAL5 Frame Basic 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 BXM, FBTC means packet discard on queueing only.
VSVD	Virtual Source Virtual Destination: (see Meaning of VSVD and Flow Control External Segments, Figure 21-9)
FCES (Flow Control External Segments)	(see Meaning of VSVD and Flow Control External Segments, Figure 21-9)
SCR	Sustainable Cell Rate: Long term limit on the rate a connection can sustain
MBS	Maximum Burst Size: Maximum number of cells which may burst at the PCR but still be compliant. Used to determine the Burst Tolerance (BT) which controls the time scale over which the SCR is policed
Policing	(see definitions of Traffic Policing, Table 21-5)
VC QDepth	VC Queue Depth
CLP Hi	Cell Loss Priority Hi threshold (% of VC QMax)
CLP Lo/EPD	Cell Loss Priority Low threshold (% of VC QMax)/Early Packet Discard. If AAL5 FBTC = yes, then for the BXM card this is the EPD threshold setting.
EFCI	Explicit Forward Congestion Indication threshold (% of VC QMax)
ICR	Initial Cell Rate: The rate at which a source should send initially and after an idle period
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
Trm (ATM Forum TM 4.0 term)	An upper bound on the time between forward RM-cells for an active source, that is, RM cell must be sent at least every Trm msec
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
RDF (ATM Forum TM 4.0 term)	Rate Decrease Factor: Controls the amount by which the cell transmission rate may decrease upon receipt of an RM cell
Nrm (ATM Forum TM 4.0 term), BXM only.	Nrm Maximum number of cells a source may send for each forward RM cell, that is, an RM cell must be sent for every Nrm-1 data cells

Table 21-7 Connection Parameter Descriptions (continued)

Parameter	Description
FRTT (ATM Forum TM 4.0 term), BXM only.	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), BXM only.	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.
IBS	Initial Burst Size
Trunk cell routing restriction (Y/N) [Y]	The default (Y) restricts ATM connection routes to include only ATM trunks. Selecting (N) allows the network to route these connections over non-ATM trunks (such as Fastpacket trunks).

Adjust Minimum SCR and PCR

Prior to Release 9.3.0, the minimum Sustainable Cell Rate (SCR) and Peak Cell Rate (PCR) of a connection supported by the BXM and UXM cards, including enhanced modes, was 50 cells per second (cps). These values were set to maintain a policing accuracy with 1% when policing is performed on a BXM or UXM card. Because of this limitation, it was impossible to offer and differentiate connection services on a UXM or BXM at speeds less than 19.2 Kbps.

In Release 9.3.0, the switch software supports connections with policing enabled and with SCR and PCR values as low as 12 cps on the BPX with certain card limitations.

Use the **dspcd** command to determine if this feature is supported on a given slot.

Use the **addcon** command to set the minimum SCR and PCR values. If these values are less than the minimum values supported on a given card, the command line interface will not allow you to set them until you have disabled policing. (A prompt will let you know about this limitation.)

Please refer to Table 21-1 for a list of cards that are supported by this feature and their performance specifications.

Table 21-8 Supported Cards and Performance Specifications

Card Name	Card Types	Minimum SCR and PCR, UPC/NPC Values
IGX-UXM	T1/E1	6 cps
IGX-UXM	IMA	6 cps
IGX-IUX	T3/E3	12 cps
IGX-UXM	OC3/STM-1	50 cps
BPX-BXM	T3/E3	12 cps
BPX-BXM	OC3/STM-1	50 cps
BPX-BXM	OC12/STM-4	50 cps
Note: The policing accuracy is always within 1%. The maximum SCR and PCR policing values are the same as the line rate.		

Constant Bit Rate Connections

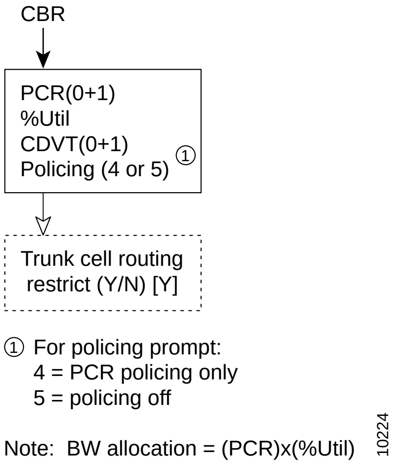
The **Cbr** (constant bit rate) category is a fixed bandwidth class. Cbr traffic is more time dependent, less tolerant of delay, and generally more deterministic in bandwidth requirements.

Cbr is used by connections that require a specific amount of bandwidth to be available continuously throughout the duration of a connection. Voice, circuit emulation, and high-resolution video are typical examples of traffic utilizing this type of connection.

A Cbr connection is allowed to transmit cells at the peak rate, below the peak rate, or not at all. Cbr is characterized by peak cell rate (PCR).

The parameters for a Cbr connection are shown in Figure 21-6 in the sequence in which they occur during the execution of the **addcon** command. The Cbr policing definitions are summarized in Table 21-8.

Figure 21-6 Cbr Connection Prompt Sequence



① For policing prompt:
4 = PCR policing only
5 = policing off

Note: BW allocation = (PCR)x(%Util)

Table 21-9 Cbr 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

Variable Bit Rate Connections

Vbr (variable bit rate) connections may be classified as either:

- **Real-Time Variable Bit Rate (rt-Vbr)**
  This category is used for connections that transmit at a rate varying with time and can be described as bursty, often requiring large amounts of bandwidth when active. It is intended for applications that require tightly constrained delay and delay variation such as compressed voice video conferencing.

  For example, video conferencing 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).
- **Non-Real Time Variable Bit Rate (nrt-Vbr)**
  This category is used for connections that are bursty but 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.

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 occur, as rt-Vbr connection routing is automatically restricted to ATM trunks.

Connection Criteria for real-time Vbr and non-real-time Vbr Connections

- Default utilization for voice traffic is 100 percent.
- 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 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
- 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 21-7 in the sequence in which they occur during the execution of the **addcon** command. The Vbr policing definitions are summarized in Table 21-9.

Figure 21-7 rt-Vbr and nrt-Vbr Connection Prompt Sequence

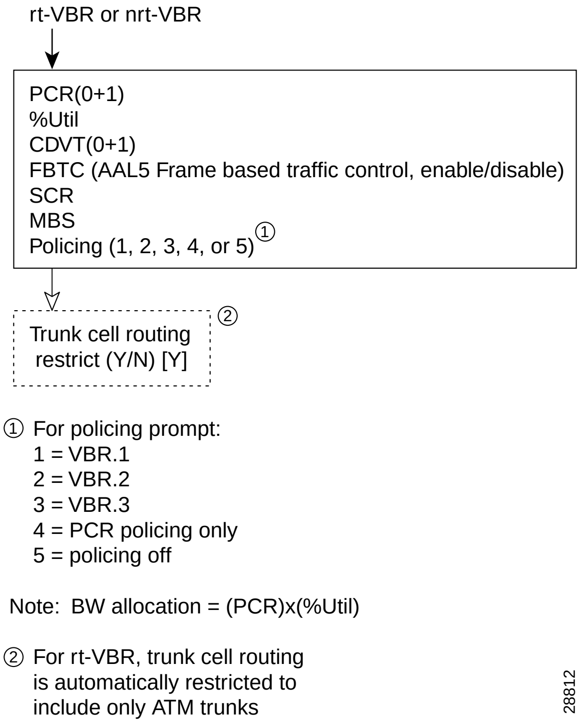

rt-VBR or nrt-VBR
PCR(0+1)
%Util
CDVT(0+1)
FBTC (AAL5 Frame based traffic control, enable/disable)
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
Trunk cell routing restrict (Y/N) [Y] ②
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
Note: BW allocation = (PCR)x(%Util)
② For rt-VBR, trunk cell routing is automatically restricted to include only ATM trunks
28812

Table 21-10 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

Available Bit Rate 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.

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 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 cards
  - Feature must be ordered

Policing for Abr connections is the same as for Vbr connections which are summarized in Table 21-9.

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 in Figure 21-8 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 21-9.

Available Bit Rate Standard Connections

The Available Bit Rate Standard (ABRSTD) connection uses VSVD congestion control.

The parameters for an ABRSTD connection are shown in Figure 21-10 in the sequence in which they occur during the execution of the **addcon** command

Figure 21-8 Abr Standard Connection Prompt Sequence

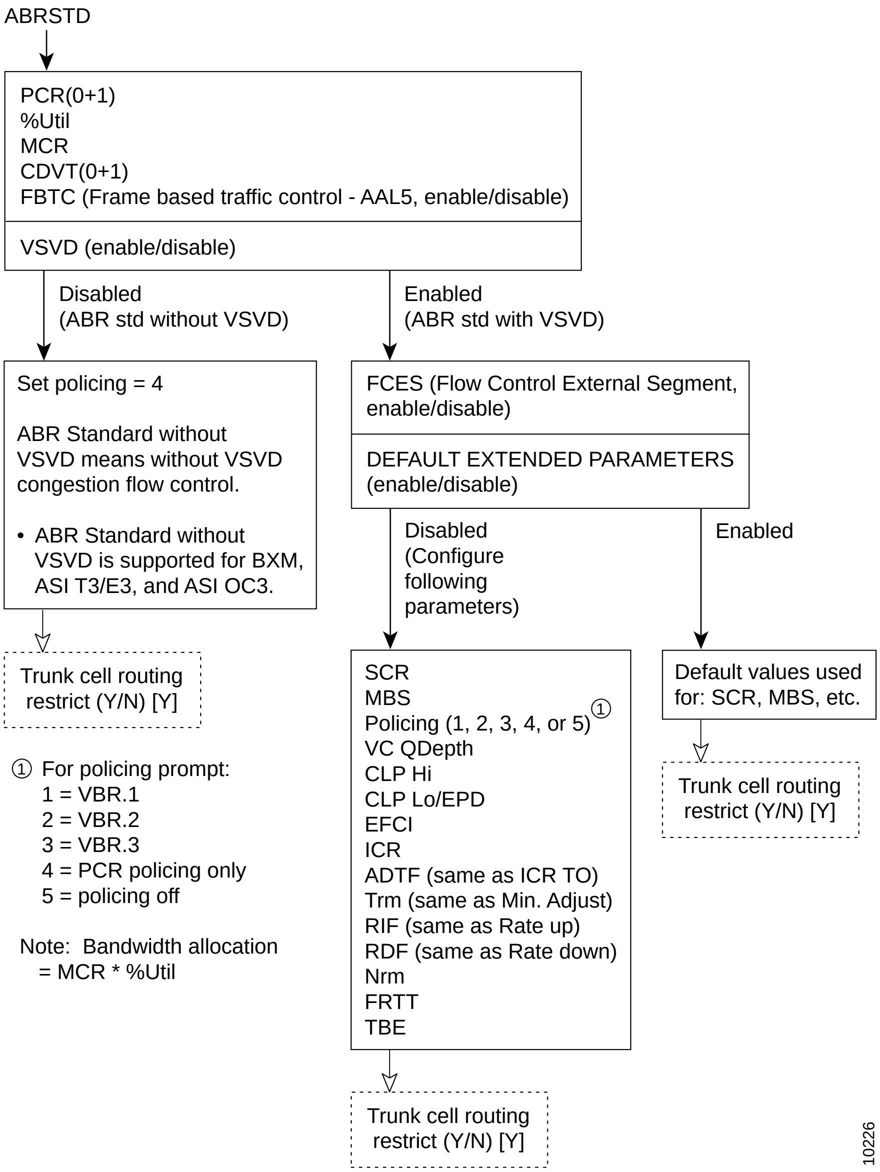
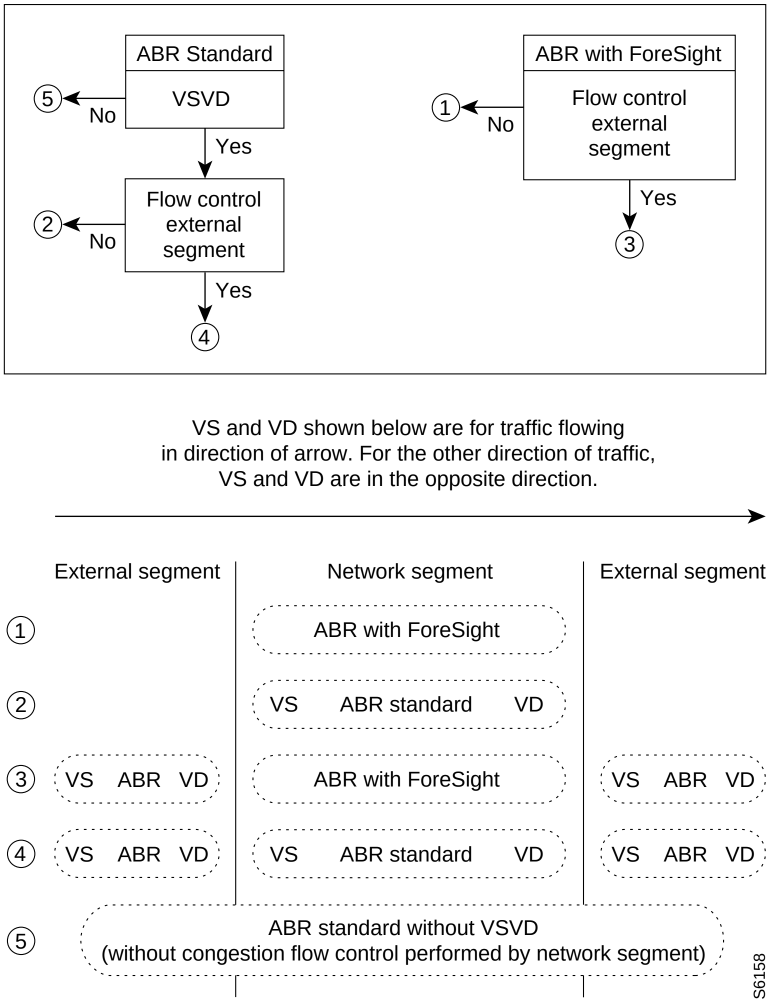

ABRSTD
PCR(0+1)
%Util
MCR
CDVT(0+1)
FBTC (Frame based traffic control - AAL5, enable/disable)
VSVD (enable/disable)
Disabled
(ABR std without VSVD)
Enabled
(ABR std with VSVD)
Set policing = 4
ABR Standard without VSVD means without VSVD congestion flow control.
• ABR Standard without VSVD is supported for BXM, ASI T3/E3, and ASI OC3.
FCES (Flow Control External Segment, enable/disable)
DEFAULT EXTENDED PARAMETERS (enable/disable)
Disabled (Configure following parameters)
Enabled
Trunk cell routing restrict (Y/N) [Y]
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as Min. Adjust)
RIF (same as Rate up)
RDF (same as Rate down)
Nrm
FRTT
TBE
Default values used for: SCR, MBS, etc.
Trunk cell routing restrict (Y/N) [Y]
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
Note: Bandwidth allocation = MCR * %Util
Trunk cell routing restrict (Y/N) [Y]
10226

Figure 21-9 Meaning of VSVD and Flow Control External Segments

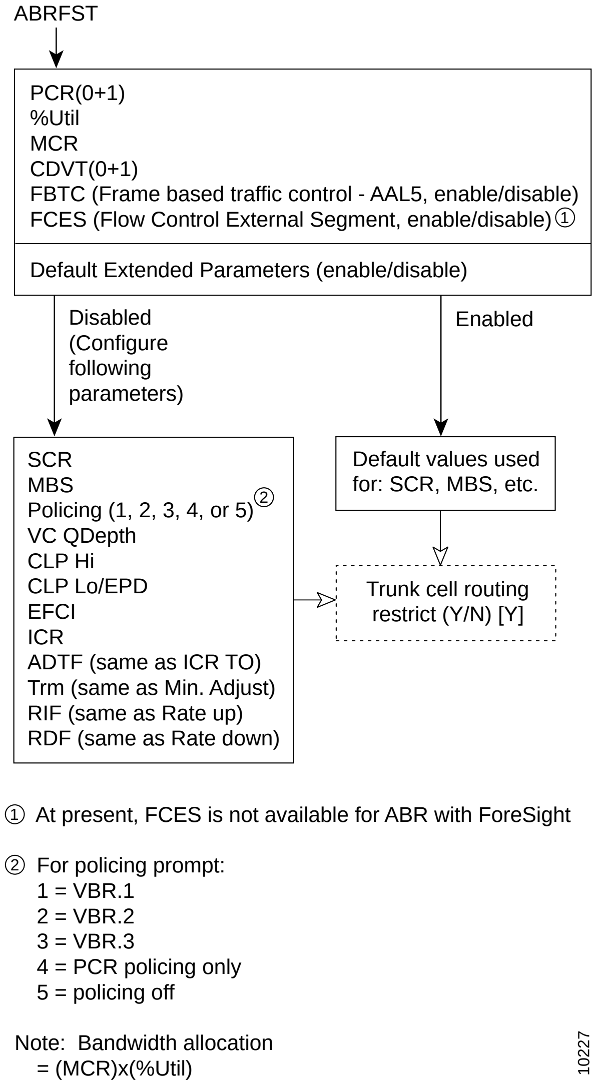

ABR Standard
VSVD
No
5
Yes
Flow control external segment
No
2
Yes
4
ABR with ForeSight
Flow control external segment
No
1
Yes
3
VS and VD shown below are for traffic flowing in direction of arrow. For the other direction of traffic, VS and VD are in the opposite direction.
External segment
Network segment
External segment
1
ABR with ForeSight
2
VS ABR standard VD
3
VS ABR VD
ABR with ForeSight
VS ABR VD
4
VS ABR VD
VS ABR standard VD
VS ABR VD
5
ABR standard without VSVD
(without congestion flow control performed by network segment)
S6158

Available Bit Rate Foresight Connections

The Available Bit Rate Foresight (ABRFST) connection uses the propriety ForeSight congestion control and is useful when configuring connections on which both ends do not terminate on BXM cards.

The parameters for an ABRFST connection are shown in Figure 21-10 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-10 Abr ForeSight Connection Prompt Sequence


ABRFST
PCR(0+1)
%Util
MCR
CDVT(0+1)
FBTC (Frame based traffic control - AAL5, enable/disable)
FCES (Flow Control External Segment, enable/disable) ①
Default Extended Parameters (enable/disable)
Disabled (Configure following parameters)
Enabled
SCR
MBS
Policing (1, 2, 3, 4, or 5) ②
VC QDepth
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as Min. Adjust)
RIF (same as Rate up)
RDF (same as Rate down)
Default values used for: SCR, MBS, etc.
Trunk cell routing restrict (Y/N) [Y]
① At present, FCES is not available for ABR with ForeSight
② For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
Note: Bandwidth allocation = (MCR)x(%Util)
10227

Unspecified Bit Rate 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 21-11 in the sequence in which they occur during the execution of the **addcon** command.

The Ubr policing definitions are summarized in Table 21-10.

Figure 21-11 Ubr Connection Prompt Sequence

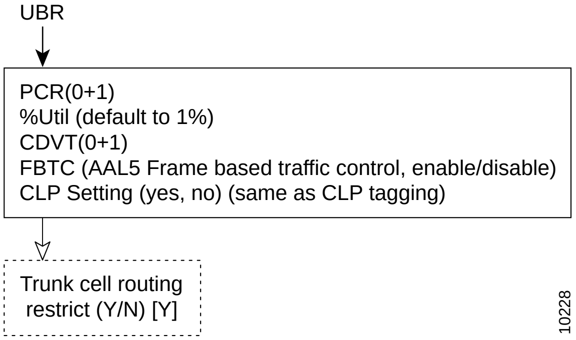

UBR
PCR(0+1)
%Util (default to 1%)
CDVT(0+1)
FBTC (AAL5 Frame based traffic control, enable/disable)
CLP Setting (yes, no) (same as CLP tagging)
Trunk cell routing restrict (Y/N) [Y]
10228

Table 21-11 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

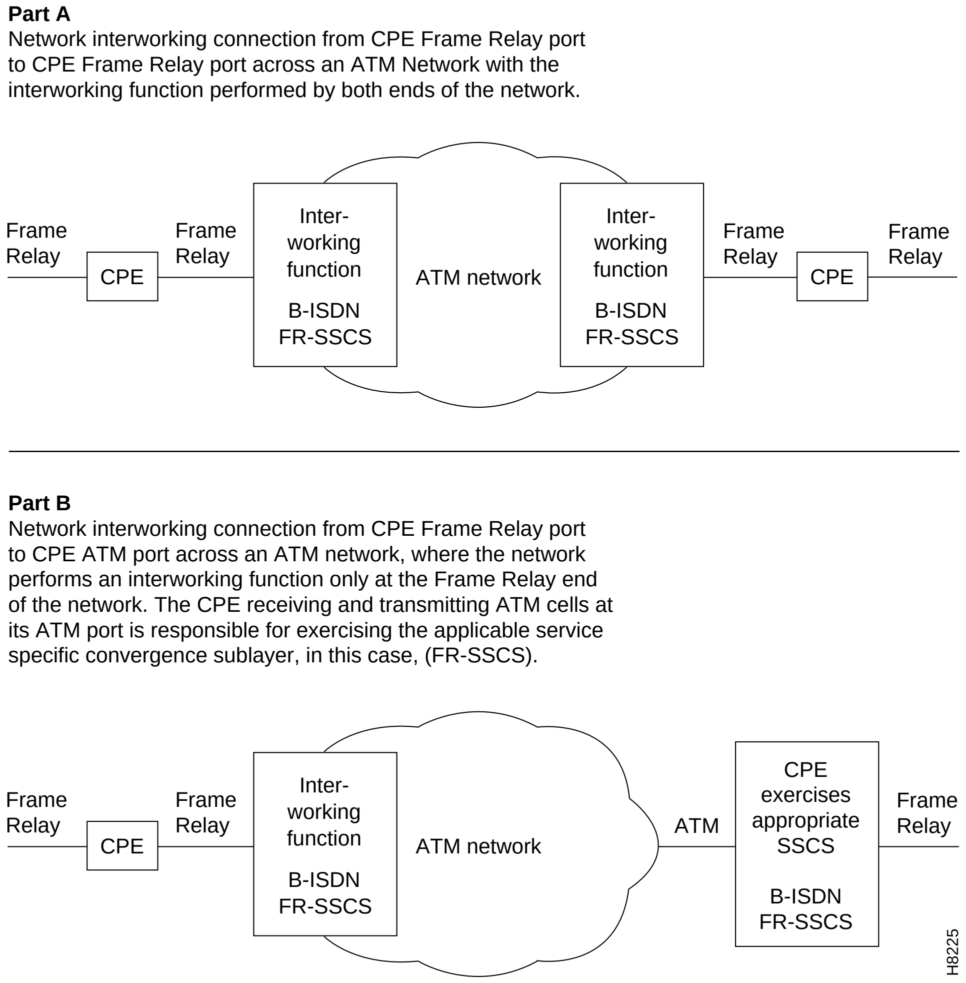
Network and Service Interworking Notes

Frame Relay to ATM Interworking enables Frame Relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking (see Figure 21-12 and Figure 21-13).

Two types of Frame Relay to ATM interworking are supported:

- Network Interworking
  Performed by the BTM card on the IGX switch and the FRSM card on the MGX 8220
- Service Interworking
  Performed by the FRSM card on the MGX 8220

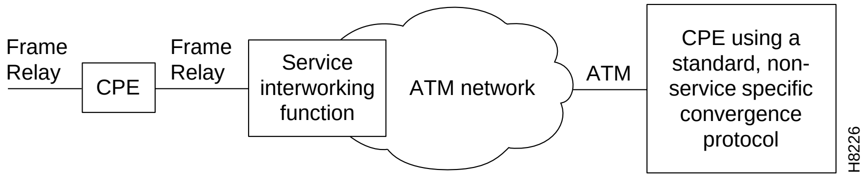
Figure 21-12 Frame Relay to ATM Network Interworking



Part A
Network interworking connection from CPE Frame Relay port to CPE Frame Relay port across an ATM Network with the interworking function performed by both ends of the network.

Part B
Network interworking connection from CPE Frame Relay port to CPE ATM port across an ATM network, where the network performs an interworking function only at the Frame Relay end of the network. The CPE receiving and transmitting ATM cells at its ATM port is responsible for exercising the applicable service specific convergence sublayer, in this case, (FR-SSCS).

Figure 21-13 Frame Relay to ATM Service Interworking



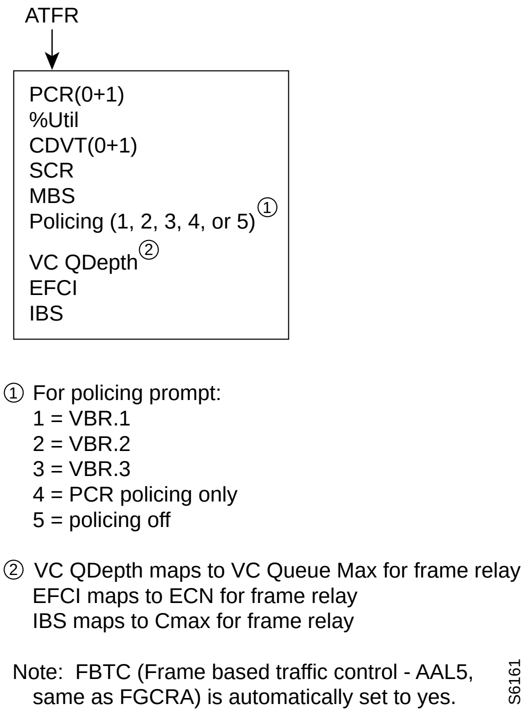
Frame Relay
CPE
Frame Relay
Service interworking function
ATM network
ATM
CPE using a standard, non-service specific convergence protocol
H8226

ATM-to-Frame Relay Network Interworking Connections

An ATM-to-Frame Relay (ATFR) connection is a Frame Relay to ATM 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 ATFR connection are shown in Figure 21-14 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-14 ATFR Connection Prompt Sequence

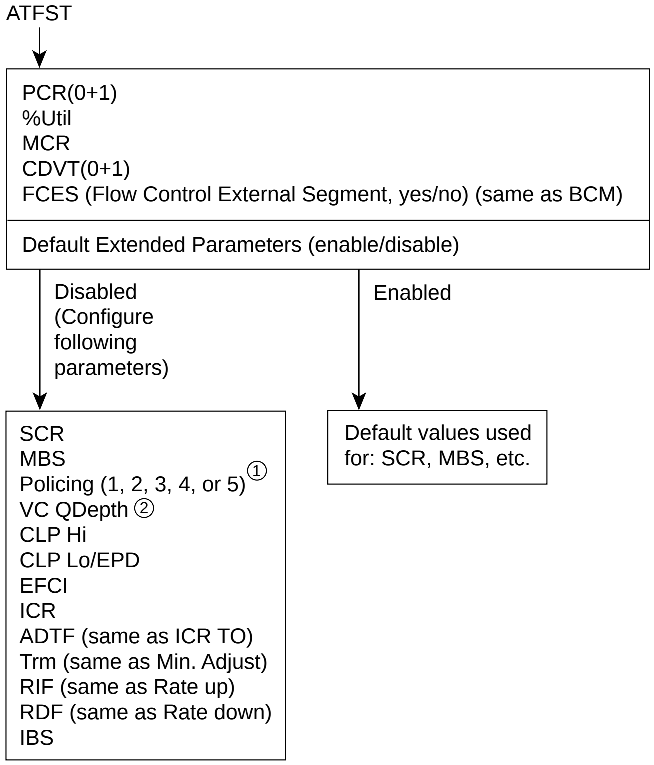

ATFR
PCR(0+1)
%Util
CDVT(0+1)
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
EFCI
IBS
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
② VC QDepth maps to VC Queue Max for frame relay
EFCI maps to ECN for frame relay
IBS maps to Cmax for frame relay
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.
S6161

Frame Relay-to-ATM Foresight Network Interworking Connection

A Frame Relay-to-ATM Foresight (ATFST) connection is a that is configured as an Abr connection with ForeSight. ForeSight congestion control is automatically enabled when connection type ATFST is selected. A number of the ATM and Frame Relay connection parameters are mapped between each side of the connection.

The parameters for an ATFST connection are shown in Figure 21-15 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-15 ATFST Connection Prompt Sequence


ATFST
PCR(0+1)
%Util
MCR
CDVT(0+1)
FCES (Flow Control External Segment, yes/no) (same as BCM)
Default Extended Parameters (enable/disable)
Disabled (Configure following parameters)
Enabled
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as Min. Adjust)
RIF (same as Rate up)
RDF (same as Rate down)
IBS
Default values used for: SCR, MBS, etc.
S6164

① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off

② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.

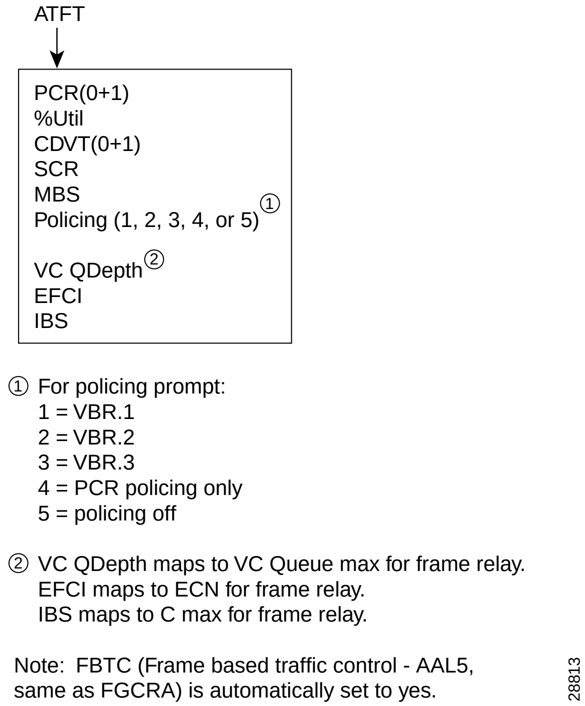
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.

Frame Relay-to-ATM Transparent Service Interworking Connections

A Frame Relay-to-ATM Transparent Service Interworking (ATFT) connection 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 21-16 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-16 ATFT Connection Prompt Sequence



① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off

② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.

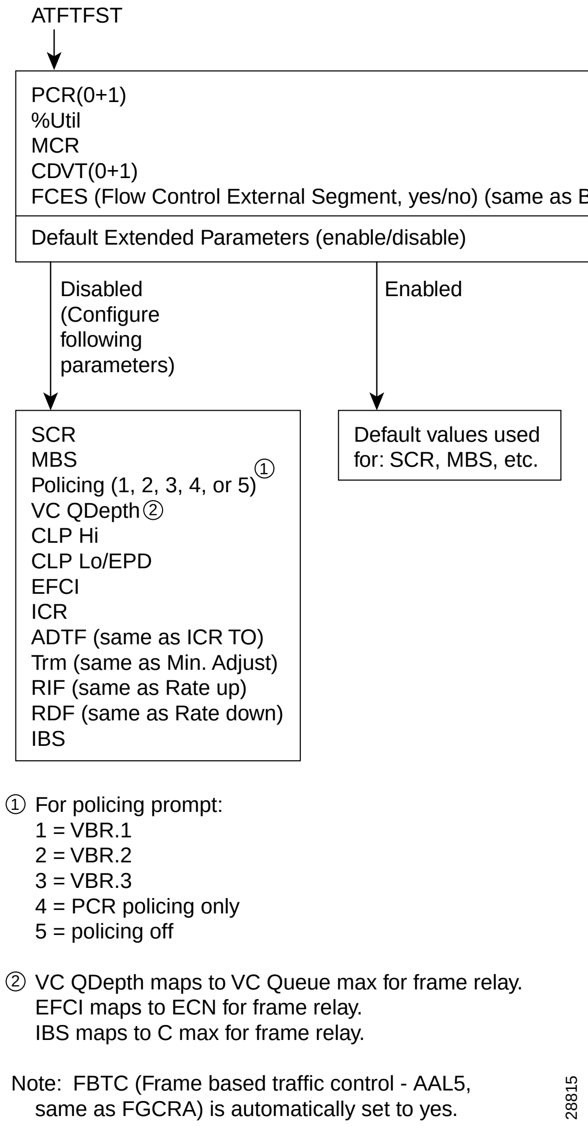
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.

Frame Relay-to-ATM Foresight Transparent Service Interworking Connections

A Frame Relay-to-ATM Foresight Transparent Service Interworking (ATFTFST**)** connection 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 21-17 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-17 ATFTFST Connection Prompt Sequence

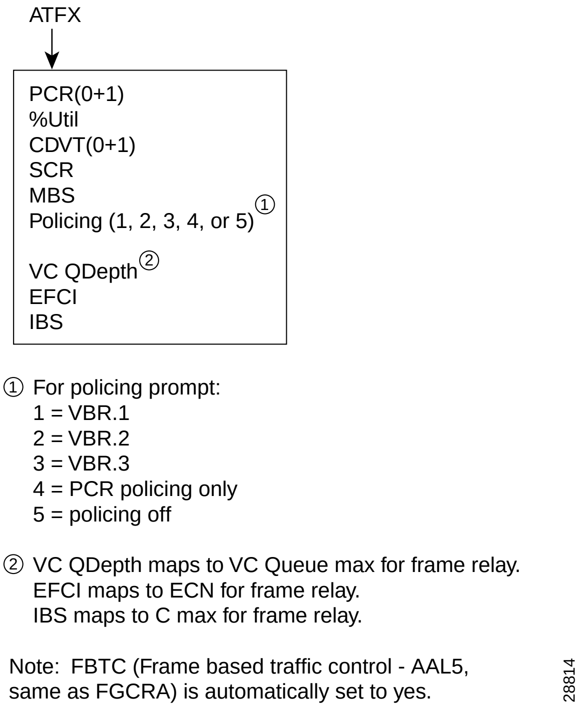

ATFTFST
PCR(0+1)
%Util
MCR
CDVT(0+1)
FCES (Flow Control External Segment, yes/no) (same as BCM)
Default Extended Parameters (enable/disable)
Disabled (Configure following parameters)
Enabled
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as Min. Adjust)
RIF (same as Rate up)
RDF (same as Rate down)
IBS
Default values used for: SCR, MBS, etc.
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.
28815

Frame Relay-to-ATM Translational Service Interworking Connections

A Frame Relay-to-ATM Translational (ATFX) 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 21-18 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-18 ATFX Connection Prompt Sequence



① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off

② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.

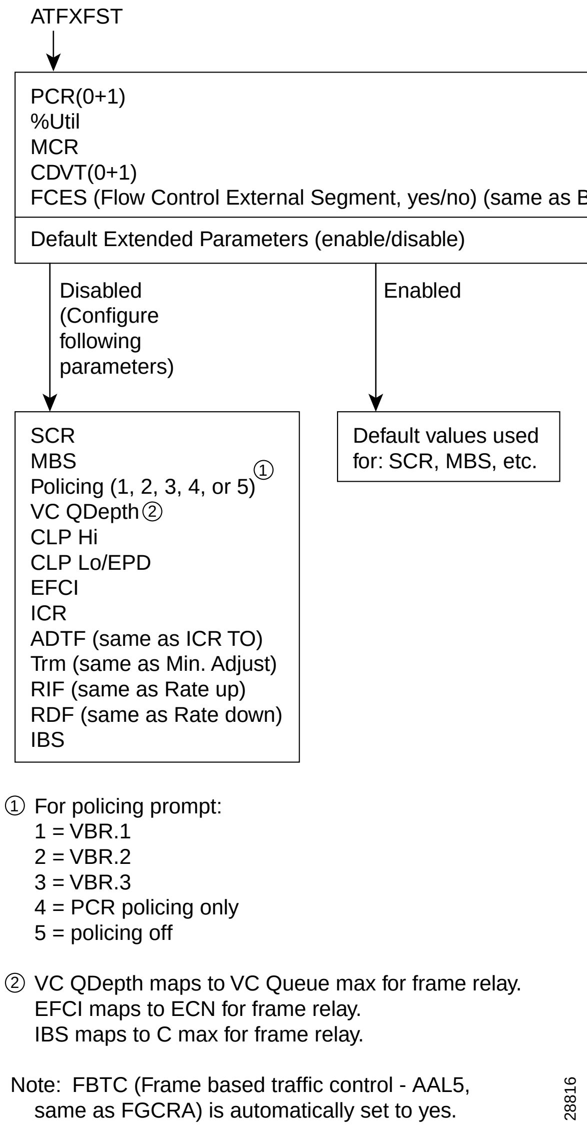
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.

Frame Relay-to-ATM Foresight Translational Service Interworking Connections

A Frame Relay-to-ATM Foresight (ATFXFST) 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 21-19 in the sequence in which they occur during the execution of the **addcon** command.

Figure 21-19 ATFXFST Connection Prompt Sequence


ATFXFST
PCR(0+1)
%Util
MCR
CDVT(0+1)
FCES (Flow Control External Segment, yes/no) (same as BCM)
Default Extended Parameters (enable/disable)
Disabled (Configure following parameters)
Enabled
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as Min. Adjust)
RIF (same as Rate up)
RDF (same as Rate down)
IBS
Default values used for: SCR, MBS, etc.
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.
28816

Traffic Policing Examples

Traffic Policing, also known as Usage Parameter Control (UPC), is implemented using either an ATM Forum single or dual-leaky bucket algorithm. The buckets represent a GCRA (Generic Cell Rate Algorithm) defined by two parameters:

- Rate (where I, expected arrival interval is defined as 1/Rate)
- Deviation (L)

If the cells are clumped too closely together, they are non-compliant and are tagged or discarded as applicable. If other cells arrive on time or after their expected arrival time, they are compliant, but three is no accrued credit.

Dual-Leaky Bucket (An Analogy)

A Generic Cell Rate Algorithm viewpoint is:

- For a stream of cells in an ATM connection, the cell compliance is based on the theoretical arrival time (TAT).
- The next TAT should be the time of arrival of the last compliant cell plus the expected arrival interval (I) where I = 1/rate.
- If the next cell arrives before the new TAT, it must arrive no earlier than new TAT - CDVT to be compliant.
- If the next cell arrives after the new TAT, it is compliant, but there is no accrued credit.

Cbr Traffic Policing Examples

Cbr traffic is expected to be at a constant bit rate, have low jitter, and is configured for a constant rate equal to Peak Cell Rate (PCR). The connection is expected to be always at peak rate.

When you add a connection, you assign a VPI.VCI address, and configure the UPC parameters for the connection. For each cell in an ATM stream seeking admission to the network, the VPI.VCI addresses are verified and each cell is checked for compliance with the UPC parameters. The Cbr cells are not enqueued, but are processed by the policing function and then sent to the network unless discarded.

For Cbr, traffic policing is based on:

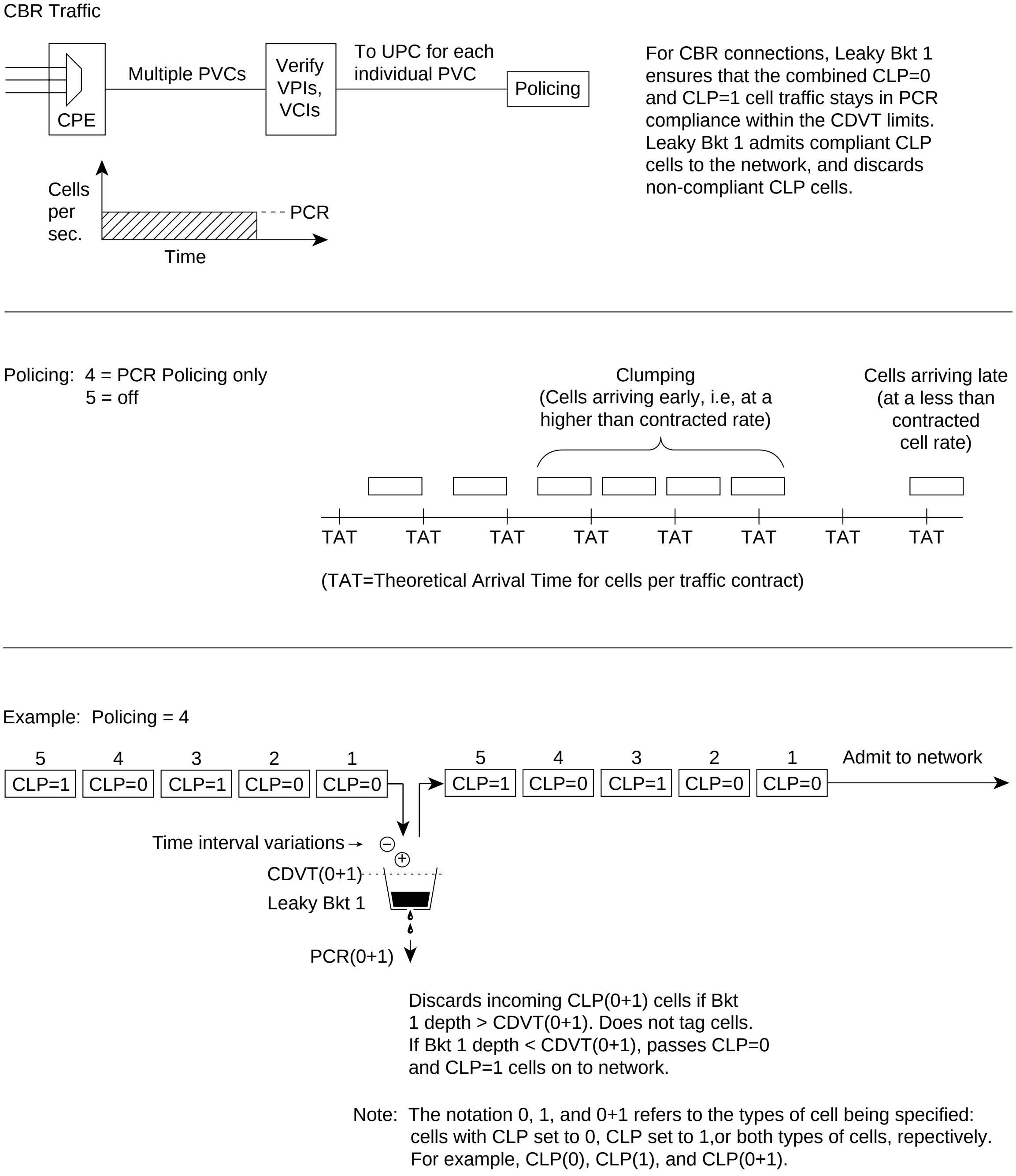
- Bucket 1
  - PCR(0+1), Peak Cell Rate
  - CDVT(0+1), Cell Delay Variation

You may configure Cbr connection with policing selected as either 4 or 5.

With policing set to 5, there is no policing.

With policing set to 4, there is single leaky bucket PCR policing as shown in Figure 21-20. The single leaky bucket polices the PCR compliance of all cells seeking admission to the network, both those with CLP = 0 and those with CLP =1. Cells seeking admission to the network with CLP set equal to 1 might have either encountered congestion along the user’s network or might have lower importance to the user and have been designated as eligible for discard in the case congestion is encountered. If the bucket depth CDVT (0+1) limit is exceeded, it discards all cells seeking admission. It does not tag cells. If leaky bucket 1 is not full, all cells (CLP =0 and CLP=1) are admitted to the network.

Figure 21-20 Cbr Connection, UPC Overview


CBR Traffic
CPE
Multiple PVCs
Verify VPIs, VCIs
To UPC for each individual PVC
Policing
Cells per sec.
PCR
Time
Policing: 4 = PCR Policing only
5 = off
Clumping
(Cells arriving early, i.e, at a higher than contracted rate)
Cells arriving late (at a less than contracted cell rate)
TAT
TAT
TAT
TAT
TAT
TAT
TAT
TAT
(TAT=Theoretical Arrival Time for cells per traffic contract)
Example: Policing = 4
5
4
3
2
1
CLP=1
CLP=0
CLP=1
CLP=0
CLP=0
5
4
3
2
1
CLP=1
CLP=0
CLP=1
CLP=0
CLP=0
Admit to network
Time interval variations→
⊖
⊕
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)

For CBR connections, Leaky Bkt 1 ensures that the combined CLP=0 and CLP=1 cell traffic stays in PCR compliance within the CDVT limits. Leaky Bkt 1 admits compliant CLP cells to the network, and discards non-compliant CLP cells.

Discards incoming CLP(0+1) cells if Bkt 1 depth > CDVT(0+1). Does not tag cells. If Bkt 1 depth < CDVT(0+1), passes CLP=0 and CLP=1 cells on to network.

Note: The notation 0, 1, and 0+1 refers to the types of cell being specified: cells with CLP set to 0, CLP set to 1,or both types of cells, repectively. For example, CLP(0), CLP(1), and CLP(0+1).

Figure 21-21 shows a Cbr.1 connection policing example, with policing set to 4, where the CDVT depth of the single leaky bucket is not exceeded, and all cells, CLP(0) and CLP(1) are admitted to the network.

Figure 21-21 Cbr.1 Connection with Bucket Compliant

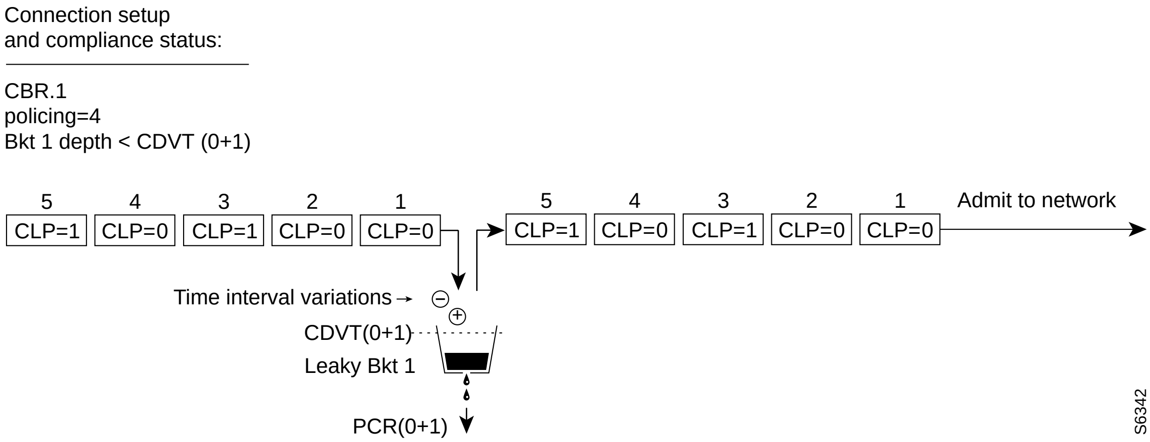
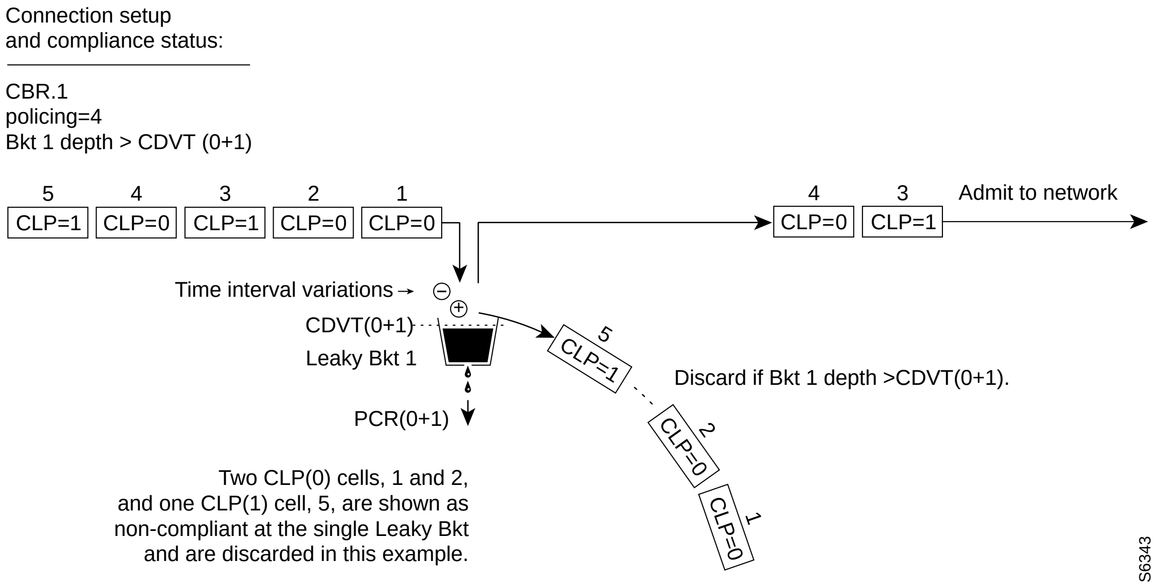


Figure 21-22 shows a Cbr connection policing example, with policing =4, where the CDVT(0+1) of the single leaky bucket is exceeded and non-compliant cells are discarded. The leaky bucket only discards cells; it does not tag them

Figure 21-22 Cbr.1 Connection, with Bucket Discarding non-Compliant Cells


Connection setup
and compliance status:
CBR.1
policing=4
Bkt 1 depth > CDVT (0+1)
5 4 3 2 1
CLP=1 CLP=0 CLP=1 CLP=0 CLP=0
4 3
CLP=0 CLP=1
Admit to network
Time interval variations
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
5 CLP=1
2 CLP=0
1 CLP=0
Discard if Bkt 1 depth >CDVT(0+1).
Two CLP(0) cells, 1 and 2,
and one CLP(1) cell, 5, are shown as
non-compliant at the single Leaky Bkt
and are discarded in this example.
S6343

Variable Bit Rate Dual-Leaky Bucket Policing Examples

The contract for a variable bit rate (Vbr) connection is set up based on an agreed upon sustained cell rate (SCR) with allowance for occasional data bursts at a Peak Cell Rate (PCR) as specified by maximum burst size MBS.

