Cisco BPX 8600 Series Installation and Configuration

Release 9.2
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-786325=
Text Part Number: 78-6325-04 Rev. B0

TTHE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

Cisco BPX 8600 Series Installation and Configuration, Release 9.2

Feedback on the Cisco BPX 8600 Series Installation and Configuration

Release 9.2, July 2001

Part No. 78-6325-04 Rev. B0

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

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

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

Cisco Systems, Inc.
Attn: Central
Documentation Services
170 West Tasman Drive
San Jose, CA 95134-9883

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

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

CISCO SYSTEMS

Documentation Response Card

Feedback on the Cisco BPX 8600 Series Installation and Configuration, Release 9.2, July 2001, Part No. 78-6325-04 Rev. B0

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

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

Overall, I am satisfied with this document.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

This document is accurate and free of errors.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

I can find the information I need in this document.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

This document is complete and offers enough relevant information for me to do my job.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

This document is written at the correct level of complexity for the subject matter.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

This document is useful to me in doing my job.
Strongly agree **5** □ **4** □ **3** □ **2** □ **1** □ Strongly disagree

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

Additional Feedback

Mailing Information

Date

Company Name

Contact Name

Mailing Address

City State/Province

Zip/Postal Code Country

Phone ( ) Extension

Fax ( ) E-mail

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN CENTRAL DOCUMENTATION SERVICES
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883

TABLE OF CONTENTS

PART 4 Configuration, General

PART 5 Configuration, MPLS

LIST OF FIGURES

LIST OF TABLES

About This Manual

This publication provides installation procedures and related information for the installation of the BPX 8600 Series wide-area switches which include the BPX 8620 switch and the BPX 8650 MPLS switch.

Refer to 9.2 Release Notes for supported features.

Documentation CD-ROM

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

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

Objectives

This publication provides information for the installation and initial startup and configuration of the BPX 8600 series.

Audience

This publication is intended for persons installing the BPX 8600 series. The 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 and with the WAN Manager Network Management System.

Cisco WAN Switching Product Name Change

The Cisco WAN Switching products have new names. Any switch in the BPX switch family (Cisco BPX® 8620 broadband switch and Cisco BPX® 8650 broadband switch) is now called a Cisco BPX® 8600 series broadband switch. The BPX Service Node switch is now called the Cisco BPX®

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

Organization

This publication is organized as follows:

PART 1 **Introduction**

Chapter 1 **Introduction**

Provides a brief introduction to the document, including a flow diagram that shows which procedures are applicable to the various options, Cisco Cabinet or Customer Cabinet, ac cabinet or dc cabinet

PART 2 **Quickstart**

Chapter 2 **Quickstart Installation and Configuration**

Provides a summary of the contents of the major parts of the manual.

PART 3 **Installation**

Chapter 3 **Installation Summary**

Provides a summary of the procedures and a flow diagram showing the overall installation tasks in PART 1.

Chapter 4 **Installation, Preliminary**

Includes preliminary instructions including site preparation information, parts checklist, and safety requirements.

Chapter 5 **Installation with Cisco Cabinets including 7000 Series Routers**

Provides installation steps for the mechanical placement of a BPX switch in a standard Cisco cabinet. This cabinet provides rear rails at a 19.86 inch (50.5 cm) setback from the front of the cabinet.

Chapter 6 **Installation with Customer Cabinet**

Provides installation steps for the mechanical placement of a BPX switch in a standard 19-inch wide customer supplied equipment cabinet or rack with a rear rail setback at 30 inches.

Chapter 7 **Installation, DC Shelf Initial Setup**

Describes how to make the DC power connections.

Chapter 8 **Installation, AC Shelf Initial Setup**

Explains how to install the AC power supply tray, power supplies, and make AC power connections.

Chapter 9 **Finishing the Installation and Power-Up**

Explains how to install the BPX switch cards, connect the line and trunk cables, connect peripherals, connect to a network management station, and initial power-up.

Chapter 10 **T3/E3 Cable Management Tray**

Provides instructions for the installation of the optional cable management tray that may be used to route cables in an open rack non-redundant configuration.

PART 4 **Configuration, General**

Chapter 11 **Configuration, Introduction**

Provides a brief introduction to BPX switch configuration, including a flow diagram showing the applicable procedures.

Chapter 12 **Configuration, Initial Setup**

Provides initial BPX switch configuration information.

Chapter 13 **Configuration, ATM Connections**

Provides general ATM description and ATM connection parameter information for CBR, VBR, UBR, and ABR connections.

Chapter 14 **Configuration BXM: PVCs, SVCs, and SPVCs**

Provides a brief description of BXM switch functions and describes command line interface commands for configuring the BXM and for configuring resource partitions for PVCs and SVCs. Refers to other chapters in this manual and to other documents, as applicable, for tag switching and SVCs and SPVCs.

Chapter 15 **Configuration, BXM Virtual Trunks**

Provides a brief overview of BXM Virtual Trunks and configuration procedures.

Chapter 16 **Configuration, BXM VSIs**

Provides a brief overview of Vitual Switch Interface features and resources and configuration procedures.

Chapter 17 **SONET APS, Configuration**

Provides a description and configuration information for the SONET Automatic Protection System (APS) which may be used to provide line and card redundancy for SMF and SMF LR BXM OC3 and OC12 cards.

Chapter 18 **Configuration, BME Multicasting**

Provides a brief overview of BME multicasting and provides configuration examples.

PART 5 **Configuration, MPLS**

Chapter 19 **Configuration General, MPLS on BPX Switch**

Provides a brief overview of MultiProtocol Label Switching (MPLS) and configuration procedures for MPLS on the BPX switch.

Chapter 20 **Configuring the BPX Switch, 7200, and 7500 Routers for MPLS**

Provides a summary overview of MPLS with respect to both the MPLS router controlling function and the BPX node slave switching function and an example of an integrated MPLS configuration procedures.

Chapter 21 **MPLS CoS with BPX 8650, Configuration**

Provides a description of MPLS CoS with the use of the BPX 8650 ATM Label Switch Router (ATM LSR). It also contains a summary example for configuring BPX 8650 LSRs, their associated LSCs (7200 or 7500 series, and Label Edge Routers

Chapter 22 **MPLS VPNS with BPX 8650, Configuration**

Provides a description of MPLS VPNs with the use of the BPX 8650 ATM Label Switch Router (ATM LSR). It also contains a summary example of the configuration of IOS to support VPNs, and references to relevant IOS documentation. Refer to 9.2 Release notes for supported features

PART 6 **Operation and Management**

Chapter 23 **Cisco WAN Manager**

Provides a brief overview of network management of the BPX switch and associated equipment by the Cisco WAN Manager, also referred to as CWM, and formerly known as StrataView Plus.

Chapter 24 **CiscoView**

Provides a brief overview of network management of the BPX switch and associated equipment by Cisco View

PART 7 **Upgrades**

Chapter 25 **Upgrading MPLS Networks to Switch SW Rel. 9.2 and BXM FW Rel. E**

Provides procedures to upgrade MPLS networks from BPX switch software Release 9.1 and BXM firmware Release C, to switch software Release 9.2.x and BXM Firmware Release E.

PART 8 **Reference**

Provides procedures to upgrade MPLS networks from BPX switch software Release 9.1 and BXM firmware Release C, to switch software Release 9.2.x and BXM Firmware Release E.

Appendix A **Cisco Cabinet Dimensions**

Illustrates typical cable management and space requirements for various system configurations in the Cisco cabinet. It also lists the height of components in inches, centimeters, and rack-mount units (RMUs).

Appendix B **BPX Switch Cabling Summary**

Provides details on the cabling required to install the BPX switch.

Appendix C **BPX Switch Peripherals**

Provides details on the peripherals used with the BPX switch including printers and modems.

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 WAN Manager Operations* document providing for procedures for using the Cisco WAN Manager network management system.
- *Cisco WAN Design Tools User Guide* provides procedures for modeling networks.
- *Cisco WAN Service Node Extended Services Processor Installation and Operation* Release *2.2* provides detailed information about the Extended Services Processor (ESP).
- Release 9.2 of the IGX/BPX documentation set, including:
    - *Cisco BPX 8600 Series Reference* provides a general description and technical details of the BPX broadband switch.
    - *Cisco IGX 8400 Series Reference* provides a general description and technical details of the IGX multiband switch.
    - *Cisco IGX 8400 Series Installation and Configuration* provides installation instructions for the IGX multiband switch.
    - *Cisco MGX 8220 Reference* provides a general description and technical details of the MGX 8220.
    - *Cisco MGX 8220 Command Reference* provides detailed information for MGX 8220 command line usage.
    - *Cisco WAN Switching Command Reference* provides detailed information on operating the BPX, IGX, and IPX systems through their command line interfaces.
    - *Cisco WAN Switching SuperUser Command Reference* provides detailed information on their command line interfaces special commands requiring SuperUser access authorization.

Conventions

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

Command descriptions use these conventions:

- Commands and keywords are in **boldface**.
- Arguments for which you supply values are in *italics*.
- 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 Dette 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

Introduction

Introduction

This document provides installation and configuration instructions for the BPX 8600 Series wide-area switches. It is divided into a number of parts. This is the first part that tells you very briefly what's in the document. If you see text or a reference underlined in this document, you can click on it to go to the linked area.

- PART 1, Introduction—Summarizes what's in this document.
- PART 2, Quickstart—Provides a quick start guide to installation and an abbreviated configuration guide. Detailed installation and configuration procedures are provided in their separate sections of this document.
- PART 3, Installation—Provides detailed installation instructions.
- PART 4, Configuration, General—Provides detailed configuration examples.
- PART 5, Configuration, MPLS—Provides detailed configuration examples.
- PART 6, Operation and Management—Provides Operation and Management and NMS information.
- PART 7, —Provides procedures to upgrade MPLS networks from BPX switch software Release 9.1 and BXM firmware Release C, to switch software Release 9.2.x and BXM Firmware Release E.
- PART 8, Reference—Provides reference information, cabling, i.e.

PART 2

Quickstart

Quickstart Installation and Configuration

Introduction

This section provides a summary of configuration procedures for the BPX. Detailed procedures are provided in later chapters of this manual.

For additional information on the BPX switch, including card descriptions and additional information on configuration, refer to the *Cisco BPX 8600 Series Reference*. For a description of the commands used to operate a BPX switch, refer to the *Cisco WAN Switch Command Reference* and *Cisco WAN Switch SuperUser Command Reference.* Refer to the *Cisco WAN Manager* manuals for information on network management.

Installation Sequence

A summary of the installation sequence for the BPX follows:

Step 1 Safety... refer to Chapter 4, Installation, Preliminary

Step 2 Site Preparation... refer to Chapter 4, Installation, Preliminary

Step 3 Unpacking... refer to Chapter 4, Installation, Preliminary

Step 4 Installing shelf in cabinet or rack... refer to Chapter 4, Installation, Preliminary

Step 5 Installing a Cisco 7200 or 7500 router on a BPX 8650... refer to Chapter 5, Installation with Cisco Cabinets including 7000 Series Routers.

Step 6 Optional Cable Management Tray... refer to Chapter 10, T3/E3 Cable Management Tray.

Finishing the Installation and Initial Power-Up

A summary of these procedures is as follows:

Power-Up and Initial Configuration... refer to:

Step 1 Installing the BPX Switch Cards

Step 2 Verifying 9.6 or 19.2 Gbps Backplane

Step 3 Upgrading to BCC-4 Cards

Step 4 Installation of APS Redundant Frame Assembly and Backcards

Step 5 Making T3 or E3 Connections

Step 6 Making an ASI-155 or BNI-155 Connection

Step 7 Making a BXM OC3 or OC12 Connection

Step 8 Making a BXM T3/E3 Connection

Step 9 Setting up the BME OC-12 Port Loop

Step 10 Alarm Output Connections

Step 11 Attaching Peripherals

Step 12 LAN Connection for the Network Management Station

Step 13 Connecting a Network Printer to the BPX Switch

Step 14 Connecting Modems

Step 15 Making External Clock Connections

Step 16 Initial Power-Up of the BPX Switch

Step 17 Provisioning the BPX Switch

Step 18 Configuration

Configuration

The following provides a summary of the procedures to configure various functions of the BPX. For more detailed information, you are referred to specific chapters in this manual, or to other associated Cisco Documents, as applicable.

Configuration, Lines, Trunks, and Connections

Lines and Trunks can be added and configured in many cases using the Cisco WAN Manager Equipment Manager. In other cases, the command line interface (CLI) is used. For additional information, refer to the *Cisco WAN Switch Command Reference*.

Configuration, ATM Connections

Connections are typically added using the Cisco WAN Manager Connection Manager. In other cases, the command line interface is used.

To add an ATM connection, for example, the following CLI command may be used:

addcon local_addr node remote_addr traffic type ...extended parameters

For example, for an abr connection:

at bpx 1, addcon 4.1.30.30 bpx2 3.1.40.40 abr ...extended parameters

For additional information, refer to Chapter 13, Configuration, ATM Connections.

Configuration, PVCs, SVCs, and SPVCs

Upping and configuring trunks. For additional information, refer to Chapter 14, Configuration BXM: PVCs, SVCs, and SPVCs. Some of the applicable CLI commands are:

```
uptrk 4.1
addtrk 4.1
upln 3.3
cnfln 3.3
cnfport 3.3
cnfportq 3.3
upport 3.3
cnfcls 1
cnfcls 2
addcon 3.1.105.55 bpx1 3.2.205.65 v ...........
cnfcon 3.1.105.55
addcon 3.1.104.54 bpx1 3.2.204.64 abr ...........
cnfcon 3.1.104.54
cnfabrparm 3
dsplns
dsptrks
```

ASI SVC Resource Partitioning

cnfport 2.1

cnfportq 2.1

BXM SVC Resource Partitioning

cnfport 13.1

cnfportq 13.1

BNI Trunk SVC Partitioning (NNI)

cnftrk 5.1

cnftrkparm 5.1

BXM Trunk SVC Resource Partitioning

cnftrk 3.1

cnftrkparm 3.1

Configuration Virtual Trunks

Refer to the configuration information in Chapter 15, Configuration, BXM Virtual Trunks.

Configuration, VSI

Refer to the configuration information in Chapter 16, Configuration, BXM VSIs.

Configuration, SONET APS

Refer to the configuration information in Chapter 17, SONET APS, Configuration.

Configuration, Multicasting PVCs, Adding Connections

The following is a short summary example of multicasting commands.

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 * * *

For additional configuration information, refer to Chapter 18, Configuration, BME Multicasting.

Configuration, MPLS

Refer to the MPLS configuration procedures in Chapter 20, Configuring the BPX Switch, 7200, and 7500 Routers for MPLS. For additional information, refer to Chapter 19, Configuration General, MPLS on BPX Switch.

For MPLS CoS Configuration information, refer to Chapter 21, MPLS CoS with BPX 8650, Configuration.

For MPLS VPN Configuration information, refer to Chapter 22, MPLS VPNS with BPX 8650, Configuration

Customer Support

Contact your local Cisco sales office for Customer Service information.

PART 3

Installation

CHAPTER 3

Installation Summary

Introduction

This part of the manual provides installation and power-up instructions for the BPX 8600 Series wide-area switches. This chapter provides a summary of the procedures and a flow diagram showing the overall installation tasks covered in *PART 3* of this manual.

- Installation instructions are provided in this part, *PART 3*.
- Configuration information, except for MPLS, is provided in *PART 4*.
- Configuration information specific to MPLS and MPLS VPNs is provided in *PART 5*.
- References to Cisco WAN Manager and CiscoView are provided in *PART 6*.
- Reference information, such as cabling, and specifications is provided in *PART 8*.

For additional information on the BPX switch, including card descriptions and additional information on configuration, refer to the *Cisco BPX 8600 Series Reference*. For a description of the commands used to operate a BPX switch, refer to the *Cisco WAN Switching Command Reference*. Refer to the *Cisco WAN Manager* manuals for information on network management.

Installation Sequence

Figure 3-1 shows the sequence of operations followed during the installation of the BPX switch. A summary of this sequence is as follows:

- *Chapter 4, Installation, Preliminary*, provides preliminary setup instructions for the mechanical installation of a BPX switch shelf. Depending on the type of rack or cabinet, the installer is then directed to either:
    - — *Chapter 5, Installation with Cisco Cabinets including 7000 Series Routers* with rear rail setback at 19.86 inches, or
    - — *Chapter 6, Installation with Customer Cabinet* that is 19 inches wide with a rear rail setback of 30 inches.
    - — Otherwise, the installation is non-standard and requires that Customer Service be contacted.

The BPX switch shelves are either AC or DC powered. At the completion of the procedures in *Chapter 5* or *Chapter 6*, the installer is directed to the appropriate power setup and connection chapter:

- *Chapter 7, Installation, DC Shelf Initial Setup*, or
- *Chapter 8, Installation, AC Shelf Initial Setup.*

The remaining installation procedures are common and the installer is directed to the final setup and configuration procedures in:

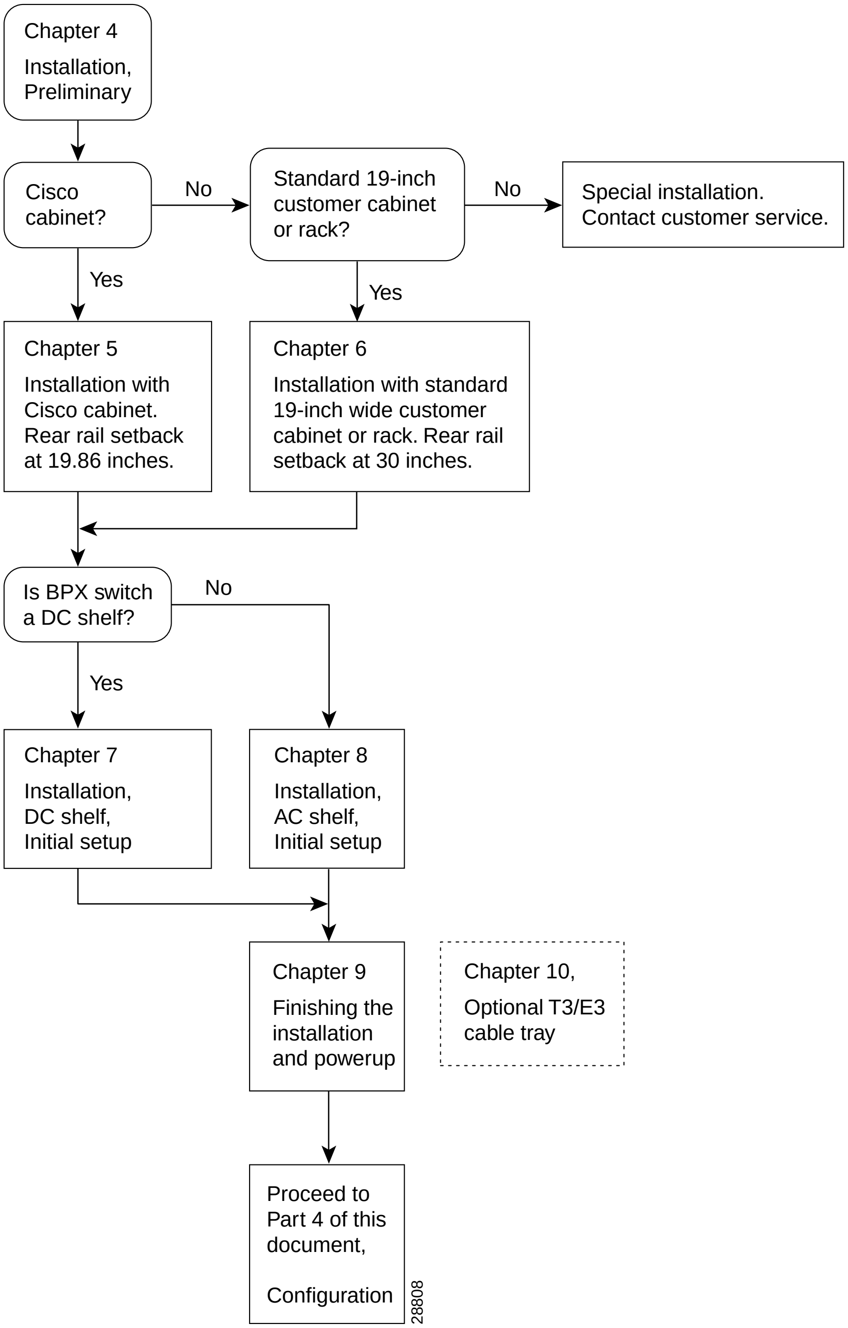
- *Chapter 9, Finishing the Installation and Power-Up*

An optional cable management tray and optional BXM T3/E3 cable management brackets are available for use with T3/E3 BXM cards. The brackets are for use with 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 10, T3/E3 Cable Management Tray*

Following the completion of these installation procedures, the BPX switch can be configured. Configuration procedures are provided in *PART 4, Configuration, General*.

Figure 3-1 Installation Sequence


Chapter 4
Installation, Preliminary
Cisco cabinet?
No
Standard 19-inch customer cabinet or rack?
No
Special installation. Contact customer service.
Yes
Yes
Chapter 5
Installation with Cisco cabinet. Rear rail setback at 19.86 inches.
Chapter 6
Installation with standard 19-inch wide customer cabinet or rack. Rear rail setback at 30 inches.
Is BPX switch a DC shelf?
No
Yes
Chapter 7
Installation, DC shelf, Initial setup
Chapter 8
Installation, AC shelf, Initial setup
Chapter 9
Finishing the installation and powerup
Chapter 10,
Optional T3/E3 cable tray
Proceed to Part 4 of this document,
Configuration
28808

Support

Contact your local Cisco sales office for Customer Service information.

Installation, Preliminary

This chapter provides preliminary installation steps for the BPX switch, including the mechanical installation of the BPX switch shelf in a Cisco cabinet or vendor supplied standard 19 inch (48.25 cm) equipment rack.

This chapter contains the following sections:

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

Warning Installation should be performed by authorized personnel only.

Site Preparation

The BPX switch has the following site preparation requirements.

- **Location**
  The BPX switch is to be installed only in a RESTRICTED ACCESS LOCATION.
- **Space**
  Each BPX switch shelf requires floor space of 22 inches (55.9 cm) wide and 80 inches (203.2 cm) deep to assure sufficient clearance around the cabinet to allow access to the front and back of the unit.
- **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 may require up to 2333 VA (13 A at 180 VAC, 10 A at 230 VAC). A maximum configuration for a DC powered BPX switch may 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.

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 which prevent radio frequency emissions from the equipment. The unit must not be operated with any unused slots left uncovered.

Refer to the following list and check the number and type of cards shipped against the number and type of card you ordered.

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

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

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

_____ For a redundant configuration, 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.

______ Correct number of ASI cards.

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

______ One line module backcard (e.g., BPX-T3-BC, BPX-E3-BC, MMF-2-BC, SMF-2-BC, or SMFLR-2-BC) for each ASI, as applicable.

______ All cables specified in the order.

Note An inventory of the installed cards is taped to the BPX switch stating 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

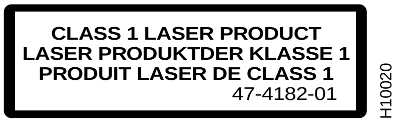
The following paragraphs contain safety information for system planners, installers, and maintenance personnel. The mechanical design of the BPX switch prevents any access to exposed voltages without the use of tools. When installed properly, all front and rear cards are held captive mechanically.

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

Laser Safety Guidelines

The optical ports contain an information label as shown in Figure 4-1.

Figure 4-1 Laser Information Label



CLASS 1 LASER PRODUCT
LASER PRODUKTDER KLASSE 1
PRODUIT LASER DE CLASS 1
47-4182-01

Warning Invisible laser 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).

Maintaining Safety with Electricity

You must install your BPX switch in accordance with national and local electrical codes. In the United States, National Fire Protection Agency (NFPA) 70, United States National Electrical Code. In Canada, Canadian Electrical Code, C22.1, part 1. In 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.

Additional safety statements are provided in the following paragraphs:

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.

The following guidelines will help to ensure your safety and protect the equipment. The list of guidelines may not address all potentially hazardous situations in your working environment so be alert and exercise good judgment at all times.

The safety guidelines are:

- 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 ear rings, 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 that is identical in size to the grounded and ungrounded branch circuit supply conductors, but is green with yellow stripes, is to be installed as part of the branch circuit that supplies the unit.

CEPT Requirements

All apparatus (e.g., 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.

Mechanical Installation

Weight

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

Cooling

Caution If the BPX switch is to be mounted in an enclosed cabinet, assure that a free flow of air in and out of the enclosure is provided. Contact Customer Service for further information.

Horizontal Positioning

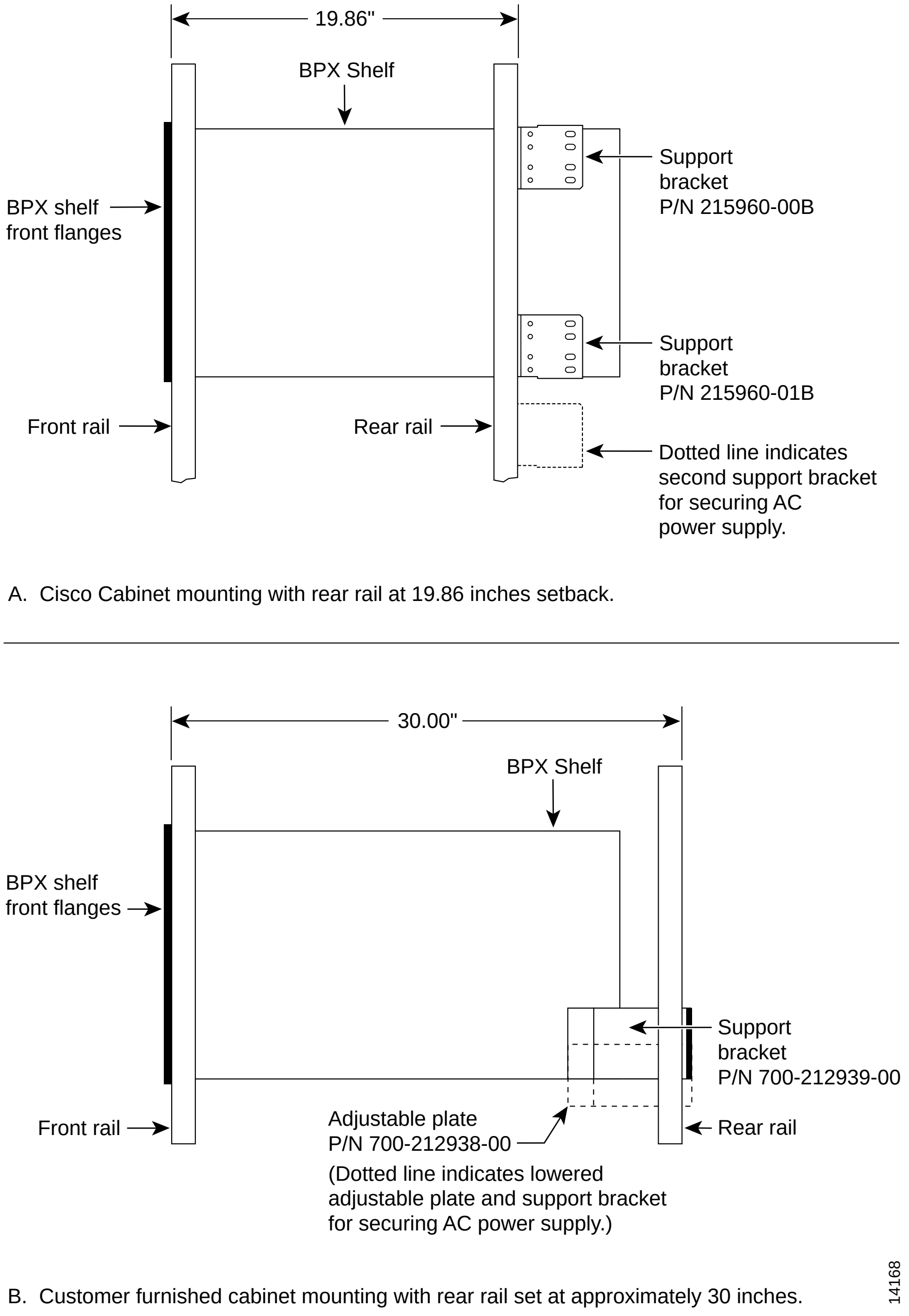
BPX switch shelves are designed to be mounted to two sets of vertical mounting rails in either a Cisco cabinet or a standard 19-inch equipment rack with unrestricted front to rear air flow. When installed in a Cisco cabinet (see Figure 4-2), the front flanges of the BPX switch are secured to the front 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 4-3) 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 *Appendix A, Cisco Cabinet Dimensions*.

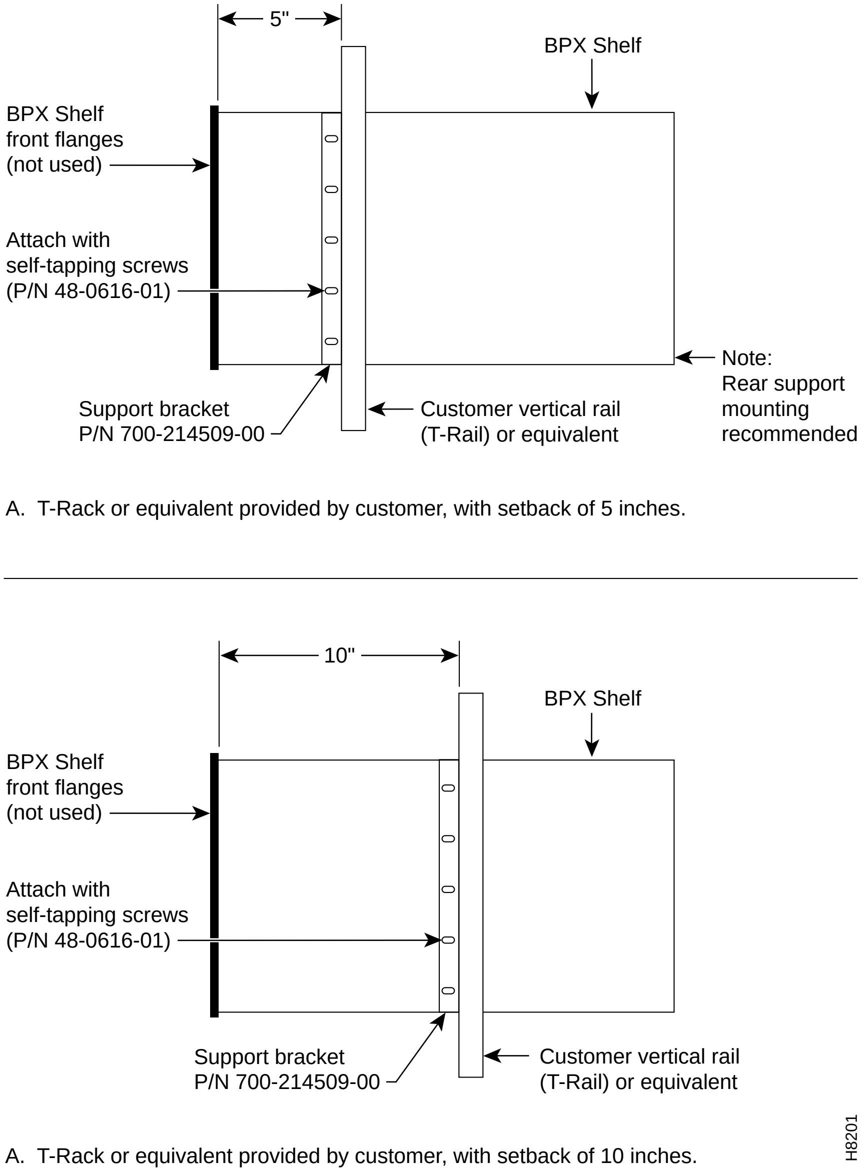
Figure 4-2 Cabinet Mounting Options for the BPX Shelf


19.86"
BPX Shelf
Support bracket P/N 215960-00B
BPX shelf front flanges
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
Rear rail
(Dotted line indicates lowered adjustable plate and support bracket for securing AC power supply.)
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 4-3 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 4-4 and Figure 4-5). Mounting flanges are permanently attached to the front edge of the BPX switch shelf. It is recommended that the shelf be mounted with all plug-in cards temporarily removed to lessen the weight.

There are two types of BPX switch shelves, AC powered and DC powered. When an AC powered BPX switch shelf is installed, an AC Power Supply Tray is installed directly below it. 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 it is slid into a cabinet.

The following instructions are for 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.

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.

To install the BPX switch in a rack proceed as follows:

Step 1 Position the shipping container and pallet in front of the cabinet with the rear of the chassis towards the cabinet. 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 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 4-6 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 4-2 through Figure 4-5 for typical mounting dimensions. Also, for typical mounting configuration examples, refer to *Appendix A, Cisco Cabinet Dimensions*. The appendix lists dimensions in inches, centimeters, and rack mounting units (RMUs). 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 4-7 and Figure 4-8).

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 the BPX switch shelf is being installed in a Cisco cabinet and is using factory installed rear rails located at a 19.86 inch setback from the front, go to Chapter 5, Installation with Cisco Cabinets including 7000 Series Routers, for instructions on actually installing the BPX shelf in a Cisco cabinet.

Step 7 If the BPX switch shelf is being installed in a customer supplied cabinet using rear rail mounting support brackets located at a setback of approximately 30 inches from the front, go to Chapter 6, Installation with Customer Cabinet, for instructions on actually installing the BPX shelf in a Customer cabinet.

Figure 4-4 Rack Mounting Dimensions, DC Powered Shelf

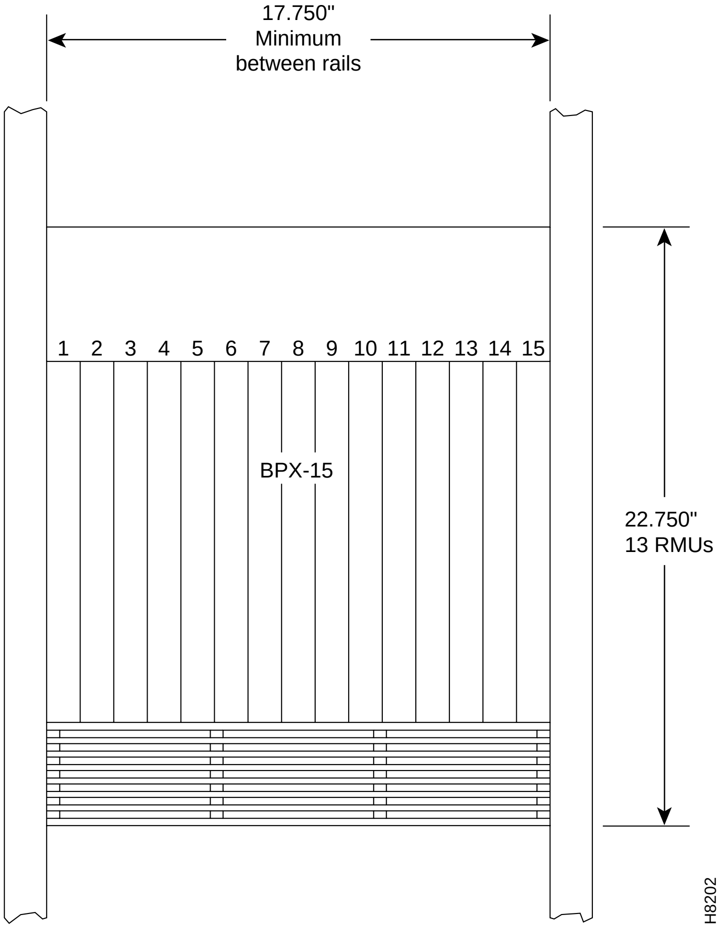


Figure 4-5 Rack Mounting Dimensions, AC Powered Shelf

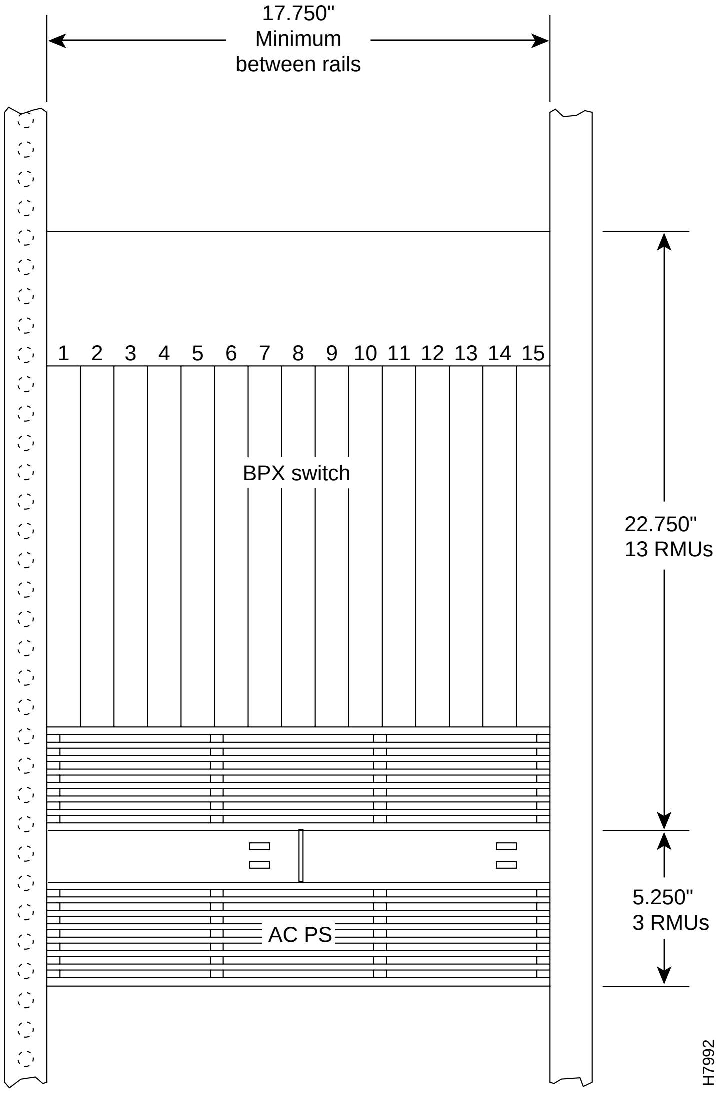


Figure 4-6 Removing an Air Intake Grille

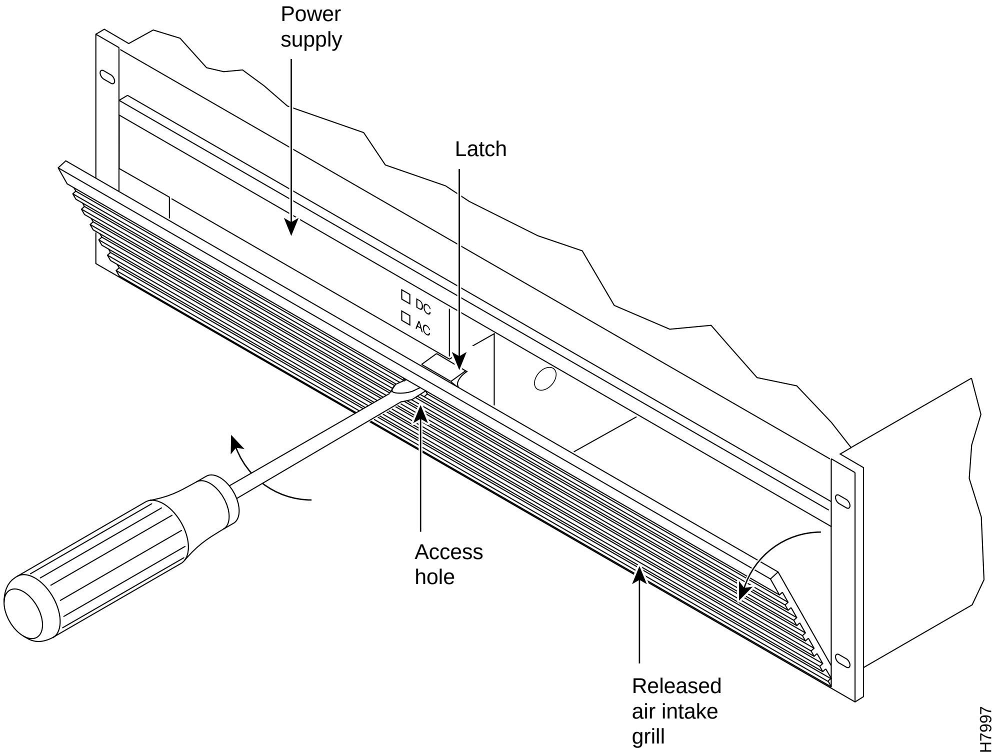


Figure 4-7 Temporary Spacer Bar and Support Brackets Installation

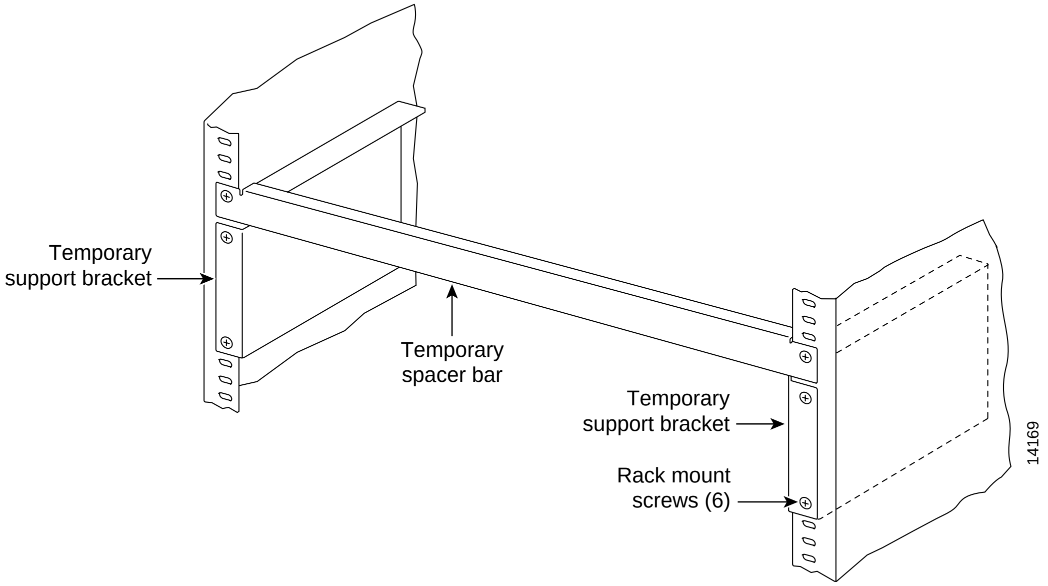
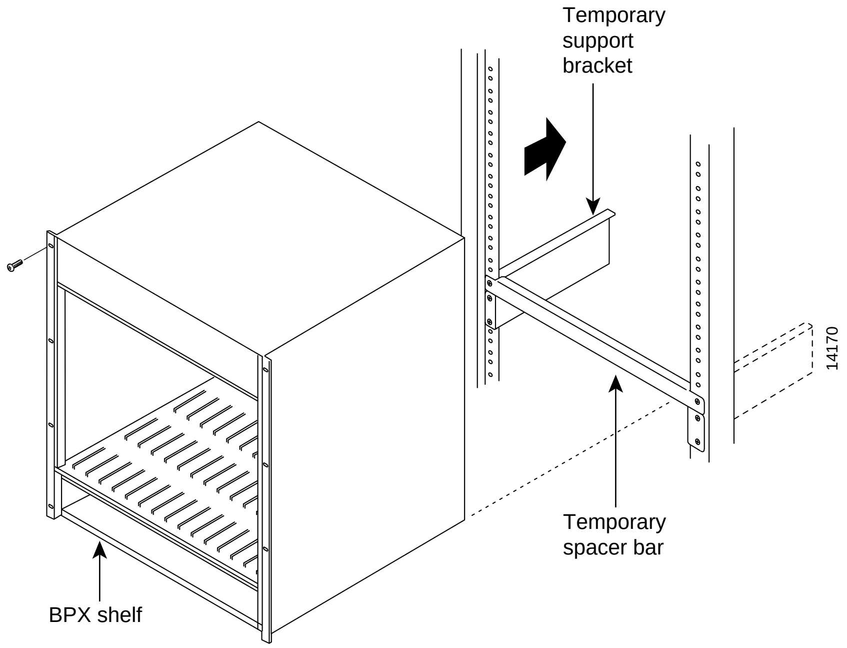


Figure 4-8 BPX Switch Shelf Aligned with Temporary Support Brackets and Bar



Installation with Cisco Cabinets including 7000 Series Routers

This chapter provides installation steps for the mechanical placement of a BPX switch shelf in a standard Cisco cabinet. This cabinet provides rear rails at a 19.86 inch (50.5 cm) setback from the front of the cabinet. This chapter also provides instructions for installing a 7200 or 7500 router in a BPX 8650 cabinet or rack.

Before proceeding to this chapter, the procedures should be completed, in:

— *Chapter 4, Installation, Preliminary*

The chapter contains the following:

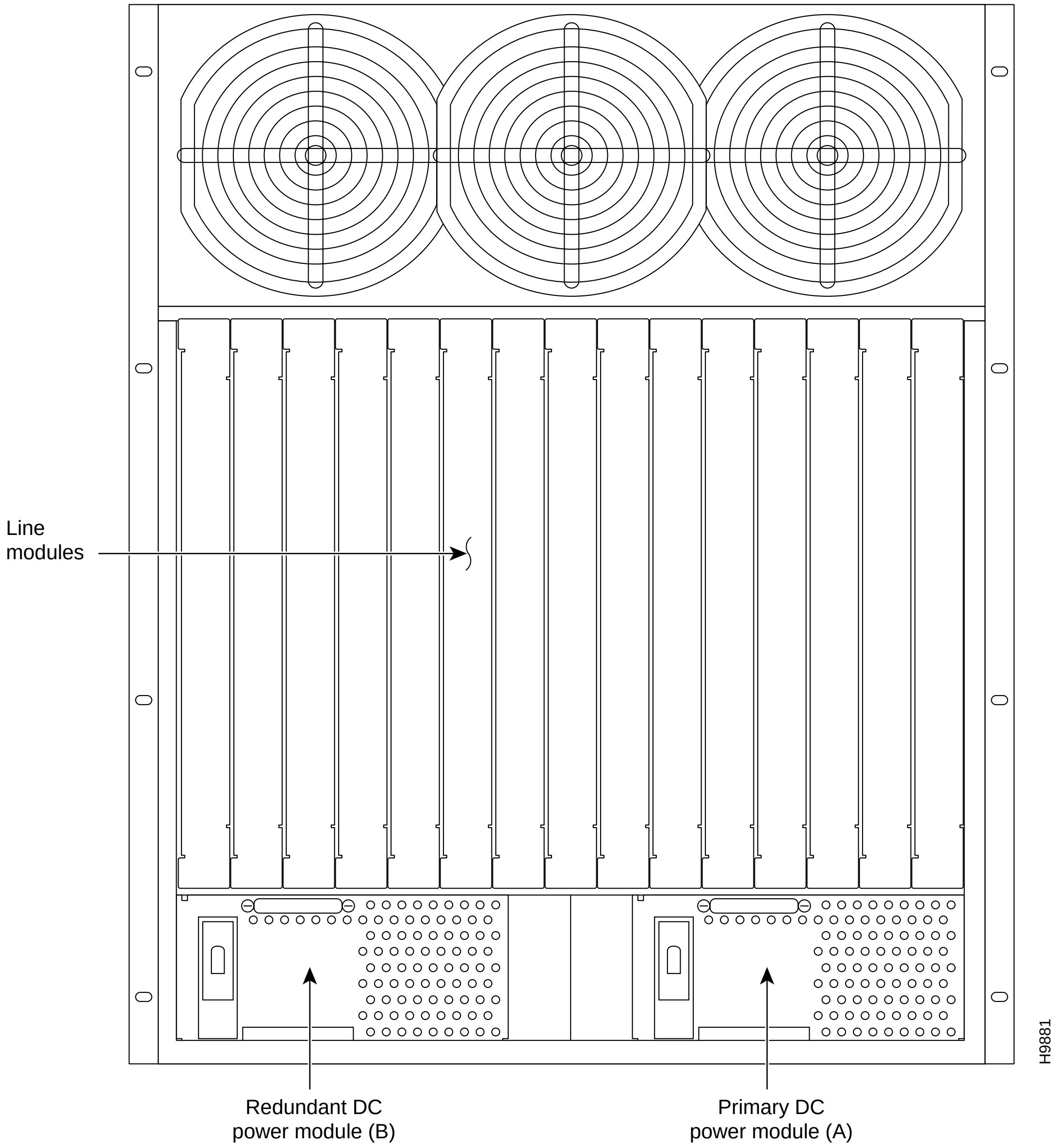
- Installing a BPX Switch in a Cisco Cabinet
- Installing a 7200 or 7500 Router in a BPX 8650 Cabinet or Rack

Installing a BPX Switch in a Cisco Cabinet

The steps in this procedure apply to a BPX switch shelf that is being installed in a Cisco cabinet and using factory installed rear rails located at 19.86 inches 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 5-1). Locate the DC Power Entry Module(s) and make sure it/they are equipped as ordered. If the BPX switch shelf is AC-powered, an AC Power Tray is installed below it as part of the installation process.

Figure 5-1 Location of DC Power Entry Module(s), Cabinet Rear View



Preliminary Procedure:

Proceed as follows to install either an AC or DC powered BPX switch shelf, referring to Figure 5-2 and Figure 5-3 and to either Figure 5-4 for DC powered systems or Figure 5-5 for AC powered systems:

Step 1 With one person on each side of the BPX shelf, lift the BPX shelf and rest it on the temporary space bar and temporary support brackets (see Figure 5-2).

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.

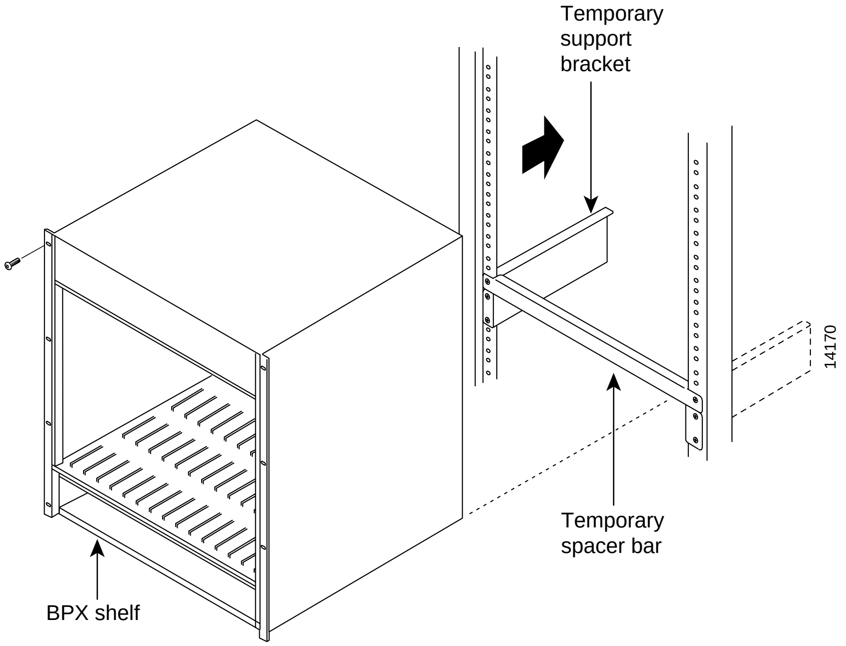
Step 3 Locate the rear support brackets (P/N 215960-00B and 215960-01B) in the miscellaneous parts kit.

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 using two each #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 installation may use a size M6 metric screw.

Warning An empty BPX switch shelf weighs 75 pounds (34 Kgs.) and requires a 2 or 3-person lift to move into place.

Figure 5-2 BPX Shelf Aligned with Temporary Support Brackets and Bar



Step 5 Attach the BPX switch shelf to the cabinet front rail using 8 each # 10-32 screws.

Step 6 An extra set of support brackets may optionally be mounted to the rear rails at the top back of the shelf. These are used to prevent any upward movement of the shelf.

Note If another device is installed above the BPX shelf, the extra set of support brackets can be used 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 7, Installation, DC Shelf Initial Setup.

Step 9 If this is an AC powered shelf, proceed to Chapter 8, Installation, AC Shelf Initial Setup.

Figure 5-3 BPX Shelf with Rear Rail Mounting at Setback of 19.86 inches

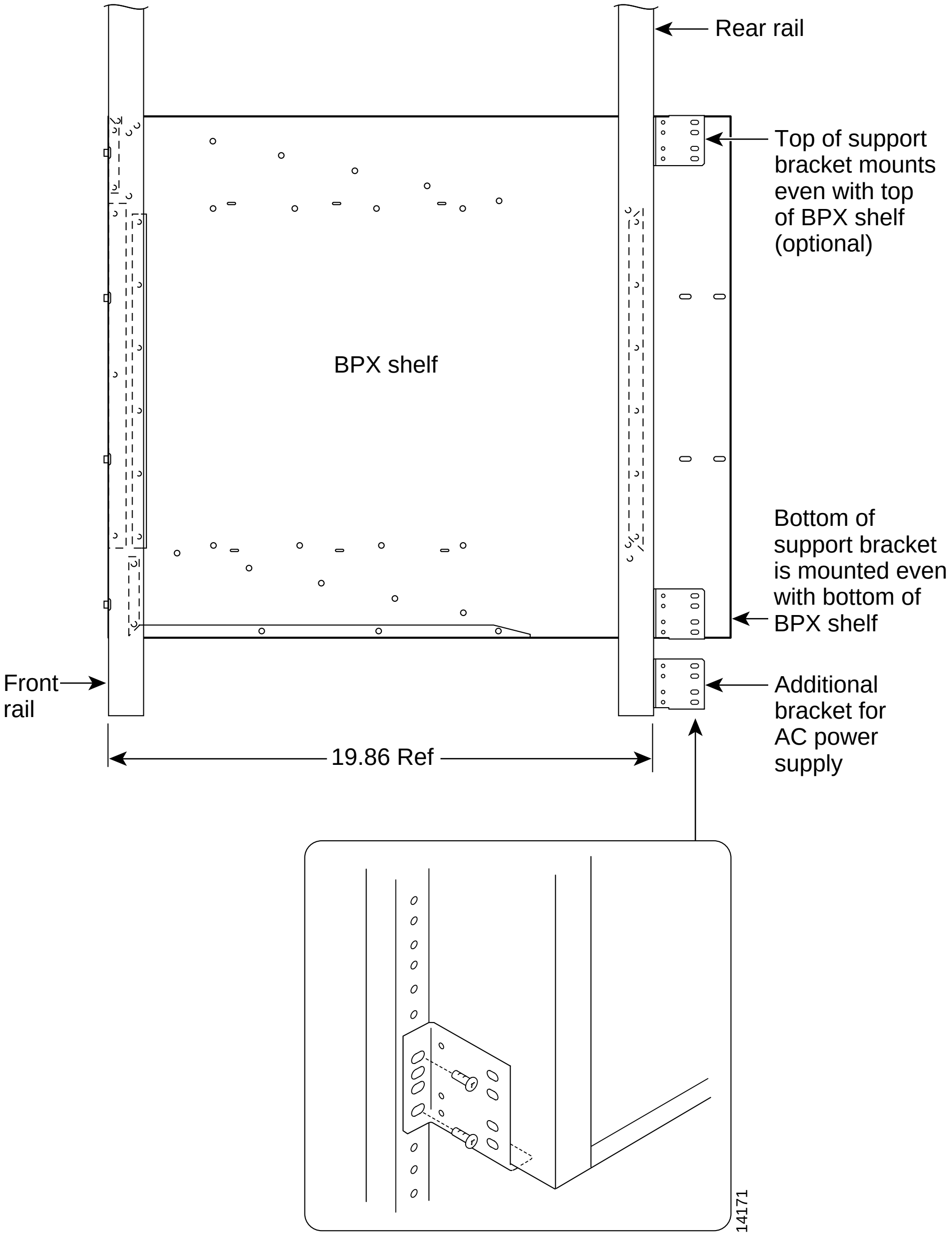

Rear rail
Top of support bracket mounts even with top of BPX shelf (optional)
BPX shelf
Bottom of support bracket is mounted even with bottom of BPX shelf
Front rail
Additional bracket for AC power supply
19.86 Ref
14171

Figure 5-4 Rear Mounting Brackets, with 19.86 Inch Rear Rail Setback (DC Systems)

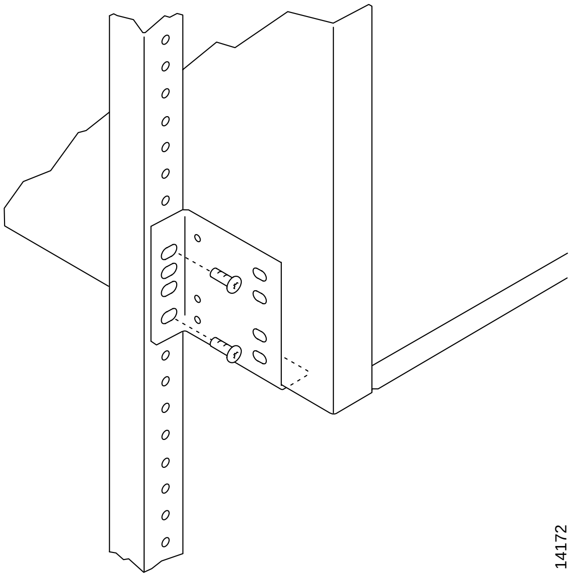
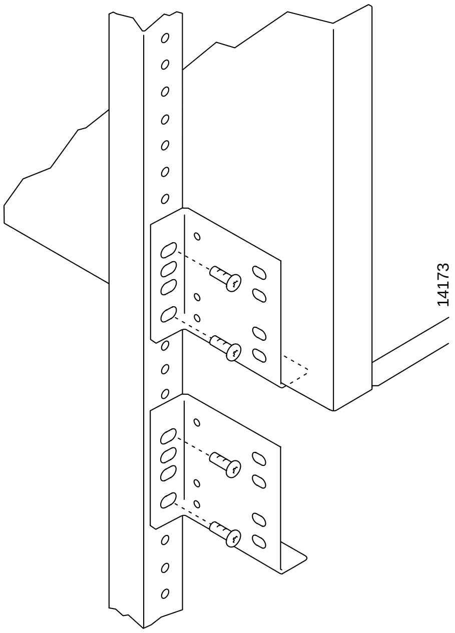


Figure 5-5 Rear Mounting Brackets, 19.86 Inch Rear Rail Setback (AC-Systems)



Installing a 7200 or 7500 Router in a BPX 8650 Cabinet or Rack

The steps in this procedure apply to a 7200 or 7500 Router Label Switch Controller assembly that is being installed 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 as follows:

(a) Place router into router enclosure as shown (see Figure 5-6) with power connector side of router towards hinged front door of router enclosure.

(b) Install power cord along top left side of router and router enclosure.

(c) Mount front hinged door to router enclosure by spreading sides of router enclosure slightly so that holes in each side of the cover engage the pins at the front of the router enclosure.

Note To open router enclosure door, use tabs on top of 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 door.

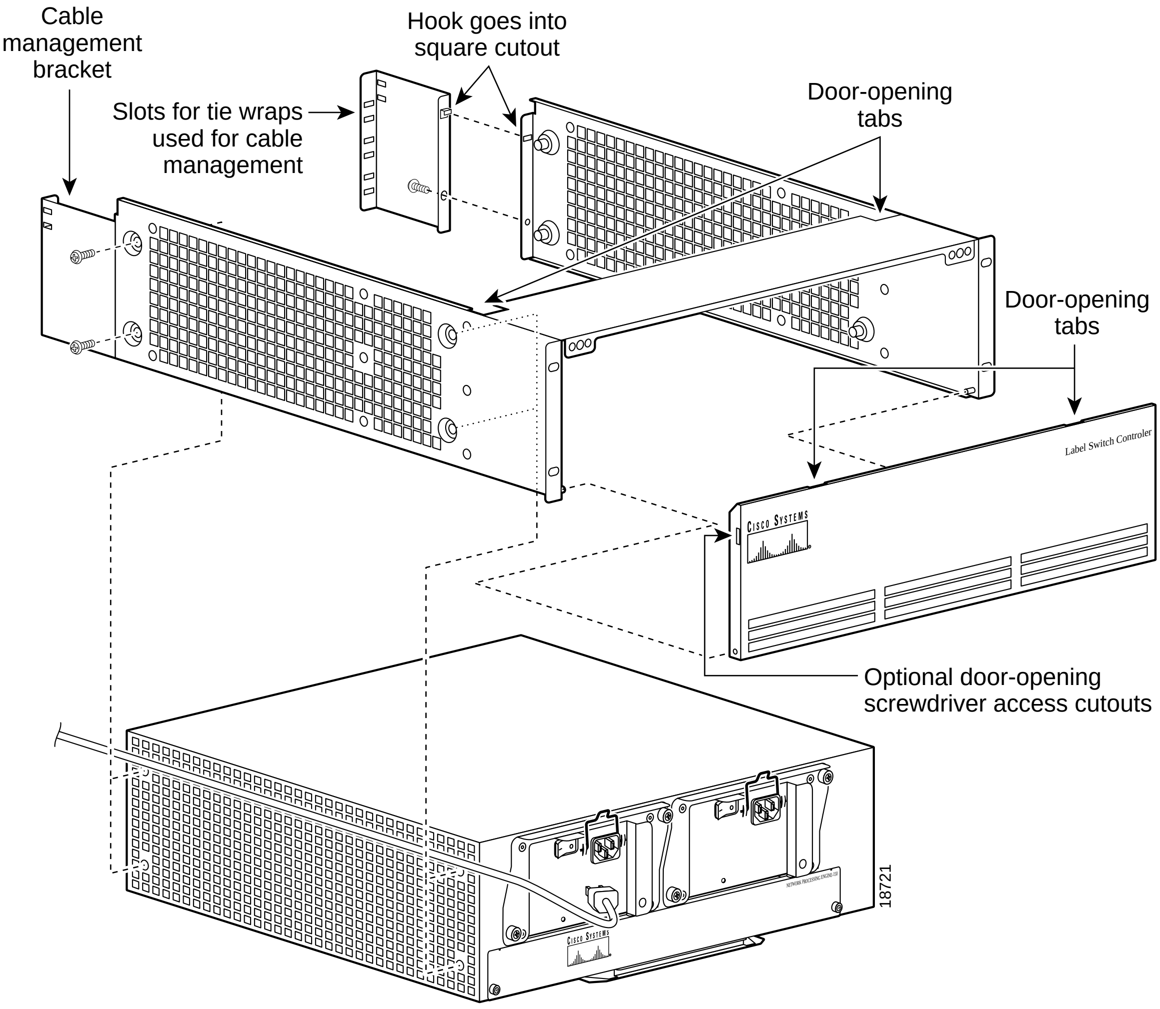
(d) Secure router to router enclosure using four screws on each side.

(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 5-6 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 one of the following:

- To install the router assembly in a BPX 8650 cabinet, proceed to “Installing Router Assembly in a Cisco Cabinet” section on page 9
- 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 10
- 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 11

Figure 5-6 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
Cisco Systems
18721

Installing Router Assembly in a Cisco Cabinet

Install router enclosure assembly in BPX 8650 cabinet as follows (see Figure 5-7):

Step 1 Slide router enclosure assembly into cabinet on top of 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 which supports the router enclosure assembly.

Step 3 Secure front of router assembly to cabinet rails with two screws on each side.

Step 4 Secure router enclosure assembly to cabinet with mounting screws.

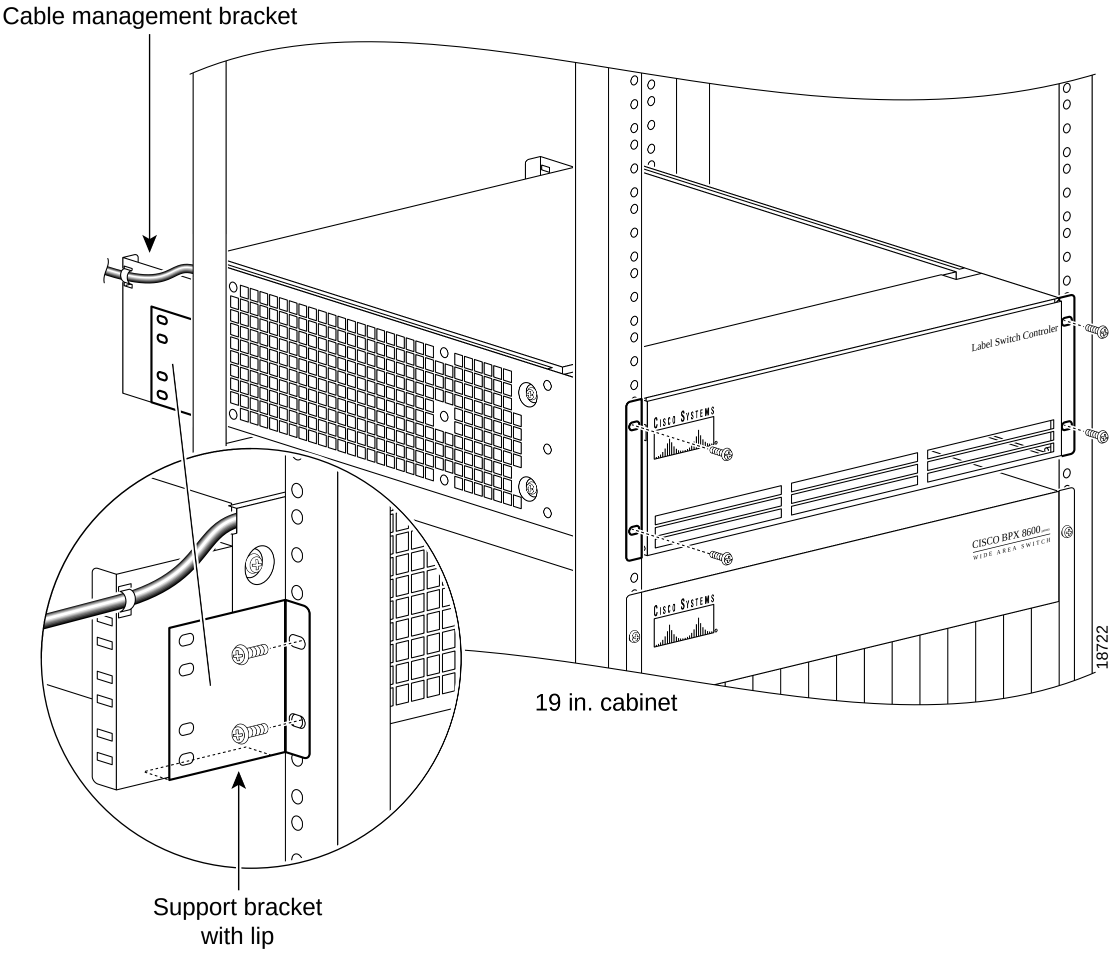
Step 5 Connect power cord to router connector receptacle at front of cabinet, and close the router enclosure assembly door.

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 7, Installation, DC Shelf Initial Setup.

Step 8 If this is an AC powered shelf, proceed to Chapter 8, Installation, AC Shelf Initial Setup.

Figure 5-7 Installing the Router Enclosure Assembly in the Cisco BPX 7650 Cabinet



Installing Router Assembly in a 19-Inch Open Rack

Install router enclosure assembly in BPX 8650 cabinet as follows (see Figure 5-8):

Step 1 Slide router enclosure assembly into cabinet on top of 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 front of router assembly to rack with two screws on each side.

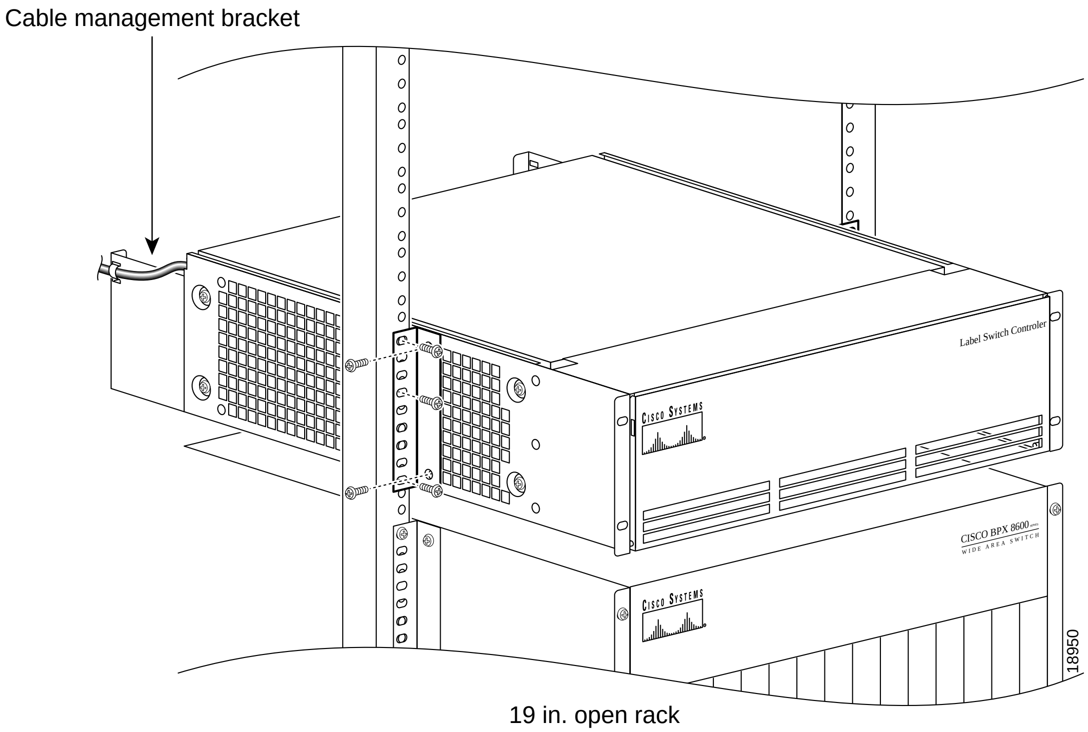
Step 4 Connect power cord to router connector receptacle at front of cabinet, and close the router enclosure assembly door.

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 7, Installation, DC Shelf Initial Setup.

Step 7 If this is an AC powered shelf, proceed to Chapter 8, Installation, AC Shelf Initial Setup.

Figure 5-8 Installing the Router Enclosure Assembly in a 19-inch Open Rack



Installing Router Assembly in a 23-Inch Open Rack

Install router enclosure assembly in BPX 8650 cabinet as follows (see Figure 5-9):

Step 1 Slide router enclosure assembly into cabinet on top of 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 router enclosure assembly into cabinet on top of BPX shelf.

Step 4 Secure front of router assembly to rack with three screws on each side.

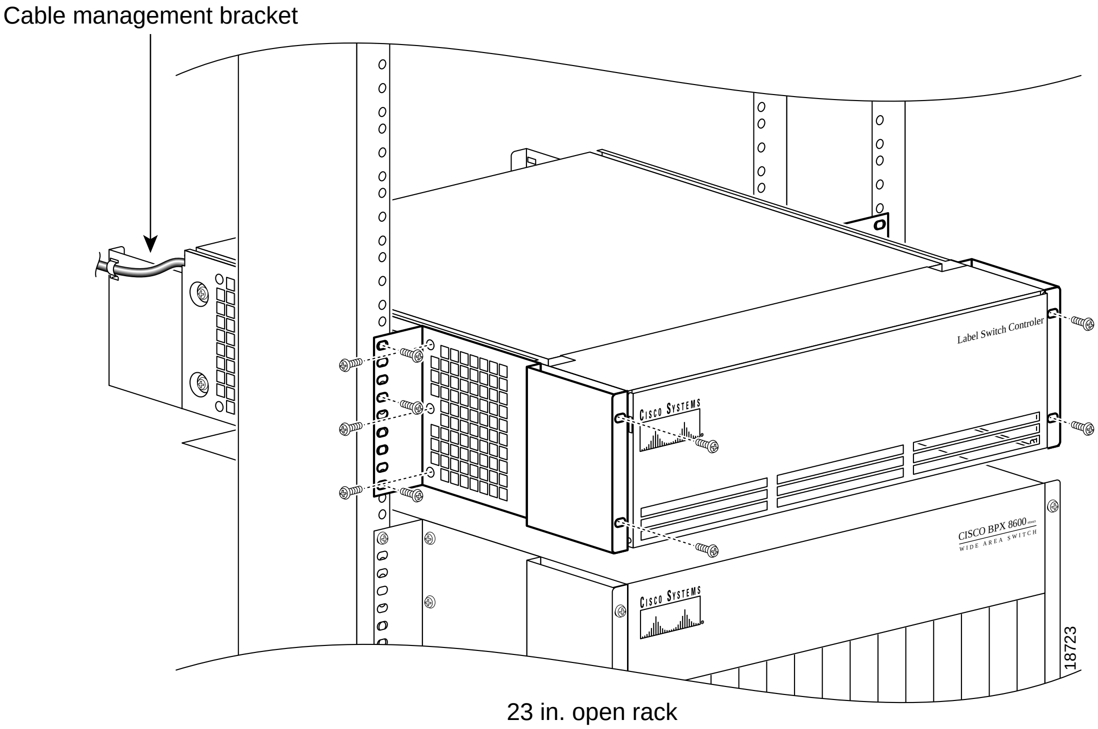
Step 5 Connect power cord to router connector receptacle at front of cabinet, and close the router enclosure assembly door.

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 7, Installation, DC Shelf Initial Setup.

Step 8 If this is an AC powered shelf, proceed to Chapter 8, Installation, AC Shelf Initial Setup.

Figure 5-9 Installing the Router Enclosure Assembly in a 23-inch Open Rack



CHAPTER 6

Installation with 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, the procedures should be completed, in:

— *Chapter 4, Installation, Preliminary*

Installing a BPX Switch, Rear Rail Setback at 30-Inch

The steps in this procedure apply to a BPX switch shelf that is being 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, an AC Power Assembly will be installed below it.

Preliminary Procedure:

Proceed as follows to install the BPX switch shelf, referring to Figure 6-1 through Figure 6-3, and to either Figure 6-4 for DC powered systems or Figure 6-5 for AC powered systems. Figure 6-2 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, lift the pallet tray and BPX switch shelf positioning the slots at the rear of the pallet tray over the locating tabs on the spacer bracket (see Figure 6-1).

Step 2 Slide the BPX switch shelf back over the support brackets and into place.

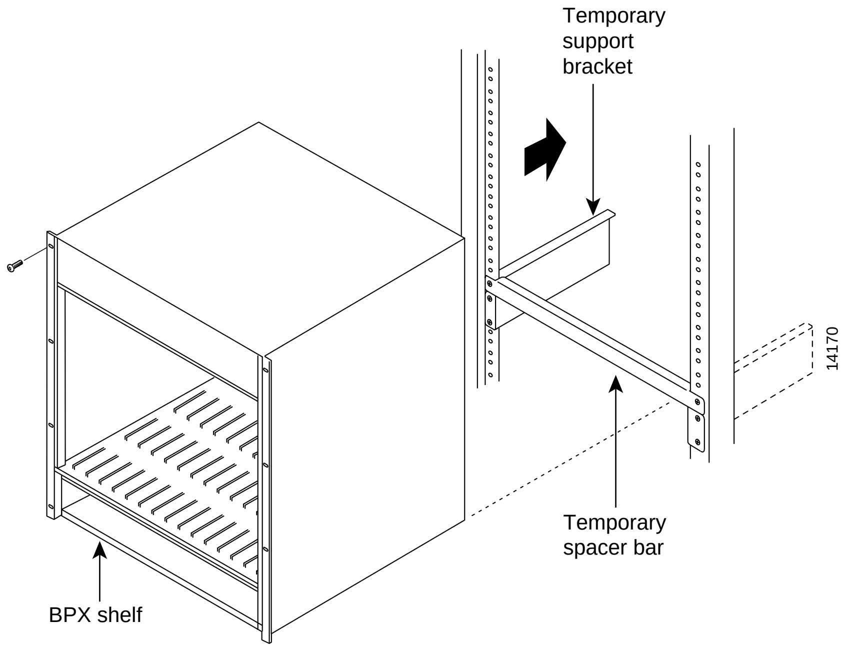
Step 3 Secure the BPX switch shelf to the front rail using 8 each #10-32 screws.

Note European installation may use a size M6 metric screw.

Step 4 Locate the two rear support brackets and adjustable plates in the miscellaneous parts kit.

Step 5 Position the adjustable plates with the tabs in the three punchouts facing up as shown in Figure 6-3.

Figure 6-1 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 may 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 7, Installation, DC Shelf Initial Setup.

Step 14 If this is an AC powered shelf, proceed to Chapter 8, Installation, AC Shelf Initial Setup.

Figure 6-2 BPX Switch with Rear Rail Mounting at Setback of 30 Inches

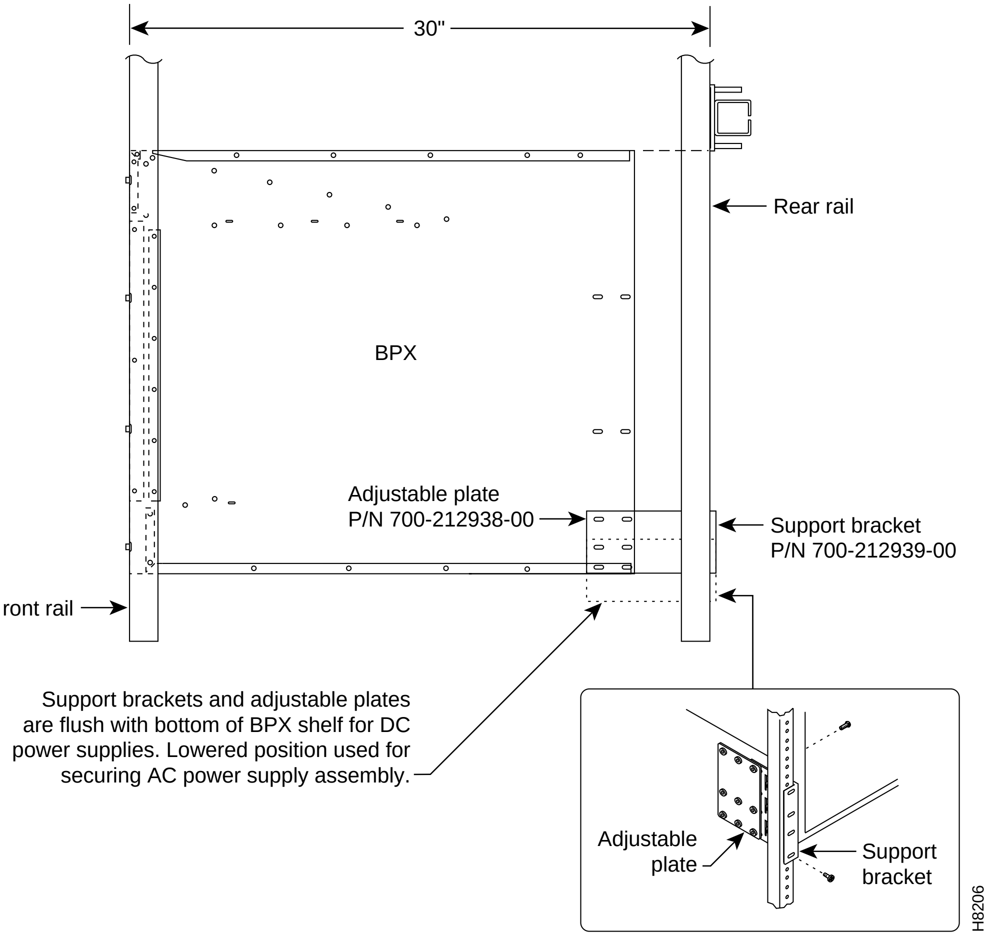

30"
Rear rail
BPX
Adjustable plate
P/N 700-212938-00
Support bracket
P/N 700-212939-00
ront rail
Support brackets and adjustable plates are flush with bottom of BPX shelf for DC power supplies. Lowered position used for securing AC power supply assembly.
Adjustable plate
Support bracket
H8206

Figure 6-3 Rear Mounting Brackets, Detail

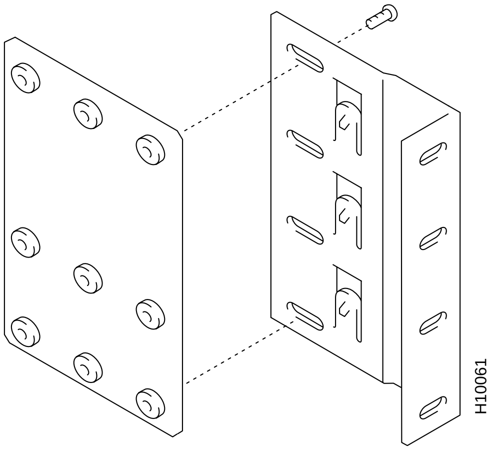


Figure 6-4 Rear Mounting Brackets, with 30 Inch Rear Rail Setback (DC Systems)

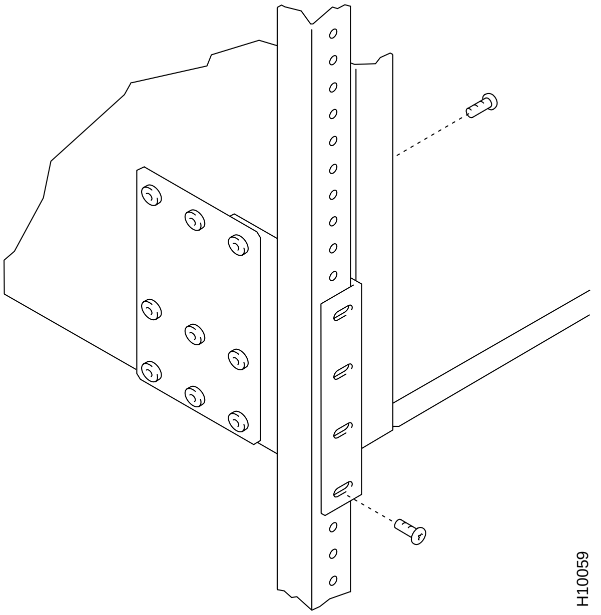
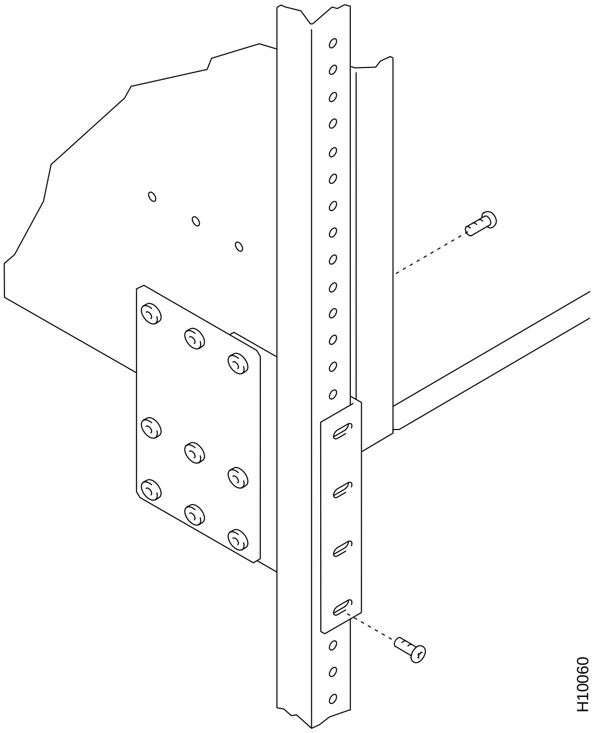


Figure 6-5 Rear Mounting Brackets, 30 Inch Rear Rail Setback (AC-Powered Systems)



Installation, DC Shelf Initial Setup

This chapter describes how to make the DC power connections.

Before proceeding to this chapter, the procedures should be completed, in either:

— Chapter 5, Installation with Cisco Cabinets including 7000 Series Routers

or

— Chapter 6, Installation with Customer Cabinet

This chapter contains the following sections:

- DC Power Input Connections
- Card Slot Fuses
- Fan Power Fuses

DC Power Input Connections

There are two ways to configure a DC-powered BPX switch as follows:

- Single DC Power Entry Module, single power feed.
- Dual DC Power Entry Module, dual power feed.

For DC systems, the wiring is connected from a -48 VDC power source to one or two DC Power Entry Modules (see Figure 7-1). This wiring is provided by the installer. A metallic conduit box that meets all electrical codes for attaching electrical conduit is factory-installed Figure 7-2. A simple plastic cover is also enclosed for customers who do not require conduit protection for the input power leads Figure 7-3. 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 can 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 7-2.) 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.

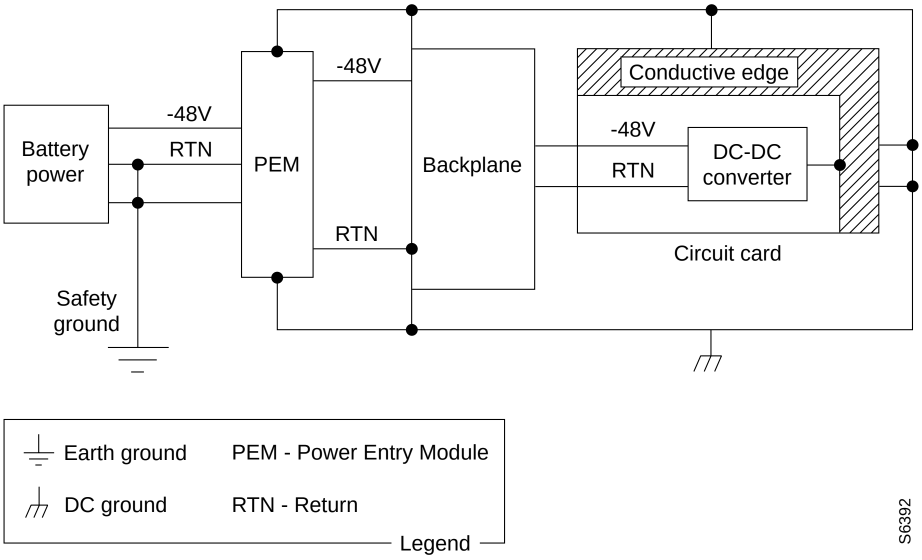
Step 3 If conduit is not required, remove the conduit box by removing the two screws, one above the terminal block and one below it.

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 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 7-1, Figure 7-2 and Figure 7-3.) 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 7-1 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 7-2 and Figure 7-3.)

Step 8 Proceed to Chapter 9, Finishing the Installation and Power-Up.

Figure 7-2 DC Power Connections—With Conduit Box

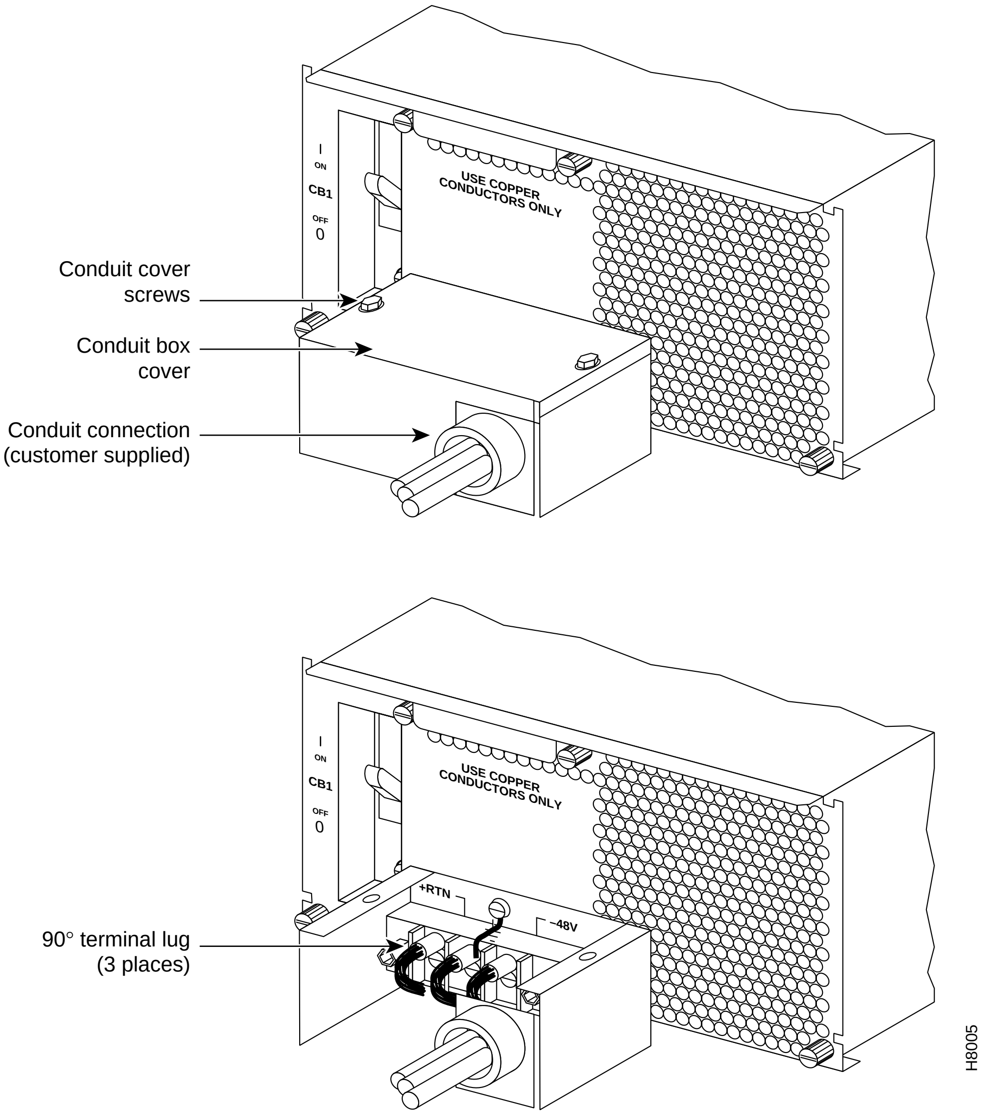
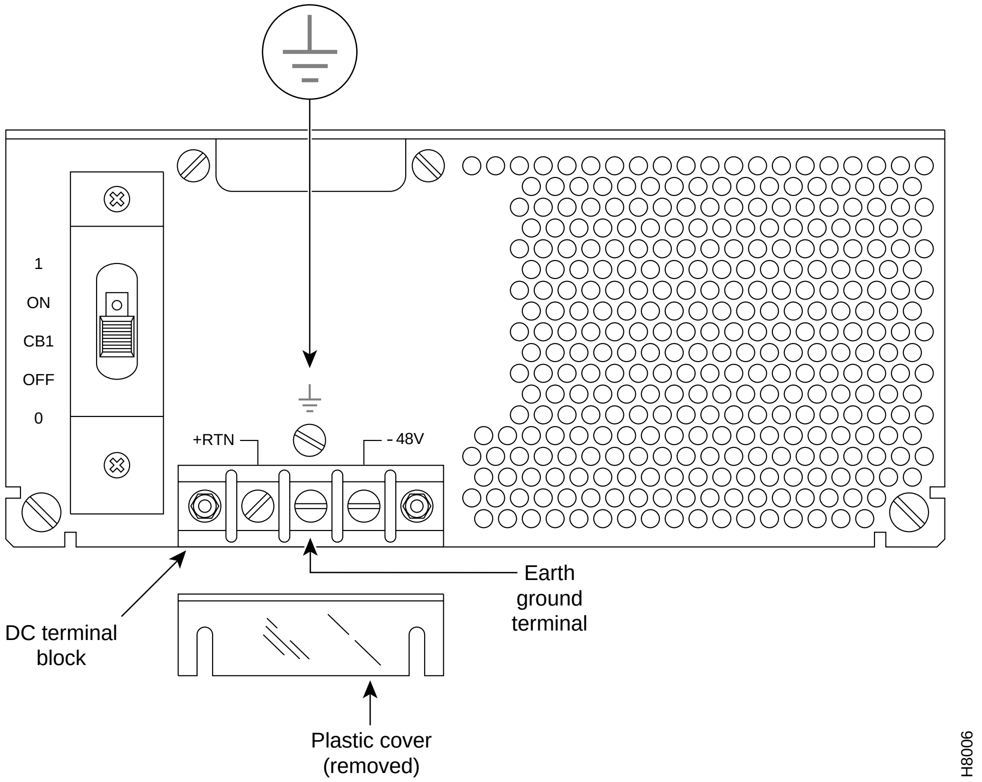

I
ON
CB1
OFF
0
USE COPPER CONDUCTORS ONLY
Conduit cover screws
Conduit box cover
Conduit connection (customer supplied)
I
ON
CB1
OFF
0
USE COPPER CONDUCTORS ONLY
+RTN
–48V
90° terminal lug (3 places)
H8005

Figure 7-3 DC Power Connections—Without Conduit Box



Card Slot Fuses

Fuses for each card slot have been added to the backplane of later versions 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.

Refer to the *Cisco BPX 8600 Series Reference* document, *Repair and Replacement* chapter, for instructions on replacement of these fuses, and 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 only be replaced 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 Refer to the *Cisco BPX 8600 Series Reference* document, *Repair and Replacement* chapter, 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 8

Installation, AC Shelf Initial Setup

This chapter explains how to install the AC power supply tray, power supplies, and make AC power connections.

Before proceeding to this chapter, the procedures should be completed, in either:

— Chapter 5, Installation with Cisco Cabinets including 7000 Series Routers

or

— Chapter 6, Installation with Customer Cabinet

This chapter contains the following sections:

- Installing an AC Power Supply Tray
- Installing an AC Power Supply
- AC Power Input Connections
- Card Slot Fuses
- Fan Power Fuses

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 and are installed 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 proceed as follows:

Step 1 Use two screws to attach each of two temporary support brackets and a temporary spacer bar to the rack (see Figure 8-1 and Figure 8-2).

Step 2 Locate the small access hole in the top center of the front Air Intake Grille on the Power Supply Tray (see Figure 8-3).

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 8-1 Temporary Spacer Bracket and Support Bracket Installation

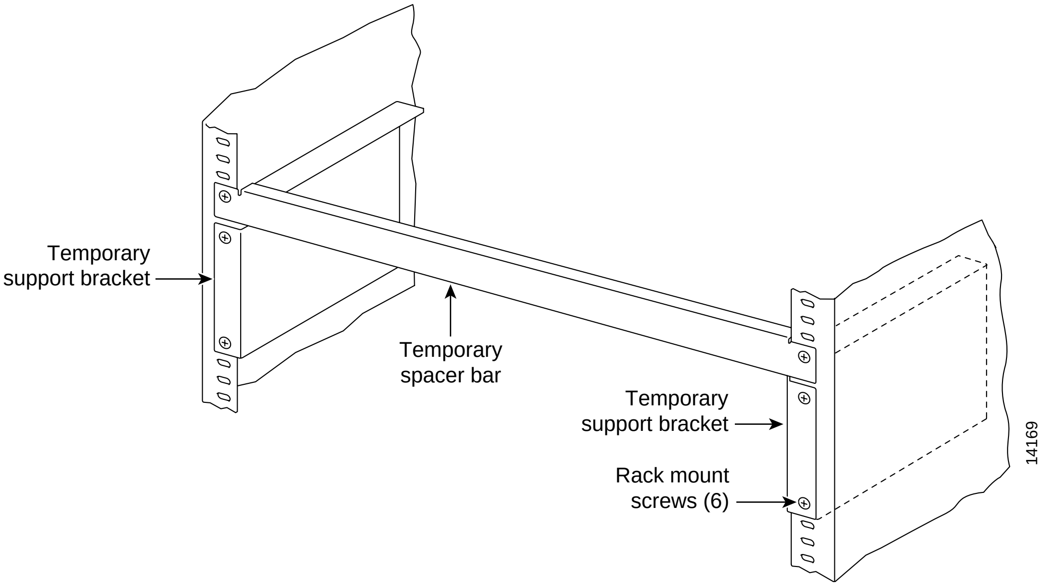


Figure 8-2 Power Supply Tray aligned with Temporary Support Brackets and Bar

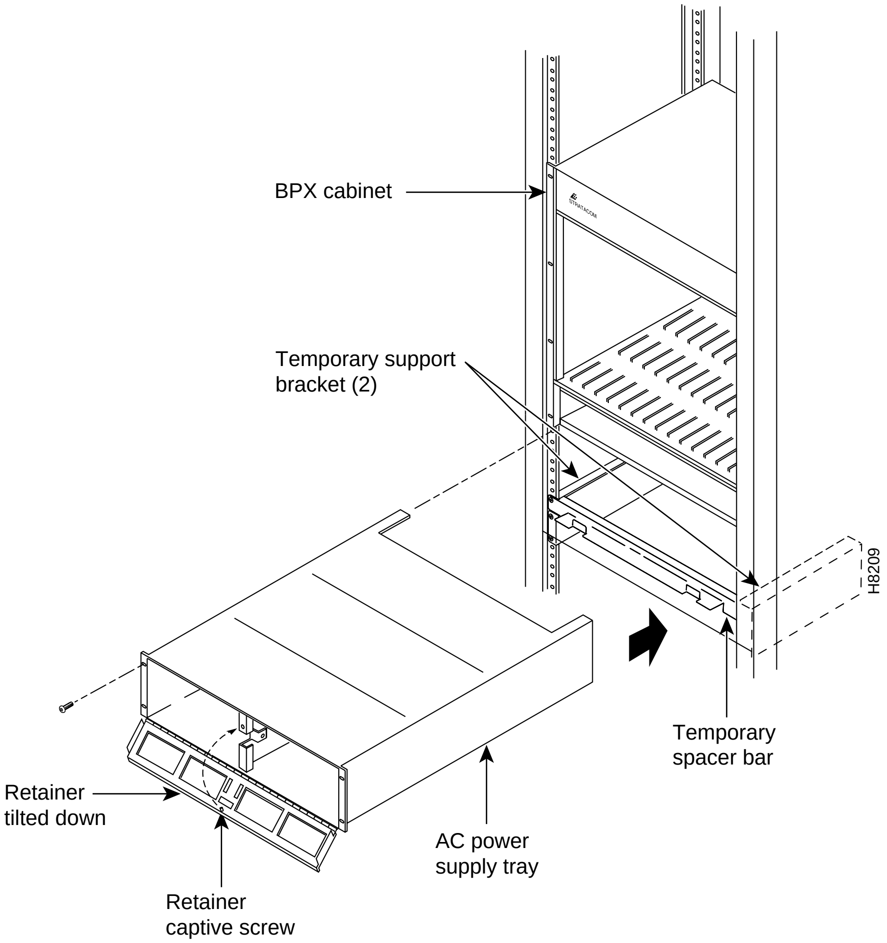
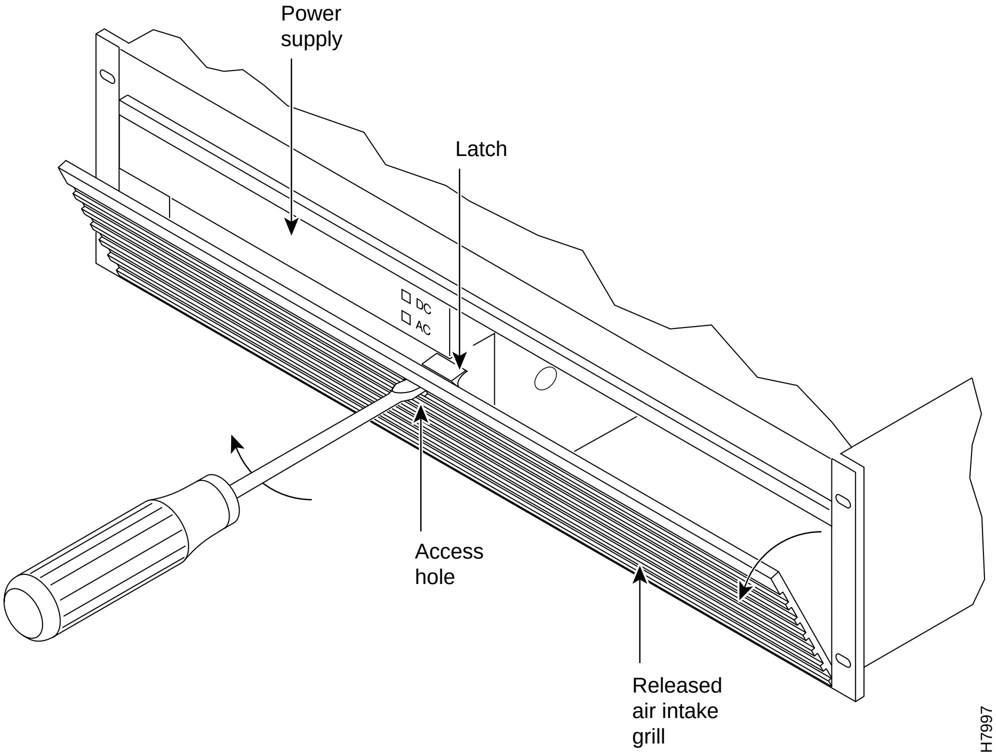


Figure 8-3 Removing an Air Intake Grille



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 8-2). If cables are attached, use 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. There should be 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 8-4 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 8-5 shows the bracket configuration only; the power supply tray position is the same as shown for in Figure 8-4.

Figure 8-4 Securing AC Power Supply Tray, 30-Inch Rail Setback

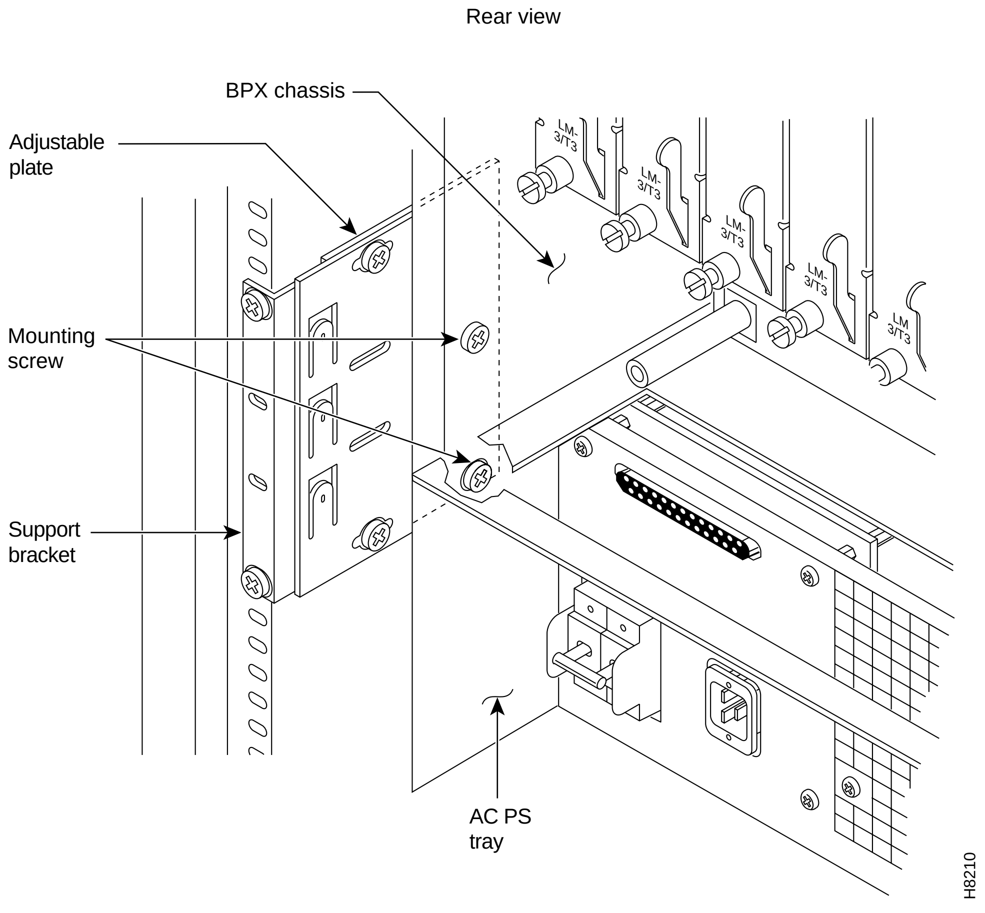
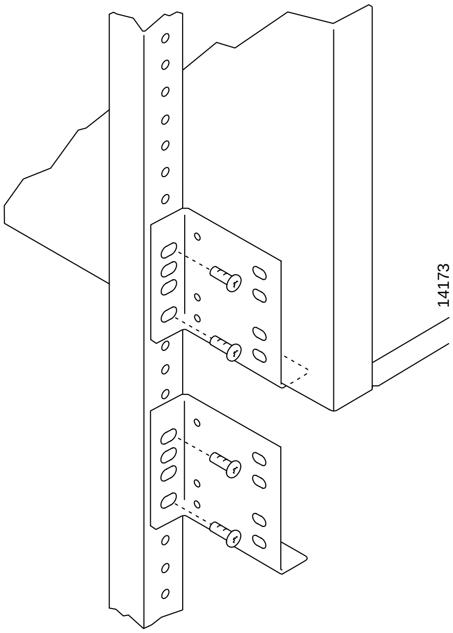


Figure 8-5 Securing an AC Power Supply Tray, 19.86 inch Rear Rail Setback

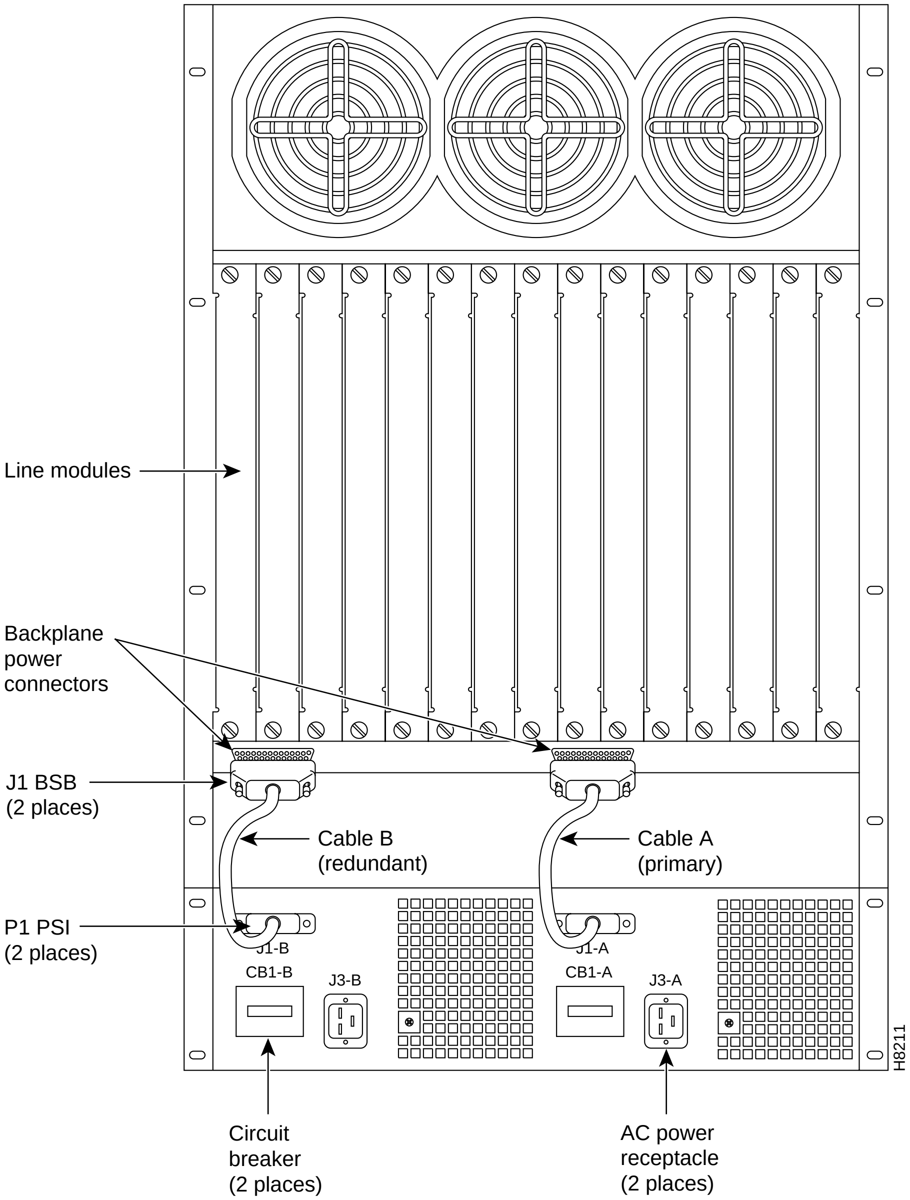


Step 9 Connect and secure a power supply interconnect cable (Cable A in Figure 8-6) between the primary AC Power Supply and the BPX switch backplane power connector.

Step 10 Connect and secure a second power supply interconnect cable (Cable B in Figure 8-6) 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 8-6 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, and mounting frame. The AC Power Supply is 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.

Proceed as follows to install an AC Power Supply in the Power Supply Tray:

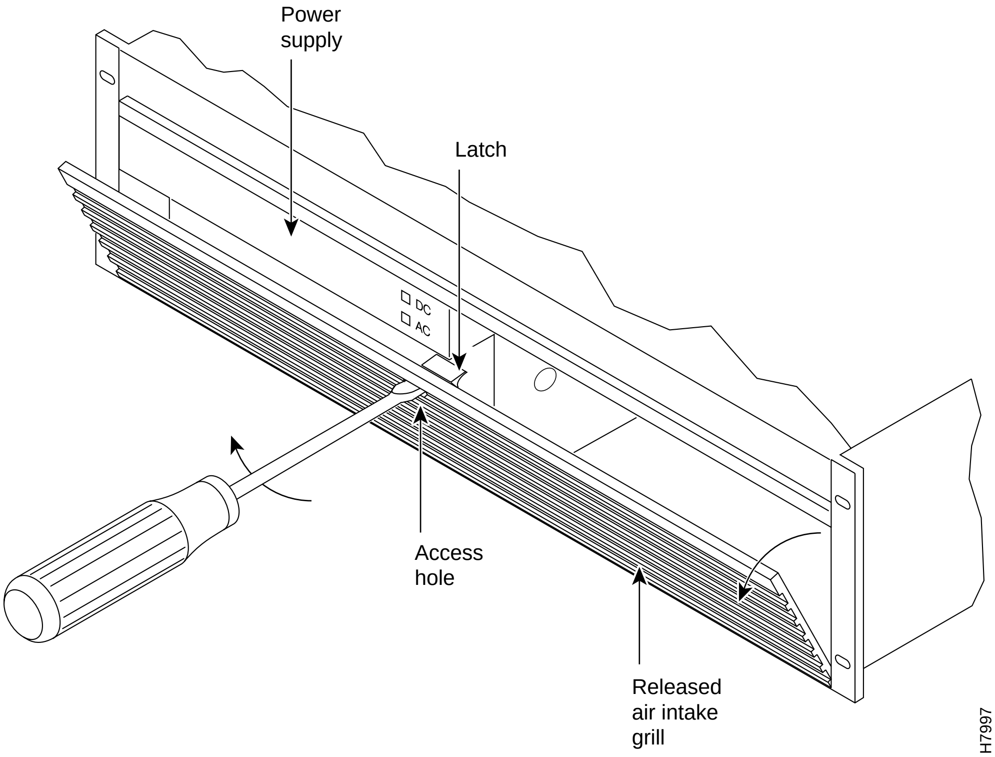
Step 1 First install the Power Supply Tray in a rack (see “Installing an AC Power Supply Tray” section).

Step 2 Set the circuit breaker(s) 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 8-7).

Figure 8-7 Removing an Air Intake Grille

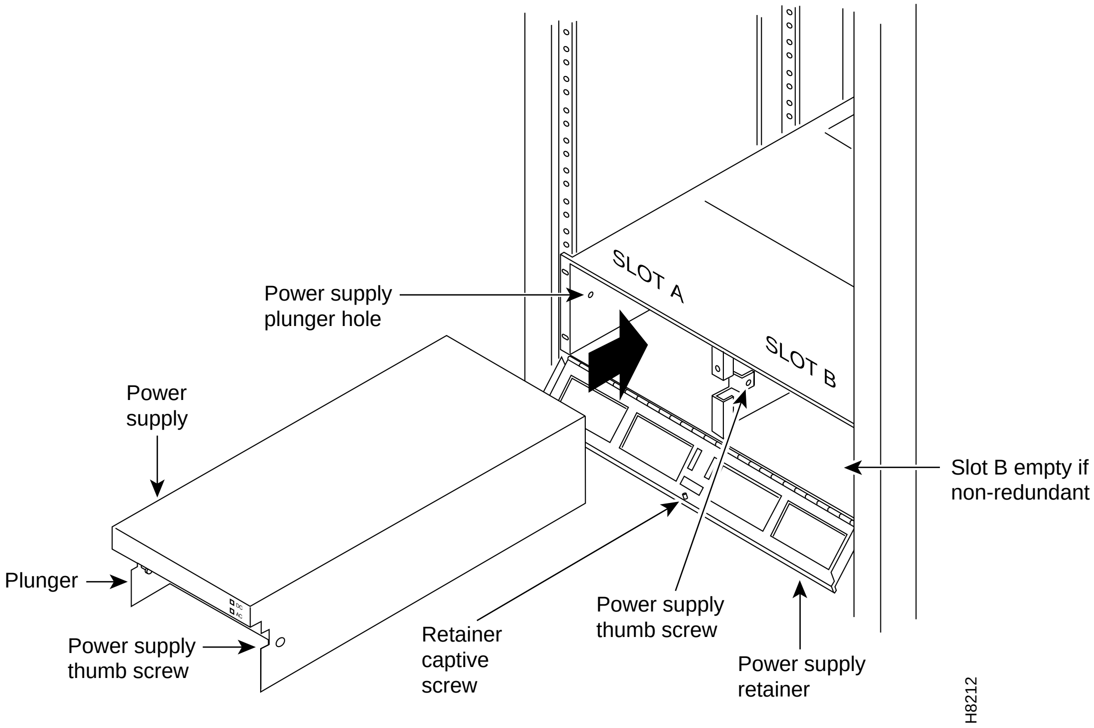


Step 4 Insert a small slotted blade screwdriver (0.20/0.25 inch blade width) into the access hole until it stops, approximately 1 inch (2.5 cm).

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 8-8).

Figure 8-8 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 8-8).

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 as follows:

- Single power supply, single AC power feed.
- Dual power supplies, single AC power feed.
- Dual power supplies, dual AC power feed.

An 8 ft. (3 m.) power cord is supplied with each AC Power Supply Assembly. To make AC power connections to the BPX switch:

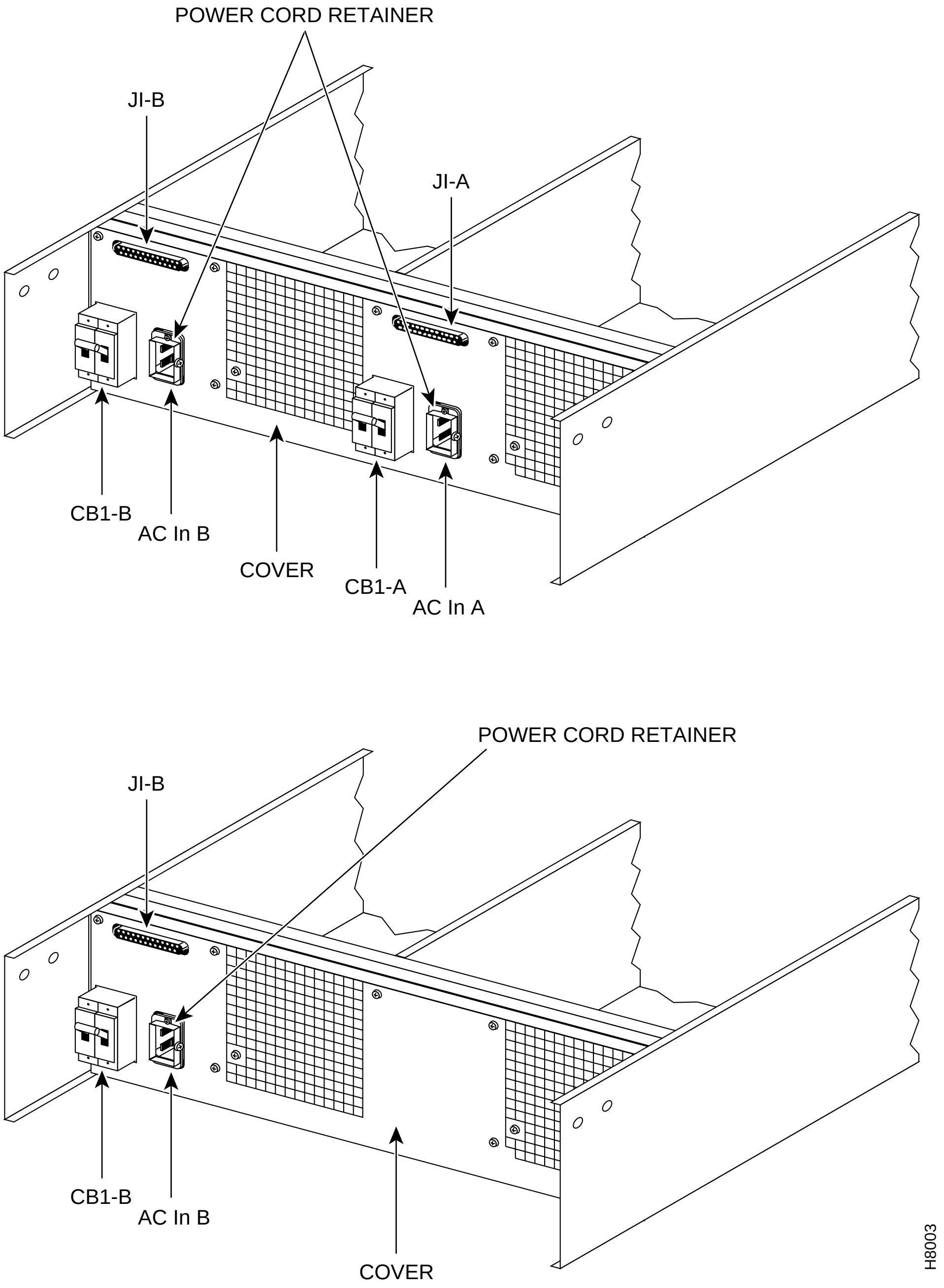
Step 1 Plug the power cord(s) into the applicable IEC connector(s) as shown in Figure 8-9 and tighten the cord retainers. A separate power cord connects to each of one or two IEC connectors depending on the version of power supply shelf provided.

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 has been changed from 15 A to 20 A to provide improved system availability for installations with a single line cord and (N+1) power supplies.

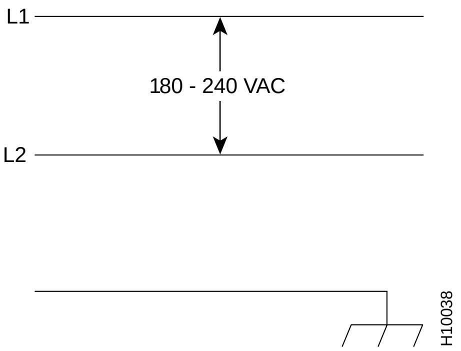
Step 3 For the dual power feed version, plug each power cord into receptacles on separate building circuits to provide protection against a power feed failure. Each building circuit should be protected with a 20A circuit breaker.

Figure 8-9 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 8-10).

Figure 8-10 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, etc. 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 (e.g., 115 VAC for domestic US use).

Step 6 Proceed to Chapter 9, Finishing the Installation and Power-Up.

Card Slot Fuses

Fuses for each card slot have been added to the backplane of later versions 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.

Refer to the *Cisco BPX 8600 Series Reference* document, *Repair and Replacement* chapter, 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 only be replaced 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 Refer to the *Cisco BPX 8600 Series Reference* document, *Repair and Replacement* chapter, 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 9

Finishing the Installation and Power-Up

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.

Before proceeding to this chapter, the procedures should be completed, in either:

— Chapter 7, Installation, DC Shelf Initial Setup, or

— Chapter 8, Installation, AC Shelf Initial Setup.

This chapter contains the following sections:

- Installing the BPX Switch Cards
- Verifying 9.6 or 19.2 Gbps Backplane
- Upgrading to BCC-4V Cards
- Installation of APS Redundant Backplane and Backcards
- Making T3 or E3 Connections
- Making an ASI-155 or BNI-155 Connection
- 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
- Attaching Peripherals
- LAN Connection for the Network Management Station
- Connecting a Network Printer to the BPX Switch
- Connecting Modems
- Making External Clock Connections
- Initial Power-Up of the BPX Switch
- Provisioning the BPX Switch
- Configuration

Installing the BPX Switch 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 9-1 and Figure 9-2, respectively. The configuration rules for the BPX switch are summarized as follows.

- For non-redundant nodes, either a Broadband Controller Card BCC-4V, BCC-3-32M, BCC-3-64M, or BCC-32 is used in front slot number 7.
- For non-redundant nodes, a BCC-3-BC backcard must be used in back slot number 7 with a BCC-4V, BCC-3-32M, or BCC-3-64M front card, or a BCC15-BC must be used in back slot number 7 with a BCC-32 front card.
- For redundant nodes, two Broadband Controller Cards, a pair of BCC-4Vs, BCC-3-32Ms, BCC-3-64Ms, or BCC-32s are used in front slot numbers 7 and 8.
- For redundant nodes, BCC-3-BC backcards must be used in back slot numbers 7 and 8 with BCC-4V, BCC-3-32M, or BCC-3-64M front cards, or BCC15-BC backcards must be used in back slot numbers 7 and 8 with BCC-32 front cards.

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, i.e., replacing a failed controller card. Contact Customer Service for assistance.

- ASM in front slot number 15.
- LM -ASM in back slot number 15.
- BNI-3T3, BNI-3E3, BNI-155 in any other front slot than 7, 8, or 15.
- LM -3T3, LM-3E3, 2OC3-SMF, 2OC3-MMF in all back slots with a BNI in the corresponding front slot.
- ASI-2T3, ASI-2E3, ASI-155 in any other front slot than 7, 8, or 15.
- LM -2T3, LM-2E3, 2OC3-SMF, 2OC3-MMF in all back slots with an ASI in the front other than 7, 8, or 15.