When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with the UPC parameters as shown in Figure 21-23.

The Vbr cells are not enqueued, but are processed by the policing function and then sent to the network unless discarded.

For Vbr, traffic policing, depending on selected policing option, is based on:

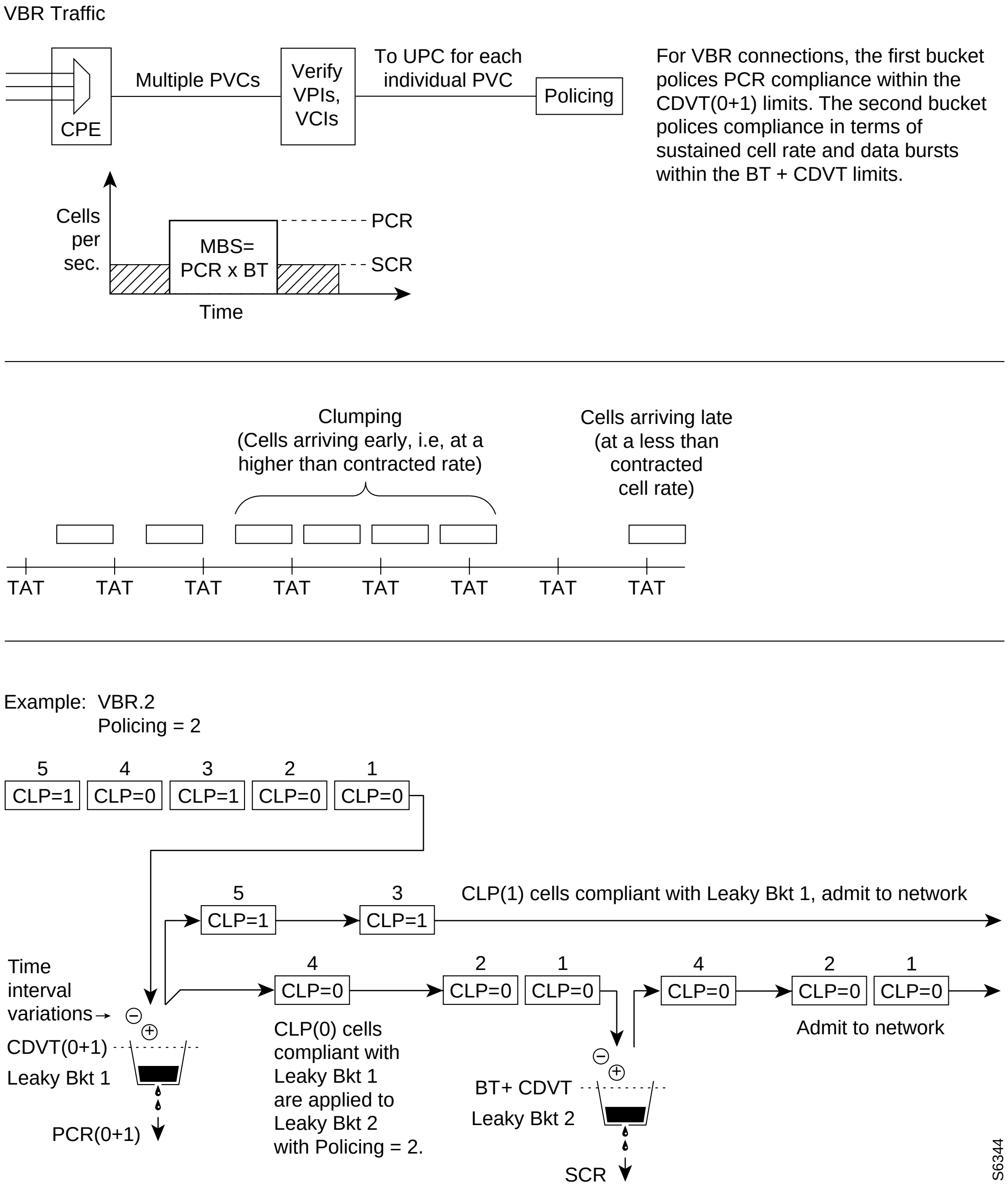
- Leaky bucket 1, PCR and CDVT
- Leaky bucket 2, SCR, CDVT, and MBS

The policing options for Vbr connections, selected by entering 1-5 in response to the policing choice prompt, are shown in Table 21-12:

Table 21-12 Policing Options for Vbr Connections

Vbr.1 Vbr with policing set to 1.	CLP(0+1) cells compliant with leaky bucket 1 are passed to leaky bucket 2; non-compliant cells are discarded. CLP(0+1) cells compliant with leaky bucket 2 are admitted to the network; non-compliant cells are discarded.
Vbr.2 Vbr with policing set to 2.	CLP(1) cells compliant with leaky bucket 1 are admitted to the network; non-compliant CLP(0+1) cells are dropped. CLP(0) cells compliant with leaky bucket 1 are applied to leaky bucket 2; non-compliant cells are dropped. CLP(0) cells compliant with leaky bucket 2 are admitted to the network; non-compliant cells are dropped.
Vbr.3 Vbr with policing set to 3.	CLP(1) cells compliant with leaky bucket 1 are admitted to the network; non-compliant CLP(0+1) cells are dropped. CLP(0) cells compliant with leaky bucket 1 are applied to leaky bucket 2; non-compliant cells are dropped. CLP(0) cells compliant with leaky bucket 2 are admitted to the network; non-compliant cells are tagged and admitted to the network.
Vbr with policing set to 4.	CLP(0+1) cells compliant with leaky bucket 1 are admitted to the network; non-compliant cells are dropped. Leaky bucket 2 is not active.
Vbr with policing set to 5.	Policing is off, so there is no policing of cells on ingress.

Figure 21-23 Vbr Connection, UPC Overview


VBR Traffic
CPE
Multiple PVCs
Verify VPIs, VCIs
To UPC for each individual PVC
Policing
For VBR connections, the first bucket polices PCR compliance within the CDVT(0+1) limits. The second bucket polices compliance in terms of sustained cell rate and data bursts within the BT + CDVT limits.
Cells per sec.
MBS= PCR x BT
PCR
SCR
Time
Clumping (Cells arriving early, i.e, at a higher than contracted rate)
Cells arriving late (at a less than contracted cell rate)
TAT
TAT
TAT
TAT
TAT
TAT
TAT
TAT
Example: VBR.2
Policing = 2
5
4
3
2
1
CLP=1
CLP=0
CLP=1
CLP=0
CLP=0
5
3
CLP=1
CLP=1
CLP(1) cells compliant with Leaky Bkt 1, admit to network
4
2
1
CLP=0
CLP=0
CLP=0
4
2
1
CLP=0
CLP=0
CLP=0
Time interval variations
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
CLP(0) cells compliant with Leaky Bkt 1 are applied to Leaky Bkt 2 with Policing = 2.
BT+ CDVT
Leaky Bkt 2
SCR
Admit to network
S6344

Leaky Bucket 1

Leaky bucket 1 polices for the PCR compliance of all cells seeking admission to the network, both those with CLP = 0 and those with CLP =1.

For example, cells seeking admission to the network with CLP set equal to 1 may have either encountered congestion along the user's network or may have lower importance to the user and have been designated as eligible for discard in the case congestion is encountered. If the bucket depth in the first bucket exceeds CDVT (0+1), it discards all cells seeking admission. It does not tag cells.

With policing set to 1 (Vbr.1), all cells (CLP=0 and CLP=1) that are compliant with leaky bucket 1, are sent to leaky bucket 2.

With policing set to 2 (Vbr.2) or to 3 (Vbr.3), all CLP=1 cells compliant with leaky bucket 1 are admitted directly to the network, and all CLP=0 cells compliant with leaky bucket 1 are sent to leaky bucket 2.

Leaky Bucket 2

For Vbr connections, the purpose of leaky bucket 2 is to police the cells passed from leaky bucket 1 for conformance with maximum burst size MBS as specified by BT and for compliance with the SCR sustained cell rate. The types of cells passed to leaky bucket 2 depend on how policing is set:

- For policing set to 5, cells bypass both buckets.
- For policing set to 4, leaky bucket 2 sees no traffic.
- For policing set to 2 or 3, the CLP(0) cells are admitted to the network if compliant with BT + CDVT of leaky bucket 2. If not compliant, cells may either be tagged (policing set to 3) or discarded (policing set to 2).
- For policing set to 1, the CLP(0) and CLP(1) cells are admitted to the network if compliant with BT + CDVT of leaky bucket 2. If not compliant, the cells are discarded. There is no tagging option.

Examples

Figure 21-24 shows a Vbr connection policing example, with policing set to 4, leaky bucket 1 compliant, and all cells being admitted to the network.

Figure 21-24 Vbr Connection, Policing = 4, Leaky Bucket 1 Compliant

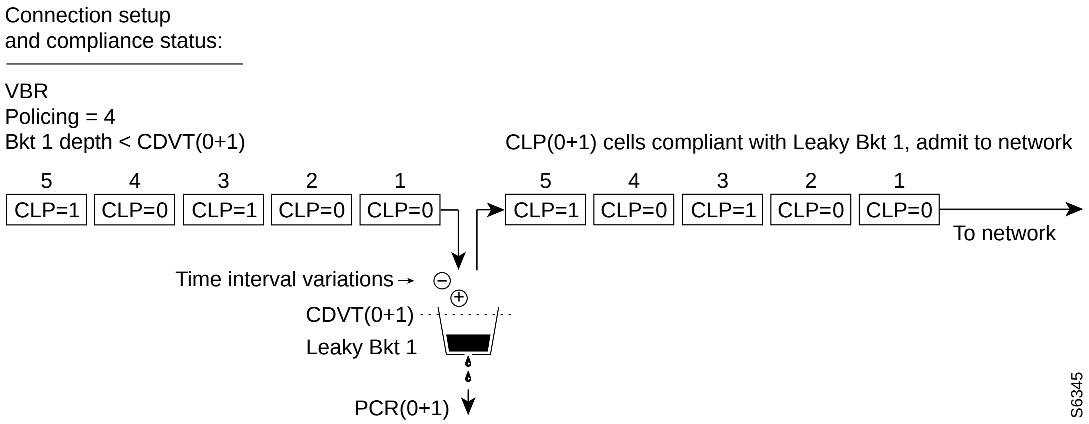


Figure 21-25 shows a Vbr connection policing example, with the policing set to 4, and leaky bucket 1 non-compliant which indicates that the connection has exceeded the PCR for a long enough interval to exceed the CDVT (0+1) limit. Non-compliant cells with respect to leaky bucket 1 are discarded.

Figure 21-25 Vbr Connection, Policing = 4, Leaky Bucket 1 Non-Compliant

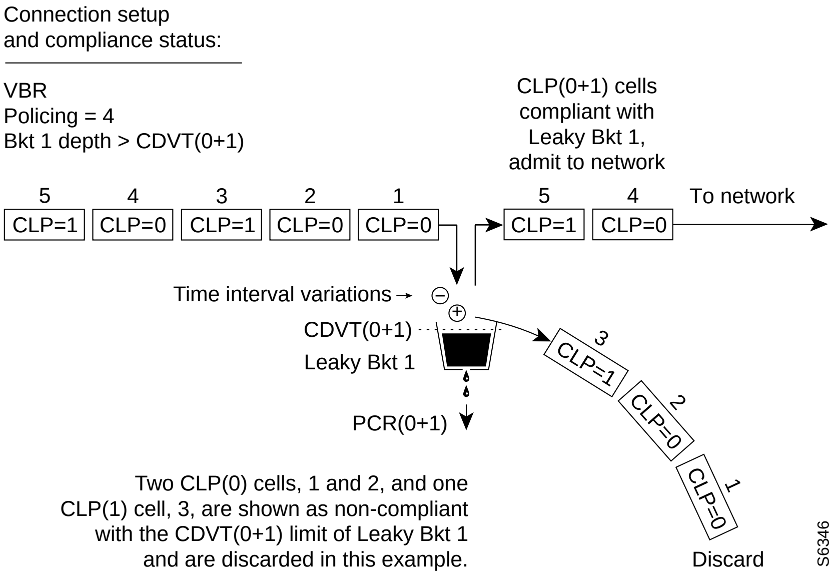


Figure 21-26 shows a Vbr.2 connection policing example, with policing = 2, and both buckets compliant. Leaky bucket two is policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with the SCR sustained cell rate.

Figure 21-26 Vbr.2 Connection, Policing = 2, with Buckets 1 and 2 Compliant

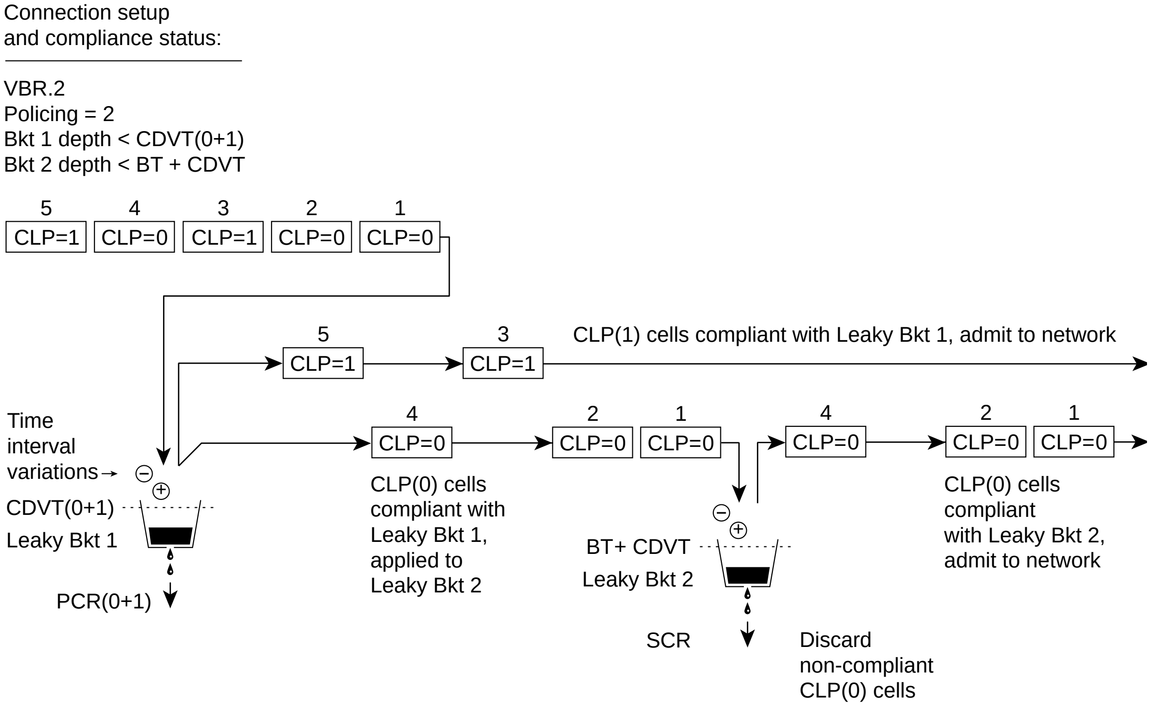


Figure 21-27 shows a Vbr.2 connection policing example, with policing set to 2, and leaky bucket 2 non-compliant. Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR (sustained cell rate).

In this example (policing set to 2), CLP tagging is not enabled, so that the cells that have exceeded the BT + CDVT limit are discarded. In the example, either the sustained cell rate could have been exceeded for an excessive interval, or a data burst could have exceeded the maximum allowed burst size.

Figure 21-27 Vbr.2 Connection, Leaky Bucket 2 Discarding CLP (0) Cells

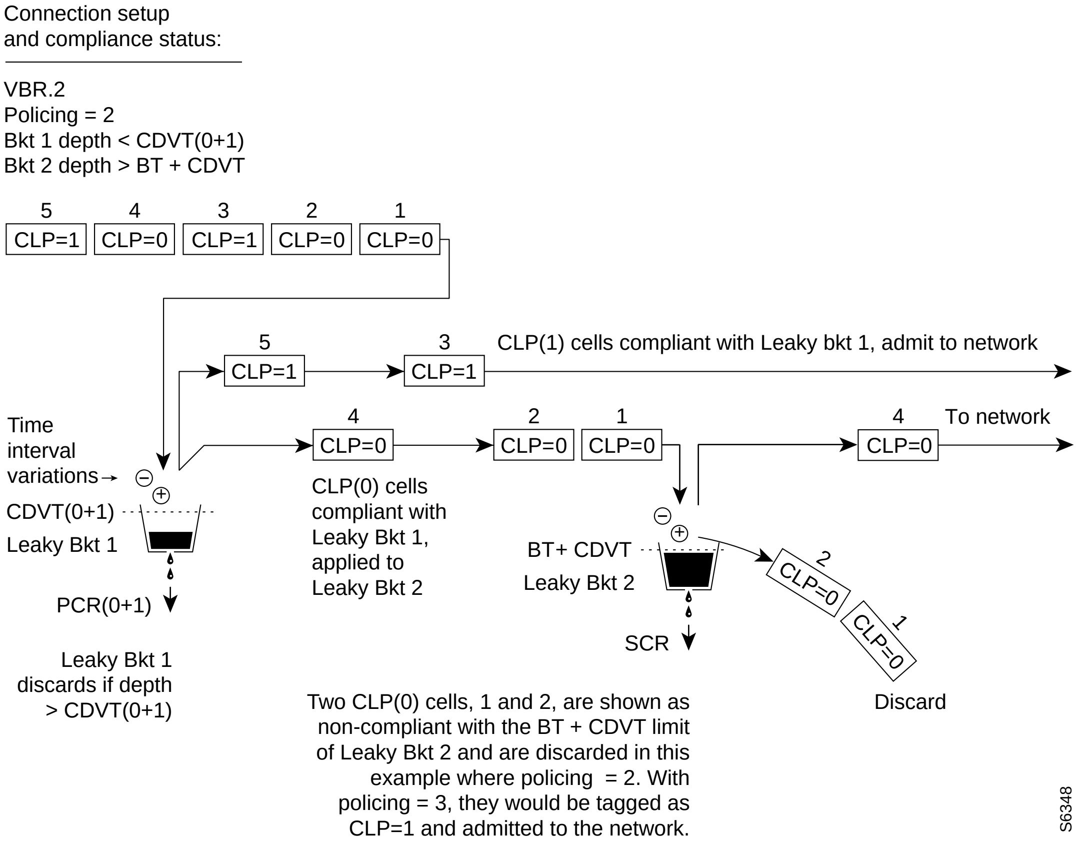

Connection setup
and compliance status:
VBR.2
Policing = 2
Bkt 1 depth < CDVT(0+1)
Bkt 2 depth > BT + CDVT
5 CLP=1
4 CLP=0
3 CLP=1
2 CLP=0
1 CLP=0
5 CLP=1
3 CLP=1
CLP(1) cells compliant with Leaky bkt 1, admit to network
4 CLP=0
2 CLP=0
1 CLP=0
4 CLP=0
To network
Time interval variations
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
CLP(0) cells compliant with Leaky Bkt 1, applied to Leaky Bkt 2
BT+ CDVT
Leaky Bkt 2
SCR
2 CLP=0
1 CLP=0
Discard
Leaky Bkt 1 discards if depth > CDVT(0+1)
Two CLP(0) cells, 1 and 2, are shown as non-compliant with the BT + CDVT limit of Leaky Bkt 2 and are discarded in this example where policing = 2. With policing = 3, they would be tagged as CLP=1 and admitted to the network.
S6348

Figure 21-28 shows a Vbr.1 connection policing example, with policing set to 1, and both buckets compliant.

Leaky bucket 1 is policing the CLP (0+1) cell stream for conformance with the PCR limit.

Leaky bucket 2 is policing the CLP (0+1) cell stream for conformance with CDVT plus maximum burst size MBS (as specified by BT), and for compliance with SCR sustained cell rate.

Figure 21-28 Vbr.1 Connection, Policing = 1, with Buckets 1 and 2 Compliant

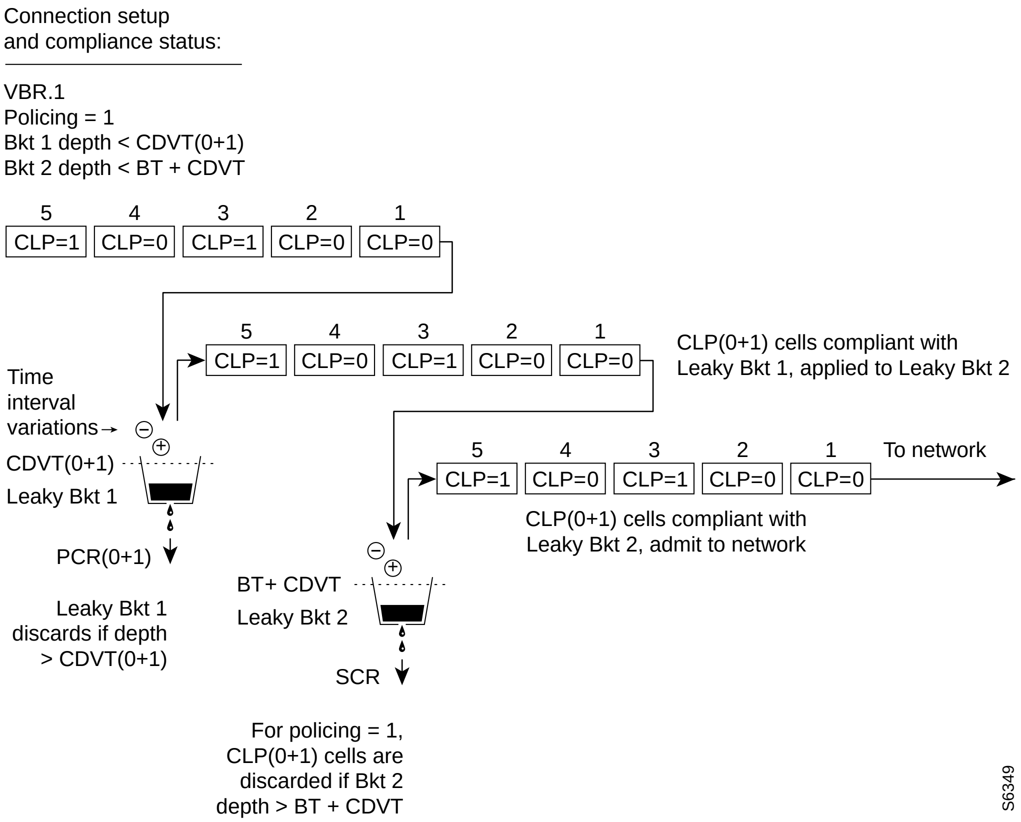


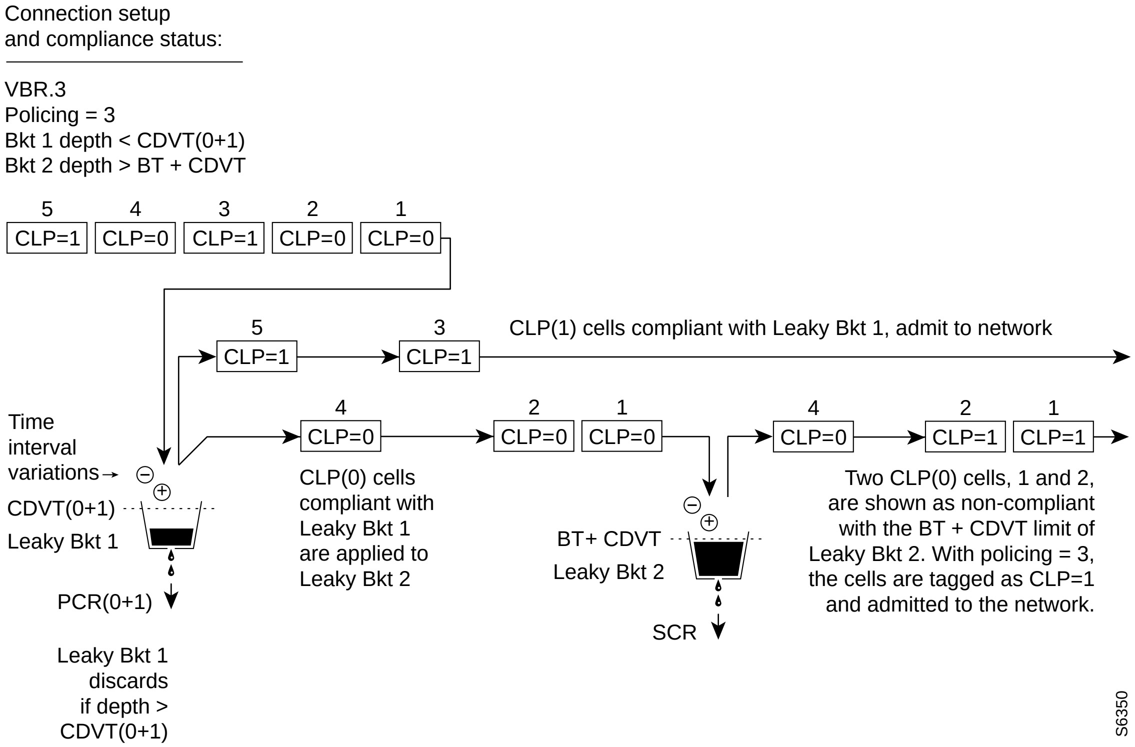
Figure 21-29 shows a Vbr.3 connection policing example, with policing set to 3, and Leaky bucket 2 shown as non-compliant.

Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR sustained cell rate.

For the policing = 3 selection, CLP tagging is enabled, so the cells that have exceeded the BT + CDVT(0+1) limit are tagged as CLP=1 cells and admitted to the network.

In this example, either the sustained cell rate could have been exceeded for an excessive interval, or a data burst could have exceeded the maximum burst size allowed.

Figure 21-29 Vbr.3 Connection, Policing = 3, with Bucket 2 non-compliant



Abr Connection Policing

Available Bit Rate (Abr) connections are policed the same as the Vbr connections, but in addition use either the Abr Standard with VSVD congestion flow control method or the ForeSight option to take advantage of unused bandwidth when it is available.

Ubr Connection Policing

The contract for a unspecified bit rate connection is similar to the Abr connection service for bursty data. However, Ubr traffic is delivered only when there is spare bandwidth in the network.

When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with the UPC parameters as shown in Figure 21-30.

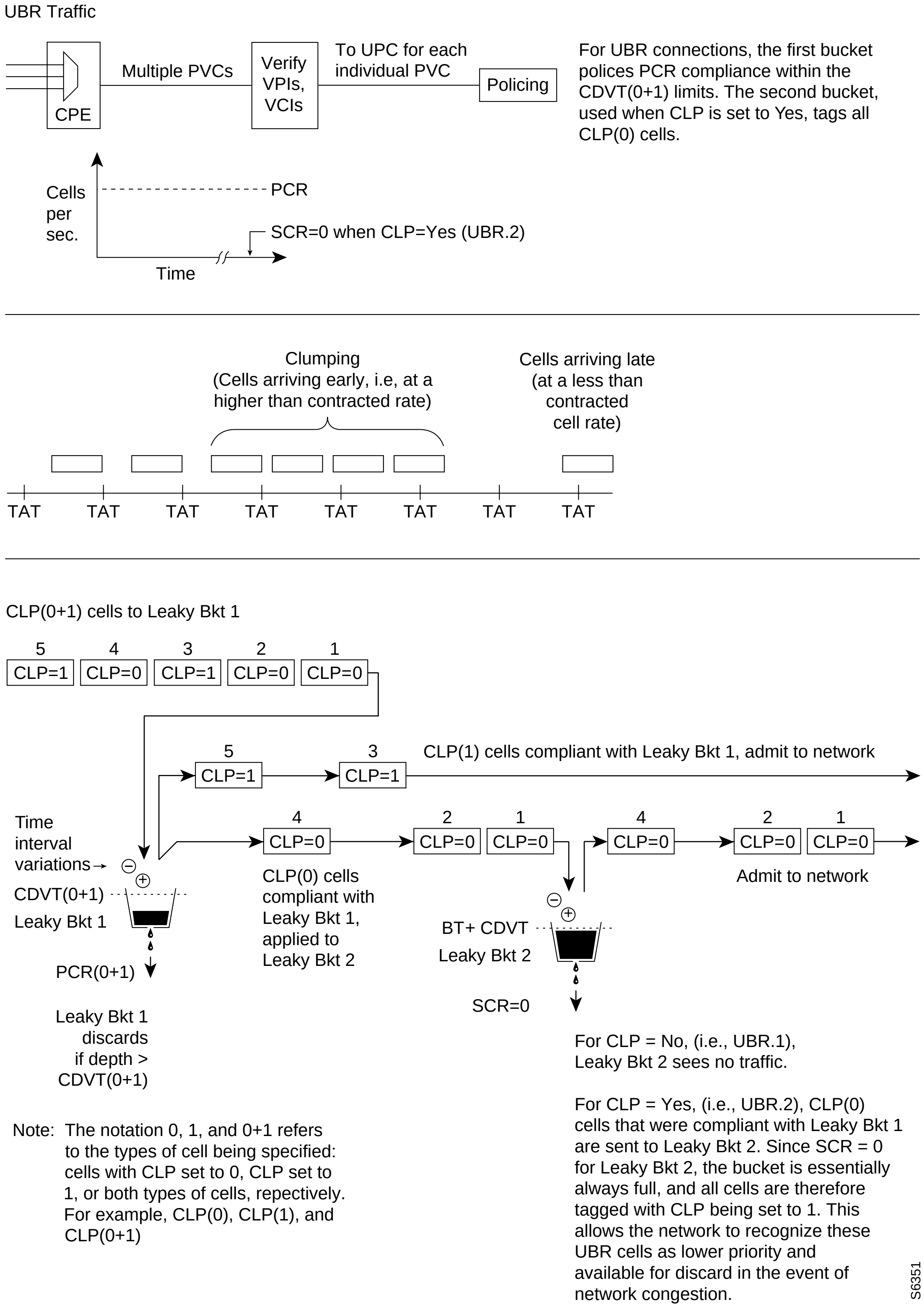
Leaky Bucket 1

Leaky bucket 1 polices the Ubr connection for PCR compliance. When CLP=No (Ubr.1), all cells that are compliant with leaky bucket 1 are applied to the network. However, these cells are treated with low priority in the network with a percentage utilization default of 1 percent.

Leaky Bucket 2

When CLP=Yes (Ubr.2), CLP(0) cells that are compliant with leaky bucket 1 are sent to leaky bucket 2. Because SCR=0 for leaky bucket 2, the bucket is essentially always full, and all the CLP(0) cells sent to leaky bucket 2 are therefore tagged with CLP being set to 1. This allows the network to recognize these Ubr cells as lower priority cells and available for discard in the event of network congestion.

Figure 21-30 Ubr Connection, UPC Overview


UBR Traffic
CPE
Multiple PVCs
Verify VPIs, VCIs
To UPC for each individual PVC
Policing
Cells per sec.
PCR
SCR=0 when CLP=Yes (UBR.2)
Time
Clumping
(Cells arriving early, i.e, at a higher than contracted rate)
Cells arriving late (at a less than contracted cell rate)
TAT
TAT
TAT
TAT
TAT
TAT
TAT
TAT
CLP(0+1) cells to Leaky Bkt 1
5 CLP=1
4 CLP=0
3 CLP=1
2 CLP=0
1 CLP=0
5 CLP=1
3 CLP=1
CLP(1) cells compliant with Leaky Bkt 1, admit to network
Time interval variations
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
Leaky Bkt 1 discards if depth > CDVT(0+1)
4 CLP=0
2 CLP=0
1 CLP=0
CLP(0) cells compliant with Leaky Bkt 1, applied to Leaky Bkt 2
BT+ CDVT
Leaky Bkt 2
SCR=0
4 CLP=0
2 CLP=0
1 CLP=0
Admit to network
S6351

For UBR connections, the first bucket polices PCR compliance within the CDVT(0+1) limits. The second bucket, used when CLP is set to Yes, tags all CLP(0) cells.

For CLP = No, (i.e., UBR.1), Leaky Bkt 2 sees no traffic.

For CLP = Yes, (i.e., UBR.2), CLP(0) cells that were compliant with Leaky Bkt 1 are sent to Leaky Bkt 2. Since SCR = 0 for Leaky Bkt 2, the bucket is essentially always full, and all cells are therefore tagged with CLP being set to 1. This allows the network to recognize these UBR cells as lower priority and available for discard in the event of network congestion.

Note: The notation 0, 1, and 0+1 refers to the types of cell being specified: cells with CLP set to 0, CLP set to 1, or both types of cells, repectively. For example, CLP(0), CLP(1), and CLP(0+1)

ATM Command List

Table 21-13 ATM Connection Commands

Mnemonic	Description
addcon	Add connection
clrchstats	Clear channel statistics
cnfabrparm	Configure Abr parameters (applies to BXM)
cnfatmcls	Configure ATM class
cnfcdparm	Configure channel statistic level on UXM/BXM cards
cnfcls	Configure class
cnfcon	Configure connection
cnfport	Configure port
cnfportq	Configure port queue
delcon	Delete connection
dnport	Down port
dspatmcls	Display ATM class
dspchstats	Display channel statistics
dspcls	Display class
dspcon	Display connection
dspconcnf	Display connection configuration
dspcons	Display connections
dsplmistats	Display LMI statistics
dspport	Display port
dspportq	Display port queue
dspportstats	Display port statistics
tstconseg	Test connection externally with OAM segment loopback cells
tstdelay	Test traffic continuity and connection roundtrip delay
upport	Up port

CHAPTER 22

Configuring Frame Relay to ATM Network and Service Interworking

Frame Relay to ATM Interworking lets you retain your existing Frame Relay services, and as your needs expand, migrate to the higher bandwidth capabilities provided by BPX switch ATM networks.

This chapter describes Frame Relay to ATM interworking:

- Service Interworking
- Networking Interworking
- ATM Protocol Stack
- BTM Interworking and the ATM Protocol Stack
- BTM Control Mapping: Frames and Cells
- OAM Cells
- Connection Management

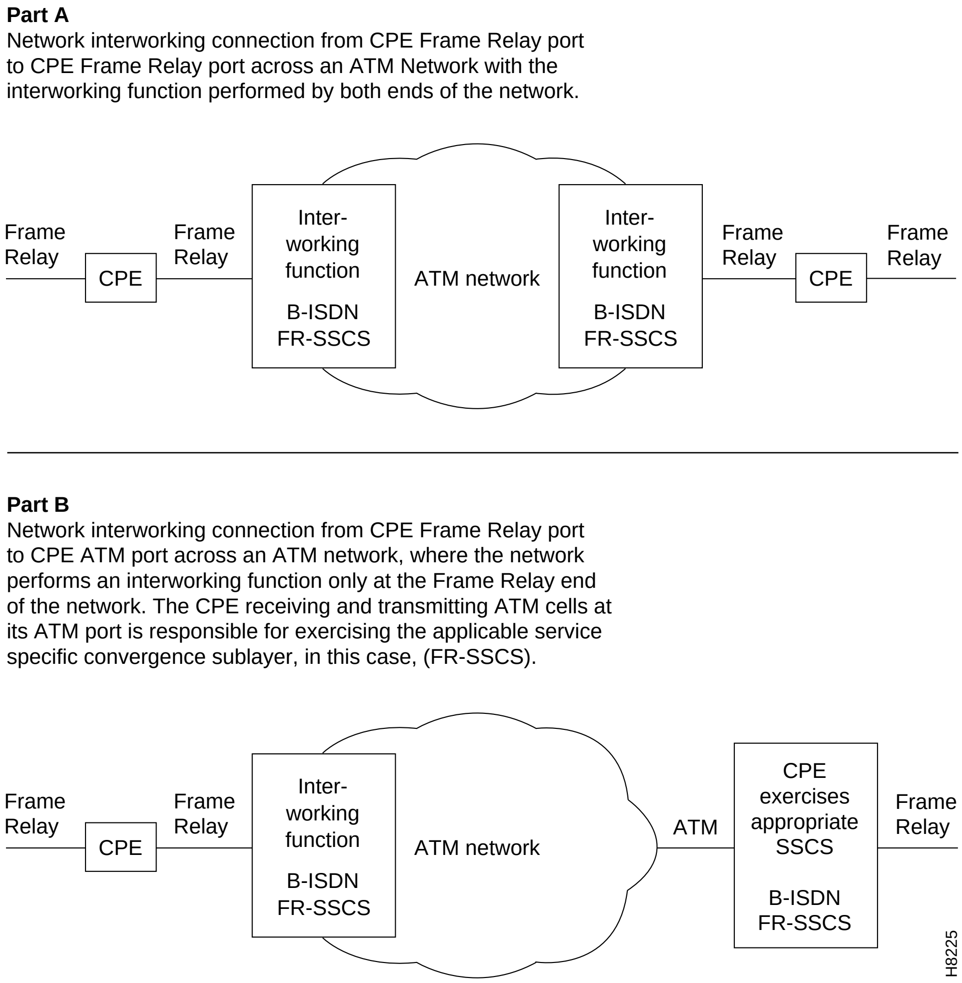
Frame Relay to ATM Interworking enables Frame Relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking (see Figure 22-1 and Figure 22-2).

Two types of Frame Relay to ATM interworking are supported:

- **Network Interworking**
  Performed by the BTM card on the IGX switch and the FRSM card on the MGX 8220.
- **Service Interworking**
  Performed by the FRSM card on the MGX 8220.

See Figure 22-3 for some examples of ATM-to-Frame Relay Interworking.

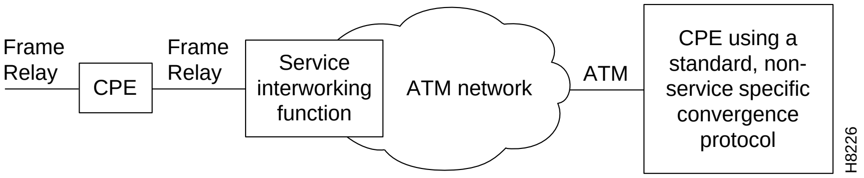
Figure 22-1 Frame Relay to ATM Network Interworking



Part A
Network interworking connection from CPE Frame Relay port to CPE Frame Relay port across an ATM Network with the interworking function performed by both ends of the network.

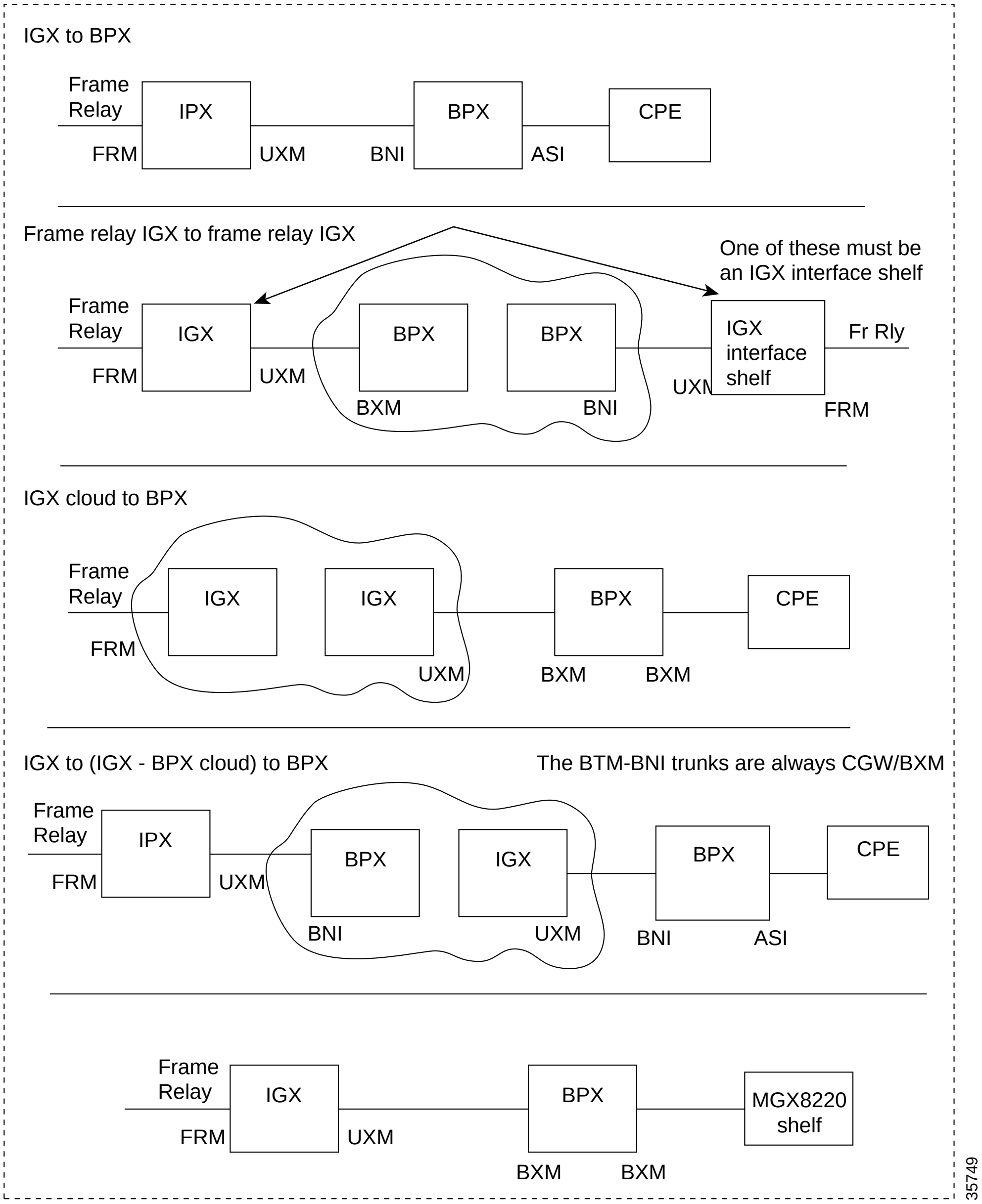
Part B
Network interworking connection from CPE Frame Relay port to CPE ATM port across an ATM network, where the network performs an interworking function only at the Frame Relay end of the network. The CPE receiving and transmitting ATM cells at its ATM port is responsible for exercising the applicable service specific convergence sublayer, in this case, (FR-SSCS).

Figure 22-2 Frame Relay to ATM Service Interworking



Frame Relay
CPE
Frame Relay
Service interworking function
ATM network
ATM
CPE using a standard, non-service specific convergence protocol
H8226

Figure 22-3 Frame Relay to ATM Interworking Examples with BTM Card on IGX Switch



UXM Interworking Examples

Service Interworking

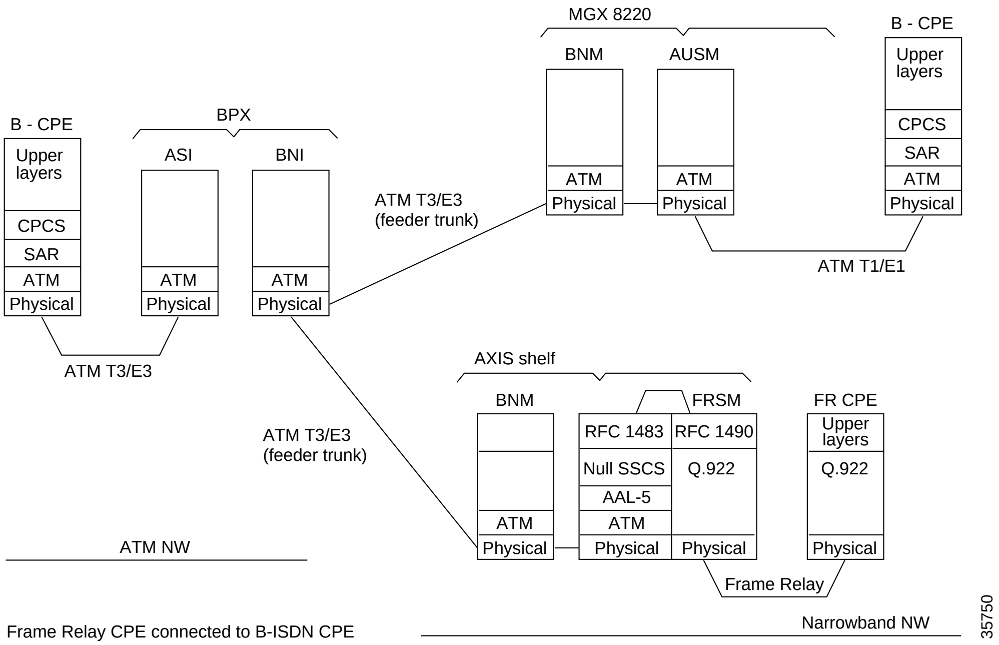
In Service Interworking, the ATM port connected to a Frame Relay port does not need to be aware that it is connected to an interworking function. However, in Network Interworking, the ATM device *does* need to be aware that it is connected to an interworking function.

The ATM device uses a standard service specific convergence sublayer, instead of using the Frame Relay FR-SSCS (see Figure 22-4).

The Frame Relay service user does not implement any ATM specific procedures, and the ATM service user does not need to provide any Frame Relay specific functions. All translational (mapping functions) are performed by the intermediate IWF.

The ATM endpoints may be any ATM UNI/NNI interface supported by the MGX 8220 or MGX 8800, such as BXM and AUSM. Translation between the Frame Relay and ATM protocols is performed in accordance with RFC 1490 and RFC 1483.

Figure 22-4 Frame Relay to ATM Service Interworking Detail



Networking Interworking

In Network Interworking, in most cases, the source and destination ports are Frame Relay ports, and the interworking function is performed at both ends of the connection as shown in Part A of Figure 22-5.

If a Frame Relay port is connected across an ATM network to an ATM device, network interworking requires that the ATM device recognize that it is connected to an interworking function (Frame Relay, in this case). The ATM device must then exercise the appropriate service specific convergence sublayer (SSCS), in this case the Frame Relay service specific convergence sublayer (FR-SSCS) as shown in Part B of Figure 22-5.