Figure 9-1 BPX Shelf (front view)

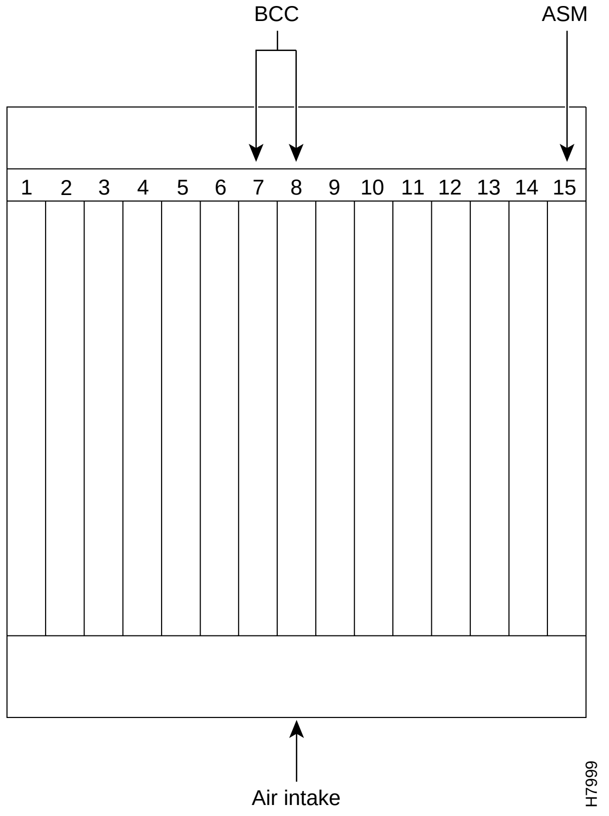
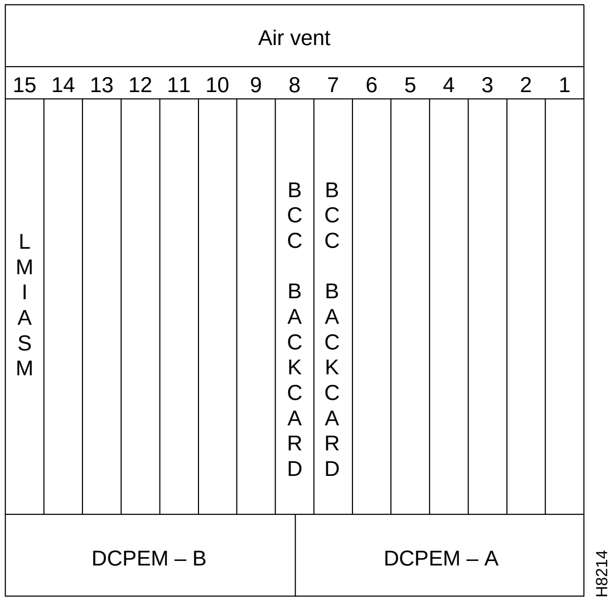


Figure 9-2 BPX Shelf (rear view, DC shelf shown)



Installing Front 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.

Caution Blank Front Card and Rear Face Plates must be used 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, some of them may need to be replaced 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.

Proceed as follows to remove/install a front card.

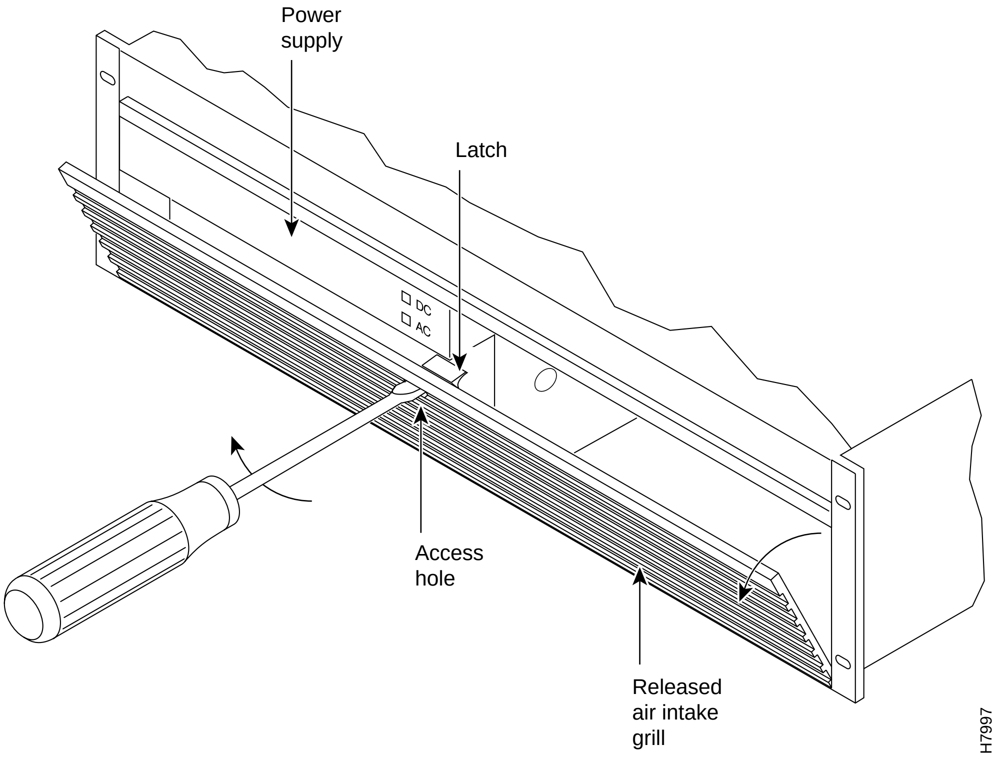
Caution Before any card is installed, always examine the chassis backplane and card cage guides for any signs of loose or misplaced EMI gasketing. Examine the backplane connectors for bent or damaged connection or pre-power pins.

Step 1 Turn off all power to the BPX switch.

Note While 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 as the cards are hot pluggable replaceable.

Step 2 Locate the small access hole in the top center of the front Air Intake Grille below the card slots (see Figure 9-3 for location).

Figure 9-3 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.

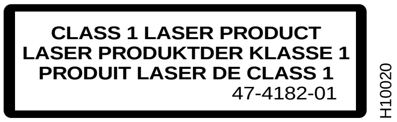
Note The card should slide in with slight friction on the adjacent board’s EMI gaskets. Investigate any binding. Do not use excessive force.

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 9-4.

Figure 9-4 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).

Proceed as follows to install back cards:

Step 1 Locate the card slot for the card to remove or install.

Step 2 For existing installations, remove any cable(s) that may be attached and tag 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 with a slotted blade screwdriver (see Figure 9-5).

Step 4 Lift the extractor handles at the top and bottom, and slide out the line module.

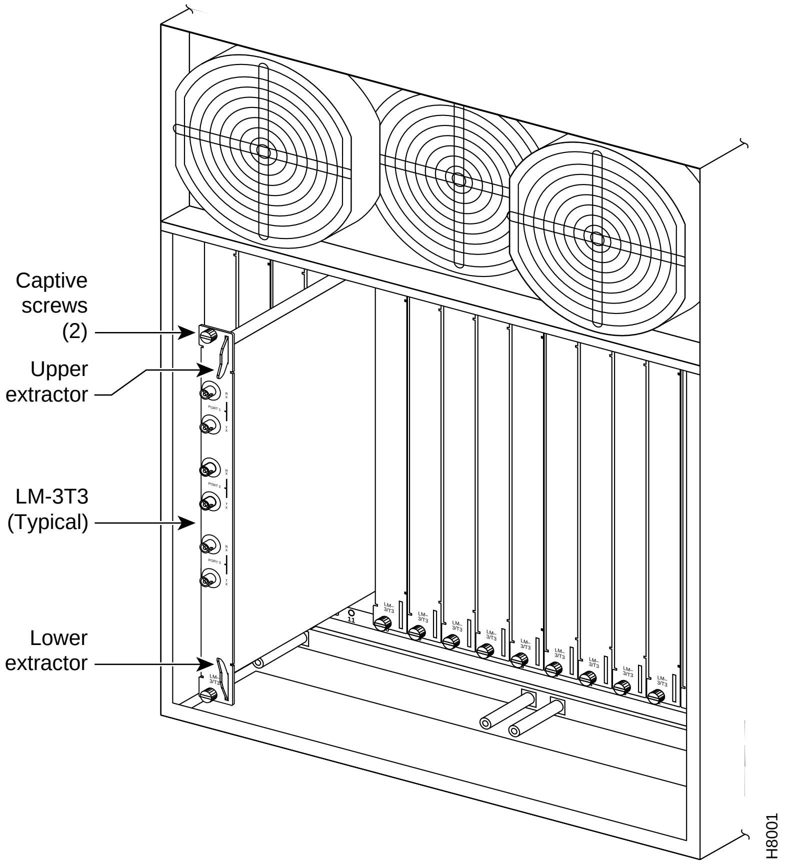
Step 5 To re-insert the line module, locate the corner edges of the card into the appropriate guide slots at the top and bottom of the card cage. Gently slide the card in all the way to the rear of the slot and push to seat the card in the connector.

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 9-5 Installing a Back Card



Verifying 9.6 or 19.2 Gbps Backplane

In order to operate the BPX Switch at 19.2 Gbps the following is required:

- 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.

The 19.2 backplane can be visually identified by the small white card slot fuses at the bottom rear of the backplane. These 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. This can be verified 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 the **cnfbpnv** command may be used to program the NOVRAM as follows:

Step 1 Enter **cnfbpnv**, and the response should be:

```
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** in order for the change to 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 Customer Service.

Upgrading to BCC-4 Cards

The backplane must be a 19.2 Gbps backplane. Refer to the previous section, Verifying 9.6 or 19.2 Gbps Backplane on page 7. To upgrade to BCC-4 cards which support the 19.2 Gbps performance of the BXM cards, proceed as follows:

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 only permitted while the standby updates to the new BCC are in progress, which will take less than one hour.

The time during which this mixture of BCC types exists must be kept to a minimum, by immediately replacing the second old type BCC with the matching one of the new type.

Installation of APS Redundant Frame Assembly and Backcards

The following procedures provide installation instructions for the SONET Automatic Protection System (APS) Redundant Frame Assemblies and backcards which may be used to provide line and card redundancy for BXM OC-3 and OC-12 cards.

The following APS protocols that are supported by the BXM are listed in Table 9-1 and shown in Figure 9-6 and Figure 9-7.

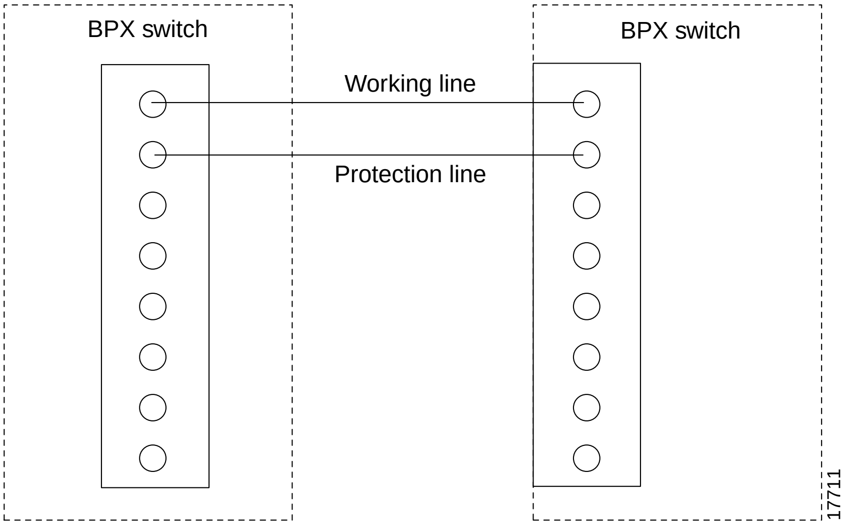
Table 9-1 BXM SONET APS

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 9-6 APS 1:1 Redundancy



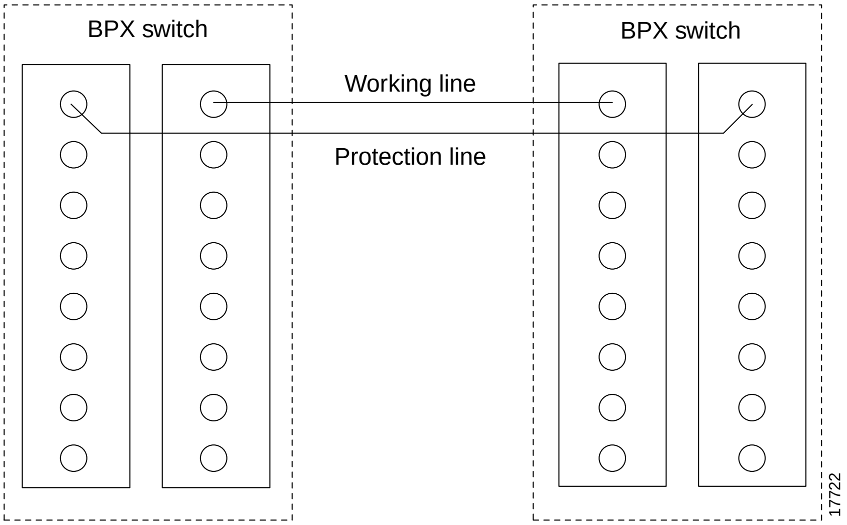
APS 1+1 Redundancy Installation

APS 1+1 redundancy, which provides both card and line redundancy 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 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 etc.).

Figure 9-7 APS 1+1 Redundancy



Proceed to install APS Redundant Frame Assembly and backcards as follows:

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 9-8).

Step 3 Carefully slide APS Redundancy Frame Assembly and APS cards into selected side-by-side slots at the back of the BPX shelf (dee Figure 9-9). Slide the APS Redundancy Frame Assembly and cards into the BPX shelf until snug against the BPX midplane (see Figure 9-10).

Step 4 Going back and forth between the screws, gradually tighten retaining screws at top and bottom of the APS backcards until they are secure.

Figure 9-8 APS Redundant Frame Assembly

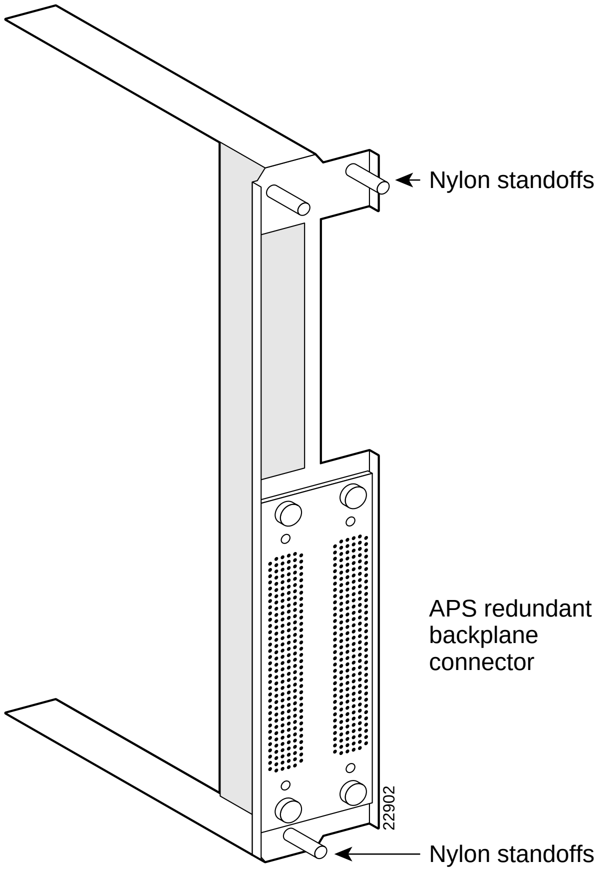


Figure 9-9 BPX Shelf, Rear View

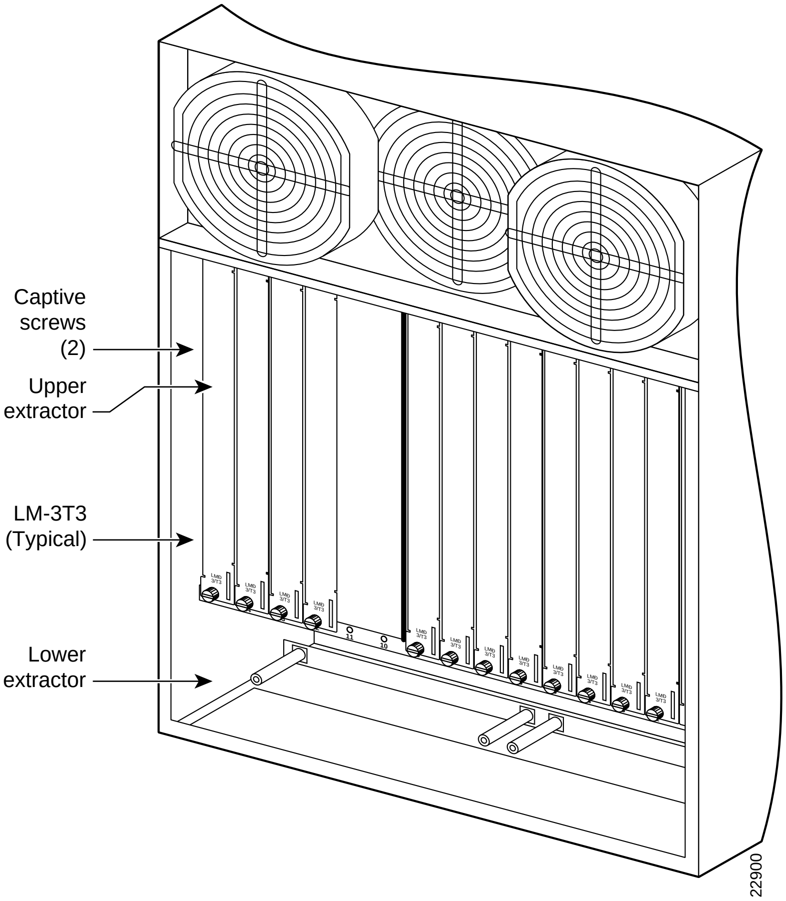
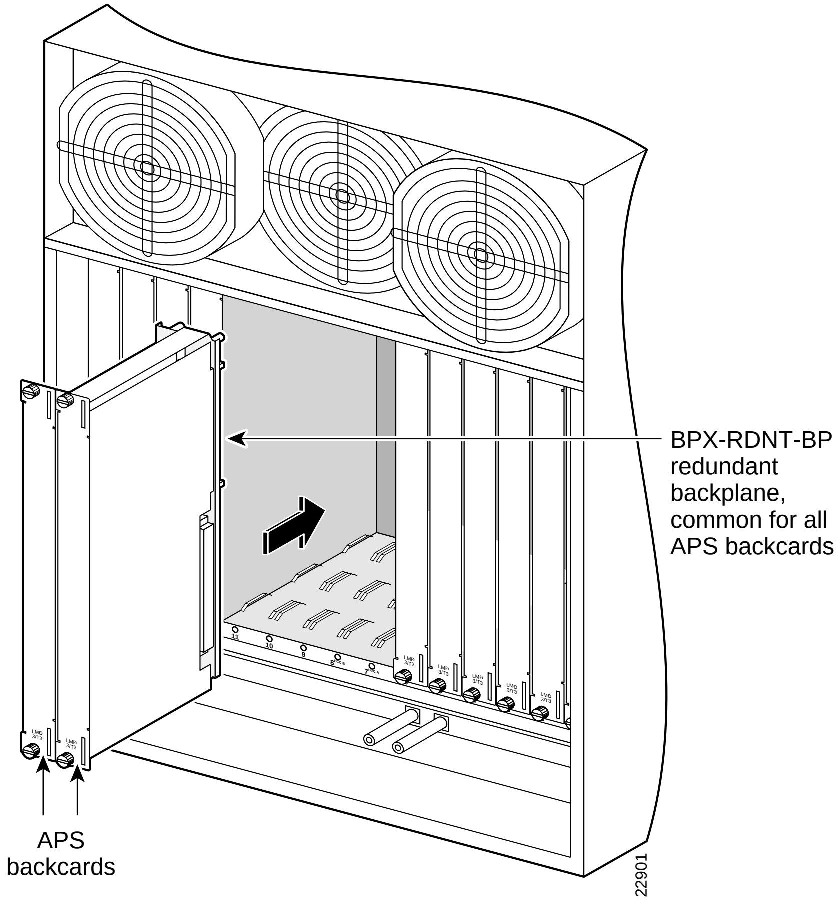


Figure 9-10 Installing APS Redundant Frame Assembly and Backcards into Place



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 (ASI backcard) provides two ports with a BNC connector each for the XMT line output and for the RCV line input. Make the T3/E3 connections to each port as follows.

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 tie-downs inside the cabinet to hold cabling in place. Pull them 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 9-11.

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 are used for each trunk or line. You'll need the 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 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 9-12). 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 9-11 Connecting T3 Cables to BPX LM-T3 (BNI T3 backcard)

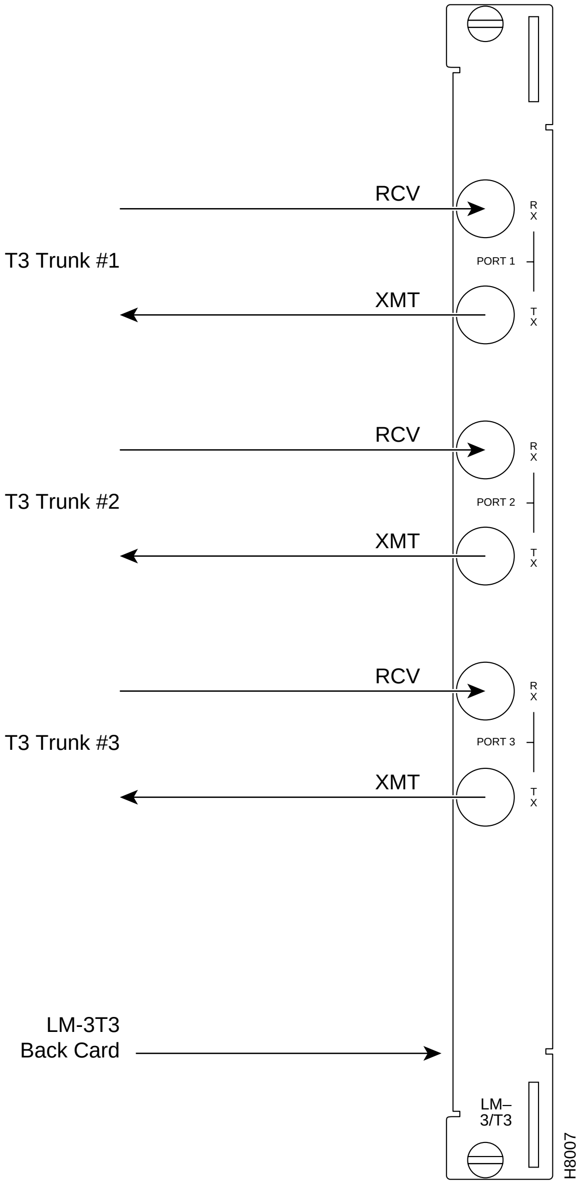
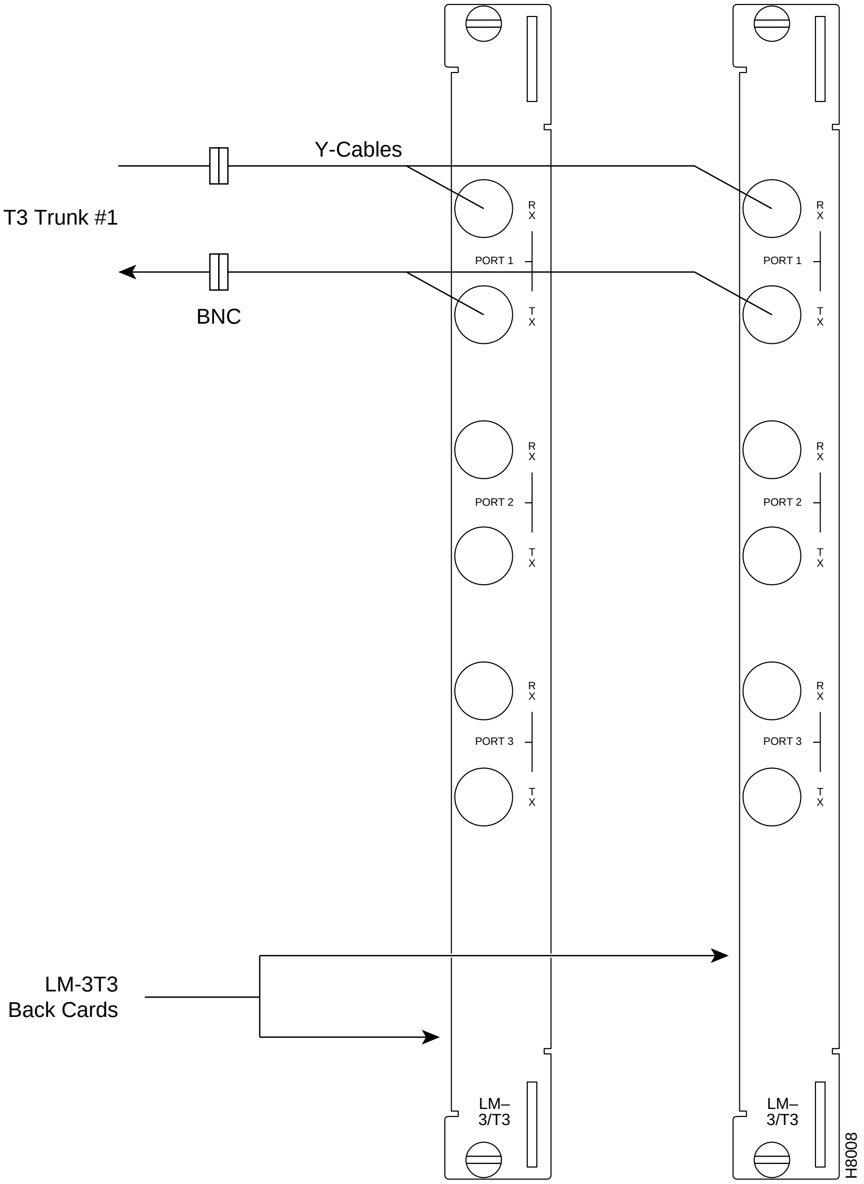


Figure 9-12 Connecting Y-Cable Adapters to a T3 Port



Making an ASI-155 or BNI-155 Connection

Each OC-3 line module provides two ports with both a transmit and receiver connector for each port. The following applies to the 2OC3-SMF and 2OC3-MMF backcards, except that Y-Cabling redundancy is supported only for the 2OC3-SMF card. Make connections as follows:

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 OC-3 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 9-13.

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. The following applies to OC-3 and OC-12 backcards, except that Y-Cabling redundancy is supported only for the SMF cards. Make connections as follows:

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.

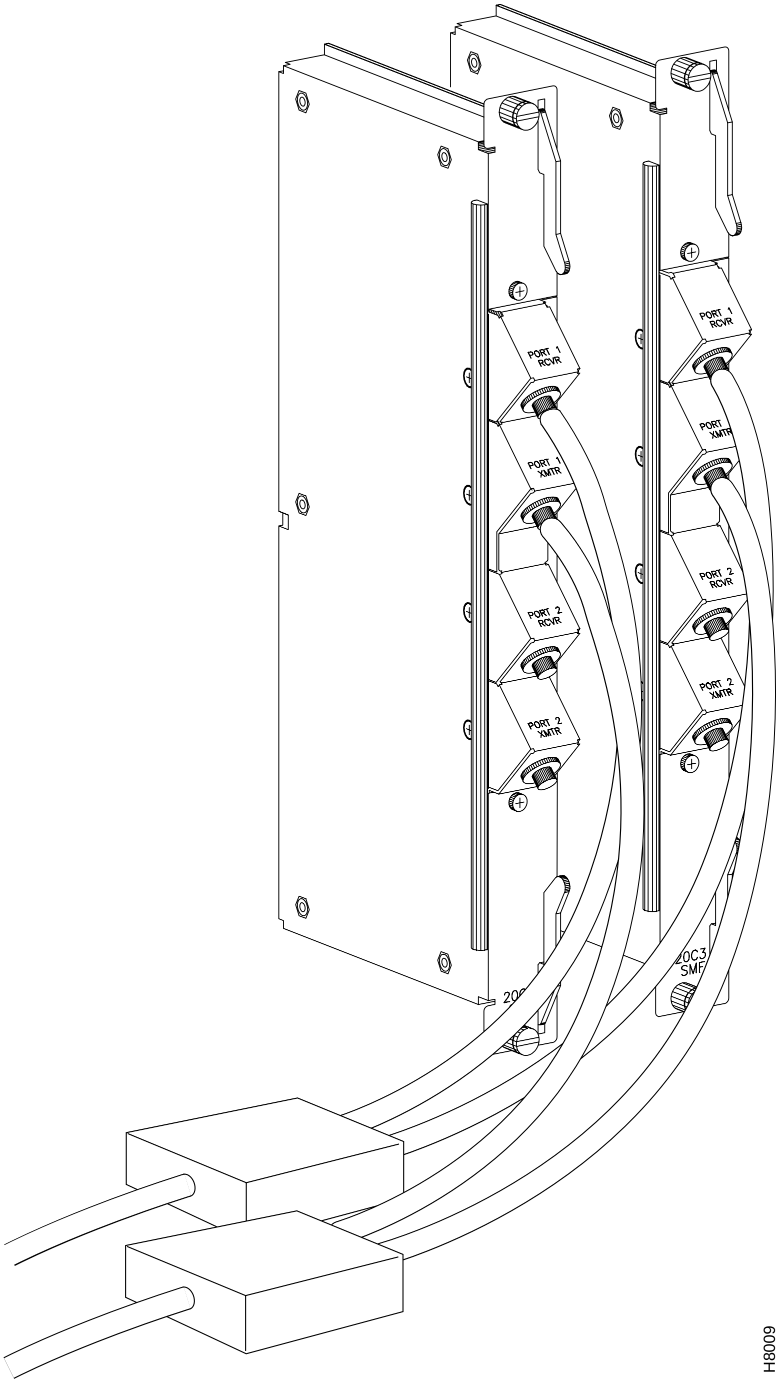
Step 4 Record which slot and port number are used for each trunk or line. You’ll need the information later when configuring the network.

Step 5 A Y-Cable redundancy connection for the SMF-2-BC backcard is shown in Figure 9-13. Y-Cable redundancy is supported only for the SMF-2-BC backcard which is used with either the BNI-155 or the ASI-155.

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 9-13). Do the same with the two RCV connectors.

Figure 9-13 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 9-14 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 9-15.

Make connections as follows:

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 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 and where Y-redundancy is not being used, an optional cable management tray is available to help route cables when a number of DS3/T3 cards are installed resulting a large number of cables to handle. Refer to Chapter 10, T3/E3 Cable Management Tray.

Figure 9-14 BXM T3/E3 Cable Connector Detail

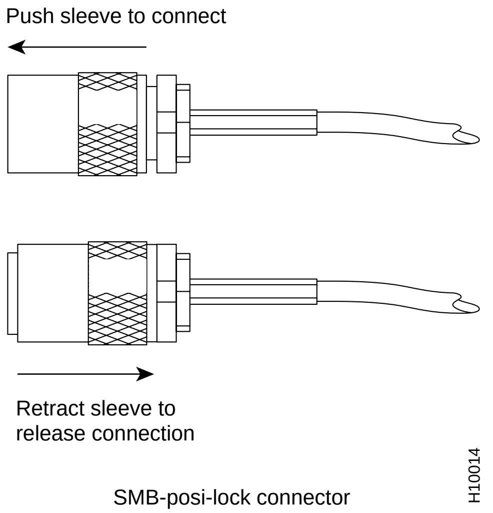
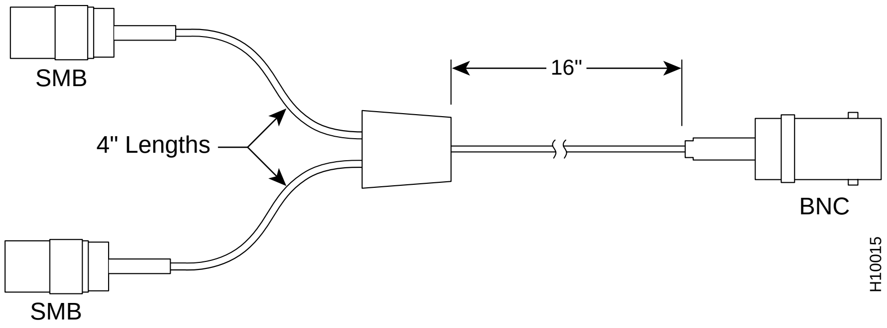


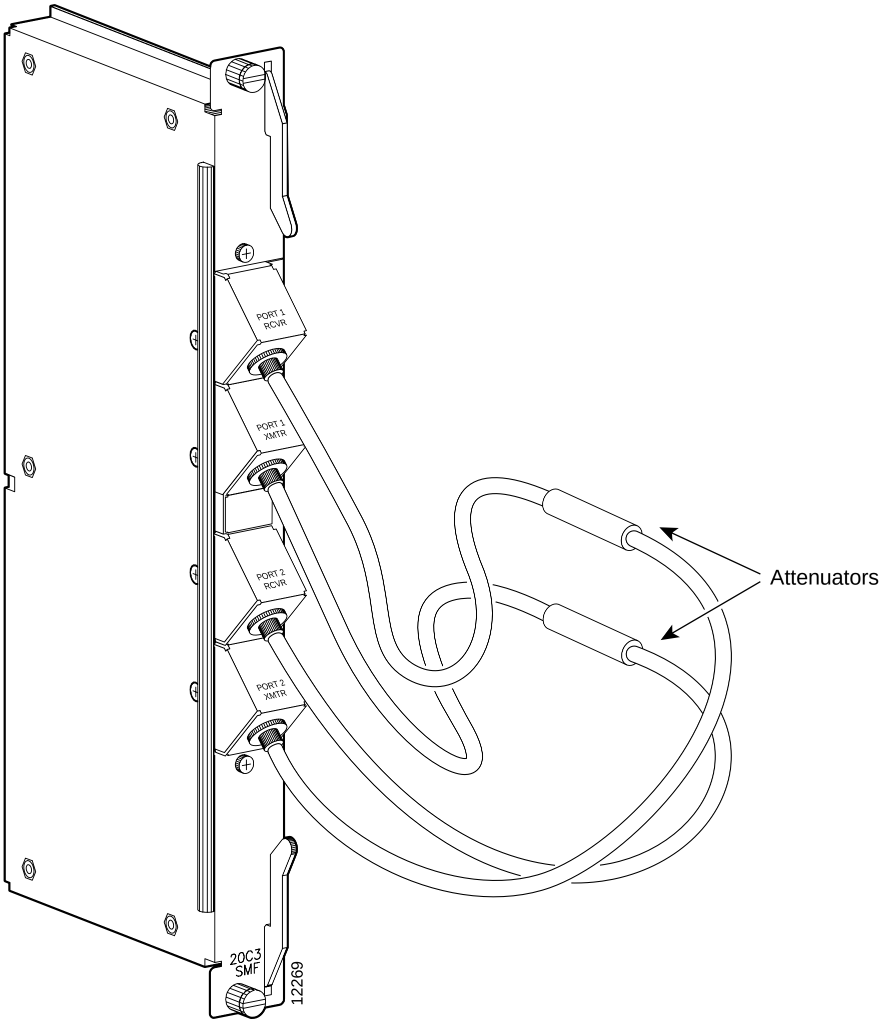
Figure 9-15 Y-Cable for BXM T3/E3 Cards



Setting up the BME OC-12 Port Loop

The two ports on the OC-12 backcard for the BME multicast card are setup of by connecting the transmit of port 1 to the receive of port 2 and the receive to port 1 to the transmit of port 2, thus looping the two ports together. This is shown in Figure 9-16.

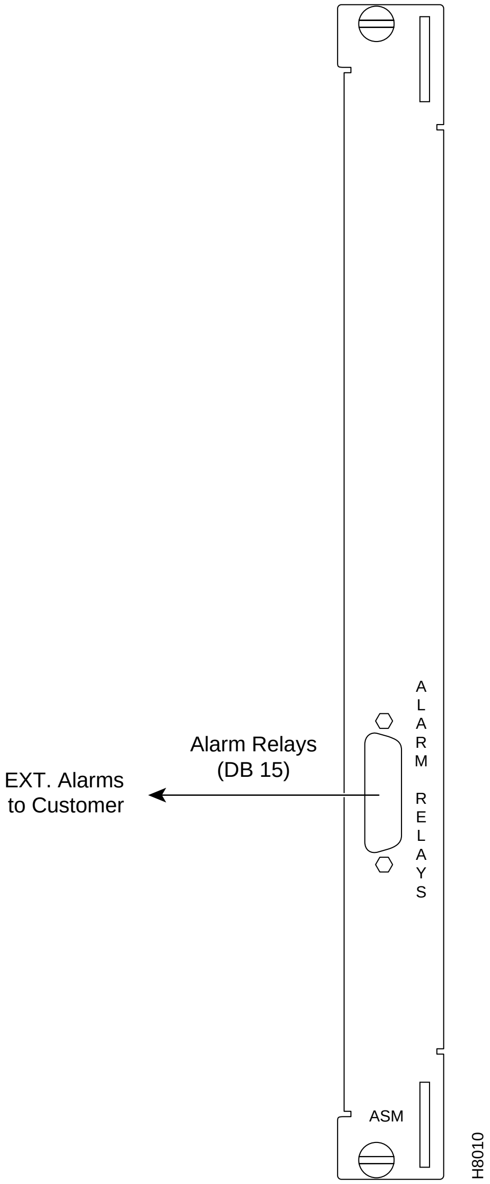
Figure 9-16 Looping Ports 1 and 2 for BME on OC-12 Backcard



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 9-17). Refer to *Appendix B, BPX Switch Cabling Summary*, for a list of the pinouts for this connector. Use switchboard cable for running these connections.

Figure 9-17 Alarm Output Connector



Attaching Peripherals

The BPX switch has two RS-232 serial data ports (labeled CONTROL port and AUXILIARY port) and an Ethernet port (labeled LAN) on the LM-BCC back card for attaching peripherals.

A network (or each domain in a structured network) must have at least one connection to a control terminal or Cisco WAN Manager network management workstation. The Cisco WAN Manager NMS workstation is used to configure and maintain all nodes in a network and report network statistical data. In addition, a network printer must be connected to the AUXILIARY port if you wish to print.

If it is desired to have Customer Service perform remote troubleshooting, a dial-in modem must be attached to the network. Procedures for attaching peripherals to the BPX switch are contained in the following paragraphs. Be sure to read the manufacturers literature to ensure that you have made the equipment ready for attachment, before attempting to attach it to the BPX switch.

Refer to the following for additional information on the following related subjects:

- *Appendix B, BPX Switch Cabling Summary*, lists the pin assignments for the BPX switch control terminal port.
- *Appendix C, BPX Switch Peripherals*, lists the control terminals supported and their required configuration settings.
- For instructions on using the switch commands, refer to the *Cisco Wan Switch Command Reference* manual.
- 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

A basic VT-100 type terminal may be connected to this port for use in entering commands to bring up a new node. (Note: Since the Cisco WAN Manager NMS workstation requires a LAN connection to a node in the network in order to perform its management functions, it is not connected to the Control Port during normal operation.)   In these procedures, the term BCC is used to refer 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, and the BCC-32 requires the BCC15-BC backcard.

Attach a terminal to the BPX switch as follows:

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 9-18, the 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 for some reason 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 9-19.

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 Set the port function for VT100/StrataView using the **cnftermfunc** command if connecting to a Cisco WAN Manager workstation. 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 using the **cnfterm** command.

Step 9 When you have completed the initial node configuration, you remove the connections to the CONTROL Port(s). 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 on-line" occurs, then the speeds will match and the terminal display will be readable.

Figure 9-18 Temporary Connections to Bring up a New Node, LM-BCC Backcard Shown

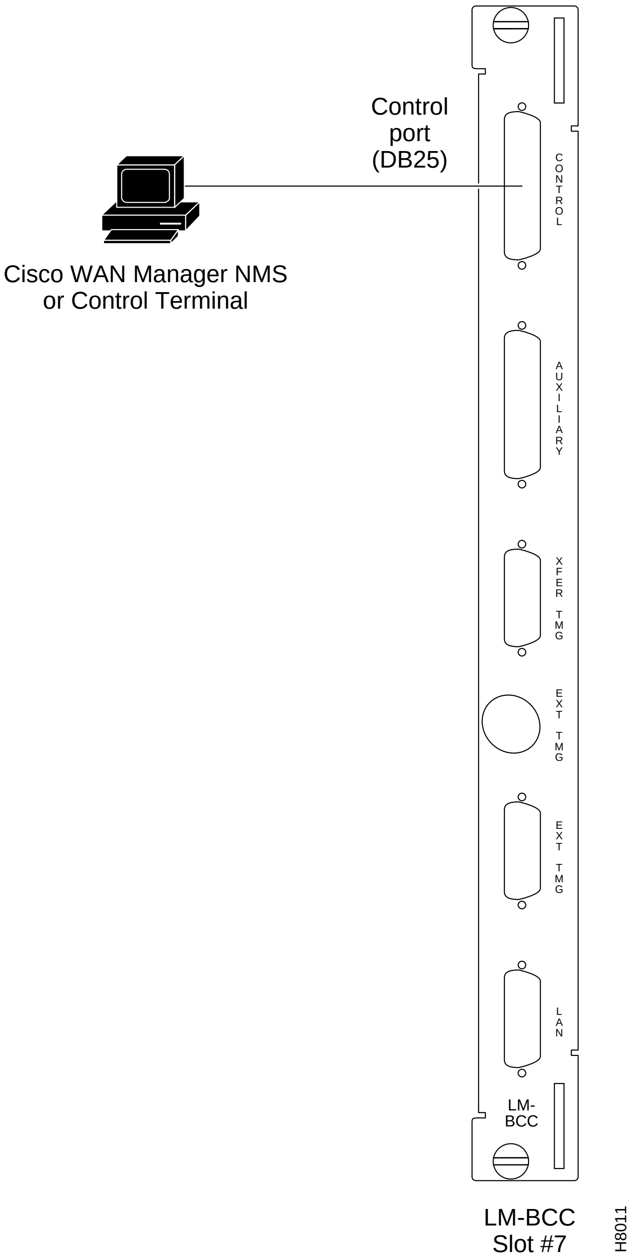
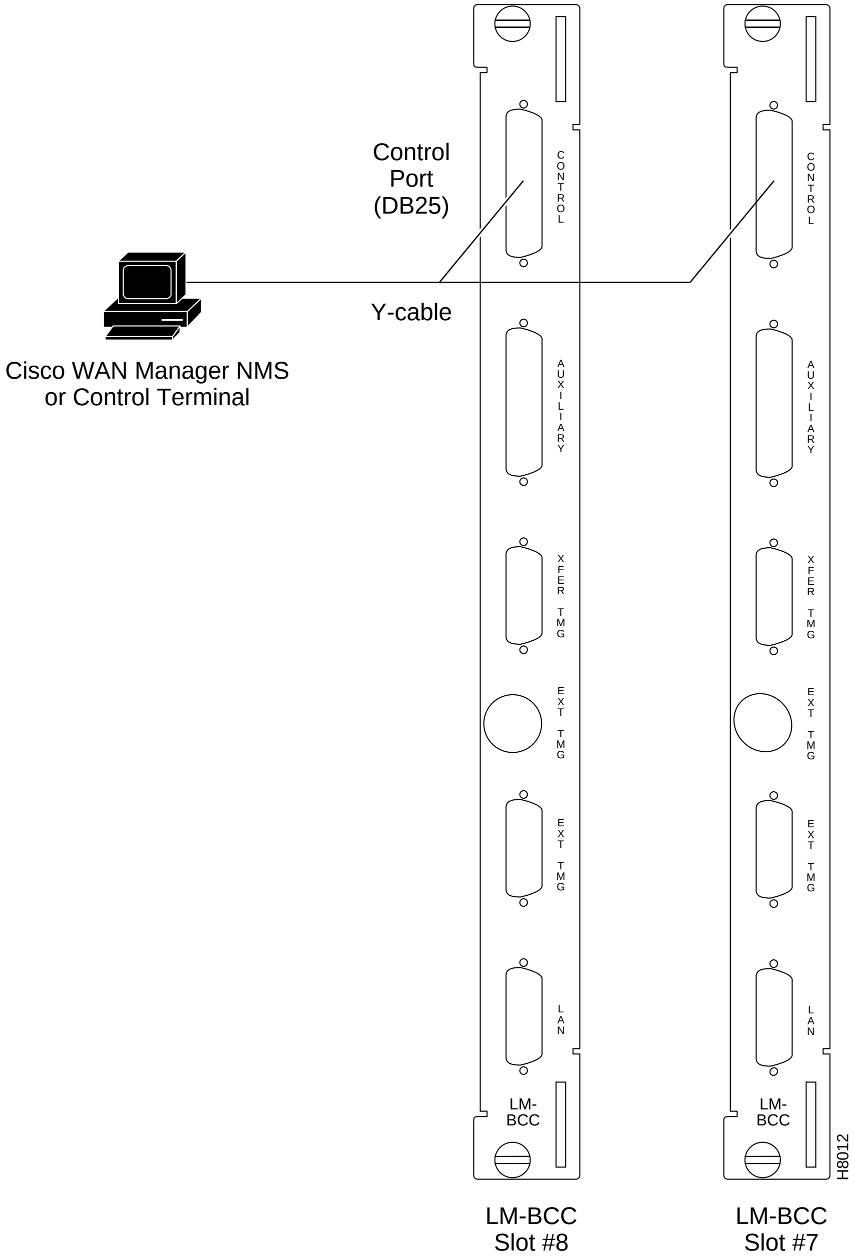


Figure 9-19 Temporary Connections to Bring up a New Node, LM-BCCs Shown

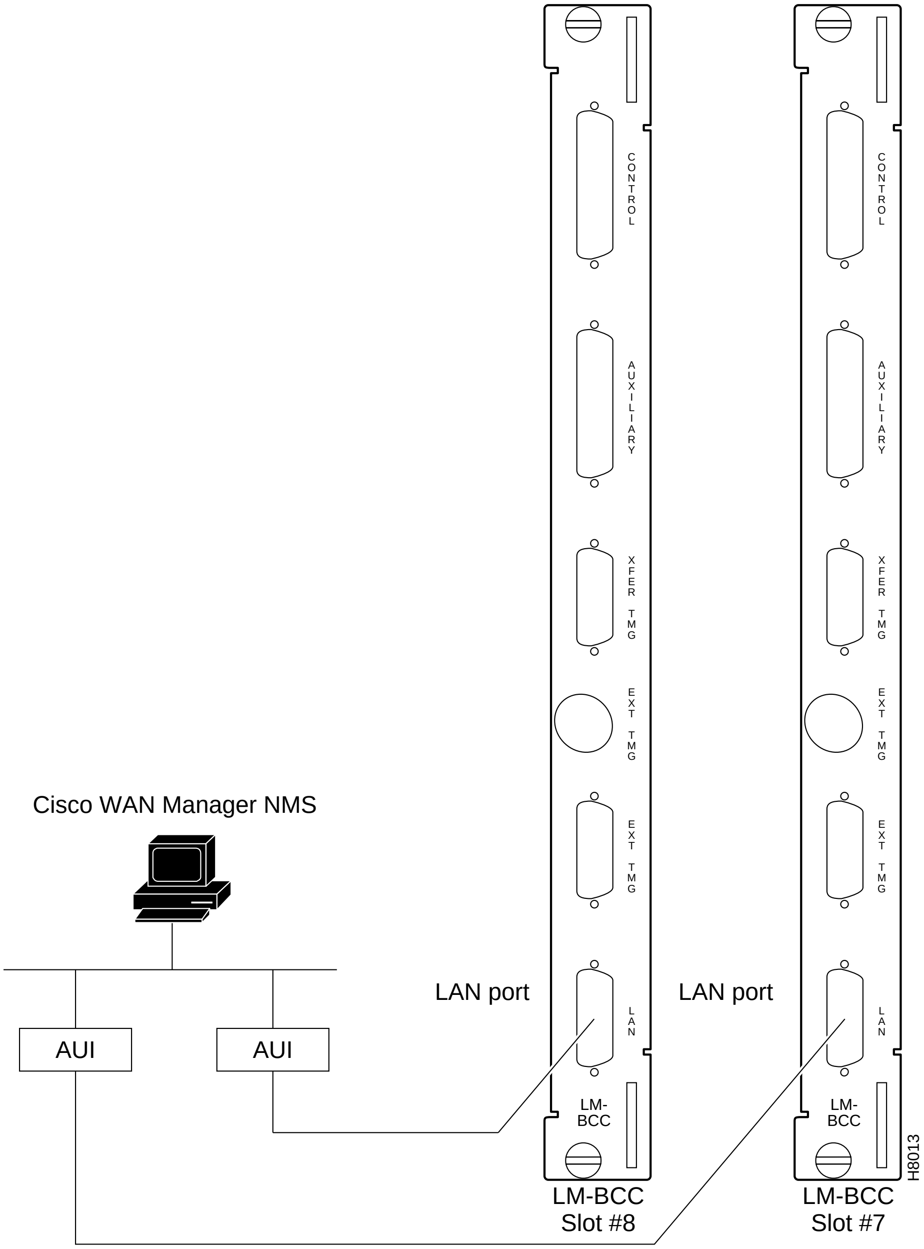


LAN Connection for the Network Management Station

The Cisco WAN Manager NMS is connected to an Ethernet port (LAN port) on a node in the network for the purpose of network management. The LAN port provides the capacity necessary for the network management traffic and network statistics collection. See Figure 9-20 illustrating this connection.

For access to the node using an Internet connection, the Internet Protocol (IP) address, IP subnet mask, TCP service port, and gateway IP address must be entered by the user with the **cnflan** command.

Figure 9-20 LAN Connections to BCC Backcards, 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.

Appendix C, BPX Switch Peripherals, lists the types of printers supported by the BPX switch along with configuration settings. Appendix B, BPX Switch Cabling Summary lists 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. Attach the printer to the BPX switch as follows:

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 9-21). Go to Step 4.

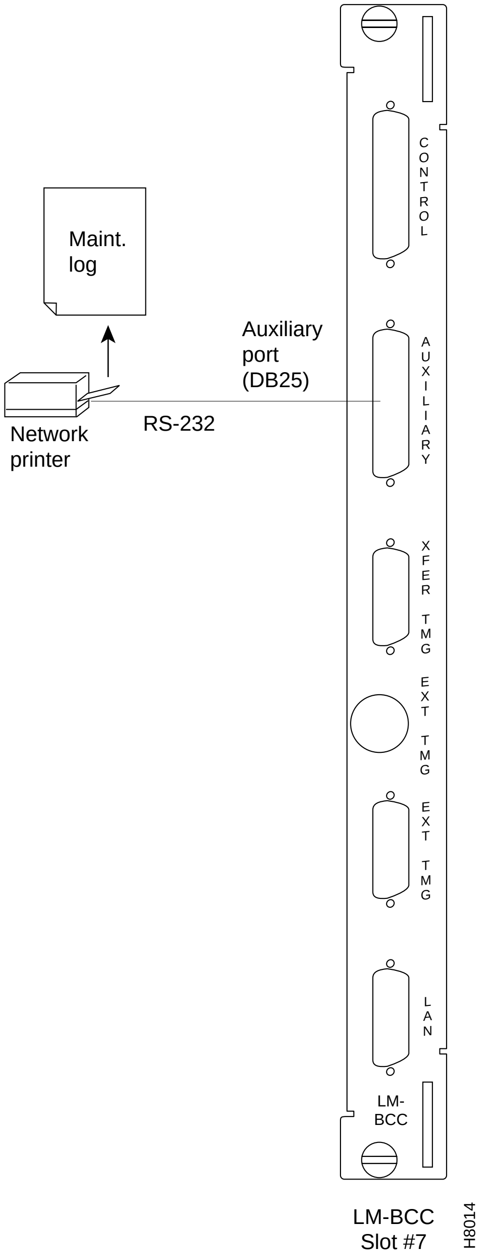
Step 3 **For nodes with redundant BCCs:** A Y-cable is required for this application. Connect one leg of the Y-cable to the AUXILIARY port connector on the LM-BCC in slot 7 and the other leg to the AUXILIARY port connector on the LM-BCC in slot 8.

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 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 using the **cnfterm** command.

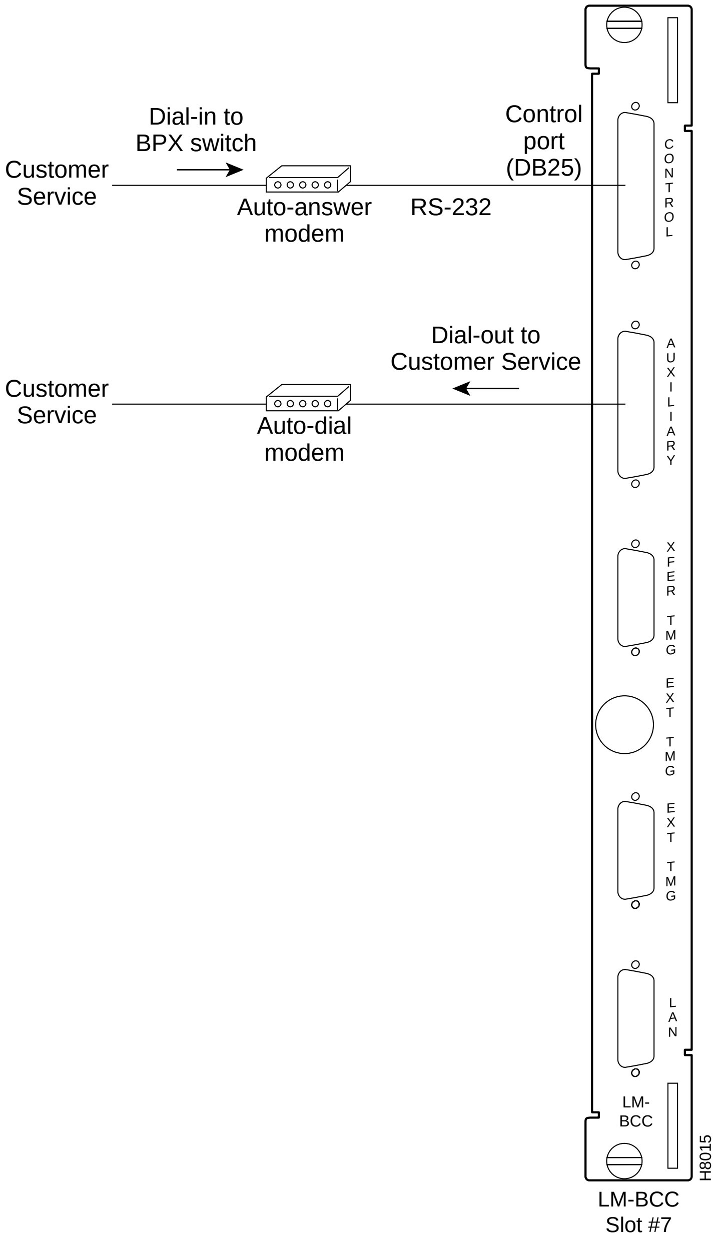
Figure 9-21 Connections to a Network Printer, LM-BCC Shown



Connecting Modems

A modem may be connected to each BPX switch to provide remote access by Customer Service (see Figure 9-22). For information on connecting and configuring a modem refer to Appendix C, BPX Switch Peripherals.

Figure 9-22 Connecting Modems to the BPX Switch, LM-BCC Shown



- An auto-answer modem is used to provide access for remote access. It is connected to the CONTROL port connector. This port is bi-directional transmit and receive.

These modems connect to a standard telephone line wall jack. The modem connections require special cables and setup procedures. Refer to *Appendix C, BPX Switch Peripherals*, for instructions on connecting and setting up the modems. If the BPX switch is equipped with redundant BCCs, an RS-232 Y-cable must be used for these connections.

Making External Clock Connections

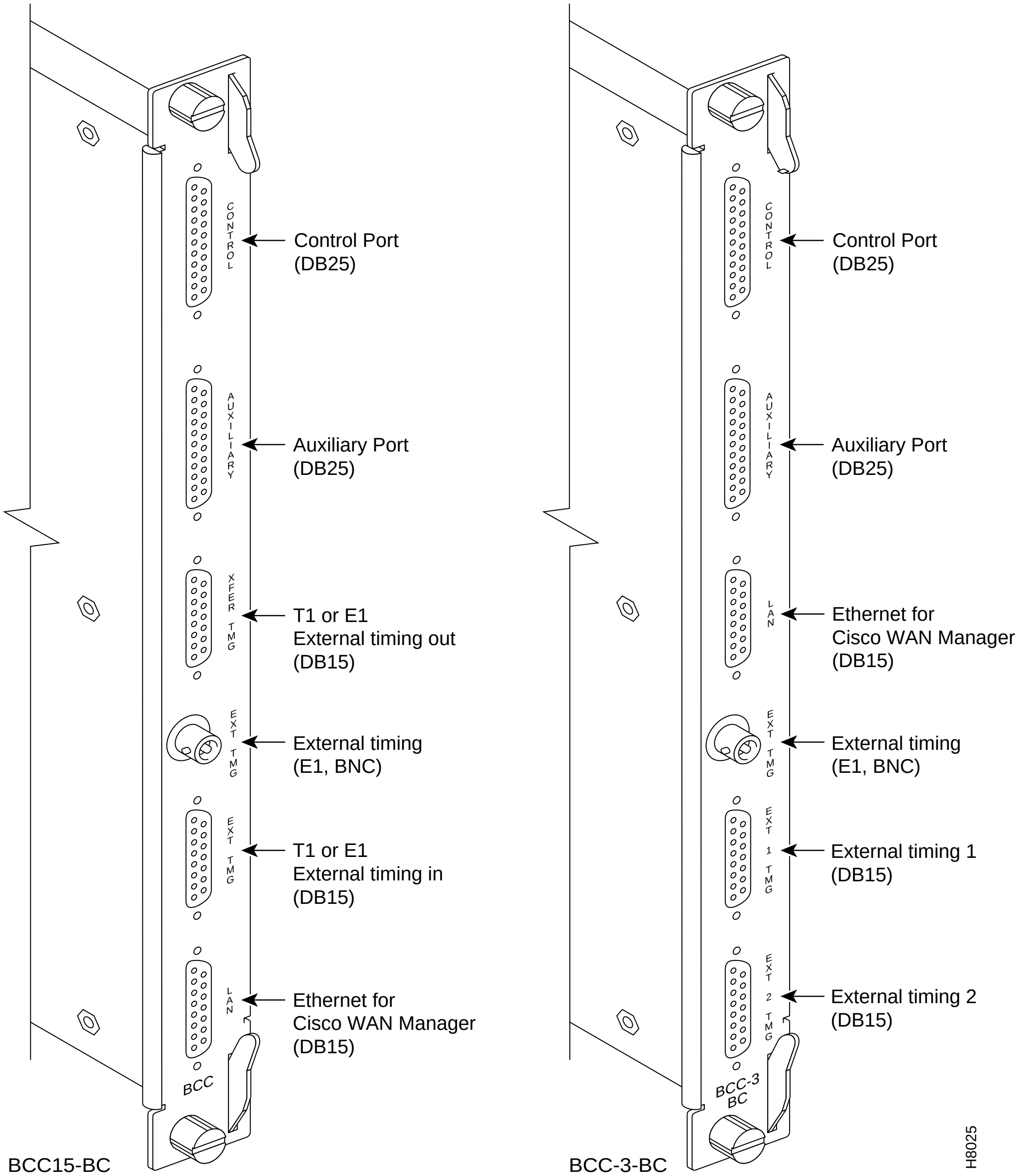
If the BPX switch is to be synchronized to some other external equipment or a local digital central office, one of two connectors on an BCC15-BC backcard (backcard for BCC-32) can be used to accept a clock input. A DB15 connector labeled EXT TMG can be used to connect a balanced T1 or E1 signal, synchronized 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), A DB15 connector labeled EXT 1 TMG can be used to connect a balanced T1 or E1 signal, synchronized from some higher-level source, to the BPX switch. 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 Customer Service for information on setting up either a 75-ohm or 120-ohm clock interface on the BCC backcard.

Figure 9-23 External Clock Source Connections to Backcards for BCCs



Initial Power-Up of the BPX Switch

Before operating the BPX switch, check that the following procedures have been performed:

Step 1 The BPX switch is connected to an appropriate power source with an isolated ground connection, per the procedures in Chapter 7, Installation, DC Shelf Initial Setup, or Chapter 8, Installation, AC Shelf Initial Setup, 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 to the appropriate LM-3T3/3E3 faceplate.

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 needed, a printer may be connected to the AUXILIARY port on the LM-BCC in back slot 7/8 and the printer power cord plugged into the appropriate power outlet.

Step 7 If needed, a modem(s) may be connected to the CONTROL port or AUXILIARY port, as applicable, on the LM-BCC in back slot 7/8, and the modem(s) power cord(s) plugged into the appropriate power wall outlet.

Step 8 From the back of the BPX switch, turn the power switches to the ON position.

Step 9 From the front of the BPX switch, observe the cards go through initial diagnostic self-tests.

- The AC power supply(ies) –48V indicator will be 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 will show “FAIL” for a few seconds, then become active or standby.
- The ASM DC LEDs should both be green indicating that the DC voltages on the two DC power busses are within tolerance.
- There may or may not be alarms showing on the ASM, BXMs, BMEs, BNIs and ASIs. Alarms may be present on ATM trunk connectors that have not been physically connected to their associated lines.

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. When that happens, do the following:

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, a terminal connected to the CONTROL port or an NMS workstation connected via a telnet session to the LAN port will display the software on-line screen as shown 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

For provisioning of the BPX switch, including configuring ports, lines, trunks, and adding connections refer to the following documents:

- *Cisco BPX 8600 Series Reference*
- *Cisco WAN Manager Operations*
- *Cisco WAN Service Node Extended Services Processor Installation and Operation*
- *Cisco WAN Switching Command Reference*
- *Cisco WAN Switching SuperUser Command Reference*

Configuration

Proceed to *Chapter 11, Configuration, Introduction*, for configuration procedures for the BPX switch.

T3/E3 Cable Management Tray

This chapter provides instructions for the installation of the optional cable management tray that may be used to route cables in an open rack non-redundant configuration.

You'll need to obtain the optional cable management tray kit and one each BXM T3/E3 cable bracket kit for each BXM T3/E3 card.

This chapter contains the following:

- Installation of Cable Management Tray
- Raising Tray for Access to PEMs
- Installing BXM T3/E3 Cable Management Bracket
- Connecting Cables to T3/E3 Cards
- Routing Cables from Cards through Cable Management Tray
- Tray Raised with Cables in Place

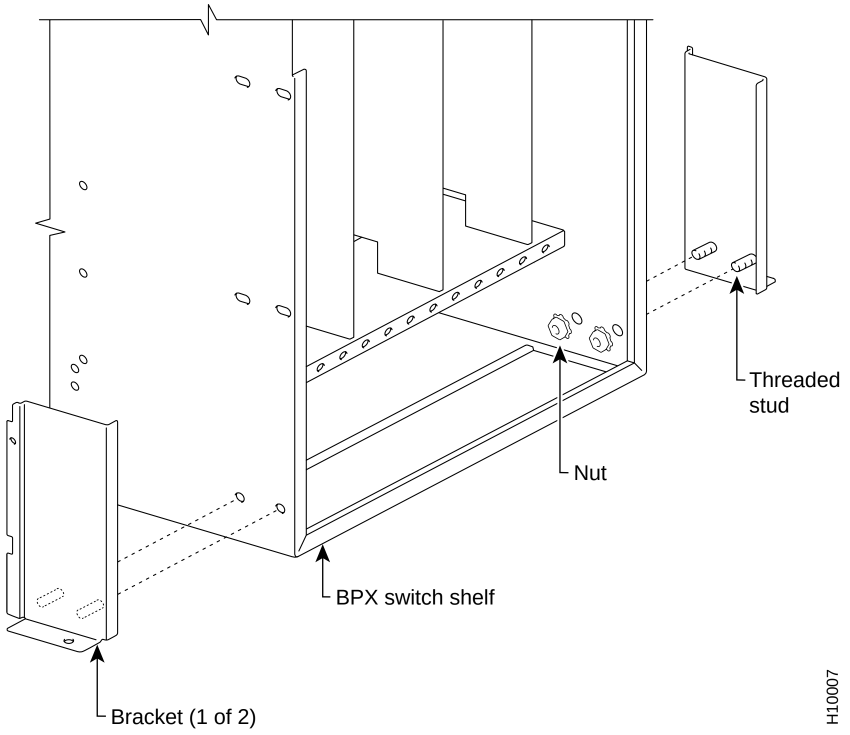
Installation of Cable Management Tray

Installing Tray Brackets

Step 1 Obtain brackets and associated hardware from kit.

Step 2 Install left and right brackets, using 2 nuts to secure each bracket, Figure 10-1.

Figure 10-1 Installation of Cable Management Tray Brackets



Installing Tray

Step 1 Using two hands to hold cable management tray, slide over brackets Figure 10-2.

Step 2 Lower tray into lower rest position Figure 10-3.

Figure 10-2 Sliding Cable Management Tray over Brackets

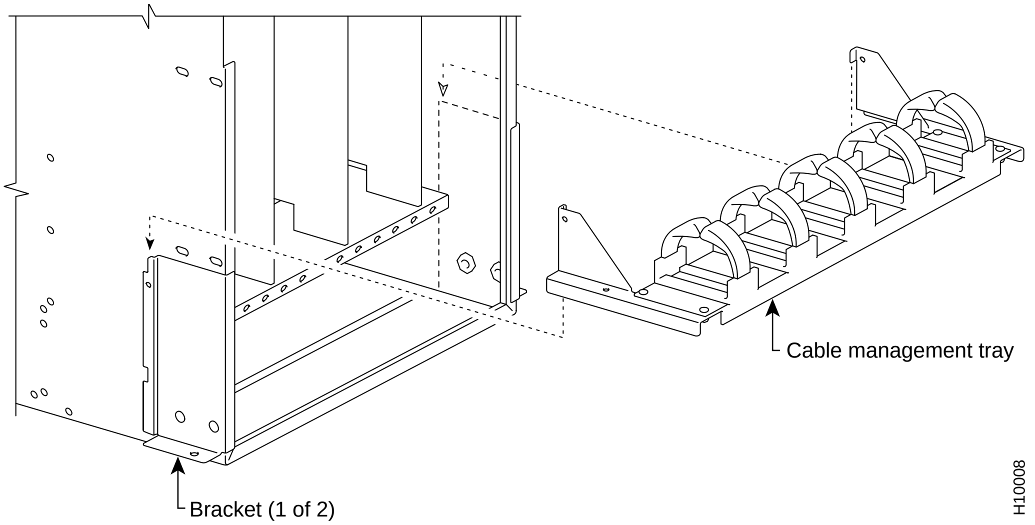
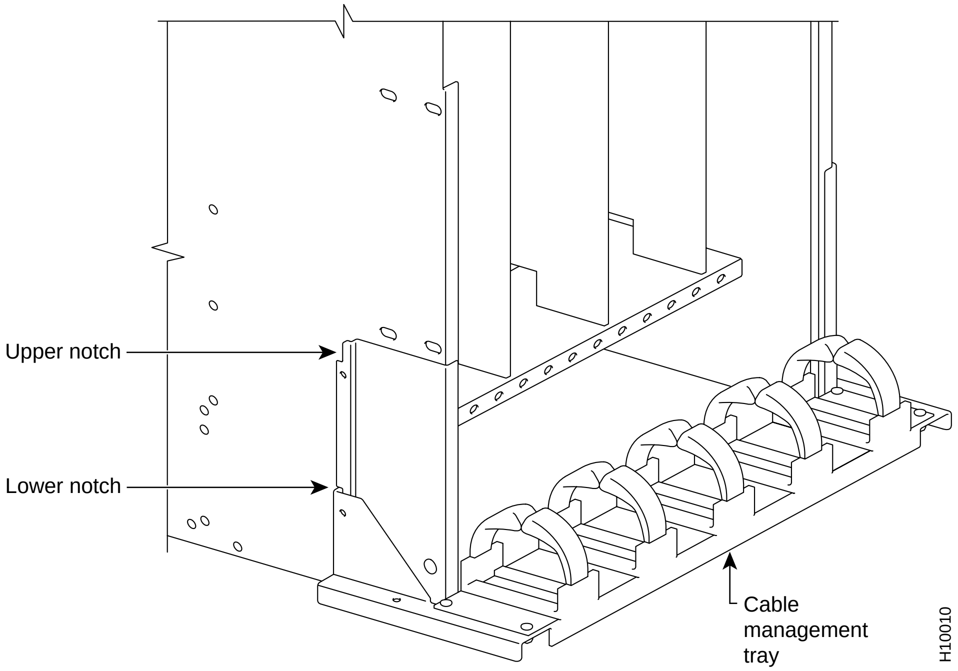


Figure 10-3 Cable Management Tray in Lowered Home Position



Raising Tray for Access to PEMs

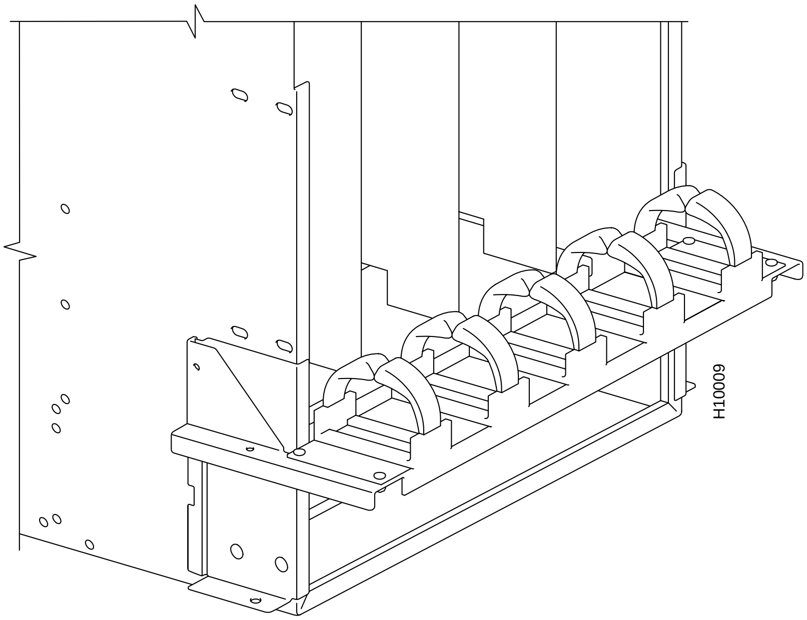
The tray is raised only when necessary to access the Power Entry Modules (PEMs), typically for replacement or to install a second PEM. Figure 10-4 shows the tray in the raised position. To raise the tray to provide access to the PEMs proceed as follows:

Step 1 Remove securing screws as necessary.

Step 2 With two hands, pull tray towards you and up.

Step 3 Raise tray to upper position and lower onto upper slots.

Figure 10-4 Cable Management Tray in Raised Position



Installing BXM T3/E3 Cable Bracket

Attach the BXM T3/E3 cable bracket to each BXM T3/E3 card as follows, Figure 10-5:

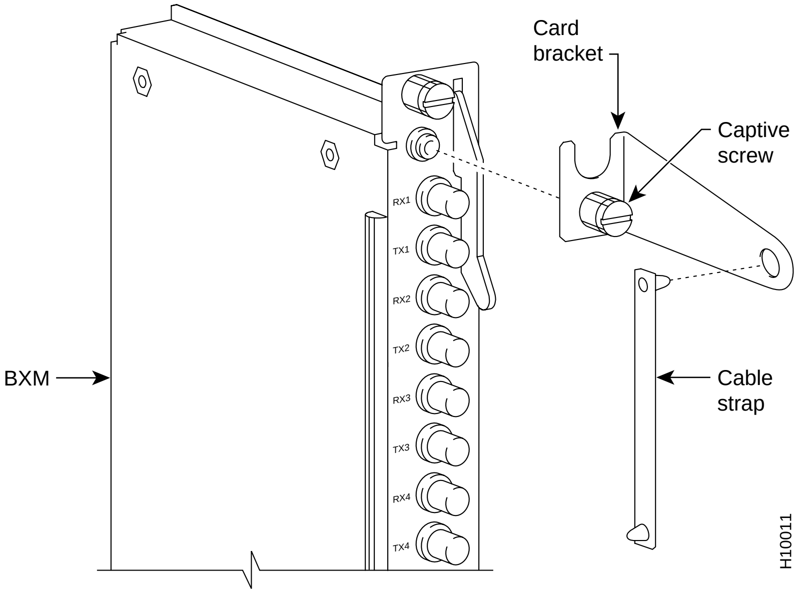
Step 1 Remove bracket from kit.

Step 2 Place bracket in position as shown.

Step 3 Screw in and tighten captive screw.

Step 4 Insert one end of cable tie through hole in bracket.

Figure 10-5 Installing BXM T3/E3 Cable Bracket



Connecting Cables to BXM T3/E3 Cards

Route cables as follows, Figure 10-6 and Figure 10-7:

Step 1 Connect cables to card by pushing on SMB connector locking sleeves as you push cable connectors on to card connectors.

Step 2 Dress cables upward to provide service loop.

Step 3 Bundle cables using cable ties.

Step 4 Wrap cable strap around cables and secure to cable management bracket.

Note Cables are disconnected from a card by pulling on the cable connector locking sleeve as you pull cable connector away from card connector.

Figure 10-6 **Connecting Cables to T3/E3 Card**

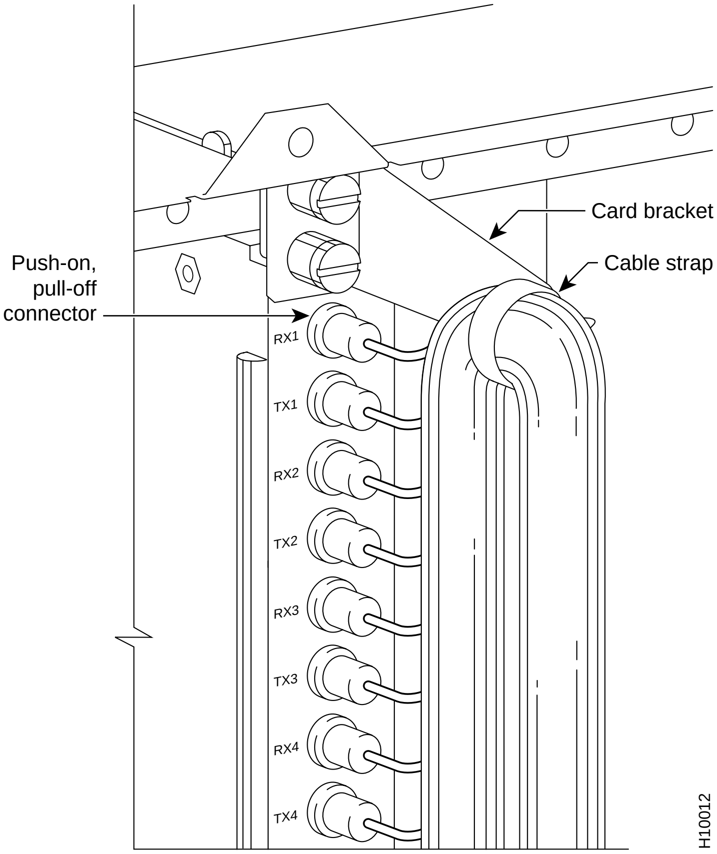
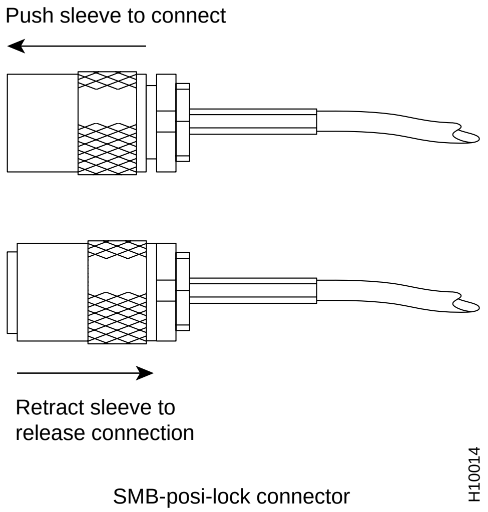


Figure 10-7 T3/E3 SMB Connector Detail



Routing Cables from Cards through Cable Management Tray

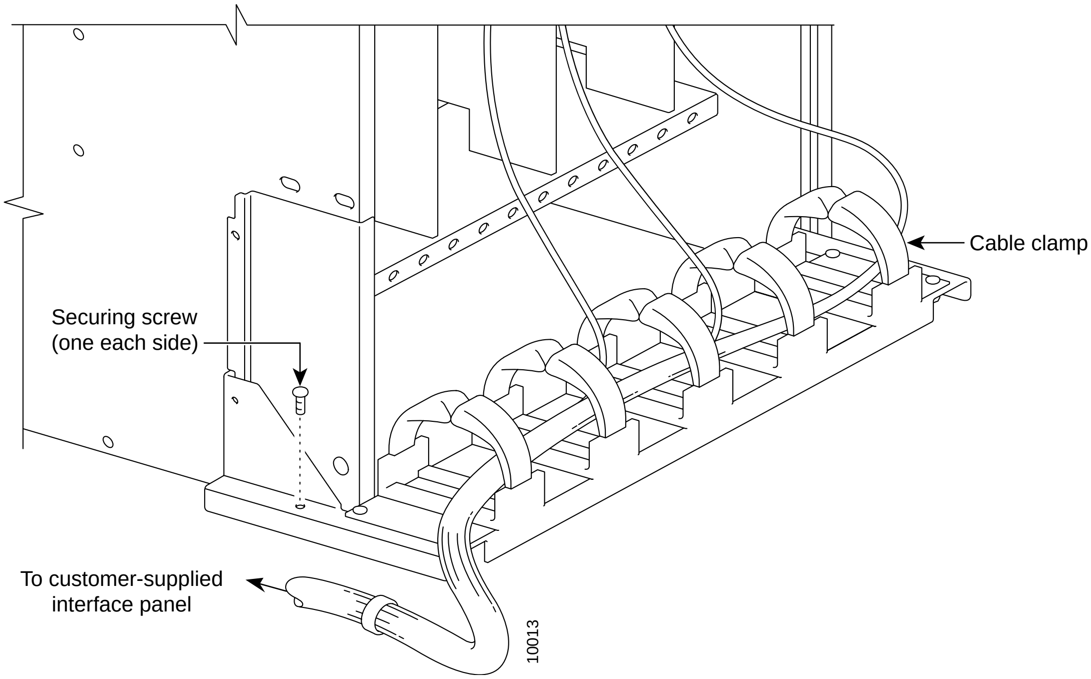
Route cables as follows, Figure 10-8:

Step 1 Verify that cable management tray is in lowered home position.

Step 2 Route cables from cards through cable clamps on cable management tray.

Step 3 Secure cable management tray to cable tray brackets by inserted and tightening securing screw, one to each bracket.

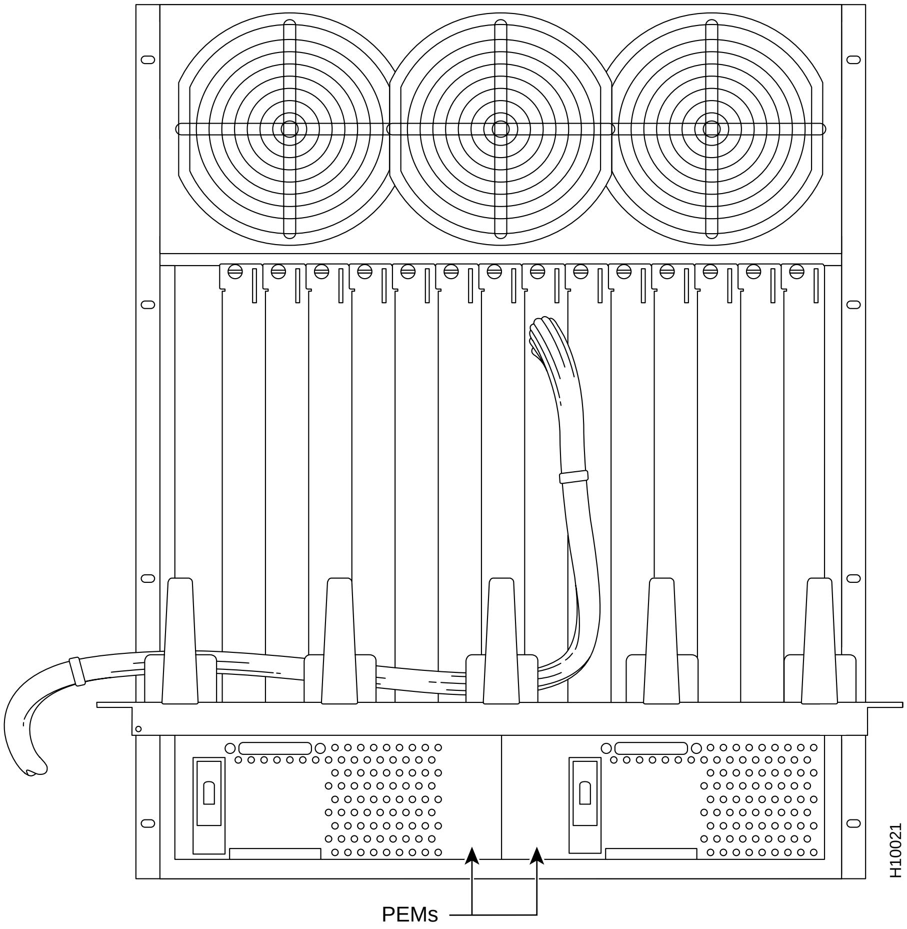
Figure 10-8 Cables Routed through Cable Management Tray in Lowered Position


Cable clamp
Securing screw (one each side)
To customer-supplied interface panel
10013

Tray Raised with Cables in Place

Figure 10-9 shows how the cable management tray is raised with cables in place, to provide access to the Power Entry Modules (PEMs).

Figure 10-9 Tray Raised with Cables in Place



PART 4

Configuration, General

Configuration, Introduction

Introduction

Detailed configuration information is provided in this part of the document. A summary of the configuration instructions is provided in the Quickstart instructions at the front of the manual, in *PART 2, Quickstart*.

For additional information on the BPX switch, including card descriptions and additional information on configuration, refer to the *Cisco BPX 8600 Series Reference*. For a description of the commands used to operate a BPX switch, refer to the *Cisco WAN Switch Command Reference*. Refer to the Cisco WAN Manager manuals for information on network management.

Configuration Procedures

Figure 11-1 shows the sequence of operations followed during the configuration of the BPX switch. A summary of this sequence is as follows:

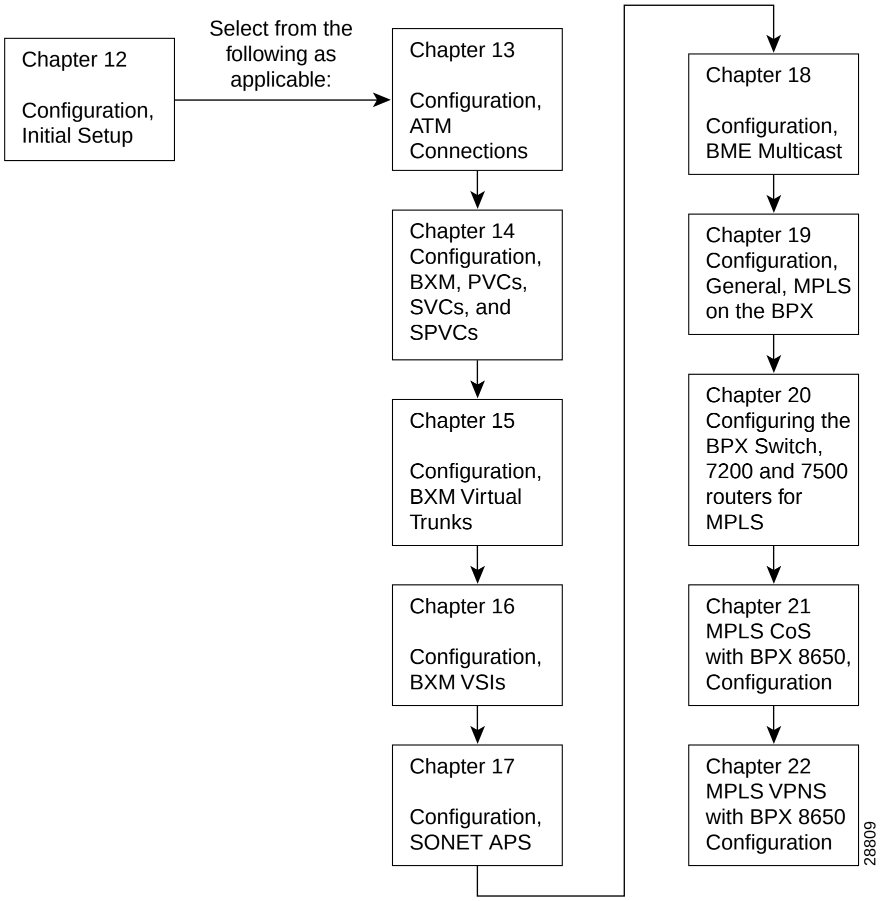
- *Chapter 12, Configuration, Initial Setup*, provides preliminary configuration instructions for the BPX switch including basic node configuration.

  As a minimum, the nodes need to be configured with name (**cnfname**), date (**cnfdate**), time (**cnftime**), time zone (**cnftmzn**), and trunks upped (**uptrk**) and added (**addtrk** or **addshelf**), as applicable. In addition, instructions are provided for configuring the nodes for operation with the Cisco WAN Manager.

The following chapters provide information and configuration examples for various types of ATM connections:

- *Chapter 13, Configuration, ATM Connections*
- *Chapter 14, Configuration BXM: PVCs, SVCs, and SPVCs*
- *Chapter 15, Configuration, BXM Virtual Trunks*
- *Chapter 16, Configuration, BXM VSIs*
- *Chapter 17, SONET APS, Configuration*
- *Chapter 18, Configuration, BME Multicasting*
- *Chapter 19, Configuration General, MPLS on BPX Switch*
- *Chapter 20, Configuring the BPX Switch, 7200, and 7500 Routers for MPLS*
- *Chapter 21, MPLS CoS with BPX 8650, Configuration*
- *Chapter 22, Configuring the BPX Switch, 7200, and 7500 Routers for MPLS*

Figure 11-1 Configuration Sequence


Chapter 12
Configuration, Initial Setup
Select from the following as applicable:
Chapter 13
Configuration, ATM Connections
Chapter 14 Configuration, BXM, PVCs, SVCs, and SPVCs
Chapter 15
Configuration, BXM Virtual Trunks
Chapter 16
Configuration, BXM VSIs
Chapter 17
Configuration, SONET APS
Chapter 18
Configuration, BME Multicast
Chapter 19 Configuration, General, MPLS on the BPX
Chapter 20 Configuring the BPX Switch, 7200 and 7500 routers for MPLS
Chapter 21 MPLS CoS with BPX 8650, Configuration
Chapter 22 MPLS VPNS with BPX 8650 Configuration
28809

Configuration, Initial Setup

This chapter contains configuration procedures.

This chapter contains the following:

- BPX Switch Management
- Initial Node Configuration Summary
- IP Setup and IP Relay Configuration
- Configuring the LAN Port

The BPX switch can be accessed through a local control port (over an RS-232 or Ethernet TCP/IP link.) An administration screen from a control terminal or from the Cisco WAN Manager Network Management Station (NMS) can issue BPX switch commands. Remote control terminal access is possible using a Virtual Terminal (vt) command if the node has been configured with a name and at least one trunk to the network has been established.

For Frame Relay connections in both tiered and non-tiered networks Cisco WAN Manager provides end-to-end configuration management using the Connection Manager. When an IPX or IGX is configured as an Interface Shelf, it can not be reached by the vt command, and Frame Relay end-to-end connections are configured from the Cisco WAN Manager via the Connection Manager over an in-band LAN connection. (Telnet can be used to access an interface shelf (e.g., IPX or IGX shelf or MGX 8220 shelf) if a Cisco WAN Manager workstation is not available to provide in-band management.)

BPX Switch Management

You can monitor, manage and troubleshoot the BPX switch using the Cisco WAN Manager Network Management Station. Commands are issued to a BPX switch through the Node Administration window. Frame Relay connections are added via the Cisco WAN Manager Connection Manager. You can display and monitor the network’s topology, monitor alarms, events, and statistics. Refer to the *Cisco WAN Manager Operations* publication for more information.

For detailed configuration information, refer to the *Cisco WAN Switch Command Referen*ce publication.

Initial Node Configuration Summary

Adding Nodes, Adding Trunks, Shelves, etc.

Refer to the applicable reference publications, *Cisco IPX Reference*, *Cisco BPX 8600 Series Referenc*e, *Cisco IGX 8400 Series Reference*, and Cisco *MGX 8220 Reference*, for node installation and operation.

As a minimum, the nodes need to be configured with name (**cnfname**), date (**cnfdate**), time (**cnftime**), timezone (**cnftmzn**), and trunks upped (**uptrk**) and added (**addtrk** or **addshelf**), as applicable. Connections can also be added now or later, after configuring the nodes for operation with the Cisco WAN Manager NMS manager.

The basic tasks to configure a BPX switch are as follows:

- Set up the node.
  - — Configure the node name (**cnfname**).
  - — Configure the time zone (**cnftmzn**).
  - — Configure date (**cnfdate**).
  - — Configure time (**cnftime**).
  - — Configure the LAN interface (**cnflan**).
  - — 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**).
- Set up the trunks to other routing nodes.Verify the correct cards are in both the local and remote nodes (**dspcds**).
  - — Up the trunk(s) at each node (**uptrk**).
  - — Configure any parameters required for the trunk at each node (**cnftrk**).
  - — Add the trunk(s) at each node (**addtrk**).
  - — Set up Y redundancy if desired (**addyred**).
- If using an IPX/IGX Interface Shelf, configure it as shelf.
  - — Up the trunk from the AIT/BTM to the BPX switch using (**uptrk**). Shelf trunks for the IPX/IGX must be upped on both the BPX routing switch and the shelf before the shelf can be joined to the Routing Network.
  - — Contact Customer Service to configure the IPX/IGX shelf option.
  - — At the BPX switch, add the IPX/IGX switch as a shelf to the BPX (**addshelf**).

The following two examples are of the screens displayed when “**dspnode**” is entered at a BPX switch and at one of its IPX shelves, respectively. The “**dspnode**” screen displayed at the “**hubone**’ BPX switch shows that it is connected to the “shlf3ipx” node via BNI trunk 3.3. The “**dspnode**” screen displayed at the “shlf3ipx” node show that it is connected to the BPX switch via AIT trunk 8.

Example of **dspnode** at node “hubone” BPX15 showing feeder shelves.