Figure 22-5 Frame Relay to ATM NW Interworking Detail

These Frame Relay-to-ATM networking interworking functions are available:

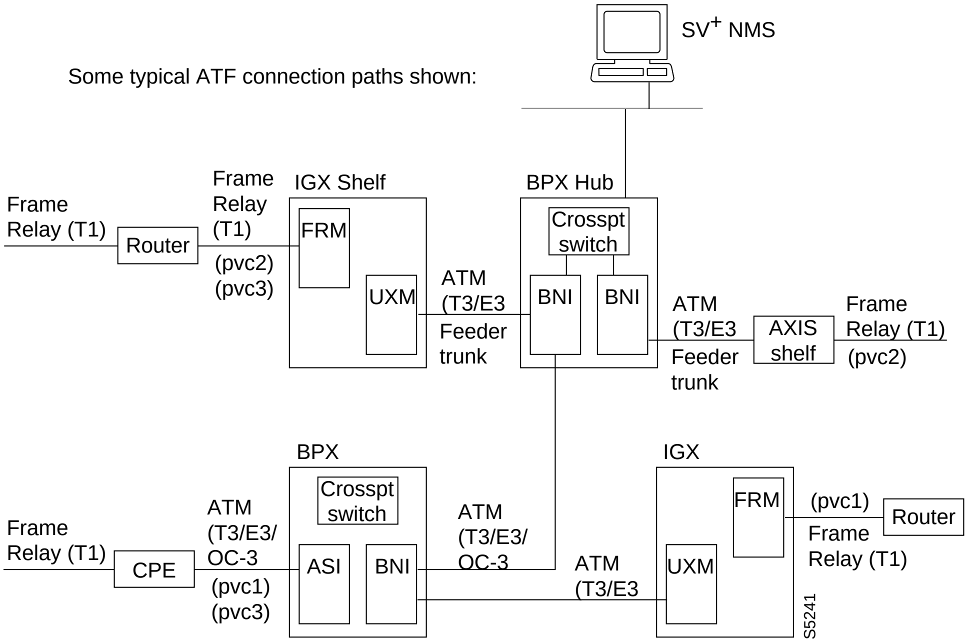
- IGX switch Frame Relay (shelf/feeder) to IGX switch Frame Relay (either routing node or shelf/feeder)
- MGX 8220 Frame Relay to MGX 8220 Frame Relay
- MGX 8220 Frame Relay to IGX switch Frame Relay (either routing node or shelf/feeder)
- IGX switch Frame Relay (either routing node or shelf/feeder) to BPX switch or MGX 8220 ATM port
- MGX 8220 Frame Relay to BPX switch or MGX 8220 ATM port

On the IGX switch, interworking is performed by the BTM card.

A simplified example of the connection paths is shown in Figure 22-6. In interworking, the BTM card receives FastPackets from the FRM, rebuilds the frames, and converts between frames and ATM cells. Data is removed from one package and placed in the other. Congestion information from the header is mapped to the new package.

This processing by the BTM trunk card is called Complex Gateway. BTM trunk cards are required on every BPX switch to IGX switch hop in a Frame Relay to ATM connection’s path.

Figure 22-6 ATF Connections, Simplified Example



The cells within the frame are expected to possess the standard ATM Access Interface cell header. The traffic is assumed to have AAL-5 PDUs, and will not function properly otherwise (framing errors will result). Within the AAL-5 PDUs, the data must be packaged in standard Frame Relay frames, one frame per PDU (with respect to the AAL-5 layer).

The UPC and ForeSight algorithms are applied according to their configured values. The cell headers are converted into the proprietary Cisco WAN switching STI format before entering the network. The cells are delivered to their destination according to the configured route of the connection. Cells can be lost due to congestion.

Discard selection is based upon the standard CLP bit in the cells. When the routing path enters an IGX switch, a BTM card that supports Interworking traffic is required to convert the connection data from cells to frames (frames to fastpackets out onto MuxBus to FRP/cell bus to FRM), and visa versa.

Additionally, the AAL-5 framing is removed upon conversion to frames, and added upon conversion to cells. At the destination (FRM), FastPackets are placed in the port queue and, when a complete frame has been assembled, the frame is played out the remote port in the original format (as provided in the frames delivered inside AAL-5 PDUs).

For each connection, only a single dlci can be played out for all traffic exiting the port, and is inserted into the frame headers. The standard LAPD framing format is played out the port on the FRM.

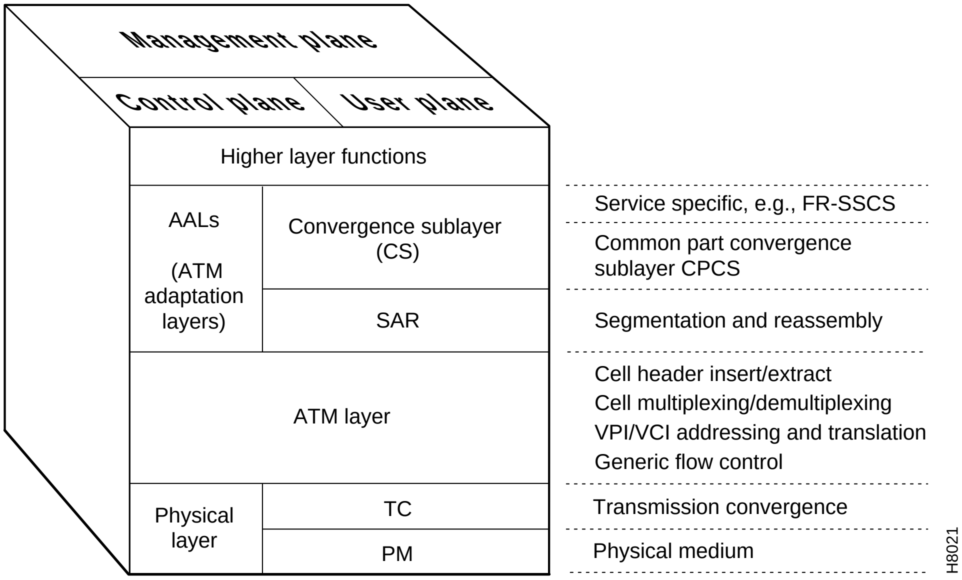
At the FRM card, several additional protocol mappings take place. First, the Interworking Unit acts as a pseudo endpoint for the purposes of ATM for all constructs that have no direct mapping into Frame Relay, such as loopbacks and FERF indications. Thus, end-to-end loopback OAM cells that ingress to FRM cards from the network are returned to the ATM network without allowing them to proceed into the Frame Relay network, which has no equivalent message construct. Further, AIS and supervisory cells and FastPackets (from the Frame Relay direction) are converted into their counterparts within the other network.

ATM Protocol Stack

A general view of the ATM protocol layers with respect to the Open Systems Interconnection model is shown in Figure 22-7. In this example, a large frame might be input into the top of the stacks. Each layer performs a specific function before passing it to the layer below. A protocol data unit (PDU) is the name of the data passed down from one layer to another and is the Service Data Unit (SDU) of the layer below it.

For Frame Relay to ATM interworking, a specific convergent sublayer, Frame Relay Service Specific Convergent Sublayer, FR-SSCS is defined. This is also referred to as FR-CS, in shortened notation.

Figure 22-7 ATM Layers


Management plane
Control plane
User plane
Higher layer functions
AALs
(ATM adaptation layers)
Convergence sublayer (CS)
SAR
ATM layer
Physical layer
TC
PM
Service specific, e.g., FR-SSCS
Common part convergence sublayer CPCS
Segmentation and reassembly
Cell header insert/extract
Cell multiplexing/demultiplexing
VPI/VCI addressing and translation
Generic flow control
Transmission convergence
Physical medium
H8021

BTM Interworking and the ATM Protocol Stack

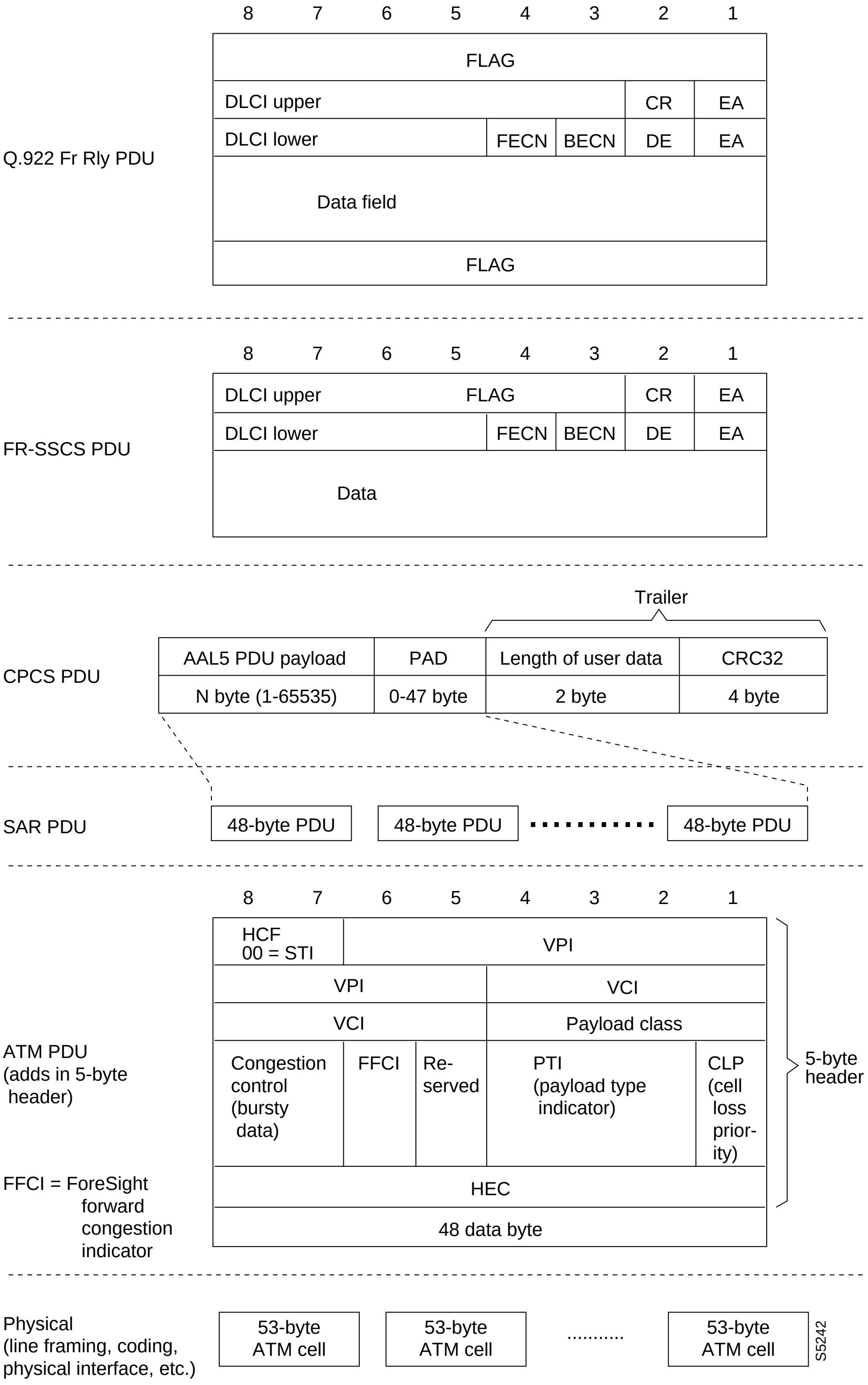
ATM to Frame Relay interworking (ATF) performs these tasks:

- Conversion of PDUs between the Frame Relay and ATM virtual circuits of the Frame Relay and ATM user devices
- Conversion between Frame Relay traffic service and ATM quality of service parameters
- Mapping of management status, including connection, port, line, and trunk status and events

Figure 22-8 depicts the function of the protocol stack layers in the interworking between ATM and Frame Relay PDUs. Interworking by the BTM card in the IGX switch includes these functions:

- Translating the ATM pvc identifier (vpi.vci) to the Frame Relay pvc identifier (dlci) and vice versa.
- Mapping the Protocol Data Unit (PDU), which is essentially the data, between the Frame Relay Service Specific Convergence Sublayer (FR-SSCS) and the Frame Relay Q.922 core protocol, and vice versa.
- On the IGX switch, Incoming Frames are converted to FastPackets by the FRM card. The FastPackets are then routed to the FRM card via the IGX switch bus and converted back into Frame Relay Q.922 frames by the BTM card. The BTM card interworking function executes four layers to convert the Frame PDU to ATM cells:
  - FRCS layer (Frame Relay Service Specific Convergence Sublayer, FRSSCS, or FRCS for in shortened notation) which uses a PDU format identical to the Q.922 core (without CRC-16 or flags).
  - CPCS layer (Common Part Convergence Sublayer) which appends a CS-PDU trailer to the FR-PDU to create a CS-PDU.
  - Segmentation and Reassembly layer (SAR) which segments the CS-PDU (Protocol Data Unit) into SAR-PDUs (48 byte data entities).
  - ATM layer which attaches an ATM header to each SAR-PDU to create an ATM-SDU (Service Data Unit). The same process is performed in the reverse order by the AIT card when transforming cells to frames.

Figure 22-8 Protocol Stack Operation



BTM Control Mapping: Frames and Cells

In addition to performing DLCI to PVC/VCC conversion, the network interworking feature provided by the BTM in the IGX switch maps cell loss priority, congestion information, and management information between Frame Relay and ATM formats as follows:

Cell Loss Priority, Frame Relay to ATM Direction

Each Frame Relay to ATM network interworking connection can be configured as one of the DE to CLP mapping choices:

- The DE bit in the Frame Relay frame is mapped to the CLP bit of every ATM cell generated by the segmentation process.

These 2 choices are not available on IGX switch NIW (network interworking):

- CLP is always 0.
- CLP is always 1.

Cell Loss Priority, ATM to Frame Relay Direction

Each Frame Relay to ATM network interworking connection can be configured as one of the CLP to DE mapping choices:

- If one or more ATM cells belonging to a frame has its CLP field set, the DE field of the Frame Relay frame will be set.

This choice is not available:

- Choosing no mapping from CLP to DE.

Congestion Indication, Frame Relay to ATM direction

- EFCI is always set to 0.

Congestion Indication, ATM to Frame Relay Direction

- If the EFCI field in the last ATM cell of a segmented frame is set, then FECN of the Frame Relay frame will be set.

For PVC Status Management

The AIT/BTM does convert OAM cells to OAM fastpackets, and vice-versa, including the AIS OAM. Also, “Abit” status is now propagated via software messaging.

The ATM layer and Frame Relay PVC Status Management can operate independently. The PVC status from the ATM layer will be used when determining the status of the FR PVCs. However, no direct actions of mapping LMI Abit to OAM AIS will be performed.

OAM Cells

OAM cell processing:

- F5 OAM loopback
- AIS
- FERF
- Cisco WAN switching Internal OAM

ATF Features

- Interworking: ATM to Frame Relay connections
- Connection Statistics
- Round Trip Delay measurements incorporated into the ForeSight algorithm
- Frame Based GCRA (FGCRA). This is an enhancement of the Generic Cell Rate Algorithm
- IBS (Initial Burst Size)
- **cnfportq**: 3 egress port queues are configurable Cbr, Vbr and Vbr w/Foresight. (Queue Bin numbers and algorithm types are NOT user selectable.)
- BCM (Backward Congestion Messages)
- ILMI and associated configuration options and statistics
- Loopback functions: **tstdly**, **tstconseg**, **addrmtlp**, **addloclp**
- Selftest/ Background tests
- OAM flows: AIS, FERF, OAM loopback
- End-to-end status updates (per FR/ATM interworking)
- Annex G and associated configuration options and statistics

ATF Limitations

- Priority Bumping is not supported across the interface shelves, but is supported across the routing network.
- Statistical Line Alarms per Software Functional Specification (that is, Bellcore standards).
- Programmable Opti Class: although 4 connection classes are supported: Cbr, Vbr, Vbr with Foresight, ATF, and ATF with ForeSight. Configuration of egress port queues and BNI trunk queues for these connection classes is available.
- Port loopback **tstport**
- Test **tstcon** is not supported at BPX switch endpoints.
- Gateway terminated inter-domain connections

ATF Connection Criteria

ATF connections are allowed between any combination of ATM and Frame Relay UNI and NNI ports. Virtual circuit connections are allowed. Virtual path connections are not.

ATF connections can be mastered by the IGX switch or BPX switch end.

ATF bundled connections and ATF point-to-point connections are not supported.

ATF connections use the Frame Relay trunk queues: bursty data A for non-ForeSight, bursty data B for ForeSight.

Bandwidth related parameters are defined using cells per second (cps) on the BPX switch and bits per second (bps) on the IGX switch. On a given endpoint node, the bandwidth parms for both ends of the ATF connection are changed/displayed using this end’s units. This saves you from having to convert from cps to bps repeatedly.

ATF with ForeSight connections use the Abr egress queue.

ATF Connection Management

Use these commands to provision and modify ATF connections:

- **addcon**
- **cnfcls**
- **cnfcon**
- **delcon**
- **dspcls**
- **dspcon**
- **dspcons**

Structure

- **NNI**
  The NNI format supports a 12-bit VPI. Abit status changes are passed to the remote end of the connection.
- **ILMI**
  The ILMI MIB and protocol was implemented in release 7.2. The additional support in consists of an activation and configuration interface, collection of statistics, and end-to-end status updates
- **LMI Annex G**
  The LMI Annex G protocol was implemented in release 7.2. The additional support consists of an activation and configuration interface, collection of statistics, and end-to-end status updates.
- **Port egress queue configuration**
  You can configure each of the pre-defined port egress queues. These queues consist of Cbr, Vbr, and Vbr with ForeSight (Abr). The configurable parameters are queue depth, EFCN threshold, and CLP thresholds.
- **Backward congestion management**
  Backward congestion management cells indicate congestion across the UNI or NNI. Transmission of these cells is enabled on a per-port basis. Software allows BCM to be configured on a UNI or NNI port for maximum flexibility should BCM over UNI be standards-defined.

Channel Statistics

Statistics are supported on a per-channel basis. A range of traffic and error statistics are available.

Channel statistics of these general types are supported:

- Cells received/transmitted, dropped, tagged as non-compliant or congested
- Cell errors
- AAL-5 frame counts, errors

Use these commands to configure and display channel statistics:

- **clrchstats**
- **cnfchstats**
- **dspchstats**
- **dspchstatcnf**
- **dspchstathist**

OAM Cell Support

OAM cells are detected and transmitted by firmware. System software displays alarm indications detected by the firmware. Additionally, loopbacks between the ATM-UNI and the ATM-CPE can be established. ForeSight round-trip delay cells are generated by firmware upon software request.

System software deals with these OAM cell flows:

- **End-to-End AIS/FERF**
  Software displays on a per-connection basis.
- **External segment loopbacks**
  Software initiates loopback of ATM-CPE via user command. The SAR creates the loopback OAM cell. External loopback cells received from the ATM-CPE are processed by the SAR.
- **Internal ForeSight round trip delay**
  Measures the RTD excluding trunk queueing delay on each ForeSight connection. Software displays the result.
- **Internal loopback round trip delay**
  Measures the RTD including trunk queueing delay on each ForeSight connection. Software displays the result.
- **Internal Remote Endpoint Status**
  These cells are generated by one end of a connection due to remote network connection failure (Abit = 0). The other end detects these cells and reports the connection status to software, which displays it.

These commands are associated with OAM cell status changes:

- **dspalms**
- **dspcon**
- **dspport**
- **tstconseg**
- **tstdly**

Diagnostics

Loopbacks

- Local loopbacks loop data back to the local ATM-TE, via the local BPX switch. Remote loopbacks loop data back to the local ATM-TE, via the whole connection route up to and including the remote terminating card.
- Local and remote connection loopbacks, and local port loopbacks, are destructive.

Card Tests

Connection Tests

- The **tstcon** command is not supported. The **tstdly** command is used for connection continuity testing.

Commands

These commands are associated with diagnostics changes:

- **addloclp**
- **addrmtlp**
- **cnftstparm**
- **dellp**
- **dspalms**
- **dspcd**
- **dspcds**
- **tstdly**

Virtual Circuit Features

The following virtual circuit features are supported:

- **Connection Groups**
  Connection groups are supported for BXM ATM Band interworking connection types, allowing termination of up to 5000 (grouped) virtual circuits per BPX switch. The connection grouping feature currently available on Frame Relay connections is expanded to include BXM ATM and interworking connections.
- **FGCRA**
  Frame-Based Generic Cell Rate Algorithm is a firmware feature that controls admission of cells to the network. It is configurable on a per-connection basis. It is a Cisco WAN switching enhancement of the ATM-UNI standard Generic Cell Rate Algorithm. System software allows configuration of FGCRA on a per-connection basis.
- **IBS**
  Initial Burst Size is an ATM bandwidth parameter that is used by firmware to allow short initial bursts, similar to the Cmax mechanism on the IGX switch. It is configurable on a per-connection basis.

- **Full VPI/VCI addressing range**
The entire range of VPI and VCI on both UNI and NNI interfaces is supported. For ATM-UNI, 8 bits of VPI and 16 bits of VCI are supported. For ATM-NNI, 12 bits of VPI and 16 bits of VCI are supported. In either case, VPC connections only pass through the lower 12 bits of the VCI field.
- **Connection Classes**
ATM and interworking connection classes are defined with appropriate bandwidth parameter defaults. These classes only apply at **addcon** time. They are templates to ease the task of configuring the large number of bandwidth parameters that exist per connection.

Commands

These commands are associated with virtual circuit feature changes:

- **addcon**
- **addcongrp**
- **cnfcon**
- **cnfatmcls**
- **delcon**
- **delcongrp**
- **dspatmcls**
- **dspcongrps**
- **grpcon**

Connection Management

Interworking connections may be added from either the BPX switch, the IGX switch, the MGX 8800, or the MGX 8220. Intra- and inter-domain interworking connections are supported.

Connection configuration parameters are endpoint-specific. Thus, the ATM-only parameters are only configurable on the BPX switch end. The IGX switch does not know about these parameters, so they cannot be configured or displayed at the IGX switch end. Parameter units are endpoint-specific also. Units on the BPX switch are cells per second, units on the IGX switch are bits per second.

Bundled interworking connections are not supported.

Virtual path interworking connections are not supported.

Because the NNI cell format has 12 bits for the VPI, the command **addcon** allows specification of VPI 0–4095 on NNI ports.

Routing

Interworking connections use the complex gateway feature of the AIT trunk card to repackage data from frames to ATM cells, and vice-versa. All BPX switch-IGX switch hops these connections route over must provide the complex gateway function.

IGX-to-IGX hops (Frame Relay connections) can be any trunk card type. This requirement simplifies the routing mechanism when dealing with structured networks, because software does not know the type of trunks in remote domains.

Bandwidth Management

Bandwidth calculations for interworking connections assume a large frame size, which minimizes the loading inefficiency of packets vs. cells. In other words, the translation between packets and cells assumes 100 percent efficiency, so the conversion is simply based on 20 payload bytes per fastpacket versus 48 payload bytes per ATM cell.

This mechanism keeps the fastpacket/cell conversion consistent with the bits per second/cells per second conversion. Thus, conversion of endpoint rates to trunk loading is straightforward.

User Interface

ATM connection classes are added for convenience. Classes can be configured as interworking or regular ATM. The **cnfcls** command is used to configure a class. The class is specified as part of the **addcon** command. ATM connection classes are maintained on all BPX switch.

A special ATM class is defined as the default interworking class. When an interworking connection is added from the Frame Relay end, the ATM-only parameters for this connection are taken from this default class.

Network-wide ForeSight parameters are supported for the Frame Relay end of interworking connections. The **cnffstparm** command is used to configure these parameters. Since the ATM end of interworking connections has per-virtual circuit ForeSight parameter configurability, the network-wide ForeSight parameters do not apply.

Note that the default ATM ForeSight parameters will match the default Frame Relay ForeSight parameters, with appropriate units conversion.

Port Management

The **cnfport** command supports these features:

- A UNI or NNI port can be configured to transmit Backwards Congestion Messages (BCM) to indicate congestion to the foreign ATM network.
- AUNI or NNI port can be configured for LMI, ILMI or no local management.

The **cnfportq** command supports configuration of queue depth, EFCN threshold, and CLP thresholds for all port egress queues (Cbr, Vbr, Vbr with ForeSight).

Signaling

System software supports these LMI/ILMI signaling actions:

- Internal network failure: software informs LMI/ILMI to set Abit = 0 for failed connections.
- Port failure/LMI Comm Failure: software informs remote nodes terminating all affected connections. Remote node BCC informs LMI/ILMI to set Abit = 0.
- LMI A = 0: software polls ILMI agent periodically for Abit status. Status changes are reflected in the **dspcon** screen.

Alarms

Abit = 0 on an NNI port causes declaration of a minor alarm. The d**spcon**, **dspcons**, and **dspalms** screens show this failure.

CHAPTER 23

Configuring BXM Virtual Switch Interface

This chapter describes the BXM Virtual Switch Interface (VSI) and provides configuration procedures:

- Virtual Switch Interface
- VSI Configuration Procedures
  - Add a controller
  - View controllers and interfaces
  - Delete a controller
  - Enable VSI ILMI functionality
  - Configure partition resources on VSI
- Overview: How VSI Works
  - VSI Masters and Slaves
  - Partitioning
- VSI Master and Slave Redundancy
- Class of Service Templates and Qbins
  - Tables of template default settings
- Summary of VSI Commands

For information on configuring SES PNNI controllers to work with BPX switches, refer to the *Cisco SES PNNI Controller Software Configuration Guide*.

For information on configuring MPLS controllers to work with BPX switches, refer to the *Cisco MPLS Controller Software Configuration Guide*.

Refer to *Cisco WAN Switching Command Reference* for details about the commands mentioned here for both PNNI and MPLS controllers. Refer to *Release Notes* for supported features.

Virtual Switch Interface

The Virtual Switch Interface (VSI) is a common control interface between the BPX 8650 or the MGX 8850 switches and an external controller that supports the VSI protocol.

VSIs allows a node to be controlled by multiple controllers, such as Multiprotocol Label Switching (MPLS) and the Service Expansion Shelf Private Network-to-Network Interface (SES PNNI).

When a VSI is activated on a port, trunk, or virtual trunk so that it can be used by a master controller, such as an 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 VSI provides a mechanism for networking applications to control the switch and use a partition of the switch resources.

VSI on the BPX provides:

- Class of Service templates
- Virtual trunk support for VSI
- Support for VSI master redundancy
- Multiple VSI partitions
- Soft and Dynamic Partitioning
- SV+ support for VSI

Multiple Partitioning

VSI was implemented first on the BPX 8650 in Release 9.1, which uses VSI to perform Multiprotocol Label Switching and allowed support for VSI on BXM cards and for partitioning BXM resources between Automatic Routing Management and a VSI MPLS controller. BPX software uses a partition to identify and assign resources such as LCNs, VPIs, and bandwidth to a controller. Multiple VSI partitions may be defined on a single physical port.

BPX Release 9.2 supports up to three VSI partitions in addition to Automatic Routing Management. The VSI partitions are controlled by VSI Masters such as the PNNI or MPLS controllers. When configuring, allocate switch resources to Automatic Routing Management and VSI slaves. Resources allocated to Automatic Routing Management and then reallocated to VSI.

Release 9.3.10 introduces Soft Partitioning and Dynamic Partitioning in order to support the smooth introduction of another VSI controller into a BPX network already configured with an existing VSI controller, easier tuning of switch resources, and the migration of Automatic Routing Management to PNNI (see the section Soft and Dynamic Partitioning later in this chapter).

Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS, previously called Tag Switching) enables routers at the edge of a network to apply simple labels to packets (frames), allowing devices in the network core to switch packets according to these labels with minimal lookup activity. MPLS in the network core can be performed by switches, such as ATM switches, or by existing routers.

MPLS integrates virtual circuit switching with IP routing to offer scalable IP networks over ATM. MPLS support data, voice, and multimedia service over ATM networks. MPLS summarizes routing decisions so that switches can perform IP forwarding, as well as bringing other benefits that apply even when MPLS is used in router-only networks.

Using MPLS techniques, it is possible to set up explicit routes for data flows that are constrained by path, resource availability, and requested Quality of Service (QoS). MPLS also facilitates highly scalable Virtual Private Networks.

MPLS assigns labels to IP flows, placing them in the IP frames. The frames can then be transported across packet or cell-based networks and switched on the labels rather than being routed using IP address look-up.

A routing protocol such as OSPF, uses the Label Distribution Protocol (LDP) to set up MPLS virtual connections (VCs) on the switch.

MPLS Terminology

MPLS is a standardized version of Cisco's original Tag Switching proposal. MPLS and Tag Switching are identical in principle and nearly so in operation. MPLS terminology has replaced obsolete Tag Switching terminology.

An exception to the terminology is Tag Distribution Protocol (TDP). TDP and the MPLS Label Distribution Protocol (LDP) are nearly identical, but use different message formats and procedures. TDP is used in this design guide only when it is important to distinguish TDP from LDP. Otherwise, any reference to LDP in this design guide also applies to TDP.

VSI Configuration Procedures

In the VSI control model, a controller sees the switch as a collection of slaves with their interfaces. The controller can establish connections between any two interfaces. The controller uses resources allocated to its partition.

Each VSI interface can be assigned a default Class of Service template upon activation. Use the switch software CLI or Cisco WAN Manager to configure a different template to an interface.

The procedure for adding a VSI-based controller such as the MPLS controller to the BPX is similar to adding an MGX 8220 interface shelf to the BPX. To attach a controller to a node to control the node, use the **addshelf** command.

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.

To configure VSI resources on a given interface, use the **cnfrsrc** command.

This section provides the basic procedures to:

- Add a controller
- View controllers and interfaces
- Delete a controller
- Enable VSI ILMI functionality
- Configure partition resources on VSI

Adding a Controller

To add an MPLS controller to any BXM trunk, use the **addshelf** command with the V (VSI) option.

To add an SES PNNI controller, use the **addshelf** command with an X option.

To identify VSI controllers and distinguish them from feeders, use the V (VSI) option of the **addshelf** command.

To add a SES PNNI controller to a BPX node through an AAL5 interface shelf or feeder type configured with VSI controller capabilities, use the **addctrlr** command.

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.

To add an MPLS controller (or a generic VSI controller that does not need AnnexG protocol):

Step 1 Up the trunk by using the **uptrk** command.

Step 2 Add an MPLS controller by using the **addshelf** command with feeder type set to "V".

Step 3 Display the controllers and interface shelves attached to the node by using the **dspnode** command.

Step 4 Display the VSI controllers on a BPX node by using the **dspctrlrs** command.

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 these commands:

Step 1 Up a trunk interface by using the **uptrk** command.

Step 2 Configure resource on the trunk interface for the PNNI controller's control channels by using the **cnfrsrc** command.

Step 3 Add the SES PNNI to the BPX and enable AnnexG protocol to run between the BPX and the SES by using the **addshelf** command with feeder type set to "X".

Step 4 Enable the VSI capabilities on the trunk interface by using the **addctrlr** command.

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 Multiprotocol Label Switching (MPLS) controller serving as an interface shelf is LSC.

In Release 9.3.10, the external network management system can query the BPX via SNMP to discover VSI controller IDs and IP addresses.

Deleting a Controller

To delete a controller or interface (feeder) shelf, first delete it from the network. Then down the port and trunk. This applies to MPLS controllers or generic VSI controllers that do not need AnnexG protocols.

To delete an MPLS controller:

Step 1 Delete an MPLS controller from a BPX node by using the **delshelf** command.

Step 2 Down the port by using the **dnport** command.

OR:

Step 3 Down the trunk by using the **dntrk** command.

To delete a PNNI controller:

Step 1 Delete the VSI capabilities on the trunk interface by using the **delctrlr** command.

Step 2 Delete the SES attached to the trunk interface by using the **delshelf** command.

Step 3 Disable the VSI resource partition allocated for PNNI controller on the trunk interface by using the **cnfrsrc** command.

Step 4 Down the trunk interface (provided no other VSI partitions are active on the trunk interface) by using the **dntrk** command.

Configuring Partition Resources on Interfaces

This section is key for configuring VSIs.

Prior to Release 9.1, LCNs, VPI range, and bandwidth allocation were managed exclusively by the BCC. With the introduction of VSI, the switch must allocate a range of LCNs, VPIs, and how much bandwidth for use by VSI (not BXM).

When configuring resource partitions on a VSI interface, the following commands are typically used:

- **cnfrsrc**
- **dsprsrc**
- **dspvsipartinfo**
- **dspvsipartcnf**
- **uptrk**
- **upln**
- **upport**

The next step to complete when adding a VSI-based controller such as an LSC or a PNNI controller is to configure resource partitions on BXM interfaces to allow the controller to control the BXM interfaces. To do this, first create resource partitions on these interfaces. Use the **cnfrsrc** command to add, delete and modify a partition on a specified interface.

You may have up to three 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 23-1 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 23-1 cnfrsrc Parameters, Ranges/Values, and Descriptions

Parameter (Object) Name	Range/Values	Default	Description
VSI partition	1–3	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	Minimum 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
PVC VPI Range 1	0–4095	-1	Dynamic partitioning
PVC VPI Range 2	0–4095	-1	Dynamic partitioning
PVC VPI Range 3	0–4095	-1	Dynamic partitioning
PVC VPI Range 4	0–4095	-1	Dynamic partitioning

Soft and Dynamic Partitioning

Soft and Dynamic Partitioning (new in Release 9.3.10) supports smooth introduction of another VSI controller into an existing BPX network already configured with an existing VSI controller, easier tuning of switch resources, and the migration of Automatic Routing Management to PNNI.

Soft Partitioning provides resource guarantees for LCNs and bandwidth per partition and a pool of resources available to all partitions in addition to the guaranteed resources. Dynamic Partitioning provides the ability to rather easily increase the allocation of a resource to a partition.

Define and manage the number of LCNs assigned to a given VSI partition by modifying the “Minimum VSI LCNs” and “Maximum VSI LCNs” fields of the **cnfrsrc** CLI command.

To give more LCNs from Automatic Routing Management to VSI, change the Min LCNs or Max LCNs to cause BPX software to produce a bigger number.

To increase the LCNs reserved to a VSI partition, increase the “Minimum VSI LCNs” or “Maximum VSI LCNs” fields of the appropriate VSI partition. The VSI LCN boundary is moved into Automatic Routing Management if there are enough free Automatic Routing Management LCNs to fulfill the request.

If there are not enough free LCNs in the Automatic Routing Management (AR) space, the **cnfrsrc** command does not fulfill a request to increase the VSI LCN space. In such a case, the **cnfrsrc** command displays a failure message showing the number of currently free AR LCNs. You can reissue the **cnfrsrc** command specifying a smaller increase to the VSI partition. If that is not acceptable, you must first delete and reroute the necessary number of AR connections. Then you can attempt **cnfrsrc** again.

Moving the VSI LCN boundary into the Automatic Routing Management space might step over LCNs that are currently allocated. BPX software reprogram the necessary channels so that new channels out of the lower AR LCN space are picked instead. Before starting the process of reprogramming the necessary number of AR connections, the **cnfrsrc** command displays a warning message and waits for your permission to proceed. The warning message shows the number of Automatic Routing Management (AR) connections that will be reprogrammed. After reprogramming the necessary channels the LCN boundary is moved into the Automatic Routing Management space.

Note You can migrate Automatic Routing Management (AutoRoute) connections only if the VPI range of the recipient VSI partition is adjacent to Automatic Routing Management. To migrate Automatic Routing Management connections to a nonadjacent VSI partition requires different VPIs within the recipient VPI boundary.

Assigning a Service Template to an Interface

The ATM Class of Service templates (or Service Class Template, SCT) provide a means of mapping a set of extended parameters. These are generally platform specific, based on the set of standard ATM parameters passed to the VSI slave in a BXM port interface during initial setup of the interface.

A set of service templates is stored in each BPX 8650 switch and downloaded to the service modules (BXMs) as needed during initial configuration of the VSI interface when a trunk or line is enabled on the BXM.

Each service template type has an associated Qbin. The Qbins provide the ability to manage bandwidth by temporarily storing cells and then serving them out based on a number of factors, including bandwidth availability and the relative priority of different Classes of Service.

When ATM cells arrive from the Edge LSR at the BXM port with one of four CoS labels, they receive CoS handling based on that label. A table look-up is performed, and the cells are processed, based on their connection classification. Based on its label, a cell receives the ATM differentiated service associated with its template type and service type (for example, label cos2 bw), plus associated Qbin characteristics and other associated ATM parameters.

A default service template is automatically assigned to a logical interface (VI) when you up the interface by using the commands **upport** and **uptrk**. The corresponding Qbin template is then copied into the card’s (BXM) data structure of that interface.

Following are some examples of assigning a default service template by using the commands **upport** and **uptrk**:

- **uptrk 1.1**
- **uptrk 1.1.1 (virtual trunk)**
- **upport 1.1**

This default template has the identifier of 1. To change the service template from service template 1 to another service template, use the **cnfvsiif** command.

To assign a selected service template to an interface (VI) use the **cnfvsiif** command, specifying the template number. It has this syntax:

cnfvsiif <slot.port.vtrk> <tmplt_id>

For example:

```
cnfvsiif 1.1 2
cnfvsiif 1.1.1 2
```

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>

```
dspvsiif 1.1
dspvsiif 1.1.1
```

To change some of the template's Qbin parameters, use the **cnfqbin** command. The Qbin is now "user configured" as opposed to "template configured."

To view this information, use the command **dspqbin**.

SCT Commands

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.

Configuring the BXM Card's Qbin

When you activate an interface by using an **uptrk** or **upport** command, a default service template (MPLS1) is automatically assigned to that interface. The corresponding Qbin templates are simultaneously set up in the BXM's data structure for that interface. This service template has an identifier of "1".

To change the service template assigned to an interface, use the **cnfvsiif** command. You can do this only when there are no active VSI connections on the BXM.

To display the assigned templates, use the **dspvsiif** command.

Each template table row includes an entry that defines the Qbin to be used for that Class of Service (see Figure 23-10).

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.

Once a service template has been assigned, 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 affect only that interface's Qbin configuration. Your changes do not affect the Qbin template assigned to that interface.

To change the template's configuration of the interface, provide new values by 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.

To see the Qbin's default service type and the Qbin number, execute the **dspsct** command.

Use the following commands to configure Qbins:

- **cnfqbin**
- **dspqbin**
- **dspqbint**

Enabling VSI ILMI Functionality for the PNNI Controller

You can enable VSI ILMI functionality both on line (port) interfaces and trunk interfaces when using PNNI. 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 Up a line interface by using the **upln** command.

Step 2 Up the port interface by using the **upport** command.

Step 3 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 of the **cnfport** command.

Step 4 Configure a VSI partition on the line interface by using the **cnfrsrc** command.

Step 5 Enable VSI ILMI functionality for the VSI partition by using the **cnfvsipart** command.

To enable VSI ILMI functionality on physical trunk interfaces:

Step 1 Up a physical trunk by using the **uptrk** command.

Step 2 Configure the trunk to enable ILMI protocol to run on the BXM card by enabling the "Protocol by the card" option of the **cnftrk** command.

Step 3 Configure a VSI partition on the trunk interface by using the **cnfrsrc** command.

Step 4 Enable VSI ILMI session for the VSI partition by using the **cnfvsipart** command.

To enable VSI ILMI functionality on virtual trunk interfaces:

Step 1 Up a virtual trunk by using the **uptrk** command.

Step 2 Configure the trunk VPI by using the **cnftrk** command. (The ILMI automatically runs on the BXM card for virtual trunks.) This is not configurable by using the **cnftrk** command.

Step 3 Configure a VSI partition on the virtual trunk interface by using the **cnfrsrc** command.

Step 4 Enable VSI ILMI functionality for the VSI partition by using the **cnfvsipart** command.

Note VSI ILMI can be enabled for only one VSI partition on the trunk interface.

To display VSI ILMI functionality on interfaces:

- Display VSI ILMI status (whether enabled or not) for various VSI partitions on the interface by using the **dspvsipartcnf** command.

VSIs and Virtual Trunking

The VSI virtual trunking feature lets you use BXM virtual trunks as VSI interfaces. Using this capability, VSI master controllers can terminate connections on virtual trunk interfaces.

Activate and configure VSI resources on a virtual trunk using the same commands you use to configure physical interfaces (for example, **cnfrsrc**, **dsprsrc**). The syntax used to identify a trunk has an optional virtual trunk identifier that you append to the slot and port information to identify virtual trunk interfaces.

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 might not contain any VPCs.

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.

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.

Once VSI is enabled on the virtual trunk, Automatic Routing Management does not include this trunk in its route selection process.

To configure a VSI virtual trunk:

Step 1 Activate the virtual trunk by using the command
uptrk <slot.port.vtrunk>

Step 2 Set up VPI value and trunk parameters by using the command
cnftrk <slot.port.vtrunk>

Step 3 Enable VSI partition by using the command
cnfrsrc <slot.port.vtrunk>

Overview: How VSI Works

This section provides detailed reference to virtual interfaces, service templates, and Qbins.

For information on configuring SES PNNI controllers to work with BPX switches, see the *Cisco SES PNNI Controller Software Configuration Guide*.

For information on configuring MPLS controllers to work with BPX switches, see the *Cisco MPLS Controller Software Configuration Guide*.

Refer to *Cisco WAN Switching Command Reference* for details about the commands mentioned here for both PNNI and MPLS controllers. Refer to *Release Notes* for supported features.

Virtual Switch Interfaces and Qbins

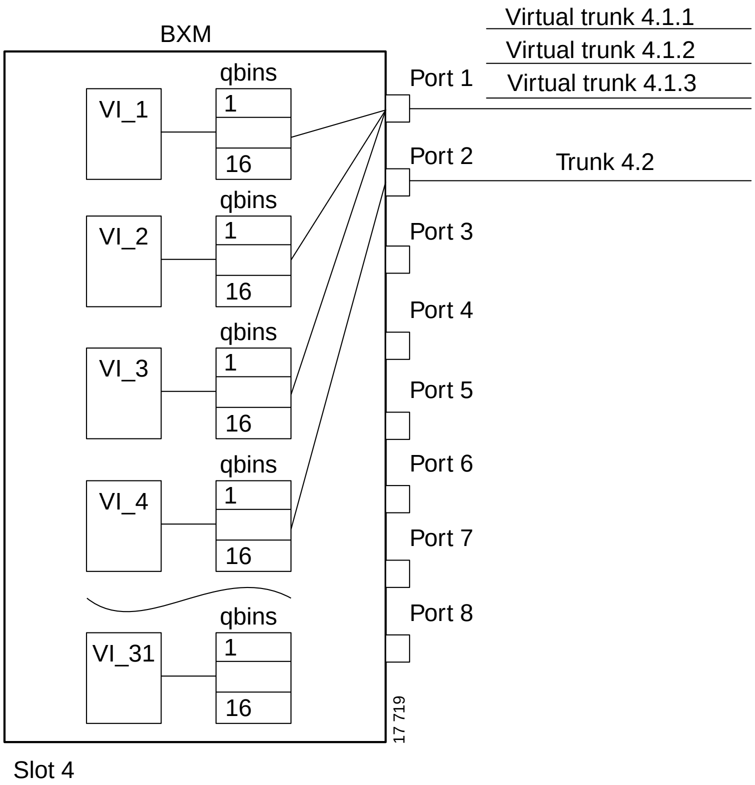
The BXM supports 31 Virtual Switch Interfaces that provide a number of resources including Qbin buffering capability. One Virtual Switch Interface is assigned to each logical trunk (physical or virtual) when the trunk is enabled. (See Figure 23-1.)

Each virtual switch interface has 16 Qbins assigned to it. Qbins 0-9 are used for Automatic Routing Management. Qbins 10 through 15 are available for use by a Virtual Switch Interface. (In Release 9.1, only Qbin 10 was used.) The Qbins 10 through 15 support Class of Service (CoS) templates on the BPX.

You may enable a Virtual Switch Interface on a port, trunk, or virtual trunk. The Virtual Switch Interface is assigned the resources of the associated virtual interface.

With virtual trunking, a physical trunk can comprise a number of logical trunks called virtual trunks. Each of these virtual trunks (equivalent to a virtual interface) is assigned the resources of one of the 31 Virtual Switch Interfaces on a BXM (see Figure 23-1).

Figure 23-1 BXM Virtual Interfaces and Qbins



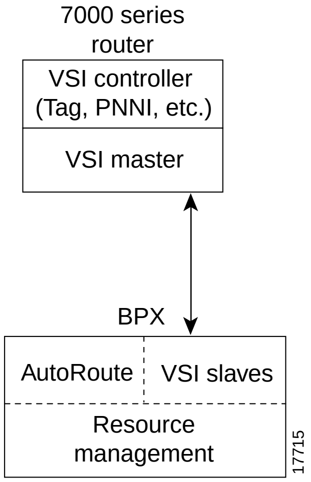
VSI Master and Slaves

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 (see Figure 23-2).

The controller sets up these types of connections:

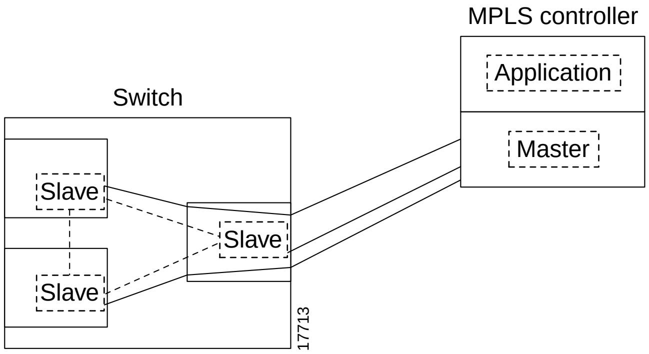
- Control virtual connections (VCs)
  - master to slave
  - slave to slave
- User Connection
  - User connection (that is, cross-connect)

Figure 23-2 VSI, Controller and Slave VSI



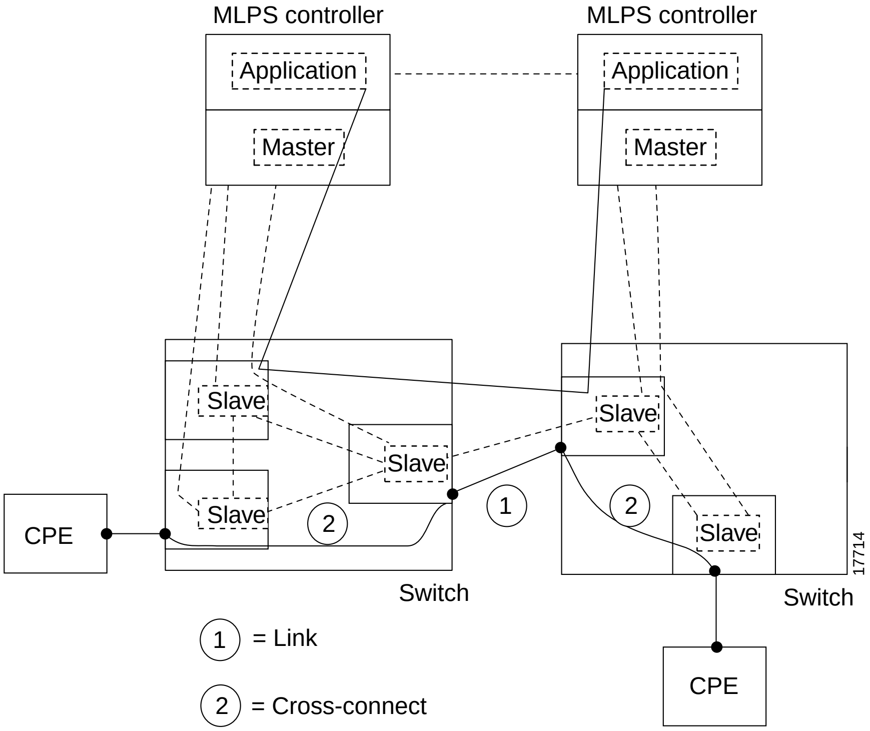
The controller establishes a link between the VSI master and every VSI slave on the associated switch. The slaves in turn establish links between each other (see Figure 23-3).

Figure 23-3 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 23-4.

Figure 23-4 Cross-Connects and Links between Switches



Connection Admission Control

When a connection request is received by the VSI slave, it is first subjected to a Connection Admission Control (CAC) process before being forwarded to the FW 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 MPLS 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.

Ingress traffic is managed differently and a pre-assigned ingress service template containing CoS Buffer links is used.

Partitioning

The Virtual Switch Interface must partition the resources between competing controllers, Automatic Routing Management, MPLS, and PNNI for example. You partition resources by using the **cnfrsrc** command.

Note Release 9.3 supports up to three partitions.

Table 23-2 shows the three resources that must be configured for a partition designated ifci, which stands for interface controller 1 in this instance.