```
hubone          TN    edgar       BPX 15    9.2       Nov. 20 1998 08:09 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 1.2     shlf1      MGX 8220  OK
 1.3     shlf2      MGX 8220  OK
 3.1     shlf1IPX   IPX/AF    OK
 3.2     shlf2IPX   IPX/AF    OK
 3.3     shlf3IPX   IPX/AF    OK
 4.1     shlf4IPX   IPX/AF    OK
 4.3     shlf5IPX   IPX/AF    OK


Last Command: dspnode
```

Example of dspnode at node Shlf3IPX showing connection to “hubone”

```
shlf3IPX          TN    edgar       IPX 8     9.2    Nov. 20 1998 09:24 PDT

                        BPX Switching Shelf Information

Trunk    Name      Type      Alarm
   8     hubone    BPX       MAJ







Last Command: dspnode


Next Command:
```

- Adding the MGX 8220 Shelf.
  - — At the BPX switch, add the MGX 8220 as a shelf to the BPX switch (**addshelf**).
- Set up ATM service lines and ports.
  - — Activate the line (**upln**).
  - — Configure the line (**cnfln**).
  - — Activate the ports (**upport**).
  - — Configure the ports (**cnfport**).
- Set up ATM connections.
  - — Add connections (**addcon**).
  - — Configure a connection type (**cnfcontyp**).

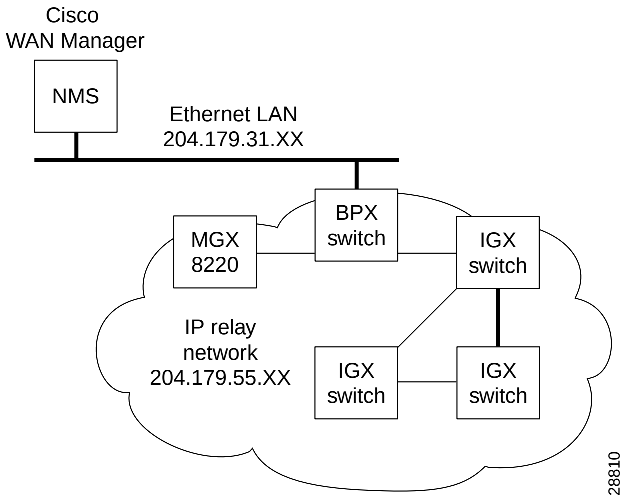
- Set up ATM to Frame Relay (ATF) connections.
  - — Add the connections (**addcon**).
  - — Configure connection classes (**cnfcls**).
  - — Configure connection groups (**addcongrp**).
- Set up Interface Shelf Frame Relay Connections in Tiered Networks.
  - — Refer to the *Cisco WAN Manager Operations* publication.
  - — Only Frame Relay connections are supported from the IPX Interface Shelf and these are added and managed by the Cisco WAN Manager Connection Manager via the SNMP protocol. All connections are treated as end-to-end.
  - — Frame Relay connections terminated at an MGX 8220 Shelf are added and managed by the Cisco WAN Manager Connection Manager via the SNMP protocol. All connections are treated as end-to-end.
  - — ATM connections terminated at an MGX 8220 Shelf are added and managed using the Cisco WAN Manager Connection Manager via the SNMP protocol. All connections are treated as end-to-end.

IP Setup and IP Relay Configuration

In setting up network management for a network, both the Cisco WAN Manager workstation and network nodes need to be configured. Cisco WAN Manager communicates over a standard physical LAN network to a gateway node or nodes, but a separate in-band IP relay network is setup for all nodes via a gateway node for SNMP and TFTP in-band communication over the node trunks.

On IPX, BPX, IGX switches, the following commands are used to configure the nodes for operation with Cisco WAN Manager: **cnflan**, **cnfnwip**, **cnfstatmast**, **cnfsnmp**. The MGX 8220 is configured with **cnfifip** and **cnfstatsmgr**. The **cnflan** command is only necessary for nodes or shelves in which the LAN port is actually connected to a physical Ethernet LAN as shown in Figure 12-1.

Figure 12-1 Cisco WAN Manager Physical LAN and IP Relay Network



Installing Cisco WAN Manager and Associated Applications

Refer to the *Cisco WAN Manager Operations*, *Cisco WAN Switching Command Reference*, and *Cisco MGX 8220 Reference* publications for additional information.

Configuring the Cisco WAN Manager Workstation (example)

Step 1 Contact your System Administrator to obtain IP addresses. Also, 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, as the NIS is disabled.

Step 3 Enter the name or IP address of the gateway node in config.sv, using physical LAN name e.g., “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 as follows:

```
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, e.g., “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.

Note Refer to the *Cisco WAN Manager Operations* and the *Cisco WAN Switching Command Reference* for additional information.

Step 1 Contact your System Administrator to obtain IP addresses for your workstation and for the BPX/IGX/IPX 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 and IPX relay addresses.

Normally, the System Administrator will provide the IP addresses for the workstation and node. Refer to the *Cisco WAN Manager Operations* manual for instructions on configuring the Cisco WAN Manager workstation.

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, IGX, or IPX switch LAN port for node sanfran has been assigned an IP address of 192.187.210.30 and a hostname 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 (e.g., corporate network), you will need to contact the system administrator.

Note 5120 is used for the LAN ports on all BPX/IPX switch ports.

Step 2 Configure the LAN port on the BPX/IPX switch 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 the following 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.IPX switch LAN port number entered in the **/etc/service** file on the workstation. It is 5120 for all BPX/IGX/IPX switches.
- **Default Gateway IP Address** is the Internet gateway address. This is the gateway that traffic is routed through if the BPX, IGX, or IPX 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. (Note: 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 12-2. 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. Since 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), which must be obtained from your System Administrator, has been entered. 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, e.g., BCC.

Example: Configuring a Control Port (Gateway Router Example)

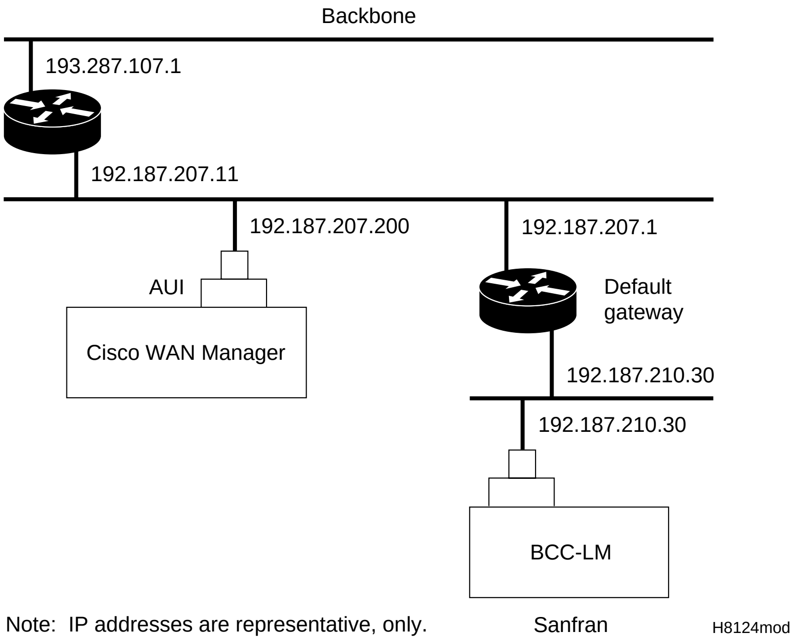
```
beta       TN    YourID.1       BPX 15    9.2    Dec. 3 1998 02:16 PST

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


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 hostname of “sanfran” entered in the **config.sv** file, you could enter the following at the Cisco WAN Manager workstation:

```
ping sanfran
```

Figure 12-2 Cisco WAN Manager LAN Connection via Gateway Router to a BPX Switch



Note: IP addresses are representative, only.

Step 5 An IP Relay address needs to 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 need to be set up for each node in the network. This is so that network management using SNMP and statistics collection using TFTP via inband ILMI may be carried out. Also, assuming an isolated network for the nodes, the workstation must be isolated from the NIS reference pages in order that the Cisco WAN Manager workstation consults the /etc/hosts table. Refer to the *Cisco WAN Manager Operations* manual for further information.

Example Display using **cnfnwip** to configure IP Relay address (required for each node):

```
beta     TN     YourID        BPX 15   9.2      Dec. 3 1998  02:11 PST

Active Network IP Address:             192.187.57.10
Active Network IP Subnet Mask:         255.255.255.192




Last Command: cnfnwip


Next Command:
```

Step 6 Once the workstation and BPX switch interface have been set up, Cisco WAN Manager can be started. The following example shows the **dsplan** screen after Cisco WAN Manager has been started and the communication sockets are active.

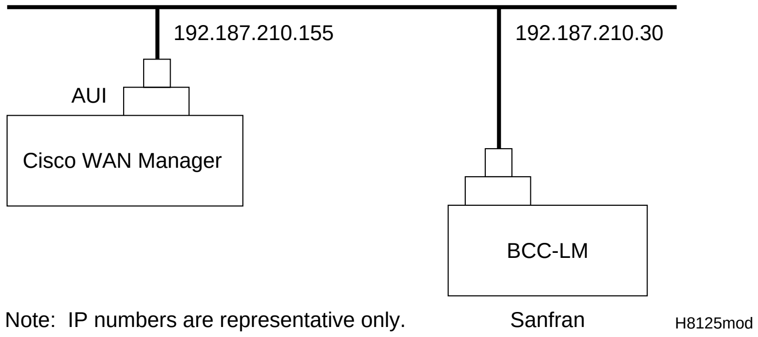
Note "Sockets" is the BSD Unix name for connections between processes, typically used in network communication.

Example of **dsplan** after Cisco WAN Manager has been started:

```
beta       TN    YourID.1       BPX 15    9.2      Dec. 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 12-3 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 12-3 Cisco WAN Manager LAN Connection to a BPX Switch (no gateway)



Note: IP numbers are representative only.

Configuring the MGX 8220 for Cisco WAN Manager NMS Operation (example)

Note The MGX 8220 was formerly referred to as the AXIS shelf.

At installation, initial access to the MGX 8220 is provided by the control port. The following is a brief overview of initial configuration. Refer to the *Cisco MGX 8220 Reference* manual for detailed information. Also refer to appropriate release notes for applicable firmware and software versions.

Step 1 Connect a terminal to the service port on the MGX 8220.

Step 2 Login.

```
login: “LoginID”

password:
card number: 3

xxxxAXIS.1.3.ASC.a >
```

Step 3 Name the shelf.

```
xxxxAXIS.1.3.ASC.a > cnfname nw1axi1
```

Step 4 Set the date.

```
nw1nw1axi1.1.3.ASC.a > cnfdate 05/02/96
```

Step 5 Set the time.

```
nw1saxi1.1.3.ASC.a > cnftime 15:31:00
```

Step 6 Enter **Help** for a list of commands.

```
nw1saxi1.1.3.ASC.a > Help
```

Step 7 Check versions of ASC, and Service Module (e.g., FRSM, AUSM) Firmware.

```
nw1axi1.1.3.ASC.a > version
*****     AXIS ASC Card *****2
    Firmware Version    = 2.1.12b_______
    Backup Boot version = model-B BT_2.0.0_______
    ASCFRSM Xilinx file = asc025.h
    ASCBNM Xilinx file  = bnmt3andsrefix
VxWorks  version 5.1.1-R3000.
Kernel: WIND version 2.4.
Made on Thu May 2 16:42:36 PDT 1996.
Boot line:
sl(0,0)

cc
```

Step 8 Enter Ethernet LAN port IP address.

```
nw1axi1.1.3.ASC.a > cnfifip
cnfifip "-ip <ip addr> -if <Interface> -msk <NetMask> -bc <Brocast addr>
"
  -ip <IP addr> where IP addr = nnn.nnn.nnn.nnn
  -if <Interface> where Interface = 26,28,37, 26: Ethernet, 28: Slip 37: ATM
  -msk <NetMask> where NetMask = nnn.nnn.nnn.nnn
  -bc <BrocastAddr> where BrocastAddr = nnnnnnnn,  n is hexdecimal, ethernet only


nw1axi1.1.3.ASC.a > cnfifip -ip 204.179.61.71 -if 26
```

You are configuring ethernet port are you sure? enter yes/no: yes

Step 9 Enter IP Relay Address for SNMP Management and Stats Collection.

```
nw1axi1.1.3.ASC.a > cnfifip -ip 204.179.55.105 -if 37
```

You are configuring atm port are you sure? enter yes/no: yes

Step 10 Configure stat master address (IP of Cisco WAN Manager workstation).

```
cnfstatsmgr "<ip address>"

nw1axi1.1.3.ASC.a > cnfstatsmgr 204.179.61.121      {this is IP address of Cisco
                                                     WAN Manager workstn}
```

Adding Virtual Trunks using BXM Cards

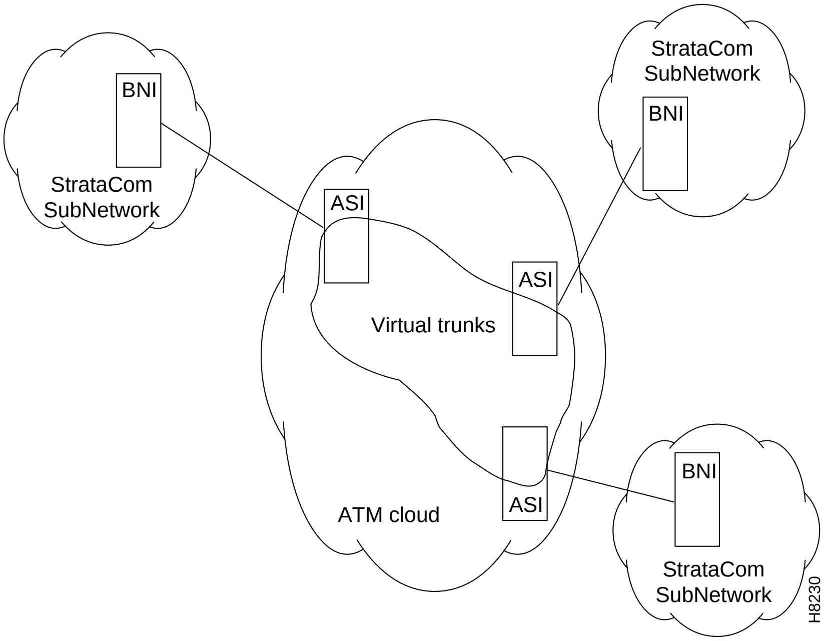
Starting with switch software Release 9.2, BXM cards support virtual trunks. For additional information, refer to Chapter 15, Configuration, BXM Virtual Trunks.

Adding Virtual Trunks using BNI and ASI Cards

This section details the steps 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 ASI and BNI firmware must be current. The following 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 an ASI UNI input at the ATM Cloud (see Figure 12-4). Proceed as follows:

Step 1 In the ATM cloud network, physically connect an ASI port at the cloud edge to each BNI port in the Cisco WAN Switching Network that is intended to have virtual trunks.

Figure 12-4 Virtual Trunks across a Cisco Wan Switching ATM Cloud



Step 2 Configure the cloud ASI ports. For each ASI port connected to a BNI virtual trunk port, do the following:

upln <slot.port>

upport <slot.port>

cnfport <slot.port> and set the *shift* parameter to "N" for no shift if the cloud contains BPX switches.

Note On an ASI connected to a CPE service line, shift on is used to shift the VCI bits in the ATM cell left four places. This results in a 12-bit VCI space rather than a 16-bit VCI space. These four bits are then used for ForeSight data. On the ASIs used to provide the UNI input to the ATM cloud, the shift off configuration must be set, so that these bits are not shifted again.

Step 3 Execute **addcon**. In the cloud network, add a virtual path ASI 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 ASI 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 configured with cnftrk in step 4.

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 CBR/VBR/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 ASI does not drop cells. These are values that Cisco recommends based on testing.

Step 4 Configure BNI virtual trunks. On the BNIs that connect to the cloud ASI ports, configure up to 32 virtual trunks, as follows:

uptrk <slot.port.vtrk>

cnftrk <slot.port.vtrk>

For **cnftrk**, make sure that the virtual trunk type and the VPI correspond to the ASI Virtual Path connections that have been set up.

addtrk <slot.port.vtrk>

Configuration, ATM Connections

This chapter describes how ATM connection services are established by adding ATM connections between ATM service interface ports in the network using ATM standard UNI 3.1 and Traffic Management 4.0. It describes BXM and ASI card operation and summarizes ATM connection parameter configuration

The chapter contains the following:

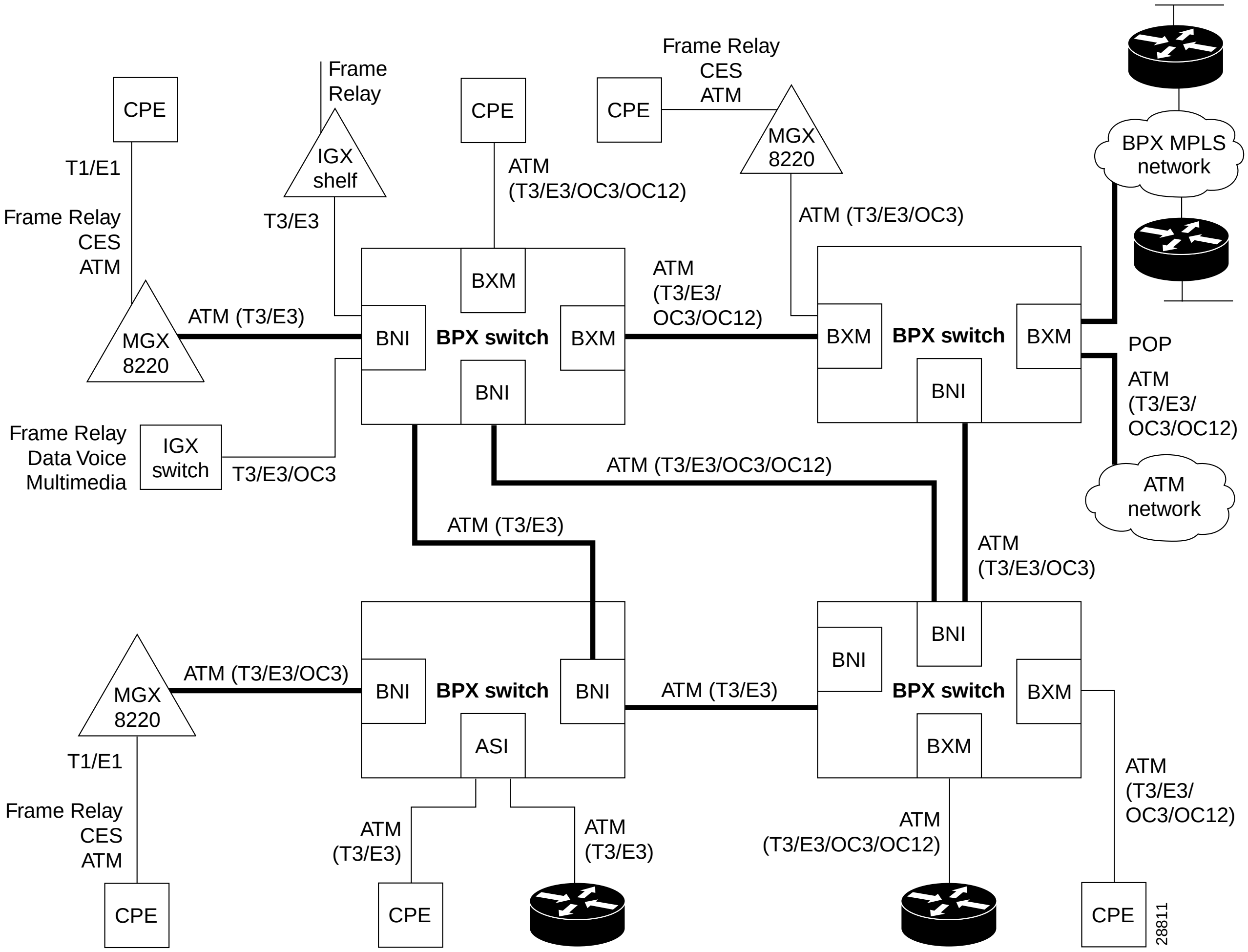
- ATM Connection Services
- SVCs
- Traffic Management Overview
- ATM Connection Requirements
- ATM Connection Flow
- rt-VBR and nrt-VBR Connections
- ATM Connection Configuration
- Traffic Policing Examples
- Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR
- LMI and ILMI Parameters

ATM Connection Services

ATM connection services are established by adding ATM connections between ATM service interface ports in the network. ATM connections can originate and terminate on the ASI (ATM Service Interface) cards, on BXM-T3/E3, BXM-155 (OC-3), and BXM-622 (OC-12) cards configured for port (service access) operation on the BPX switch, or on the MGX 8220 (using the AUSM card for the MGX 8220). Frame relay to ATM network interworking connections are supported between either BXM or ASI cards to the IPX, IGX, or MGX 8220. Frame relay to ATM service interworking connections are supported between either BXM or ASI cards to FRSM cards on the MGX 8220.

Figure 13-1 is a depiction of ATM connections over a BPX switch network. It shows ATM connections via BXM-T3/E3, BXM-155, BXM-622, ASI-1, and ASI-155 cards, as well as over MGX 8220 switches. It also shows Frame Relay to ATM interworking connections over the MGX 8220, IPX, and IGX shelves. For further information on the MGX 8220, refer to the *Cisco MGX 8220 Reference* document.

Figure 13-1 ATM Connections over a BPX Switch Network



SVCs

When an Extended Services Processor (ESP) is co-located with a BPX switch, ATM and Frame Relay Switched Virtual Circuits (SVCs) are supported in addition to Permanent Virtual Circuits (PVCs). For further information on ATM SVCs, refer to the *Cisco WAN Service Node Extended Services Processor Installation and Operation* document.

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 13-1 summarizes the major attributes of each of the traffic management classes:

Table 13-1 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		
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:

- PCR (Peak Cell Rate in cells/sec): the maximum rate at which a connection can transmit.
- CDVT (Cell Delay Variation Tolerance 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.
- MBS (Maximum Burst Size in cells): is the maximum number of cells that may burst at the PCR but still be compliant. This is used to determine the BT (Burst Tolerance) which controls the time scale over which the SCR (Sustained Cell Rate) is policed.
- MCR (Minimum Cell Rate in cells per second): is the minimum cell rated contracted for delivery by the network.

QoS (Quality of Service) parameters are defined as:

- CDV (Cell Delay Variation): a measure of the cell jitter introduced by network elements.
- Max CTD (Cell Transfer Delay): is the maximum delay incurred by a cell (including propagation and buffering delays.
- CLR (Cell Loss Ratio): is the percentage of transmitted cells that are lost.

Congestion Control Feedback:

- With ABR, provides a means to control flow based on congestion measurement.

Standard ABR notes:

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 13-2 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.

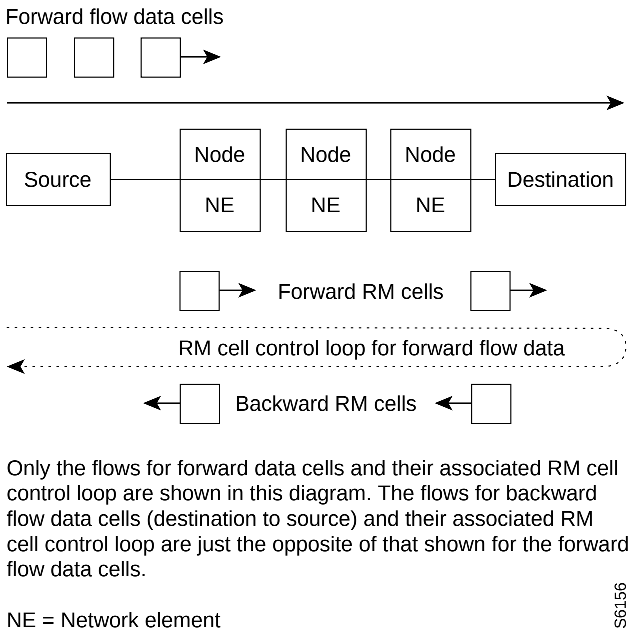
A source generates forward RM cells which are turned around by the destination and returned to the source as backward RM-cells. These backward RM-cells may carry feedback information from the network elements and/or the destination back to the source.

The parameter Nrm is defined as the maximum number of cells a source may send for each forward RM cell, i.e., 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), and Unspecified Bit Rate (UBR). ABR with VSVD supports explicit rate marking and Congestion Indication (CI) control.

Figure 13-2 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

ForeSight may be used for congestion control across BPX/IGX switches for connections that have one or both end points terminating on ASI-T3/E3 or BXM cards. 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. The BXM cards also support the VSVD congestion control mechanism as specified in the ATM Traffic Management 4.0 standards.

ATM Connection Requirements

There are two connection addressing modes supported. The user may enter a unique VPI/VCI address in which case the BPX switch functions as a virtual circuit switch. Or the user 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 AutoRoute feature once the connection endpoints are specified.

ATM connections can be added 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 as 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.

When adding ATM connections, first the access port and access service lines connecting to the customer CPE need to be configured. Also, the trunks across the network need to configured appropriately for the type of connection. Following that the **addcon** command may be used 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, the BXM is configured for port mode, a line is upped with the **upln** command and configured with the **cnfln** command. Then the associated port is configured with the **cnfport** command and upped with the **upport** command. Following this, the ATM connections are added via the **addcon** command with the syntax.

Connection Routing

ATM connections for a BXM or ASI card are identified as follows:

- slot number (in the BPX switch shelf where the BXM or ASI is located)
- port number (one of the ATM ports on the BXM or ASI)
- 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 AutoRoute feature is standard with all BPX, IGX, and IPX switches. The network automatically detects trunk failures and routes connections around the failures.

addcon Command Syntax

The following parameters are entered for the BXM **addcon** command. Depending upon the connection type, the user is prompted for the appropriate parameters as shown in the following:

```
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 runing Rel. 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 wil retain existing connection classes. Therefore, it won’t have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command.

Field	Value	Description
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, the user can instead enter a class number to select a pre-configured template, for example, class 4 for NTR-VBR, and class 3 for RT-VBR. The class of service templates can be modified as required using the **cnfcls/cnfatmcls** command and displayed using the **dspcls/dspatmcls** command.

Note For a new node running 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node will retain existing connection classes. Therefore, it won’t have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command.

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, using the **addcon** command, these service types are selected by entering one of the CLI service type entries shown in Table 13-2 when prompted:

Table 13-2 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 using the addcon command, these service types are selected by entering one of the CLI service type entries shown in Table 13-3 when prompted:

Table 13-3 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. 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.

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 13-3 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 on page 12*.

Note In this example, BXM cards are referenced. However, connection flow through BNI trunk and ASI service cards is similar, although they do not support all the features provided by BXM cards.

Ingress from CPE 1 to BXM 3

ATM cells from CPE 1 that are applied to BXM 3, Figure 13-3, 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, e.g., 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, etc.

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 on page 12*.

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.

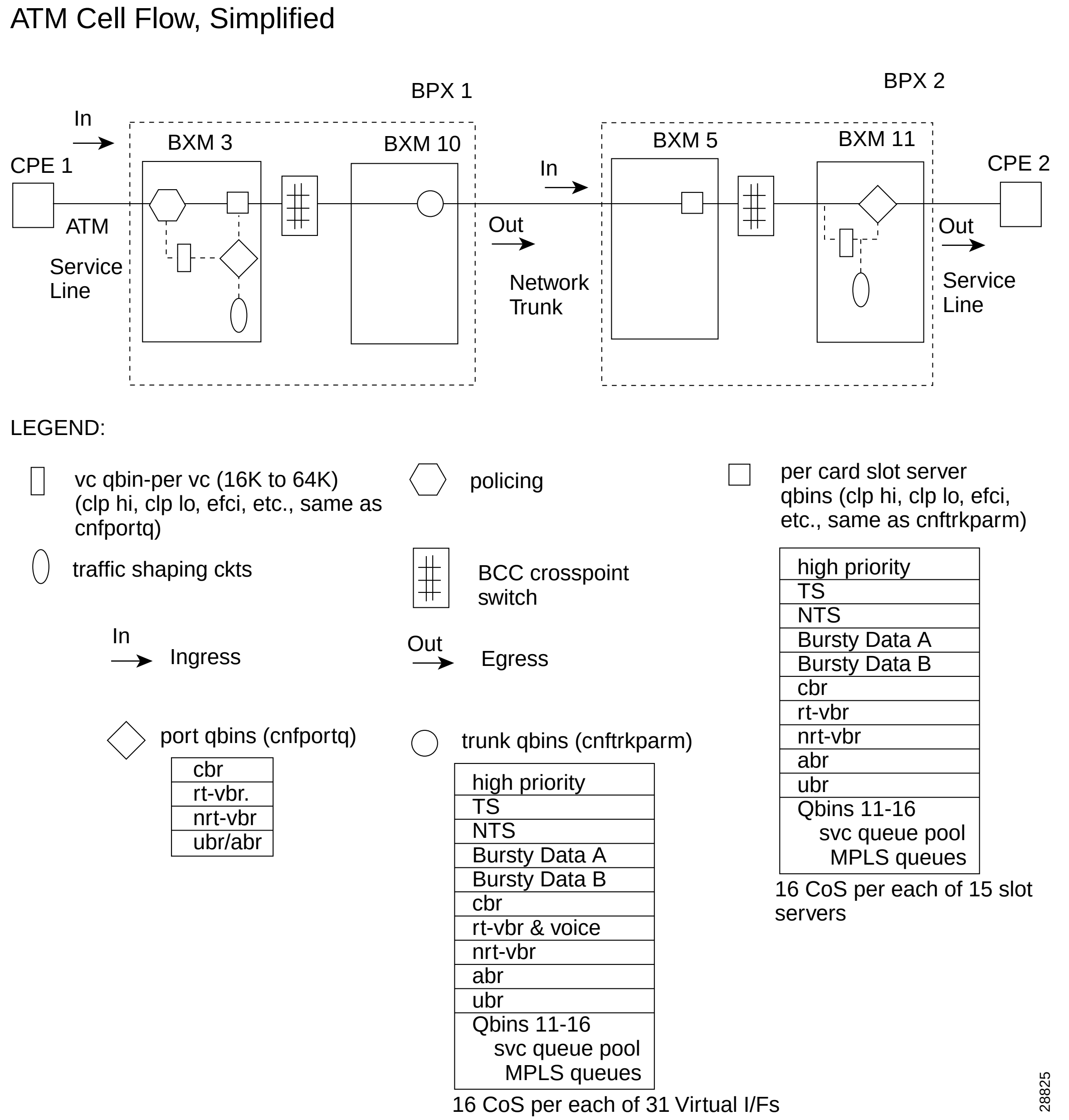
Cells are served out from the slot servers via the BPX backplane to the BCC crosspoint switch. The cells are served out on a fair basis with priority based on class of service, time in queue, bandwidth requirements, etc.

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, e.g., 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 13-3 ATM Connection Flow via BPX Switches



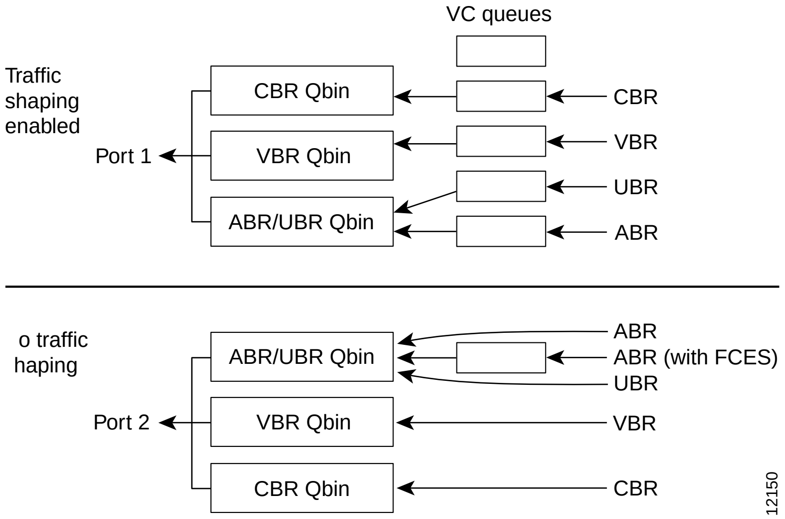
Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR

With the introduction of traffic shaping for CBR, VBR, and UBR, the user has 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 configured by the user for the connection.

Figure 13-4 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 13-4 Traffic Shaping Example



Traffic Shaping Rates

Traffic shaping rates are listed in Table 13-4.

Table 13-4 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. The **cnfport** and **cnfln** command is used to enable and disable the function on a per port basis. The cnftrk command is used 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 the user modifies the connection parameters. See the following examples of the **cnfln**, **cnfport**, and **cnftrk** commands:

Example of **cnfln**:

```
pubsbpx1       TN    silves    BPX 8620  9.2.2    Aug. 1 1999  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  9.2.2    Aug. 1 1999  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  9.2.2G    Aug. 1 1999  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

With Rel. 9.2.20 and later, rt-VBR and nrt-VBR connections are specified separately when adding a connection using the **addcon** command by entering 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 or ASI 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, and nrt-VBR connections are configured per class 2 service parameters. These class parameters can be changed using the **cnfcls/cnfatmcls** command, or the parameters can be entered individually for each connection by specifying 'yes' to the extended parameters prompt of the **addcon** command.