Table 23-2 ifci Parameters (Virtual Switch Interface)

ifci parameters	Min	Max
lcns	min_lcnsi	max_lcnsi
bw	min_bwi	max_bwi
vpi	min_vpi	max_vpi

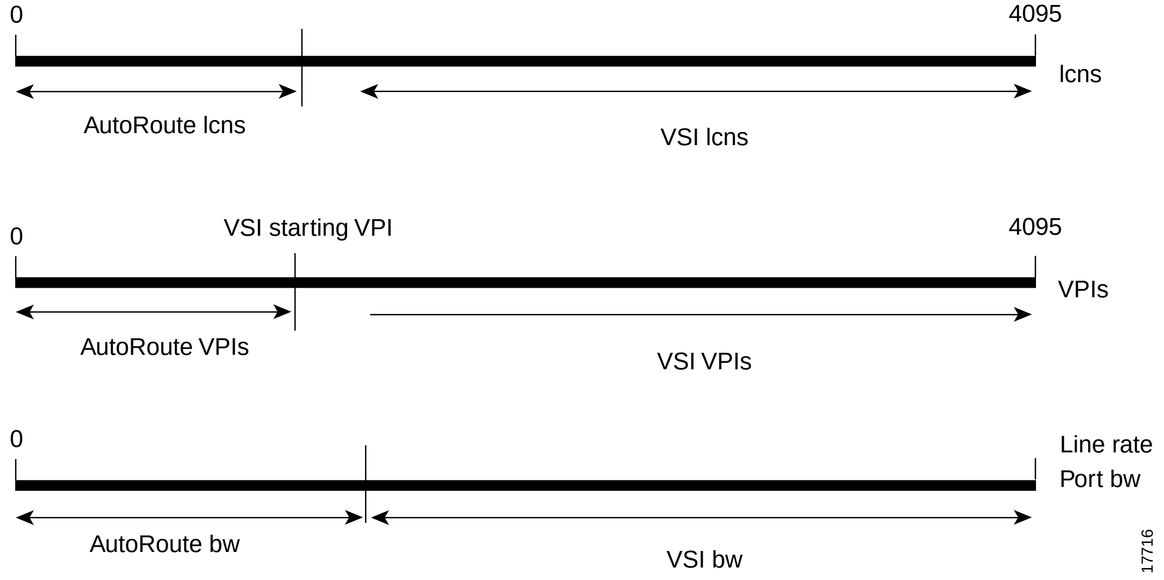
Some ranges of values available for a partition are listed in Table 23-3:

Table 23-3 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 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, use the **cnfrsrc** command on the BPX switch. A view of the resource partitioning available is shown in Figure 23-5.

Figure 23-5 Graphical View of Resource Partitioning, Automatic Routing Management, and VSI



Multiple Partitioning

You can configure partition resources between Automatic Routing Management PVCs and three VSI controllers (LSC or PNNI). Up to three 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. With Release 9.2.3, six new Service Class Templates were added for interfaces (for a total of nine) 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:

- Up to three VSI partitions are supported.
- Resources cannot be redistributed amongst different VSI partitions.
- The resources that are allocated to a partition: LCNS, Bandwidth and VPI range.
- Resources are also allocated to Automatic Routing Management. The resources allocated to Automatic Routing Management can be freed from Automatic Routing Management and then allocated to VSI.
- No multiple partitions on Virtual Trunks. A Virtual Trunk is managed by either Automatic Routing Management or by a single VSI partition.
- Only one VSI controller can be added to a BPX interface. Other controllers must be added to different interfaces on the switch.

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 an 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 an associated set of resources.

Consider a BPX switch with 4 interfaces:

- 10.1
- 10.2.1
- 11.1
- 11.7.1

Also assume the resource partitioning in Table 23-4.

Figure 23-6 Virtual Switches

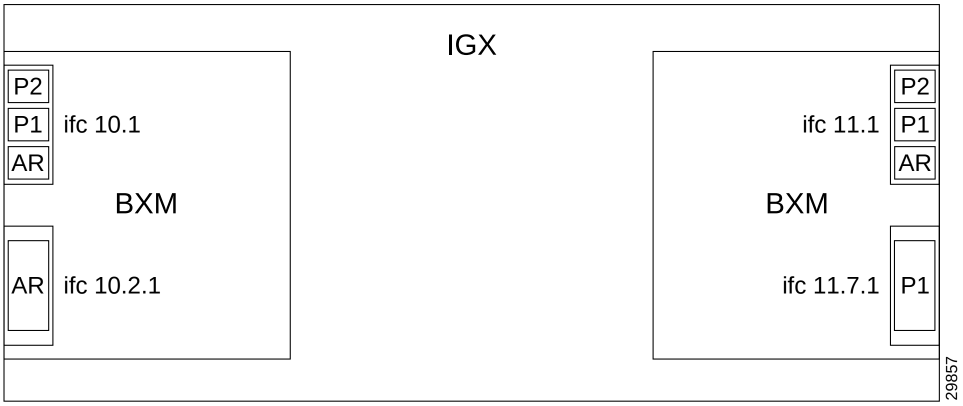


Table 23-4 Partitioning Example

Interface	Automatic Routing Management	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:

- Automatic Routing Management:
  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 these parameters on a VSI partition on an interface:

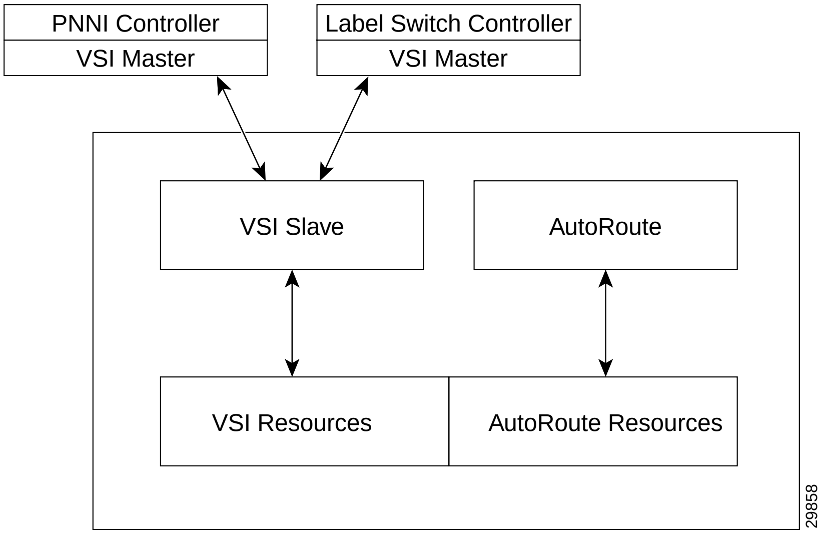
- **min lcn**: guaranteed LCNs for the partition on the interface.
- **max lcn**: total number of LCNs the partition is allowed for setting up connections on the interface.
- **min bw**: guaranteed bandwidth for the partition on the interface.
- **max bw**: maximum bandwidth for this partition on the 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 Automatic Routing Management and VSI

In addition to partitioning of resources between VSI and Automatic Routing Management, multiple partitioning allows subpartitioning of the VSI space among multiple VSI partitions. Multiple VSI controllers can share the switch with each other and also with Automatic Routing Management.

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 Automatic Routing Management resources remains the province of the switch software.

Figure 23-7 Resource Partitioning Between Automatic Routing Management 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 interslave channels and master-slave controllers for all controllers in all partitions.

VSI Master and Slave Redundancy

The ability to have multiple VSI controllers is referred to as VSI master redundancy. Master redundancy 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**
  Both controllers can be active in a partition, and can control the resources simultaneously.
- **Exclusive redundancy**
  Only one controller is active at a time. It is up to the controllers to resolve which 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.

For illustrations of a VSI Master and Slave, see to Figure 23-3. For an illustration of a switch with redundant controllers that support master redundancy, see to Figure 23-8.

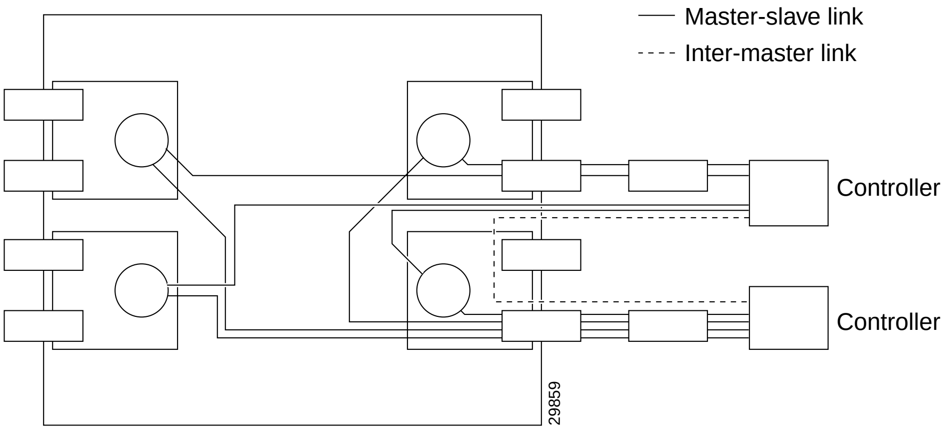
Switch software supports master redundancy in these ways:

- 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 intercontroller 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 intermaster channel through the switch.

Figure 23-8 below shows a switch with redundant controllers and the connectivity required to support master redundancy.

Figure 23-8 Switch with Redundant Controllers to Support Master Redundancy



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.

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 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 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 feeders that can be attached to a BPX hub. The total number of interface shelves (feeders) and controllers is 16.

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.

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 bringup, 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.

The following sections describe some of the communication between the switch software and firmware to support VSI master and slave redundancy.

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. 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.

A maximum of two partitions are possible. 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 to 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.

What 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. 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 MPLS controllers to one partition, and one or more redundant PNNI controllers 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.

Note The Controller ID for a PNNI controller must be 2.

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 by using 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. These values are default. You can modify them by using the **addctrlr** command.

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 by 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 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 interslave 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 having been deleted. Only when a given partition is disabled will the slaves 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:

- interslave
- master-slave
- 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.

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 leg from the VSI master to the backplane, through the directly connected slave
- 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 that 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.

Because 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.

Also, when the standby slave VSI card is first started (either by having been inserted into the slot, or if you issue 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, these are the hot standby operations between active and standby card:

1. CommBus messages are duplicated to standby slave VSI card by the BCC.
   Operation 1 does not need to implement because it had been done 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.
   Operation 2 is normal data transferring, which occurs after both cards are in-sync.
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 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.

Class of Service Templates and Qbins

Class of Service Templates (COS Templates) provide a means of mapping a set of standard connection protocol parameters to “extended” platform-specific parameters. Full Quality of Service (QoS) implies that each VC is served through one of a number of Class of Service buffers (Qbins), which are differentiated by their QoS characteristics.

A Qbin template defines a default configuration for the set of Qbins for a logical interface. When you assign a template 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.

Qbin templates deal only with Qbins that are available to VSI partitions, which are 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.

How Service Class Templates Work

The Service Class templates provide a means of mapping a set of extended parameters, which are generally platform specific, based on the set of standard ATM parameters passed to the VSI slave during connection setup.

A set of service templates is stored in each switch (such as BPX) and downloaded to the service modules (such as BXMs) as needed.

The service templates contains two classes of data:

- Parameters necessary to establish a connection (that is, per VC), including entries such as UPC actions, various bandwidth-related items, per VC thresholds, and so on.
- Parameters necessary to configure the associated Class of Service buffers (Qbins) that provide QoS support.

The general types of parameters passed from a VSI Master to a Slave include:

- A service type identifier
- QoS parameters (CLR, CTD, CDV)
- Bandwidth parameters (such as 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 32-bit service type identifier. Current identifiers are for:

- ATM Forum service types
- Automatic Routing Management
- MPLS Switching

When a connection setup request is received from the VSI master in the Label Switch Controller, the VSI slave (in the BXM, for example) uses the service type identifier to index into a Service Class Template database containing extended parameter settings for connections matching that index. The slave uses these values to complete the connection setup and program the hardware.

One of the parameters specified for each service type is the particular BXM Class of Service buffer (Qbin) to use. The Qbin buffers provide separation of service type to match the QoS requirements.

Service templates on the BPX are maintained by the BCC and are downloaded to the BXM cards as part of the card configuration process for:

- Y-red card additions
- BCC (control card) switchovers
- Cards with active interfaces and that are reset (hardware reset)
- BCC (control card) rebuilds

The templates are nonconfigurable.

Structure of Service Class Templates

There are three types of templates:

- VSI Special Types
- ATMF Types
- MPLS Types

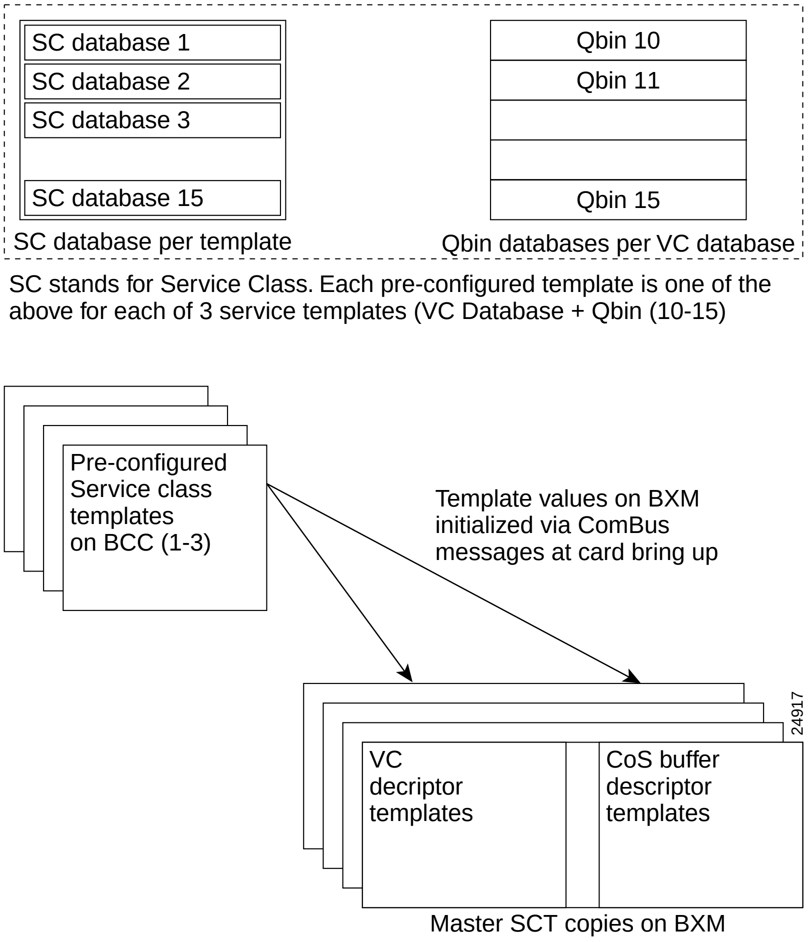
You can assign any one of the nine templates to a Virtual Switch Interface. (See Figure 23-9.)

Each template table row includes an entry that defines the Qbin to be used for that Class of Service. See Figure 23-9 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 23-9 Service Template Overview

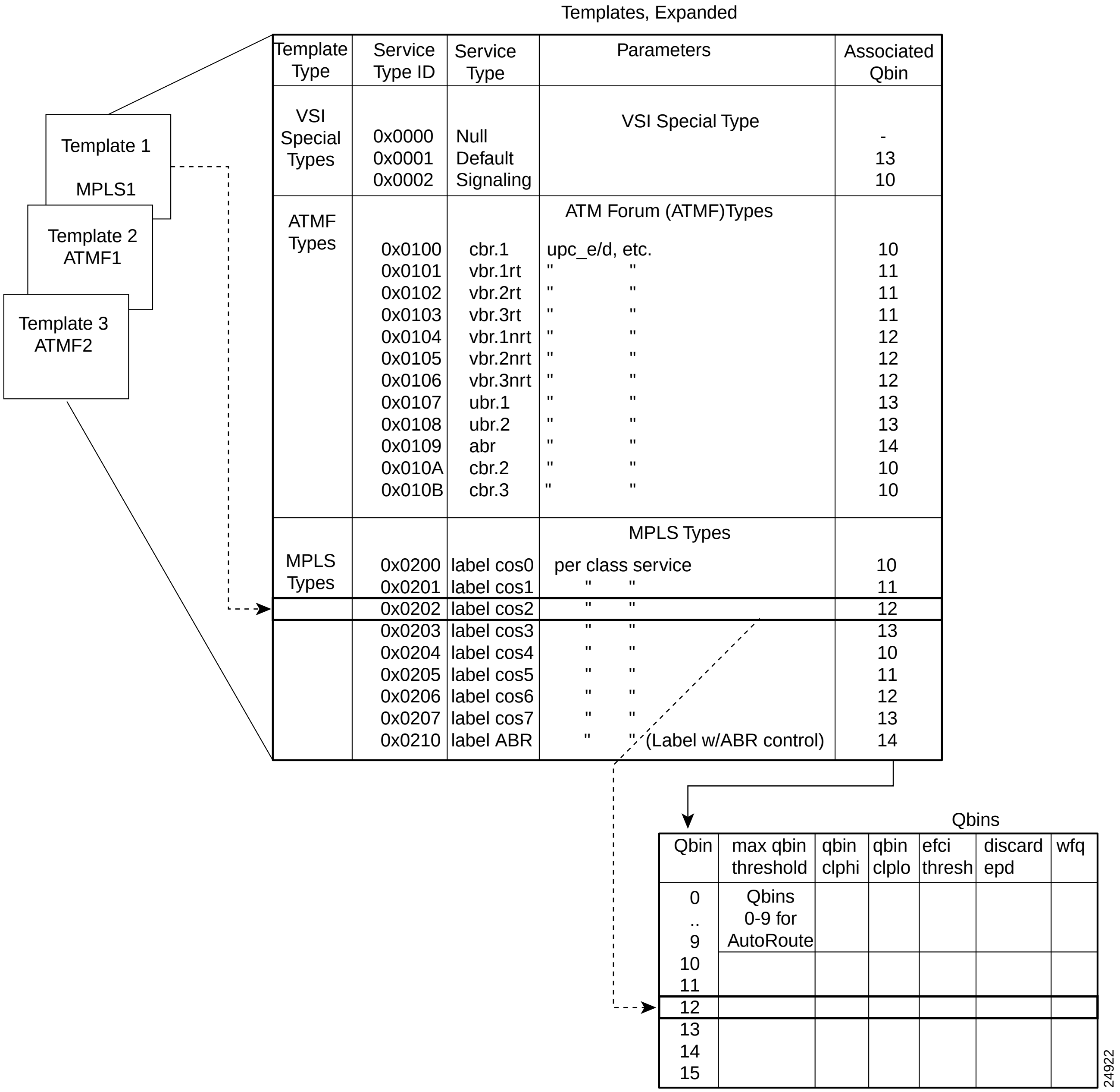


Qbin templates are used only with Qbins that are available to VSI partitions, specifically, Qbins 10 through 15. Qbins 10 through 15 are used by the VSI on interfaces configured as trunks or ports. The rest of the Qbins (0–9) are reserved for and configured by Automatic Routing Management.

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 23-10 Service Template and Associated Qbin Selection



Templates, Expanded

Template Type	Service Type ID	Service Type	Parameters	Associated Qbin
VSI Special Types			VSI Special Type	
	0x0000	Null		-
	0x0001	Default		13
	0x0002	Signaling		10
ATMF Types			ATM Forum (ATMF)Types	
	0x0100	cbr.1	upc_e/d, etc.	10
	0x0101	vbr.1rt	" "	11
	0x0102	vbr.2rt	" "	11
	0x0103	vbr.3rt	" "	11
	0x0104	vbr.1nrt	" "	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			MPLS Types	
	0x0200	label cos0	per class service	10
	0x0201	label cos1	" "	11
	0x0202	label cos2	" "	12
	0x0203	label cos3	" "	13
	0x0204	label cos4	" "	10
	0x0205	label cos5	" "	11
	0x0206	label cos6	" "	12
	0x0207	label cos7	" "	13
	0x0210	label ABR	" " (Label w/ABR control)	14

Qbins

Qbin	max qbin threshold	qbin clphi	qbin clplo	efci thresh	discard epd	wfq
0 .. 9	Qbins 0-9 for AutoRoute					
10 11						
12						
13 14 15						

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 23-5. A list of the supported service sub-categories is shown in LCNs.

Table 23-5 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.

There are three service types:

- VSI Special Type
- ATMF Types
- MPLS types

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 23-6.

Table 23-6 Service Category Listing

Template Type	Service Type Identifiers	Service Types	Associated Qbin
VSI Special Types	0x0000	Null	-
	0x0001	Default	13
	0x0002	Signaling	10
ATMF Types	0x0100	Cbr.1	10
	0x0101	Vbr.1-RT	11
	0x0102	Vbr.2-RT	11
	0x0103	Vbr.3-RT	11
	0x0104	Vbr.1-nRT	12
	0x0105	Vbr.2-nRT	12
	0x0106	Vbr.3-nRT	12
	0x0107	Ubr.1	13
	0x0108	Ubr.2	13
	0x0109	Abr	14
	0x010A	Cbr.2	10
	0x010B	Cbr.3	10
MPLS Types	0x0200	label cos0, per-class service	10
	0x0201	label cos1, per-class service	11
	0x0202	label cos2, per-class service	12
	0x0203	label cos3, per-class service	13
	0x0204	label cos4, per-class service	10
	0x0205	label cos5, per-class service	11
	0x0206	label cos6, per-class service	12
	0x0207	label cos7, per-class service	13
	0x0210	label Abr, (Tag w/ Abr flow control)	14

VC Descriptors

A summary of the parameters associated with each of the service templates is provided in Table 23-7 through Table 23-10. Table 23-11 provides a description of these parameters and also the range of values that may be configured if the template does not assign an arbitrary value.

Table 23-7 lists the parameters associated with Default (0x0001) and Signaling (0x0002) service template categories.

Table 23-7 VSI Special Service Types

Parameter	VSI Default (0x0001)	VSI Signalling (0x0002)
Qbin Number	10	15
UPC Enable	0	*
UPC CLP Selection	0	*
Policing Action (GCRA #1)	0	*
Policing Action (GCRA #2)	0	*
PCR	-	300 kbps
MCR	-	300 kbps
SCR	-	-
ICR	-	-
MBS	-	-
CoS Min BW	0	*
CoS Max BW	0	*
Scaling Class	3	3
CAC Treatment ID	1	1
VC Max Threshold	Q_max/4	*
VC CLPhi Threshold	75	*
VC CLPlo Threshold	30	*
VC EPD Threshold	90	*
VC EFCI Threshold	60	*
VC discard selection	0	*

Table 23-8 and Table 23-9 lists the parameters associated with the PNNI service templates.

Table 23-8 ATM Forum Service Types, Cbr, Ubr, and Abr

Parameter	Cbr.1	Cbr.2	Cbr.3	Ubr.1	Ubr.2	Abr
Qbin Number	10	10	10	13	13	14
UPC Enable	1	1	1	1	1	1
UPC CLP Selection	*	*	*	*	*	*
Policing Action (GCRA #1)	*	*	*	*	*	*
Policing Action (GCRA #2)	*	*	*	*	*	*
PCR						
MCR	-	-	-	*	*	*
SCR	-	-	-	50	50	*
ICR	-	-	-	-	-	*
MBS	-	-	-	-	-	*

Table 23-8 ATM Forum Service Types, Cbr, Ubr, and Abr (continued)

Parameter	Cbr.1	Cbr.2	Cbr.3	Ubr.1	Ubr.2	Abr
CoS Min BW	0	0	0	0	0	0
CoS Max BW	100	100	100	100	100	100
Scaling Class	*	*	*	*	*	*
CAC Treatment ID	*	*	*	*	*	*
VC Max Threshold	*	*	*	*	*	*
VC CLPhi Threshold	*	*	*	*	*	*
VC CLPlo Threshold	*	*	*	*	*	*
VC EPD Threshold	*	*	*	*	*	*
VC EFCI Threshold	*	*	*	*	*	*
VC discard selection	*	*	*	*	*	*
VSVD/FCES	-	-	-	-	-	*
ADTF	-	-	-	-	-	500
RDF	-	-	-	-	-	16
RIF	-	-	-	-	-	16
NRM	-	-	-	-	-	32
TRM	-	-	-	-	-	0
CDF						16
TBE	-	-	-	-	-	16777215
FRTT	-	-	-	-	-	*

Table 23-9 ATM Forum Vbr Service Types

Parameter	Vbrrt.1	Vbrrt.2	Vbrrt.3	Vbrnrt.1	Vbrnrt.2	Vbrnrt.3
Qbin Number	11	11	11	12	12	12
UPC Enable	1	1	1	1	1	1
UPC CLP Selection	*	*	*	*	*	*
Policing Action (GCRA #1)	*	*	*	*	*	*
Policing Action (GCRA #2)	*	*	*	*	*	*
PCR						
MCR	*	*	*	*	*	*
SCR	*	*	*	*	*	*
ICR	-	-	-	-	-	-
MBS	*	*	*	*	*	*
CoS Min BW	0	0	0	0	0	0
CoS Max BW	100	100	100	100	100	100
Scaling Class	*	*	*	*	*	*
CAC Treatment ID	*	*	*	*	*	*
VC Max Threshold	*	*	*	*	*	*
VC CLPhi Threshold	*	*	*	*	*	*
VC CLPlo Threshold	*	*	*	*	*	*
VC EPD Threshold	*	*	*	*	*	*
VC EFCI Threshold	*	*	*	*	*	*
VC discard selection	*	*	*	*	*	*

* indicates not applicable

Table 23-10 lists the connection parameters and their default values for label switching service templates.

Table 23-10 MPLS Service Types

Parameter	CoS 0/4	CoS 1/5	CoS 2/6	CoS3/7	Tag-Abr
Qbin #	10	11	12	13	14
UPC Enable	0	0	0	0	0
UPC CLP Selection	0	0	0	0	0
Policing Action (GCRA #1)	0	0	0	0	0
Policing Action (GCRA#2)	0	0	0	0	0
PCR	-	-	-	-	cr/10
MCR	-	-	-	-	0
SCR	-	-	-	-	P_max
ICR	-	-	-	-	100
MBS	-	-	-	-	-
CoS Min BW	0	0	0	0	0
CoS Max BW	0	0	0	0	100
Scaling Class	3	3	2	1	2
CAC Treatment	1	1	1	1	1
VC Max	Q_max/4	Q_max/4	Q_max/4	Q_max/4	cr/200ms
VC CLPhi	75	75	75	75	75
VC CLPlo	30	30	30	30	30
VC EPD	90	90	90	90	90
VC EFCI	60	60	60	60	30
VC discard selection	0	0	0	0	0
VSVD/FCES	-	-	-	-	0
ADTF	-	-	-	-	500
RDF	-	-	-	-	16
RIF	-	-	-	-	16
NRM	-	-	-	-	32
TRM	-	-	-	-	0
CDF	-	-	-	-	16
TBE	-	-	-	-	16777215
FRTT	-	-	-	-	0

VC Descriptor Parameters

Table 23-11 describes the connection parameters that are listed in the preceding tables and also lists the range of values that may be configured, if not already preconfigured.

Every Service Class does not include all parameters. For example, a Cbr service type have fewer parameters than an Abr service type.

Note Not every Service Class has a value defined for every parameter listed in Table 23-11 below.

Table 23-11 Connection Parameter Descriptions and Ranges

Object Name	Range/Values	Template Units
Qbin Number	10–15	Qbin #
Scaling Class	0–3	enumeration
CDVT	0–5M (5 sec)	secs
MBS	1–5M	cells
ICR	MCR–PCR	cells
MCR	50–LR	cells
SCR	MCR–LineRate	cells
UPC Enable	0–Disable GCRAs 1–Enabled GCRAs 2–Enable GCRA #1 3–Enable GCRA #2	enumeration
UPC CLP Selection	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	enumeration
Policing Action (GCRA #1)	0–Discard 1–Set CLP bit 2–Set CLP of untagged cells, disc. tagged cells	enumeration
Policing Action (GCRA #2)	0–Discard 1–Set CLP bit 2–Set CLP of untagged cells, disc. tagged cells	enumeration
VC Max		cells
CLP Lo	0–100	%Vc Max
CLP Hi	0–100	%Vc Max
EFCI	0–100	%Vc Max

Table 23-11 Connection Parameter Descriptions and Ranges (continued)

Object Name	Range/Values	Template Units
VC Discard Threshold Selection	0–CLP Hysteresis 1–EPD	enumeration
VSVD	0: None 1: VSVD 2: VSVD with external Segment	enumeration
Reduced Format ADTF	0–7	enumeration
Reduced Format Rate Decrease Factor (RRDF)	1–15	enumeration
Reduced Format Rate Increase Factor (RRIF)	1–15	enumeration
Reduced Format Time Between Fwd RM cells (RTrm)	0–7	enumeration
Cut-Off Number of RM Cells (CRM)	1–4095	cells

Qbin Dependencies

Qbin templates deal only 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.

The available Qbin parameters are shown in Table 23-12.

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 23-12 Service Template Qbn Parameters

Template Object Name	Template Units	Template Range/Values
Qbin Number	enumeration	0–15 (10–15 valid for VSI)
Max Qbin Threshold	msec	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 Hystersis 2–Frame Discard
Weighted Fair Queueing	enable/disable	0: Disable 1: Enable

Qbin Default Settings

The Qbin default settings are shown in Table 23-13. The Service Class Template default settings for Label Switch Controllers and PNNI controllers are shown in Table 23-14.

Note Templates 2, 4, 6, and 8 support policing on PPD.

Table 23-13 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

Table 23-13 Qbin Default Settings (continued)

Qbin	Max Qbin Threshold (usec)	CLP High	CLP Low/EPD	EFCI	Discard Selection
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
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 23-14 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	Hystersis
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 23-14 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 policier and CLP for 2nd policier 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 policier 1 and CLP for policier 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 23-14 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

Summary of VSI Commands

Table 23-15 Commands for Setting up a VSI (Virtual Switch Interface) Controller

Mnemonic	Description
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.
addshelf	Add a trunk between the hub node and interface shelf or VSI MPLS controller.)
cnfqbin	Configure Qbin card. If you answer Yes when prompted, the command will use the card Qbin values from the Qbin templates.
cnfrsrc	Configure resources, for example, for Automatic Routing Management PVCs and MPLS controller (LSC).

Table 23-15 Commands for Setting up a VSI (Virtual Switch Interface) Controller (continued)

Mnemonic	Description
cnfvsiif	Configure VSI Interface or a different template to an interface.
cnfvsipart	Configure VSI partition characteristics for VSI ILMI.
delctrlr	Delete a controller, such as a Service Expansion Shelf (SES) PNNI controller, from a BPX node.
delshelf	Delete a trunk between a hub node and access shelf.
dspcd	Display the card configuration.
dspchuse	Display a summary of channel distribution in a given slot.
dspctrlrs	Display the VSI controllers, such as an PNNI controller, on a BPX node.
dspqbin	Displays Qbin parameters currently configured for the virtual interface.
dspqbintmt	Display Qbin template.
dsprsrc	Display LSC resources.
dspsct	Display Service Class Template 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> SC lists all the parameters of that Service Class.
dspvsiif	Display VSI Interface.
dspvsipartcnf	Display information about VSI ILMI functionality.
dspvsipartinfo	Display VSI resource status for the trunk and partition.

CHAPTER 24

Configuring BXM Virtual Trunks

This chapter describes Broadband Switch Module (BXM) virtual trunks, a feature supported by the BXM cards beginning with switch software Release 9.2:

- Overview
- How Virtual Trunking Works
- Connection Management
- General Procedure to Set Up a Trunk
- Example: Virtual Trunk Across an ATM Network
- Command Overview
- Compatibility Between Cards in Virtual Trunks

Note: Virtual trunking is a purchased feature; Cisco Customer Service must enable it on each node where you intend to use virtual trunking.

Overview

Virtual trunking provides connectivity for Cisco switches through a public ATM cloud as shown in Figure 24-1. Because a number of virtual trunks can be configured across a physical trunk, virtual trunks provide a cost effective means of connecting across a public ATM network. Each virtual trunk typically uses only part of a physical trunk's resources. Yet, like regular trunks, virtual trunks can carry high-priority traffic.

The 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.

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.

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.

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 (see Figure 24-1). The virtual path ID (VPI) is provided by the ATM cloud administrator (for example, service provider).

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 (such as, 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.

There are two general types of virtual trunks:

- **Automatic Routing Management Virtual Trunks**
  These are PVP or SPVP connections that carry Automatic Routing Management PVC connections.
- **VSI Virtual Trunks**
  These are PVP or SPVP connections that carry MPLS or PNNI connections. VSI Virtual Trunks and MPLS Virtual Trunks differ in a number of ways including the way in which their endpoints are configured.

Typical ATM Hybrid Network with Virtual Trunks

With the BPX switch, you can set up virtual networks with either the Broadband Network Interface (BNI) card or with the BXM card. The virtual trunks originate and terminate on:

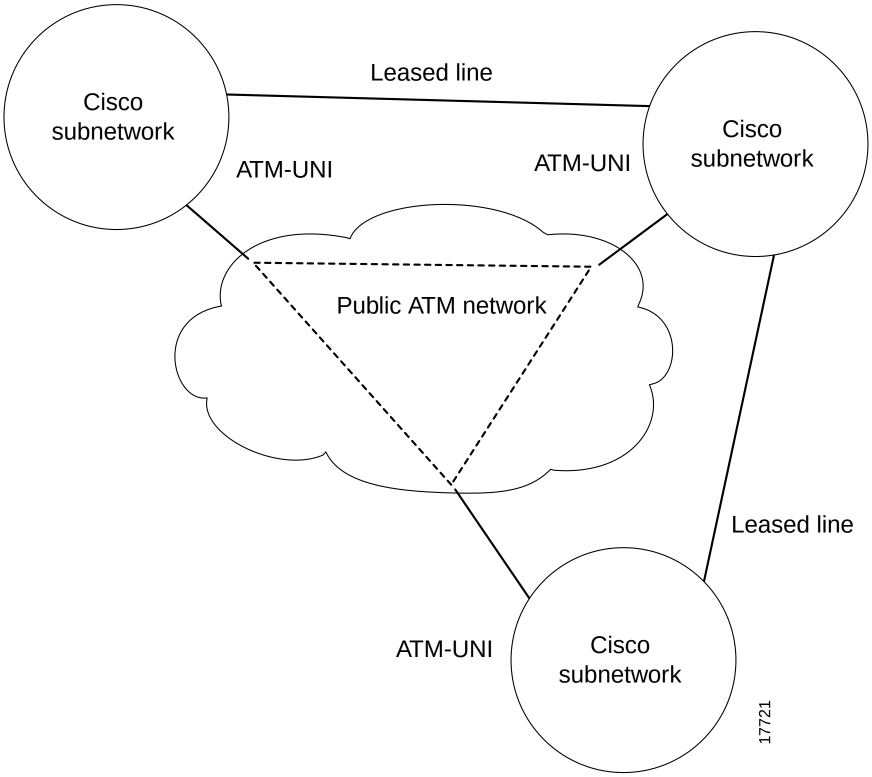
- BXMs to BXMs;
  or
- BXMs to UXMs (IGX switch);
  or
- BNIs to BNIs
- ***But not***
  BNIs to BXMs or UXMs.

When the Cisco network port is a BXM accessing a port in the Public ATM network, the Public ATM port may be a UNI or NNI port on a BXM or other standards-compliant UNI or NNI port.

When the Cisco network port is a BNI accessing a port in the Public ATM network, the Public ATM port must be a port on a BPX.

Figure 24-1 shows three Cisco WAN switching networks, each connected to a Public ATM Network via a physical line. The Public ATM Network is shown linking all three of these subnetworks to every other one with a full meshed network of virtual trunks. In this example, each physical line is configured with two virtual trunks.

Figure 24-1 Typical ATM Hybrid Network using Virtual Trunks



Benefits of Virtual Trunking

Virtual trunking benefits include:

- Reduced cost by dividing a single physical trunk's resources among a number of virtual (logical) trunks. Each of these virtual trunks supplied by the public carrier need be assigned only as much bandwidth as needed instead of the full T3, E3, OC-3, or OC-12 bandwidth of an entire physical trunk.
- Migration of PNNI and MPLS services into existing networks.

  VSI Virtual Trunks allow PNNI or MPLS services to be carried over part of a network that does not support PNNI or MPLS services. The part of the network that does not support PNNI or MPLS may be a public ATM network, or simply consist of switches that have not yet had PNNI or MPLS enabled.
- Utilization of the full mesh capability of the public carrier to reduce the number of leased lines needed between nodes in the Cisco WAN switching networks.
- Choice of keeping existing leased lines between nodes, but using virtual trunks for backup.
- Ability to connect BXM trunk interfaces to a public network using standard ATM UNI cell format.
- Virtual trunking can be provisioned via either a Public ATM Cloud or a Cisco WAN switching ATM cloud.

The BXM card provides several combinations of numbers of VIs, ports, and channels as listed in Table 24-1, depending on the specific BXM card.

Note A virtual trunk cannot be used as a feeder trunk. Feeder connections cannot be terminated on a virtual trunk.

Table 24-1 Virtual Trunk Criteria

	Number of VIs	Max LCNs	Default LCNs
BXM	31	32000	16320

This syntax describes a virtual trunk:

```
UXM/BXM:slot.port.vtrunk
```

slot = slot number (1–32) Keep in mind that on the BPX slots 7 and 8 are reserved for BCCs and slot and 15 is reserved for the ASM card.

port = port number (1–16)

vtrunk = virtual trunk number (1–31 on BXM) (1–15 on UXM)

Card Capacities

These three principles define card capacities for virtual trunking:

- The maximum number of virtual trunks that may be configured per card equals the number of virtual interfaces (VIs).
- Valid virtual trunk numbers are 1 through 31 per port.
- The maximum number of virtual trunks is limited to the number of virtual interfaces (VIs) available on the card and each logical trunk (physical or virtual) utilizes one VI.

For example, the BXM supports 31 virtual interfaces and therefore up to 31 virtual trunks may be defined within one port.

Thus maximum capacities are:

- 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.

Trunk Redundancy

Trunk redundancy refers to one of two features:

- SONET Automatic Protection Switching (APS)
  With Release 9.2, APS line redundancy is supported. APS line redundancy is available only 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. For more information, refer to the *Chapter 25, Configuring SONET Automatic Protection System*.

- Y-redundancy
  The original trunk redundancy feature is an IGX-only feature and is not used for virtual trunks. The commands **addtrkred**, **deltrkred**, and **dsptrkred** are 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
- a BTM and a BNI card

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**).

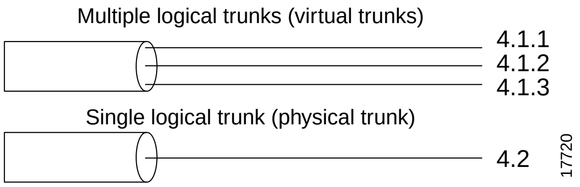
Trunk redundancy depends on the applicable commands, the trunk card in the adjacent slot, and the standard trunk cable. You can execute trunk redundancy commands only on the IGX node.

The BPX node does not require information regarding this feature.

How Virtual Trunking Works

In Figure 24-2, three virtual trunks 4.1.1, 4.1.2, and 4.1.3 are shown configured on a physical trunk that connects to the port 4.1 interface of a BXM. Also, a single trunk is shown configured on port 4.2 of the BXM. In this example, four VIs have been used, one each for virtual trunks 4.1, 4.2, and 4.3, and one for physical trunk 4.2.

Figure 24-2 Virtual and Physical Trunks on a BXM


Multiple logical trunks (virtual trunks)
4.1.1
4.1.2
4.1.3
Single logical trunk (physical trunk)
4.2
17720

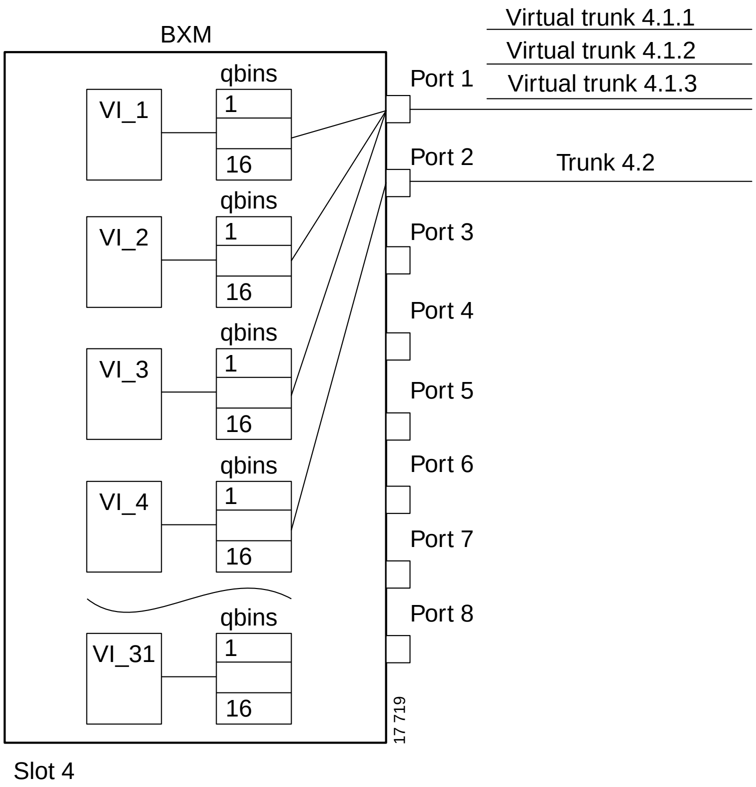
Each logical trunk, whether physical or virtual is assigned a virtual interface when it is activated.

A BXM card has 31 possible egress virtual interfaces. Each of these interfaces in turn has 16 Qbins assigned to it.

In the example in Figure 24-3, port 1 has three virtual trunks (4.1.1, 4.1.2, and 4.1.3), each of which is automatically assigned a virtual interface (VI) with the VI's associated 16 Qbins. Port 2 is shown with a single physical trunk (4.2) and is assigned a single VI.

On a 1-port BXM-622 card, for example, up to 31 virtual interfaces can be used on the port corresponding to 31 virtual trunks. On an 8-port BXM 155 card, for example, the 31 VIs would be distributed to the active trunks, standard or virtual. If trunks were activated on all eight ports, the maximum number of VIs which can be assigned to one port is 24 (31 less 1 for each of the other 7 trunks activated on the card).

Figure 24-3 BXM Egress VIrtual Interfaces and Qbins



Automatic Routing Management connections use Qbins 0 through 9.

Virtual Switch Interfaces (VSIs), which support master controllers use Qbins 10 through 15, as applicable. The BXM can concurrently support MPLS and Automatic Routing Management, or PNNI and Automatic Routing Management, or MPLS and PNNI at the same time on a given VSI.

Virtual Trunks Across a Public ATM Cloud

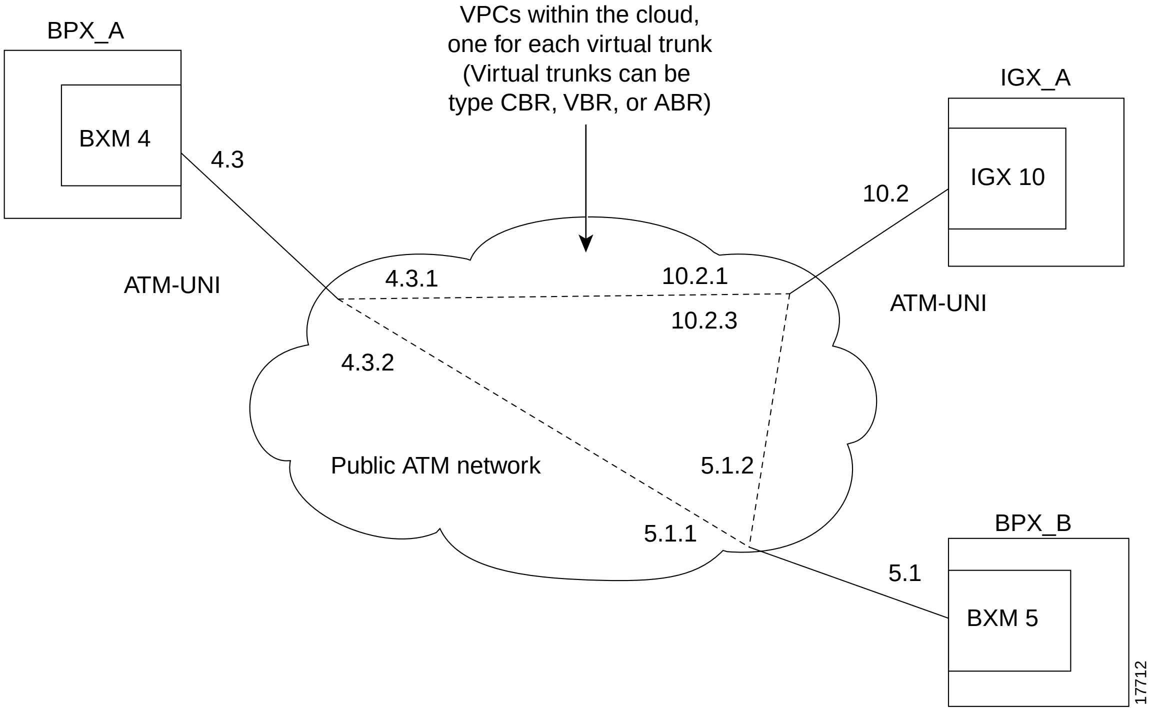
An example of a number of virtual trunks configured across a Public ATM Network is shown in Figure 24-4. There are three virtual trunks shown across the network, each with its own unique VPC.

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 that supports the traffic types shown in Table 24-2.

Figure 24-4 Virtual Trunks across a Public ATM Network



Routing with Virtual Trunks

Automatic Routing Management, PNNI, and MPLS each use different routing mechanisms. However, the routing mechanisms meet the following criteria when dealing with virtual trunks:

- **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 by using **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.

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 uses only those virtual trunks that can support the traffic type of the connection.

Virtual trunking is supported by these features:

- **Integrated Local Management Interface (ILMI)**
  ILMI provides data and control functions for the virtual trunking feature. It is not necessary to configure the ATM ports to block signalling traffic to Cisco equipment 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 during trunk addition, 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 (such as 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.

Connection Management

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 because the port interface to the ATM cloud is a physical configured as either a UNI or NNI interface, as specified by the administrator of the ATM cloud.

Cell Header Formats

Cells transmitted to a virtual trunk use the standard UNI or NNI cell format.

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. The trunk card at the edge of the cloud ensures that cells destined for a cloud VPC have the correct VPI/VCI.

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 is an 12-bit value ranging from 1 through 4095. The VCI is a 16-bit value ranging from 1 through 65535.

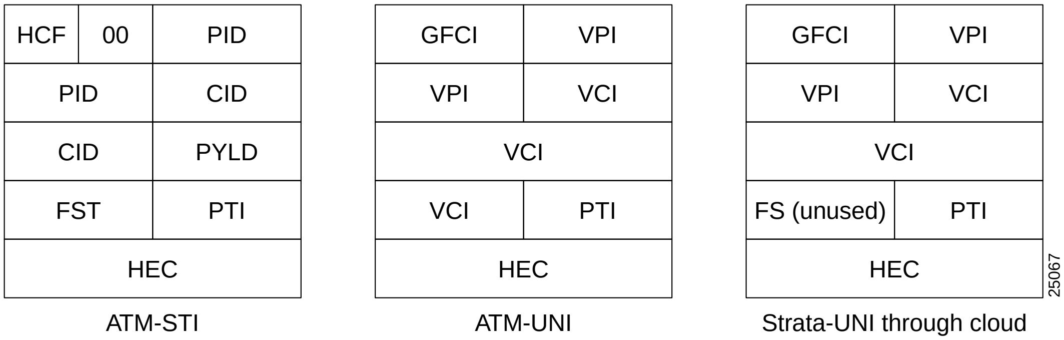
The VPI value across the virtual trunk is identical for all cells on a single virtual trunk. The VCI value in these cells determines the final destinations of the cells. On BNI cards, for virtual trunking a modified ATM UNI cell format (Strata-UNI) stores the ForeSight information, as applicable, in 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.

Figure 24-5 shows three different cell header types, ATM-STI, ATM-UNI, and Strata-UNI through a cloud. The ATM-NNI header which is not shown, 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.

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 (such as, 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.

Figure 24-5 ATM Virtual Trunk Header Types



Bit Shifting for Virtual Trunks

The ATM-STI header uses four of the VPI bit spaces for additional control information. 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 header.

This bit shifting is shown in Table 24-2. A BNI in the Cisco subnetwork can interface to a BXM (port configured for port mode) in the cloud. The BXM in the cloud is configured for no shift in this case.

A BXM in the Cisco subnetwork can interface to a BXM UNI port or other UNI port in the cloud. The BXM in the cloud is configured for bit shifting as shown in Table 24-2.

Table 24-2 Bit Shifting for Virtual Trunking

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

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. Only the BXM and UXM are discussed here.