Note For a new node running software release 9.2.20 or later, the rt-VBR connection class number is 3. An upgraded node wil retain existing connection classes. Therefore, it won't have the rt-VBR connection class 3. However, the user can configure the connection classes to whatever service and parameters they want using the **cnfcls/cnfatmcls** command. For nrt-VBR connections in a new node, running 9.2.20, a number of connection classes are pre-configured, including 2, 4, 5, and 6.

Examplef cnfcls 3, for rt-VBR

```
pubsbpx1       TN    silves:1        BPX 8620  9.2.2G    July 16 1999 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%
- For rt-VBR connections, all nodes must be running at least Rel. 9.2.20. The user interface will block the addition of rt-VBR connections in a network running pre-9.2.20 SWSW.
- When upgrading to Rel. 9.2.20, all existing VBR connections are re-designated as nrt-VBR connections.
- BXM, ASI, and UXM (IGX switch) cards can terminate rt-VBR connections and support rt-VBR queues.
- On the BPX switch BXM and BNI trunks support rt-VBR queues, and on the IGX switch only UXM trunks support rt-VBR queues.
- In rel 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 trafficshould not be routed over FastPacket trunks.)
- With release 9.2.20, rt-vbr is supported only on single-segment connections (e.g., 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).

Connection Management

The BPX Command Line Interface (CLI) and Cisco WAN Manager accept the same connection policing and bandwidth parameters as in previous releases for both rt-VBR and nrt-VBR service.

The displayed **addcon** parameter prompts for both rt-VBR and nrt-VBR connections are the same. These prompts are: PCR, %util, CDVT, FBTC flag, SCR, MBS, and Policing Type.

There is no change in CDVT usage and the previous policing system.

When using the **addcon** command without the extended parameters, rt-VBR connections, automatically use the parameters provided by connection class 3 which contains pre-determined values. Similarly, nrt-VBR connections use connection class 2. The values of a connection class can be modified by using the **cnfcls**/**cnfatmcl** command. These values are displayed by the **dspcls**/**dspatmcls** commands.

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.

- The user can configure the Qbin values separately for rt-VBR and nrt-VBR classes on trunks 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.

The following 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. A user can configure these separately, 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  9.2.2G    July 16 1999 10:47 PDT

Port:       2.2     [ACTIVE  ]
Interface:          LM-BXM
Type:               UNI
Speed:              353208 (cps)

SVC Queue Pool Size:          0
CBR Queue Depth:              600     rt-VBR Queue Depth:                0
CBR Queue CLP High Threshold: 80%     rt-VBR Queue CLP High Threshold:   80%
CBR Queue CLP Low Threshold:  60%     rt-VBR Queue CLP Low/EPD Threshold: 60%
CBR Queue EFCI Threshold:     60%     rt-VBR Queue EFCI Threshold:       80%
nrt-VBR Queue Depth:          5000    UBR/ABR Queue Depth:               20000
nrt-VBR Queue CLP High Threshold: 80% UBR/ABR Queue CLP High Threshold:  80%
nrt-VBR Queue CLP Low Threshold:  60% UBR/ABR Queue CLP Low/EPD Threshold:60%
nrt-VBR Queue EFCI Threshold: 60%     UBR/ABR Queue EFCI Threshold:      20%


This Command: cnfportq 2.2
```

Related Switch Software Commands

The following 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.

Related Documentation

For additional information on CLI command usage, refer to the Release 9.2, Cisco WAN Switching Command Reference and Super User manuals.

ATM Connection Configuration

The following figures and tables describe the parameters used to configure ATM connections:

- Table 13-5, 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 13-6, 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 13-5 through Figure 13-10.
- Table 13-7, Connection Parameter Descriptions
  - This table defines the connection parameters listed in Table 13-6.

The following figures list the connection parameters in the same sequence as they are entered when a connection is added:

- Figure 13-5, CBR Connection Prompt Sequence
- Figure 13-6, rt-VBR and nrt-VBR Connection Prompt Sequence
- Figure 13-7, ABR Standard Connection Prompt Sequence

The following 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 13-8 is not available for ABR with ForeSight.

- Figure 13-8, Meaning of VSVD and Flow Connection External Segments

The following figures list the connection parameters in the same sequence as they are entered when a connection is added:

- Figure 13-9, ABR ForeSight Connection Prompt Sequence
- Figure 13-10, UBR Connection Prompt Sequence
- Figure 13-13, ATFR Connection Prompt Sequence
- Figure 13-14, ATFST Connection Prompt Sequence
- Figure 13-15, ATFT Connection Prompt Sequence
- Figure 13-16, ATFTFST Connection Prompt Sequence
- Figure 13-17, ATFX Connection Prompt Sequence
- Figure 13-18, ATFXFST Connection Prompt Sequence

Note With DAX connections, the trunk cell routing restriction prompt is not displayed since there is no trunking involved.

Table 13-5 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 13-6 Connection Parameters with Default Settings and Ranges

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC3 & OC12 RANGE	ASI T3/E3 RANGE	ASI-155 RANGE
PCR(0+1)[50/50]	50- T3/E3 cells/sec 50 - OC3 50 - OC12	T3: MCR – 96000 E3: MCR – 80000 Limited to MCR – 5333 cells/sec for ATFR connections.	OC3 (STM1): 0 – 353200

Table 13-6 Connection Parameters with Default Settings and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC3 & OC12 RANGE	ASI T3/E3 RANGE	ASI-155 RANGE
%Util [100/100] for UBR [1/1]	0 - 100%	1 - 100%	1 - 100%
MCR[50/50]	cells/sec 6 - T3/E3OC3/0C12	T3: 0 – 96000 cells/sec E3: 0 – 80000 cells/sec	N/A

FBTC (AAL5 Frame Base Traffic Control):
for rt/nrt-VBR [disable]
for ABR/UBR [enable]
for Path connection [disable]
	enable/disable
	Note With the BXM, FBTC means packet discard on queueing only.
		enable/disable
		Note With the ASI, FBTC means packet discard on both policing and queueing.
			enable/disable
			Note With the ASI, FBTC means packet discard on both policing and queueing.

CDVT(0+1):
for CBR [10000/10000],
others [250000/250000]
	0 - 5,000,000 usec	T3/E3 1 – 250,000 usecs.	OC3/STM1: 0 – 10000 usecs.

VSVD[disable]	enable/disable	enable/disable	Select disable, as only ABR w/o VSVD is supported.
FCES (Flow Control External Segment) [disable]	enable/disable	enable/disable	N/A
Default Extended Parameters[enable]	enable/disable	enable/disable	N/A
CLP Setting[enable]	enable/disable	enable/disable	enable/disable
SCR [50/50]	cells/sec 50 - T3/E3OC3/OC12	T3: MCR – 96000:T3 E3: MCR – 80000: E3 Limited to MCR – 5333 cells/sec for ATFR connections.	OC3/STM1: 0 – 353200
MBS [1000/1000]	1 - 5,000,000cells	T3/E3: 10 – 24000 cells	OC3 (STM1): 10 – 1000 cells
Policing[3] For CBR: [4]	1 - VBR.1 2 - VBR.2 3 - VBR.3 4 - PCR policing only 5 - off	1 - VBR.1 2 - VBR.2 3 - VBR.3 4 - PCR policing only 5 - off	1 - VBR.1 2 - VBR.2 3 - VBR.3 4 - PCR policing only 5 - off
ICR: max[MCR, PCR/10]	MCR - PCR cells/sec	MCR - PCR cells/sec	N/A
ADTF[1000]	62 - 8000 msec	1000 – 255000 msecs.	N/A
Trm[100]	ABRSTD: 1 - 100 msec ABRFST: 3 - 255 msec	20 – 250 msecs.	N/A
VC QDepth [16000/16000] For ATFR/ATFST [1366/1366]	0 - 61440 cells	Applies to T3/E3 only ABR: 1 – 64000 cells ATFR: 1 – 1366 cells	ATFR: 1 – 1366 cells

Table 13-6 Connection Parameters with Default Settings and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC3 & OC12 RANGE	ASI T3/E3 RANGE	ASI-155 RANGE
CLP Hi [80/80]	1 - 100%	1 – 100%	N/A
CLP Lo/EPD [35/35]	1 - 100%	1 – 100%	N/A
EFCI [30/30] For ATFR/ATFST [100/100]	1 - 100%	1 – 100%	0 - 100%
RIF:			N/A
For ForeSight: max[PCR/128, 10]	If ForeSight, then in absolute (0 - PCR)	If ForeSight, then in absolute (0 – PCR)	
For ABR STD[128]	If ABR then 2^n (1 - 32768)	If ABR, then 2^n (1 – 32768)	
RDF:			N/A
For ForeSight [93]	If ForeSight, then % (0% - 100%)	If ForeSight, then % (0% – 100%)	
For ABR STD [16]	If ABR then 2^n (1 - 32768)	If ABR, then 2^n (1 – 32768)	
Nrm[32], BXM only	2 - 256 cells	N/A	N/A
FRTT[0], BXM only	0 - 16700 msec	N/A	N/A
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	N/A	N/A
IBS[1/1]	0 - 24000 cells	T3/E3 ABR: 0 - 24000 cells ATFR: 1 - 107 cells	0 - 999 cells
Trunk cell routing restrict (Y/N) [Y]	Y/N	Y/N	Y/N

Table 13-7 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 13-7 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 ASI, FBTC means packet discard on both policing and queueing. With the BXM, FBTC means packet discard on queueing only.
VSVD	Virtual Source Virtual Destination: (see Meaning of VSVD and Flow Control External Segments, Figure 13-8)
FCES (Flow Control External Segments)	(see Meaning of VSVD and Flow Control External Segments, Figure 13-8)
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 13-5)
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. For ASI cards, regardless of the FBTC setting, this is the CLP Lo 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, i.e., 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, i.e. an RM cell must be sent for every Nrm-1 data cells
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

Table 13-7 Connection Parameter Descriptions (Continued)

Parameter	Description
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 (e.g., Fastpacket trunks).

CBR 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 13-5 in the sequence in which they occur during the execution of the **addcon** command. The CBR policing definitions are summarized in Table 13-8.

Figure 13-5 CBR Connection Prompt Sequence

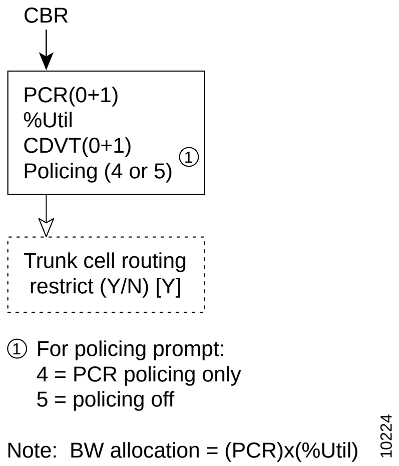


Table 13-8 CBR Policing Definitions

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

rt-VBR and nrt-VBR Connections

VBR (variable bit rate) connections may be classified as rt-VBR or nrt-VBR connections.

The rt-VBR (real-time variable bit rate) category is used for connections that transmit at a rate varying with time and that can be described as bursty, often requiring large amounts of bandwidth when active. The rt-VBR class is intended for applications that require tightly constrained delay and delay variation such as compressed voice video conferencing. For example, video conferencing which requires real-time data transfer with bandwidth requirements that can vary in proportion to the dynamics of the video image at any given time. The rt-VBR category is characterized in terms of PCR, SCR (sustained cell rate), and MBS (maximum burst size).

The nrt-VBR (non-real time variable bit rate) category is used for connections that are bursty but are not constrained by delay and delay variation boundaries. For those cells in compliance with the traffic contract, a low cell loss is expected. Non-time critical data file transfers are an example of an nrt-VBR connection. A nrt-VBR connection is characterized by PCR, SCR, and MBS.

Configuring VBR connections. The characteristics of rt-VBR or nrt-VBR are supported by appropriately configuring the parameters of the VBR connection.

Note When configuring a rt-VBR connection, the trunk cell routing restriction prompt does not occur, as rt-VBR connection routing is automatically restricted to ATM trunks.

The parameters for a VBR connection are shown in Figure 13-6 in the sequence in which they occur during the execution of the **addcon** command. The VBR policing definitions are summarized in Table 13-9.

Figure 13-6 rt-VBR and nrt-VBR Connection Prompt Sequence

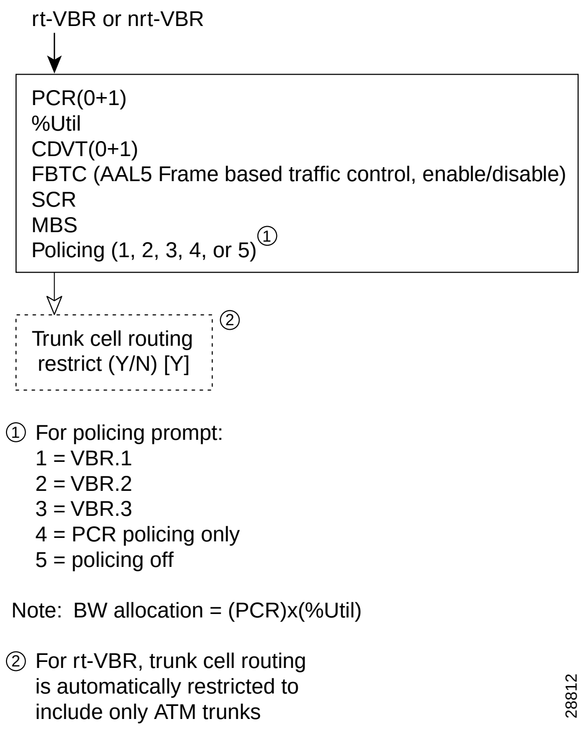

rt-VBR or nrt-VBR
PCR(0+1)
%Util
CDVT(0+1)
FBTC (AAL5 Frame based traffic control, enable/disable)
SCR
MBS
Policing (1, 2, 3, 4, or 5)①
②
Trunk cell routing restrict (Y/N) [Y]
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
Note: BW allocation = (PCR)x(%Util)
② For rt-VBR, trunk cell routing is automatically restricted to include only ATM trunks
28812

Table 13-9 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

ABR Notes

The term ABR is used to specify one of the following:

- ABR standard without VSVD (This is ABR standard without congestion flow control.)
  - — Supported by BXM, ASI-T3 (& ASI-E3), and ASI OC3 cards.
- ABR standard with VSVD. (This is ABR standard with congestion flow control as specified by the ATM Traffic Management, Version 4.0)
  - — Also, referred to as ABR.1.
  - — Supported only by BXM cards.
  - — Feature must be ordered.
- ABR with ForeSight congestion control
  - — Also, referred to as ABR.FST.
  - — Supported by BXM and ASI-T3 (& ASI-E3) cards.
  - — Feature must be ordered.

ABR Connections

The **ABR** (available bit rate) category utilizes a congestion flow control mechanism to control congestion during busy periods and to take advantage of available bandwidth during less busy periods. The congestion flow control mechanism provides feedback to control the connections flow rate through the network in response to network bandwidth availability. The ABR service is not restricted by bounding delay or delay variation and is not intended to support real-time connections. ABR is characterized by: PCR and MCR.

Policing for ABR connections is the same as for VBR connections which are summarized in Table 13-9.

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 13-7 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 13-8.

ABRSTD Connections

The **ABRSTD** connection uses VSVD congestion control.

The parameters for an ABRSTD connection are shown in Figure 13-9 in the sequence in which they occur during the execution of the **addcon** command

Figure 13-7 ABR Standard Connection Prompt Sequence

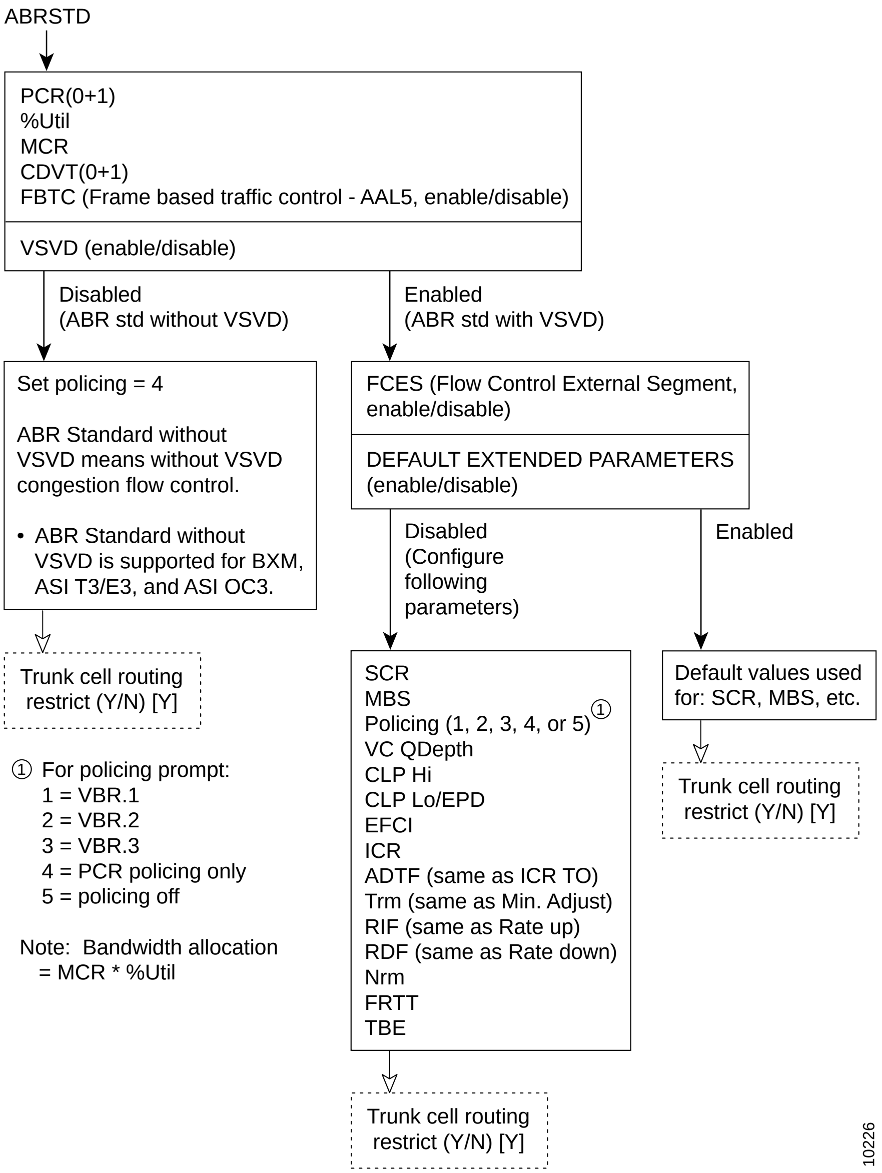
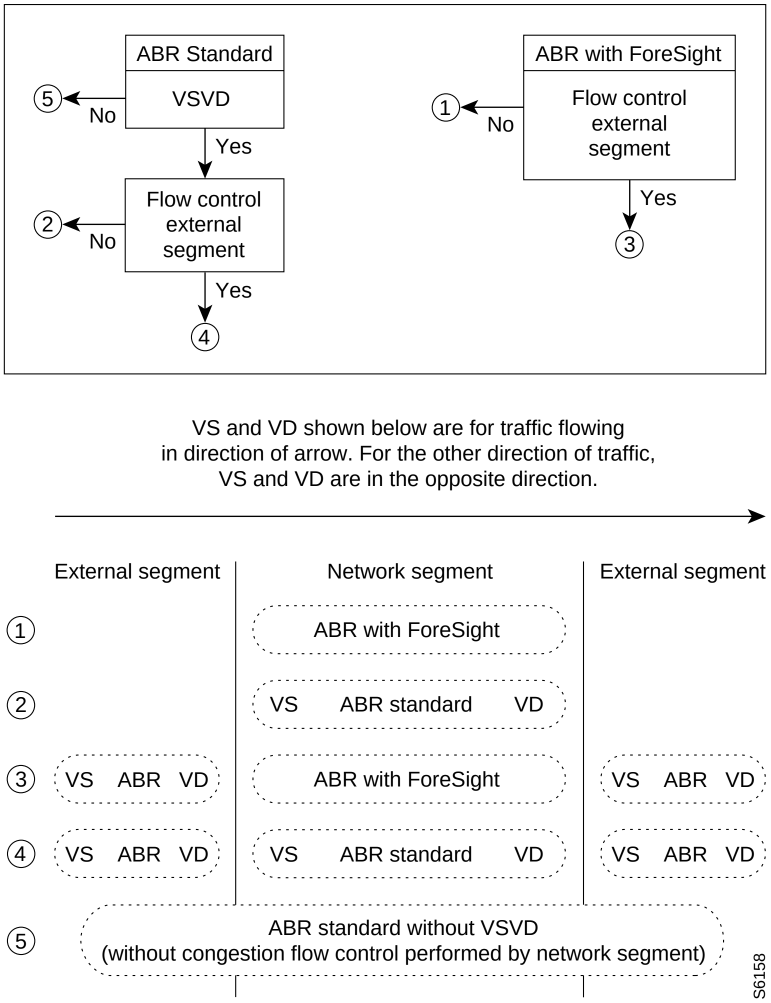

ABRSTD
PCR(0+1)
%Util
MCR
CDVT(0+1)
FBTC (Frame based traffic control - AAL5, enable/disable)
VSVD (enable/disable)
Disabled
(ABR std without VSVD)
Enabled
(ABR std with VSVD)
Set policing = 4
ABR Standard without VSVD means without VSVD congestion flow control.
• ABR Standard without VSVD is supported 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 13-8 Meaning of VSVD and Flow Control External Segments

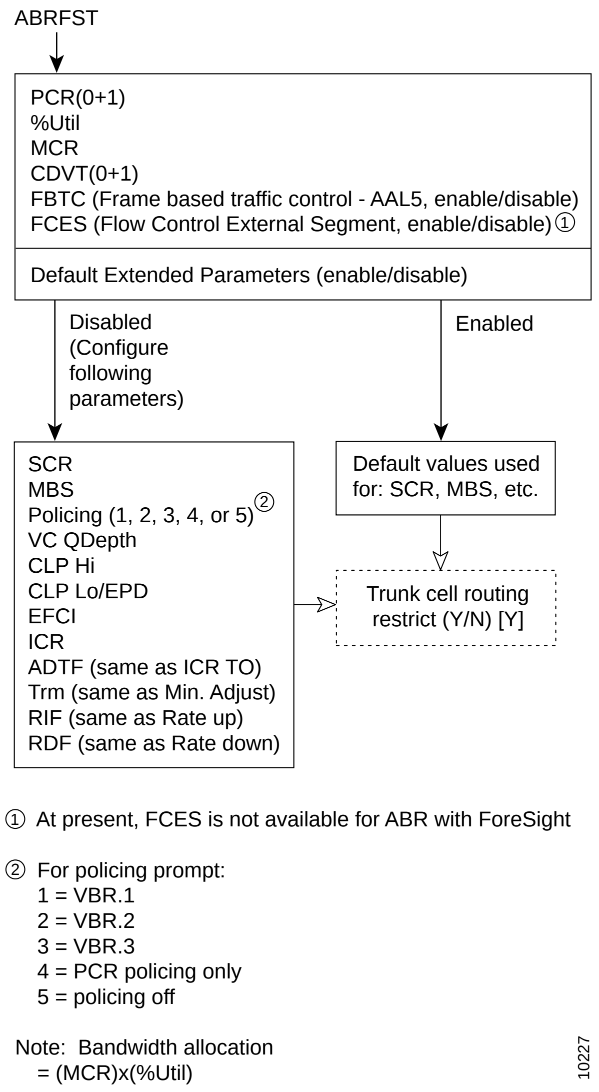

ABR Standard
VSVD
No
5
Yes
Flow control external segment
No
2
Yes
4
ABR with ForeSight
Flow control external segment
No
1
Yes
3
VS and VD shown below are for traffic flowing in direction of arrow. For the other direction of traffic, VS and VD are in the opposite direction.
External segment
Network segment
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

ABRFST Connections

The **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 13-9 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-9 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

UBR Connections

The unspecified bit rate (UBR) connection service is similar to the ABR connection service for bursty data. However, UBR traffic is delivered only when there is spare bandwidth in the network. This is enforced by setting the CLP bit on UBR traffic when it enters a port.

Therefore, traffic is served out to the network only when no other traffic is waiting to be served first. The UBR traffic does not affect the trunk loading calculations performed by the switch software.

The parameters for a UBR connection are shown in Figure 13-10 in the sequence in which they occur during the execution of the **addcon** command.

The UBR policing definitions are summarized in Table 13-10.

Figure 13-10 UBR Connection Prompt Sequence

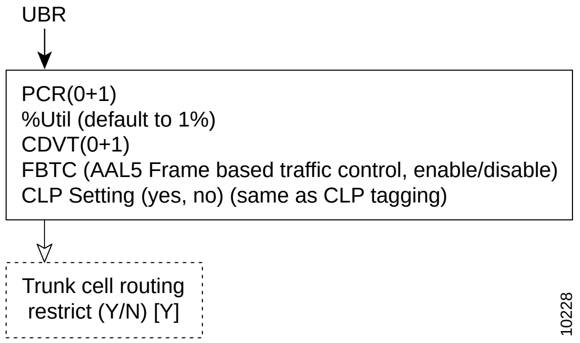

UBR
PCR(0+1)
%Util (default to 1%)
CDVT(0+1)
FBTC (AAL5 Frame based traffic control, enable/disable)
CLP Setting (yes, no) (same as CLP tagging)
Trunk cell routing restrict (Y/N) [Y]
10228

Table 13-10 UBR Policing Definitions

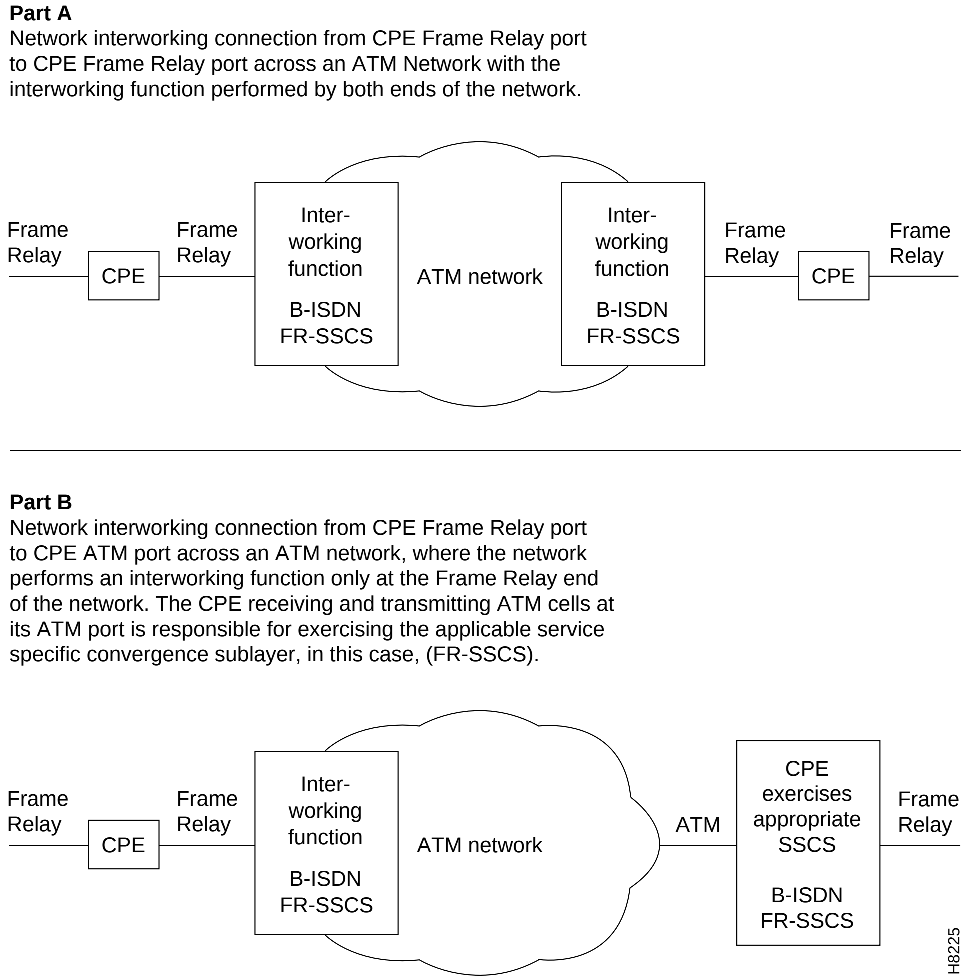
Connection Type	ATM Forum TM spec. 4.0 conformance definition	PCR Flow (1st leaky bucket)	CLP tagging (for PCR flow)	SCR Flow (2nd leaky bucket)	CLP tagging (for SCR flow)
UBR	**UBR.1** when CLP setting = no	**CLP(0+1)**	no	off	n/a
UBR	**UBR.2** when CLP setting = yes	**CLP(0+1)**	no	**CLP(0)**	**yes**

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 13-11 and Figure 13-12).

Two types of Frame Relay to ATM interworking are supported, Network Interworking and Service Interworking. The Network Interworking function is performed by the BTM card on the IGX switch. The FRSM card on the MGX 8220 supports both Network and Service Interworking.

Figure 13-11 Frame Relay to ATM Network Interworking



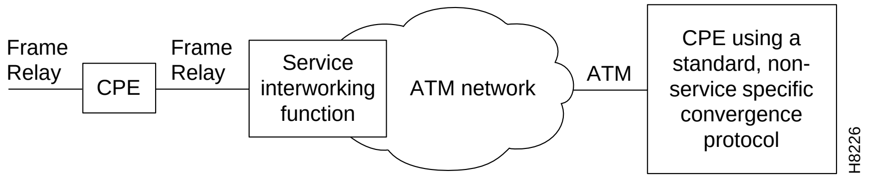
Part A

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 13-12 Frame Relay to ATM Service Interworking



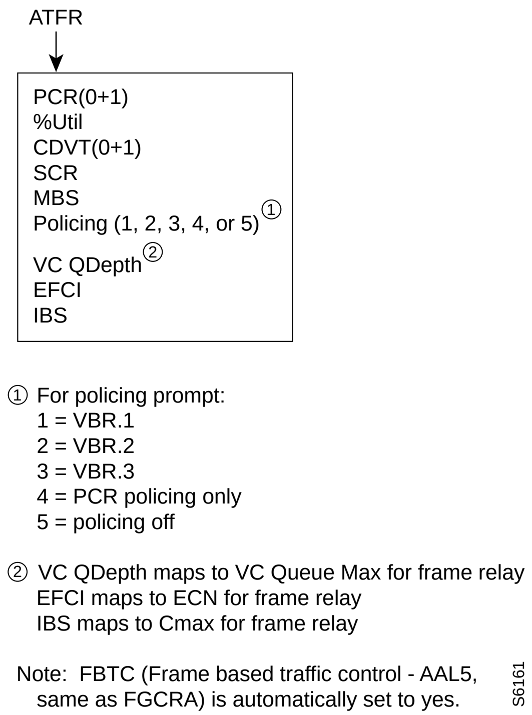
Frame Relay
CPE
Frame Relay
Service interworking function
ATM network
ATM
CPE using a standard, non-service specific convergence protocol
H8226

ATFR Network Interworking Connections

An **ATFR** (ATM to Frame Relay) 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 13-13 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-13 ATFR Connection Prompt Sequence

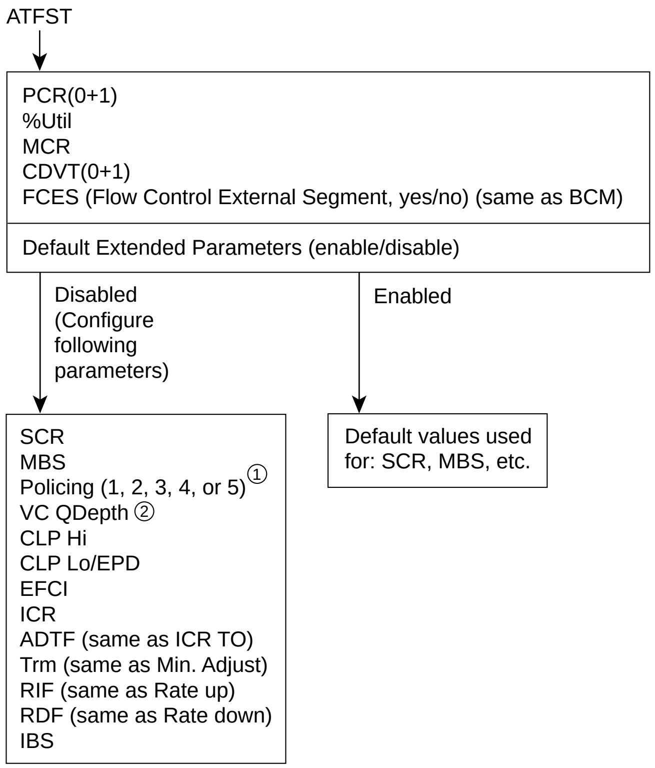

ATFR
PCR(0+1)
%Util
CDVT(0+1)
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
EFCI
IBS
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
② VC QDepth maps to VC Queue Max for frame relay
EFCI maps to ECN for frame relay
IBS maps to Cmax for frame relay
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.
S6161

ATFST Network Interworking Connection

An **ATFST** connection is a Frame Relay to ATM connection 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 13-14 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-14 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.

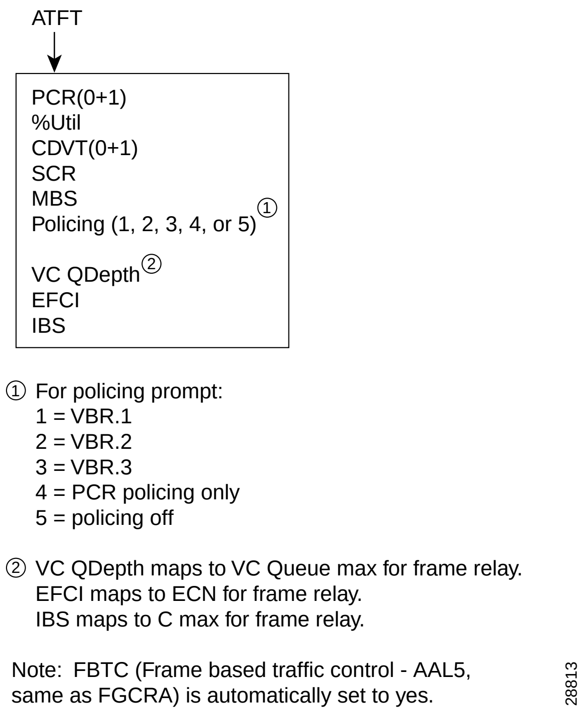
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.

ATFT Transparent Service Interworking Connections

An **ATFT** connection is a Frame Relay to ATM transparent Service Interworking connection and is configured as a VBR connection, with a number of the ATM and Frame Relay connection parameters being mapped between each side of the connection..

The parameters for an ATFT connection are shown in Figure 13-15 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-15 ATFT Connection Prompt Sequence

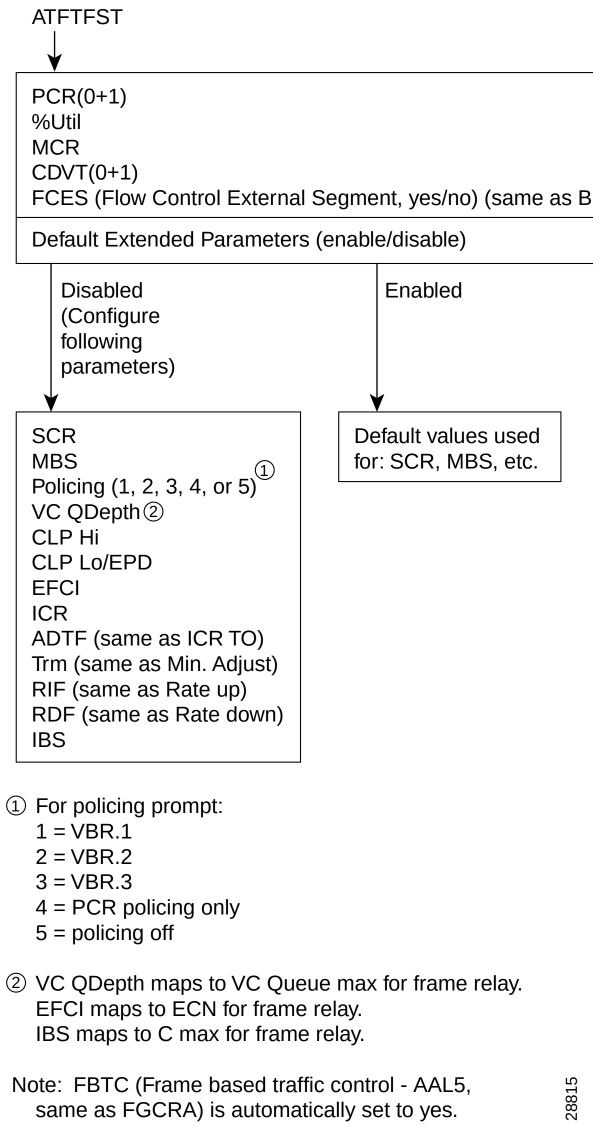

ATFT
PCR(0+1)
%Util
CDVT(0+1)
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
EFCI
IBS
① For policing prompt:
1 = VBR.1
2 = VBR.2
3 = VBR.3
4 = PCR policing only
5 = policing off
② VC QDepth maps to VC Queue max for frame relay.
EFCI maps to ECN for frame relay.
IBS maps to C max for frame relay.
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.
28813

ATFTFST Transparent Service Interworking Connections

An **ATFTFST** connection is a Frame Relay to ATM transparent Service Interworking connection that is configured as an ABR connection with ForeSight. ForeSight congestion control is automatically enabled when connection type ATFTFST is selected. A number of the ATM and Frame Relay connection parameters are mapped between each side of the connection.

The parameters for an ATFTFST connection are shown in Figure 13-16 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-16 ATFTFST Connection Prompt Sequence

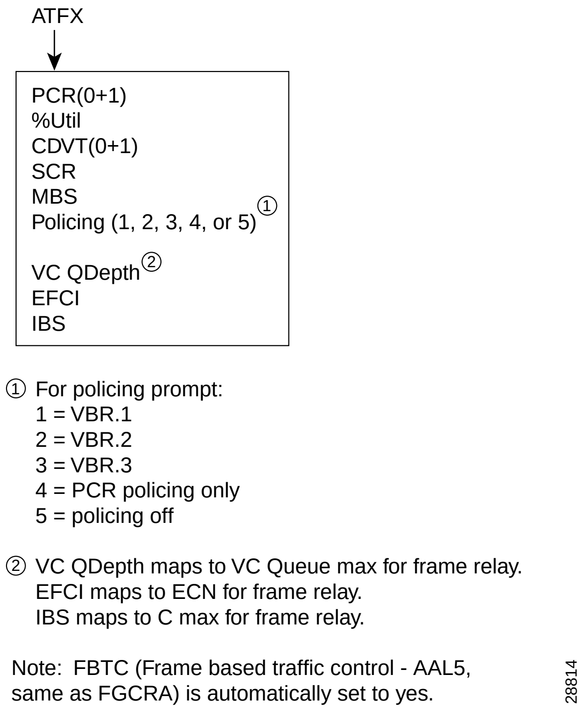

ATFTFST
PCR(0+1)
%Util
MCR
CDVT(0+1)
FCES (Flow Control External Segment, yes/no) (same as BCM)
Default Extended Parameters (enable/disable)
Disabled (Configure following parameters)
Enabled
SCR
MBS
Policing (1, 2, 3, 4, or 5) ①
VC QDepth ②
CLP Hi
CLP Lo/EPD
EFCI
ICR
ADTF (same as ICR TO)
Trm (same as 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

ATFX Translational Service Interworking Connections

An **ATFX** connection is a Frame Relay to ATM translational Service Interworking connection and is configured as a VBR connection, with a number of the ATM and Frame Relay connection parameters being mapped between each side of the connection..

The parameters for an ATFX connection are shown in Figure 13-17 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-17 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.

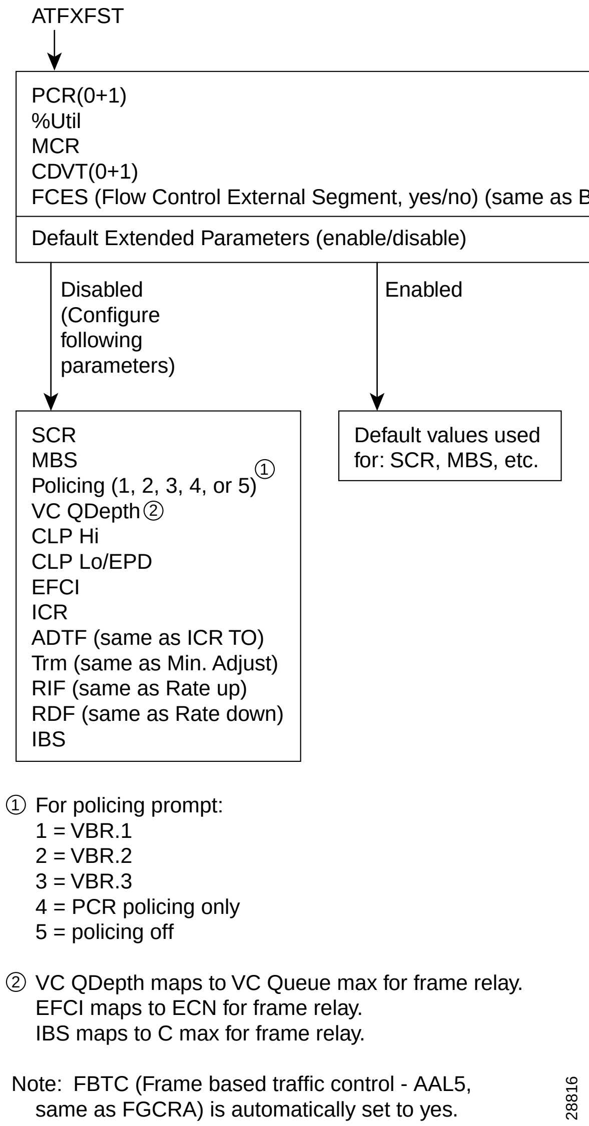
Note: FBTC (Frame based traffic control - AAL5, same as FGCRA) is automatically set to yes.

ATFXFST Translational Service Interworking Connections

An **ATFXFST** connection is a Frame Relay to ATM translational Service Interworking connection that is configured as an ABR connection with ForeSight. ForeSight congestion control is automatically enabled when connection type ATFXFST is selected. A number of the ATM and Frame Relay connection parameters are mapped between each side of the connection.

The parameters for an ATFXFST connection are shown in Figure 13-18 in the sequence in which they occur during the execution of the **addcon** command.

Figure 13-18 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 GCRA viewpoint is as follows:

- 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.

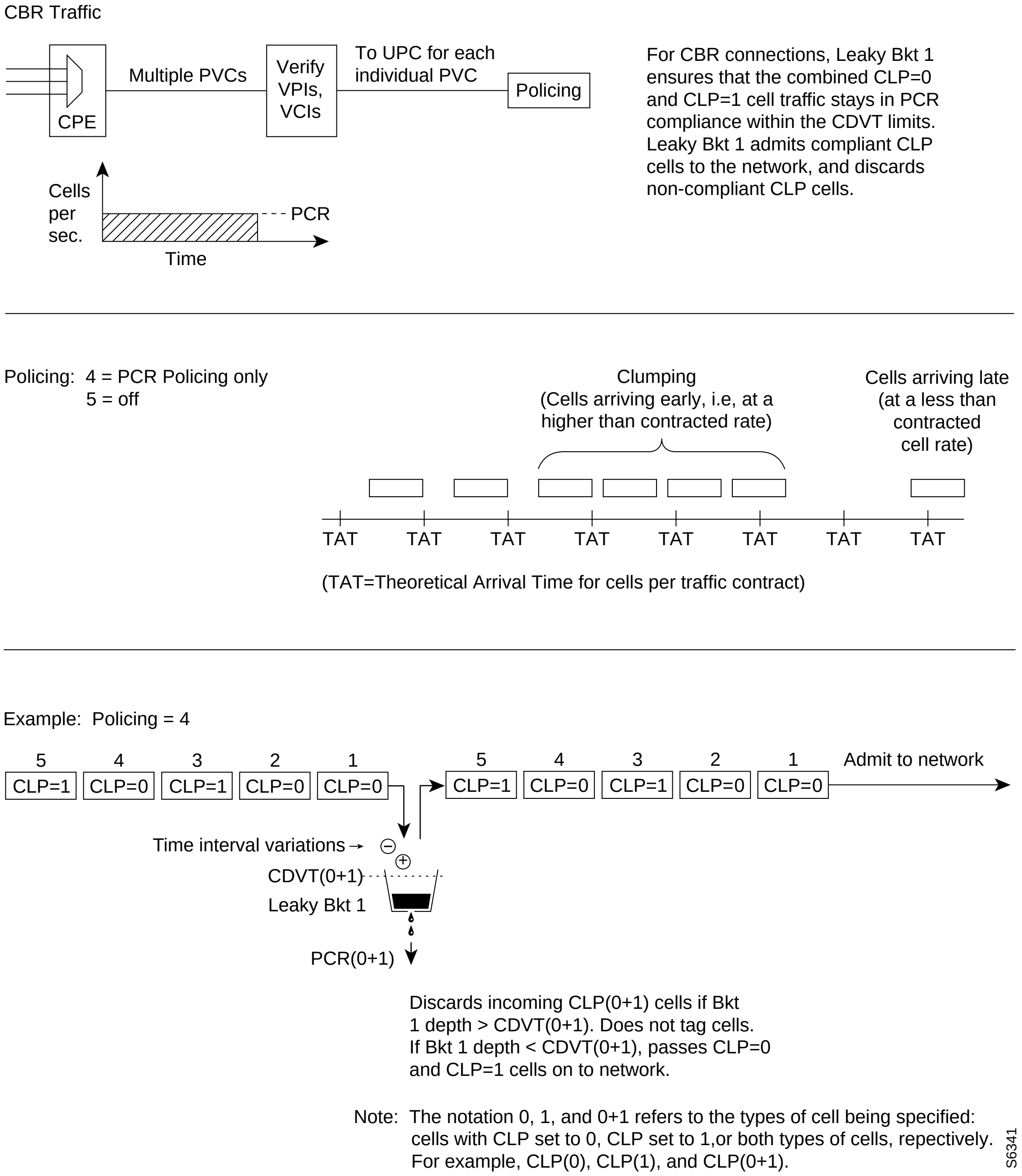
When a connection is added, a VPI.VCI address is assigned, and the UPC parameters are configured for the connection. For each cell in an ATM stream seeking admission to the network, the VPI.VCI addresses are verified and each cell is checked for compliance with the UPC parameters. The CBR cells are not 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

The CBR connection may be configured 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 13-19. 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 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 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 13-19 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)
S6341

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 13-20 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 13-20 CBR.1 Connection with Bucket Compliant

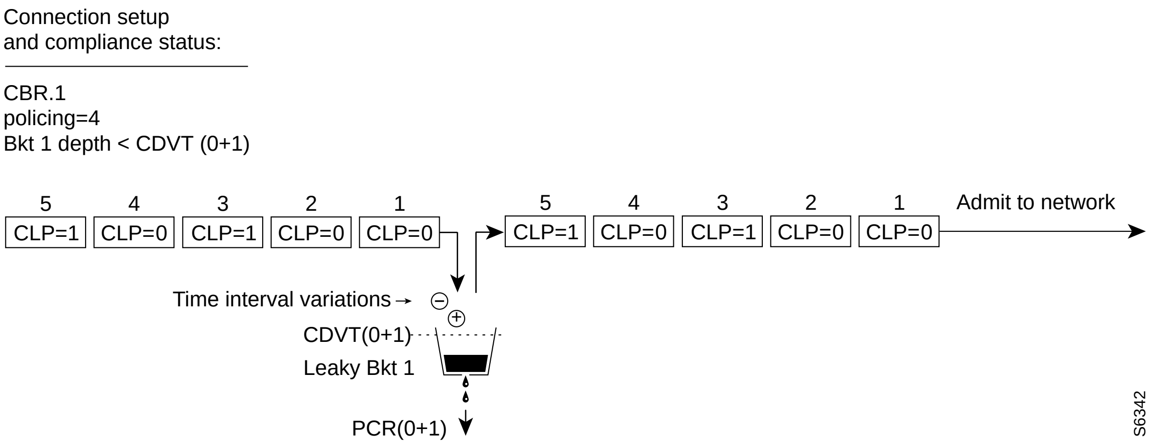
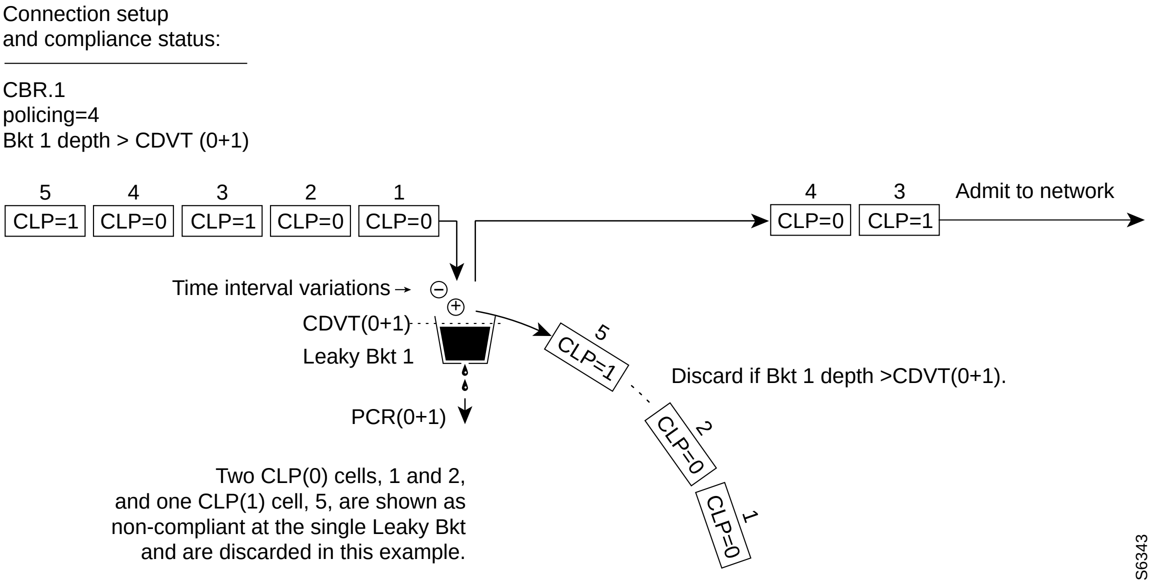


Figure 13-21 shows a CBR connection policing example, with policing =4, where the CDVT(0+1) of the single leaky bucket is exceeded and non-compliant cells are discarded. The leaky bucket only discards cells; it does not tag them

Figure 13-21 CBR.1 Connection, with Bucket Discarding non-Compliant Cells



VBR Dual-Leaky Bucket Policing Examples

The contract for a variable bit rate 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 13-22.

The VBR cells are not enqueued, but are processed by the policing function and then sent to the network unless discarded.

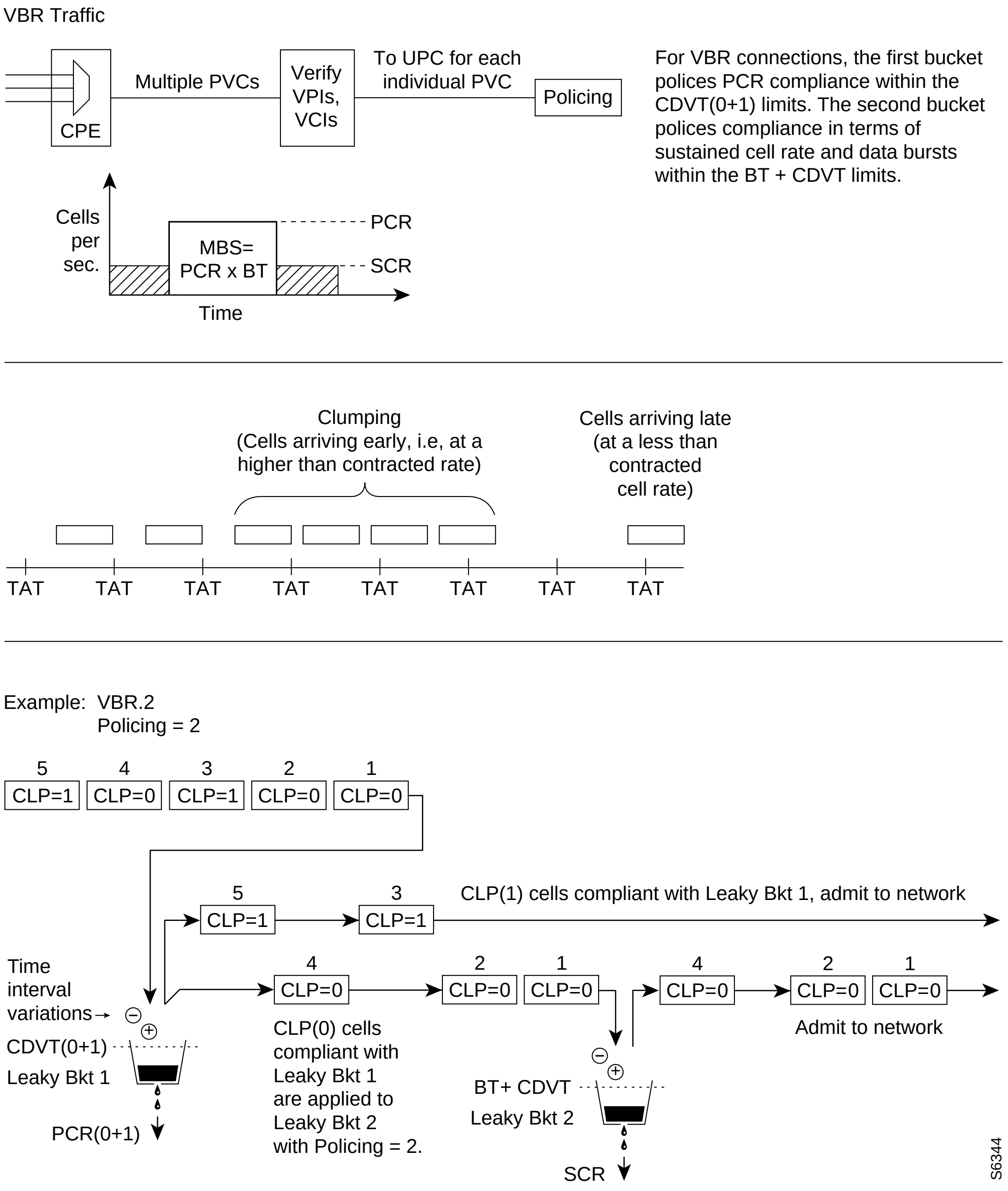
For VBR, traffic policing, depending on selected policing option, is based on:

- Leaky bucket 1, PCR and CDVT
- Leaky bucket 2, SCR, CDVT, and MBS

The policing options, selected by entering 1-5 in response to the policing choice prompt, are as follows 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 13-22 VBR Connection, UPC Overview



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.

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 13-23 shows a VBR connection policing example, with policing set to 4, leaky bucket 1 compliant, and all cells being admitted to the network.

Figure 13-23 VBR Connection, Policing = 4, Leaky Bucket 1 Compliant

.

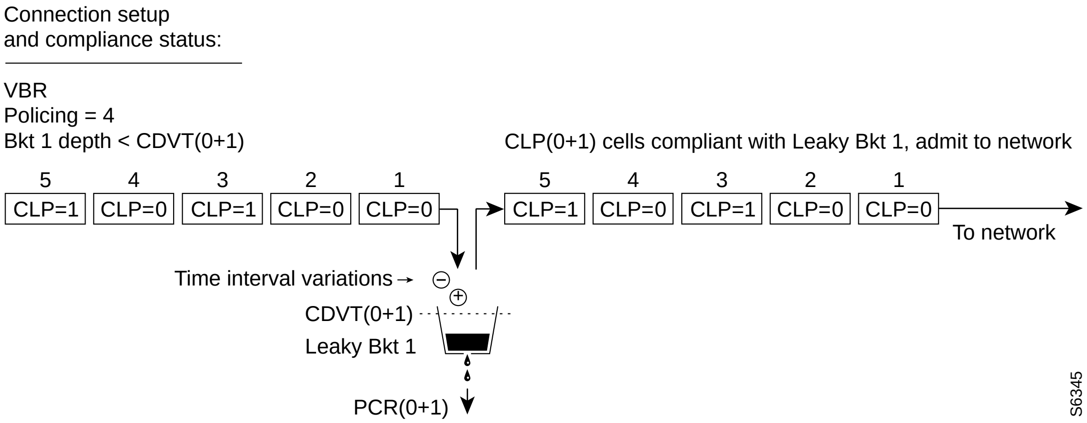


Figure 13-24 shows a VBR connection policing example, with the policing set to 4, and leaky bucket 1 non-compliant which indicates that the connection has exceeded the PCR for a long enough interval to exceed the CDVT (0+1) limit. Non-compliant cells with respect to leaky bucket 1 are discarded.

Figure 13-24 VBR Connection, Policing = 4, Leaky Bucket 1 Non-Compliant

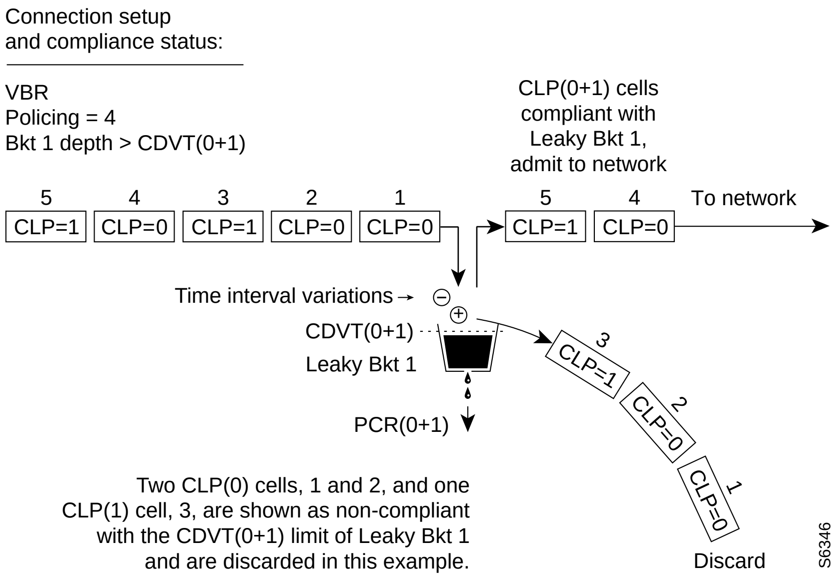


Figure 13-25 shows a VBR.2 connection policing example, with policing = 2, and both buckets compliant. Leaky bucket two is policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with the SCR sustained cell rate.