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 through 65535) excluding the node numbers and blind addresses. A port uses the VPI to differentiate connections which have the same conid.

You can change the number of channels per virtual trunk once the trunk has been added to the network. Decreasing the number of channels on an added virtual trunk will cause connection reroutes whereas 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.

VPC Configuration with the ATM Cloud

In order 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 ports. If the cloud consists of IGX nodes, the access points within the cloud are UXM ports.

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 during the addition of the trunk.

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, ForeSight 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 Vbr configured trunk is best suited to carrying frame relay and Vbr traffic, and so on.

An Abr configured trunk is best suited to carrying ForeSight 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.

You 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.

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 Transmit Queuing

In the BXM, the egress cell traffic out a port is queued in 2 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, these types of traffic are queued separately:

Table 24-3 Virtual Trunk Traffic Types

Automatic Routing Management	
	voice
	time-stamped
	non time-stamped
	high-priority
	bursty data A (bdataA)
	bursty data B (bdataB)
	cbr
	vbr
	abr
VSI	
	MPLS Classes of Service
	UBR
	PNNI traffic

These classes are all queued separately, and the overall queue depth of the virtual interface is the sum of all the queue depths shared by all the available queues. Because each virtual trunk occupies one virtual interface (VI), the overall queue depth available for the virtual trunk is that of its VI.

You do not directly configure the VI.

You use the **cnftrkparm** command to configure the queues within Automatic Routing Management virtual trunks.

You use the **cnfvsiif** and **cnfqbin** commands to configure the queues within VSI virtual trunk VIs.

General Procedure to Set Up a Trunk

Before setting up a trunk, you must first finish setting up the 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.

The Ports and Trunks feature 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.

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 24-4 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

To setup a trunk:

Step 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.

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.

Step 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 24-3. (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.

Step 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 need to add only one end of the trunk.

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.

Setting up a BNI Virtual Trunk through an ATM Cloud

The following example is 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 a BXM port to each BNI port that is likely to carry virtual trunks.

Step 3 For each 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 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 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 24-5.

Table 24-5 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 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 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 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 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

This example is a general explanation of 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 a BXM port to each BXM port that is likely to carry virtual trunks.

Step 3 For each 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 24-6 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.

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 24-6 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 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 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 BXM 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 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 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*.)

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.

BXM cards support up to 31 virtual trunks, while UXM cards support up to 15 virtual trunks.

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
- traffic classes

The **addtrk** command verifies this when you add the trunk.

Example: Virtual Trunk Across an ATM Network

The procedure in this section gives the specific commands for every step in adding one virtual trunk across an ATM network. This is a very typical situation.

This procedures assumes this hypothetical situation:

- 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 24-6).

Given this situation, you would perform these steps:

1. Initial Setup		Contact Customer Service to enable virtual trunking on the nodes in your network.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.

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.
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 you choose by 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
- the number of connection channels supported

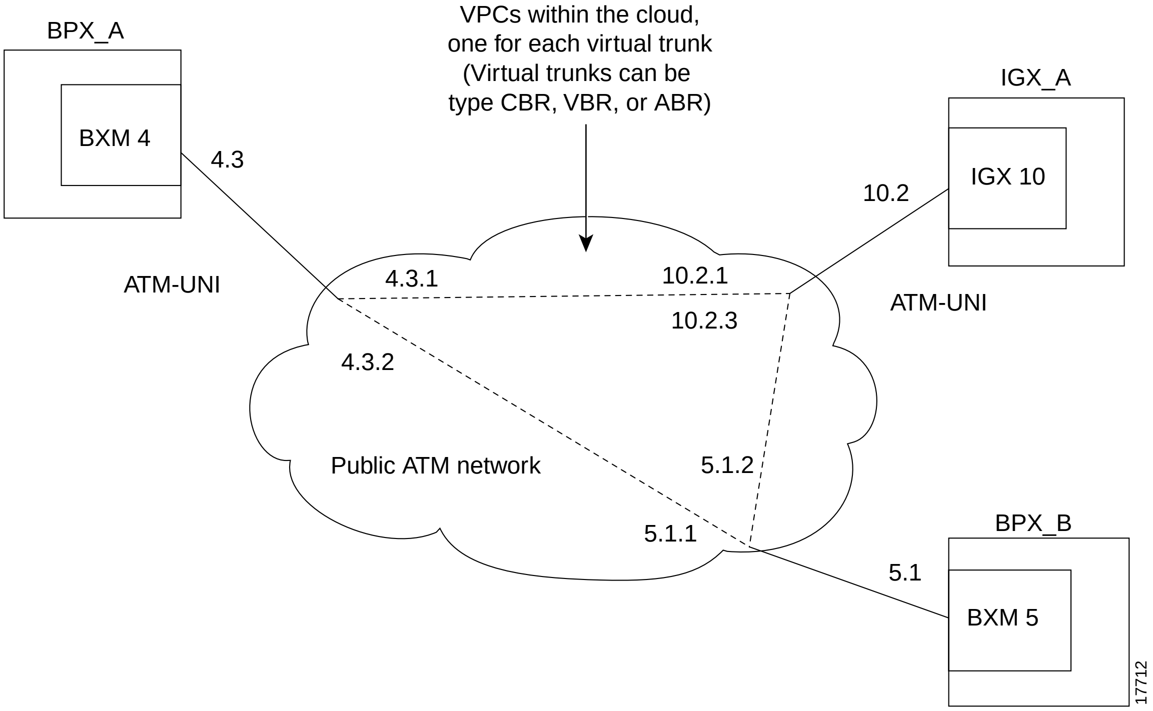
Use the **addtrk** command to check for matching values before allowing the trunk to be added to the network topology.

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 24-6 Addition of Virtual Trunks Across a Public ATM Network



Adding Virtual Trunks Using BNI Cards

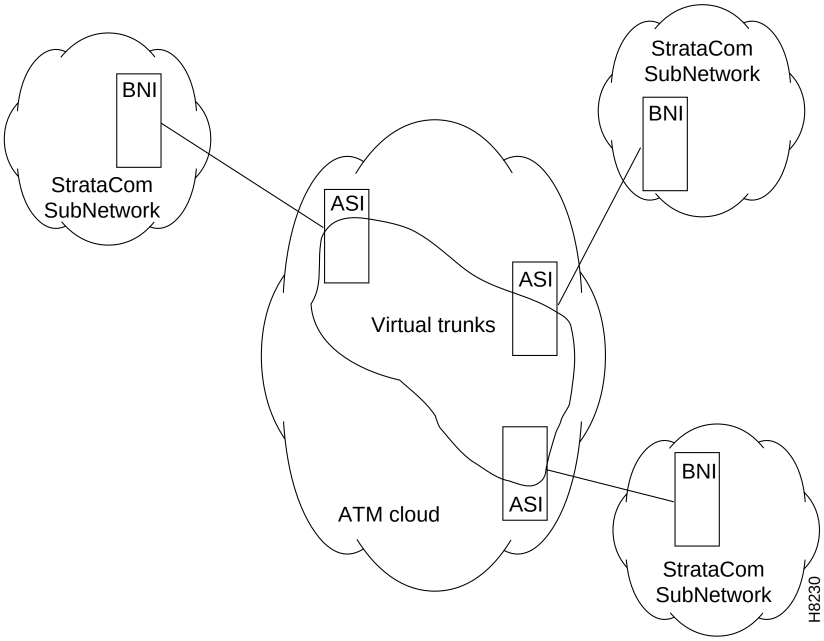
This section is a general procedure for setting up a virtual trunk.

Virtual trunking is an optional feature that must be enabled by Cisco prior to adding virtual trunks. Also, revision levels of BNI firmware must be current.

This procedure assumes that Cisco equipment is used in the ATM Cloud as well as in the Cisco WAN Switching subnetworks. In this case, a BNI output from the subnetwork is connected to a UNI input at the ATM Cloud (see Figure 24-7).

Step 1 In the ATM cloud network, physically connect a port at the cloud edge to each BNI port in the Cisco WAN Switching Network that is intended to have virtual trunks.

Figure 24-7 Virtual Trunks across a Cisco Wan Switching ATM Cloud



Step 2 Configure the cloud ports. For each port connected to a BNI virtual trunk port, run these commands:

upln <slot.port>

upport <slot.port>

cnfport <slot.port> and set the *shift* parameter to "N" for no shift if the cloud contains BPX Execute **addcon**. In the cloud network, add a virtual path connection for each virtual trunk that is to route through the cloud. An example of this syntax is:

addcon joker 5.1.1.* swstorm 6.2.10.*

Where 5.1 and 6.2 are ports hooked up and configured for virtual trunking. Daxcons are acceptable.

Note that the third number is the VPI which must correspond to the virtual trunk VPI you configured by using **cnftrk** in Step 3.

When the cloud is a public ATM service and not a Cisco WAN Switching cloud, the VPI is provided by the carrier, as well as the guaranteed BW associated with the VPI.

The Constant Bit Rate (Cbr), Variable Bit Rate (Vbr), and Available Bit Rate (Abr) parameters must also correspond to the Virtual Trunk Type of the virtual trunk. For T3, set PCR to the bandwidth of the virtual trunk, and CDVT to 24000 for the connection so that the card does not drop cells. These are values that Cisco recommends based on testing.

Step 3 Configure the Broadband Network Interface (BNI) virtual trunks. On the BNIs that connect to the cloud ports, configure up to 32 virtual trunks:

uptrk <slot.port.vtrk>

cnftrk <slot.port.vtrk>

For **cnftrk**, make sure that the virtual trunk type and the VPI correspond to the Virtual Path connections that have been set up.

addtrk <slot.port.vtrk>

Command Overview

The command summarized here are specific to virtual trunk usage on the BPX, using the BXM cards. For complete information about each these commands, refer to the *Cisco WAN Switching Command Reference* and *Cisco WAN Switch SuperUser Command Reference.*

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.

Primary Configuration Commands

The primary commands used for configuration of virtual trunks are:

- **cnftrk**
  Configure trunk
- **cnfrsrc**
  Configure conids (lcns) and bandwidth
- **cnftrkparm**
  Configure trunk parameters

Configuration using cnftrk

The main parameters for **cnftrk** are:

- transmit trunk rate
- trunk VPI
- Virtual Trunk Type
- Connection Channels
- Valid Traffic Classes.

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 24-7

Table 24-7 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

Configuration with cnfrsrc

Use **cnfrsrc** 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. You configure this value by using the **cnfsrc** command on the BPX.

Table 24-8 lists the number of connection ids for virtual trunks on various cards.

Table 24-8 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 OptiClass queues on a single virtual trunk.

When a physical port attribute change is made, you are notified that all trunks on the port are affected.

APS Redundancy

Virtual trunks support APS redundancy on BXM OC-3 and OC-12 ports. For more information, refer to the section on APS Redundancy in this manual. You configure this by using primarily these commands:

- **addapsln**
- **delapsln**
- **switchapsln**
- **cnfapsln**

The prior Y-redundancy is not supported by virtual trunks, nor the related commands, **addtrkred**, **deltrkred**, and **dsptrkred**.

Virtual Trunk Commands

Because 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 that 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 separates 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 documentation for information the IGX and UXM.

The entries in Table 24-9 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 24-9 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
deltrk	Deletes a trunk from the network
dntrk	Downs a trunk
dspcntrstats	View, in real-time, all counter statistics of a specified entity
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

Table 24-9 Virtual Trunk Commands Common to BXM and UXM (IGX) (continued)

Command	Description
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 24-10 are IGX (UXM) specific, or behave differently than their BPX counterparts. Refer to the IGX 8400 Series documentation for further information about UXM virtual trunk commands.

Table 24-10 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 24-11 are BPX specific.

Table 24-11 Virtual Trunk Commands BXM/BNI

Command	Description
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)

Compatibility Between Cards in Virtual Trunks

Virtual trunking is supported on the BNI and BXM cards in the BPX, and on the UXM card in the IGX. Note that firmware levels on these cards must be current.

While virtual trunking is supported on the BPX and IGX, BNI virtual trunks are not compatible with BXM/UXM virtual trunks 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).

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.

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

Channel Capacities. In Release 9.2, networking channels are pre-allocated only for Automatic Routing Management 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 24-11 for networking channel capacities for virtual trunks.

Table 24-12 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.

Virtual Trunking Interactions with Other Features

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 24-13 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
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 24-13 lists the interface types which can be supported on a single card.

Table 24-14 Interface Types that can be Supported on a Single Card

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

Supported Card Types

Table 24-3 shows the communication technology for each node type, card combination, and line type.

Table 24-15 Supported Card Types

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

Table 24-15 Supported Card Types (continued)

Node Type	Front Card	Back Card	Line Types	Technology
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	BXM-622-2	SMF-622-2 SMFLR-622-2	OC-12 (STM4)	ATM

CHAPTER 25

Configuring SONET Automatic Protection System

This chapter contains a description and configuration information for the SONET Automatic Protection System (APS) which may be used to provide line and card redundancy for BXM OC-3 and OC-12 cards:

- Introduction
- Tiered Management Control
- Operation Criteria
- APS 1+1 (Card and Line Redundancy)
- APS 1:1 (Line Redundancy)
- APS 1 +1 Annex B Card and Line Redundancy
- Test Loops
- Notes on APS Messages
- APS K1 Command Precedence
- APS Command Summary

The APS alarms are listed in *Chapter 27, Alarms and Statistics*.

Refer to the *Cisco WAN Switch Command Reference* for further information on configuration and monitoring commands.

To troubleshoot the APS configuration and operations, see *Chapter 28, Troubleshooting*.

Introduction

Automatic Protection Switching (APS) configures 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, within a specified period after an active line failure.

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 to which the user refers.

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, (**cnfapsln** command), the hardware automatically 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 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.

Implementation 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 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 25-1 and shown in Figure 25-2 and Figure 25-3, respectively. APS 1+1 Annex B has the same general layout as shown in Figure 25-2, except that the active line is called the primary, and the standby line is referred to as the secondary.

Table 25-1 BXM SONET APS

Protocol	Description
APS 1+1	The APS 1+1 redundancy provides card and line redundancy, using the same numbered ports on adjacent BXM backcards.
APS 1:1	The APS 1:1 redundancy provides line redundancy, using adjacent lines on the same BXM backcard.
APS 1+1 Annex B	The APS 1+1 Annex B redundancy provides 1+1 high-speed protection, which can be configured only for bi-directional, non-revertive protection switching. For Annex B, the active line is referred to as the “primary section” and the standby line is referred to as the “secondary section”. Manual switching (switchapsln) is not allowed in the APS 1+1 Annex B implementation.

Tiered Management Control

SONET is defined across three elements, section, line, and path as shown in Figure 25-1 and described in Table 25-2. An advantage of this tiered approach is that management control can be exercised at each level, for example at the section level independent of the line or path level.

Note APS on the BPX requires the use of single mode fiber, not multi-mode fiber, on both ends of the trunk. The PXM cards on any connected MGXs should also be single mode fiber.

Figure 25-1 SONET Section, Line, and Path

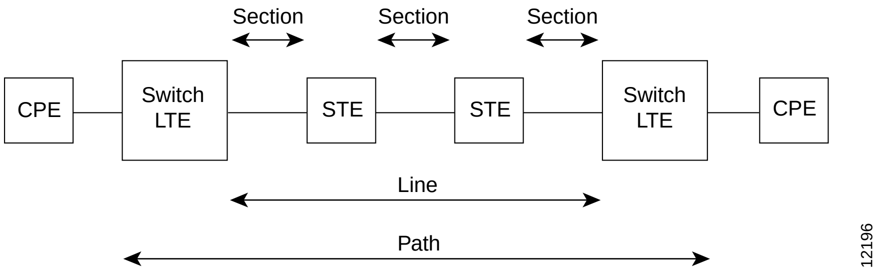


Table 25-2 SONET Section, Line, and Path Descriptions

Unit	Description
Section	A section is the fiber optic cable between two active elements such as simple repeaters. The active element terminating these sections is called Section Terminating Equipment (STE).
Line	A line is a physical element that contains multiple sections and repeaters and is terminated by line terminating equipment (LTE) at each end.
Path	A path includes sections and lines and terminates at the customer premises equipment (CPE).

Table 25-3 provides a cross-reference between OC-*n* optical carrier levels and the equivalent STS-*n* and SDH-*n* levels. It also includes the associated line rates.

Table 25-3 Digital Hierarchies

OC-n Optical Carrier	STS-n Synchronized Transport Signal	Line Rates (Mbps)	SDH-n Synchronized Digital Hierarchy	STM-n Synchronous Transport Module
OC-1	STS-1	51.84		
OC-3	STS-3	155.52	SDH-1	STM-1
OC-12	STS-12	622.08	SDH-4	STM-4
OC-48	STS-48	2488.32	SDH-16	STM-12

Manual Operation

SONET Automatic Protection Switching configures a pair of SONET lines for line redundancy so that the interface hardware automatically switches from a working line to the protection line **or vice versa** within a specified period after an active line failure.

However, you may use the **switchapsln** command to manually control switching. The last user switch request (**switchapsln**) per line pair is saved by switch software so that the APS can be configured correctly in the event of a node rebuild.

Figure 25-2 APS 1+1 Redundancy

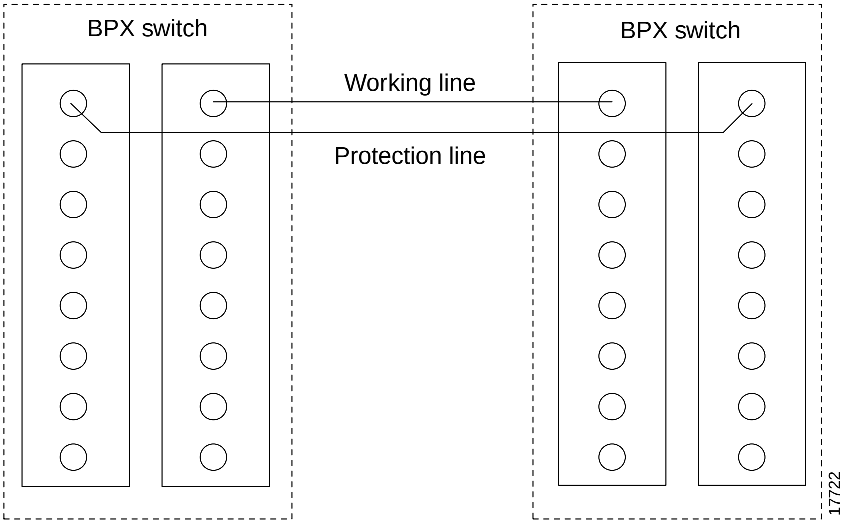
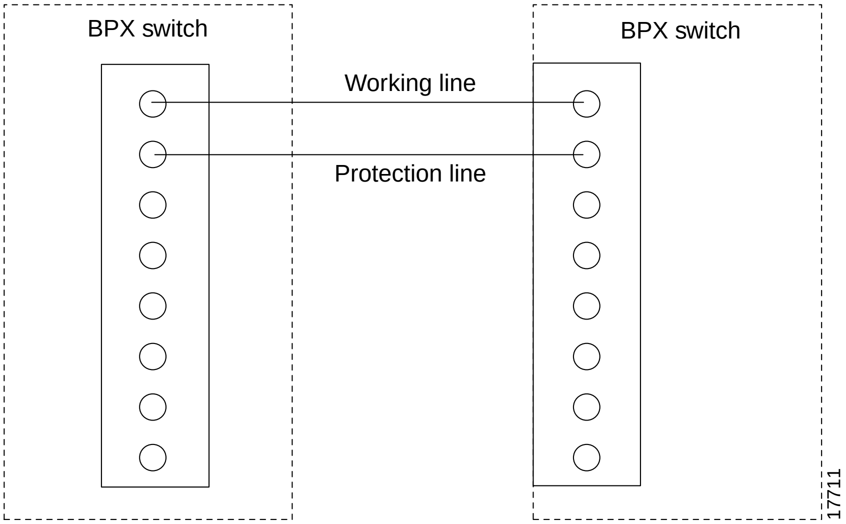


Figure 25-3 APS 1:1 Redundancy



Operation Criteria

APS cards provide both front and backcard LED displays providing line and card status active and standby status.

APS Front Card Displays

The front card LED functions are listed in Table 25-4.

Table 25-4 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 backcards used for APS 1+1 with front card redundancy have an LED which indicates whether the backcard 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 backcard LED functions are listed in Table 25-5.

Note In the APS 1+1 configuration, when the primary card is active and the protection line is active, LEDs on both backcards are green. The LED of the secondary is green because that backcard is carrying traffic. The LED of the primary backcard is green, because that is in the physical path of the front card in receiving traffic from the protection line. When the backcard LED is green do not pull out the backcard, because it will disrupt traffic. When the LED is yellow it is OK to pull out the backcard, but it should be put back as soon as possible, because the card will be needed in the event of a switchover.

Table 25-5 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 may 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 backcards. The two redundant BXM backcards are plugged into the APS redundant frame assembly as shown in Figure 25-4. The types of available backcards are:

The types of redundant backcard and backplane sets required are:

- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622-2 (2 port, long reach, SMF, FC connector)

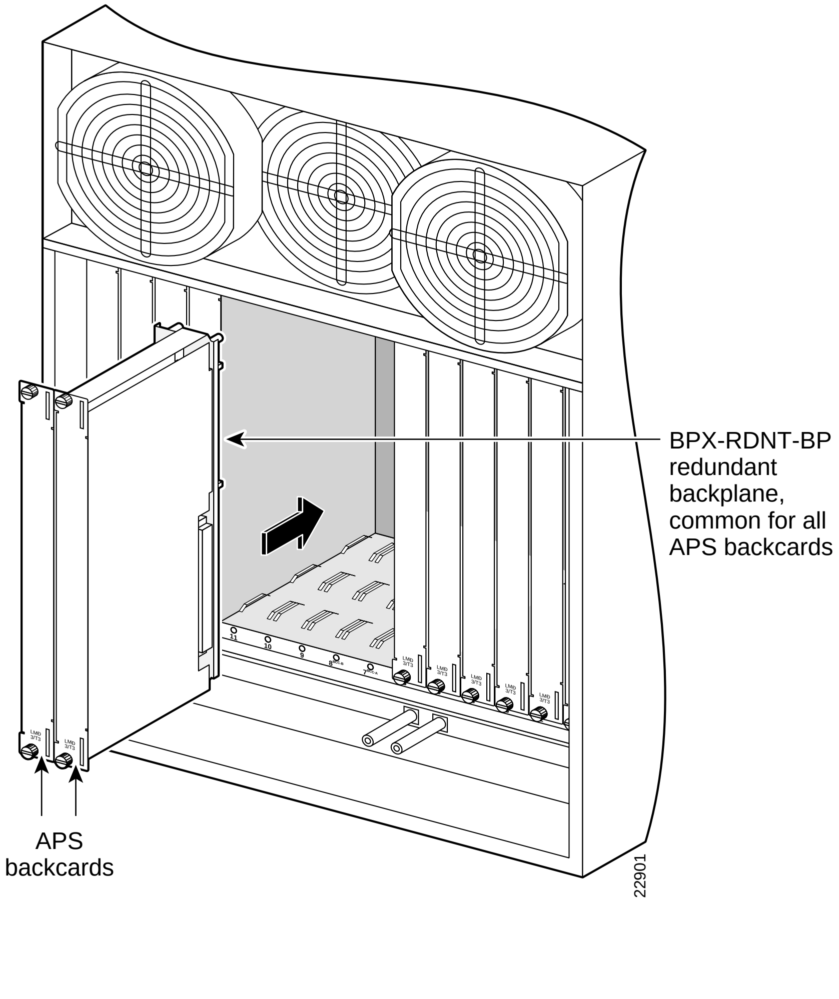
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- BPX-RDNT-SM-622-2 (2 port, medium reach, SMF, FC connector)

  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-622-2R-BC= (for BPX-RDNT-LR-622-2)
- 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)

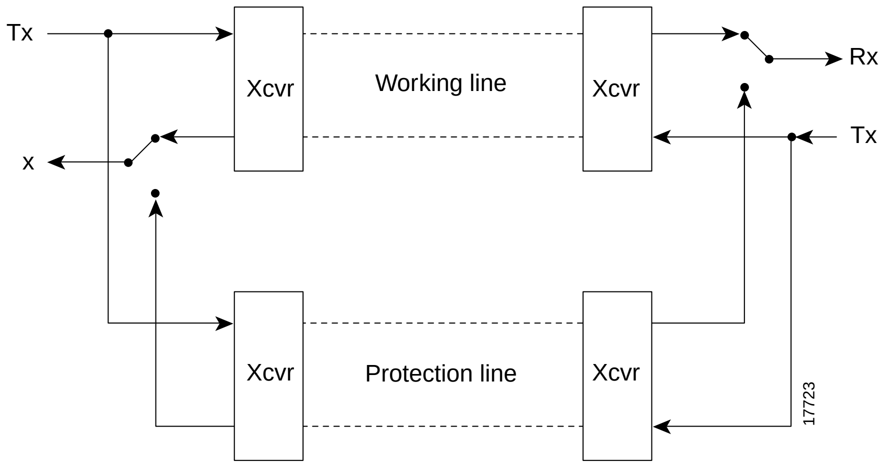
Figure 25-4 APS 1+1 Redundancy, Installing APS Backcards in APS Redundant Backplane



Traffic protected by APS 1+1 redundancy is carried via the working line and the protection line simultaneously (see Figure 25-5). Bridging is implemented such that the same payloads are transmitted identically over the working line as the protection line.

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. Since both working and protection line transport identical information, the receiving ends can switch from one to the other without the need for coordinating with the transmit end.

Figure 25-5 SONET APS 1+1 Detail



To set up APS, the **addapsln** command is used.

- 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 the 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 backcard of the pair may be used independently by independent front cards. The switch software disallows configuration of APS if 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 dividers, the APS card pairs can only be inserted in certain slots. These are slots 2 through 5 and 10 through 13. The mechanical dividers are located at slots 1 and 2, 5 and 6, 9 and 10, and 13 and 14.

With current card cages, this limitation is removed, and the APS card pairs 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).

APS +1 Redundancy Criteria

To implement the APS 1+1 redundancy:

Step 1 Set up Y-redundancy

Step 2 Then add APS

Ensure that these requirements are met:

- The two BXM front cards reside in the same two adjacent slots as the APS backcards
- The APS backcards are inserted into the APS redundant backplane assembly.
- The working lines on the backcard must be connected to the same slot as the primary front card
- The protection lines connected 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 may add APS at any time after Y-redundancy is configured as long as the protection line is in the standby state. You may add APS even if lines and trunks are upped and the card is passing traffic.

Note Normally 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 a MGX 8220 (feeder shelf) or other device which does not support APS. In that case, Y-cables or straight cables may be used with APS.

When APS is configured on a card pair, switch software checks to ensure that both cards match and support APS.

For APS 1+1 redundancy, the same numbered ports on adjacent BXM backcards 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 backcards 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** execute the same command. The newer name is **switchcdred** which replaces **switchyred**, but **switchyred** may still be used for those familiar with that command.

The **switchcdred (switchyred)** command can be used 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 **switchdred** will cause the working line to be active if there is no line condition on 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.

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** is issued. On a **switchcdred**, 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 (switchyred)** command after performing a service switch with the **switchapsln** command so that the backcard that the service switch selects has its associated front card active.

Notes on switchapsln

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 you wish to perform repetitive switchapsln commands, you should issue a clear switch between each W-P, P-W pair of commands, for example:

```
switchapsln 2.1  1
```

Configuring APS 1+1

This an example of configuring APS 1+1 redundancy:

Step 1 Verify that appropriate front and back cards are installed along with 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 these 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 redundant line on port 1 for BXM OC-3 cards and APS backcards 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** 2.1

Step 7 **upln** 2.1 {or **uptrk**, as applicable

APS 1:1 (Line Redundancy)

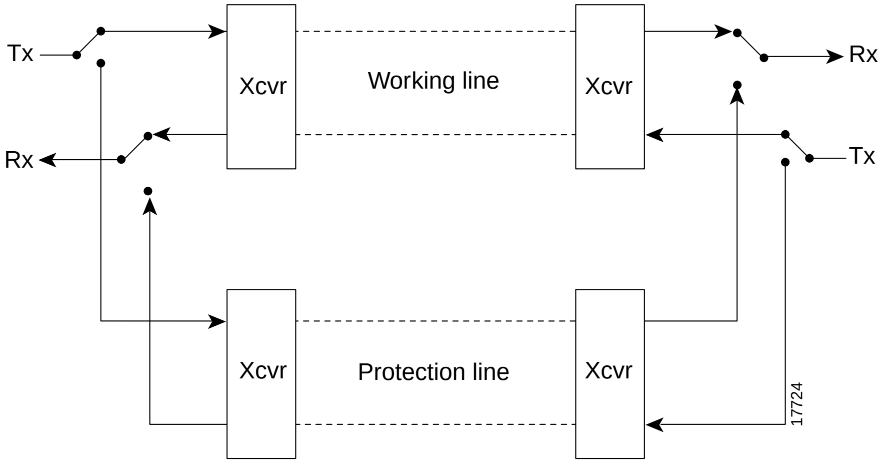
The APS 1:1 feature provides port and line redundancy for a single BXM front card and associated OC-3 or OC-12 redundant backcard.

There is no new hardware required to support APS 1:1. A single front card with a standard backcard is used.

Two adjacent lines on the same card are used. The maximum number of connections supported by a non-enhanced BXM card is reduced by half for APS 1:1 operation. Using enhanced BXM cards, the number of available connections is not decreased.

Similarly to APS 1+1, SONET APS 1:1 requires that for every working line, there must exist a redundant protection line (see Figure 25-6). 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 switches, this coordination between the equipment at both ends is more complex.

Figure 25-6 SONET APS 1:1 Detail



To set up APS, the **addapsln** command is used.

- Before the **addapsln** is used, the switch software will not attempt to use or monitor the protection line; only the working line is used.
- If the **addapsln** 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 prior to 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 which may be paired are:

- 1 and 2
- 3 and 4
- 5 and 6
- 7 and 8

Either of the two lines may be designated as working line and the other as the protection line.

The switching of the working and protection lines is controlled by BXM firmware/hardware under the APS protocol.

The BPX firmware/hardware performs switching between the protection and working lines in the event of a line or port failure.

The user may add APS as long as the working and protection line are in the standby state. Lines and trunks can only be upped after APS 1:1 is added.

Configuring APS 1:1

This 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

APS 1 +1 Annex B Card and Line Redundancy

The APS 1 +1 Annex B feature is similar to the APS 1+1 feature, with the main difference being that APS 1+1 Annex B redundancy only can be configured for bi-directional operation and non-revertive switching.

General Criteria

APS 1 + 1 Annex B can be configured only 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.

Configuring APS 1+1 Annex B

The following is an example of configuring APS 1+1 redundancy:

Step 1 Verify that appropriate front and back cards are installed along with 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 backcards in slots 1 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** specifies the type of APS, in this example APS 1 + 1, Annex B.

Step 6 **cnfapsln** 1.1

Step 7 **upln** 1.1 {or **uptrunk**, as applicable

Test Loops

The test commands **addlnloclp** and **addlnrmtlp** may affect service even when APS is configured. In all APS configurations, if the working line is looped, both lines will be looped and traffic disrupted.

Notes on APS Messages

When adding an APS 1+1 line or trunk by 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 by using the **dspcd** command under the "Backcard 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".

This is an example of **dspcd** 2:

```
swwye     TN       silves        BPX8620      9.3 March 9  2000

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 K1 Command Precedence

The possible conditions which may cause/prevent a switch are listed in Table 25-6. The list is arranged starting from highest precedence and ending with lowest precedence. Refer to the *Cisco WAN Switching Command Reference* for further description and information.

Table 25-6 K1 Switching Conditions

APS K1 Command Precedence
Lock out of Protection
Forced Switch
Signal Fail
Signal Degrade
Manual Switch
Wait To Restore
Reverse Request
Do not Revert
No Request

APS Command Summary

Commands to support APS are listed in Table 25-7, and defined in more detail in the *Cisco WAN Command Reference* where you will find thorough information on each of these commands, as well as other commands not listed here.

Table 25-7 APS Commands

Command	Description
New Commands Added for Management of 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 (option 1...6, S)	Controls the APS user switching interface.
cnfapsln slot.port	Configures the APS parameters on a line.
New Commands for Card Redundancy for APS 1+1	
addcdred	Adds redundancy across two cards.
dpscdred	Display redundant cards.
delcdred	Deletes redundancy configuration for cards.
switchcdred	Switches active and redundant cards.
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 backcard APS attributes. For the front card, displays that card supports APS 1+1 and APS 1:1. For the back card, displays if backcard is a redundant backcard, and if so, the slot number of the redundant backcard. 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.

Configuring BME Multicasting

This chapter presents an overview of multicasting, a description of the BME card used on the BPX switch for multicasting for PVCs, and configuration instructions:

- Introduction
- BME Operation
- Hot Standby Backup
- Configuration

Introduction

The BME provides multicast services in the BPX switch. It is used in conjunction with a two-port OC-12 backcard.

Multicasting point-to-multipoint services meets the demands of those requiring virtual circuit replication of data (Frame Relay and ATM) performed within the network. Some examples of functions benefiting from multicasting are:

- Retail—point-of-sale updates
- Router topology updates
- Desktop multimedia
- Video conferencing
- Video distribution, for example, IP multicast video networks to the desktop
- Remote learning
- Medical imaging

  BME Standards are:

- UNI 3.1 Multicast Server
- UNI 4.0 Leaf Initiated Joins and related standards

Multicasting point-to-multipoint connections benefits include:

- Decreased delay in receiving data
- Near simultaneous reception of data by all leaves

BME Features

- The BME is a two-port OC-12 card
- Supports up to 1000 multicast groups
- Supports up to 8064 connections, at 4032 per port. It can support the following combinations:
  - 1000 roots with 8 leaves in each multicast group
  - 100 roots with 80 leaves in each multicast group
  - 2 roots with 4000 leaves in each multicast group
  - or any other such combination.
- Supports Cbr, Ubr, Vbr, and ATFR connections
- Hot standby

BME Requirements

- Firmware of type BMEMK, where K is the model number for BME.
- **upln** is used to bring up line 1 and line 2.
- **upport** is used to bring up port 1 and port 2, respectively.

BME Restrictions

- BMEs can function in the following two BPX node configurations:
  - BCC-4s
  - BXMs
- VC frame merge is not currently supported

Address Criteria

- The VPI of a multicast connection indicates the multicast group to which it belong.
- The VPI.VCI assigned to a multicast connection is unique for that card.
- If the VCI = 0 for a multicast connection, this indicates a root connection.
- If the VCI is not = 0 for a multicast connection, this indicates a leaf connection.
- If the root connection of a given multicast group is added to port 1 of the two port card, then the leaves belonging to that multicast group must be added to port 2, and vice versa.

  For example, if 12.1.50.0 is added on port 1, then the leaves should be:

  12.2.50.50
  12.2.50.100
  12.2.50.101 and so on.

  Similarly, if a root 12.2.60.0 is added on port 2, then the leaves should be

  12.1.60.101
  12.1.60.175, and so on.

Connection Management Criteria

Root connections and leaf connections can be added in any order:

- Add root first and then leaves.
- Add leaves first and then root.
- Add root in between adding leaves.

Root and leaf connections can be deleted in any order.

Root can be deleted and replaced with a new root.

Connection Management with Cisco WAN Manager

Cisco WAN Manager management includes these functions:

- Connection filtering by multicast type (root/leaf)
- Multicast connection addition, deletion, and modification
- Multicast view of multicast group of a selected connection
- No multicast specific statistics support
- No service MIB support

BME Operation

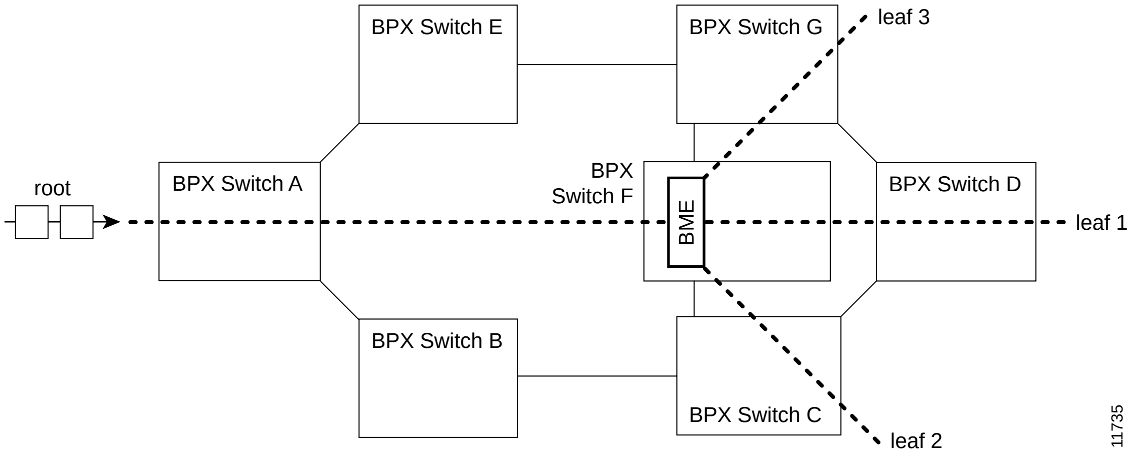
Cables are connected between port 1 and port 2 of the backcard, transmit to receive and receive to transmit.

Note Removing the physical loopback cables or placing line 1 or 2 into loopback will prevent the cells from the root reaching the leaves.

BME Cell Replication

Figure 26-1 shows a BME with a single root input multicasting with 3 leaves. The root connection can be added at a BPX switch (BPX switch A) distant from where the traffic is replicated by the BME card (BPX switch F) and routed through a number of BPX nodes. Similarly, the leaves can be routed from the multicasting node through a number of nodes before reaching their destination.

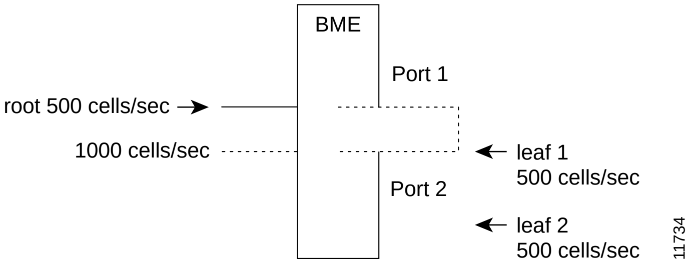
Figure 26-1 Replication of a Root Connection into Three Leaves



Cell Replication Stats

As an example of how traffic appears on the BME, if there is one root at port 1 with two leaves at port 2, and traffic is passed on the root at 500 cells per sec, then one should see an egress port stat of 1000 cells per sec on port 1 and an ingress port stat of 1000 cells per sec on port 2, as shown in Figure 26-2.

Figure 26-2 Example of Traffic, One Root and Two Leaves



Adding Connections

Two multicasting groups are shown in Figure 26-3. For purposes of the illustration only a few leaves are shown for each connection. However, as described previously, each multicasting group could contain up to 8064 connections.

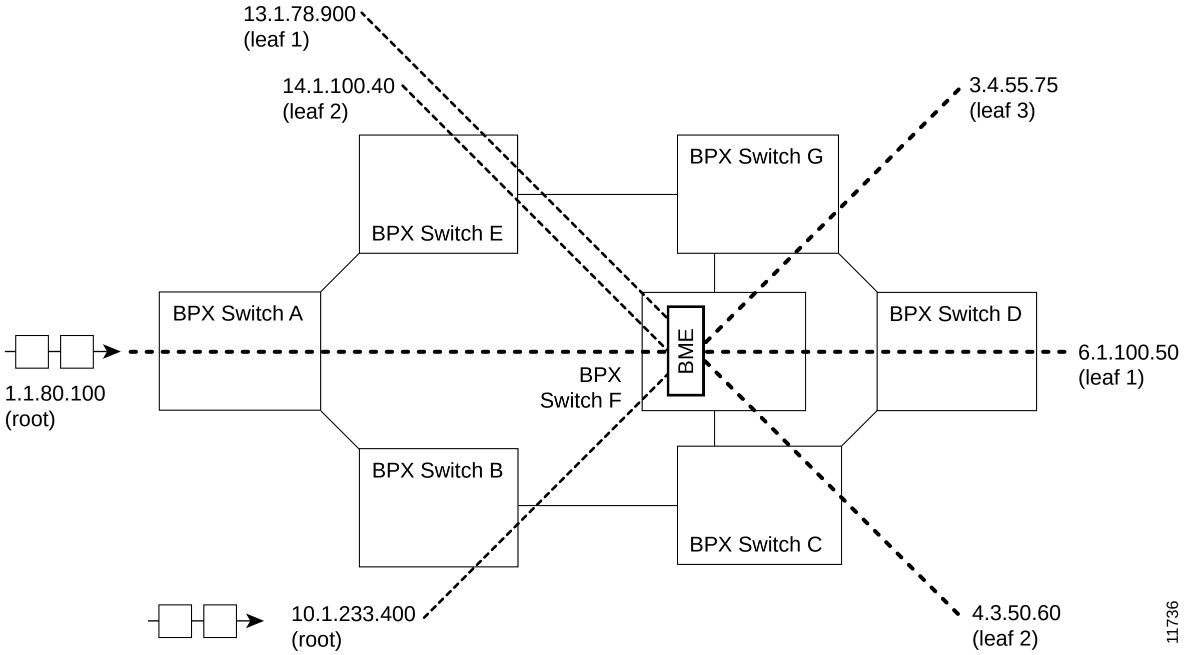
In this example, the two connections with a VCI of 0 each define a multicasting root connection. Their VPI defines a broadcasting group.

One group is defined by 2.1.70.0, where the VCI of zero defines the root connection to a BME, and the VPI of 70 defines a group. All the leaves in that group are of the form 2.2.70.x.

The other group is defined by 2.2.80.0, where the VCI of zero defines the root connection to a BME, and the VPI of 80 defines a group. All the leaves in that group are of the form 2.1.80.x.

Group 2.1.70.x	**Action**	**Command**
at bpx switch_F,	add input to root	addcon 2.1.70.0 bpx switch_A 1.1.80.100 c 500 * * *
at bpx switch_F,	add leaf 1	addcon 2.2.70.101 bpx switch_D 6.1.100.50 c 500 * * *
at bpx switch_F,	add leaf 2	addcon 2.2.70.100 bpx switch_C 4.3.50.60 c 500 * * *
at bpx switch_F,	add leaf 3	addcon 2.2.70.102 bpx switch_G 3.4.55.75 c 500 * * *
Group 2.2.80.x		
at bpx switch_F,	add input to root	addcon 2.2.80.0 bpx switch_B 10.1.233.400 v 4000 * * *
at bpx switch_F,	add leaf 1	addcon 2.1.80.201 bpx switch_E 13.1.78.900 v 4000 * * *
at bpx switch_F,	add leaf 2	addcon 2.1.80.100 bpx switch_E 14.1.100.40 v 4000 * * *

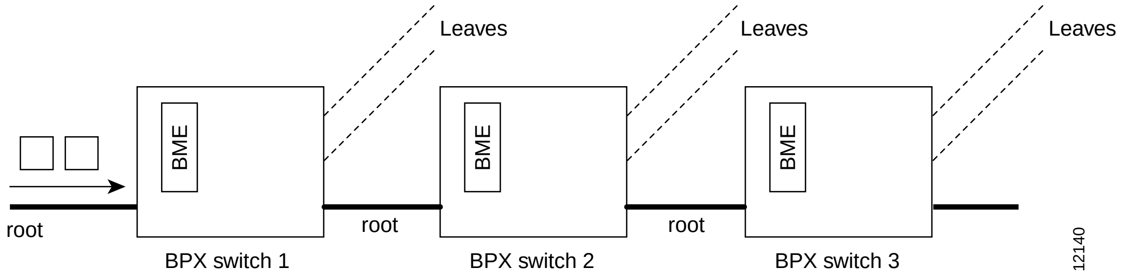
Figure 26-3 Adding Multicasting Connections



Multisegment Multicast Connections

Figure 26-4 shows an example of a multisegment multicast connection where a leaf connection from one BME can become a root connection for another BME. This capability allows the users to configure multisegment, multicast tree topologies.

Figure 26-4 Multi-Segment Multicast Connections



Multicast Statistics

Channel statistics are available for leaf connections on the BME end. However, channel statistics are not available for the root connection on the BME end.

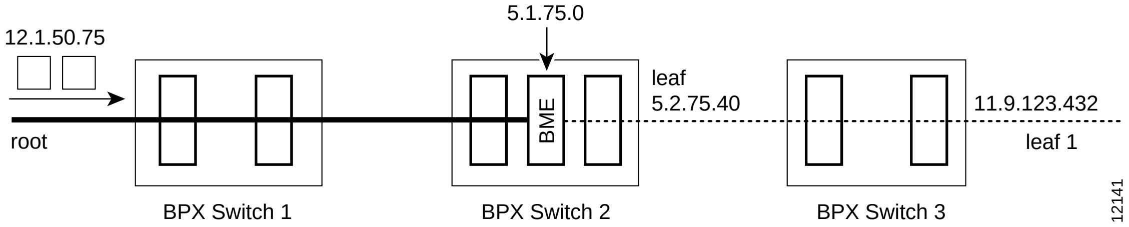
For the example in Figure 26-5, execute the following commands to display channel statistics for the leaf connections:

- **dspchstats** 12.1.50.75 on BPX switch 1 (available)
- **dspchstats** 5.2.75.40 on BPX switch 2 (available)
- **dspchstats** 11.9.123.432 on BPX switch 3 (available)

For the example in Figure 26-5, the following command will not display channel statistics (because 5.1.75.0 is a root connection):

- **dspchstats** 5.1.75.0 on BPX switch 2 (not available)

Figure 26-5 Statistics Collection



Policing

Policing is supported on all leaf connections on the BME end.

All policing types available on the BXM are available on the BME leaves.

No policing functionality is available on the root connection on the BME end.

Hot Standby Backup

BME cards can be set up to provide hot standby backup. Both cards are set up with port 1 connected to port 2 on the same card to provide the multicasting connection, transmit to receive and receive to transmit. There is no Y-cabling connection between the cards, and they do not have to be adjacent to each other.

Use the **addyred** command to enable hot standby backup between the cards.

Note The addyred command must be used before any connections are added to the active card. The command will be rejected if used after connections have been added to the active card.

Configuration

If the multicast tree has a large number of leaf connections, for example, 3000, then the **cnfportq** command should be used to configure the Qbin threshold to be greater than needed for half the number of leaves so as to assure that the multicast group will have no discards. The Qbin default depth is about 1200 cells.

The following is a Qbin example using the **cnfportq** command:

```
j4b           VT    SuperUser     ~ BPX 15    9.3 March 24 2000 16:59 PST
Port:       3.2     [ACTIVE  ]
Interface:          LM-BXM
Type:               NNI
Speed:              1412830 (cps)
SVC Queue Pool Size:          0
CBR Queue Depth:              1200
CBR Queue CLP High Threshold: 80%
CBR Queue CLP Low Threshold:  60%
CBR Queue EFCI Threshold:     80%
VBR Queue Depth:              10000   UBR/ABR Queue Depth:               40000
VBR Queue CLP High Threshold: 80%     UBR/ABR Queue CLP High Threshold:  80%
VBR Queue CLP Low Threshold:  60%     UBR/ABR Queue CLP Low Threshold:   60%
VBR Queue EFCI Threshold:     80%     UBR/ABR Queue EFCI Threshold:      30%

This Command: cnfportq 3.2
SVC Queue Pool Size [0]:
Virtual Terminal      CD
```

CHAPTER 27

Alarms and Statistics

This chapter describes some of the tools provided for detecting and identifying network and equipment problems that are available to the network operator:

- Automatic Alarm Reporting to Cisco Customer Service
- Network Statistics
- APS Alarms
- Trunk Statistics
- Trunk Alarms
- Event Logging
- BME Alarms

Considerably more advanced tools are built into the system software for exclusive use by Cisco Customer Service personnel. These advanced tools require in-depth knowledge of the hardware and software and are used generally to locate the less common types of system problems.

Automatic Alarm Reporting to Cisco Customer Service

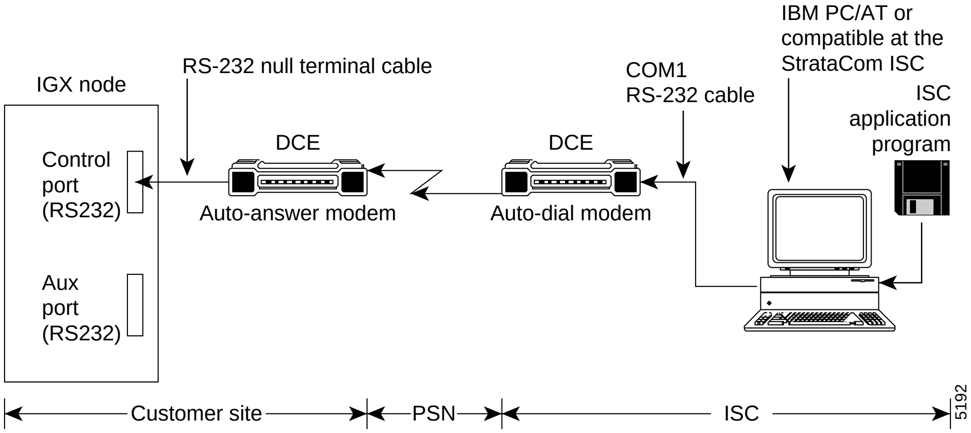
Do not perform any disruptive tests or repairs to the network on your own. Before commencing with troubleshooting, call Cisco Customer Service so that they can provide you with assistance in locating a fault.

In a network with Cisco BPX 8600 series broadband switches and Cisco IGX 8400 series multiband switches it is recommended that at least one node be configured to transmit alarms automatically to Cisco Customer Service Figure 27-1 illustrates the hardware configuration required for implementation. This can be a Cisco IGX 8400 series multiband switch.

When an alarm occurs on the network, the autodial modem automatically dials the specified telephone number. An auto-answer modem at Cisco Customer Service answers the call and directs it to a dedicated personal computer. The alarm is logged under the network ID (an ASCII character string) specified by the network administrator and approved by Cisco Customer Service personnel.

If the auto-answer modem at Customer Service is busy when an alarm arrives, then the autodial modem will keep dialing until the call is completed. A suggested modem is the Codex V.34 RSA 28.8 K modem.

Figure 27-1 Automatic Alarm Reporting



Network Statistics

Cisco WAN Manager collects network statistical data on the operation of the network and stores them in its database. They are available for display on the Cisco WAN Manager console in either tabular form or as bar charts. Statistics can be a useful source of information for troubleshooting problems that do not necessarily cause a major or minor alarm indication or for locating intermittent failures that may occur at random.

There are four classes of statistics:

- Trunk statistics
- Line statistics
- Connection statistics
- Frame Relay port statistics

Most statistics are collected on demand and must be enabled by the system operator. The operator can set the collection interval, the sampling times, and the number of collection buckets to tailor the statistics for either long-term network performance evaluation or short term for network troubleshooting.

Table 27-1 lists the statistics categories and the general nature of the statistics collected in each category. Note this is not a complete list of statistics but merely indicates some of the various conditions monitored. Refer to the *Cisco WAN Manager Operations* document for a complete listing.

Table 27-1 Typical Statistics Collected

Statistics Category	Types of Statistics
Trunk statistics	Various trunk errors, bipolar violations, frame bit errors, loss of signal, etc.
	Packet errors and out of frame
	FastPackets and ATM cells of various types transmitted/dropped
	Transmitted ATM cell counts
	Received ATM cell counts

Table 27-1 Typical Statistics Collected (continued)

Statistics Category	Types of Statistics
	Cells with CLP and EFCN set
	ATM header error counts
	DS3 PLCP error counts
	Bdata queue dropped cells
Line statistics	Various circuit line errors, bipolar violations, frame bit errors, loss of signal, and so on
Connection statistics	Packets transmitted and received
	Transmitted and received data bytes
	Frame relay frames transmitted/discarded
	Frames transmitted with FECN or BECN or DE set
	Packets with CLP bit set dropped
	Seconds in service
Frame Relay Port	Frames transmitted and received
	Bytes transmitted and received
	Frames received with CRC or other errors
	Frames discarded at the connection ingress
	Frames discarded at the connection egress
	Frames discarded at the port egress
	LMI messages sent or dropped for various errors
	DE frames dropped

APS Alarms

The APS alarms are listed in Table 27-2. The list includes the class or state of the alarm: minor, major, information, or clear.

Statistical alarms are not cleared when a Y-red switch occurs. You can clear these statistics as appropriate.

Note On the active line/trunk, alarms (such as LOS and LOF) and statistics (such as 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.

Table 27-2 APS Alarms

Class	Name	Description
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 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 signaling information in the K1/K2 bytes.
Minor	APS Channel Mismatch	Can happen in only 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 (PSB) failure. 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 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 high-priority signal degrade condition. An automatically initiated switch due to a “soft failure” condition resulting from the line BER exceeding a preselected 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 27-2 APS Alarms (continued)

Class	Name	Description
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 preselected 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 high-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 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 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 bidirectional 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.

Table 27-2 APS Alarms (continued)

Class	Name	Description
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 nonrevertive 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	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 means that one side supports 1+1 and other end of the line is configured for 1:1, or the directional or revertive parameter does not match. FW cannot bring the two ends into compliance on the fly; the user must correct the configuration error.

What 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 that are reported in the 0x55 Line Alarms command and are discussed in other documentation.

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 signaling information in the K1/K2 bytes. There is a problem with the protection line's physical layer. One has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting in loopback and so on).
- **Channel Mismatch**
  Can happen in only 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. One has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting in loopback and so on).
- **Prot Sw Byt FAIL**
  Protection Switch Byte (PSB) failure. 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. One has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting in 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. One has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting in 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 bidirectional and the other end is unidirectional (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**
  This indicates that on the local end of an APS 1+1 configuration, 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**
  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)

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 the both the BPX and the IGX, physical line statistics are displayed on the **dspphyslnstats**, **dspphyslnstathist**, and **dspphyslnerrs** screens. These commands accept only physical line numbers (that is: slot.port).
- **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 statistics are displayed on the **dsptrkstats**, **dsptrkstahist**, and **dsptrkerrs** screens. These commands accept only 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 you use the debug command **dspchstats**.
- **Counter statistics:** Use the command **dspcntrstats** to display in real-time all counter statistics of specified entity.

Table 27-3 is a list of trunk statistics including statistics type, card type, and line type, as applicable.

Table 27-3 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

Table 27-3 Trunk Statistics (continued)

Statistic	Stat Type	Card Type	Line Type
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	All
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
Qbin Statistics to support VSI For Each Traffic Type: (V,TS,NTS, Abr, Vbr, Cbr, BdatB, BdatA,HP) For UXM trunks: Qbins 10 through 15 For BXM and UXM line ports: Qbins 1 through 15			
Cells served	Logical	UXM/BXM	All
Cells received	Logical	UXM/BXM	All
Cells discarded count	Logical	UXM/BXM	All

Trunk Alarms

Trunk alarms fall into two categories:

- **Logical Trunk Alarms**
  Statistical alarming is provided on cell drops from each of the 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 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.

Physical and Logical Trunk Alarm Summary

Table 27-4 is a list of physical and logical trunk alarms.

Table 27-4 Physical and Logical Trunk Alarms

Alarm Type	Physical					Logical	Statistical	Integrated
	T1	E1	T3	E3	SONET			
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	

Table 27-4 Physical and Logical Trunk Alarms (continued)

	Physical							
Alarm Type	**T1**	**E1**	**T3**	**E3**	**SONET**	**Logical**	**Statistical**	**Integrated**
VBR Cells Dropped						X	X	
ABR Cells Dropped						X	X	

Event Logging

All trunk log events are modified to display the virtual trunk number. The examples in Table 27-5 and Table 27-6 show the log messaging for activating and adding a virtual trunk 1.2.1.

I

Table 27-5 IGX Log Messaging for Activating and Adding a VT

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 27-6 BPX Log Messaging for Activating and Adding a VT

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:

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

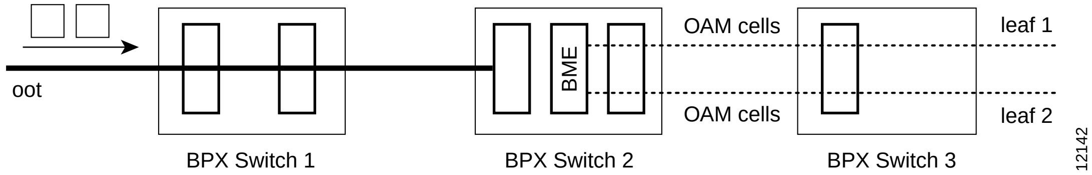
Message	Description
“Port does not support virtual trunking”	Port is not configured for virtual trunks
“Mismatched virtual trunk configuration”	Ends of virtual trunk have different configuration
“Maximum trunks for card has been reached”	The trunk card is out of VIs

BME Alarms

OAM cells

OAM cells coming into the root are multicast into the leaves along with data, as shown in Figure 27-2.

Figure 27-2 OAM Cells

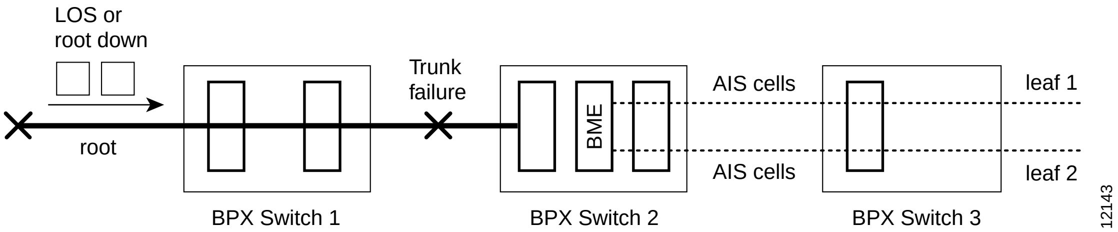


AIS cells

AIS cells are automatically generated on the leaves, as shown in Figure 27-3, when:

- There is a loss of signal (LOS) on the far end of the root
- There is a trunk failure
- When the root connection is downed using the **dncon** command

Figure 27-3 Alarms



Qbin Statistics

Qbin statistics allow network engineers to properly engineer and overbook the network on a per Class-of-Service (or per Qbin) basis.

Switch software collects statistics for:

- BXM Automatic Routing Management Qbin (Qbin numbers 1-9) on Automatic Routing Management trunks.
- Qbin numbers 10-15 assigned for use by VSI traffic. These statistics are helpful for configuring MPLS or PNNI controllers.

The resulting statistics are displayed in Cisco WAN Manager and may also be viewed by using the command line interface (CLI).

These Qbin statistics are available:

- cells served
- cells received
- cells discarded

Because all Qbins provide the same statistical data, the Qbin number together with its statistic forms a unique statistic type. One unique statistic type is “Cells served out of Qbin-10.” Another unique statistic type is “Cells discarded by Qbin-11,” and so on.

Trunk and port counter statistics for Qbins 1-15 can be collected by SNMP.

Qbin summary and counter statistics can be enabled as TFTP or USER (not AUTO) interval statistics. Unlike the cell discard statistics on BXM trunk Qbins 1-9, all cell-discard statistics on Qbins 10-15 are not AUTO statistics.

The next two sections are a brief introduction the commands described in the *Cisco WAN Switching Command Reference.* For detailed explanations and tables of Qbin statistics, see the Qbin commands in the *Cisco WAN Switching Command Reference* and the *Cisco WAN Manager User’s Guide.*

Interval Statistics

There are two ways you can collect interval traffic statistics (per Qbin) on the switch:

- Cisco WAN Manager’s SCM collects and views statistics on all BXM trunks on a BPX (TFTP statistics). See the Cisco WAN Manager documentation.
- The command line interface (CLI).

Use these commands to collect interval statistics:

- **cnftrkstats**
  Collect USER statistics of one statistic type on a specific specified trunk.
- **dsptrkstathist**
  View interval statistics of one statistic type on a specific specified trunk.
- **cnfportstats**
  Collect USER statistics of one statistics type on a specified port.
- **dspportstathist**
  View statistics of one statistics type on a specified port.

Summary and Counter Statistics

Use these commands to collect summary and counter statistics:

- **dspcntrstats**
  View, in real-time, all counter statistics of a specified entity.
- **dspqbinstats**
  View all Qbin summary statistics on a specified trunk/port.
- **clrtrkerrs**
  Reset or clear the summary statistics of all statistic types on a specified trunk.
- **clrportstats**
  Reset or clear the summary statistics of all statistics types on a specified link.

PART 5

Troubleshooting and Maintenance

CHAPTER 28

Troubleshooting

This chapter describes periodic maintenance procedures and general troubleshooting procedures:

- Preventive Maintenance
- Troubleshooting the BPX Switch
- APS Configuration Problems
- Operational Problems
- BME Connection Diagnostics
- Troubleshooting VSI Problems
- Troubleshooting Commands

After an alarm occurs, use the BPX switch software to isolate the problem. If a BPX switch part has failed, then it must be replaced. See “Chapter 29, Replacing Parts.”

Preventive Maintenance

You perform most monitoring and maintenance of the BPX switch via the BPX switch operating system software. Preventive maintenance of the BPX switch hardware is minimal and requires only that you periodically check:

1. The node supply voltage and internal cabinet temperature by using the **dspasm** command. The temperature should not exceed 50°C.
2. The event log by using the **dsplog** command.
3. The Software Abort Table by using the **dspabortlog** command**.**
4. The network alarm status by using the **dspalms** command.

Software Error and Abort Tables

The BPX software logs noncritical errors into the Software Error Table. It contains up to 12 entries.

The BPX 9.3.X software logs critical errors into a separate Software Abort Table, so that there is no chance of critical errors being overwritten by noncritical errors. It contains up to 12 entries. Use the command **dspabortlog** to display the contents of the Software Abort Table and the command **clrabortlog** to clear it.

Troubleshooting the BPX Switch

This section describes basic troubleshooting steps to be taken for some of the more obvious node failures (refer to Table 28-1). This is not an exhaustive set of procedures, and does not take into account any of the diagnostic or network tools available to troubleshoot the BPX switch. Refer to the *Cisco WAN Switching Command Reference* for information on commands and command usage.

Caution Do not perform any disruptive tests or repairs to the BPX switch on your own. Before proceeding with troubleshooting, call Customer Service so they can provide you with assistance in locating the fault and provide repair information.

General Troubleshooting Procedures

The BPX switch runs self-tests continuously to ensure proper function. When the node finds an error condition that affects its operation, it downs the card or trunk affected. It then selects a standby card or alternate trunk if one is available.

The FAIL indicators on the cards indicate that the system has found these cards defective in some mode, and now considers them as failed cards. Use Table 28-1 to find the cause and obtain the information on replacing the failed component.

Caution Never remove the active BCC until the standby BCC has entered the Standby mode. Using the **dspcd** command is the only reliable way to determine that the standby BCC has finished updating and has entered the Standby mode.

Caution When using Table 28-1 for troubleshooting, call Cisco Customer Service before performing any disruptive testing or attempting to repair the BPX switch. This ensures that you have isolated the correct problem area. It also enables Cisco Customer Service to provide assistance in performing the necessary procedures.

Warning **Contact Cisco Customer Service before attempting to replace fuses on backplane.**

Table 28-1 Troubleshooting the BPX Switch

Symptom	Probable Cause	Remedy
Front panel LED on individual card not lighted.	Card Fuse.	Check card fuse. Replace if defective. Try another card of the same type. If still no LED lighted, backplane card slot fuse may be defective.
No front panel LEDs are lighted.	AC Systems: Circuit Breakers on AC Power Supply Tray. DC Systems: Circuit breakers on Power Entry Module(s) switched off.	Switch on circuit breakers. If problem persists, pull all cards and power supplies out to see if a shorted card or supply exists.
	BPX switch power cord plug dislodged from AC receptacle.	Check that no one is working on the system, shut off source breaker, then reconnect power cord.
Power supply **ac** LED lit but **dc** LED not lit.	Power supply defective.	Check DC on LEDs on ASM. If out, remove and replace power supply. If on, PS LED probably defective.
Card front panel **fail** LED lit.	Card failed self-test.	Check status of card at NMS terminal using **dspcds** screen. If alarm confirmed, try card reset (**resetcd** command). Finally, remove and replace the card.
Card **stby** LED on.	Card is off-line.	Not a problem as long as primary card is active.
ASM **major** or **minor** LED on.	Service-affecting (major) or non-service-affecting (minor) system fault.	Check NMS event log to identify problem reported.
	Failed card in local node.	See remedy for card **fail** LED indication.
	Network trunk failed.	Observe **Port** LEDs on each BNI or BXM (ports configured in trunk mode). Use NMS **dsptrk to** locate failure.
	Failure in remote node. May be another BPX switch.	Use NMS **dspnw** screen to locate node in alarm. Refer to *Cisco WAN Switching Command Reference* for additional information.
	Internal temperature is higher than normal resulting from blocked air flow or defective fan.	Check front and back of node cabinet for freedom of air flow. Replace any fan that may have failed or slowed. Use NMS **dsppwr** screen to check node temperature.
ASM **hist** LED lit.	If no other alarm indications, a fault occurred in the past but has been cleared.	Press ASM **history clear** button. Check NMS event log to determine cause.
BXM **Port** LED is red or orange (BXM configured for trunk mode).	Trunk is in local or remote alarm.	Use NMS **dsptrk** screen to confirm trouble.
BNI **Port** LED is red or orange.	Trunk is in local or remote alarm.	Use NMS **dsptrk** screen to confirm trouble. Use short BNC loopback cable at LM-BNI connectors for local test of trunk. Loop trunk at DSX-3 cross-connect to check cable.

Table 28-1 Troubleshooting the BPX Switch (continued)

Symptom	Probable Cause	Remedy
No BXM **card** or **port** LED on.	No trunks or lines, as applicable on card, are upped. Card has not necessarily failed.	Up at least one of the trunks or lines, as applicable, associated with the card (Trunks if BXM configured for trunk mode, lines if BXM configured for port mode).
No BME **card** or **port** LED on.	No lines are upped. Card has not necessarily failed.	Up at least one of lines, as applicable, associated with the card.
No BNI **card** or **port** LED on.	No trunks on card are upped. Card not necessarily failed.	Up at least one of the trunks associated with the card.
BXM **Port** LED is red or orange (BXM configured for port mode)	Line is in local or remote alarm.	Use NMS **dsplns** screen to confirm trouble.
BME **Port** LED is red or orange	Line is in local or remote alarm.	Use NMS **dsplns** screen to confirm trouble.
BCC **fail** LED flashing	Downloading system software or configuration data.	Wait for download to complete.
BCC **LAN** LED flashing	Normal for node connected to NMS terminal over Ethernet. If it does **not** flash, there may be problems with node to NMS data path.	Check that the cabling to the NMS is firmly connected to the LAN port on the LM-BCC back card. An alternate connection is to the control port.
No BCC card LED on.	Preparing to download new software (momentary condition).	Wait for download to begin.
	Command issued to run a software revision that was not available in the network.	Check that proper s/w revision is available on another node or on NMS.

Displaying the Status of Cards in the Node

When a card indicates a failed condition on the alarm summary screen, use the Display Cards (**dspcds**) command to display the status of the circuit cards on a node. The information displayed for each card type includes the card slot number, software revision level, and the status of the card.

The possible status description for each card type are listed in Table 28-2. Refer to the *Cisco WAN Switching Command Reference* for more information on the Display Cards command.

Table 28-2 Card Status for the BPX Switch

Card Type	Status[1]	Description
All card types	Active	Active card.
	Active - F	Active card with no terminal failure.
	Standby	Standby card.
	Standby - F	Standby card with no terminal failure.
	Standby - T	Standby card performing diagnostics.
	Standby - F -T	Standby card with no terminal failure performing diagnostics.
	Failed	Card with terminal failure.

Table 28-2 Card Status for the BPX Switch (continued)

Card Type	Status[1]	Description
	Unavailable	Card is present but it may be in one of the following states: a. The node does not recognize the card. b. The card is running diagnostics.
	Down	Downed card.
	Empty	No card in that slot.
BCC	Same status as for all card types, plus:	
	Updating	Standby BCC downloading the network configuration from an active BCC. Note: Red FAIL LED flashes during updating.
	Cleared	BCC is preparing to become active.
	Downloading Software	There are downloader commands that appear when the system is down loading software to the BCC.
	Minor	BCC Redundancy alarm indicates node is configured for redundancy but no standby BCC is equipped.

[1] Cards with an F status (no terminal failure) are activated only when necessary. Cards with a failed status are never activated.

System Troubleshooting Tools

You can perform a number of manually initiated tests from the Cisco WAN Manager NMS console to assist in system troubleshooting. These tests may be included in a job so they can be scheduled to run remotely at a specified time if desired.

User-Initiated Tests

Several user-initiated tests can be used to diagnose system problems. These tests are self-contained in that they do not require the use of external test equipment. They also do not require you to place a loopback at the far end to test both directions of transmission. These tests are listed in Table 28-3.

Several display commands can be used to obtain information that may be helpful in troubleshooting system problems. These are also listed in Table 28-3.

Table 28-3 System Troubleshooting Commands Available

Command	Description
Test Connection (**tstcon**)—Frame Relay	Performs a bidirectional test of the specified Frame Relay connection or range of connections by inserting a test pattern and comparing the returned pattern with the pattern transmitted. A pass or fail indication appears next to the tested connection in the Display Connections screen.
Test Connection (**tstcon**)—data	Same as above except for synchronous data connections.
Test Connection (**tstcon**)—voice	Same as above except for voice connections.
Test Delay (**tstdelay**)—Frame Relay	Measures the round-trip delay over the selected Frame Relay connection.
Test Port (**tstport**)—Frame Relay	Tests the operation of the selected Frame Relay port on the node.

Table 28-3 System Troubleshooting Commands Available (continued)

Command	Description
Test Port (**tstport**)—data	Same as above except for synchronous data ports.
Display Connection States (**dspconst**)	Displays in real-time the status of all voice connections terminating at a specified node.
Display Breakout Box (**dspbob**)—Frame Relay	Displays in real-time the status of data and control leads on selected Frame Relay connection.
Display Breakout Box (**dspbob**)—data	Same as above for synchronous data connections.
Display Breakout Box (**dspbob**)—trunk	Same as above for network subrate trunks.
Display Buses (**dspbuses**)	Displays the status of system buses.
Display Slot Errors (**dspsloterrs**)	Displays any data errors associated with the slots in a BPX node.
Display Slot Alarms (**dspslotalms**)	Displays any alarms associated with the slots in a BPX node.
Display Trunk Errors (**dsptrkerrs**)	Displays any data errors associated with the network trunks connected to a node.

Loopback Tests

Various loopback paths can be set up to help diagnose transmission problems. These rely on the use of external test equipment to provide the source of a test signal.

The available loopback commands are listed in Table 28-4.

You set up a local loopback path (LL) in the local node at the PAD card (FRP) associated with the port or connection to be tested. You then apply a test signal to the input. This passes through the associated Interface Card (FRI), is sent to the Frame Relay PAD card (FRP) over the system bus where it is looped back toward the input. This tests the cabling and the local node processing of the signal.

Table 28-4 System Loopback Tests

Command	Description
Add Local Loopback (**addloclp**)—Frame Relay port	Adds a loopback path at the Frame Relay port from the transmit side back to the receive side at the local node.
Add Local Loopback (**addloclp**)—Frame Relay connection	Does the same as above only for an individual Frame Relay connection.
Add Local Loopback (**addloclp**)—data	Adds a loopback path at the synchronous data port from the transmit side back to the receive side at the local node.
Add Local Loopback (**addloclp**)—voice	Adds a loopback path for an individual voice channel on a circuit line at the local node.
Add Remote Loopback (**addrmtlp**)—Frame Relay port	Adds a loopback path at the Frame Relay port from the transmit side back to the receive side at the remote node.
Add Remote Loopback (**addrmtlp**)—Frame Relay connection	Does the same as above only for an individual Frame Relay connection.
Add Remote Loopback (**addrmtlp**)—data	Adds a loopback path at the synchronous data port from the transmit side back to the receive side at the remote node.

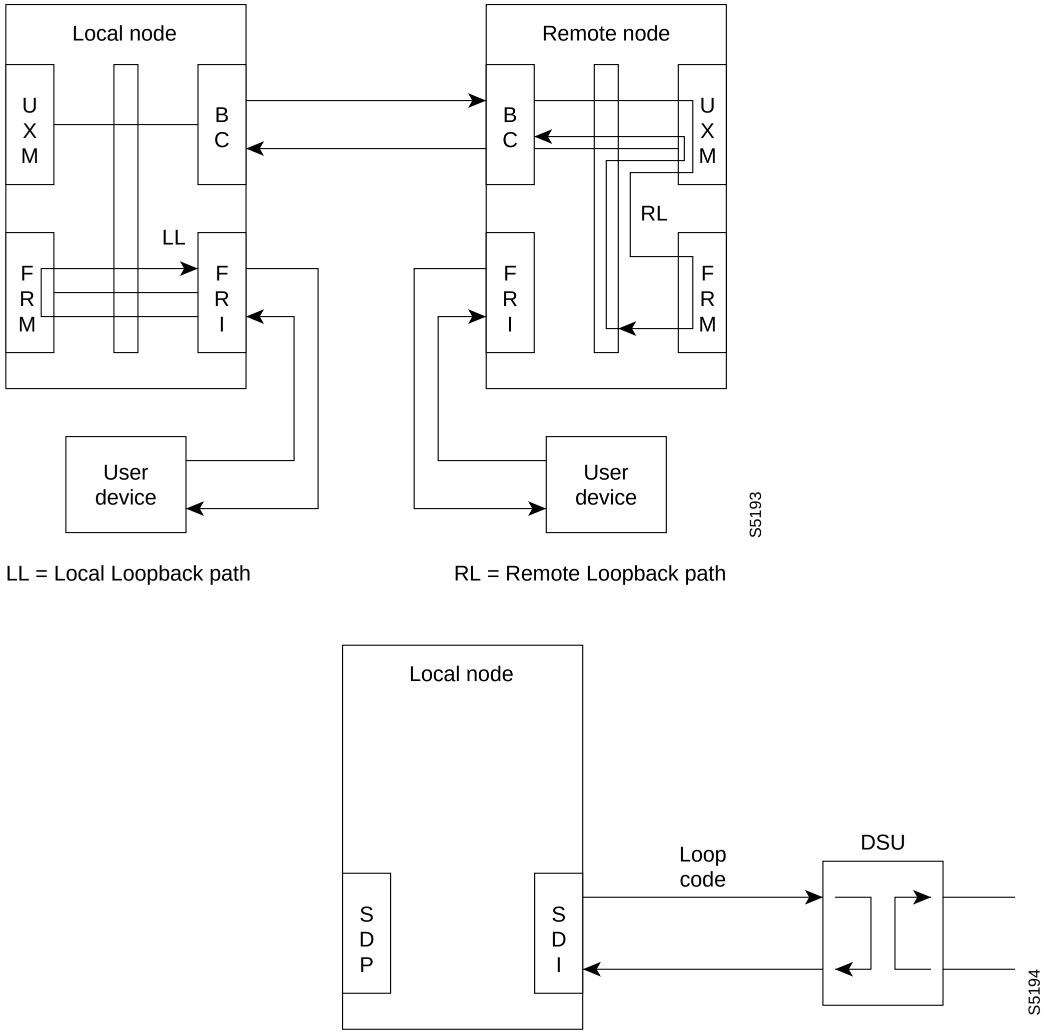
Table 28-4 System Loopback Tests

Command	Description
Add Remote Loopback (**addrmtlp**)—voice	Adds a loopback path for an individual voice channel on a circuit line at the remote node.
Add External Loopback (**addextlp**)—data	Activates a near end or far end loopback on an external device, such as a DSU, connected to a synchronous data port.

A remote loopback path (RL) is set up in the remote node also at the PAD card (FRP). But, in this case, the signal travels over the network and through the remote node processing equipment but does not include the remote node Interface Card (FRI) or associated cabling. These components would be tested using another local loopback at the remote node.

The external loopback command finds limited use in data applications where an external data interface unit (DSU or CSU) is attached to the local node data interface card, illustrated by the SDI card in . The local node transmits the appropriate loopback codes out the circuit line towards the external device and then sets up the appropriate loopback path (See Figure 28-1).

Figure 28-1 Network Loopback Paths



Connection Testing

System software includes a Test Connection (**tstcon**) command for testing network connections. This test is initiated by the network operator from the NMS console and can be performed at any time, but it momentarily interrupts traffic on the connection during the test. Connection testing should be performed only when an alarm has been reported from the connection or during off-hours.

Test Connection tests both directions of transmission from end to end and displays a pass or fail indication for each connection tested. You may specify:

- a single connection
- all connections
- all connections of a particular type (voice, data, or Frame Relay)
- a starting and ending connection number

In addition to testing the connection, the Test Connection routine will attempt to isolate and repair any failure it detects. The controller card at the node where the Test Connection (**tstcon**) command is issued instructs the service card to build packets containing special test frames. These packets are sent across the network to the terminating node, which depacketizes them, repacketizes the frame, and sends them back to the originating node where the returned frame is analyzed.

If the returned test pattern is incorrect, the system goes into an automatic fault isolation mode. Controllers in the various nodes along the connection route communicate with each other over an overhead message channel separate from the normal circuits.

The test pattern continues to be transmitted and analyzed at each node along the path as it is transmitted and as it is received until the failed network element is identified. Redundant cards may be switched into operation and routing tables in associated network trunk cards may be reprogrammed in an attempt to correct the problem. If all else fails, the suspected path and/or network component is then reported to the network manager (NMS).

External Device Window

External devices connected to network nodes, such as bridges, routers, or sub-rate multiplexers may be accessed through the NMS Window command. This feature provides a direct command line interface to external devices from the NMS console. Depending on the capability of the external device, it is often possible to report status and alarms and to control or configure the device through an RS232 port connection.

The following example illustrates a Window display of a router connected to the local node. In this example, the window is used to initiate a ping of the router connection.

```
Example: NMS Window to a Local Router
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 Echos to 192.9.202.1, timeout is 2 seconds:

. . . . .