Figure 13-25 VBR.2 Connection, Policing = 2, with Buckets 1 and 2 Compliant

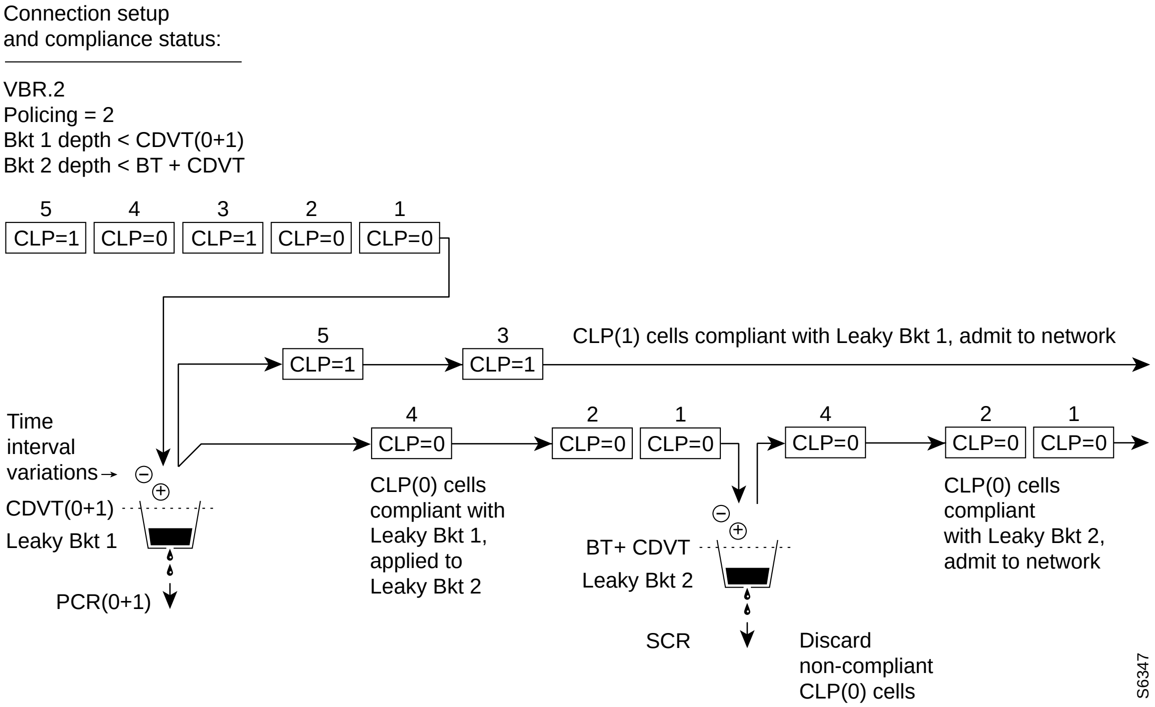


Figure 13-26 shows a VBR.2 connection policing example, with policing set to 2, and leaky bucket 2 non-compliant. Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR (sustained cell rate). In this example (policing set to 2), CLP tagging is not enabled, so 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 13-26 VBR.2 Connection, Leaky Bucket 2 Discarding CLP (0) Cells

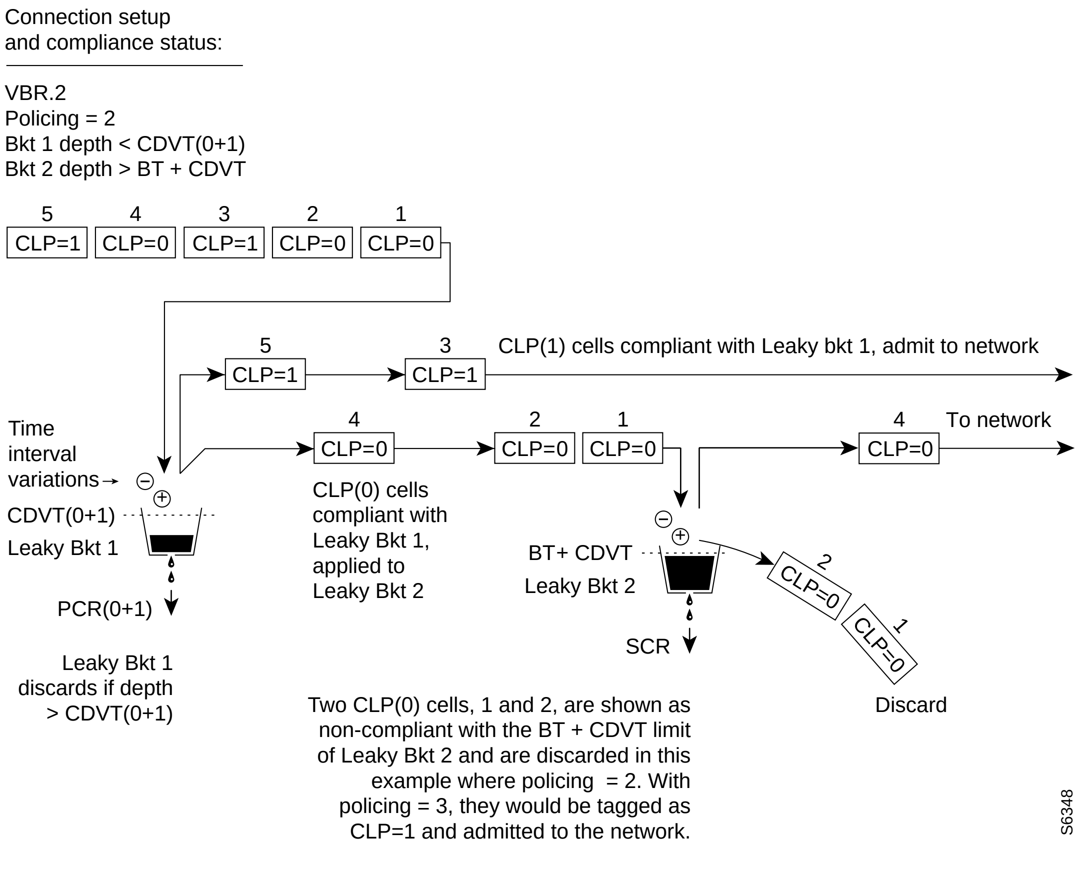

Connection setup
and compliance status:
VBR.2
Policing = 2
Bkt 1 depth < CDVT(0+1)
Bkt 2 depth > BT + CDVT
5 CLP=1
4 CLP=0
3 CLP=1
2 CLP=0
1 CLP=0
5 CLP=1
3 CLP=1
CLP(1) cells compliant with Leaky bkt 1, admit to network
Time interval variations→
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
Leaky Bkt 1 discards if 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
4 CLP=0
To network
2 CLP=0
1 CLP=0
Discard
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 13-27 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 13-27 VBR.1 Connection, Policing = 1, with Buckets 1 and 2 Compliant

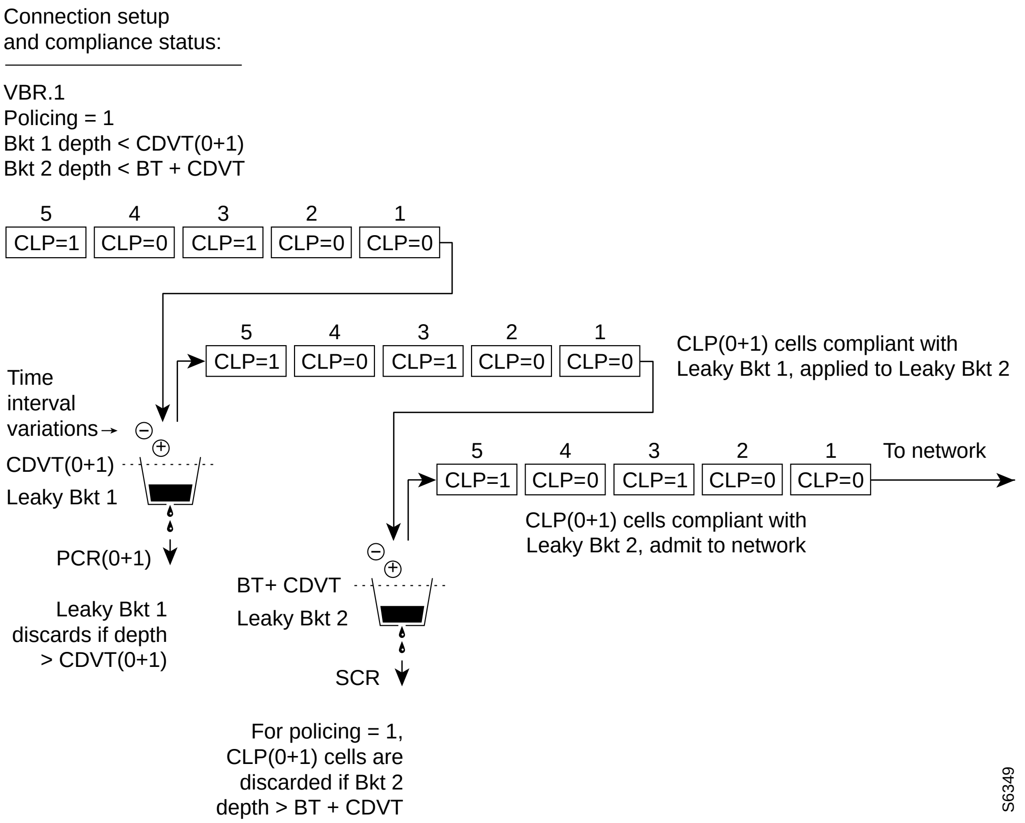
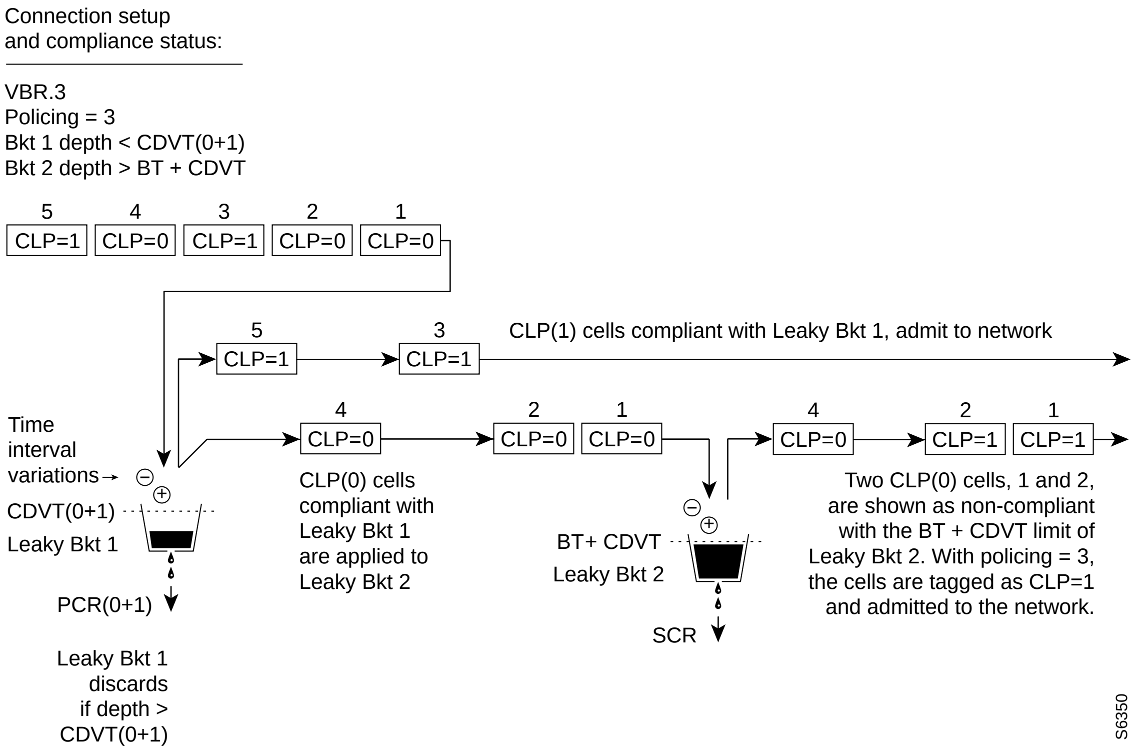


Figure 13-28 shows a VBR.3 connection policing example, with policing set to 3, and Leaky bucket 2 shown as non-compliant. Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR sustained cell rate. For the 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 13-28 VBR.3 Connection, Policing = 3, with Bucket 2 non-compliant


Connection setup
and compliance status:
VBR.3
Policing = 3
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
2
CLP=1
1
CLP=1
Time interval variations
CDVT(0+1)
Leaky Bkt 1
PCR(0+1)
Leaky Bkt 1 discards if depth > CDVT(0+1)
CLP(0) cells compliant with Leaky Bkt 1 are applied to Leaky Bkt 2
BT+ CDVT
Leaky Bkt 2
SCR
Two CLP(0) cells, 1 and 2, are shown as non-compliant with the BT + CDVT limit of Leaky Bkt 2. With policing = 3, the cells are tagged as CLP=1 and admitted to the network.
S6350

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 13-29.

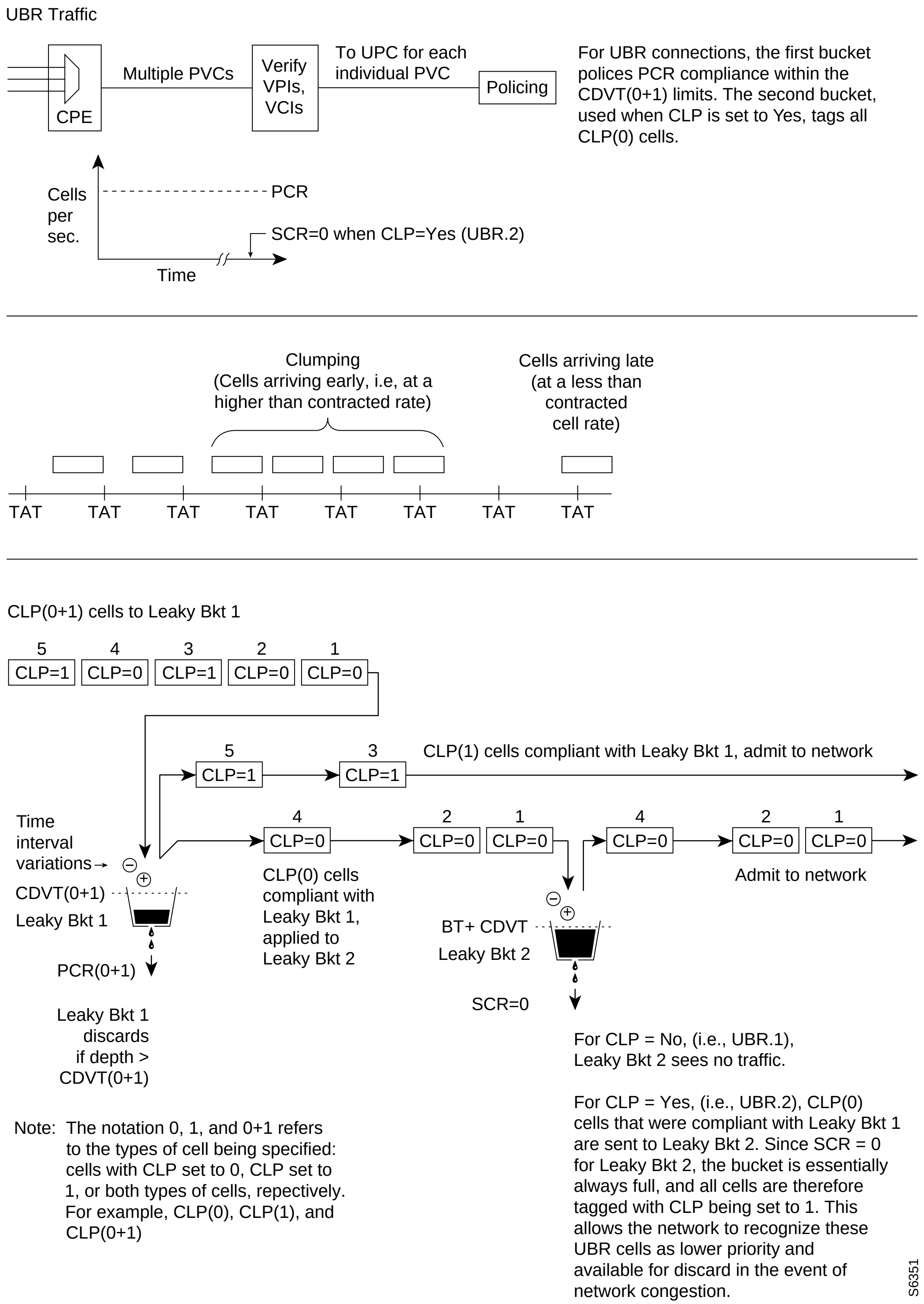
Leaky Bucket 1

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 % utilization default of 1%.

Leaky Bucket 2

When CLP=Yes (UBR.2), CLP(0) cells that are compliant with leaky bucket 1 are sent to leaky bucket 2. Since 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 13-29 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)
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
Leaky Bkt 1 discards if depth > CDVT(0+1)
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)

LMI and ILMI Parameters

The following is a listing of the LMI and ILMI parameters for the ASI and BXM:

For ILMI information, refer to Table 13-11.

Table 13-11 ILMI Parameters

Parameter	Description
VPI.VCI	VCCI for ILMI signaling channel equal 0.16
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.
Addr Reg Enab	SVC Address Registration procedures enabled.

For the LMI information, refer to Table 13-11.

LMI Parameters

Parameter	Description
VPI.VCI	VCCI 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

LMI and ILMI Enhancements on BXM

LMI and ILMI functions for the BXM card are moved to the card from the BCC to localize these functions. These functions support virtual UNIs and trunk ports - a total of 256 sessions on different interfaces (ports, trunks, virtual UNIs) per BXM.

Early Abit Notification with Configurable Timer on ILMI/LMI Interface

The time to reroute connections varies depending on different parameters, such as the number of connections to reroute, reroute bundle size, etc. It is important to notify the CPE if a connection is derouted and fails to transport user data after a specified time interval. However, it is also desirable not to send out Abit = 0, then Abit =1 when a connection is derouted and rerouted quickly. Such notifictions may prematurely trigger the CPE backup facilities causing instabilities in an otherwise stable system.

The early Abit Notification with configurable timer feature provides a way to send Abit = 0 status changes over the LMI interface or to send ILMI traps over the ILMI interface after connections are derouted a certain amount of time. The time period is configurable. The configurable time allows the user the flexibility to synchronize the operation of the primary network and backup utilities, such as dialed backup over the ISDN or PSTN network. The feature can be turned on using the **cnfnodeparm** command. For further information, refer to the *Rel. 9.2.20 Cisco WAN Switching Command Reference*.

CHAPTER 14

Configuration BXM: PVCs, SVCs, and SPVCs

This chapter includes a brief overview of the BXM card sets and instructions for configuring the BXM. It also describes resource partitioning for the BPX switch. The resource partitioning section provides procedures for UNI port resource partitioning for the BXM and ASI and procedures for NNI or trunk resource partitioning for the BXM and BNI.

The chapter includes the following:

- Label Switching
- Dynamic Resource Partitioning for SPVCs
- BXM Cards
- User Commands
- Configuring Connections
- Command Line Interface Examples
- Configuring the BPX Switch for SVCs
- Configuring the MGX 8220
- Resource Partitioning

Label Switching

Starting with switch software Release 9.1, the BXM also supports label switching. Partitions for the BXM can be allocated either between:

- SVCs and PVCs

  or

- Tag switching virtual circuits (TVCs) and PVCs

For information on Tag Switching, refer to *Chapter 19, Configuration General, MPLS on BPX Switch*.

Dynamic Resource Partitioning for SPVCs

Also, with switch software Release 9.1, the BXM card supported dynamic resource partitioning to support the conversion of PVCs to soft permanent virtual circuits (SPVCs). This feature is described in the *Cisco WAN Service Node Extended Services Processor Installation and Operations* for Release 2.2 document.

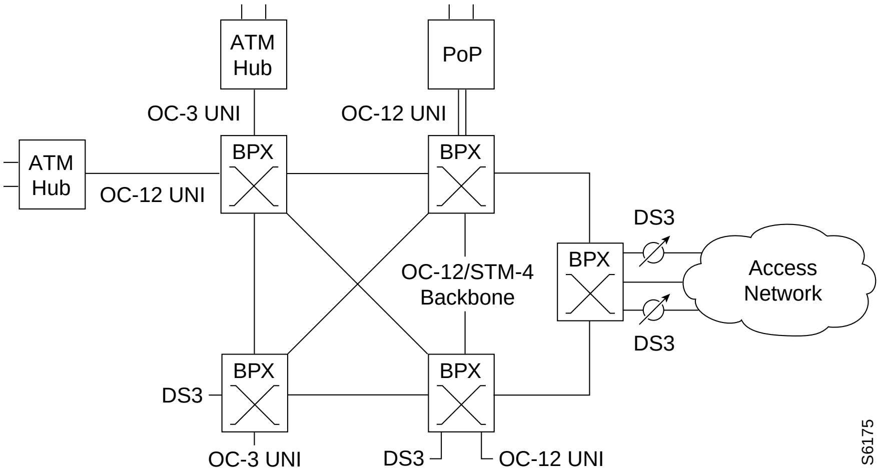
BXM Cards

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 of 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 14-1.

The BXM card group includes the BXM-T3/E3, BXM-155, and BXM-622. These cards may be configured to support either trunk (network) or port (service access) interfaces. The BXM T3/E3 is available in 8 or 12 port versions with T3/E3 interfaces. The BXM-155 is available in 4 or 8 port versions with OC-3/STM-1 interfaces. The BXM-622 is available in 1 or 2 port versions with OC-12/STM-4 interfaces. The BXM card sets 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 13, Configuration, ATM Connections*.

Figure 14-1 A BPX Switch Network with BXM Cards



The BXM cards are designed to support all the following service classes: Constant Bit Rate (CBR), real time and non real time Variable Bit Rate (rt-VBR and nrt-VBR), Available Bit Rate (ABR with VSVD, ABR without VSVD, and ABR using ForeSight), and Unspecified Bit Rate (UBR). ABR with VSVD supports explicit rate marking and Congestion Indication (CI) control.

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 14-1and Table 14-2 list the available front and back card options for the BXM-T3/E3, BXM-155, and BXM-622.

Table 14-1 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/34Mbps)		
BXM-T3-8	8	100K/130K	16K/32K[1]	BPX-T3/E3-BC
BXM-E3-8	8	100K/130K	16K/32K[1]	BPX-T3/E3-BC
BXM-T3-12	12	100K/230K	16K/32K[1]	BPX-T3/E3-BC
BXM-E3-12	12	100K/230K	16K/32K[1]	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/32K[1]	SMF-622 SMFLR-622 SMFXLR-622

[1] 32K conns are supported when stats level 0 is turned on. It does not support per-VC nor per-VP queuing, no VSI support, and this card is used only for trunks. Support for 32K conns and stats level 0 cannot be guaranteed in future firmware upgrades (MFJ+); therefore, it should be used cautiously.

*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 14-2 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

User Commands

This section provides a preliminary summary of configuration, provisioning, and monitoring commands associated with the BXM cards. These commands apply to initial card configuration, line and trunk configuration and provisioning, and connection configuration and provisioning.

New or modified commands include but are not limited to:

Connection Provisioning

- **addcon**-add connection
- **cnfcon**-configure connection
- **dspcon**-display connection

Diagnostics

- **addlnloclp**-add local loopback to line
- **addlnlocrmtlp**-add local remote loopback to line
- **dellnlp**-delete local or remote loopback

Test

- **tstconseg**-test connection externally with OAM segment loopback cells
- **tstdelay**-test connection round trip delay

Statistics

- Line and Trunk statistics
    - **cnflnstats**-configure line statistics collection
    - **dsplnstatcnf**-display statistics enabled for a line
    - **dsplnstathist**-display statistics data for a line
    - **cnftrkstat**s-configure trunk statistics collection
    - **dsptrkstatcnf**-display statistics enabled for a trunk
    - **dsptrkstathist**-display statistics data for a trunk
- Channel Statistics
    - **cnfchstats**-configure channel statistics collection
    - **dspchstatcnf**-display statistics configuration for a channel
    - **dspchstathist**-display statistics data for a channel
    - **dspchstats**-display channel statistics (multisession permitted)
- Line Statistics
    - **cnfslotalm**-configure slot alarm threshold
    - **dspslotalms**-display slot alarms

- **clrslotalm**-clear slot alarm
- **dspsloterrs**-display slot errors

- Statistical Trunk/Line Alarms
  - **cnflnalm**-configure line alarm threshold
  - **dsplnerrs**-display line errors
  - **dsplnalmcnf**- display line alarm configuration
  - **clrlnalm**-clear line alarm

Configuring Connections

Connections are typically provisioned and configured using Cisco StrataView Plus. However, the connections can also be added using the BPX switch command line interface (CLI). This may be appropriate during initial local node setup and when a Strata View Plus workstation is not available.

There are two connection addressing modes supported. The user may enter a unique VPI/VCI address in which case the BPX switch functions as a virtual circuit switch. Or the user 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.

Connections are routed between CPE connected to BXM ports. Before adding connections, the BXM is configured for port mode.

Note The initial command to up a trunk (**uptrk**) or to up a line (**upln**) on the BXM card configures all the ports of the card to be either trunks or lines (UNI port access). Following the **uptrk** command at each port, the **addtrk** command is used to activate a trunk for network access.

A line is upped with the **upln** command and configured with the **cnfln** command. Then the associated port is configured with the **cnfport** command and upped with the **upport** command. Following this, the ATM connections are added via the **addcon** command.

The slot number is the BXM card slot on the BPX switch. The port number is one of the ports on the BXM, the VPI is the virtual path identifier, and the VCI is the virtual circuit identifier.

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 AutoRoute feature once the connection endpoints are specified.

Connections can be either Virtual Path Connections (VPC) or Virtual Circuit Connections (**VCC**). Virtual Path Connections are identified by an * in the VCI field. Virtual Circuit Connections specify both the VPI and VCI fields.

Configuration Management

The following parameters are entered for the BXM **addcon** command. Depending upon the connection type, the user is prompted with appropriate parameters as shown below.

Syntax:

```
addcon local_addr node  remote_addr   traffic_type  ...extended parameters
```

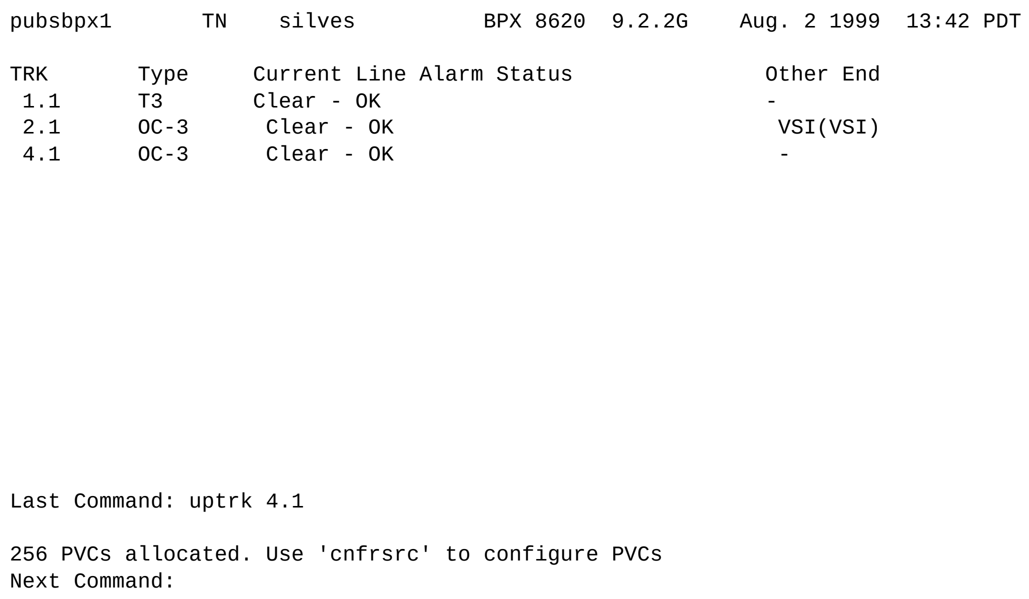
Field	Value	Description
local/remote_addr	slot.port.vpi.vci	card slot, port, and desired VCC or VPI connection identifier
node		slave end of connection
traffic_type		type of traffic, chosen from CBR, VBR, ABR, and UBR
extended parameters		parameters associated with each connection type

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".

Command Line Interface Examples

The following pages have a number of command examples, including configuring BXM lines and trunks and adding connections terminating on BXM cards.

An example of the **uptrk** command for trunk 1 on a BXM in slot 4 of a BPX switch follows:



```
pubsbpx1       TN    silves         BPX 8620  9.2.2G    Aug. 2 1999  13:42 PDT

TRK       Type     Current Line Alarm Status               Other End
 1.1      T3       Clear - OK                              -
 2.1      OC-3      Clear - OK                              VSI(VSI)
 4.1      OC-3      Clear - OK                              -










Last Command: uptrk 4.1

256 PVCs allocated. Use 'cnfrsrc' to configure PVCs
Next Command:
```

Note The initial command to up a trunk (**uptrk**) or to up a line (**upln**) on the BXM card configures all the ports of the card to be either trunks or lines (UNI port access). Following the **uptrk** command at each port, the **addtrk** command is used to activate a trunk for network access.

An example of the **cnftrk** command for trunk 4.1 of a BXM card follows:

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  13:40 PDT

TRK  4.1 Config    OC-3     [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 4.1


Transmit Rate [ 1-353208 ]:
```

An example of the **addtrk** command follows:

```
pubsbpx1       TN    silves         BPX 8620  9.2.2G    Aug. 2 1999  13:45 PDT

TRK       Type     Current Line Alarm Status               Other End
 1.1      T3       Clear - OK                              -
 2.1      OC-3      Clear - OK                              VSI(VSI)
 2.4      OC-3      Clear - OK                              -










Last Command: dsptrks


Next Command:
```

An example of the **upln** command for UNI port access on a BXM card follows:

```
pubsbpx1       TN    StrataCom       BPX 8620  9.2.2G    Aug. 2 1999  13:54 PDT

Line      Type     Current Line Alarm Status
 2.2      OC-3      Clear - OK
 2.3      OC-3      Clear - OK













Last Command: upln 2.2

256 PVCs allocated. Use 'cnfrsrc' to configure PVCs
Next Command:
```

Note The initial command to up a trunk (**uptrk**) or to up a line (**upln**) on the BXM card configures all the ports of the card to be either trunks or lines (UNI port access). Following the **upln** command at each port, the upport command is used to activate a port for UNI access.

An example of the **cnfln** command follows:

```
pubsbpx1       TN    StrataCom       BPX 8620  9.2.2G    Aug. 2 1999  13:55 PDT

LN   2.2 Config    OC-3     [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

This Command: cnfln 2.2


Loop clock (N):
```

An example of the **cnfport** command for port 3 of a BXM card in slot 3 follows:

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  13:56 PDT

Port:       2.2     [INACTIVE]
Interface:          LM-BXM                     CAC Override:     Enabled
Type:               UNI                        %Util Use:        Disabled
Shift:              SHIFT ON HCF (Normal Operation)
SIG Queue Depth:    640                        Port Load:        0 %

Protocol:           NONE                       Protocol by Card: No










This Command: cnfport 2.2


NNI Cell Header Format? [N]:
```

An example of the **cnfportq** command follows:

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  13:57 PDT

Port:       2.2     [INACTIVE]
Interface:          LM-BXM
Type:               UNI
Speed:              353208 (cps)

SVC Queue Pool Size:          0
CBR Queue Depth:              600     rt-VBR Queue Depth:                5000
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:       60%
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


SVC Queue Pool Size [0]:
```

An example of the **upport** command follows:

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  13:58 PDT

Port:       2.2     [ACTIVE  ]
Interface:          LM-BXM                     CAC Override:     Enabled
Type:               UNI                        %Util Use:        Disabled
Shift:              SHIFT ON HCF (Normal Operation)
SIG Queue Depth:    640                        Port Load:        0 %

Protocol:           NONE                       Protocol by Card: No










Last Command: upport 2.2


Next Command:
```

An example of the **cnfatmcls** command for class 2 follows:

```
pubsbpx1       TN    StrataCom       BPX 8620  9.2.2G    Aug. 2 1999  13:59 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: cnfatmcls 2


Enter class type (rt-VBR, nrt-VBR, CBR, UBR, ABRSTD, ABRFST, ATFR, ATFST, ATFT,
ATFTFST, ATFX, ATFXFST):
```

An example of the **cnfcls** command for class 3 follows:

```
pubsbpx1       TN    StrataCom       BPX 8620  9.2.2G    Aug. 2 1999  14:02 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: cnfatmcls 3


Enter class type (rt-VBR, nrt-VBR, CBR, UBR, ABRSTD, ABRFST, ATFR, ATFST, ATFT,
ATFTFST, ATFX, ATFXFST):
```

An example of the **addcon** command for a VBR connection 3.1.105.55 that originates at port 2 of a BXM card in slot 2 follows:

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  14:05 PDT

 Local           Remote      Remote                             Route
 Channel         NodeName    Channel         State  Type        Avoid COS O
 2.2.16.16       pubsbpx1    2.3.66.66       Ok     rt-vbr
 2.3.66.66       pubsbpx1    2.2.16.16       Ok     rt-vbr










Last Command: addcon 2.2.16.16 pubsbpx1 2.3.66.66 rt-VBR * * * * * * *


Next Command:
```

An example of the **cnfcon** command for a rt-VBR connection 2.2.16.16 follows.

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  14:06 PDT

Conn:  2.2.16.16        pubsbpx1    2.3.66.66         rt-vbr    Status:OK
   PCR(0+1)     % Util       CDVT(0+1)       AAL5 FBTC        SCR
   50/50       100/100     250000/250000         n          50/50

     MBS         Policing
 1000/1000           3









This Command: cnfcon 2.2.16.16


PCR(0+1) [50/50]:
```

An example of the **addcon** command for an ABR connection follows. In this case, the choice to accept the default parameters was not accepted, and individual parameters were configured for a connection using ABR standard VSVD flow control.

```
pubsbpx1       TN    StrataCom       BPX 8620  9.2.2G    Aug. 2 1999  14:12 PDT

 From            Remote      Remote                             Route
 2.2.17.17       NodeName    Channel         State  Type        Avoid COS O
 2.3.66.66       pubsbpx1    2.2.16.16       Ok     rt-vbr













This Command: addcon 2.2.17.17 pubsbpx1 2.3.67.67 abrstd 100/100 95/95 * * e e e
 d 70/70 * 3 * * * 65/65 * * * * * * * *

Add these connections (y/n)? y
```

An example of the **cnfcon** command for an ABR connection follows:

```
pubsbpx1       TN    silves         BPX 8620  9.2.2G    Aug. 2 1999  14:14 PDT

Conn:  2.2.17.17        pubsbpx1    2.3.67.67         abrstd    Status:OK
   PCR(0+1)     % Util      MCR           CDVT(0+1)       AAL5 FBTC VSVD  FCES
  100/100       95/95     50/50          250000/250000         y      y     y

     SCR            MBS      Policing   VC Qdepth    CLP Hi CLP Lo/EDP    EFCI
   70/70        1000/1000        3    16000/16000    80/80    35/35      65/65

     ICR           ADTF  Trm     RIF      RDF    Nrm     FRTT            TBE
   50/50           1000  100        128    16     32           0        1048320





This Command: cnfcon 2.2.17.17


PCR(0+1) [100/100]:
```

An example of the **cnfabrparm** command follows:

```
pubsbpx1       TN    YourID:1       BPX 15    9.2       Jun. 8 1998  00:21 GMT

ABR Configuration for BXM in slot 3

Egress CI Control  : N
ER Stamping        : N
Weighted Queueing  : N









Last Command: cnfabrparm 3


Next Command:
```

An example of the **dsplns** command follows:

```
pubsbpx1       TN    YourID       BPX 15    9.2       Jun. 8 1998  00:22 GMT

Line    Type   Current Line Alarm Status
 3.1    OC-3    Clear - OK
 3.2    OC-3    Clear - OK
 3.3    OC-3    Clear - OK
 3.4    OC-3    Clear - OK
 5.1    T3     Clear - OK
 5.2    T3     Clear - OK







Last Command: dsplns


Next Command:
```

Configuring the BPX Switch LAN and IP Relay

During the configuration of BPX switch interfaces, you must make sure that the BPX switch IP address, SNMP parameters, and Network IP address are set consistent with your local area network (Ethernet LAN). Use the following BPX switch commands to set these parameters:

- **cnflan—**This is a Super User level command and must be used to configure the BPX switch BCC LAN port IP address and subnet mask.
- **cnfsnmp**—This command is used to configure the SNMP Get and Set community strings for the BPX switch as follows:
    - Get Community String = public
    - Set Community String = private
    - Trap Community String = public.
- **cnfnwip**—This is a Super User level command which is used 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 Cisco StrataView Plus.

The use of these commands is covered in the *Cisco WAN Switch Command Reference* or the *Cisco WAN Switch Superuser Command Reference*. Super User commands must be used only by authorized personnel, and must be used carefully.

Configuring the MGX 8220

MGX 8220 installation and configuration are covered in the *Cisco MGX 8220 Reference*. During the configuration of BPX switch interfaces, you must make sure that the MGX 8220 IP address is set up consistent with your local area network (Ethernet LAN). Use the following MGX 8220 command to set the proper IP addresses:

cnfifip -ip <ip address> -if <interface type> -msk <subnet mask address> -bc <broadcast address>

The use of this command is covered in the *Cisco MGX 8220 Command Reference.*

Resource Partitioning

Starting with switch software Release 8.4, resources on BPX switch UNI ports and NNI trunks can be divided between SVCs and PVCs, or LVCs and PVCs. This is known as resource partitioning and is done through the Command Line Interface for the BPX switch and the MGX 8220.

These resources for BXM, ASI, and BNI cards can be partitioned appropriately between SVCs or PVCs.

In this release, you can have both a PNNI controller and a Cisco 6400 controller, each in its own partition controlling the same VSI slave.

MPLS

Starting with switch software release 9.1, the BXM also supports Multiprotocol Label Switching (MPLS). Partitions for the BXM can be allocated either between:

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

For information on MPLS Switching, refer to to the chapter “MPLS on BPX Switch.”

Dynamic Resource Partitioning for SPVCs

Also, starting with switch software Release 9.1, the BXM card supports dynamic resource partitioning to support the conversion of PVCs to soft permanent virtual circuits (SPVCs). This feature is described in the *Cisco WAN Service Node Extended Services Processor Installation and Operations for Release 2.2* document.

Summary

This section provides procedures for:

- UNI Port Resource Partitioning, BXM
- NNI or Trunk Resource Partitioning, BXM

Note Resource partitioning also has to be done for the line between the ESP ATM NIC and the BXM in the BPX switch. Refer to the *Cisco WAN Service Node Extended Services Processor Installation and Operation for Release 2.2* document.

BXM SVC Resource Partitioning

A BXM card used as a UNI port can be configured to support ATM SVCs. The BXM will have to be added and upped like a standard PVC port. The BXM port will have to upped as a line (upln) to function as a UNI port.

Note The initial command to up a trunk (**uptrk**) or to up a line (**upln**) on the BXM configures all the physical ports on a BXM card to be either trunks or ports. They can not be inter-mixed.

For additional information on using the BPX switch command line interface and applicable commands, refer to the *Cisco WAN Switch Command Reference* manual. These procedures will concentrate on those commands that are specific to SVC resource partitioning.

Before partitioning SVC resources, you must determine which BXM UNI ports will support ATM SVCs. The BXM must have its resources partitioned to support SVCs. The following resources must be partitioned:

- SVC Channels
- SVC VPI Min
- SVC VPI Max
- SVC Bandwidth
- SVC Queue Pool Size.

To partition the BXM port, follow these steps:

Step 1 Log in to the BPX switch.

Step 2 Using the upln and upport commands, up the line and port which is going to be connected to ATM CPE.

Step 3 Make sure the port is configured as UNI.

Step 4 Enter the **cnfport <port num>** command, shown in the following example:

Example: BXM cnfport Command

```
ins-bpx6       TN    SuperUser       BPX 15    9.2   Sep. 24 1998 07:37 GMT

Port:       13.1    [ACTIVE  ]
Interface:          LM-BXM
Type:               UNI                        %Util Use:        Disabled
Speed:              353208 (cps)
Shift:              SHIFT ON HCF (Normal Operation)
SIG Queue Depth:    640

Protocol:           NONE
  SVC Channels:                      1000
  SVC VPI Min:                       0
  SVC VPI Max:                       10
  SVC Bandwidth:                     300000 (cps)


This Command: cnfport 13.1


NNI Cell Header Format? [N]:
```

Step 5 Configure the SVC Channels, SVC VPI Min, SVC VPI Max, and SVC Bandwidth as desired.

Step 6 Next you need to configure the SVC Port Queue depth with the cnfportq <portnum> command shown in the following example.

Example: BXM cnfportq Command

```
ins-bpx6       TN    SuperUser       BPX 15    9.2    Sep. 24 1998 07:39 GMT

Port:       13.1    [ACTIVE  ]
Interface:          LM-BXM
Type:               UNI
Speed:              353208 (cps)

SVC Queue Pool Size:          5000
CBR Queue Depth:              600
CBR Queue CLP High Threshold: 80%
CBR Queue CLP Low Threshold:  60%
CBR Queue EFCI Threshold:     80%
VBR Queue Depth:              5000    UBR/ABR Queue Depth:               20000
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 13.1


SVC Queue Pool Size [5000]:
```

Step 7 Configure the SVC Queue Pool Size parameter to a value greater than 0 (zero); the default is 0 and needs to be changed for SVCs to operate.

Step 8 Partition the SVC resources for every BXM which is to support ATM SVCs in the BPX switch.

NNI Trunk SVC Resource Partitioning

The BXM card may have resources partitioned to support SVCs.

Note It is important to reserve the maximum number of channels before SVCs or PVCs are in use, because SVC partitioning parameters may not be changed if any SVC or PVC is in use on the entire card.

BXM Trunk SVC Resource Partitioning

When the BXM is used as a trunk in a BPX switch network, it needs to have its resources partitioned to support SVCs. The BXM card will have to upped as a trunk (**uptrk**).

Note The initial command to up a trunk (**uptrk**) or to up a line (**upln**) on the BXM configures all the physical ports on the card to be either lines or trunks. They can not be inter-mixed.

For additional information on using the BPX switch command line interface and applicable commands refer to the *Cisco WAN Switch Command Reference* manual. These procedures concentrate on those commands that are specific to SVC resource partitioning.

The following BXM trunk resources must be partitioned for SVCs:

- SVC Channels
- SVC Bandwidth
- SVC Queue Pool Size.

To partition the BXM trunk resources for SVCs, follow these steps:

Step 1 Log in to the BPX switch

Step 2 Make sure the BXM has been upped as a trunk with **uptr**k <trunk_num> command.

Step 3 Enter the **cnftrk <trk num>** command, shown in the following example:

Example: BXM cnftrk Command

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  14:23 PDT

TRK  2.4 Config    OC-3     [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 ]:
```

Step 4 Configure the SVC VPI Min, SVC Channels and SVC Bandwidth as desired.

Step 5 Next configure the SVC Queue depth with cnftrkparms <trunk_num> command shown in the following example:

Example: BXM cnftrkparm Command

```
pubsbpx1       TN    silves          BPX 8620  9.2.2G    Aug. 2 1999  14:24 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


Which parameter do you wish to change:
```

Step 6 Configure the SVC Queue Pool Size as desired.

Step 7 Partition the SVC resources for all the other BXMs in the BPX switch.

Configuration, BXM Virtual Trunks

This chapter provides a description of BXM virtual trunks, a feature supported by the BXM cards beginning with switch software Release 9.2. Refer to Release Notes for supported features.

The chapter contains the following:

- Overview
- Functional Description
- Connection Management
- Configuration
- Trunk Redundancy
- Networking
- Trunk Statistics
- Trunk Alarms
- Event Logging
- Command Reference

Overview

Virtual trunking provides connectivity for Cisco switches through a public ATM cloud as shown in Figure 15-1. Since 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, as each virtual trunk typically uses only part of a physical trunk's resources.

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.

The ATM equipment in the cloud must support virtual path switching and transmittal of ATM cells based solely on the VPI in the cell header. Within the cloud, one virtual trunk is equivalent to one VPC since the VPC is switched with just the VPI value. The virtual path ID (VPI) is provided by the ATM cloud administrator (such as, Service Provider). The VCI bits within the header are passed transparently through the entire cloud (see Figure 15-1).

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.

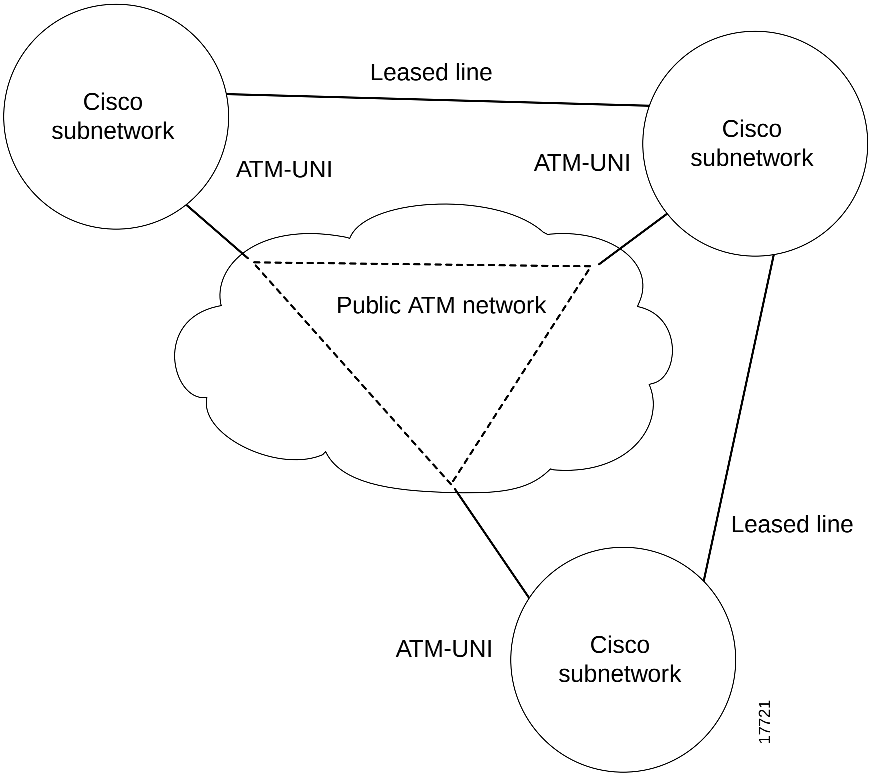
Typical ATM Hybrid Network with Virtual Trunks

Figure 15-1 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.

With the BPX switch, virtual networks can be set up with either the 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, ASI, 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 an ASI port on a BPX.

Figure 15-1 Typical ATM Hybrid Network using Virtual Trunks



Features

Virtual trunking benefits include the following:

- 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 which does not support PNNI or MPLS services. The part of the network which does not support PNNI or MPLS may be a public ATM network, or simply consist of switches which 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 15-1, depending on the specific BXM card.

Table 15-1 Virtual Trunk Criteria

	Number of VIs	Max LCNs	Default LCNs
BXM	31	32000	16320

Feature summary:

- The maximum number of virtual trunks that may be configured per card equals the number of virtual interfaces (VIs). In Release 9.2, the BXM supports 31 virtual interfaces, and therefore up to 31 virtual trunks.
- For the BXM a maximum of 31virtual trunks may be defined within one port. 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.

The following syntax describes a virtual trunk:

UXM/BXM:slot.port.vtrunk

slot = slot number (1-32, as applicable. For example, on the BPX slots 7 and 8 are reserved for BCCs and slot and 15 is reserved for the ASM card.)

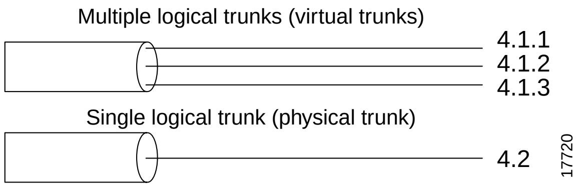
port = port number (1-16)

vtrunk = virtual trunk number (1-31 on BXM) (1-15 on UXM)

Functional Description

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. In Figure 15-2, 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 15-2 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

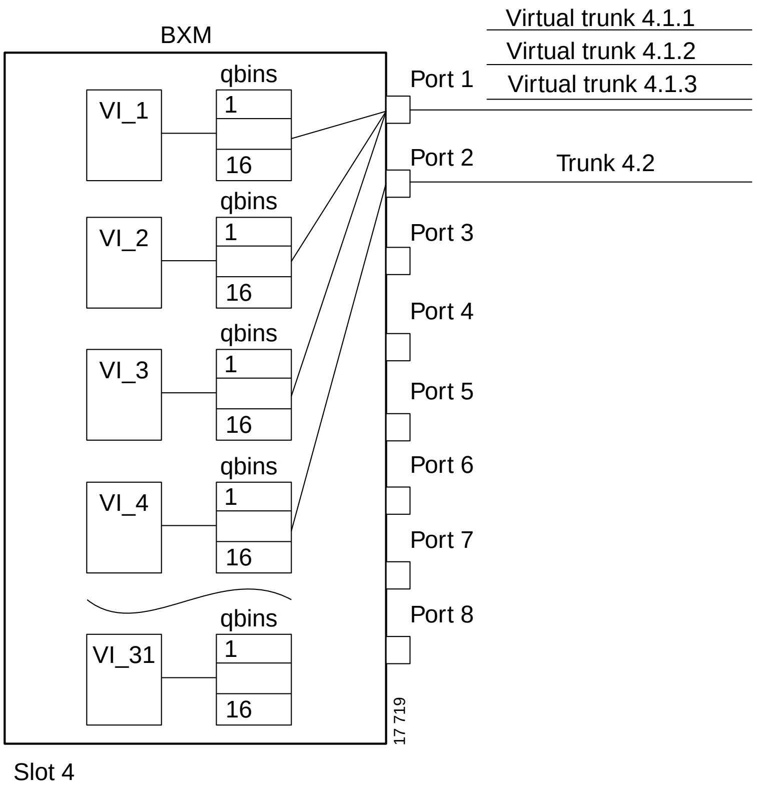
Virtual Interfaces

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 15-3, 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).

AutoRoute connections use qbins 0-9. Virtual Switch Interfaces (VSIs), which support master controllers use qbins 10-15, as applicable. Currently, on the BXM, MPLS and AutoRoute, or PNNI and AutoRoute can be supported simultaneously, but not MPLS and PNNI at the same time on a given VSI.

Figure 15-3 BXM Egress VIrtual Interfaces and Qbins



VSI Virtual Trunks and AutoRoute Virtual Trunks

There are two general types of virtual trunks: AutoRoute Virtual Trunks and VSI Virtual Trunks.

AutoRoute Virtual Trunks are PVP or SPVP connections which carry AutoRoute PVC connections.

VSI Virtual Trunks are PVP or SPVP connections which 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.

Virtual Trunk Example

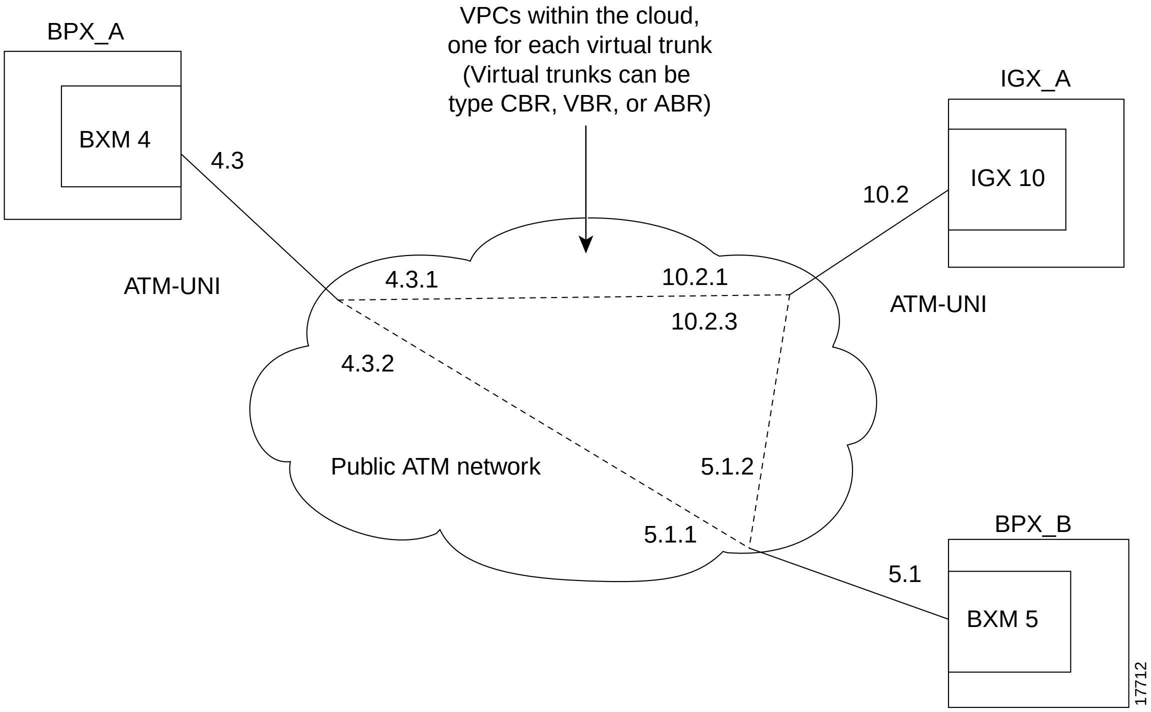
An example of a number of virtual trunks configured across a Public ATM Network is shown in Figure 15-4. There are three virtual trunks shown across the network, each with its own unique VPC.

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 which supports the traffic types shown in Table 15-2.

Figure 15-4 Virtual Trunks across a Public ATM Network



Virtual Trunk Transmit Queuing

In the BXM, the egress cell traffic out a port is queued in 2 stages. First it is queued per Virtual Interface (VI), each of which supports a virtual trunk. Within each VI, the cell traffic is queued in accordance with its type of service. These types are as follows:

Table 15-2 Virtual Trunk Traffic Types

AutoRoute	
	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. Since each virtual trunk occupies one virtual interface (VI), the overall queue depth available for the virtual trunk is that of its VI.

The user does not directly configure the VI. The **cnftrkparm** command is used to configure the queues within AutoRoute virtual trunks. The **cnfvsiif** and **cnfqbin** commands are used to configure the queues within VSI virtual trunk VIs; refer to *Chapter 16, Configuration, BXM Virtual Trunks*.

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 since 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

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

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

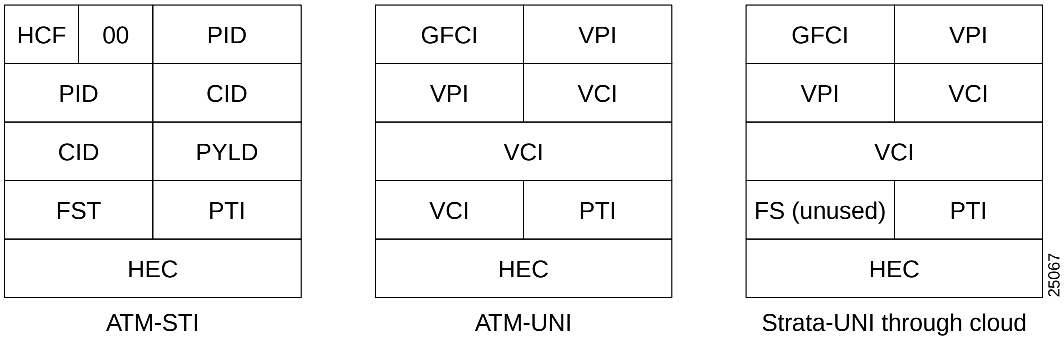
The VPI value across the virtual trunk is identical for all cells on a single virtual trunk. The VCI value in these cells determines the final destinations of the cells.On BNI cards, for virtual trunking a modified ATM UNI cell format (Strata-UNI) stores the ForeSight information, as applicable, in the 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 15-5 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 15-5 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 15-3. A BNI in the Cisco subnetwork can interface to an ASI or BXM (port configured for port mode) in the cloud. The ASI or BXM in the cloud is configured for no shift in this case.

A BXM in the Cisco subnetwork can interface to an ASI UNI port, BXM UNI port, or other UNI port in the cloud. The BXM or ASI in the cloud is configured for bit shifting as shown in Table 15-3.

Table 15-3 Bit Shifting for Virtual Trunking

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

Routing with Virtual Trunks

AutoRoute, PNNI, and MPLS all 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. The traffic classes allowed per virtual trunk are configured by the user with **cnftrk**. The routing algorithm excludes virtual trunks whose traffic class is not compatible with the candidate connection to be routed.
- Connection Identifier (Conid) Capacity—Each virtual trunk has a configurable number of connection channels reserved from the card. The routing algorithm checks for adequate channel availability on a virtual trunk before selecting the trunk for a route.

Virtual Trunk Bandwidth

The total bandwidth of all the virtual trunks in one port cannot exceed the maximum bandwidth of the port. The trunk loading (load units) is maintained per virtual trunk, but the cumulative loading of all virtual trunks on a port is restricted by the transmit and receive rates for the port.

Virtual Trunk Connection Channels

The total number of connection channels of all the virtual trunks in one port cannot exceed the maximum number of connection channels of the card. The number of channels available is maintained per virtual trunk

Cell Transmit Address Translation

All cells transmitted to a virtual trunk have a translated cell address. This address consists of a VPI chosen by the user and a VCI (ConId) chosen internally by the software. The trunk firmware is configured by the software to perform this translation.

Cell Receive Address Lookup

The user-chosen VPI is the same for all cells on a virtual trunk. At the receiving end, multiple virtual trunks can send cells to one port. The port must be able to determine the correct channel for each of these cells. The VPI is unique on each trunk for all the cells, but the VCI may be the same across the trunks. Each port type has a different way of handling the incoming cell addresses. 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 (1-65535) excluding the node numbers and blind addresses. A port uses the VPI to differentiate connections which have the same conid.

The number of channels per virtual trunk can be changed 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.

Primary Configuration Criteria

The primary commands used for configuration of virtual trunks are **cnftrk**, **cnfrsrc**, and **cnftrkparm**.

Note A virtual trunk cannot be used as a feeder trunk. Feeder connections cannot be terminated on a virtual trunk.

Configuration with **cnftrk**

The main parameters for **cnftrk** are transmit trunk rate, trunk VPI, Virtual Trunk Type, Connection Channels, and 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 15-4

Table 15-4 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**

cnfrsrc is used to configure conids (lcns) and bandwidth. The conid capacity indicates the number of connection channels on the trunk port which are usable by the virtual trunk.

This number cannot be greater than the total number of connection channels on the card. The maximum number of channels is additionally limited by the number of VCI bits in the UNI cell header. For a virtual trunk, the number is divided by the maximum number of virtual trunks on the port to determine the default. This value is configured by the **cnfsrc** command on the BPX. Table 15-5 lists the number of connection ids for virtual trunks on various cards.

Table 15-5 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.

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.

If the link to the public cloud from the private network is using BNI cards, then access points within the cloud are ASI ports. The BNI card uses an STI header. The ASI port cards within the cloud are configured to not shift the VCI when forming the STI header. The command **cnfport** allows the user to configure no shifting on the port.

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, etc.
- VBR Trunk: ATM VBR traffic, frame relay traffic, etc.
- ABR Trunk: ATM ABR traffic, ForeSight traffic, etc.

A CBR configured trunk is best suited to carrying delay sensitive traffic such as voice/data, streaming video, and ATM CBR traffic, etc.

A VBR configured trunk is best suited to carrying frame relay and VBR traffic, etc.

An ABR configured trunk is best suited to carrying ForeSight and ABR traffic, etc.

Two-stage queueing at the egress of virtual trunks to the ATM cloud allows shaping of traffic before it enters the cloud. However, the traffic is still routed on a single VPC and may be affected by the traffic class of the VPC selected.

A user can configure any number of virtual trunks up to the maximum number of virtual trunks per slot (card) and the maximum number of logical trunks per node. These trunks can be any of the three trunk types, CBR, VBR, or ABR.

A user can configure any number of virtual trunks between two ports up to the maximum number of virtual trunks per slot and the maximum number of logical trunks per node. These trunks can be any of the three trunk types.

Virtual Trunk Cell Addressing

Cells transmitted to a virtual trunk use the standard UNI or NNI cell format.

The trunk card at the edge of the cloud ensures that cells destined for a cloud VPC have the correct VPI/VCI. The VPI is an 12-bit value ranging from 1-4095. The VCI is a 16-bit value ranging from 1-65535.

BXM/UXM Two Stage Queueing

The UXM and BXM share the same queueing architecture. The egress cells are queued in 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, voice, Time-Stamped, Non Time-stamped, High Priority, BDATA, BDATB, CBR, VBR, and ABR traffic is queued separately. The overall queue depth of the VI is the sum of all the queue depths for all the available queues. The user does not directly configure the VI.

The user command **cnftrkparm** is used to configure the queues within the virtual trunk.

Configuration

Connectivity is established through the public ATM cloud by allocating virtual trunks between the nodes on the edge of the cloud. With only a single trunk port attached to a single ATM port in the cloud, a node uses the virtual trunks to connect to multiple destination nodes across the network thereby providing full or partial meshing as required.

From the perspective of the Cisco node, a virtual trunk is equivalent to a VPC provided by an ATM cloud where the VPC provides the connectivity through the cloud.

Virtual Trunk Example

The following is a typical example of adding one virtual trunk across an ATM network. On one side of the cloud is a BPX with a BXM trunk card in slot 4. On the other side of the cloud is an IGX with a UXM trunk card in slot 10. A virtual trunk is added between port 3 on the BXM and port 2 on the UXM (see Figure 15-6).

Perform the following: .

Step 1	Initial Setup		Contact Customer Service to enable virtual trunking on the nodes in your network.
Step 2	In the public ATM cloud		Obtain the VPCs for the virtual trunks for the service provider. These are the VPCs that are configured within the ATM cloud by the service provider to support the virtual trunks.
Step 3	At BPX_A	uptrk 4.3.1 uptrk 4.3.2	Up virtual trunks 4.3.1 and 4.3.2 on BXM port 4.3.
Step 4	At BPX_A	cnftrk 4.3.1 ... cnftrk 4.3.2 ...	Configure the virtual trunks to match the cloud’s VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, etc.
Step 5	At BPX_A	cnfrsrc 4.3.1 ... cnfrsrc 4.3.2 ...	Configure the number of conids, bandwidth, etc., available for the virtual trunks.
Step 6	At BPX_B	uptrk 5.1.1 uptrk 5.1.2	Up virtual trunks 5.1.1 and 5.1.2 on BXM port 5.1.
Step 7	At BPX_B	cnftrk 5.1.1 ... cnftrk 5.1.2 ...	Configure the virtual trunks to match the cloud’s VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, etc.
Step 8	At BPX_B	cnfrsrc 5.1.1 ... cnfrsrc 5.1.2 ...	Configure the number of conids, bandwidth, etc., available for the virtual trunks.
Step 9	At IGX_A	uptrk 10.2.1 uptrk 10.2.3	Up virtual trunks 10.2.1 and 10.2.3 on IGX trunk port 10.2.

Step 10	At IGX_A	cnftrk 10.2.1 ... cnftrk 10.2.3 ...	Configure the virtual trunks to match the cloud's VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, etc.
Step 11	At IGX_A	cnfrsrc 10.2.1 ... cnfrsrc 10.2.3 ...	Configure the number of conids, bandwidth, etc., available for the virtual trunk.
Step 12	At BPX_A	addtrk 4.3.1 IGX_A 10.2.1 addtrk 4.3.2 BPX_B 5.1.1	Add the virtual trunks between three nodes. Using addtrk 10.2.1 ... at IGX_A and addtrk 5.1.1 ... at BPX_B would also add the virtual trunks.
Step 13	At BPX_B	addtrk 5.1.2 IGX_A 10.2.3	Add the virtual trunks between the two nodes. Using addtrk 10.2.3 ... at IGX_A would also add the virtual trunks.

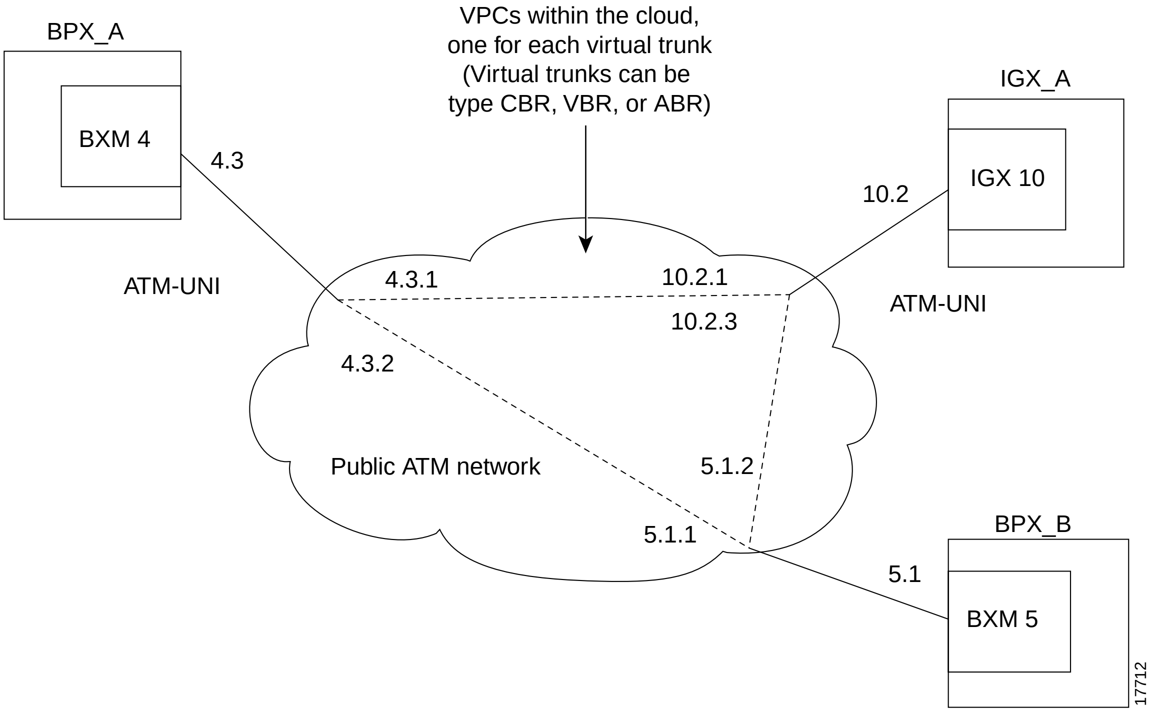
The VPI values chosen using **cnftrk** must match those used by the cloud VPC. In addition, both ends of the virtual trunk must match with respect to: Transmit Rate, VPC type, traffic classes supported, and the number of connection channels supported. The **addtrk** command checks for matching values before allowing the trunk to be added to the network topology.

The network topology as seen from a **dsptrks** command at BPX_A would be:

BPX_A 4.3.1-10.2.1/IGX_A

BPX_A 4.3.2-5.1.1/BPX_B

Figure 15-6 Addition of Virtual Trunks across a Public ATM Network



Trunk Redundancy

Trunk redundancy can refer to one of two features:

- SONET Automatic Protection Switching (APS)
- Y-redundancy

APS Redundancy

With Release 9.2, APS line redundancy is supported. APS line redundancy is only available on BXM SONET trunks and is compatible with virtual trunks. The trunk port supporting virtual trunks may have APS line redundancy configured in the same way it would be configured for a physical trunk. The commands **addapsln**, **delapsln**, **switchapsln**, and **cnfapsln** are all supported on virtual trunk ports. The syntax for these commands is unchanged; they accept a trunk port parameter as *slot.port*. For more information, refer to the Chapter 17, "SONET APS, Configuration."

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.

Networking

Virtual Trunk Configuration

The characteristics of a virtual trunk used by connection routing are maintained throughout the network. This information—virtual trunk existence, traffic classes and connection channels—is sent to every node to allow the routing algorithm to use the trunk correctly. Routing only uses those virtual trunks which can support the traffic type of the connection.

ILMI

ILMI provides data and control functions for the virtual trunking feature.

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.

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 stats are displayed on the **dspphyslnstats**, **dspphyslnstathist**, and **dspphyslnerrs** screens. These commands only accept physical line numbers (i.e.,. slot.port). These commands are new to the BPX in this release.

- **Logical trunk** statistics refer to counts on trunks that are visible to users as routing entities. This includes physical trunks and virtual trunks.

  Logical trunk stats are displayed on the **dsptrkstats**, **dsptrkstahist**, and **dsptrkerrs** screens. These commands only accept logical trunk numbers and display only logical trunk stats.

- **VI statistics** are a subset of the logical trunk statistics.
- **Queue statistics** are a subset of the logical trunk statistics.
- **Channel statistics** are not polled by software on trunks. However, they are available if the debug command **dspchstats** is used.

A listing of trunk statistics including statistics type, card type, and line type, as applicable, is provided in Table 15-6.

Table 15-6 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

Table 15-6 Trunk Statistics (Continued)

Statistic	Stat Type	Card Type	Line Type
PLCP UAS	Physical	BXM	T3
LOC errors	Physical	UXM/BXM	E3/Sonet
LOP errors	Physical	UXM/BXM	Sonet
Path AIS errors	Physical	UXM/BXM	Sonet
Path RDI errors	Physical	UXM/BXM	Sonet
Section BIP-8 counts, ES, and SES	Physical	UXM/BXM	Sonet
Line BIP-24 counts, ES, and SES	Physical	UXM/BXM	Sonet
Line FEBE counts, ES, and SES	Physical	UXM/BXM	Sonet
Section SEFS	Physical	UXM/BXM	Sonet
Line UAS and FarEnd UAS	Physical	UXM/BXM	Sonet
Clock Loss Transitions	Physical	UXM	T1/E1
Frame Loss Transitions	Physical	UXM	T1/E1
Multiframe Loss	Physical	UXM	T1/E1
CRC errors	Physical	UXM	T1/E1
BPV	Physical	UXM	T1
Frame bit errors	Physical	UXM	E1
Unknown VPI/VCI count	Physical	UXM/BXM	All
Errored LPC cell count	Physical	UXM	All
Non-zero GFC cell count	Physical	UXM/BXM	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
For Each Traffic Type: (V,TS,NTS,ABR,VBR,CBR, BdatB, BdatA,HP)			
Cells served	Logical	UXM/BXM	All
Maximum Qbin depth	Logical	UXM/BXM	All
Cells discarded count	Logical	UXM/BXM	All

Trunk Alarms

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 which are shared with all the other virtual trunks on the port. These alarms are cleared and set together for all the virtual trunks sharing the same port.

Physical and Logical Trunk Alarm Summary

A listing of physical and logical trunk alarms is provide in Table 15-7.

Table 15-7 Physical and Logical Trunk Alarms

	Physical							
Alarm Type	**T1**	**E1**	**T3**	**E3**	**SONET**	**Logical**	**Statistical**	**Integrated**
LOS	X	X	X	X	X		X	X
OOF	X	X	X	X	X		X	X
AIS	X	X	X	X	X		X	X
YEL	X	X	X	X	X			X
PLCP OOF			X					X
LOC				X	X			X
LOP					X			X
PATH AIS					X			X
PATH YEL					X			X
PATH TRC					X			X
SEC TRC					X			X
ROOF	X	X						X
FER	X	X						X
AIS16	X	X					X	X
IMA	X	X						X
NTS Cells Dropped						X	X	
TS Cells Dropped						X	X	
Voice Cells Dropped						X	X	
Bdata Cells Dropped						X	X	

Table 15-7 Physical and Logical Trunk Alarms (Continued)

	Physical							
Alarm Type	**T1**	**E1**	**T3**	**E3**	**SONET**	**Logical**	**Statistical**	**Integrated**
BdatB Cells Dropped						X	X	
HP Cells Dropped						X	X	
CBR Cells dropped						X	X	
VBR Cells dropped						X	X	
ABR Cells dropped						X	X	

Event Logging

All trunk log events are modified to display the virtual trunk number. The examples in Table 15-8 and Table 15-8 and Table 15-9 show the log messaging for activating and adding a virtual trunk 1.2.1.

I

Table 15-8 IGX Log Messaging for Activating and Adding 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 15-9 BPX Log Messaging for Activating and Adding 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 in Table 15-10

Table 15-10 Virtual Trunk Error Messages

Message	- Description
“Port does not support virtual trunking”	- Port is not configured for virtual trunks
“Port configured for virtual trunking”	- Port is not configured for a physical trunk
“Invalid virtual trunk number”	- Virtual trunk number is invalid
“Maximum trunks per node has been reached”	- Trunk limit per node has been reached
“Invalid virtual trunk VPI”	- Virtual trunk VPI is invalid
“Invalid virtual trunk traffic class”	- Virtual trunk traffic class is invalid
“Invalid virtual trunk VPC type”	- Virtual trunk VPC type is invalid
“Invalid virtual trunk conid capacity”	- Virtual trunk conid capacity is invalid
“Mismatched virtual trunk configuration”	- Ends of virtual trunk have different configuration
“Maximum trunks for card has been reached”	- The trunk card is out of VIs

Command Reference

The following command descriptions are summaries specific to virtual trunk usage on the BPX, using the BXM cards, and do not necessarily have complete descriptions covering all facets of the commands. For complete information about these commands, refer to the Release 9.2 *Cisco WAN Switch 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.

- Three main commands are used for configuring virtual trunks. These are **cnftrk**, **cnftrkparm**, and **cnfrsrc** which configure all port and trunk attributes of a trunk. When a physical port attribute change is made, the user is notified that all trunks on the port are affected.
- Virtual trunks support APS redundancy on BXM OC-3 and OC-12 ports. The commands **addapsln**, **delapsln**, **switchapsln**, and **cnfapsln** are the main commands. For more information, refer to the section on APS Redundancy in this manual. The prior Y-redundancy is not supported by virtual trunks, nor the related commands, **addtrkred**, **deltrkred**, and **dsptrkred**.

A summary of these commands is provided in the following pages:

Virtual Trunk Commands

Note Since a virtual trunk is defined within a trunk port, its physical characteristics are derived form the port. All the virtual trunks within a port have the same port attributes.

If a physical trunk is specified on a physical port which supports multiple virtual trunks, the command is applied to all virtual trunks on the physical port. **If a virtual trunk is specified for a command which configures information related to the physical port, then the physical port information is configured for all virtual trunks.**

With Release 9.2, the BPX statistics organization is modified to separate logical and physical trunk statistics. This is also the method used on the UXM card on the IGX 8400 series switches.

Virtual Trunks Commands Common to BXM and UXM

The following commands are available on both the IGX and the BPX and have the same results. Refer to the IGX 8xxx Series documentation for information the IGX and UXM.

The entries in Table 15-11 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 15-11 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

Table 15-11 Virtual Trunk Commands Common to BXM and UXM (IGX) (Continued)

Command	Description
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
dsplogtrk	displays the logical trunk information
dspphyslnstatcnf	displays the statistics configuration for a physical line
dspphyslnstathist	displays the statistics collection result for a physical line
dsptrkcnf	displays the trunk configuration
dsptrkcons	displays the number of connections routed over a trunk
dsptrkerrs	displays the trunk errors for a logical trunk
dsptrks	displays the upped/added trunks
dsptrkstatcnf	displays the configured statistics collection for a trunk
dsptrkstathist	displays the statistics collection results for a trunk
dsptrkstats	displays the summary trunk statistics for a trunk
dsptrkutl	displays the utilization/traffic for a logical trunk
prtphyslnerrs	print the trunk errors for a physical line
prttrkerrs	prints the trunk errors for a logical trunk
prttrks	prints the active logical trunks
uptrk	ups a trunk

Virtual Trunk UXM Commands

The commands listed in Table 15-12 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 15-12 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 15-13 are BPX specific.

Table 15-13 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)

cnfrsrc

The **cnfrsrc** command is used to configure resource partitions. The resources currently available for configuration are the number of conids and the trunk bandwidth.

Syntax

cnfrsrc <slot>.<port>.<vtrunk> [options]

Example