Success rate is 100 percent
```

Troubleshooting SONET Automatic Protection System

Introduction

For APS line redundancy, these problems can occur:

- APS Configuration Problems, page 28-10
  - Not Able to Correctly Set Up APS 1+1 Line Redundancy Configuration, page 28-10
  - Unable to Set Up APS 1:1 Line Redundancy Configuration, page 28-11
  - Operator Information about APS Architectures, page 28-11
- Operational Problems, page 28-12
  - What the Various APS Switches Mean
  - Unable to Perform APS External Switch After Forced or Manual APS Switch, page 28-13
  - APS Manual Switch to a Line Does Not Occur Right Away, page 28-13
  - Switch Occurs After Lockout Issued, page 28-13
  - APS Switch Made to a Line in Alarm, page 28-14
  - Reverse Switch, page 28-14
  - APS Switch Occurs at the Same Time as a Y-Red Switch, page 28-14
  - APS Switch Occurs After Issuing an APS Clear Switch, page 28-15
  - APS Switch Occurs Even Though APS Forced Switch in Effect, page 28-15
  - APS Line is Failing to Switch, page 28-15
  - Large Cell Loss When Performing a Front Card Switchover, page 28-15
  - APS Service Switch Description, page 28-15
  - APS Line Does Not Seem to Switch and Active Line is in Alarm, page 28-16
  - BXM Back Card LED Green and Yellow Indications, page 28-17
  - BXM Port LED States, page 28-17
- APS Alarms
  - What Do APS Alarms Represent

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 set up the APS line redundancy configuration. For APS 1+1 configurations, BPX software supporting APS and BXM firmware supporting APS must be used.

These 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.

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.

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 does not let you configure any combination of APS architectures.

Initial Investigation: You can change the APS configuration by using the **cnfapsln** command; however, not all combinations are allowed. Here is a table of combinations allowed and disallowed.

	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**
Bidirectional	Default	Not Valid	Valid option	Valid option	Not Valid	Default
Unidirectional	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**).

Operational Problems

This section describe possible APS operational problems and troubleshooting techniques for each.

Initial Investigation of APS Switch Operations

There are ten reasons an APS switch might occur. You can view these logged reasons by using the **dsplog** command. When the BXM switches an APS line it returns an event message to the SWSW with the reason why it switched and which line is active.

This list shows the possible conditions that might 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 preselected threshold (**cnfapsln**).
5. Manual Switch
An external user requested switch that 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 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 bidirectional 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: After performing 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), when the user again tries to perform a forced switch to the protection line, nothing happens.

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: After issuing 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-requested) APS clear switch (**switchapsln** Ln1 Ln2 1) will disable the lockout.

APS Switch Made to a Line in Alarm

Description: After performing a forced switch to a line with a line alarm, the switch is successful in 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 enables you 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 Y-Red 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 Y-red (**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 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 bidirectional and the other is unidirectional.

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 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 result of the card redundant switch (Y-red switch) and there will be up to 250 ms 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 applicable only to APS 1+1 configuration. It enables switching all APS lines on a card by using 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.

Important: Be sure that the associated front card is active for the back card that is to remain in the rack. You might 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: 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 preceding 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, this could be the problem (see 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 that 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".

Workaround: 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 you 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 effect 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 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 the 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.

BME Connection Diagnostics

- **tstconseg** and **tstdelay** commands may be used to troubleshoot a leaf connection both from the BME end point as well as on the other end point.
- **tstconseg** is available on the root connection only on the non-BME end point.
- **tstconseg** is not supported from the BME end of the root connection.
- **tstdelay** is not supported on root connections.

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 coexist. 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 worst case is if the BPX has all BXM cards in the node, therefore the master end point (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 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

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 that will support more than one port group. The commands **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, typically.

(num_chans / num_of_port_groups).

cnfrsrc Fails with “Available Channels is 0”

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.

This might not be a problem because the user might 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 workaround depends on where the problem is. If the problem is with PVCs, try **cnfrsrc** and change the number of pvcs. Since **switchcc** will rebuild the channel database, try executing **switchcc**.

Here is a list of things that should be done:

- Capture the **dspchuse** screen and compare against the **cnfrsrc** and **cnftrk** commands.
- 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** or node rebuild.

cnfrsrc Fails with "Automatic Routing Management is Currently Using the Channel Space"

This error is indicates that there are Automatic Routing Management channels currently configured on the space that the user wants for VSI.

For example: The BXM card supports 100 channels, with 50 of the channels configured for PVCs and 50 for VSI ranging from 51–100. Assume that the card has five connections on channel 45–49. Now change the configuration of PVCs to 10. The command will work since only five 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.

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 workaround is to 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, delete and re-add the connection.

Troubleshooting Commands

Table 28-5 Troubleshooting Command List

Command	Full Name
addalmslot	Add alarm slot
addextlp	Add external loopback
addloclp	Add local loopback
addlocrmtlp	Add local-remote loopback
addrmtlp	Add remote loopback
clrabortlog	Clear critical errors from the Software Abort Table
clrchstats	Clear channel statistics

Table 28-5 Troubleshooting Command List (continued)

Command	Full Name
clrclkalm	Clear clock alarm
clrclnalm	Clear circuit line alarm
clrclnerrs	Clear circuit line errors
clreventq	Clear the events queues
clrlnalm	Clear line alarm
clrlnerrs	Clear line errors
clrlog	Clear log
clrmsgalm	Clear message alarm
clrphyslnalm	Clear physical line alarms
clrphyslnerrs	Clear physical line errors
clrportstats	Clear port statistics
clrslotalms	Clear slot alarms
clrsloterrs	Clear slot errors
clrtrkalm	Clear trunk alarm
clrtrkerrs	Clear trunk errors
clrtrkstats	Clear trunk statistics
cnflnalm	Configure line alarm
cnfoamlpbk	Configure OAM loopback test
cnfslotalm	Configure slot alarm
cnftrkalm	Configure trunk alarm
dellp	Delete loopback
dncd	Down card
dspabortlog	Display critical errors in the Software Abort Table
dspalms	Display alarms
dspbuses	Display Buses
dspclnerrs	Display circuit line errors
dspcntrstats	Display in realtime all counter statistics of s specified entity.
dspeventq	Display the event queue names and the data in each.
dspfrcbob	Display FRC-2/FRM-2 breakout box
dsplog	Display event log
dsplnalmcnf	Display line alarm configuration
dsplnerrs	Display line errors
dspoamlpbk	Display OAM loopback test
dsppwr	Display power
dspslotalms	Display slot alarms
dspsloterrs	Display slot errors

Table 28-5 Troubleshooting Command List (continued)

Command	Full Name
dspslotstatcnf	Display slot statistics configuration
dspsv3	Display Cisco WAN Manager L3 (layer 3) Link Control Blocks
dsptrafficgen	Display whether Traffic Generation feature for card slot is enabled
dsptrkerrs	Display individual or all trunk errors
prtclnerrs	Print circuit line errors
prtlnerrs	Print line errors
prtlog	Print log
prttrkerrs	Print trunk errors
resetcd	Reset card
resetpc	Reset Port Concentrator
switchcc	Switch controller card
tstcon	Test connection
tstconseg	Test connection segment
tstdelay	Test delay
tstpcs	Test Port Concentrator Shelf
tstport	Test port
tstubus	Test cell bus

Replacing Parts

This chapter describes the replacement of major BPX switch components:

- Replacing a Front Card
- Replacing a Line Module
- Replacing a DC Power Entry Module
- Replacing an AC Power Supply
- Replacing the Fan Assembly

After an alarm occurs, use the BPX switch software to isolate the problem. If an BPX switch part has failed, then it must be replaced. For information on alarms, see *Chapter 27, Alarms and Statistics*. For general procedures dealing with problems, see *Chapter 28, Troubleshooting.*

Caution Only authorized personnel should remove and replace parts on the BPX switch system.

Parts should be replaced only by qualified personnel who have taken the Cisco training courses or been trained by a qualified system manager. For assistance in diagnosing or replacing a failed part, call Cisco Customer Service.

When replacing a part, save the electrostatic bag, foam, and carton that the new part comes in. These packaging materials are needed for returning the failed part to Cisco. Contact Customer Service for information on returning parts.

Replacing a Front Card

The BPX switch front cards are:

- Broadband Controller Card (BCC)
- BXM-T3/E3, BXM-155, BXM-622
- Broadband Network Interface Card (BNI)
- Alarm and Status Monitor (ASM)

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the wrist strap lead to the cabinet.

When a card has failed, the red FAIL indicator for that card turns on. Before replacing it, check to see if the card needs only to be reseated. After reseating the card, wait for it to run its self-tests to see if the ACTIVE light comes on. If the card is seated correctly, but the FAIL light is still on, replace the card.

To remove a front cards:

Step 1 If the front panel **fail** lamp is on, remove the card and go to Step 3. Otherwise, go to Step 2.

Step 2 Check the status of the card by using the **dspcd** or **dspcds** commands. It should be failed or standby if the node is actively carrying traffic.

Step 3 If an active BNI card must be replaced, "down" it first by using the **dncd** command. Removing an active card affects operation only slightly if there is a standby card.

Step 4 If a BCC has failed, the other BCC will switch from standby mode to active. Use the **dspcd** command to verify that the standby BCC has entered the active mode. Then you can remove the failed BCC.

Caution Never remove the active BCC until the standby BCC has entered the "active" mode. Using the **dspc**d command is the only reliable way to determine that the standby BCC has finished updating and has entered the "active" mode.

Step 5 Unlatch the Air Intake Grille. Locate the small access hole in the top, center of the Air Intake Grille.

Step 6 Fully insert a medium, flat-bladed screwdriver in the access hole.

Step 7 Rotate the screwdriver to release the spring latch holding the grille. (Figure 29-1). The top of the grille should pop out.

Step 8 Tilt the grille forward to approximately a 45° angle.

Step 9 Put on a wrist strap to discharge any static.

Step 10 Rotate the top and bottom card extractors on the front of the card.

Step 11 Hold the card at the top and bottom and gently slide it out of the slot.

To install a front card in the BPX switch:

Step 1 Unlatch the Air Intake Grille as described in Step 5 through Step 8 of the previous procedure for removing the front card.

Step 2 Remove the replacement card from the antistatic shipping container.

Step 3 Hold the replacement card at top and bottom and gently insert it over the guides, and slide it all the way to the rear of the cabinet.

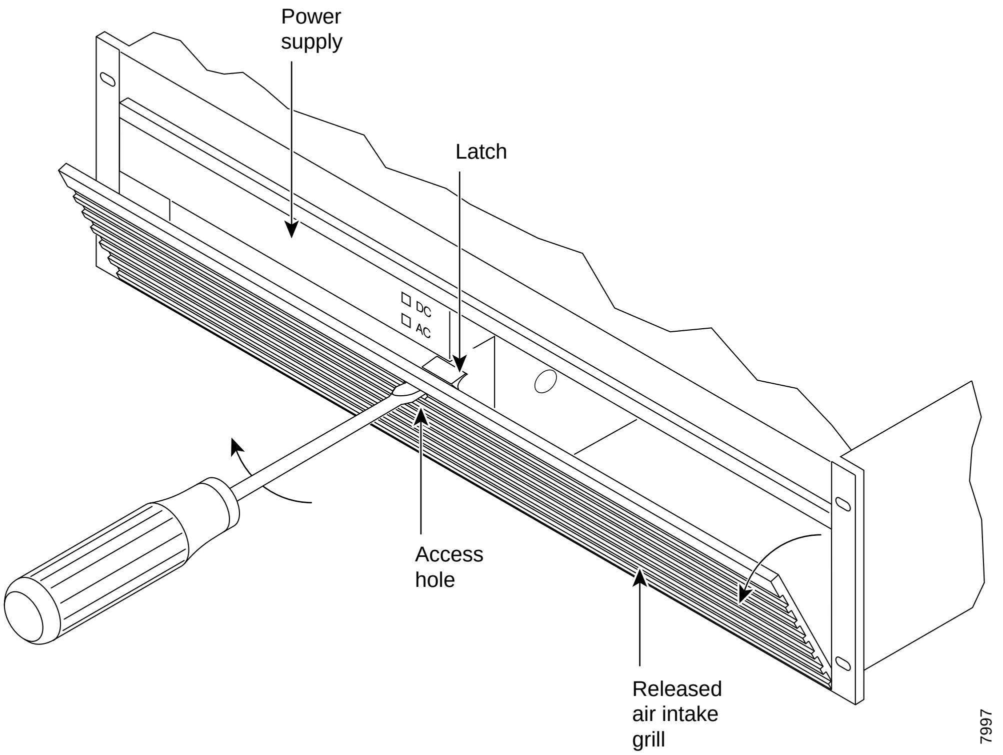
Note The card should slide in easily with a light sliding friction from the EMI gaskets on adjacent cards. If it does not, check to see if there is anything restricting it—do not use excessive force.

Step 4 Rotate the top and bottom latches on the card and push the card into the rear connector. You will feel the card seat itself as you push it in.

Step 5 Press firmly on the top and bottom extractors to complete the card seating process. The extractor should snap back to a vertical position after the card is properly seated.

Step 6 Replace the air intake grille by swinging it up and pressing in at the top until the latch snaps into place.

Figure 29-1 Unlatching the Air Intake Grille



Replacing a Line Module

The configuration of the back card may be slightly different depending on whether it is a single card or redundant card configuration. A standby card in a redundant card configuration may be removed without disrupting system operation even if it is a BCC. Removing a single card, however, will cause a system outage.

Caution Removing an active, single back card disrupts service on the node.

To remove a line module:

Step 1 Check the status of the card using the **dspcd** or **dspcds** command. It should be failed or standby or replacement will affect operation of the node.

Step 2 If an active card needs to be replaced, “down” it first with the **dncd** command. Removing an active card affects operation only slightly if there is a standby card.

Step 3 Before removing a LM-BCC, make sure the standby BCC **stby** indicator is on steady. A flashing **stby** indicator indicates it is in the process of downloading either configuration data or software and is not ready to accept a transfer.

Step 4 For a single card configuration, disconnect the cables from the back card face plate. Make a note of the location of each cable so that it can be replaced correctly.

Step 5 For a redundant card configuration, disconnect the appropriate leg of the Y-cable connecting to the back card to be replaced. DO NOT REMOVE THE OTHER LEG GOING TO THE BACKUP CARD.

Step 6 Loosen the two captive screws on the back card faceplate and, pulling on the top and bottom card extractors, slide the card straight out of the shelf slot. (See Figure 29-2.)

To install a line module:

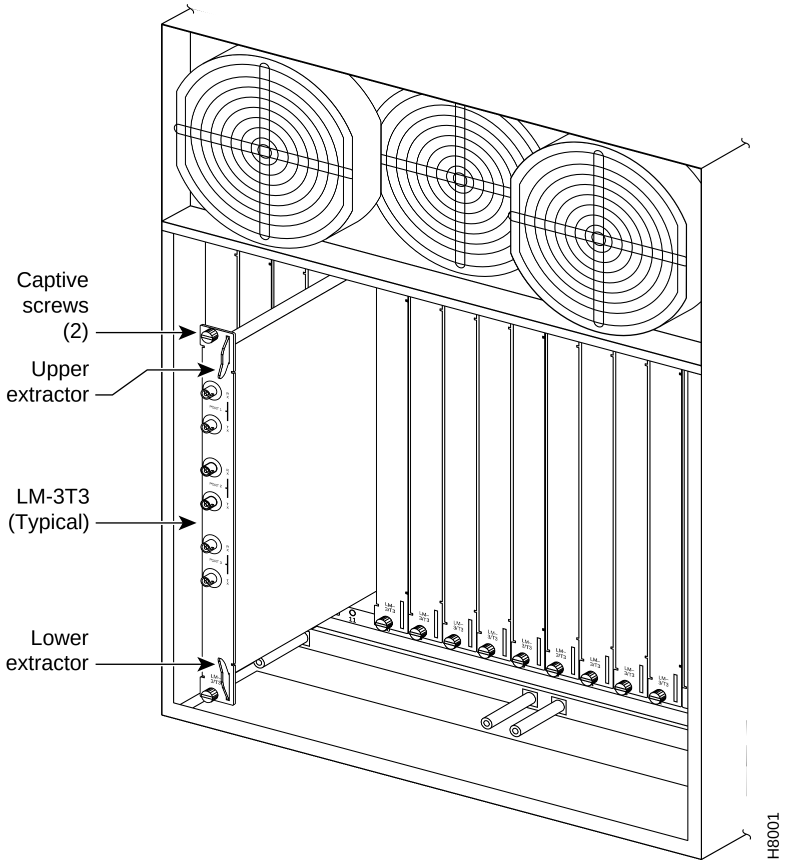
Step 1 Insert the line module (such as, LM-3T3) into the slot from which the defective card was removed (see Figure 29-2).

Step 2 Tighten the two captive screws. Tighten securely, but do not overtighten.

Step 3 Reconnect the T3 trunk cables to the LM-3T3 connectors from which they were disconnected.

Step 4 Perform the appropriate steps to bring the lines that were disconnected back on line.

Figure 29-2 Removing a Line Module



Replacing a DC Power Entry Module

DC Power Entry Modules (PEMs) contain few active components so they should rarely need replacement. Access is from the back of the node.

To remove a PEM:

Step 1 Check the node system voltage by using the Display Power (**dsppwr)** command. Note which input has failed, A or B. Power Supply A is the unit on the right side facing the rear of the node.

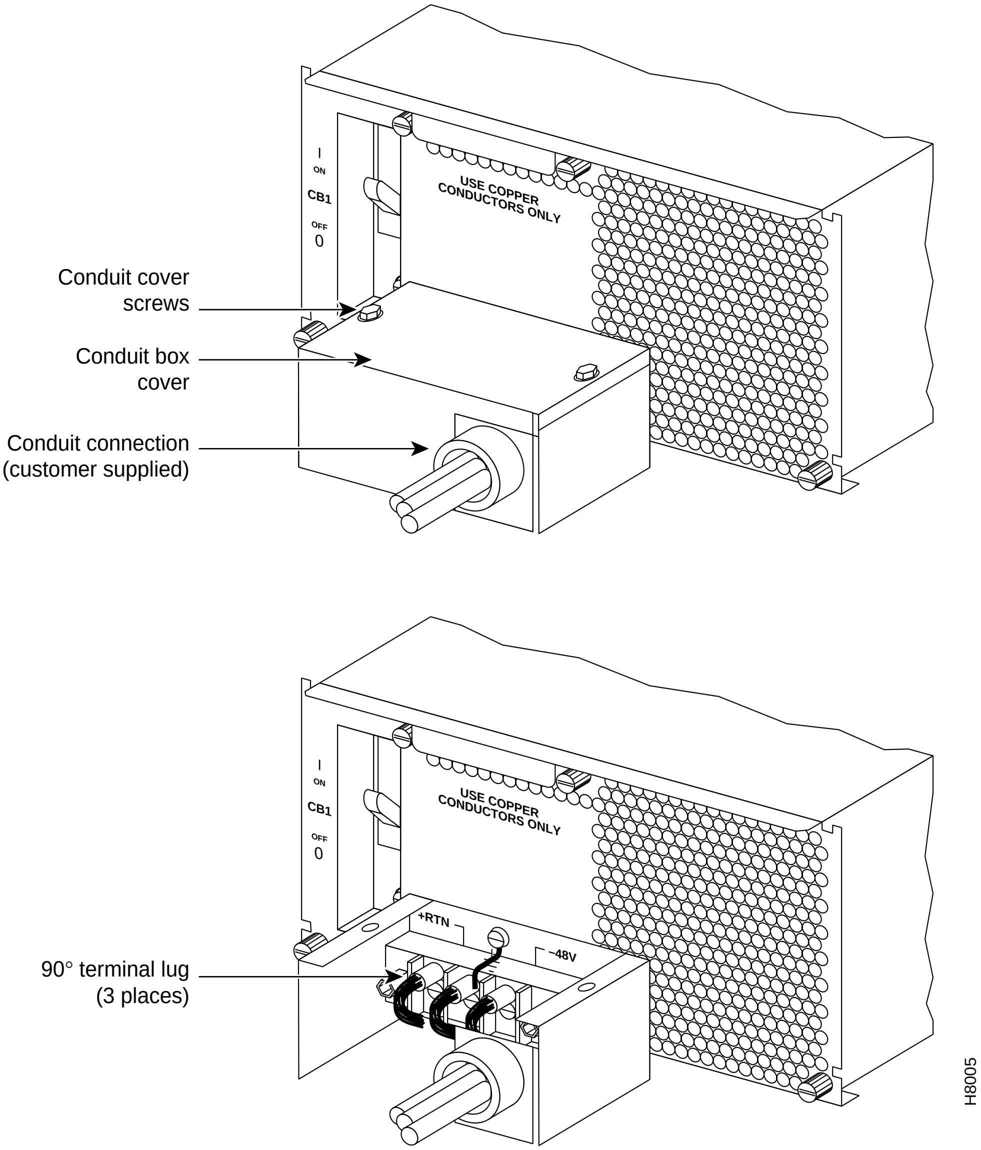
Step 2 Turn off the primary source of power to the PEM to be replaced.

Step 3 Turn off the circuit breaker on the PEM to be replaced.

Step 4 Remove the two screws holding the conduit box cover (see Figure 29-3). Or, remove the plastic cover plate over the input terminal block.

Step 5 Remove the power input wiring at the PEM terminal block.

Figure 29-3 DC Power Entry Module with Conduit Box



Step 6 If a conduit box is used, remove it. Remove the ground screw above the middle terminal block connector (see Figure 29-3).

Step 7 Remove the two standoffs on each side of the terminal block and pull the conduit box straight back. Set it aside. Do not try to remove the terminal block.

Step 8 Loosen the two captive screws (at the bottom corners) holding the PEM. Loosen the two connector jackscrews adjacent to the finger pull.

Step 9 Grasp the finger pull lip at the top of the PEM and pull the unit straight out.

Step 10 Replacement is the reverse of removal.

Replacing an AC Power Supply

BPX switches are powered by redundant power supplies; either power supply can supply the current requirements of the node. The AC Power Supply is part of an assembly which is replaced as a single unit. Access to the AC Power Supply assembly is from the front, but first, the Air Intake Grille must be removed.

To remove a power supply:

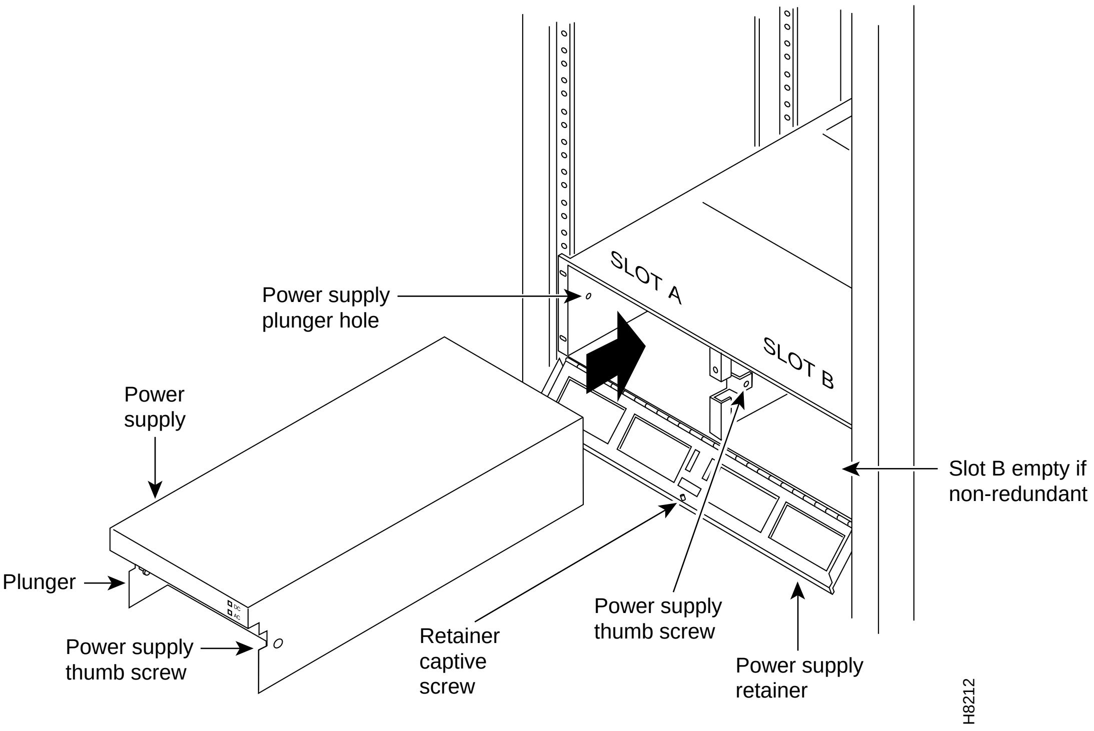
Step 1 If you haven’t already done so, check the status and output voltage of the power supplies at the node using the **dspasm** command. Note which power supply is failed, A or B. Power supply A is on the right side facing the rear of the node.

Step 2 Remove the Air Intake Grille. Locate the small access hole in the top, center of the Air Intake Grille.

Step 3 Fully insert a flat-bladed screwdriver (with a 1/4 in. blade) in the access hole.

Step 4 Rotate the screwdriver to release the spring latch holding the Air Intake Grille (see Figure 29-4). The grille should pop out.

Figure 29-4 AC Power Supply Assembly



Step 5 Tilt the grille forward approximately a 45° angle, then lift if out and set it aside. This exposes the power supply retainer bracket.

Step 6 With a flat-bladed screwdriver, loosen the retainer bracket hold-down screw in the center of the bracket and tilt the bracket.

Step 7 Identify which power supply needs replacement. Power supply A is the unit on the left, B is on the right. In most cases, the failed unit will be identified by a front panel lamp indication.

Step 8 There are two power supply securing fasteners, one on each side of the power supply assembly (Figure 29-4). The one on the left of each supply is a spring-loaded pin, the one on the right of each supply is a normal thumb-screw. Loosen the thumb-screw on the right.

Step 9 With the right hand, grip the power supply under the front panel. With the left hand, pull out the spring-loaded pin on the left side of the supply and hold it out as you pull out the power supply assembly.

Step 10 The power supply assembly weighs approximately 15 pounds (33 Kgs.). Support the bottom of the power supply as you pull it straight out, until it is free of the shelf.

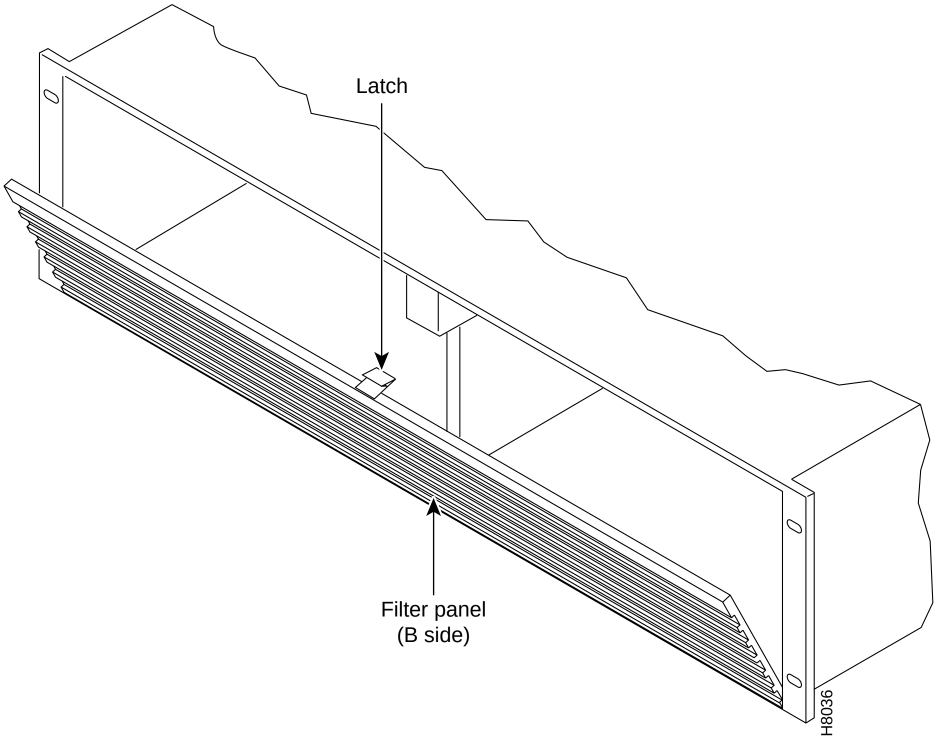
Field-Installing a Second AC Power Supply

To field-install a redundant power supply:

Step 1 If the front Air Intake Grille has already been removed, go to the next step.
If not, remove it using Step 2 through Step 6 of the previous procedure.

Step 2 If converting a node from single to redundant powering, first remove the blank filler panel over position B (right side). With Air Intake Grille open, remove three screws attaching the filler panel to the retainer bracket (see Figure 29-5).

Figure 29-5 Removing Blank Filler Panel (B side shown)



Step 3 Slide a replacement power supply assembly into the tracks of the power supply shelf.

Step 4 When the power supply is completely seated, the spring-loaded pin will snap into place to assure that the power supply has mated with its connector.

Step 5 Screw in the thumb-screw on the right side of the power supply assembly until it is finger tight.

Step 6 Flip the retaining bracket up and tighten its thumbscrew.

Step 7 Reinstall the Air Intake Grille and press firmly on the top, center of the Air Intake Grille until the latch snaps into place.

Step 8 Check the status and output voltage of the replacement power supply using the **dspasm** command. Make sure the status is OK and the output voltage is 48V.

Replacing the Fan Assembly

The Fan Assembly provides the primary cooling for the BPX switch and is located at the top, rear of the BPX switch cabinet.

There are three fans in the Fan Assembly. The fan on the right (number 1) and the one on the left (number 3) can be changed out individually with very little effort or interruption in the operation of the node. However, to replace the fan in the middle (number 2) you must first power down the node and remove the Fan Assembly.

Caution You must work quickly but carefully to prevent heat buildup in the node, which could damage the cards.

To replace fan number 1 or number 3 in the Fan Assembly:

Step 1 Use the **dspasm** command to check the status of the three fans.

Step 2 From the rear of the BPX switch, visually check that the fan(s) is indeed not turning or turning slowly.

Step 3 From the back of the cabinet, unplug the small fan power cord from its appropriate receptacle on the Fan Assembly.

Step 4 Remove the two screws holding the fan and the fan shield to the-fan housing. Be careful not to drop the hardware into the rear of the cabinet.

Step 5 Remove the fan. Replace the fan in reverse order. Use the existing fan grille.

To replace fan number 2 requires powering down the node and replacing the whole Fan Assembly. Under normal ambient room temperatures, this can be scheduled for the next available quiet time.

To replace fan number 2:

Step 1 Use the **dspasm** command to check the status of the three fans.

Step 2 From the rear of the BPX switch, visually check that fan number 2 is not turning or turning slowly.

Step 3 At the rear of the BPX switch, turn the circuit breakers OFF to power down the node.

Step 4 Loosen the eight captive screws holding the Fan Assembly in place.

Step 5 With one hand, pull the Fan Assembly back just far enough to gain access to the Fan Assembly power cord. This cord connects to the Fan Assembly to the backplane.

Step 6 Unplug the power cord and remove the Fan Assembly.

Step 7 Plug the power cord in the replacement Fan Assembly into the backplane connector.

Step 8 Install the replacement Fan Assembly.

Step 9 Tighten the eight screws holding the Fan Assembly in place.

Replacing the Temperature Sensing Unit

The temperature sensing unit is located on the ASM card. If the temperature indication displayed by using the **dspasm** command does not appear to be correct, try a replacement ASM card.

Replacing Card Slot and Fan Fuses on the System Backplane

There is a separate fuse provided on the System Backplane for each card slot. These fuses are numbered F4 through F18, corresponding to card slots F15 down through F1 (see Figure 29-6).

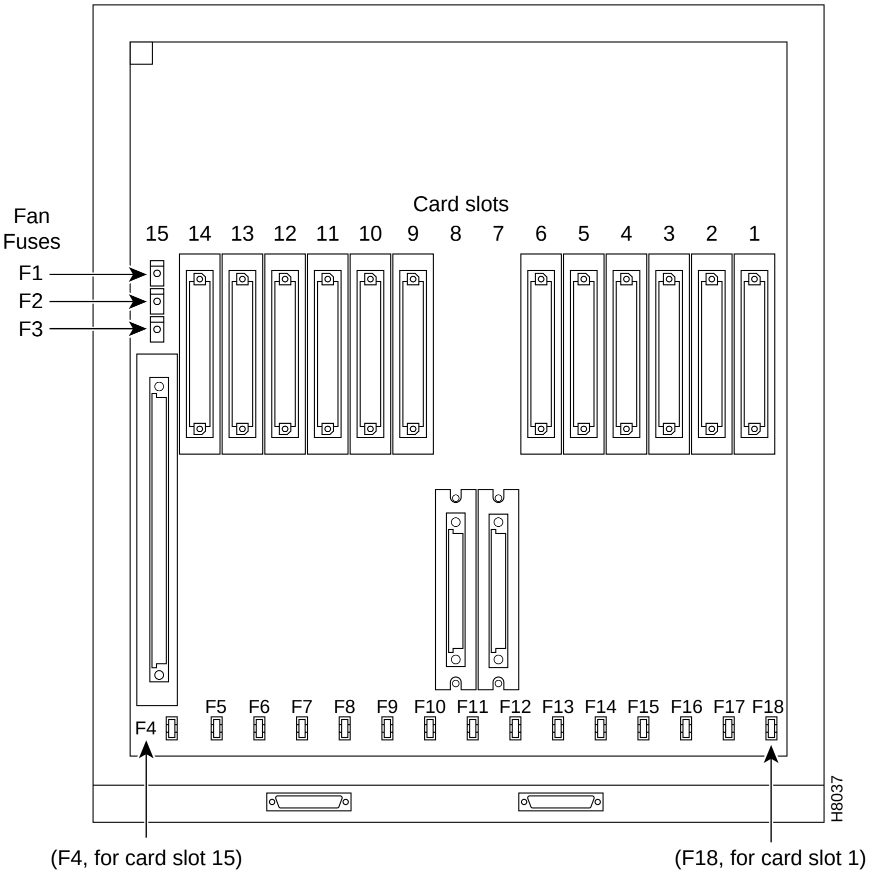
There are three separate fan fuses provided on the System Backplane. These fuses are numbered F1 through F3, corresponding to Fans 1 through 3 (see Figure 29-6).

Warning **For both personnel safety and to prevent equipment damage, power down the BPX switch before replacing fan fuses F1 through F3, or card slot fuses F4 through F18 on the System Backplane. For continued protection against risk of fire, replace only with same type and rating of fuse.**

Backplane fuses rarely need replacement. Backplane fuses are intended to prevent catastrophic damage to the backplane in the event of accidental shorting of -48VDC on the backplane to chassis ground. This type of event could be caused by bent backplane pins, inadvertent contact of conductive elements (EMI Cans, EMI Gaskets, and so on.) to power pins, or (in the case of a fan fuse) a pinched wire harness.

These fuses are located in sockets on the backplane and are therefore not readily accessible. A special tool and a special set of instructions are required for fuse replacement. It is recommended that only factory-trained personnel perform the procedure. Contact Customer Service for further information.

Figure 29-6 Card Slot and Fan Fuse Locations on System Backplane



CHAPTER 30

BPX Node Specifications

This chapter lists information for the BPX system specifications. For the latest information, refer to Cisco online documents.

System Capacity:	1 shelf with 15 card slots. Requires 1 or 2 dedicated slot(s) for BCC card. Requires 1 dedicated slot for ASM card.
Network Interface:	T3, E3, OC3, and OC12.
Network Trunks:	32 per node max.
Network Interface Protocol:	ATM layer using 53-byte cell.
Cell Switching:	Crosspoint switch matrix, non-blocking.
Switch Capacity:	9.6 Gbps or 19.2 Gbps (with BCC-4).
Slot Rate:	800 Mbps each, including overhead.
Connection Rate:	20 million cell connections/sec. between slots.
Classes of Service:	32 queues per port, assignable.
Clock Sources:	Internal, free-running oscillator, Stratum 3. Phase-locked to any appropriate network interface. External input at T1 or E1 rate.
Clock Output:	Single clock output at T1 or E1 rate for synchronizing co-located IGX node or CPE.
Cabinet Size:	22.75 inches (57.8 cm) high 19.0 inches (48.25 cm) wide 27.0 inches (68.6 cm) deep

Weight, approx: 73 lb. (33.2 kg.) empty BPX shelf, w/fans but no PS.
6 lb. (2.7 kg.) each card.
18 lb. (8.2 kg.) empty AC Power Supply Tray.
16 lb. (7.3 kg.) each AC Power Supply.
2 lb. (0.9 kg.) each DC Power Entry module.

Clearance Requirement: At least 30 inches front and rear clearance; nominal 12 inch side clearance.

Power Source: AC system: 180 – 264 VAC, 47 to 63 Hz.
DC system: –42 to –56 VDC.

Power Requirements: AC BPX-15: 13 A at 180 VAC (2300 VA).
DC BPX-15: 40 A at –42 VDC (1680W).

Input Power Connector: AC: 3-conductor IEC receptacle. 8 feet (2.4 m.) power cord supplied.
DC: 3 Ring lug screw terminal connectors.

Circuit Breakers: AC: 15 A on AC power supply assembly.
DC: 40A on power entry module.

Fuses: Individual Backplane Card slot fuses, F1 through F3 for Fans 1 through 3, and F4 through F18 for card slots 1 through 15, 5A-120VAC rating.

Operating Environment: Operating Conditions are listed in Table 30-1.

Shock: Withstands 10G, 10 ms. at 1/2 sine wave.

Vibration: Withstands 1/4 G, 20–500 Hz.

Heat Transfer to Room: **U**p to 7200 BTUs depending on node configuration.

Table 30-1 Ambient Temperature and Humidity Limits

	Limits	
Conditions	**Fahrenheit**	**Centigrade**
Operating Temperature	+40 to +100 degrees	+4.5 to +38 degrees
Recommended	+68 to + 86 degrees	+20 to +30 degrees
Short-Term Temperature[1]	+35 to +120 degrees	+1.7 to + 49 degrees
Operating Relative Humidity	20% to 55% (non-condensing)	
Short-Term Relative Humidity	10% to 80% non-condensing	

[1] Room temperature refers to conditions at a location 5 feet above the floor and 15 inches in front of the equipment.

ATM Trunk Interface (BXM-T3/E3 Cards)

Characteristic	**T3 (DS3)**	**E3**
Line Rate:	44.736 Mbps +/- 20 ppm	34.368 Mbps +/- 20 ppm
Line Code:	B3ZS	HDB3
Cell Transfer Rate:	96,000 cells per second (PLCP mode) 104268 cells per second (HEC/Direct mode)	80,000 cells per second
Framing:	ANSI T1.107, T1.107a	ITU T G804, G.832
Signal Level:	TA-TSY-000773 (PLCP)	ITU-T G.703
Transmission Convergence Sublayer:	DS3 PLCP frame format DS3 HEC mapped format	G.832 E3 frame format
	T3 (DS3) and E3	
Port Interface, trunk mode, -framing:	Framing for T3, C bit parity per ANSI T1.107/107A	
-port alarm processing	RDI (yellow alarm) and AIS	
Port Interface, port (UNI) mode:		
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF	
Connector:	SMB	

ATM Trunk Interface (BXM-15zM-622 Cards)

Line Rate:	622.08 Mbps	
Line Code:	NRZ	
Signal Level:	Min dBm	Max dBM
SMF IR TX	-15	-8
SMF IR RX	-28	-8
SMF LR TX	-2	+2
SMF LR RX	-28	-8
Framing Format:	STS-12c, STM-4	
Port Interface:	LMI, ILMI	
ATM Cell Rate:	1,412,830 cells per second	
Jitter:	ATM Forum UNI 3.1	
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF, LOP, Path AIS, Path Yellow	
Line Errors Counted:		
Connector:	SMF-FC	
Max. Cable Lengths:	SMF IR ~20 KM	
	SMF LR ~40 KM	
Indicators:	Card status Port status	

ATM T3 Trunk Interface (BNI-T3, LM-3T3)

Line Rate:	44.736 Mbps ± 20 ppm, asynchronous
Line Code:	B3ZS
Signal Level:	DSX-3
Framing Format:	C-bit parity is monitored. No other framing or control bits in the DS3 frame are either altered or monitored.
Protocol:	Physical Layer Convergence Protocol per AT&T Publication TA-TSY-000772 and 000773
ATM Cell Rate:	96,000 cells per second
Alarms Sent:	Remote
Alarms Received:	AIS Loss of Signal Remote Loss of Framing
Line Errors Counted:	BPV Parity Bit Errors
Jitter:	Meets ACCUNET T45 specification (Pub 54014)
Connector:	75 ohm BNC
Recommended Cable Lengths:	450 feet (150 m.) to a DS3 crossconnect
Indicators:	Card status Port status

ATM E3 Trunk Interface (BNI-E3, LM-3E3)

Line Rate:	34.368 Mbps ± 20 ppm, asynchronous
Line Code:	HDB3
Signal Level:	CCITT G.703
Framing Format:	CCITT G.804, G.832
Port Interface:	75 ohm unbalanced
Barrier:	Fully barriered per EN 41003
ATM Cell Rate:	80,000 cells/sec
Jitter:	per CCITT G.823
ATM Layer Protocol:	per CCITT I.361 with HEC
Port Alarm Processing:	AIS Loss of Signal Remote Alarm Indication Loss of Framing
Line Errors Counted:	BPV Parity Bit Errors
Connector:	75 ohm BNC
Max. E3 Cable Lengths:	100 meters. Cabling must not exceed -6 dB/1000 feet at E3 rates. Cisco supplies cable with a maximum attenuation of 7 dB/1000 feet, but the maximum cable length must not exceed 100 meters.
Indicators:	Card status Port status

ATM OC3 Trunk Interface (BNI-OC3, LM-OC3)

Line Rate:	155.52 Mbps	
Line Code:	NRZ	
Signal Level:	Max	Min
MMF TX	–8 dBm	–15 dBm
MMF RX	–8 dBm	–28 dBm
SMF LR TX	0 dBm	–5 dBM
SMF LR RX	–10 dBm	–34 dBm
Framing Format:	STS-3c, STM1	
Port Interface:	LMI, ILMI	
ATM Cell Rate:	353,208 cells/sec.	
Jitter:	< 0.1 UI p-p, < 0.01 UI rms	
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF, LOP, Path AIS, Path Yellow	
Line Errors Counted:	Section BIP8, Line BIP24, Line FEBE, Path BIP8, Path FEBE	
Connector:	MMF SC SMF FC/PC	
Max. Cable Lengths:	MMF ~2 KM KM SMF IR ~20 KM SMF LR ~40 KM	
Indicators:	Card status Port status	

ATM Service Interface (BXM-T3/E3 Cards)

Capacity:	8 or 12 ports per card
Interface:	DS3/T3/E3
Line Rate:	DS3 44.736 Mbs, E3 34.368 Mbps
No. of channels per card:	16,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (BXM-155 Cards)

Capacity:	4 or 8 ports per card
Interface:	OC-3c/STM-1
Line Rate:	155.52.08 Mbps
No. of channels per card:	16,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (BXM-622 Cards)

Capacity:	2 ports per card
Interface:	OC-12c/STM-4
Line Rate:	622.08 Mbps
No. of channels per card:	16,000/32,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (ASI-1, LM-2T3)

Capacity:	2 ports per card
Interface:	T3
Line Rate:	96,000 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	32, 16 per line (port) includes CBR, VBR, and ABR queues

ATM Service Interface (ASI-1, LM-2E3)

Capacity:	2 ports per card
Interface:	E3
Line Rate:	80,000 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	32, 16 per line (port) includes CBR, VBR, and ABR queues

ATM Service Interface (ASI-2, LM-OC3)

Capacity:	2 ports per card
Interface:	OC3
Line Rate:	353,208 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	

PART 6

BPX Specifications

CHAPTER 31

BPX Switch Cabling Summary

This chapter specifies the cabling required to install the BPX switch:

- Trunk Cabling
- Power Cabling
- LM-BCC Cabling
- External Alarm Cabling
- Standard BPX Switch Cables
- Redundancy "Y" Cable

Note In all cable references:
The Transmit direction is **from** the BPX switch.
The Receive direction is **to** the BPX switch.

Trunk Cabling

Trunk cables connect the customer DSX-3 crossconnect point or T3-E3 Interface Module to the BPX switch at the LM-3T3 back card. See Table 31-1.

Table 31-1 Trunk Cables

Cable Parameter	Description
Type:	75-ohm coax cable (RG-59 B/U for short runs, AT&T 734A for longer runs). Two per T3/E3 line (XMT and RCV). For European shipment of the BXM-E3 cards, in order to meet CE mark transient test requirement (IEC1000-4-4), RG-17G double shielded SMB cable must be used.
Max. Length:	450 feet max. between the BPX switch and the DSX-3/E3 point.
Connector:	Terminated in male BNC; Rx is receive from trunk, Tx is transmit to trunk.

Power Cabling

Power connections are made to the AC Power Supply Shelf or the DC Power Entry Module at the rear of the BPX switch. See Table 31-2 and Table 31-3. (next page) for acceptable cable and wire types.

AC Powered Nodes

AC power cables may be provided by you or ordered from Cisco. Several standard cables are available (see Table 31-2). AC cables with other plugs or different lengths may be special ordered.

For those who wish to construct their own power cable, the cable must mate with an IEC320 16/20A male receptacle on the rear of the AC Power Supply Assembly.

Table 31-2 AC Power Cables

Cable Parameter	Description
Cable:	Provided with 8 feet (2.3 m.) of 3-conductor wire with plug.
Plug: customer end	20 A NEMA L620, 3-prong plug (domestic) or 13 A 250 Vac BS1363, 3-prong fused plug (UK, Ireland) CEE 7/7 (Continental Europe) AS3112 (Australia/New Zealand) CEI23-16/VII (Italy)

DC Powered Nodes

DC wiring (Table 31-3) is generally provided by the customer.

Table 31-3 DC Power Wiring

Cable Parameter	Description
Wiring:	Single conductor, 8 AWG recommended wire gauge, 75°C insulation rating, copper conductors only. Provision is provided for attaching conduit.
Connection:	90° ring lug for #10 screw terminal block.

LM-BCC Cabling

LM-BCC cabling connects data ports on the LM-BCC to Cisco WAN Manager network management workstations, control terminals, and modems. It is also used for external clock inputs from a clock source.

See for more details on peripherals that can be attached to these ports.

Auxiliary and Control Port Cabling

The auxiliary and control ports are used to connect one of the nodes in the network to a control terminal, StrataView NMS workstation, or modem connections for remote alarm reporting or system monitoring. Refer to Table 31-4 and Table 31-5 for details on this cable.

Table 31-4 Auxiliary and Control Port Cabling

Cable Parameter	Description
Interface:	RS-232 DCE ports.
Suggested Cable:	24 AWG, 25-wire. A straight-through RS-232 cable is used for a terminal or printer connection. A null modem cable may be needed when interfacing with modems on either port.
Cable Connector:	DB-25, subminiature, male. Table 31-5 contains a list of the port pin assignments.
Max. Cable Length:	50 feet (15 m)

Table 31-5 Auxiliary and Control Port Pin Assignments

Pin#	Name	Source	Description
1	FG	both	Frame Ground
2	TxD	DTE	Transmit Data
3	RxD	DCE	Receive Data
4	RTS	DTE	Request to Send
5	CTS	DCE	Clear to Send
6	DSR	DCE	Data Set Ready
7	SG	both	Signal Ground
8	CD	DCE	Carrier Detect
20	DTR	DTE	Data Term Ready

LAN Port Cabling

The LAN connection is used to connect one of the nodes in the network to a Cisco WAN Manager NMS workstation. See Table 31-6 and Table 31-7.

Table 31-6 LAN Port Cabling

Cable Parameter	Description
Interface:	Ethernet DCE port.
Suggested Cable:	TBS
Cable Connector:	DB-15, subminiature, male. Table 31-7 contains a list of the port pin assignments.
Max. Cable Length:	50 feet (15 m.) max. to interface adapter.

Table 31-7 LAN Port Pin Assignments

Pin #	Name	Pin #	Name
1	Shield	---	---
2	Collision Presence +	9	Collision Presence -
3	XMT +	10	XMT -
4	Reserved	11	Reserved
5	RCV +	12	RCV -
6	Power return	13	Power (+12V)
7	Reserved	14	Reserved
8	Reserved	15	Reserved

Modem Cabling

Refer to *Chapter 15, Connecting Temporary Terminal and Attaching Peripherals*, for modem cabling information.

External Clock Input Cabling

This cabling is for making external clock connections for use by the BCC-32 and BCC-4 backcards.

The BCC-32 uses the BCC-bc backcard.

The discontinued BCC-3 and BCC-4 both use the BCC-3-bc backcard.

T1 Clock Cabling

Table 31-8 through Table 31-11 lists T1 clock cabling details.

Table 31-8 External Clock Cabling

Cable Parameter	Description
Cable Type:	22 AWG, ABAM individually shielded twisted pair. Two pair per T1 line (1 transmit and 1 receive).
Cable Connector:	Male DB-15 subminiature. See Table 31-10 through Table 31-11 for pinouts.
Max. Cable Length:	533 ft (162 m.) maximum between the BPX switch and the first repeater or CSU. Selection of cable length equalizers.

Table 31-9 T1 Connection to XFER TMG on BCC-bc

Pin #	Description
1	Transfer timing ring
2	Transfer timing tip
3 & 4	Transfer timing shield

Table 31-10 T1 Connection to EXT TMG on BCC-bc

Pin #	Description
2	Receive pair shield
3	Receive tip
11	Receive ring

Table 31-11 T1 Connection to EXT 1 or EXT 2 on BCC-3-bc

Pin #	Description	Function
1	Transmit tip	Transmit T1 timing signal synchronized to the node
2	Transmit pair shield	
3	Receive tip	Receive clock for synchronized clock source for node
4	Receive pair shield	
7	Transfer timing tip	
8	Transfer timing shield	
9	Transmit ring	
11	Receive ring	
15	Transfer timing ring	

E1 Clock Cabling

Table 31-12 through Table 31-15 lists E1 clock cabling details.

Table 31-12 E1 Connector Pin Assignments for External Clock

Connector	Description
Cable Type:	75-ohm coax cable for unbalanced connection or 100–120-ohm twisted pair for balanced connection. Two cables/pairs (1 transmit, 1 receive) per E1 line.
Cable Connector:	Two female BNC for unbalanced connection; male DB15 for balanced connection. See Table 31-13 and Table 31-15 for pinouts.
Max. Cable Length:	Approximately 100 meters maximum between the BPX switch and the first repeater or CSU. Equalizer for cable length.

Table 31-13 E1 Connection 75 Ohm to EXT TMG on BCC-bc or BCC-3-bc

Connector	Description
BNC	Receive E1 from trunk

Table 31-14 E1 Connection 100/120 Ohm to EXT TMG on BCC-bc

Pin #	Description
2	Receive pair shield
3	Receive tip
11	Receive ring

Table 31-15 E1 Connection 100/120 Ohm to EXT 1 or EXT 2 on BCC-3-bc

Pin #	Description	Function
1	Transmit tip	Transmit T1 timing signal synchronized to the node
2	Transmit pair shield	
3	Receive tip	Receive clock for synchronized clock source for node
4	Receive pair shield	
7	Transfer timing tip	
8	Transfer timing shield	
9	Transmit ring	
11	Receive ring	
15	Transfer timing ring	

External Alarm Cabling

This cable (Table 31-16) is for connecting network alarm outputs to the LM-ASM ALARM OUTPUT connector only. Table 31-17 lists the pinouts for the network alarm outputs.

Table 31-16 External Alarm Cabling

Cable Parameter	Description
Interface:	Dry-contact relay closure
Wire:	24 AWG, shielded, 6-pair
Connector:	DB-15, Subminiature, male

Table 31-17 Network Alarm Pin Assignments

Pin	Alarm	Description
1	Audible—Major	Normally open
2		Common
9		Normally closed
4	Visual—Major	Normally open
5		Common
12		Normally closed
7	unused	n.c.
8	unused	n.c.
3	Audible—Minor	Normally open
11		Common
10		Normally closed
6	Visual—Minor	Normally open
14		Common
13		Normally closed
15	unused	n.c.

Standard BPX Switch Cables

Table 31-18 lists the various cables that may be ordered directly from Cisco.

Cable lengths are specified as a suffix to the Cisco model number. For example 5610-50 indicates a 50 foot cable. Cables are generally available in standard lengths of:

- 10 ft (3 m)
- 25 ft (7.6 m)
- 50 ft (15 m)
- 75 ft (22.8 m)
- 100 ft (30 m)

Lengths of 101 ft. (30 m.) to 600 ft. (183 m.) are available on a special order.

When a cable is connectorized, the connector gender (male-female) is indicated as well as the number of pins. For example RS-232/M25-M25 indicates a cable terminated with a male DB25 at both ends.

Table 31-18 Standard Cables Available from Cisco

Model#	Description	Usage
T3-E3-10 T3-E3-25 T3-E3-50 T3-E3-75 T3-E3-xx	75 Ω coax/BNC-BNC, 10' 75 Ω coax/BNC-BNC, 25' 75 Ω coax/BNC-BNC, 50' 75 Ω coax/BNC-BNC, 75' length to be specified	T3 or E3 trunk interface
5620	RS-232/M25-F25	Control port to control terminal, StrataView, or ext. window device
5621	RS-232/M25-M25 special	Control or Aux. port to modem
5623	RS-232/M25-M25	Aux. port to ext. window device
5601	Ground cable	DC
5670	Molex-pigtail	DC
5671	Spade lug-pigtail	DC

Redundancy “Y” Cable

The redundancy cables are a special “Y” cable available from Cisco. They are required for redundant trunk and data interfaces.

Table 31-19 lists the Y-cables used with various BPX switch back cards.

Table 31-19 Redundancy Y-Cables

Y - Cable	Used On	Cisco P/N
T3 trunk	LM-3T3	TBS
E3 trunk	LM-3E3	TBS
Aux./Cont. ports	LM-BCC	TBS
Ext. Clk. In	LM-BCC	TBS
Ext. Clk. Out	LM-BCC	TBS

CHAPTER 32

AT3-6ME (T3 to T2) Interface Adapter

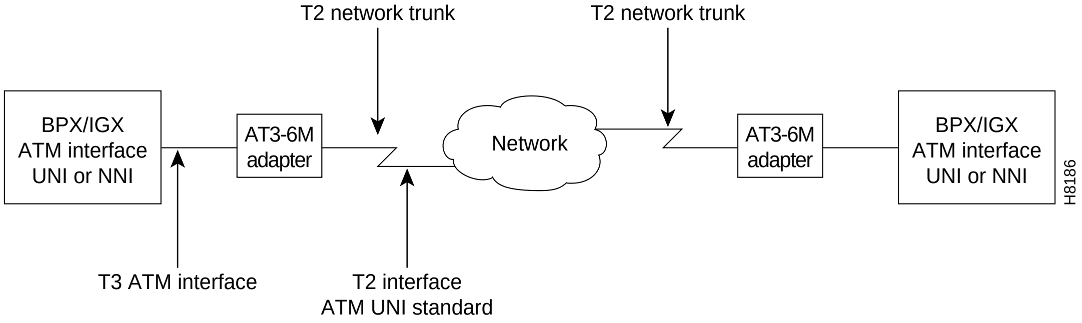
This chapter describes the AT3-6ME Interface Adapter, sometimes referred to as the T3-T2 Interface Adapter. It is used with the BPX switch to provide a 6 Mbps ATM network interface to T2 transmission facilities.

Application

The AT3-6ME Interface Adapter is used with the BPX Broadband ATM Switch in applications where it is required to interface a 6 Mbps T2 digital network facility to the 45 Mbps T3 ATM port on the BPX or IGX node.

Applications include networks where T2 transmission facilities are available. Users with ATM networks who require somewhat more bandwidth than is provided by the T1 or E1 ATM network connections but do not need the full T3 bandwidth provided by the BPX ATM network ports can also benefit from using the AT3-6ME Interface Adapter. See Figure 32-1 for a typical application.

Figure 32-1 Network Application



General Description

The AT3-6ME Interface Adapter is a bi-directional device that provides a conversion between transmission systems of different transmission rates:

- the North American T3 (44.736 Mbps)
- the Japanese 6M (T2).

The AT3-6ME Interface Adapter is used only in ATM networks. The adapter is transparent to both users and the network.

The T3 interface operates at 44.736 Mbps with the B-ISDN Physical Layer Convergence Protocol (PLCP) and meets the ATM Forum standards. The T2 interface operates at 6 Mbps according to the Japanese Nippon Telephone & Telegraph (NTT) User-Network Interface (UNI) specifications.

ATM cells from one interface are mapped to the other interface enabling users with ATM node equipment with North American T3 ATM ports to operate in a T2 network. The ATM cell throughput on a T2 digital trunk using this adapter is limited to 14,490 cells per second.

The cell transfer rate for T2 is greatly reduced from the T3 cell rate from a BPX port. It is very important to restrict the cell rate from the node when using a T2 trunk. Cell rate adaptation is done via software trunk configuration at the T3 ATM interface, where the non null cell throughput is limited to the T2 capacity. In the T2 to the T3 direction, the T3 ATM interface has more than enough capacity to accommodate the T2 cell rate.

The Interface Adapter can buffer a 70-cell burst at the T3 rate before the T2 interface will begin to drop cells. Cells will continue to be dropped until the T3 interface returns to a rate that complies with the bandwidth of the T2 interface.

All alarms and line errors are passed through the Interface Adapter unchanged. Any existing network management system has an instant view of the actual network transmission system. Errors at the ATM layer propagate through from one interface to the other, thus you have complete knowledge and statistical information regarding the network status at all times. Therefore a special network management interface is not required.

Because the T3 interface is asynchronous and the T2 is synchronous, you can configure the AT3-6ME to carry the synchronization information through from one interface to the other. The synchronization is carried through the T3 interface using the PLCP-embedded 8 KHz. The T2 interface clock may be generated locally or it may be slaved to the public network.

Equipment Description

The AT3-6ME is fully contained in a metallic housing designed to be mounted in a 19" equipment rack. It occupies only one rack mounting space and is powered from normal AC line powering. The power supply accommodates an input voltage over the range 90 to 240 VAC, 50 or 60 Hz.

Interface Connectors

The interface connectors are located on the rear panel (see Table 32-1 and Figure 32-2). These connectors include:

- Two T3 BNC connectors, XMT and RCV.
- Two 6M BNC connectors, XMT and RCV.
- A single RS-232 male, subminiature 9-pin control terminal interface.
- AC input connector with integral fuse.

The control terminal is a standard RS-232 interface DTE interface. No hardware handshake is required for the interface. The diagnostic display comes up immediately. It operates at 9.6 Kbps with any ASCII terminal.

Table 32-1 Rear Panel Connectors

Connector	Type	Description
T3 RX	BNC	Receive T3 input from BPX or IGX ATM port.
T3 TX	BNC	Transmit T3 output to BPX or IGX ATM port.
T2 RX	BNC	Receive 6 MB input from T2 facility.
T2 TX	BNC	Transmit 6 MB input to T2 facility.
RS-232	DB9	Control terminal connection.
Primary Power	IEC	AC power input with fuse.

Front Panel Indicators

The front panel of the system provides LED indicators for the alarm status of the transmit and the receive T3 and the T2 interfaces (refer to Table 32-2 and Figure 32-2). Also on the front panel are indications for power and for operating status (Fail/Active).

The Overflow LED indicates that the cell rate coming from the T3 interface exceeds the bandwidth of the T2 facility and that the Interface Adapter buffer has overflowed.

Table 32-2 Front Panel Indicators

Indicator	Color	Description
T3 Receive Status—AIS	Green	Alarm Indication signal detected on the RCV T3 line.
T3 Receive Status—RAI	Yellow	Remote Alarm Indication signal detected on the receive T3 line.
T3 Receive Status—LOS	Red	Loss of receive T3 signal.
T3 Receive—LOF	Red	Loss of frame on receive T3 signal.
T3 Transmit Status—AIS	Green	Alarm Indication signal detected on the transmit T3 line.
T3 Transmit Status—RAI	Yellow	Remote Alarm Indication signal detected on the transmit T3 line.
T3 Transmit Status—LOS	Red	Loss of transmit T3 signal.
T2 Receive Status—AIS	Green	Alarm Indication signal detected on the RCV T2 line.
T2 Receive Status—RAI	Yellow	Remote Alarm Indication signal detected on the receive T2 line.
T2 Receive Status—LOS	Red	Loss of receive T2 signal.
T2 Receive—LOF	Red	Loss of frame on receive T2 signal.
T2 Transmit Status—AIS	Green	Remote Alarm Indication signal detected on the transmit T2 line.
T2 Transmit Status—RAI	Yellow	Loss of transmit T2 signal.
T2 Transmit Status—LOS	Red	Loss of frame on transmit signal.
Overflow	Red	T3 receive cell rate exceeds the T2 line capacity.
FT2	Red	Fractional T2 indication for future use.

Table 32-2 Front Panel Indicators (continued)

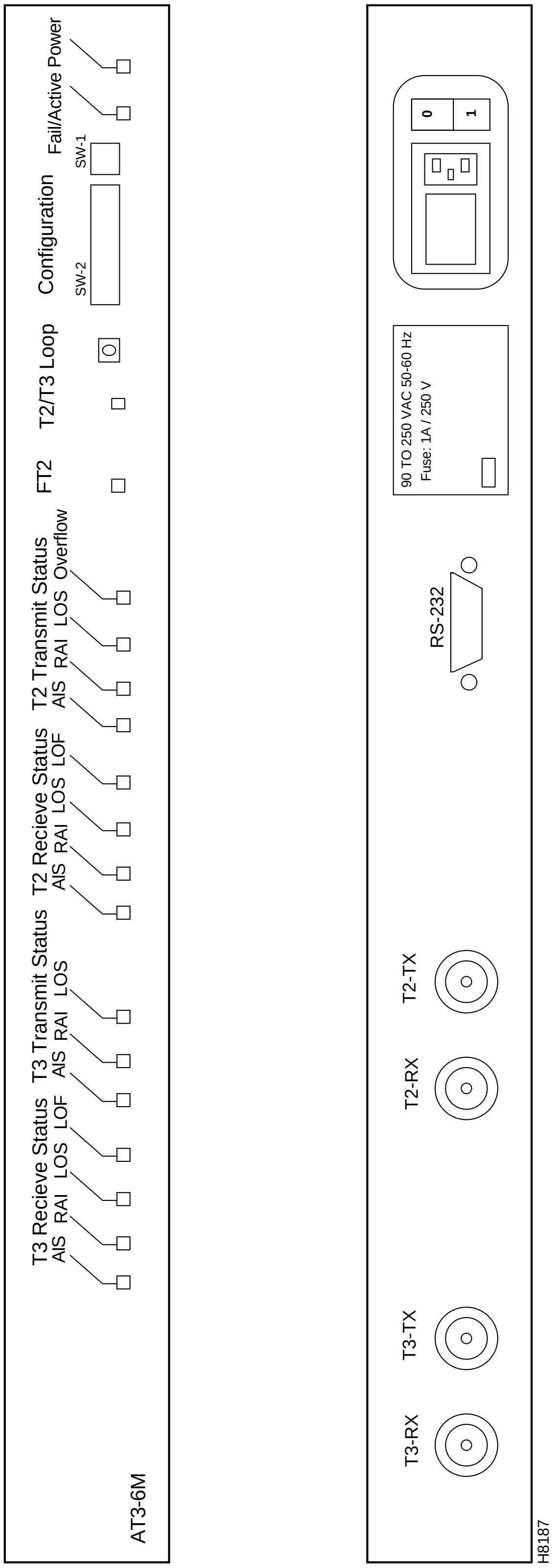
Indicator	Color	Description
T3/T2 loop	Red	Indicates the unit is in loop back mode, external toward the T3 and T2 line interfaces.
Active/Fail	Green/Red	Upon power up the system will go through extensive self tests. If self-test passes, the Active/Fail LED will be green; if self-test fails the LED will be RED.
Power	Green	Power ON indication.

DIP Switches

The adapter has two front panel DIP switches:

- a two-position (SW-1)
  This controls the configurations that may interrupt operation and should be done through a two-step operation.
- a 12-position (SW-2) switch
  This enables all other configuration parameters.

Figure 32-2 Front and Rear Panel Features



Installation

Install the AT3-6ME in a rack adjacent to the BPX enclosure (allowing room for any AC Power Supply Assembly that you might need to mount) wherever there is space for the AT3-6ME adapter.

System Connections

Two short BNC-BNC cables are required to connect the AT3-6ME to the BPX node.

Step 1 For use with BPX switch, connect one cable between one of the three TX connectors on a selected BPX LM-3T3 card and the T3-RX connector on the AT3-6ME back panel.

Step 2 Connect the other cable between the associated RX connector on the BPX LM-3T3 or ATMT card and the T3-TX connector on the AT3-6ME back panel.

Step 3 Connect the cable coming from the 6 Mbps facility to the T2-RX connector on the AT3-6ME.

Step 4 Connect the cable going to the 6 Mbps facility to the T2-TX connector on the AT3-6ME.

Step 5 Connect the AC power cord to the IEC connector on the rear of the AT3-6ME.

AT3-6ME Configuration

You configure the adapter by setting a group of DIP switches located on the front panel. There are two sets of switches:

- a 12-position switch
- a two position switch.
  This switch enables the configuration change via the terminal and enable/disable the loop push button located in the front panel (to secure against accidental operation).

Review both Table 32-3 and Table 32-4. Set the appropriate DIP switches with the power off.

Table 32-3 DIP Switch SW-1 Selection Guide

Switch	Position	Function
1	Down	Enable configuration via the TTY.
1	Up	Disable configuration via the TTY (default).
2	Down	Enable front panel loop push button.
2	Up	Disable front panel loop push button (default).

Table 32-4 DIP Switch SW-2 Selection Guide

Switches	Position	Function
1 2	Up Up	Internal synchronization source for the T2 transmitter
1 2	Up Down	Slave T2 transmitter to T3 line
1 2	Down Down	Slave T2 transmitter to T2 receiver
3 4	Up Up	Long length T3 cable
3 4	Up Down	Medium length T3 cable
3 4	Down Down	Short length T3 cable; system is co located to IGX or BPX[1] (default)
5, 6	don't care	Unused
7	Up	ATM converter mode
7	Down	Test Mode
8	Up	Enable BPV relay from T2 to T3
8	Down	Disable PV relay from T2 to T3
9	Up	Long length T2 cable
9	Down	Short length T2 cable (default)[1]
10, 11, 12	Don't care	Unused

[1] T2 and T3 cable length should be set to "short" upon power-up for self-test.
Upon LOS, defaults to "internal synchronization."

BPX or IGX Port Configuration

You configure the trunk on the BPX or IGX node by using Cisco WAN Manager network management workstation or a local control terminal.

Step 1 Telnet to the first node equipped with an AT3-6ME.

Step 2 Use the Configure Trunk (**cnftrk**) command to select T2 for the Tx Trunk Rate.

Step 3 Set the RCV Trunk Rate to 28980 cps.

Step 4 Repeat steps 1 through 3 for all other nodes using the AT3-6ME.

Operation

This section describes the operating modes for the AT3-6ME. The unit is designed for unattended operation. Any failures in the unit or any line alarms or errors will be propagated.

Power-Up Sequence

During the system power-up, the unit goes through a self test procedure:

- The Power LED turns green.
- The Active/ Fail LED stays off until the self test sequence is completed. Through the self test, all LEDs light up.
- At the end of the self test the loop LED comes on for about 5 seconds.
- When the test is completed successfully the Active/Fail LED turns green.

If the system fails self test, it will repeat the self-test twice more. If it continues to fail, the Active/Fail LED turns red.

Normal Operation

In standard operation, the AT3-6ME system relays ATM cells from the T2 6M to the T3 interface. To accommodate for the difference in the transmission rate, the AT3-6ME removes all null cells from the T3 interface. The T3 sources connected to the AT3-6ME must regulate their ATM Cell rate not to exceed the T2 6M cell rate. The AT3-6ME can absorb up to 70 cells in a single burst.

The AT3-6ME Interface Adapter can interface to any ATM UNI or NNI line at the T2 or T3 rate. The AT3-6ME Relays alarms and errors from one interface to the other. It relays the alarm and error conditions as indicated in Table 32-5.

Table 32-5 Alarm Handling

Alarms Passed Thru (both directions)	Errors Relayed Thru (both directions)
AIS	HEC Error—both directions.
RAI	BPV (up to 10^{-5} rate)—6M to T3 only.
LOS	
LOF	

Remote Loop Operation

The AT3-6ME can create a remote loop on both the T3 and the T2 sides for test purposes. You can manually activate the loop by pressing a front-panel switch or through the control terminal. The loopbacks are through looping relays at the two interfaces and they operate simultaneously.

To activate the loop from the front panel:

Step 1 Enable the proper DIP switch on SW-1.

Step 2 Press and hold the front panel push button for one second. This is to prevent accidental operation of the loop.

Once the loop is set, you can remove it by operating the loop switch a second time. Otherwise it will automatically remove itself after one hour.

Terminal Operation

The system is designed to operate without a terminal. The terminal interface is designed for diagnostics and maintenance purpose only. The terminal interface is always active and continuously displays the user prompt. The terminal interface operating parameters are:

Electrical Interface:	RS232
DTE/DCE:	DCE
Speed:	9.6 Kbps
Handshake:	NON
Connector:	Male DB9

Upon power up:

- The system goes through power up diagnostics:
- The terminal displays the diagnostics sequence.
- Upon successful self test the unit is available for operation.
- The terminal displays the actual set up of the system represented by the DIP switches (see Table 32-6).
- If the configuration was overwritten through the TTY, the terminal will display the actual set up that could be different then the dip switch setting.

Table 32-6 DIP Switch Settings

1	2	3	4	5	6	7	8	9	10	11	12	1	2
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

Commands

You enter commands after the user prompt to:

- Display the various error counters and alarms associated with the T2 line and the T3 port interface
- Select the source of timing for the DSU
- Enable and remove the remote loop

Table 32-7 lists available commands for use with the AT3-6ME terminal interface while Table 32-8 indicates the display format.

Table 32-7 Command Summary

Command	Parameters	Meaning
?		Help Menu.
dspstat		Display status.

Table 32-7 Command Summary (continued)

Command	Parameters	Meaning
dspstat clear		Clears the status display.
Override dipsw	0 1	Disable TTY configuration entry. Enable TTY configuration entry. Operates only when DIP switch 1-1 is down.
Sync source	0 1 2	System is slaved to the 6M line. System is slaved to the T3 line. System runs of its internal clock.
Remote loop	No of seconds stop	Enable remote loop back operation. Cancel the loop back operation.

Table 32-8 Status Display

Status	T3[1]	T2[1]
BPV	NNN	NNN
Parity Errors	NNN	X
Framing Errors	NNN	NNN
PLCP Framing Errors	NNN	X
HEC Errors	NNN	NNN
RX Cells	NNN	NNN
TX Cells	NNN	NNN
AIS	1/0	1/0
1/0	1/0	1/0
LOF	1/0	1/0
Overflow	X	1/0

[1] X = not available

Specifications

These are the specifications for the AT3-6ME Interface Adapter:

Table 32-9 T3 Interface

Line rate:	44.736 Mbps ±20 ppm
Framing format:	C-bit parity
Line code:	B3ZS
Physical layer:	PLCP format
ATM layer:	UNI per the ATM Forum UNI 3.0 specification
Cell Rate:	Up to 96,000 cells/sec.
Connector:	75 ohm BNC

Table 32-10 T2 Interface

Line rate:	6.312 Mbps
Line code:	B8ZS
Synchronization:	Internal 6.312 Mbps ±30 ppm or Slave to the incoming 6 Mbps line or Slave to the T3 PLCP frame
Framing format:	ITU-T G.703
ATM Layer:	Per NTT UNI specification dated 1993
Queue:	75 cell FIFO
Cell Rate:	Up to 14,490 cells/sec.
Connector:	75 ohm BNC

Table 32-11 Power

Input Power:	90 VAC to 250 VAC, 50/60 Hz
Power consumption:	30 watts
Input Power Connector:	Universal power entry module with fuse
Fuse size:	1/2A 250 VAC

Table 32-12 Mechanical

Rack Mounting Space:	1 rack mount space, 19" rack
Size:	19" x 1.75" x 8.5"

Table 32-13 Terminal Interface

Speed:	9.6 Kbps
Type:	DTE
Handshake:	NONE
Connector:	DB9

PART 7

Appendices

Upgrade Information

This appendix provides special upgrade information.

Upgrade BXM to BXM-E Cards

You can now gracefully upgrade your Broadband Switch Module (BXM) card to a BXM-E card without any service interruption (on Y-red BXMs).

The enhanced BXM-E card (version DX or EX) supports a higher connection density (32K) than either the legacy BXM or regular BXM-E cards. Both DX and EX versions have the same connection density, providing the ability to upgrade networks with the high connection density BXM-Es on trunk side, port side, or a combination of trunks and ports.

Prior to this feature, upgrading a functioning legacy BXM or regular BXM-E card (configured in low-connection-density mode), to the DX or EX version of BXM-E (configured in higher connection density mode) required deleting all existing connections terminating on the active BXM card and reestablishing the connections on the new card.

After the BXM-E card replaces the BXM card, the switch software programs all channels on the new active card or on the hot standby card. The performance effect due to programming the channels is minimal since the process is done only once for each BXM card. If the cards are Y-red, Automatic Routing Management traffic still can be transported through the active card while the standby BXM-E is programmed.

This section contains both automatic and automatic and manual upgrade scenarios. The benefit of manually upgrading is that the logical database is not automatically upgraded, thus permitting you to fall back from BXM-E to BXM without mismatch. The concept of mismatch is introduced when BXM cards are configured as Y-redundancy or 1+1 APS. BXM cards with different connection densities are not declared as mismatch, so long as the physical density of the latest inserted card is greater or equal to the density of the other card in the Y-redundancy pair.

If VSI was configured on the legacy card, the VSI partition is expanded to allow the extra LCNs. The additional LCNs are allocated to the first port of the first enabled VSI. This provides a convenient way to fall back to a former VSI configuration.

Summary of Commands

A full description of these commands is located in the *WAN Switching SuperUser Command Reference*.

Figure A-1 BXM-BXM-E Upgrade Commands

Command	Description	Default	Consult
cnfnodeparm	Configure node parameters, auto BXM upgrade parameter. If set to “Y,” the Switch software upgrades the logical database as soon as both the legacy BXMs are replaced by BXM-Es in Y-red case, or the active legacy BXM is replaced by a BXM-E in non-Y-red cases. If set to “N,” you must upgrade the logical database manually using the **upgdlogcd** command.	Y	*WAN Switching SuperUser Command Reference*
cnfcdparm	Configure card parameters. This command is used to set the standby card to the appropriate channel statistics level and number of connections.	N/A	*WAN Switching SuperUser Command Reference*
upgdlogcd	Upgrade logical card database. The **upgdlogcd** <log_card_num> is used to manually upgrade the logical card database. When using the **upgdlogcd** command, the **cnfnodeparm** “auto BXM upgrade” parameter must be set to “N.” When performing the upgrade, switch back to the legacy card *before* the **upgdlogcd** command is initiated.	N	*WAN Switching SuperUser Command Reference*

Upgrade Options

Use one of the following upgrade options described in Figure A-2.

Figure A-2 Upgrade Options

Option	Used when...	Steps
Y-Red BXMs, manual	Legacy BXMs are Y-red and the “auto BXM upgrade parameter” is set to “N” for the **cnfnodeparm** command.	1. Remove the standby BXM card and replace it with the BXM-E card. 2. BXM-E card scan be flagged as “Mismatch” if the configured channel statistics level or number of connections is smaller than those configured on the active BXM card. Use the command **cnfcdparm** <BXM-E slot_num> to configure the desired level of channel statistics and number of connections, if not already configured. The BXM-E card is reset after the **cnfcdparm** command is executed. After the BXM-E card boots, there should be no mismatch. 3. Y-red the switch so that the standby BXM-E becomes active. 4. Repeat steps 1-2 for the other slot. **You still can fall back to the legacy card up to this point.** 5. Upgrade the logical card using the command **upgdlogcd** <log_card_num>. Switch software upgrades the logical database from the number of connections configured on the legacy BXM card to the number of connections configured in step 2 and 4. From this point on, mismatch is declared if the legacy card is reinserted. **Note** During upgrading Y-red BXM cards to BXM-E cards, the level of service disruption is expected to be the same as the one experienced when **switchyred** is executed for Y-red legacy BXMs.
Y-red BXMs, automatic	Legacy BXMs are Y-red and the “auto BXM upgrade” parameter is set to Y for the **cnfnodeparm** command.	1. Remove the standby BXM card and replace it with the BXM-E card. 2. BXM-E card can be flagged as ‘Mismatch’ if the configured channel statistics level or number of connections is smaller than those configured on the active BXM card. Use the command **cnfcdparm** <BXM-E slot_num> to configure the desired level of channel statistics and number of connections, if not already configured. The BXM-E card is reset after the **cnfcdparm** command is executed. After the BXM-E card boots, there should be no mismatch. 3. Y-red the switch so that the standby BXM-E becomes active. 4. Repeat steps 1-2 for the other slot. 5. Switch software automatically upgrades the logical database when step 4 is done. **Note** During upgrading Y-red BXM cards to BXM-E cards, the level of service disruption is expected to be the same as the one experienced when **switchyred** is executed for Y-red legacy BXMs.

Figure A-2 Upgrade Options (continued)

Option	Used when...	Steps
Standalone BXM, manual	Legacy BXM card is non-Y-red and the “auto BXM upgrade” parameter is set to “N” for the **cnfnodeparm** command.	1. Use an empty slot to configure the BXM-E card for the desired level of channel statistics and number of connections. The channel statistics level and number of connections must be either equal to or higher than the ones configured on the legacy BXM card that it is replacing. While this step is optional, if skipped, the BXM-E card may not have the desired channel statistics level and appropriate number of connections. 2. Remove the BXM card and replace it with the BXM-E card. If step 1 is skipped, the BXM-E card can create a mismatch if it does not have the desired configuration. In that case, use the command **cnfcdparm** <BXM-E slot_num> to set the card to the desired level of channel statistics and number of connections. This may prolong service disruption. 3. Issue the **upgdlogcd** <log_card_num> command to upgrade the logical card database. Switch software upgrades the logical database from the number of connections configured on the legacy BXM card to the number of connections configured in step 1. From this point on, mismatch is declared if the legacy card is reinserted. **Note** In non-Y-red cases, the traffic disruption is unavoidable because the legacy BXM has to be removed and replaced with the BXM-E card.
Standalone BXM, automatic	Legacy BXM card is non-Y-red and the “auto BXM upgrade” parameter is set to ‘Y’ for the **cnfnodeparm** command.	1. Use an empty slot to configure the BXM-E card for the desired level of channel statistics and number of connections. The channel statistics level and number of connections must be either equal to or higher than the ones configured on the legacy BXM card that it is replacing. While this step is optional, if skipped, the BXM-E card may not have the desired channel statistics level and appropriate number of connections. 2. Remove the BXM card and replace it with the BXM-E card. If step 1 is skipped, the BXM-E card can create a mismatch if it does not have the desired configuration. In that case, use the command **cnfcdparm** <BXM-E slot_num> to set the card to the desired level of channel statistics and number of connections. This may prolong service disruption. 3. Switch software automatically upgrades the logical database when step 2 is done. **Note** In non-Y-red cases, the traffic disruption is unavoidable because the legacy BXM has to be removed and replaced with the BXM-E card.

Upgrade Protection from Release 9.3 to a Later Release

Release 9.3 includes an Upgrade Protection feature. This section provides guidelines on upgrades from BPX switch software Release 9.3 to later releases.

Active statistics collection interferes with the software upgrade process. Prior to Release 9.3, you were responsible for turning statistics off before beginning the software upgrade procedure.

The Upgrade Protection feature introduced in 9.3 protects you against the effects of failing to turn off statistics. In 9.3, statistics collection is automatically turned off by the system when you enter the loadrev 1 phase. You are now prevented from running loadrev/runrev during the time that statistics collection is enabled. When you execute loadrev, the switch gives this message “Warning: Statistics collection will be automatically disabled.”

In addition to statistics collected by Cisco WAN Manager, the local statistics collection state machines are also disabled at this time.

Upgrade Protection applies only to a “graceful upgrade,” that is, an upgrade to a standby controller card. There is no change to the “non-graceful upgrade” procedure.

This feature is operational only when upgrading from Release 9.3 to a later release. Upgrade from Release 9.2 to 9.3 does not use this 9.3 feature. Upgrade Protection is used in intraversion upgrades, such as an upgrade between 9.3.1 and 9.3.2

If you attempt to load an older release than the one currently running, you will be warned that downgrades are not supported. You may override this warning and continue at your own risk. This feature is meant to warn you early in case an invalid release is inadvertently loaded.

If you need to see certain statistics at this phase of the upgrade, you are allowed to restart state machines one at a time. However, it is your responsibility to disable all these machines before entering the runrev phase.

Procedure

The process of upgrading a network from one release of switch software to another involves several phases:

Step 1 Load the new software image into the switches of the network by using **loadrev 1**

Step 2 Upgrade the new image in standby controller cards (assuming graceful software upgrade) by using **upgrade**. If you need to see certain statistics at this phase of the upgrade, you are allowed to restart state machines one at a time. However, it is your responsibility to disable all these machines before entering the runrev phase.

Step 3 Run the new software revision, retaining the old revision and configuration for fallback protection, by using **runrev.**

Step 4 Load the new revision into all controller cards in each node, purging all traces of the old revision, and completing the upgrade. Use **loadrev 2.**

When you complete the upgrade by entering the loadrev 2 phase, the Upgrade Protection feature re-enables all the statistics state machines that were active when upgrades were started. If CWM statistics are desired, you must use CWM to restart collection.

Feature Mismatching

Feature mismatching provides customers a graceful migration path to Release 9.2 features.

Switch Software Release 9.1 and previous releases of switch software mismatched cards if the capabilities in the logical card database did not match exactly the capabilities of the physical card. This restriction does not allow customers to gracefully migrate their BXM/UXM cards.

The current 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.

BPX switch software features perform these feature mismatching functions:

- Command Line Block
  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.

Feature mismatch is supported by these BPX switch software features:

- 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

Refer to the 9.2 Release Notes for up-to-date information on feature support, and software, hardware, and firmware requirements.

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

Switch software provides an upgrade path for each of the Release 9.2 features. Table A-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. It also describes the process of upgrading firmware in a scenario where a single active card and Y-cable is in use.

Table A-1 Upgrading Firmware When Single Active Card and Y-Cable is 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
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.

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 to 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 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 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.

Table A-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
Active Y-cable configuration with the Secondary Card supporting fewer channels than defined in the logical card (primary card) database.	Secondary card mismatch
Active Y-cable configuration with the primary card supporting fewer channels than the logical card database.	Primary card mismatch
Active Y-cable configuration with the primary or secondary cards (or both) supporting more channels then the logical card database: neither card will mismatch although the additional channels are NOT available to the user.	No
Standby Y-cable configuration with the primary or secondary cards supporting different number of channels.	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, this 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 to ensure that both the primary and secondary cards support the activated features. 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.

Considerations for Feature Mismatch Checking

Following are some things to be aware of related to feature mismatch:

- Consider a situation where a user replaces 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.

GLOSSARY

A

A-bit (active bit) The bit in the frame relay frame header that indicates the status of the far end user device and the status of the PVC segment in the foreign network.

A-law An analog to digital encoding scheme used to convert voice samples to an 8-bit data word used in CEPT E1 multiplex equipment. (See also µ-law.)

ABR (Available Bit Rate) ATM connection type for bursty traffic, such as data. Provides closed loop control of service rate that allows connections to use additional bandwidth when available. ABR may be used with ATM Traffic Management 4.0 standards VSVD flow congestion control, or with the proprietary ForeSight flow congestion control. (See also CBR and VBR.)

ACO (Alarm Cut Off) A switch to turn off the audible alarm outputs from a node while leaving the visual alarm outputs unchanged.

adaptive voice An optional feature that disables VAD from connections using it whenever there is excess bandwidth available to allow the normal encoded voice to be carried on the packet line. (See also VAD.)

ADPCM (Adaptive Differential Pulse Code Modulation) A compression method that samples voice 8,000 times per second, and uses the changes between samples as the basis for compression. Increases the capacity of a T1 line from 24 to 48 channels.

ADTF (Allowed Cell Rate Decrease Factor) Time permitted between sending RM cells before the rate is decreased to ICR.

AIT-E3 (ATM Interworking Trunk E3 Interface Card) The AIT-E3 backcard provides an E3 interface for the BTM (IGX switch) ATM trunk cards.

AIT-T3 (ATM Interworking Trunk T3 Interface Card) The AIT-T3 backcard provides a T3 interface for the BTM (IGX switch) ATM.

alternate routing An automatic rerouting of a failed connection by a node to a new route through the network to maintain service.

AMI (Alternate Mark Inversion) The line code used for T1 and E1 lines where the “1s” or “marks” on the line alternate between positive polarity and negative polarity.

arbiter A BPX administration processor that polls each network port to control the data flow in and out of the crosspoint switch matrix.

ARI (Alarm Relay Interface Card) An alarm interface back card for the IGX switches.

A

ARM (Alarm Relay Module) An alarm front card for the IGX switch.

ASM (Alarm/Status Monitor Cards) An alarm front card and back card set for the BPX switch.

ATM (Asynchronous Transfer Mode) Data transmission that uses a very flexible method of carrying information, including voice, data, multimedia, and video between devices on a local or wide area network using 53-byte cells on virtual circuits. The 53 byte cell consists of data and a small header. (See also cell relay.)

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 intefaces. The router forwards the cells from these interfaces using labels carried in the VPI and/or VCI field.

ATM Switched Virtual Circuits (SVCs) A member of the INS product family that uses ATM SVC Server Shelves and software to enhance a Cisco WAN switching network with ATM switched virtual circuits.

ATM SVC Server Shelf An adjunct processor used in the INS ATM SVC application to enhance traditional Cisco WAN switching networks with ATM switched virtual circuits. The ATM SVC Server Shelf is co-located with and connected to a BPX switch.

auxiliary port An RS-232 port on the front panel of the SCC card used for connecting a printer or an out-dial modem. This port is a one-way, outgoing port.

B

B3ZS (Bipolar with Three Zero Suppression) A protocol for T3 lines that converts a channel word with three consecutive zeros into a code which at the far end is converted back to three zeros.

B8ZS (Bipolar with Eight Zero Suppression) A T1 line protocol that converts a channel word with eight consecutive zeros into a code which, at the far end, is converted back to eight zeros. Allows 64 Kbps clear channel operation while assuring the ones density required on the T1 line.

bandwidth reservation A software feature that allows circuits to automatically become active (or "upped") at a specified time and date and downed at some later time and date. For circuits that do not need to be available 100% of the time.

B channel In ISDN, a full-duplex, 64-kbps channel used to send user data. Also known as the bearer channel. Compare with D channel.

BCC The switch control card in the BPX is the Broadband Control Card, with a 68040 processor.

BC-E1 (Backcard E1) E1 interface card used on IGX switches.

B

BC-E3 (Backcard E3) E3 interface card used on IGX switches.

BC-J1 (Backcard J1) J1 interface card used on IGX switches.

BC-SR (Backcard Subrate) Subrate interface card used on IGX switches.

BC-T1 (Backcard T1) T1 interface card used on IGX switches.

BC-T3 (Backcard T3) T3 interface card used on IGX switches.

BC-Y1 (Backcard Y1) Y1 interface card used on IGX switches.

BDA (Bframe Destination Address) The address of the slot.port.channel for which the Bframe is destined. This address is part of the Bframe header and is only used across the switch fabric locally in the node.

Bframe The BPX frame is the 64-byte format for messages used to encapsulate ATM cells which are sent across the switch fabric.

bipolar violations Presence or absence of extra “1” bits on a T1 transmission facility caused by interference or a failing line repeater. These extra or missing bits interrupts one of the rules for bipolar pairs of a digital transmission line.

BISDN (broadband ISDN) ITU-T communication standards designed to handle high-bandwidth applications. Compare with ISDN.

BNI (BPX Network Interface Card) The front card used to network BPX switches together and to connect to AXIS and IGX nodes configured as shelves. Supports T-3, E-3, and OC3 trunks carrying ATM cells.

BPX Switch The Cisco Broadband Packet Exchange (BPX): A high-speed broadband, high-capacity ATM cell relay network switch from for private and public networks, 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).

BRI (Basic Rate Interface) ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data. Compare with PRI.

bundled connections Frame relay connections grouping a number of ports into one permanent virtual circuit.

BTM (Broadband Trunk Module) The BTM provides an ATM trunk interface for the IGX switch. The BTM operates in conjunction with a backcard, AIT-T3, or AIT-E3.

B

BXM

The Broadband Switch Module (BXM) cards are a series ATM port cards for the BPX switch: BXM-T3/E3, BXM-155, or BXM-622. These can be configured for either trunk or line (service access) modes. These cards and support ATM Traffic Management 4.0, including VSVD congestion flow control. Various 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 chipset's architecture supports up to 64K bi-directional cross-connect legs per BXM card. The BXM has very flexible input and output queueing facilities, a SAR (Segmentation Assembly and Reassembly) capability, and a MIPS 4650 control processor.

C

CAS (Channel Associated Signalling)

A signalling mode in E1 transmission where the signalling bits for all 30 E1 channels are carried in timeslot 16. Timeslots 1 to 15 and 17 to 31 carry encoded voice bits only.

CBR (Constant Bit Rate)

ATM Connection type for constant bit rate traffic such as voice or synchronized data requiring a low variation in delay. (See also, VBR and ABR.)

CCDV (Compliant Cell Delay Variation)

A parameter utilized in defining ATM Constant Bit Rate service. The amount of delay that is acceptable between ATM cells for them to be accepted as compliant (usable).

CCITT (Consultive Committee for International Telephone and Telegraph)

An international telecommunications advisory committee established under the United Nations to recommend worldwide standards for data and voice communications.

CCS (Common Channel Signalling)

A carrier signalling mode in E1 transmission where signalling bits are not used. CCS typically separates user data from signalling information. A signalling channel is used to provide signalling for all other user data channels in the system.

CDVT (Cell Delay Variation Tolerance)

Controls time scale over which the PCR is policed.

Cell

A unit of data with a fixed number of bytes. For ATM the cell size is 53 bytes.

cell relay

A form of digital communications using fixed length cells consisting of data and a small header. IPX FastPacket was an early implementation of cell relay. The 53 byte ATM cell consists of data and a small header.

CEPT

CEPT is the European Conference of Posts and Telecommunications Administrations. This association is comprised of European Telecommunications service providers that participate in relevant areas of the work of CEN/CENELEC.

CGA (Carrier Group Alarm)

A major alarm condition for a T1 multiplexer or PABX that results in all channels being taken out of service.

channel

The logical end point for a connection.

C

circuit line A T1 or E1 line that connects a user device, such as a PABX or channel bank to a switch. Carries customer DS0 voice and data circuits. (See also line.)

Cisco StrataView Plus A Unix-based workstation and software used as a network management system (NMS) for Cisco WAN switching networks. It is part of the StrataSphere group. Provides a graphical user interface for configuration, maintenance, administration of the network. Collects and displays network statistics.

clear channel capability When all eight bits of a channel word in the T1 line signal are available for transmitting customer data with no restrictions on content. Also referred to as 64 Kbps clear channel.

Cmax A frame relay connection parameter that specifies the number of packets allowed in the initial burst of data after which the data bandwidth is reduced to the connection's minimum specified bandwidth.

CLLM Consolidated Link Layer Management. A protocol used to transmit ForeSight messages across the frame relay NNI port.

CLP (Cell loss priority) Cell loss Priority. CLP Hi and CLP Lo thresholds are configurable.

Complex Gateway Refers to interworking of a connection with respect to the IGX nodes. For example, in a Frame Relay to ATM interworking, the Frame Relay data is extracted from FastPackets and transformed to ATM cells with redundant overhead bits discarded.

composite data rate The sum of the data rates for all circuits transmitting on the same synchronous or frame relay data card.

control port An RS-232 port on the face plate of a back card for a controller card (BCC, NPC, NPM.) that may used for connecting a control terminal. This port is bi-directional.

COS (Class of Service) The priority assigned each user connection. Defines which circuits get rerouted first during a network failure.

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.
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 Service Expansion Shelf (SES) is based on CommBus messaging accessed through interfaces to the BPX cards.

CoSB See Class of Service (CoS) Buffer.

C

courtesy downing A software feature that is used to conserve network bandwidth by automatically “downing” a voice connection when the signalling status indicates an inactive (on-hook) circuit. The circuit is automatically “upped” when the circuit becomes active.

CRC (Cyclical Redundancy Check) A method of error checking that detects errors in a block of data. Unlike parity checks, the CRC can detect multiple data errors within the block and thus equipment using a CRC error check can derive a error rate.

crosspoint switch A two-dimensional data switch type that is arranged in a matrix of all input connections along one axis and all output connections along the other axis. Each input and output line has a switch point where the two axis intersect that can be enabled (switch closed) or disabled (switch open). The central matrix switch providing the switching matrix for traffic routing by the BPX switch.

CSU (Channel Service Unit) A network protection unit that terminates any T1 span line connected to the carrier's central office, providing receive direction regeneration and maintenance loopback for the 1.544 Mbps signal.

D

D4-format A digital signal format with 24 eight-bit channels plus one synchronizing bit per T1 line. Channels are assigned in a straight, numeric sequence.

DACS (Digital Access and Control System) Equipment, usually found in the telephone company central office, that is used to groom and retime the 24 channels in a DS1 signal. Individual DS0 channels can be cross-connected from one DS1 source and inserted in another DS1 source either with the same or with a different channel number.

DAS Server Shelf The adjunct processor used in INS Dial-Up Frame Relay applications to provide frame relay dial-up and dial-backup circuits. The DAS Server Shelf is co-located with and connected to an IGX switch.

DCE (Data Communications Equipment) As defined by the RS-232 standard, any device that transmits or receives information. Usually used with data terminal equipment (DTE, like a computer or network node).

D channel A message-oriented ISDN signalling channel, typically carried in DS24 of a PRI on T1 facilities or TS16 of a PRI on E1 facilities. Compare to B channel.

DDS (Digital Data Service) An AT&T dial-up data service offering for 2.4 to 56 Kbps over subscriber loop cable. Requires a Data Service Unit, DSU, at customer premise for interface to the DDS trunk.

Device Code The first 8 bits of a FastPacket Address.

DFM (Data Frame Multiplexing) An optional feature that saves data channel bandwidth by analyzing data channel content and suppressing repetitive data patterns.

Dial Access Switching Another name for the INS Dial-Up Frame Relay application.

Dial-Up Frame Relay An INS application that uses a DAS Server Shelf and software to enhance Cisco WAN switching networks with frame relay soft permanent virtual circuits (SPVCs) for dial-up dial-backup connections.

D

DLCI (Data Link Connection Identifier) A field in a frame relay data packet that identifies the destination for the data.

domain A grouping of nodes sharing common interests or attributes.

domain name A unique name consisting of the letter "D" immediately followed by a number (1–8) delineated by a "." (period) from the node name (1–8 characters maximum). Example: D1.alpha.

domain number A number from 1–8 assigned with the **cnfdmn** command. The number assigned is part of the domain name.

DPNSS Digital Private Network Signalling System. A common-channel message-oriented signalling protocol commonly used by private branch exchanges (PBXes). The INS Voice Network Switching application supports DPNSS signalling.

DS0 (Digital Signal 0) A 64 Kbps channel used to transmit encoded voice and/or data. There are 24 DS0 channels in a circuit T1 (DS1) line. DS0 data is transmitted using one or more DS0 circuits in a T1 or E1 circuit line.

DS0A An extension of DS0 that defines the format for assembling various low-speed data circuits (1.2 to 19.6 Kbps) into a single 64 Kbps DS0 channel.

DS1 (Digital Signal 1) A digital transmission standard that carries 24 individual channels in a bipolar, high-speed line signal at 1.544 Mbps. DS1 signal level is ±3V.

DSI (Digital Speech Interpolation) An algorithm that analyzes DS0 voice bits for non-speech codes. Suppresses these bits to conserve packet line bandwidth and inserts a code to indicate to the far end that these bits have been removed. Similar to DFM for data channels. Also, referred to as VAD (Voice Activity Detection).

DTE (Data Terminal Equipment) As defined by the RS-232 standard, any device that generates or utilizes information. (See also, DCE.)

E

E1 European transmission service at the rate of 2.048 Mbps.

E3 Transmission service at a rate of 34.368 Mbps.

ECN (Explicit Congestion Notification) A frame relay feature to signal the onset of network congestion to external devices. Sets FECN and BECN bits in frame relay header to indicate forward and backward congestion.

SES The Service Expansion Shelf is the controller on which the BPX's PNNI implementation runs. It is SPARC-based.

F

Fast EIA Same as interleaved EIA. Seven data circuit control leads in each direction are transmitted in alternating bytes with data. For fast control lead response to data being turned on and off but with a sacrifice in packet line bandwidth

FBTC (Frame Based Traffic Control) An AAL5 frame based traffic control that provides the possibility of discarding the whole frame, not just one compliant cell. This avoids wasting bandwidth by continuing to send the cells in a frame once a cell has been found to be non-compliant.

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.

FGCRA (Frame Based Generic Cell Rate Algorithm) An enhancement option to GCRA that allows an entire frame to be discarded if any of its cells are non-compliant, rather than transmitting a partial frame over the network.

flat network A non-structured network, a network in which there are no junction nodes or domains.

foreign network An adjacent network that is owned and managed by a different party than the one that owns the local network.

ForeSight A proprietary optional feature that uses feedback techniques to dynamically allocate extra bandwidth to frame relay and ATM connections when the network bandwidth is available and not used by other connections. (See also VSVD.)

frame forwarding A software feature allowing point-to-point frame relay type connection for various data applications that do not conform to the Frame Relay Interface Specification.

frame relay connection class A tag for a frame relay circuit which indicates the class of service to be provided for this connection. Parameters associated with a connection class include minimum information rate guaranteed, peak information rate expected, maximum network delay, and so on.

FRI (Frame Relay Interface Card) The backcard for an FRM (IGX switch) card. The FRI provides V.35, X.21, T1, or E1 interfaces.

FRM (Frame Relay Module) An IGX frame relay front card that supports 1-4 data ports, and in single-port mode, operates up to 2.048 Mbps. The card is used in conjunction with FRI-V.35, X.21, T1, or E1 backcards.

FRM-2 (Frame Relay Module) An IGX frame relay front card that provides an interface to the frame relay Port Concentrator Shelf (PCS). The card is used with the FRI-2-X.21 backcard which connects to the PCS.

Frame Relay Service A packet interface data transmission protocol used for connecting widely-separated LANs. Characterized by long intervals of no data to be sent interspersed with bursts of large volumes of data; sometimes referred to as “bursty data”.

FRTT (Fixed Round Trip Time) The sum of the fixed and propagation delays from the source to a destination and back.

Full Status Report A message sent across the NNI indicating the A-bit status of all connections routed across this NNI frame relay port.

G

gateway A node configured to handle both T1 and E1 packet and circuit lines for direct interface international circuits.

GCRA (Generic Cell Rate Algorithm) GCRA is a “continuous leaky-bucket” process that monitors the cell depth in the input queue for each PVC to determine whether to admit a new cell to the network without setting the Cell Loss Priority bit.

global addressing A frame relay addressing convention that uses the DLCI to identify a specific end device somewhere else in the frame relay network. In a global addressing scheme, the DLCI is a unique number for each port in the network.

grouped connections Frame relay connections grouping a number of ports onto one permanent virtual circuit. Similar to bundled connections except the grouped connections do not have to be contiguous, nor do they all have to be added simultaneously.

H

HDB3 (High Density Bipolar Three) A line interface for E1, similar to B8ZS for T1, which eliminates patterns with eight or more consecutive zeros. Allows for 64 Kbps clear channel operation and still assure the ones density required on the E1 line.

HDP (High Speed Data PAD) An IGX front card that supports one to four medium speed, synchronous data channels.

I

IGX Switch A multi-service, multi-band ATM cell relay network switch for private and public networks.

Intelligent Network Server (INS) INS is the broad name for a range of products that enhance traditional Cisco WAN switching networks. These products include Dial-Up Frame Relay, Voice Network Switching, and ATM Switched Virtual Circuits.

interleaved EIA Same as “Fast EIA”.

ISDN (Integrated Services Digital Network) A service provided by the telephone company or OCC that supports combined customer voice and data connections over the twisted pair subscriber loop. Requires special equipment at the customer premise and a connecting central office switch that is capable of providing ISDN.

IPX Switch A narrowband cell relay network switch from for private and public networks.

J

J1 A. multiplexed 24-channel circuit line to a PBX conforming to the Japanese TTC-JJ-20 circuit standard. Similar to E1, it operates at 2.048 Mbps.

J

junction node A node handling inter-networking of domains.

junction trunk A packet line connecting junction nodes.

L

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.

LCON The logical connection used to represent an individual routing entity.

LDM (Low Speed Data Module) An IGX data front card that supports up to 8 synchronous or asynchronous data ports. When used with an LDI4/DDS, an LDP can provide 56-Kbps Digital Data Service (DDS) interfaces to the IGX switch.

line Connects a user device to a service interface, for example, a router to an AUSM card, a data line to a data card, a frame relay line to an FRP or a port concentrator, or a T1 or E1 line to a CDP card.

link The network connection between two nodes.

LMI (Local Management Interface) The protocol and procedures for control of frame relay connections. Used for configuration, flow control, and maintenance of these connections.

local addressing A frame relay addressing convention that uses the DLCI to identify the frame relay port at the interface between the user device and the frame relay network. In local addressing, a particular DLCI is used only at the local FR connection. The DLCI may be reused at any other node in the network.

local alarm An alarm indicating that the associated T1 line is down due to a local failure of its receive path.

local bus An utility bus (LB/0 or LB/1) located on the midplane, which provides the electrical connections between various front and back cards. For example, the front and back cards of the Low Speed Data PAD group (LDP and LDI) plug into this utility bus.

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.

logical port A frame relay circuit consisting of either 1, 6, 24 (T1,) or 31 (E1) contiguous DSO's on a T1 or E1 physical port.

LSR Label Switching router, which is an MPLS (Multiprotocol Label Switching) router.

M

major alarm A local or remote failure that is affecting operation of the network.

MBS (Maximum Burst Size) Maximum number of cells which may burst at the PCR but still be compliant.

MCR (Minimum Cell Rate) The minimum cell rate that is supported by an ATM connection for an ABR connection.

MIR (Minimum Information Rate) The minimum information rate that is supported by a frame relay connection.

minor alarm A local or remote failure that is not affecting operation of the network, but nonetheless should be investigated.

N

n+1 redundancy A redundancy method in which a group of cards share the same standby redundant card.

Network-to-Network Interface (NNI) The protocol at a frame relay port that serves as a bidirectional interface between a local Cisco WAN switching network and a separate and independent “other” network.

node An IGX or BPX switch serving as a connection point to the network. At a node, connections from service lines are routed to trunks for transmission to other nodes in the network.

NPM (Network Processor Module) Micro-processor based system controller front card that contains the software used to operate the IGX switch.

NRM Maximum number of cells a source may send for each forward RM cell, that is, an RM cell must be sent for every Nrm-1 data cells.

NTM (Network Trunk Module) IGX front card that coordinates fastpacket trunk traffic to another node via a number of backcards: T1, E1, Y1, and subrate (RS449, X.21, and V.35).

O

OC-3 Standard optical transmission facility rate of 155.20 Mbps.

OCC (Other Common Carrier) In the United States, reference to all the other telecommunications companies providing various transmission services other than AT&T.

P

packet line Packet line referred to a line used to carry FastPackets between nodes in a network. The term in these documents is replaced by the more general “trunk” which is defined as a physical link from node to node, node to shelf, or node to network. The trunk may be one that supports 24-byte FastPackets (packet trunk), or one that supports 53 byte ATM cells (cell trunk).

packet switching A system that breaks data strings into small units (packets), then individually addresses and routes them through the network.

PAD (Packet Assembler/Disassembler) A device that converts a serial data stream into discrete packets in the transmit direction and converts the received packets back into a serial data stream. Adds header information in the transmit packet to allow it to be routed to the proper destination.

partially-interleaved EIA One control lead in each direction, generally RTS-CTS, is transmitted in same byte as seven data bits. For fast control lead response to data being turned on and off.

PBX (private branch exchange) Digital or analog telephone switchboard, classified as customer premise equipment (CPE), used to connect private and public telephone networks.

PCM (Pulse Code Modulation) The system for transmitting telephone signals digitally. Voice is sampled 8000 times per second and converted to an 8-bit digital word.

PCR (Peak Cell Rate) The maximum rate for an ATM connection at which cells are allowed into the network.

PCS (Port Concentrator Shelf) The PCS is an external shelf that expands the capacity of the FRP card. The PCS is sued with the FRM-2 (IGX switch) card to 44 frame relay connections. The PCS connects to the FRI-2.X.21 backcard.

PIR (Peak Information Rate) The peak level in bits per second allowed for a frame relay connection.

PLCP (Physical Layer Convergence Protocol) A protocol defined for use with Switched Megabit Data Service. Used on DS3 ATM trunks in the BPX switch.

PLPP (Physical Layer Protocol Processor) A custom VLSI processor used in the T3 ATM port interface of the BPX BNI card to handle the coding and decoding of the PLCP bit structure. Functions handled by the PLPP include header check sequence generation and checking, DS3 framing, and optional payload scrambling/descrambling.

plesiochronous network A network where there is more than one source of network timing. The multiples sources must be operating at the same frequency but are not phase locked (synchronous) with each other.

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 Refers to a signal connection on a data back card that interfaces to a customer circuit or data device. The number of ports on a card ranges from 1 to 8 depending on the particular card type.

“Port” is synonymous with “Interface.”

The VSI makes no distinction between trunk ports and end-point ports.

P

PRI (Primary Rate Interface) An ISDN interface to primary rate access. Primary rate access consists of a single D channel for signalling and 23 (T1) or 30 (E1) B (bearer) channels for user data. A PRI is typically carried on T1 or E1 facilities.

privilege level A level between 1 and 6 that is assigned to each command. Each operator is assigned a privilege level by the system administrator. The operator may only access and execute commands equal to or lower than his or her own privilege level. Level 1 is the highest and level 6 is the lowest.

PVCs Permanent Virtual Connections (circuits). Connections that are assigned but not connected until data is sent, thereby not using bandwidth when idle.

Q

QQ.921/Q.931 ITU-T specifications for the ISDN use network interface (UNI) data link layer.

QSIG A common-channel message-oriented signalling protocol, defined by the European Telecommunications Standard Institute (ETSI), commonly used by private branch exchanges (PBXes). The INS Dynamic Network Switching application supports QSIG signalling to the Cisco WAN switching network.

queue A buffer that is used to temporarily hold data while it waits to be transmitted to the network or to the user.

R

RRIF (Rate increase factor) Controls the amount by which the cell transmission rate may increase upon receipt of an RM cell.

RDF (Rate decrease factor) Controls the amount by which the cell transmission rate may decrease upon receipt of an RM cell.

red alarm Another name for local alarm as the local alarm lamp on most digital transmission equipment is red in color.

remote alarm An alarm indicating that the associated T1 line is down due to a receive line failure on another node. (See also yellow alarm.)

RPS (repetitive pattern suppression) Also called data frame multiplexing (DFM). An option for data circuits where repeating strings of data are replaced on the packet line by a single occurrence of the data string and a code that indicates to the far end how may repetitions of the string was being transmitted. Used to conserve network bandwidth.

robbed bit signaling A type of signaling used on T1 lines where the signaling bits for each channel are substituted for the least significant voice bit in each channel word during frames 6 and 12.

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.

R

RS-232 A physical and electrical interface standard for a low-speed, unbalanced, serial, data interface adopted by the EIA committee on data communications. Generally used for data circuits operating at data rates below 56 Kbps.

RS-422/423 Another EIA standard electrical interface for serial data circuits operating at higher data rates than RS232. RS422 is a balanced interface; RS423 is unbalanced. Uses RS-449 for the physical interface (connector).

RS-449 The physical interface for the RS422 and R423 electrical interfaces. Contains the Processor Controller Card and the PCC utility bus, and provides system timing and control via the system bus.

S

SSAR (Segmentation and Reassembly) The process of breaking a dataframe containing data from a number of virtual paths or circuits apart so that the individual paths/circuits can be switched by reassembling the data into a new frame with a different sequence.

SCM (System Clock Module) An IGX backcard that works in conjunction with the NPM. The SCM provides a centralized clock generation function and provides serial and LAN port interfaces.

SCR (Sustainable Cell Rate) Rate above which incoming cells are either tagged or discarded.

SDP (Synchronous Data PAD)

SDI (Synchronous Data Interface) The back card for the HDM (IGX switch) cards. The SDI is available with V.24, X.21, and V.35 interfaces.

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. 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.

Simple Gateway Refers to FastPacket to ATM interworking with respect to the IGX node. In the simple gateway mode, FastPackets are encapsulated in their entirety into cells. Compare with complex gateway.

SIU (Serial Interface Unit) A set of circuits common to all BPX cards used for transmitting and receiving via the crosspoint switch.

S

Soft PVC A PVC in the INS Dial-Up Frame Relay application that is dormant in the networks database until it is activated by a call into the network by a user.

spanning tree An network topology in which there is only one path available between any two sources in a frame relay multicast group. Spanning trees are required to prevent frames broadcast from a single source to multiple receptors from circulating endlessly around the network a result of frame relay circuits not having properly closed loops.

speech detection Determining the presence or absence of speech for Digital Speech Interpolation. Performed in either the CDP card.

split clock A data clocking configuration where the timing for the transmit data is obtained from one source (such as a user device) and the timing for the receive data is obtained from another source (such as a switch).

Status Enquiry A message transmitted by a FR NNI port requesting an updated status from the attached foreign network. This message is used as a heartbeat to detect when a port has failed.

StrataBus On the BPX switch, contains crosspoint wiring used to carry ATM trunk data between both the network interface and service interface modules and the crosspoint switch as well as providing control, clock, and communications.

subrate data Multiple low-speed data circuits carried in a single DS0 timeslot.

superrate data Single high-speed data circuit carried in multiple DS0 timeslots.

SCR (Sustained Cell Rate) Long term limit on the rate a connection can sustain.

SVC (switched virtual circuit) A virtual circuit that is dynamically established on demand and torn down when transmission is complete. SVS do not need to reserve any network resources when they are not in use. Called a switched virtual connection in ATM terminology. Compare with PVC.

T

T1 The standard US. multiplexed 24-channel voice/data digital span line. Operates at a data rate of 1.544 Mbps.

T3 Transmission service at DS3 rate of 44.736 Mbps.

TBE (Transient Buffer Exposure) The negotiated number of cells that the network would prefer to limit the source to send during the start-up period.

TDM (time division multiplexing) The process of combining several communication channels by dividing a channel into time increments and assigning each channel to a timeslot.

timestamp A field in certain FastPacket formats that indicates the amount of time the packet has spent waiting in queues during the transmission between its source and destination nodes. Used to control the delay experienced by the packet.

Trm An upper bound on the time between RM cells for an active source, i.e., RM cell must be sent at least once every Trm msec.

T

trunk A physical link between two nodes. The trunk may be one that supports 24-byte FastPackets (packet trunk), or one that supports 53 byte ATM cells (cell trunk.)

trunk conditioning A set of signalling and information bits that indicate a DS1 line failure.

trunk queues The buffers in packet line cards (NTC, TXR) where the various FastPackets are queued up for transmission over the packet line(s). The buffers attempt to prioritize each packet so it experiences minimum delay.

U

μ-law An analog to digital encoding scheme used to convert voice samples to an 8-bit data word used in D3/D4 T1 multiplex equipment.

UBR Unspecified Bit Rate.

UNI (User to Network Interface) The user to network interface, used for ATM connection to CPE. Compare with NNI.

UPC (Usage Parameter Control) A general procedure for controlling the rate of user data applied to an ATM network. There are a number of different algorithms for performing UPC. See also GCRA.

USART (Universal Synchronous/Asynchronous Receiver Transmitter) A single-chip device used in certain applications that allows microprocessors to communicate with input/output (I/O) devices.

User to Network Interface (UNI) The protocol at a frame relay port that passes information between the network and the user device attached to the port.

V

V.21 A CCITT interface standard often used for data transmission over modems.

V.35 A data communications interface standard adopted by the CCITT. Often used for data circuits operating at 56 Kbps and above.

VAD (Voice Activity Detection) Used to statistically compress voice by not sending packets in the absence of speech.

VBR (Variable Bit Rate) Connection type for variable bit rate traffic such as bursty data. Compare with CBR and ABR.

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.

V

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).

VC_Q Frame relay buffer allocation parameter that specifies the maximum queue size reserved in the FRP card for the FR connection.

virtual circuit A circuit that acts like it is an individual transmission path but is actually shared with other circuits over a single transmission path. Compare with PVCs.

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.

VNS The adjunct processor used in the INS Voice Network Switching application. The VNS is co-located with and connected to an IGX switch.

Voice Network Switching An INS application used to provide voice or data switched virtual circuits over a Cisco WAN switching network for PBXes using either QSIG or DPNSS signalling.

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 switches 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.

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.

V

VS/VD (Virtual Source/Virtual Destination) ATM Forum Traffic Management 4.0 method of providing congestion flow control for ABR connection types. Resource Management (RM) cells are used to convey management information between sources and destinations.

vt (virtual terminal) An control terminal that is the active control terminal at one node but is physically attached to another node.

W

WAN (Wide Area Network) A network of transmission circuits generally spanning a large region or territory for transmission of voice and data between widespread end users. An IGX/BPX network is an example of a WAN.

X

X.21 A CCITT standard for data interfaces transmitting at rates up to approximately 2 Mbps.

X.25 A commonly-used standard that defines the protocol for low-speed data packet networks.

XON/XOFF A simple communications protocol for controlling the flow of data from one device to another. An XON sent from a receiving device indicates it is ready to accept data and the transmitting device may begin to output data. An XOFF from the receiving device indicates that it can no longer store any more data and the transmitting device should temporarily cease transmitting.

Y

YY-cable(s) A short adapter cable forming an electrical branch (thus the term Y) for connecting a single customer data or trunk connection to two identical back cards to provide hardware redundancy on the IGX switch.

Y-cable redundancy A redundancy type used in the switch when a 1:1 card redundancy is implemented using a split or Y-cable for the data connection between the user device and the primary and standby interface card.

Y1 A digital trunk conforming to the Japanese “Y” circuit standard, for use as a packet line. Similar to T1, it operates at 1.544 Mbps.

yellow alarm Another name for remote alarm as the remote alarm lamp on digital transmission equipment is always yellow in color.

INDEX