```
cnfrsrc 4.1.1 256 26000 1 e 512 7048 2 15 26000 100000 .....
```

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX switch	

Related Commands

cnftrk, **cnftrkparm**

Parameters—cnfrsrc

Parameter (cnfrsrc)	Description
slot.port.num	Specifies the slot and port number and virtual trunk number if applicable.
maxpvclcns	The maximum number of LCNs allocated for AutoRoute PVCs for this port. For trunks there are additional LCNs allocated for AutoRoute that are not configurable. The **dspcd** <slot> command displays the maximum number of LCNs configurable via the **cnfrsrc** command for the given port. For trunks, "configurable LCNs" represent the LCNs remaining after the BCC has subtracted the "additional LCNs" needed. For a port card, a larger number is shown, as compared with a trunk card. Setting this field to zero would enable configuring all of the configurable LCNs to the VSI.
maxpvcbw	configure bandwidth -------------------
partition	--
e/d	-- default is d
minvsilcns	--
maxvsilcns	--
vsistartvpi	--
vsiendvpi	--
vsiminbw	--)
vsimaxbw	--.

cnftrk

Configures trunk parameters. A trunk has a default configuration after it activated with the **uptrk** command. This default configuration can be modified using the cnftrk command.

Syntax:

cnftrk <slot>.<port>.<vtrunk> [options]

Example

```
cnftrk 4.1.1 ....................................
```

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX, IGX switch	

Related Commands

cnfrsrc, **cnftrkparm**

Parameters-cnftrk

All physical options can be specified on virtual trunks. If a physical option is changed on a virtual trunk (VT), the change is propagated to all VTs on the trunk port. X in the table indicates the parameter is configurable. X* in the virtual trunk columns indicates the parameter is a physical parameter, and changing the value for one VT on the port will automatically cause all VTs on the port to be updated with the same value. The UXM parameters are included here, as the configuration of a virtual trunk across an ATM cloud could quite possibly have a BPX at one end and an IGX at the other end.

.

	BXM		UXM	
Parameter-cnftrk	**Physical**	**Virtual**	**Physical**	**Virtual**
Transmit Trunk Rate	X	X	X	X
Receive Trunk Rate	X	X	X	X
Pass Sync	X	X*	X	X*
Loop Clock	X	X*	X	X*
Statistical Reserve	X	X	X	X
Header Type	X	X*	X	X*
Trunk VPI		X	X	X
Routing Cost	X	X	X	X
Virtual Trunk Type		X		X
Idle Code	X	X*	X	X*
Restrict PCC traffic	X	X	X	X

	BXM		UXM	
Parameter-cnftrk	**Physical**	**Virtual**	**Physical**	**Virtual**
Link Type	X	X*	X	X*
Line Framing	X	X*	X	X*
Line Coding			X	X*
Line Cable type			X	X*
Line cable length	X	X*	X	X*
HCS Masking	X	X*	X	X*
Payload Scramble	X	X*	X	X*
Connection Channels	X	X	X	X
Gateway Channels			X	X
Valid Traffic classes	X	X	X	X
Frame Scramble	X	X*	X	X*
Deroute Delay Time	X	X	X	X
Vc (Traffic) Shaping	X	X	X	X

Description

The following describes some of the major parameters in more detail:

Transmit Trunk Rate—This parameter indicates the trunk load. This value is configured by **cnfrsrc** on BXMs.

Virtual Trunk Type—The VPC type indicates the configuration of the VPC provided by the ATM cloud. Valid VPC types are CBR, VBR, and ABR.

Traffic classes—The traffic classes parameter indicates the types of traffic a trunk may support. By default a trunk supports all traffic classes, i.e., any type of traffic can be routed on any type of VPC. However, to prevent unpredictable results, a more appropriate configuration would be to configure traffic classes best supported by the VPC type:

High priority traffic can be routed over any of the VPC types:_

VPC Type	Recommended Traffic Classes
CBR	All Traffic classes
VBR	ATM VBR, Bdata, Bdatb (ForeSight), ABR
ABR	ATM ABR, Bdatb (ForeSight)

VPC VPI—The VPI configured for a virtual trunk matches the VPI for the VPC in the cloud. Every cell transmitted to this trunk has this VPI value. Valid VPC VPIs depend on the port type.

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

Conid Capacity—The conid capacity indicates the number of connection channels on the trunk port 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, this number is divided by the maximum number of virtual trunks on the port to get the default. This value is configured by **cnfrsrc** on BPXs.

Port Type	Max Conids
BXM/UXM	1-(#channels on card)
BNI T3/E3	1-1771
BNI OC-3	1-15867 (3837 max/VTRK)

Header Type—The cell header can be changed from NNI to UNI. UNI is the default for virtual trunks, but it may be necessary to configure this parameter to NNI to match the header type of the VPC provided by the cloud. This is a new configurable parameter for physical and virtual trunks.

Example

Configure virtual trunk 6.1.5 with the following command:

cnftrk 6.1.5 ....

```
node4        TRM    sall         IGX 16    9.2         Sep. 22 1998 16:35 PDT

TRK  6.1.5 Config       OC-3     [366792cps] UXM slot: 6
Transmit Trunk Rate:  353208 cps          Frame Scramble:       Yes
Rcv Trunk Rate:       353207 cps          Cell Framing:         STS-3C
Pass sync:            Yes                 Cell Header Type:     UNI
Loop clock:            No                 Virtual Trunk Type:   CBR
Statistical Reserve:  1000   cps          Virtual Trunk VPI:    20
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels:  256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,VBR,ABR

Last Command: cnftrk 6.1.5 ...........
```

cnftrkparm

Configures trunk parameters. The BXM and UXM virtual trunks have the same 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 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.

Syntax

cnftrkparm <slot>.<port>.<vtrunk> [options]

Example

```
cnftrkparm 4.1.1  .....
```

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX switch	

Related Commands

cnftrk, **cnfrsrc**

Parameters—cnftrkparm

	BXM		UXM	
Descriptions	**Physical**	**Virtual**	**Physical**	**Virtual**
Queue Depth - Voice	X	X	X	X
Queue Depth - NTS	X	X	X	X
Queue Depth - TS	X	X	X	X
Queue Depth - Bdata A	X	X	X	X
Queue Depth - Bdata B	X	X	X	X
Queue Depth - High Priority	X	X	X	X
Queue Depth - CBR	X	X	X	X
Queue Depth - VBR	X	X	X	X
Queue Depth - ABR	X	X	X	X
Max Age - Voice	X	X	X	X
Red Alm - I/O	X	X*	X	X*
Yel Alm - I/O	X	X*	X	X*
Lo/Hi CLP and EFCN Bdata A	X	X	X	X
Lo/Hi CLP and EFCN Bdata B	X	X	X	X

	BXM		UXM	
Descriptions	Physical	Virtual	Physical	Virtual
Lo/Hi CLP for CBR	X	X	X	X
Lo/Hi CLP for VBR	X	X	X	X
Low/Hi CLP, and EFCN for ABR	X	X	X	X
EPD and EFCN for CBR and VBR			X	X
SVC Queue pool size	X	X		
Gateway Efficiency			X	X*

dspload

Displays trunk loading

Sytax

dspload <slot>.<port>.<vtrunk>

Example:

Display loading of 13.3.12 with the following command:

dspload 13.3.13

```
node4        TRM    sall         IGX 16    9.2         Sep. 22 1998 16:35 PDT

Configured Trunk Loading:  TRK jerry 13.3.12 -- 4.2.10 george
    Load Type         Xmt-c      Rcv-c       Trunk Features
    NTS                   0          0       Terrestrial
    TS                    0          0       No ZCS
    Voice                 0          0       No Complex Gateway (this end)
    BData A               0          0       Virtual (CBR, Voice, NTS, TS)
    BData B               0          0
    CBR                1560       1560
    VBR                   0          0       Conids Used (Max):   1( 1874)
    ABR                   0          0
    Total In Use       1560       1560
    Reserved           1000       1000
    Available        350640     350640
    Total Capacity   353200     353200
--------------------------------------------------------------------------------
Last Command: dspload 13.3.12
```

dsprts

Displays the routes used by all connections on a node.

Syntax

dsprts

Example

Display routes by entering the following command:

dsprts

```
ziggy            TN       sall      BPX 15       9.2      June 9 1998 12:00 PDT

Channel      Route
10.1.1.1
             ziggy 13.3.12-- 4.2.10 rita
Pref:        Not Configured









--------------------------------------------------------------------------------
Last Command: dsprts
```

dsptrkcnf

Displays trunk configuration.

Syntax

dsptrk <slot>.<port>.<vtrunk>

Example

Display configuration of virtual trunk 6.1.5 with the following command:

dsptrkcnf 6.1.5

```
node4        TRM    sall         IGX 16    9.2         Sep. 22 1998 16:35 PDT

TRK  6.1.5 Config       OC-3     [366792cps] UXM slot: 6
Transmit Trunk Rate:  353208 cps          Frame Scramble:       Yes
Rcv Trunk Rate:       353207 cps          Cell Framing:         STS-3C
Pass sync:            Yes                 Cell Header Type:     UNI
Loop clock:            No                 Virtual Trunk Type:   CBR
Statistical Reserve:  1000   cps          Virtual Trunk VPI:    20
Idle code:            7F hex
Restrict PCC traffic: No
Link type:            Terrestrial
HCS Masking:          Yes
Payload Scramble:     Yes
Connection Channels:  256
Gateway Channels:     256
Valid Traffic Classes:
         V,TS,NTS,FR,FST,CBR,VBR,ABR

Last Command: dsptrkcnf 6.1.5 ...........
```

dsptrks

Displays basic trunk information for a node

Syntax

dsptrks

Example

Display trunks by entering the following command:

dsptrks

```
--------------------------------------------------------------------------------
ziggy            TN       sall      BPX 15     9.2     June 9 1998 12:00 PDT
TRK      Type      Current Line Alarm Status                           Other End
13.3.12  OC-3       Clear - OK                                          rita/4.2.10
9.1      T3        Clear - OK                                          damian/2.2









--------------------------------------------------------------------------------
Last Command: dsptrks
```

Configuration, BXM VSIs

This chapter provides a brief description of the BXM Virtual Switch Interfaces (VSIs) and some of the new features with Release 9.2. Refer to *Cisco WAN Switch Command Reference* for further details. Refer to Release Notes for supported features.

The chapter contains the following:

- Virtual Switch Interfaces
- VSI Master and Slaves
- Class of Service (COS) Templates

Virtual Switch Interfaces

Virtual Switch Interfaces (VSIs) allow a node to be controlled by multiple controllers such as MPLS, PNNI, and so on. These control planes can be external or internal to the switch.

When a virtual switch interface (VSI) is activated on a port, trunk, or virtual trunk for use by a master controller, such as a PNNI controller, or a MPLS controller, the resources of the virtual interface associated with the port, trunk or virtual trunk are made available to the VSI.

VSI Controller

A VSI controller, such as an MPLS controller, is added to a BPX switch using the **addshelf** command with the VSI option. In the MPLS case, the routing protocol such as OSPF, uses the Label Distribution Protocol (LDP) to set up MPLS virtual connections (VCs) on the switch.

Virtual Interfaces

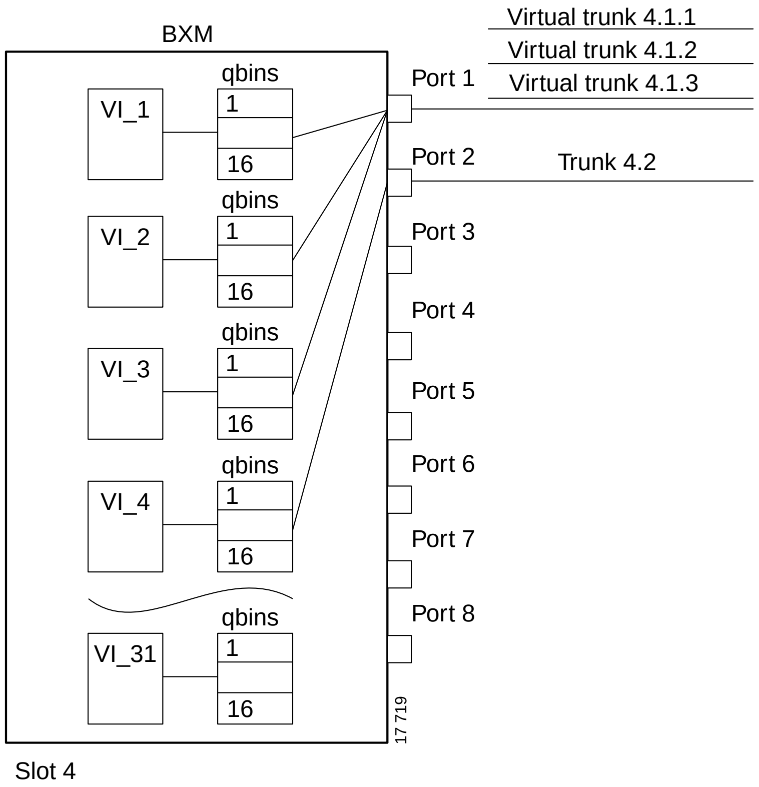
The BXM has 31 virtual interfaces that provide a number of resources including qbin buffering capability. One virtual interface is assigned to each logical trunk (physical or virtual) when the trunk is enabled. (See Figure 16-1.)

Each virtual interface has 16 qbins assigned to it. Qbins 0-9 are used for Autoroute and 10-15 are available for use by a VSI enabled on the virtual interface. (In Release 9.1, only qbin 10 was used.) The qbins 10-15 support class of service (CoS) templates on the BPX.

A virtual switch interface may be enabled 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, and each of these virtual trunks is assigned the resources of one of the 31 virtual interfaces on a BXM (see Figure 16-1).

Figure 16-1 BXM Virtual Interfaces and Qbins



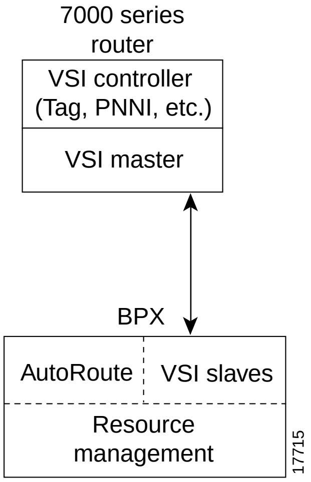
VSI Master and Slaves

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 16-2).

The controller sets up the following types of connections:

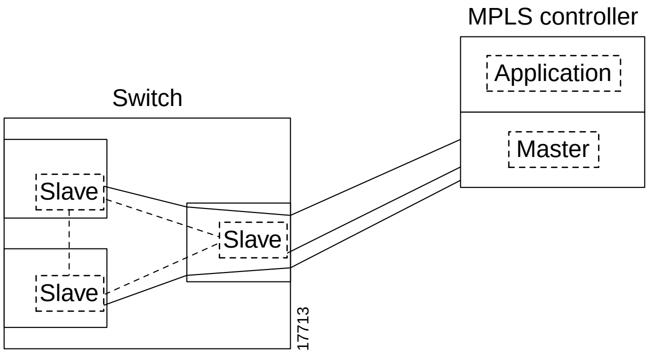
- Control virtual connections (VCs)
  - Master to Slave
  - Slave to Slave
- User Connection
  - User connection (that is, cross-connect)

Figure 16-2 VSI, Controller and Slave VSIs



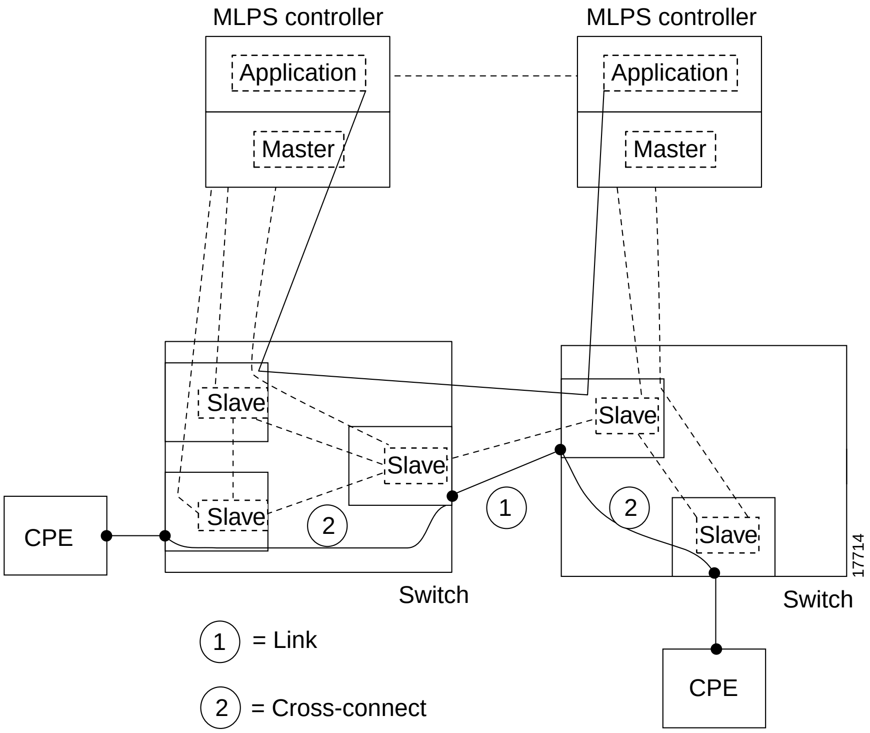
The controller establishes a link between the VSI master and every VSI slave on the associated switch. The slaves in turn establish links between each other (see Figure 16-3).

Figure 16-3 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 16-4.

Figure 16-4 Cross Connects and Links between Switches



Partitioning

Partitioning. The VSIs need to partition the resources between competing controllers, Autoroute, Tag, and PNNI for example. Partitioning is done with the **cnfrsrc** command.

Note Release 9.2.3 supports one or two partitions.

For Release. 9.1 and Release 9.2, just one controller (of a particular type) is supported. However, you can have different types of controllers splitting up a partition's assets. For example, Autoroute and tag, or Autoroute and PNNI (svcs), but not both PNNI and MPLS for Release 9.1 and Release 9.2.

The resources that need to be configured for a partition are shown in Table 16-1 for a partition designated ifci, which stands for interface controller 1 in this instance. The three parameters that need to be distributed are number of logical connections (lcns), bandwidth (bw), and virtual path ids (vpi).

Table 16-1 ifci Parameters (Virtual Switch Interface)

ifci parameters	Min	Max
lcns	min_lcnsi	max_lcnsi
bw	min_bwi	max_bwi
vpi	min_vpi	max_vpi

The controller is supplied with a logical lcn connection number, that is slot, port, and so on., information that is converted to a logical connection number (lcn).

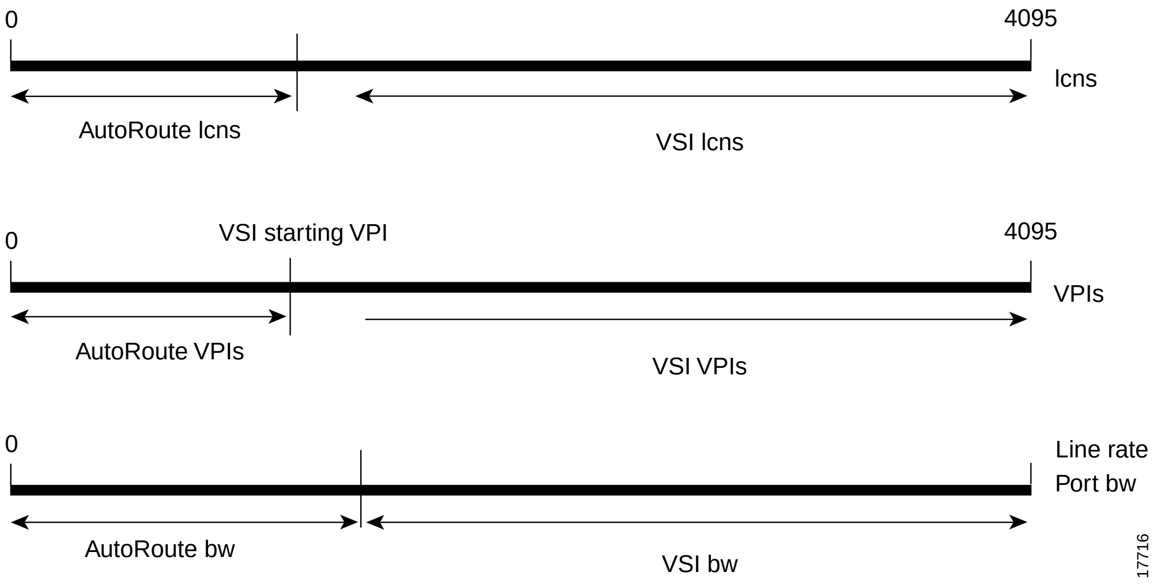
Some ranges of values available for a partition are listed in Table 16-2:

Table 16-2 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 Autoroute or vsi, not both

When a trunk is added, the entire bandwidth is allocated to Autoroute. To change the allocation in order to provide resources for a vsi, the **cnfrsrc** command is used on the BPX switch. A view of the resource partitioning available is shown in Figure 16-5.

Figure 16-5 Graphical View of Resource Partitioning, Autoroute and vsi



Class of Service Templates

Class of Service Templates (COS Templates) provide a means of mapping a set of standard connection protocol parameters to “extended” platform specific parameters. Full 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.

When you activate an interface with an **uptrk** or **upport** command, a default service template is automatically assigned to that interface. The corresponding qbin templates are simultaneously set up in the BXM’s data structure.

Functional Description

The service class template 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 (e.g., BPX) and downloaded to the service modules (e.g., BXMs) as needed.

The service templates contains two classes of data. One class consists of parameters necessary to establish a connection (that is, per VC) and includes entries such as UPC actions, various bandwidth related items, per VC thresholds, and so on. The second class of data items includes those 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 (e.g. 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
- Autoroute
- 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.

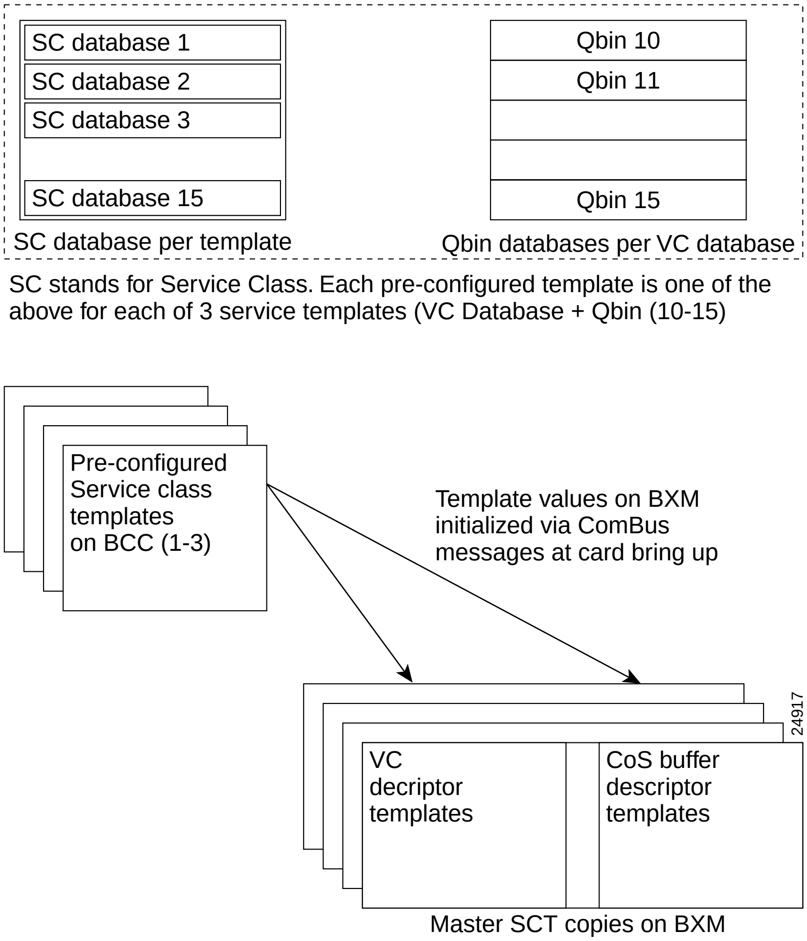
Service templates on the BPX are maintained by the BCC and are downloaded to the BXM cards as part of the card configuration process as a result of card activation, rebuild, or switchover. In Release 9.2 the templates are non-configurable.

There are 3 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 16-6.)

Figure 16-6 Service Template Overview


SC database 1
SC database 2
SC database 3
SC database 15
SC database per template
Qbin 10
Qbin 11
Qbin 15
Qbin databases per VC database
SC stands for Service Class. Each pre-configured template is one of the above for each of 3 service templates (VC Database + Qbin (10-15)
Pre-configured Service class templates on BCC (1-3)
Template values on BXM initialized via ComBus messages at card bring up
VC decriptor templates
CoS buffer descriptor templates
Master SCT copies on BXM
24917

Structure

When the **upport** or **uptrk** command is used to activate an interface on the BXM card, the default service template, which is MPLS1, is assigned to the interface. This service template has an indentifier of “1”. The service template assigned to an interface can be changed with the **cnfvsiif** command. This can be done only when there are no active VSI connections on the BXM. The templates can be displayed with the **dspvsiif** command.

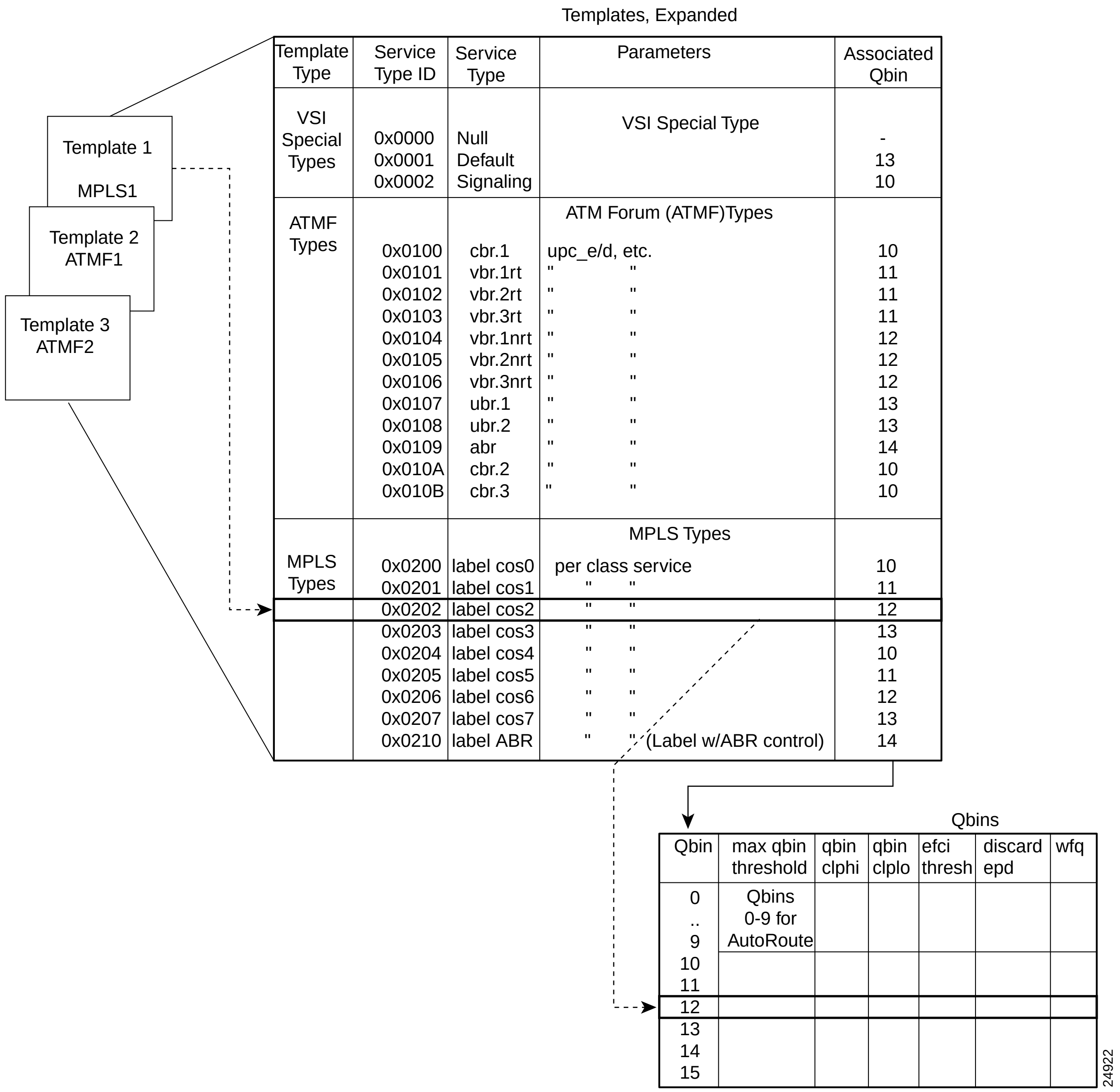
Each template table row includes an entry that defines the qbin to be used for that class of service (see Figure 16-7).

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.

Qbin templates only are used with qbins that are available to VSI partitions, namely qbins 10 through 15. Qbins 10 through 15 are used by the VSI on interfaces configured as trunks or ports. The rest of the qbins (0-9) are reserved for and configured by Autoroute.

Figure 16-7 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						

Downloading Service Templates

Service templates are downloaded to a card (BXM) under the following conditions:

- add y-red card
- on a BCC (control card) switchover
- when a card has active interfaces and is reset (Hardware reset)
- on a BCC (control card) rebuild

Assignment of a Service Template to an interface

A default service template is assigned to a logical interface (VI) when the interface is upped via upport/uptrk.

For example:

- **uptrk 1.1**
- **uptrk 1.1.1 (virtual trunk)**
- **upport 1.1**

This default template has the identifier of 1. Users can change the service template from service template 1 to another service template using the **cnfvsiif** command.

The **cnfvsiif** command is used to assign a selected service template to an interface (VI) by specifying the template number. It has the following syntax:

cnfvsiif <slot.port.vtrk> <tmplt_id>

For example:

- **cnfvsiif 1.1 2**
- **cnfvsiif 1.1.1 2**

The **dspvsiif** command is used 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**

Card Qbin Configuration

When an interface (VI) is activated by **uptrk** or **upport**, the default service template is assigned to the interface (VI). The corresponding qbin template is then copied into the card’s (BXM) data structure of that interface. A user can change some of the qbin parameters using the **cnfqbin** command. The qbin is now “user configured” as opposed to “template configured”. This information may be viewed on the **dspqbin** screen.

Qbin dependencies

The available qbin parameters are shown in Table 16-3. Notice that the qbins available for VSI are restricted to qbins 10-15 for that interface. All 31 possible virtual interfaces are each provided with 16 qbins.

Table 16-3 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	u sec	1-2000000
QBIN CLP High Threshold	% of max Qbin threshold	0 - 100
QBIN CLP Low Threshold	% of max Qbin threshold	0 - 100
EFCI Threshold	% of max Qbin threshold	0 - 100
Discard Selection	enumeration	1 - CLP Hystersis 2 - Frame Discard
Weighted Fair Queueing	enable/disable	0: Disable 1: Enable

Additonal service template commands are:

dspsct: This command is used to display the 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> SC lists all the parameters of that Service Class.

dspqbintmt: displays the qbin templates.

cnfqbin {configures the qbin, The user can answer yes when prompted and the command will used the card qbin values from the qbin templates.

dspqbin {displays qbin parameters currently configured for the virtual interface.

dspvsipartinfo {displays some VSI resources for a trunk and partition.

dspcd {display the card configuration.

Extended Services Types Support

The service-type parameter for a connection is specified in the connection bandwidth information parameter group. The service-type and service-category parameters determine the service class to be used from the service template.

Connection Admission Control

For Release 9.2, 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.

Note Service templates used for egress traffic are described here. Ingress traffic is managed differently and a pre-assigned ingress service template containing CoS Buffer links is used.

Supported Service Types

The service type identifier is a 32-bit number. In Release 9.2.30, there are three service types: VSI Special Type, ATMF Types, and MPLS types. A list of supported service types is shown in Table 16-4.

Table 16-4 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 16-5 through Table 16-8. Table 16-9 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 16-5 lists the parameters associated with Default (0x0001) and Signaling (0x0002) service template categories.

Table 16-5 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 16-6 and Table 16-7 lists the parameters associated with the PNNI service templates.

Table 16-6 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	-	-	-	-	-	*
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 16-7 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 16-8 lists the connection parameters and their default values for tag switching service templates.

Table 16-8 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 16-9 describes the connection parameters that are listed in the preceding tables and also lists the range of values that may be configured, if not pre-configured.

Every service class does not include all parameters. For example, a CBR service type have fewer parameters than an ABR service type.

Note Every service class does not have a value defined for every parameter listed in Table 16-9 below.

Table 16-9 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. tag'd cells	enumeration
Policing Action (GCRA #2)	0 - Discard 1 - Set CLP bit 2 - Set CLP of untagged cells, disc. tag'd cells	enumeration
VC Max		cells
CLP Lo	0 - 100	%Vc Max
CLP Hi	0 - 100	%Vc Max
EFCI	0 - 100	%Vc Max
VC Discard Threshold Selection	0 - CLP Hysteresis 1 - EPD	enumeration

Table 16-9 Connection Parameter Descriptions and Ranges (Continued)

Object Name	Range/Values	Template Units
VSVD	0: None 1: VSVD 2: VSVD w / 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

SONET APS, Configuration

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. Refer to the *Cisco WAN Switch Command Reference* for further information on configuration and monitoring commands.

This chapter contains the following:

- Introduction
- 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 Alarms
- APS K1 Command Precedence
- Command Reference
- Troubleshooting Notes

Introduction

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 17-1 and shown in Figure 17-1 and Figure 17-2, respectively. APS 1+1 Annex B has the same general layout as shown in Figure 17-1, except that the active line is called the primary, and the standby line is referred to as the secondary.

Table 17-1 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 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.

Automatic 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.

Upon detection of a signal fail condition (that is, LOS, LOF, Line AIS, or Bit Error Rate in excess of a configured limit) or a signal degradation condition (that is, BER exceeding a configured limit), the hardware switches from the working line to the protection line. This case assumes that the working line was the active line and the protection line was not in alarm.

If the "Revertive" option is enabled, (**cnfapsln** command), the hardware switches back to the working line from the protection line after a configured time period called "Wait to Restore" (**cnfapsln** command) has elapsed. The working line must be in a clear state for this to occur. The revertive option is the default for APS 1:1 but not for APS 1+1.

Coordination between the interfaces on the two ends of the lines is provided via an in-band protocol.

Manual Operation

The **switchapsln** command may be used to control switching manually. 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 17-1 APS 1+1 Redundancy

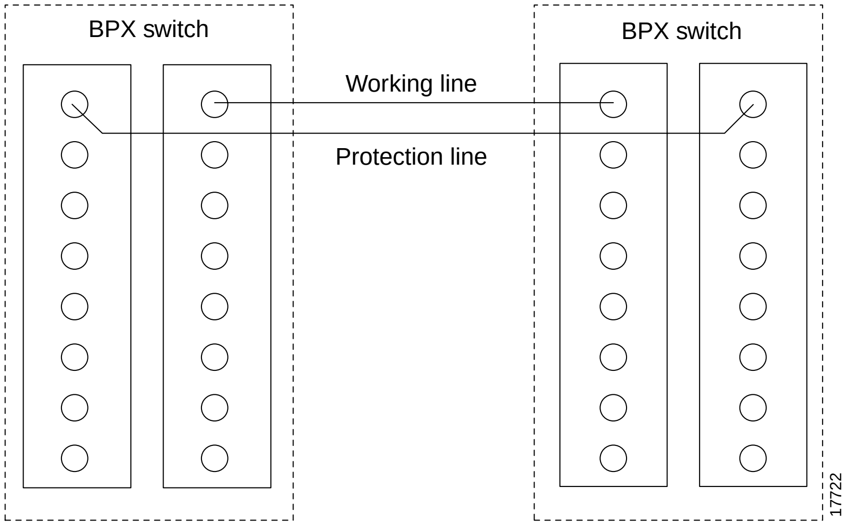
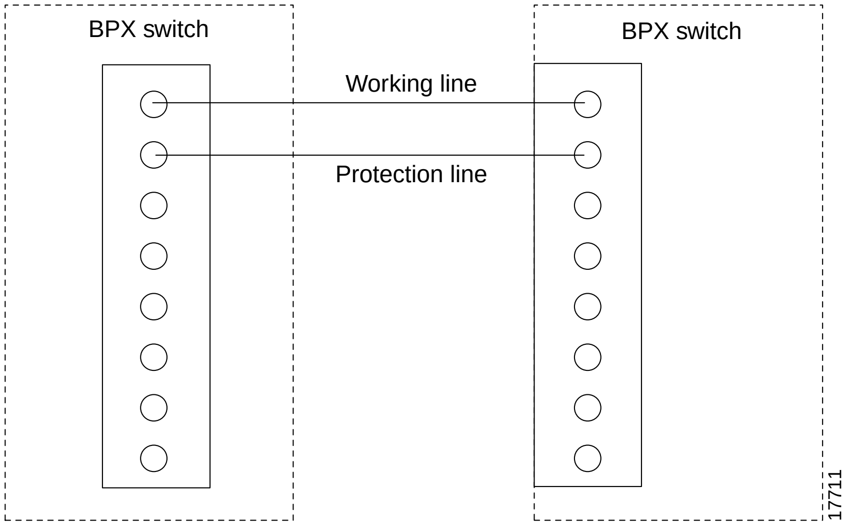


Figure 17-2 APS 1:1 Redundancy



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 17-2.

Table 17-2 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 17-3.

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 17-3 BXM Back Card for APS 1+1 LED Display

LED	Description
Green	The card has at least one active line and may not be removed without affecting service.
Yellow	The card has no active lines and my be removed.
Red	Not used and not applicable.

APS 1+1 (Card and Line Redundancy)

The APS 1+1 feature requires two BXM front cards, an APS redundant frame assembly, and two redundant type BXM backcards. The two redundant BXM backcards are plugged into the APS redundant frame assembly as shown in Figure 17-3. The types of available backcards are:

The types of redundant backcard and backplane sets required are:

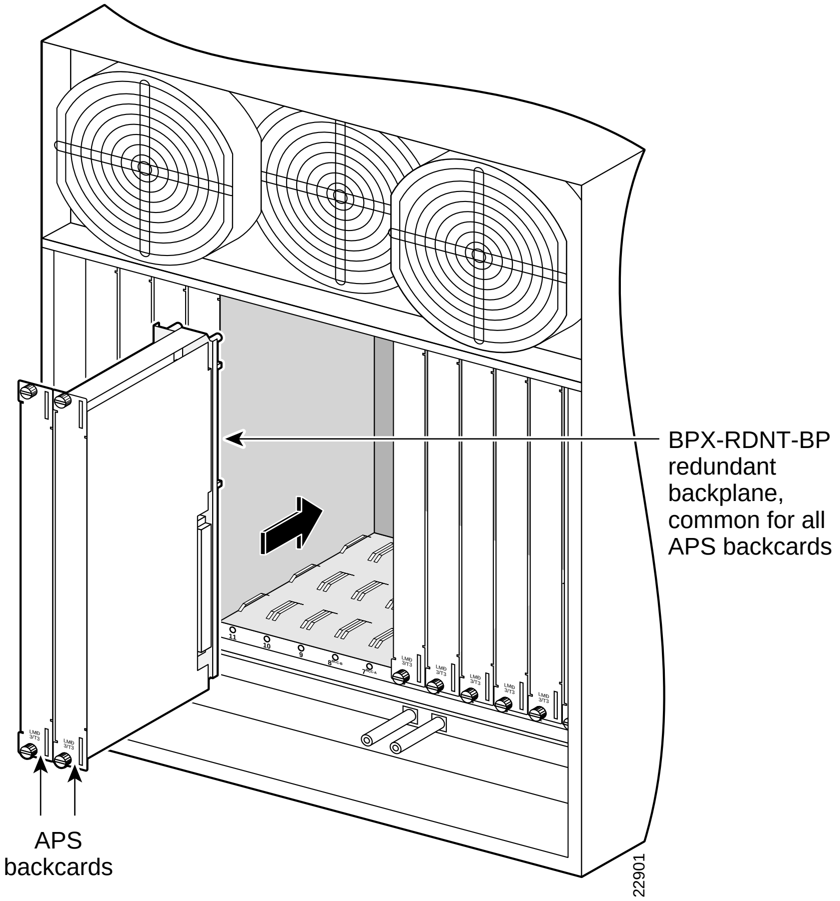
- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622-2 (2 port, long reach, SMF, FC connector)
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- 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)

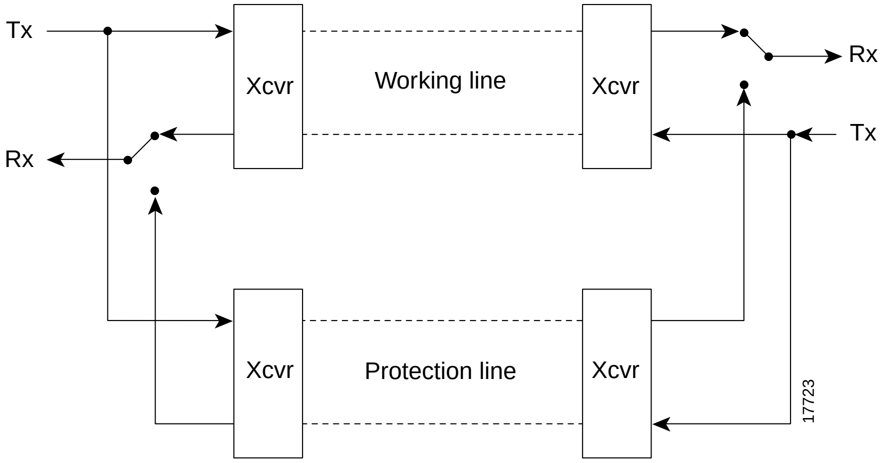
Figure 17-3 APS 1+1 Redundancy, Installing APS Backcards in APS Redundant Backplane



Traffic protected by APS 1+1 redundancy is carried via the working line and the protection line simultaneously (see Figure 17-4). 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 17-4 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 etc.).

APS +1 Redundancy Criteria

The APS 1+1 redundancy is implemented by first setting up Y-redundancy, then adding APS.

When card redundancy is implemented, the two BXM front cards must reside in the same two adjacent slots as the APS backcards which must be 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 and 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, etc.

The user may add APS at any time after Y-redundancy is configured as long as the protection line is in the standby state. The user 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.

Other Notes:

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.

Some switchapsln Notes

With APS 1+1, when repetitive **switchapsln** commands are issued, up to two in a row can be executed sequentially, when alternating between options 3 and 4 (forced switch), or 5 and 6 (manual switch), but no more. Attempts to execute a third **switchapsnln** will not succeed, and the following error message is displayed:

```
“Cannot request manual W->P when manual P->W switch in progress”
```

If users desire to perform repetitive switchapsln commands, they need to issue a clear switch between each W-P, P-W pair of commands, for example:

```
switchapsln 2.1  1
```

Configuration Procedure, APS 1+1

The following is an example of configuring APS 1+1 redundancy:

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 **the following commands** and verify chan half= no, and standard= GR-253 (default)

cnfcdaps 2.1 N 1

cnfcdaps 3.1 N 1

Step 4 Execute the following command, for example, for 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)

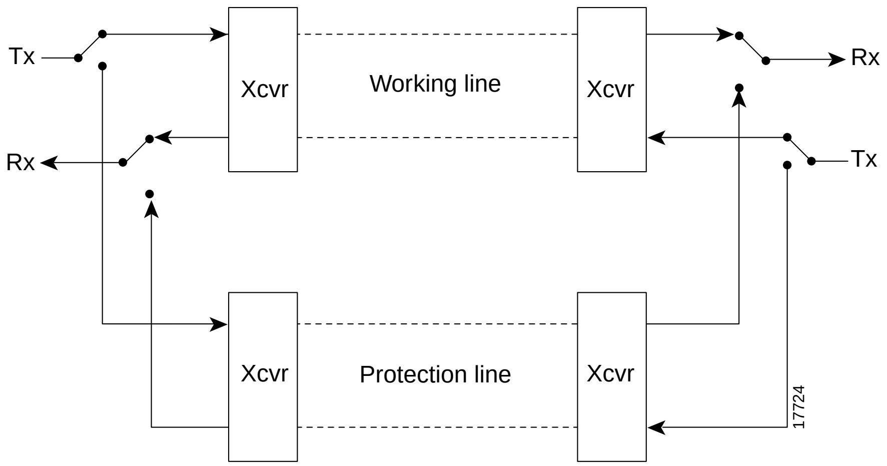
The APS 1:1 feature provides port and line redundancy for a single BXM front card and associated OC-3 or OC-12 redundant backcard.

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 17-5). 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. Since 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 equipments at both ends and thus is more complex.

Figure 17-5 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.

Configuration Procedure, APS 1:1

The following is an example of configuring APS 1:1 redundancy:

Note Before configuring for APS 1:1 redundancy, all card connections must be deleted using the **delcon** command

Step 1 Ensure that lines are connected, for example on ports 1 and 2 of a BXM in slot 3.

Note The last entry, “2”, in the **addapsln** command specifies the type of APS, in this example APS 1:1.

Step 2 Execute **cnfcdaps** and verify chan half= yes (not default), and standard= GR-253 (default)

cnfcdaps 3.1 Y 1

Step 3 **addapsln** 3.1 3.2 2 {addapsln<slot.port> <slot.port> <1|2|3|4|5>

Step 4 **upln** 3.1 {or uptrk, as applicable

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 only be configured for bi-directional operation and non-revertive switching on a line.

Note In non-revertive switching, to avoid data loss, a line is not automatically switched back to active after a failure is corrected.

Configuration Procedure, APS 1+1 Annex B

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** are service affecting even when APS is configured. In all APS configurations if the working line is looped, both lines will be looped and traffic disrupted.

Notes on APS Messages

When adding an APS 1+1 line or trunk using addapsln, if the working slot’s paired redundant slot is not a legal protection slot, or if firmware can’t 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.”

The redundant card information can be displayed with 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”. The following example is of dspcd 2:

```
swwye     TN       silves        BPX8620      9.2.20       Aug. 9  1999

Detailed Card Display for BXM-155 in slot 2

Status:          Active
Revision:        DDA                   Backcard Installed
Serial Number    652774                  Type:          LM-BXM
Fab Number       28-2158-02              Revision       EW
Queue Size       228300                  Serial Number  1..1...
Support: 4 Pts, OC-3, FST,  VcShp         Supp: 4 Pts, OC-3, SMF, RedSlot:3
Support: VT, ChStLv 2, VSIlvl 2
Support: APS (FW, HW1+1)
Support: OAMLp, TrfcGen
#Ch: 8128, PG[1] :8123
#Sched_Ch:16284

Last Command: dspcd 2
```

APS Alarms

The APS alarms are listed in Table 17-4. The listing includes the class or state of the alarm, minor, major, info, or clear.

Statistical Alarms

Statistical alarms are not cleared when a YRED switch occurs. The user can clear these stats as appropriate.

Note On the active line/trunk, alarms (e.g., LOS and LOF) and statistics (e.g., 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 17-4 APS Alarms

Class	Name	Description
Minor	APS Standard Mismatch	In a 2 card APS 1+1 configuration, one card is programmed for GR-253 and the other card is programmed for ITUT.
Minor	APS Card Missing	Indicates that either a BXM frontcard or backcard supporting this APS line is detected as missing by a BXM.
Clear	APS OK	APS line is up with no alarms.
Clear	APS Deactivated	APS line is down.
Minor	APS Lines looped	APS line is looped.
Minor	APS Remote Signal Failure	A remote signal failure indicates that there is a problem with the far end signalling information in the K1K2 bytes.
Minor	APS Channel Mismatch	Can only happen in bidirectional mode and indicates that there is a problem with the underlying APS channel protocol. The receive K2 channel number does not equal the transmit K1 channel number.
Minor	APS Protection Switch Byte Failure	Protection Switch Byte failure or PSB. In bidirectional mode indicates that there is an invalid K1 byte. The receive K1 request does not match the reverse request and is less than the transmit K1 request. In all modes a PSB alarm indicates that K1/K2 protocol is not stable.
Minor	APS Far End Protection Failure	Far end protection failure indicates that the far end’s protection line is failing. When there is Signal Failure on the protection channel, the remote end sees Far End Protection Fail.
Minor	APS Architecture Mismatch	Architecture mismatch means that the APS configuration on one end of the line does not match the APS configuration at the other side of the line. Specifically GR-253 at one end and ITUT at the other or 1+1 at one end and 1:1 at the other.
Info	APS Init/Clear/Revert	A BXM APS event indicating that the BXM APS has been initialize or a clear switch has occurred or a revert switch has occurred.
Info	Cannot perform a Clear/Revert switch	A BXM APS event indicating that the BXM APS was unable to perform a clear or revertive switch.
Info	APS Manual switch	A BXM APS event indicating that the BXM APS has performed a user requested manual switch.
Info	Cannot perform a Manual switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested manual switch.
Info	APS Signal Degrade LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal degrade condition. An automatically initiated switch due to a “soft failure” condition resulting from the line BER exceeding a pre-selected threshold (**cnfapsln**).
Info	Cannot perform a Signal Degrade LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal degrade condition.

Table 17-4 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 pre-selected threshold (**cnfapsln**).
Info	Cannot perform a Signal Degrade HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal degrade condition.
Info	APS Signal Failure LoPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a low priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a Signal Failure LoPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a low priority signal failure condition.
Info	APS Signal Failure HiPri switch	A BXM APS event indicating that the BXM APS performed a switch due to a high priority signal failure condition. An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
Info	Cannot perform a Signal Failure HiPri switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a high priority signal failure condition.
Info	APS Forced switch	A BXM APS event indicating that the BXM APS has performed a user requested forced switch.
Info	Cannot perform a Forced switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested forced switch.
Info	APS Lockout switch	A BXM APS event indicating that the BXM APS has performed a user requested switch which prevents switching from working line to protection line from taking place.
Info	Cannot perform a Lockout switch	A BXM APS event indicating that the BXM APS was unable to perform a user requested lockout of protection switch.
Info	WTR switch	A BXM APS event indicating that the BXM APS performed a switch due to a Wait to Restore timeout. A state request switch due to the a revertive switch back to the working line because the wait-to-restore timer has expired.
Info	Cannot perform a WTR switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a WTR condition.
Info	Exercise switch	Not supported.
Info	Cannot perform a Exercise switch	Not supported.
Info	Reverse switch	A BXM APS event indicating that the BXM APS performed a switch due to a reverse request. A state request switch due to the other end of an APS bi-directional line performing an APS switch.

Table 17-4 APS Alarms (Continued)

Class	Name	Description
Info	Cannot perform a Reverse switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a reverse switch request.
Info	No Revert switch	A BXM APS event indicating that the BXM APS performed a switch due to a Do not Revert. A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
Info	Cannot perform a No Revert switch	A BXM APS event indicating that the BXM APS was unable to perform a switch due to a Do not Revert switch request.
Minor	Standby Line Section Trace	APS standby line alarm.
Minor	Standby Line Path Trace	APS standby line alarm.
Minor	Standby Line path yellow alarm	APS standby line alarm.
Minor	Standby Line path AIS	APS standby line alarm.
Minor	Standby Line loss of pointer	APS standby line alarm.
Minor	Standby Line loss of cell	APS standby line alarm.
Minor	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 1 side supports 1+1 and other end of 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.

APS K1 Command Precedence

The possible conditions which may cause/prevent a switch are listed in Table 17-5. 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 17-5 K1 Switching Conditions

APS K1 Command Precedence
Lock out of Protection
Forced Switch

Table 17-5 K1 Switching Conditions

APS K1 Command Precedence
Signal Fail
Signal Degrade
Manual Switch
Wait To Restore
Reverse Request
Do not Revert
No Request

Command Reference

APS Command Summary

A number of commands have been added and modified to support APS. These are listed in Table 17-6, and defined in more detail in the following pages. Refer to the *Cisco WAN Command Reference* for information on commands not described here and for additional detailed information on commands.

Table 17-6 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.

addapsln/delapsln

The **addapsln** command adds APS for BXM OC-3 or OC-12 lines. The user specifies the desired APS Protocol when adding a new APS line pair. The **delapsln** command deletes APS for the lines.

Syntax

addapsln <slot.port1> < slot.port2> <protocol>

Parameter	Description
slot.port1	The desired working line number.
slot.port2	The desired protection line number.
protocol	1: 1+1 2: 1:1 3: 1+1 Annex B 4: 1+1 Ignore K1K2 bytes

When the command is exercised, the switch software does the following:

- Verifies that the slot.port arguments support APS.
- Verifies that the appropriate backcard is installed.
- Verifies that the protection port is not already active.
- If card redundancy is already configured for the 2 slot case (APS 1+1), verifies that the primary card is the same type as the working line card.

Example:

The user is required to enter the slot.port pair and the protocol option. If the user does not enter the protocol option a menu listing the options is displayed.

```
Example:

alexa       TRM    genre    BPX 15        9.2         Sep. 9 1998          16:08 PDT

                            Actv     Current Line      Current APS          Last User
Work/Protect    Protocol    Line     Alarm Stat        Alarm StatCard       Switch Req
2.1 3.1         1+1         WORK     OK                APS OK               Clear

Command: addapsln 2.1 3.1 1
```

addcdred

Note Entering addcdred or addyred executes the same command. The newer name is addcdred which replaces addyred, but addyred may still be used for those familiar with that command.

The **addcdred** command enables card and line redundancy for the cards on the IGX and BPX. It lets you add card and line redundancy for APS 1+1 across two BXM OC-3 or OC-12 cards. You also use it before enabling APS 1:1 line redundancy. It works similarly to the addyred command.

Syntax

addcdred <primary slot> <secondary slot>

Example 1

```
addcdred 2 3
```

Related Commands

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

Attributes

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

Table 17-7 addcdred–Parameters

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

Description

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

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

When configuring APS 1+1 card and line redundancy, you must execute the **addcdred** command before using **addapsln**.

Redundant card sets must have the following characteristics:

- The primary and secondary card sets must be identical.
- For APS 1+1 card redundancy only, the primary and secondary card sets must reside in adjacent slots. (This restriction only applies to APS 1+1 Card and Line Redundancy.) APS 1+1 is not supported on a single-card option.
- Secondary card sets must not currently be active.

- Neither the primary nor secondary card set may already be part of a redundant set.
- Redundancy applies to the entire card and not specific trunks or lines.

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

Note When SONET Automatic Protection Switching (APS) is configured in release 9.2, you will not be able to use the **addyred** or **delyred** commands on a card configured for APS 1:1 architecture. That is, you will not be able to execute the **addyred** command, then configure the APS 1:1 architecture. Similarly, you will not be able to configure APS 1:1, then execute the **addyred** command. You will be blocked from executing these commands at the command line interface.

In Release 9.2, to ensure that only cards with the Idle Code Suppression feature enabled on them are allowed to be a Y-redundancy pair, **addcdred** blocks cards that have different idle code suppression capability.

cnfapsln

The **cnfapsln** command allows the user to configure various APS line parameters.

Syntax

cnfapsln <slot.port> <SFBER> < SDBER> <Revertive_mode> <WTR> <Direction>

Parameter	Description	Range
slot.port	Slot and port of the line to be configured.	-
SFBER	Signal Fail Bit Error Rate threshold which will cause an APS switch.	Default 3, range 3 - 12
SDBER	Signal Degrade Bit Error Rate for line degradation.	Default 5, range 5 - 12
Revertive mode	Revert to Working line after WTR interval expires. User enters numeral 0 or 1. This only applies to automatic switches. Revertive switching does not take place as a result of user-initiated switching.	Default 1, range 0, 1 0 = revertive 1 = non-revertive
WTR	Wait to restore interval. After a switch from a Working to a Protection line, this is the interval in minutes to wait before attempting to switch back to the Working line. This is not applicable if the Revertive Mode option is set to N (Non-revertive).	Default 5: range 1 - 12 minutes
Direction	Direction of switching. Uni-directional is switching in only one direction. With Bidirectional, after one side switches, then the other side also switches.	Default is 0, unidirectional, range 0/1 where 0 is unidirectional and 1 is bidirectional.

```
Example:
```

```
alexa       TRM    genre        BPX 8620      9.2         Sep. 9 1998    16:15 PDT

APS Configuration parameters for Working, Protection lines 1.1, 1.2

APS Protocol:                                         1+1

Signal Fail BER threshold (10 to the -n):             3
Signal Detect BER threshold (10 to the -n):           5
Revertive Switching:                                  Yes
Wait to Restore Timer:                                5 minutes
Uni/Bi Directional Switching:                         Unidirectional

Command:cnfapsln 1.1
```

cnfcdaps

The **cnfcdaps** command sets the APS 1:1 channels option and the APS standard option on the card.

Syntax

cnfcdaps <slot> <Y/N> < 0/1>

Parameter	Description
slot	Specifies the desired BXM APS slot number.
Y/N	Disable/Enable the channels option on the card.
0/1	0 = ITUT, 1 = GR253

When the command is exercised, the switch software does the following:

- Checks that the slot is a BXM OC-3 or OC-12 card.
- Verifies that the BXM card version supports APS.
- Issues a warning if any trunks or lines are upped on the card, and if so, issues a warning that a card mismatch may occur.
- Issues a warning if this card is Y redundant and its redundant card has a different APS standard configured.

```
bpx1           TN    StrataCom       BPX 8620  9.2    May  11 1999 09:38 PDT
>
>APS Card Configuration parameters for card 6
>
>Channels Halved for APS operation:              Yes
>APS Standard for Card:                          GR-253
>
>
>
>
>
>
>
>
>
>
>
>
>This Command:cnfcdaps 6
>
>
>Enter channels halved option (Y or N):
>
```

dspapsln

The **dspapsln** command displays the currently configured APS lines and their status.

Syntax

dspapsln

```
>bpx1           TN    StrataCom       BPX 8620  9.2    May  11 1999 09:37 PDT
>
>             Actv Active Line      Standby Line     Current APS      Last User
>Work/Protect Line Alarm Status     Alarm Status     Alarm Status     Switch Req
> 6.3  6.4    WORK OK               OK               APS OK           Clear
> 6.5  6.6    WORK OK               OK               APS OK           Clear
> 6.7  6.8    PROT OK               Loss of Sig(RED) Loss of Sig(RED) Clear
>10.1 11.1    WORK OK               OK               APS OK           Clear
>10.2 11.2    WORK OK               OK               APS OK           Clear
>10.3 11.3    NONE Deactivated      APS Deactivated  APS Deactivated  Clear
>10.4 11.4    NONE Deactivated      APS Deactivated  APS Deactivated  Clear
>10.5 11.5    NONE Deactivated      APS Deactivated  APS Deactivated  Clear
>10.6 11.6    NONE Deactivated      APS Deactivated  APS Deactivated  Clear
>10.7 11.7    WORK OK               OK               APS OK           Clear
>10.8 11.8    WORK OK               OK               APS OK           Clear
>
>
>Last Command:dspapsln
```

dsplog/dspalms

Syntax

dsplog

dspalms

APS alarms are displayed with the **dsplog** command, and propagated to the Cisco WAN Manager. Refer to Notes on APS Messages on page 17-14, in the preceding paragraphs, for a listing that includes the Class and **dsplog** text of each APS alarm.

Also, the **dspalms** command includes a row for APS alarms.

```
Example:

alexa       TRM    genre         BPX 15      9.2       May. 9 1998           16:35 PDT


Alarm summary   (Configured alarm slots: None)
Connections Failed:                                    None
TRK Alarms:                                                None
Line Alarms:                                               None
Cards Failed:                                              None
Slots Alarmed:                                             1 Major
Missing Cards:                                             1
Remote Node Alarms:                                        1 Minor
Remote Domain Alarms:                                      None
APS Alarms:                                  1 Major, 1 Minor

Interface Shelf Alarms:                                    None
ASM Alarms:                                                None




Last Command: dspalms
```

switchapsln

The **switchapsln** command controls the APS user switching interface.

Syntax

switchapsln<slot.port> <switchoption> [S]

Parameter	Description	
slot.port	The desired working line number	
switch option	1. Clear	Clears last user request.
	2. Lockout	Prevents specified APS pair from being switched to protection line. If protection line is already active, switch is made back to the working line.
	3. Forced switch (Working to Protection line)	Forced Working to Protection line switch. If Working line is active, switch is made to Protection line unless the Protection line is locked out or in the SF condition or Forced Switch is already in effect. Forces hardware to switch to the Protection line even if it is in alarm.
	4.Forced switch (Protection to Working line)	Protection line is active, switch is made to Working line unless a request of equal or higher priority is in effect. This Protection to Working line switch only applies to APS 1+1.
	5. Manual switch (Working to Protection Line)	Switch from Working to Protection line unless a request of equal or higher priority is in effect. **Note** Not applicable to APS 1+1, Annex B.
	6. Manual switch (Protection to Working line)	This Protection to Working line switch only applies to APS 1+1. **Note** Not applicable to APS 1+1, Annex B.
S	If S is entered as an additional parameter, a service switch is performed for all ports on the card such that all lines are forcibly switched to one backcard so that the other card of the pair can be removed for service. Be sure that the associated frontcard is active for the backcard that is to remain in the rack. You may have to perform a **switchcdred** command so that the backcard that the service switch changes to has its associated front card active.	

switchcdred/switchyred

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

Syntax

switchcdred <slot.port> <slotport>

Example 1

```
switchcdred
```

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

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

Typically, when APS and card redundancy are implemented together, the term Y-redundancy actually refers to card redundancy because there is no Y cable connecting two backcards to one line. With SONET APS 1+1 card redundancy, there is a primary and a secondary front card/back card pair. The redundant front card must be in Hot Standby state before a switchover can occur. When a front card failure is detected, the switchover should happen automatically (when card redundancy has been implemented). However, for the APS application, the active line is not switched if the line status is good. If the line has Loss of Signal (or other defects), it will be switched to the redundant line. (The line refers to the physical cable attached to the output of the backcard.)

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

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

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

Other Notes:

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** 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.

Troubleshooting Notes

Introduction

Automatic Protection Switching (APS) is the ability to configure a pair of SONET lines for line redundancy so that hardware automatically switches from a Working line to a Protection line when the Working line fails, and vice versa. Each redundant line pair consists of a Working Line and a Protection Line. The concept of Working and Protection Lines is similar to the concept of Primary and Secondary Y Redundant cards. That is, the Working line is the logical line which the user refers to.

Left undisturbed, hardware performs line switching automatically. Upon detection of a Signal Fail condition (LOS, LOF, Line AIS or Bit Error Rate exceeding a configured limit) or a Signal Degrade condition (BER exceeding a configured limit), hardware switches from the Working Line to the Protection Line (assuming the Working line was the Active line and the Protection line is not in alarm). If the Revertive option is Enabled, hardware switches back to the Working line automatically after a configured time period called Wait to Restore has elapsed (assuming the Working line is now OK). Coordination between the two ends of the line is accomplished using the in-band protocol.

During setup, the commands **addapsln**, **cnfcdaps**, and **cnfapsln** are used to create the line-redundant pair. Also, appropriate front cards, back cards, and a special RDNT-BP daughter backplane are required for APS 1+1 configurations.

During operation, signal failure or signal degradation can cause APS “switchovers”. A switchover is when the line that was active gives up control to its partner line. This partner line now becomes the “active” line, while the original active line becomes the “standby” line.

For APS line redundancy, the following problems can occur:

- APS Configuration Problems on page 17-31
  - Not Able to Correctly Set Up APS 1+1 Line Redundancy Configuration on page 17-31
  - Unable to set up APS 1:1 line redundancy configuration on page 17-31
  - Operator information about APS architectures on page 17-32
- Operational Problems on page 17-33
  - What the various APS switches mean on page 17-33
  - Unable to perform APS external switch after forced or manual APS switch. on page 17-33
  - APS manual switch to a line does not occur right away. on page 17-34
  - Switch occurs after lockout issued. on page 17-34
  - APS switch made to a line in alarm. on page 17-34
  - Reverse switch on page 17-35
  - APS switch occurs at the same time as a yred switch. on page 17-35
  - APS switch occurs after issuing an APS clear switch. on page 17-36
  - APS Switch Occurs even though APS Forced switch in effect. on page 17-36
  - APS line is failing to switch on page 17-36
  - Large cell loss when performing a front card switchover on page 17-37
  - APS service switch description on page 17-37
  - APS line does not seem to switch and active line is in alarm on page 17-37

APS Configuration Problems

The following sections describe possible APS configuration problems.

Not Able to Correctly Set Up APS 1+1 Line Redundancy Configuration

Description

The **addapsln** user interface command fails to execute correctly for APS 1+1 line addition.

Initial Investigation

The **addapsln** command is used to setup the APS line redundancy configuration. For APS 1+1 configurations, BPX software supporting APS and BXM firmware supporting APS must be used. Also the following hardware requirements must be met:

- BXM-Enhanced OC-3 or OC-12 front cards. BXM -155-4 or BXM-155-8 frontcard 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 backcards (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 backcard 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 backcard frame.
- A newer backcard frame removes the slot restriction of having to put daughter backplane and APS backcards in slots 2-5 and 10-13.

Workaround

None.

Unable to set up APS 1:1 line redundancy configuration

Description

The **addapsln** user interface command fails to execute correctly for APS 1:1 line addition.

Initial Investigation

For APS 1:1 configuration, two adjacent lines on the same card are used. No special hardware is required however the maximum connections supported must be reduced by half using the **cnfcdaps** command. FW and SW support of APS is required.

Workaround

APS 1:1 can be run on non APS enhanced BXM card by halving the number of channels the card can support (**cnfcdaps**). No special backcards are needed for APS 1:1.

Detailed Debugging

For APS 1:1 configuration the APS line must be configured (**addapsln**) before a line (**upln**) or trunk (**uptrk**) can be upped. Conversely, the line or trunk must be downed before the APS line can be deleted (**delapsln**). Use **dspapsln** to verify that the APS line has been added.

Operator information about APS architectures

Description.

The **cnfapsln** user interface command fails to allow the user to configure any combination of APS architectures.

Initial Investigation.

The APS configuration can be changed using the **cnfapsln** command, however not all combinations are allowed. Here is a table of combinations allowed and disallowed.

Table 17-8 Possible APS System Architectures

	APS 1:1		**APS 1+1, 1+1 ignore K1**		**APS 1+1 Annex B**	
Mode	**Revertive**	**Non-revertive**	**Revertive**	**Non-revertive**	**Revertive**	**Non-revertive**
Bi-directional	Default	Not Valid	Valid option	Valid option	Not Valid	Default
Uni-directional	Not Valid	Not Valid	Valid option	Default	Not Valid	Not Valid

Once the APS configuration 1+1, 1:1, 1+1 Annex B, or 1+1 ignore K1 is chosen by the **addapsln**, it cannot be changed except by deleting the APS line (**delapsln**) and re-adding the APS line with the new configuration (**addapsln**).

Work Arounds

None.

Operational Problems

The following sections describe possible APS operational problems.

What the various APS switches mean

Description

There are ten reasons an APS switch may occur. These reasons can be seen logged 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.

Initial Investigation

The following list shows the possible conditions which may cause/prevent a switch. The list is arranged starting from highest precedence and ending with lowest precedence.

1. Lock out of Protection - An external user requested switch which prevents switching from working line to protection line from taking place.
2. Forced Switch - An external user requested switch which forces a switch from working line to protection line or vice-versa even if there is an alarm on the destination line.
3. Signal Fail - An automatically initiated switch due to a signal failure condition on the incoming OC-N line including loss of signal, loss of frame, AIS-L defects, and a line BER exceeding 10-3.
4. Signal Degrade - An automatically initiated switch due to a “soft failure” condition resulting from the line BER exceeding a pre-selected threshold (cnfapsln).
5. Manual Switch - An external user requested switch which requests a switch from working line to protection line or vice-versa but only if there is no alarm on the destination line.
6. Wait To Restore - A state request switch due to the a revertive switch back to the working line because the wait-to-restore timer has expired.
7. Exercise - Not supported
8. Reverse Request - A state request switch due to the other end of an APS bi-directional line performing an APS switch.
9. Do not Revert - A state request due to the external user request being cleared (such as a forced switch) while using non-revertive switching.
10. No Request - A state request due to the external user request being cleared (such as a forced switch) while using revertive switching.

Unable to perform APS external switch after forced or manual APS switch.

Description

The user performs a forced switch from the working line to the protection line (**switchapsln** Ln1 Ln2 3) and then another forced switch back to working line (**switchapsln** Ln1 Ln2 4). After this the user again tries to perform a forced switch to the protection line but sees nothing happen.

Investigation

Once a forced switch is made from the working line to the protection line and back again, a clear switch (**switchapsln** Ln1 Ln2 1) must be issued in order to perform another forced switch. This applies to APS manual and lockout switching also.

With APS 1+1, when repetitive **switchapsln** commands are issued, up to two in a row can be executed sequentially, when alternating between options 3 and 4 (forced switch), or 5 and 6 (manual switch), but no more. Attempts to execute a third **switchapsnln** will not succeed, and the following error message is displayed:

```
“Cannot request manual W->P when manual P->W switch in progress”
```

If users desire to perform repetitive switchapls commands, they need to issue a clear switch between each W-P, P-W pair of commands, for example:

```
switchapsln 2.1  1
```

APS manual switch to a line does not occur right away.

Description

The user has issued a manual switch either to working or protection line. The switch did not occur because the destination line was in alarm. When the alarm is cleared on that line the switch does occur.

Explanation

The BXM firmware remembers the ”last user switch request” (also called external request) and tries to switch to that line when it becomes available.

Switch occurs after lockout issued.

Description

With protection line active, the user issues an APS switch lockout and a switch occurs back to the working line.

Investigation

This is normal operation. When the protection line is active and an APS switch lockout is issued, a switch to the working line will happen. The lockout function locks the working line as active. Only an external (user request) APS clear switch (**switchapsln** Ln1 Ln2 1) will disable the lockout.

APS switch made to a line in alarm.

Description.

The user performs a forced switch to a line with a line alarm. The switch is successful making an alarmed line active with possible loss of traffic.

Investigation

It is normal operation for a forced switch to cause a switch to a line even though it may be faulty. This allows the user to “force” a switch to standby line even if it is in alarm. A traffic outage may occur. During a manual switch request, the BXM firmware decides whether the switch should occur and the switch may not occur if there is an alarm on the standby line. An APS clear switch will allow automatic switching to resume following a forced switch.

Reverse switch

Description

User performs a forced or manual switch on local end of APS line in bidirectional mode but other end indicates a reverse switch was performed.

Investigation

This is normal operation. A reverse switch in bidirectional mode occurs on the far end of the APS line when the local end of the APS line performs a switch for any reason.

APS switch occurs at the same time as a yred switch.

Description

Two related scenarios could cause this to occur.

1. A forced or manual switch is in effect. In **dspapsln**, the Last User Switch Request is forced or manual w->p or p->w. If a **switchcdred**/**switchyred** is performed (could be caused by card failure or physically removing card also) the front card switches and an APS switch occurs.
2. A clear switch is in effect. In **dspapsln**, the Last User Switch Request is clear. If a **switchyred** is performed (could be caused by card failure or physically removing card also) the front card switches and an APS switch occurs.

Explanation

Following a **switchcdred/switchyred**, or active card reset the BXM card will be instructed to perform an APS switch to align itself with the Last User Switch Request (**switchapsln**).When a yred (switchcdred) switch takes place on a BXM card pair being used for APS 1+1, the card being switched is sent configuration messages including the last user switch request. The BXM card will initially become active in an APS “clear” switch mode following a **switchcdred** or reset. This means that the APS switching is on automatic. However if the Last User Switch Request is a manual or forced switch, the software sends this request to the BXM, and the BXM will switch to this line if it is not already active. This switch is done to comply with the users last APS switch request.

In the second case, if the last user request is “clear”, full automatic APS switching is in effect with the working line being active by default. When there is no last user switch request (**switchapsln** to protection, for example) to switch to any particular line, the working line will become active.

APS switch occurs after issuing an APS clear switch.

Description

User issues an APS clear switch (**switchapsln** Ln1 Ln2 1) command while protection line is active and a switch occurs to the working line.

Explanation

This is normal operation. An APS clear switch request causes the APS switching mechanism in the BXM to initialize. This will cause a switch back to the working line if the working line is in better shape than the protection line. If the protection line is not faulty, no switch will occur.

APS Switch Occurs even though APS Forced switch in effect.

Description

A forced switch to protection line is performed. LOS on protection line causes a switch back to working line even though a forced switch is in progress

Explanation

Signal Fail on Protection line has higher priority than Forced switch. Whenever the protection line is in failure, there will be a switch to working line, even if the working line is failed or there is a forced W->P in effect.

APS line is failing to switch

Description

The user issues an APS forced or manual switch request but no switch occurs

Investigation

This could be due to a forced, manual, or lockout switch being in progress and a clear switch is required (switchapsln Ln1 Ln2 1). Need to issue an APS clear switch (**switchapsln**) to exit forced, manual, or lockout switch state.

If running the ITUT APS standard protocol which does not report an Architecture Mismatch APS alarm the problem could be that one end of the line is bi-directional and the other is uni-directional.

Check that configuration is the same on both ends, specifically uni/bidirectional mode, 1:1/1+1 configuration.

A manual switch will not occur if the standby line is in alarm.

Large cell loss when performing a front card switchover

Description

A line which is configured for APS 1+1 line redundancy has its active front card switched either due to card failure, **switchyred** (**switchcdred**), or resetting the card. A loss of cells is observed.

Investigation

Cell loss at card switchover is not due to faulty APS. It is a a result of the card redundant switch (YRED switch) and there will be up to 250ms worth of traffic disruption during BXM front card switchovers.

APS service switch description

Description

What is an APS service switch? Does it work on APS 1:1 configurations?

Investigation

An APS service switch is only applicable to APS 1+1 configuration. It allows the user to switch all the APS lines on a card with a single **switchapsln** command with an “s” option at the end of the command. All APS lines on this card pair will be switched and made active on a single backcard allowing the other backcard to be removed for service. **IMPORTANT**: Be sure that the associated front card is active for the backcard which is to remain in the rack. You may have to perform a **switchcdred** so that the backcard that the service switch switches to has its associated front card active. A service switch is not required in order to remove a BXM front card with APS 1+1 lines on it. The card redundancy will handle the switch to the other card without affecting the lines.

APS line does not seem to switch and active line is in alarm

Description of problem

A major line alarm is indicated on the active line yet it remains active due to no APS switch to the redundant line.

Initial Investigation

1. Verify that the configuration is correct (**dspapsln**, **cnfapsln**). See above configuration problems.
2. Use **dspapsln** to check the APS line’s status. The **dspapsln** display shows the active and standby line’s alarm status. It also shows if there are any APS alarms. If the active line alarm status shows OK but the standby line alarm status shows an alarm then a switch will not occur due to the standby line alarm. Troubleshoot the standby line problem. If the standby line alarm status shows OK but the active line alarm status shows an alarm then a switch should have occurred and there is a more obscure problem. If there is an APS alarm shown under Current APS alarms then this

could be the problem, see above section on APS Alarms. If APS 1+1 is configured, use **dspcds** to check the status of the protection line’s card. If there is a problem with this card a switch may not occur.

3 Verify the sequence of events by using **dsplog** and tracing the entries which contain information about this line or APS on this line. If a switch was attempted and succeeded due to a Loss of Signal, the message “APS SignalFail switch from LN 1 to LN 2” should be logged. If the switch failed there will be a message such as “Cannot do APS SigFail switch from LN 1 to LN 2”.

Work Around

Perform a clear switch on each end of the APS line (**switchapsln 2.1 1**). This may get both ends in sync and clear up the problem.

A forced switch from working to protection may be performed (example: **switchapsln 2.1 3**). **WARNING:** If the protection line is in LOS and we force a switch to it, traffic will be lost.

If the line is an APS 1+1 line, then the front cards are redundant and the user may try a **switchcdred** (**switchyred**) to induce APS switching. This should normally have no affect on APS switching. APS switching and card redundancy switching are independent.

The BXM card may be reset in combination with an APS clear switch either before of after the reset at both ends of the APS line. Perform an APS clear switch on both on both ends of the line. Reset the BXM cards (**resetcd h**).

BXM backcard 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 backcard LED is meant to show whether the card is currently being used by at this time. Green means that this card is in use. Yellow means that the card is not in use and could be removed for service. If the standby line’s card’s LED is green it means that part of this card is being used at this time. This could happen due to the APS 1+1 cross over circuit where the working line’s front card is active but the protection line itself is active. The working line’s backcard is being used to shunt traffic to the protection line’s backcard.

BXM Port LED states

Scenario

For an APS 1+1 or APS 1:1 line pair, the port LEDS are the same color on working and protection line.

Explanation

To switch software, the APS line pair is a single logical line. Although required to send BXM messages to both lines, these messages will be the same message. Thus switch software cannot send different LED states to the BXM for the same APS line. The BXM firmware makes the protection line LED state the same as the working line LED state.

Alarms

What do APS Alarms Represent.

The following sections describe APS alarm types

Description

An APS alarm occurs in **dspalms** and **dspapsln**.

Initial Investigation

APS alarms can be of two types. There are APS specific alarms and there are line alarms reported by the standby line. The standby line alarm will be displayed in the dspapsln screen under “Standby Line Alarm Status”. If there are no other APS specific alarms, the standby line alarms will also show under “Current APS Alarm Status”. The meaning of the standby line alarms are the same as the meaning of the active line alarms which are reported in the 0x55 Line Alarms command and are discussed in other documentation. The APS specific alarms consist of seven alarms in addition to APS OK, and APS Deactivated, and Line Looped.

Some of the APS alarms reflect problems with the underlying APS channel protocol, the K1/K2 bytes. The K1 byte carries the request for a switch action on a specific channel to the remote end of the line. The K2 byte indicates the status of the bridge in the APS switch and also carries mode information.

- **Remote Signl FAIL** - A remote signal failure indicates that there is a problem with the far end signalling information in the K1K2 bytes. There is a problem with the protection line’s physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback etc.).
- **Channel Mismatch** - Can only happen in bidirectional mode and indicates that there is a problem with the underlying APS channel protocol. The receive K2 channel number does not equal the transmit K1 channel number. There is a problem with the protection line’s physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback etc.).
- **Prot Sw Byt FAIL** - Protection Switch Byte failure or PSB. In bidirectional mode indicates that there is an invalid K1 byte. The receive K1 request does not match the reverse request and is less than the transmit K1 request. In all modes a PSB alarm indicates that K1/K2 protocol is not stable. There is a problem with the protection line’s physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback etc.). This alarm will be seen if the local end of an APS working line or trunk is connected directly to the remote end’s protection line or trunk.
- **APS Card Missing** - This alarm is seen in APS 1+1 configurations when BXM firmware determines that any BXM front or back card is missing. Check **dspcds** or look in the **dsplog** to see which card associated with the APS line is missing.

- **FarEnd Prot FAIL** - Far end protection failure indicates that the far end's protection line is failing. When there is Signal Failure on the protection channel, the remote end sees Far End Protection Fail. There is a problem with the protection line's physical layer. So, one has to disable APS and try to bring up the protection line as a normal line and diagnose the physical layer (by putting loopback, etc).If the other end shows the "Architect Mismtch" APS alarm then the APS standards could be different at each end. Use cnfcdaps or cnfapsln to check for this.
- **Architect Mismtch** -Architecture mismatch indicates that one end of the APS line is configured for APS 1+1 and the other end is configured for APS 1:1 which will not work. If the line is configured for GR-253 standard operation an architecture mismatch can also mean that one end is bi-directional and the other end is uni-directional (ITUT will not report this). Verify that the APS architecture is configured the same on either end of the APS lines using the **cnfapsln** command. This alarm will also be seen if the local end of an APS working line or trunk is connected directly to the remote end's protection line or trunk. In this case one end of the line usually will have a "Prot Sw Byt FAIL" alarm present. If the other end shows the "FarEnd Prot FAIL" APS alarm then the APS standards could be different at each end. Use cnfcdaps or cnfapsln to check for this.
- **Standard Mismatch** - indicates that on the local end of an APS 1+1 configuration that one card is running the ITUT standard and the redundant card is running the GR-253 standard. Use the **cnfcdaps** command to check and change the standard.
- Usr Line Loop - The line is looped. Use the dellnlp command to clear the loop. Both working and protection lines are looped when an APS line is looped.
- **APS Standby Line Alarms** are also shown as APS alarms unless there is a higher priority APS alarm (those above) masking the standby line alarm. The APS standby alarms are the integrated line alarms reported by the standby line in the BXM Line Alarms message (0x55). If one of these alarms is shown, there is a problem with the standby line. Trouble shoot 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)
  - —
  - —

Configuration, BME Multicasting

This chapter contains an overview of multicasting, a description of the BME card used on the BPX switch for multicasting for PVCs, and configuration information.

This chapter contains the following:

- Introduction
- Standards
- Multicasting Benefits
- Multicasting Overview
- Connection Management Criteria
- Connection Management with Cisco WAN Manager
- BME Operation
- Alarms
- Hot Standby Backup
- Configuration
- Connection Diagnostics
- List of Terms
- Related Documents
- Configuration Management

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 users 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, e.g., IP multicast video networks to the desktop
- Remote learning
- Medical imaging

Standards

- UNI 3.1 Multicast Server
- UNI 4.0 Leaf Initiated Joins and related standards

Multicasting Benefits

Multicasting point-to-multipoint connections benefits include:

- Decreased delay in receiving data
- Near simultaneous reception of data by all leaves

Multicasting Overview

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 and BXMs only
  - BCC-3 control cards and legacy cards only, including BNIs and ASIs
- 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 etc. 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, etc.

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 the following 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

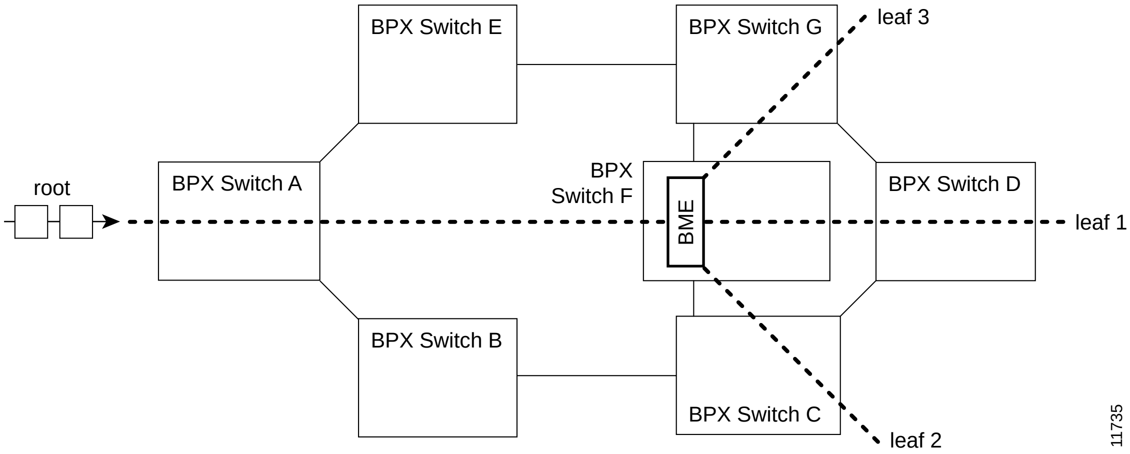
Cables are connected between port 1 and port 2 of the backcard, transmit to receive and receive to transmit.

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 18-1 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.

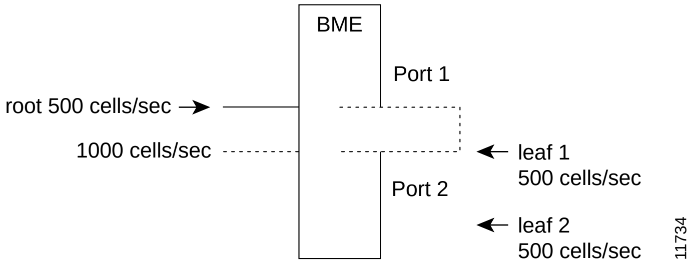
Figure 18-1 Replication of a Root Connection into Three Leaves



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/sec, then one should see an egress port stat of 1000 cell/sec on port 1 and an ingress port stat of 1000 cells/sec on port 2, as shown in Figure 18-2.

Figure 18-2 Example of Traffic, One Root and Two Leaves

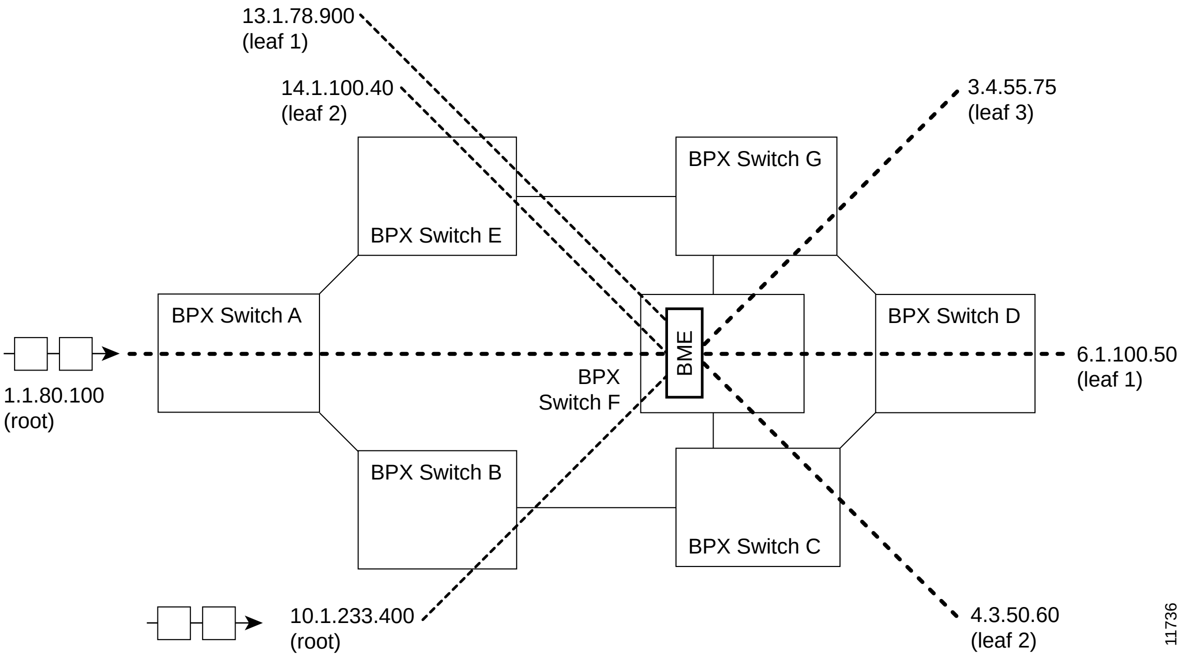


Adding Connections

Two multicasting groups are shown in Figure 18-3. 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. Also, in this example, the two connections with a VCI of 0 each define a multicasting root connection. Their VPI defines a broadcasting group. For example, 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 * * *

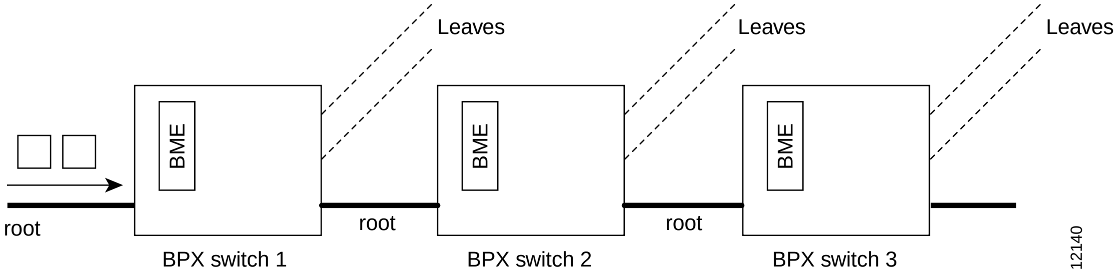
Figure 18-3 Adding Multicasting Connections



Multi-Segment Multicast Connections

Figure 18-4 shows an example of a multi-segment multicast connection where a leaf connection from one BME can become a root connection for another BME. This capability allows the users to configure multi-segment multicast tree topologies.

Figure 18-4 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 18-5, execute the following commands to display channel statistics for the leaf connections:

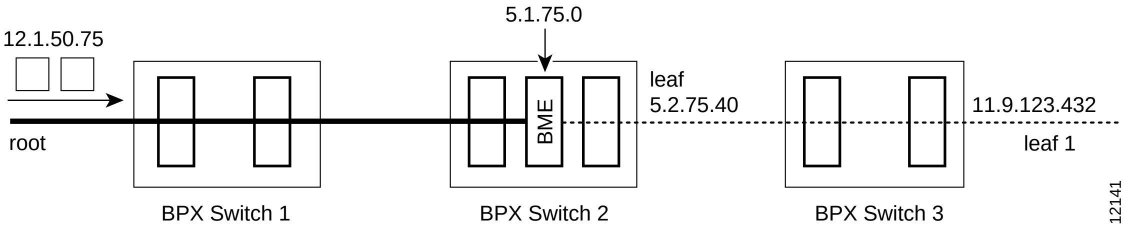
- **dspchstats** 12.1.50.75 on BPX switch 1 (available)
- **dspchstats** 5.2.75.40 on BPX switch 2 (available)

- **dspchstats** 11.9.123.432 on BPX switch 3 (available)

For the example in Figure 18-5, 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 18-5 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.

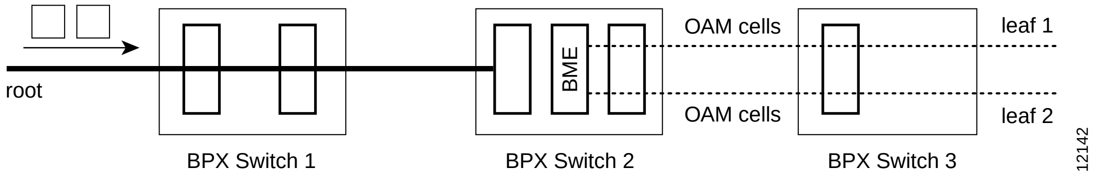
No policing functionality is available on the root connection on the BME end.

Alarms

OAM cells

OAM cells coming into the root are multicast into the leaves along with data, as shown in Figure 18-6.

Figure 18-6 OAM Cells

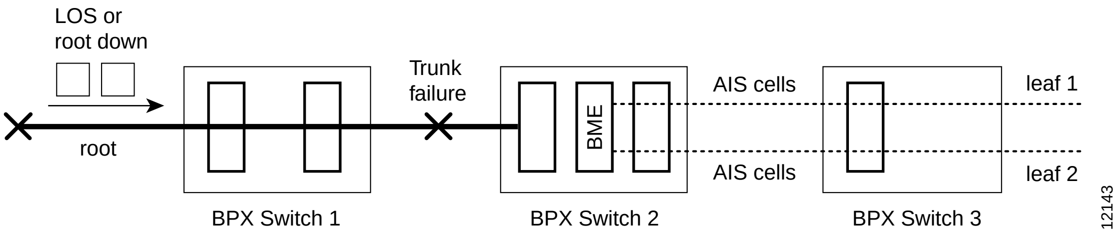


AIS cells

AIS cells are automatically generated on the leaves, as shown in Figure 18-7, 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 18-7 Alarms



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.

The **addyred** command is used to enable hot standby backup between the cards. *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    9.2      Nov. 24 1998 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
```

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.

List of Terms

BME

The card used in the BPX switch to provide multicasting.

Related Documents

- *Cisco WAN Switching Command Reference*

Configuration Management

The BPX switch must be initially installed, configured, and connected to a network.

Following this, multi-casting connections can be added to the BPX switch.

PART 5

Configuration, MPLS

CHAPTER 19

Configuration General, MPLS on BPX Switch

This chapter contains an overview of label switching (MPLS based) and information for configuring the BPX 8650 for the label switching feature.

For a configuration example of MPLS without CoS refer to *Chapter 20, Configuring the BPX Switch, 7200, and 7500 Routers for MPLS*. For configuration of MPLS with CoS, refer to *Chapter 21, MPLS CoS with BPX 8650, Configuration*. For configuration information with respect to MPLS VPNs, refer to *Chapter 22, MPLS VPNS with BPX 8650, Configuration.*

Refer to Release Notes for supported features.

This chapter contains the following:

- Introduction
- MPLS/Tag Terminology
- Label Switching Benefits
- Label Switching Overview
- Elements in a Label Switching Network
- Label Switching Operation at Layer 3
- Label Switching in an ATM WAN
- Label Switching and the BPX 8650
- Label Switching Resource Configuration Parameters
- Requirements
- List of Terms
- Related Documents
- Configuration Management
- Configuration Criteria
- Configuration Example
- Checking and Troubleshooting
- Provisioning and Managing Connections
- Statistics
- Command Reference

Introduction

Label 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. Label switching in the network core can be performed by switches, such as ATM switches, or by existing routers.

MPLS/Tag Terminology

The following lists the change of terminology to reflect the change from “label” to “mpls” terms.

Old Designation	New Designation
Tag Switching	MPLS, Multiprotocol Label Switching
Tag (short for Tag Switching)	MPLS
Tag (item or packet)	Label
TDP (Tag Distribution Protocol)	LDP (Label Distribution Protocol) **Note** Cisco TDP and LDP (MPLS Label Distribution Protocol) are nearly identical in function, but use incompatible message formats and some different procedures. Cisco will be changing from TDP to a fully compliant LDP.
Tag Switched	Label Switched
TFIB (Tag Forwarding Information Base)	LFIB (Label Forwarding Information Base)
TSR (Tag Switching Router)	LSR (Label Switching Router)
TSC (Tag Switch Controller)	LSC (Label Switch Controller
ATM-TSR	ATM-LSR (ATM Label Switch Router, such as, BPX 8650)
TVC (Tag VC, Tag Virtual Circuit)	LVC (Label VC, Label Virtual Circuit)
TSP (Tag Switch Protocol)	LSP (Label Switch Protocol)
TCR (Tag Core Router)	LSR (Label Switching Router)
XTag ATM (extended Tag ATM port)	XmplsATM (extended mpls ATM port)

Label Switching Benefits

For multi-service networks, label switching enables the BPX switch to provide 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 multi-service providers.

For internet service providers (ISPs) using ATM switches at the core of their networks, label switching enables the Cisco BPX 8600 series, the 8540 Multiservice Switch Router, and other Cisco ATM switches to provide a more scalable and manageable networking solution than just overlaying IP over an ATM network. Label switching avoids the scalability problem of too many router peers and provides support for a hierarchical structure within an ISPs network, improving scalability and manageability. Furthermore, label switching provides a platform for advanced IP services such as Virtual Private Networks and IP Class of Service (CoS) on ATM switches.

By integrating the switching and routing functions, label switching combines the reachability information provided by the router function with the traffic engineering optimizing capabilities of the switches.

When integrated with ATM switches, label switching takes advantage of switch hardware that is optimized to take advantage of the fixed length of ATM cells, and to switch these cells at wire speeds.

Label Switching Overview

Label switching is a high-performance, packet (frame) forwarding technology. It integrates the performance and traffic management capabilities of data link layer 2 with the scalability and flexibility of network layer 3 routing.

Label switching enables switch networks to perform IP forwarding. 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.

With label switching 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.

In conventional layer 3 forwarding, 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.

In the most common case, the only relevant field in the header is the destination field. However, as other fields could be relevant, a complex header analysis must be done at each router through which the packet travels.

In label switching the complete analysis of the layer 3 header is performed just once, at the edge label switch router (LSR) at each edge of the network. It is here that the layer 3 header is mapped into a fixed length label, called a label.

At each router across the network, only the label needs to 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.

Elements in a Label Switching Network

The basic elements in a label switching network are edge LSRs, label switches, and a label distribution protocol as defined in the following:

- Edge label routers

  Edge label switch routers are located at the boundaries of a network, performing value-added network layer services and applying labels to packets. These devices can be either routers, such as the Cisco 7500, or multilayer LAN switches, such as the Cisco Catalyst 5000.

- Label switches

  These devices switch labeled packets or cells based on the labels. Label switches may also support full Layer 3 routing or Layer 2 switching in addition to label switching. Examples of label switches include the Cisco 6400, the 8540 Multiservice Switch Router, Cisco BPX 8650, and Cisco 7500 from Cisco.

- Label distribution protocol

  The label distribution protocol (LDP) is used in conjunction with standard network layer routing protocols to distribute label information between devices in a label switched network.

Label Switching Operation at Layer 3

Label switching operation comprises two major components:

- Forwarding
- Control

Forwarding

The forwarding component is based on label swapping. When a label switch (or router in a packet context) receives a packet with a label, the label is used as an index in a Label Forwarding Information Base (LFIB). Each entry in the LFIB consists of an incoming label and one or more sub-entries of the form:

```
<outgoing label, outgoing interface, outgoing link level information>
```

For each sub-entry, the label switch replaces the incoming label with the outgoing label and sends the packet on its way over the outgoing interface with the corresponding link level information.

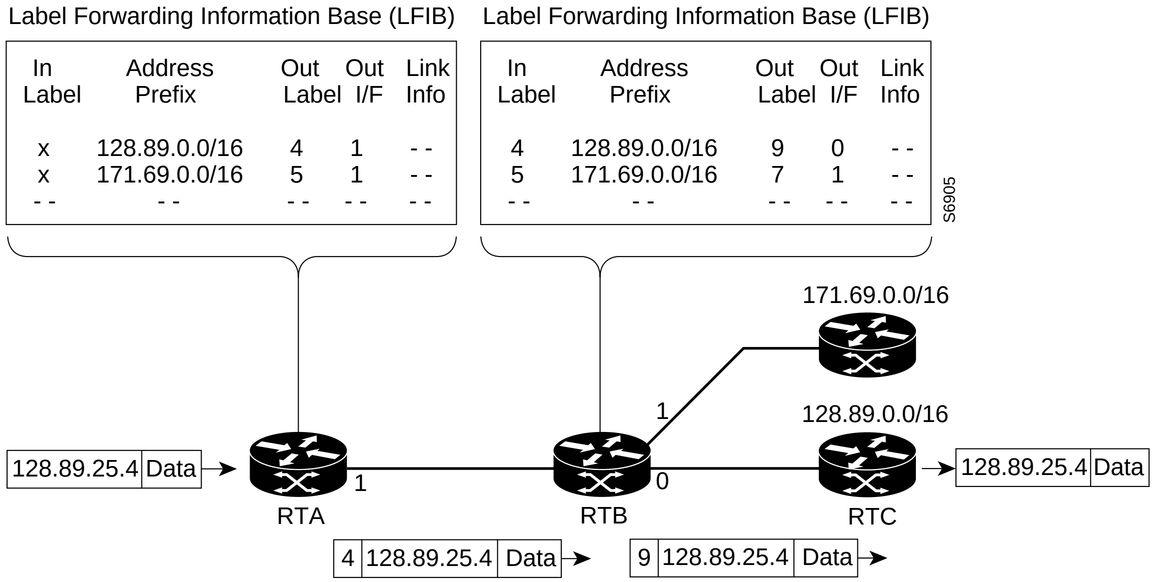
Figure 19-1 shows an example of label switching. It shows an unlabeled IP packet with destination 128.89.25.4 arriving at Router A (RTA). RTA checks its LFIB and matches the destination with prefix 128.89.0.0/16. (The /16 denotes 16 network masking bits per the Classless Interdomain Routing (CIDR) standard.) The packet is labeled with an outgoing label of 4 and sent toward its next hop RTB. RTB receives the packet with an incoming label of 4 that it uses as an index to the LFIB. The incoming label of 4 is swapped with outgoing label 9, and the packet is sent out over interface 0 with the appropriate layer 2 information (such as, MAC address) according to the LFIB. RTB did not have to do any prefix IP lookup based on the destination as was done by RTA. Instead, RTB used the label information to do the label forwarding. When the packet arrives at RTC, it removes the label from the packet and forwards it as an unlabeled IP packet.

Control

The control component consists of label allocation and maintenance procedures. The control component is responsible for creating label bindings between a label and IP routes, and then distributing these label bindings to the label switches.

The label distribution protocol (LDP) is a major part of the control component. LDP establishes peer sessions between label switches and exchanges the labels needed by the forwarding function.

Figure 19-1 Label Forwarding Information Base (LFIB) in an IP Packet Environment



Label Forwarding Information Base (LFIB)

In Label	Address Prefix	Out Label	Out I/F	Link Info
x	128.89.0.0/16	4	1	- -
x	171.69.0.0/16	5	1	- -
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

In Label	Address Prefix	Out Label	Out I/F	Link Info
4	128.89.0.0/16	9	0	- -
5	171.69.0.0/16	7	1	- -
- -	- -	- -	- -	- -

Label Switching in an ATM WAN

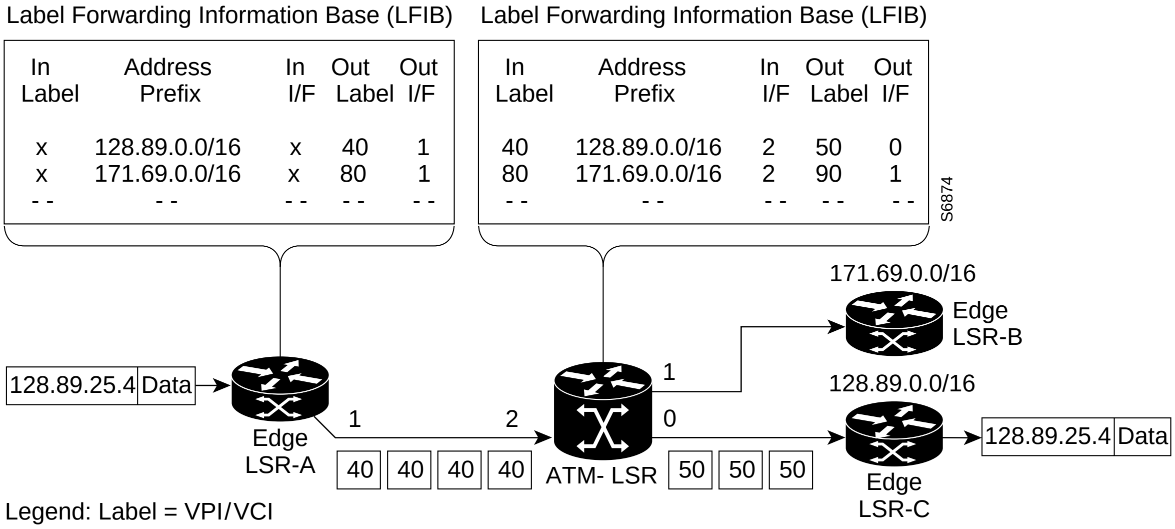
With label switching over an ATM network, the forwarding and control components can be described as follows:

- Forwarding: In an ATM environment, the label switching forwarding function is carried out identically to normal switching. The label information needed for label switching can be carried in the VCI field within one or a small number of VPs. The labels are actually the VCIs.
- Control: For the control component over ATM networks, a label distribution protocol is used to bind VCIs to IP routes. The switch also has to participate in IP routing protocols such as OSPF, BGP, and RSVP.

Forwarding

Figure 19-2 shows the forwarding operation of an ATM switch in which the labels are designated VCIs. In Figure 19-2, an unlabeled IP packet with destination 128.89.25.4 arrives at router A (RTA). RTA checks its LFIB and matches the destination with prefix 128.89.0.0/16. RTA converts the AAL5 frame to cells, and sends the frame out as a sequence of cells on VCI 40. RTB, which is an ATM Label Switch Router (LSR) controlled by a routing engine, performs a normal switching operation by switching incoming cells on interface 2/VCI 40 to interface 0/VCI 50.

Figure 19-2 Label Forwarding Information Base (LFIB) in an ATM Environment



Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
x	128.89.0.0/16	x	40	1
x	171.69.0.0/16	x	80	1
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
40	128.89.0.0/16	2	50	0
80	171.69.0.0/16	2	90	1
- -	- -	- -	- -	- -

Control

ATM-LSRs use the downstream-on-demand allocating mechanism. Each ATM-LSR maintains a forwarding information base (FIB) that contains a list of all IP routes that the ATM-LSR uses. This function is handled by the routing engine function which is either embedded in the switch or runs on an outside controller. For each route in its forwarding information base, the edge ATM LSR identifies the next hop for a route. It then issues a request via LDP to the next hop for a label binding for that route.

When the next hop ATM-LSR receives the route, it allocates a label, creates an entry in its LFIB with the incoming label changed to the allocated outgoing label. The next action depends on whether the label allocation is in an optimistic mode or a conservative mode. In optimistic mode, it will immediately return the binding between the incoming label and the route to the LSR that sent the request. However, this may mean that it is not immediately able to forward labeled packets which arrive, as the ATM-LSR may not yet have an outgoing label/VCI for the route. In conservative mode, it does not immediately return the binding, but waits until it has an outgoing label.

In optimistic mode, the LSR that initiated the request receives the binding information, it creates an entry in its LFIB, and sets the outgoing label in the entry to the value received from the next hop. The next hop ATM LSR then repeats the process, sending a binding request to its next hop, and the process continues until all label bindings along the path are allocated.

In conservative mode, the next hop LSR sends a new binding request to its next hop, and the process repeats until the destination ATM edge LSR is reached. It then returns a label binding to the previous ATM-LSR, causing it to return a label binding, and so on until all the label bindings along the path are established.

Figure 19-3 shows an example of conservative allocation. ATM edge LSR RTA is an IP routing peer to ATM-LSR RTB. In turn, ATM-LSR RTB is an IP routing peer to ATM-LSR-RTC. IP routing updates are exchanged over VPI/VCI 0/32 between RTA-RTB and RTB-RTC. For example:

1 RTA sends a label binding request toward RTB in order to bind prefix 128.89.0.0/16 to a specific VCI.

2 RTB allocates VCI 40 and creates an entry in its LFIB with VCI 40 as the incoming label.

3 RTB then sends a bind request toward RTC.

4 RTC issues VCI 50 as a label.

5 RTC sends a reply to RTB with the binding between prefix 128.89.0.0/16 and the VSI 50 label.

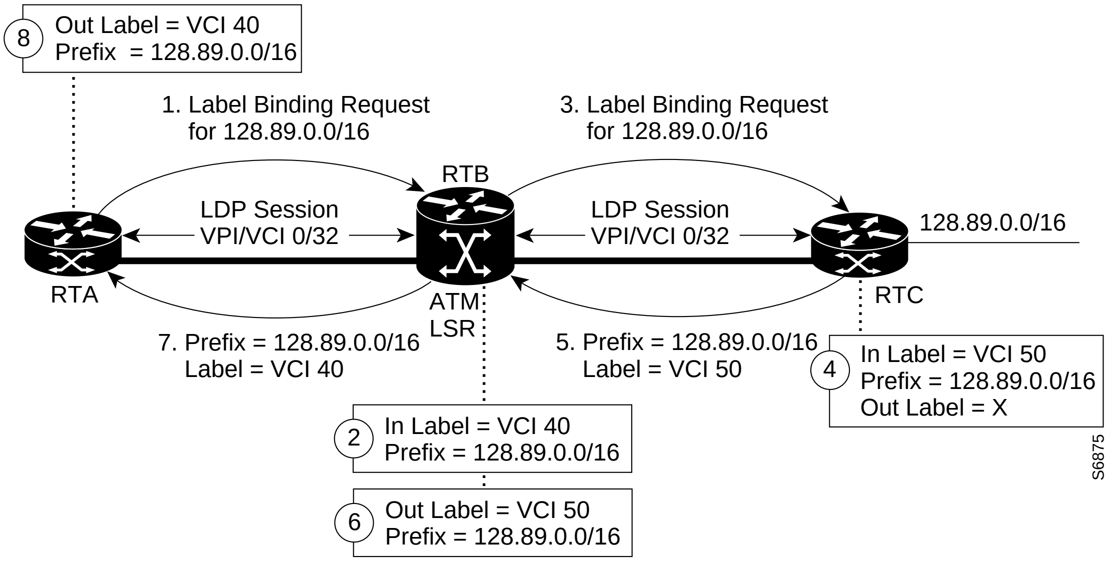
6 RTB sets the outgoing label to VCI 50.

7 RTB sends a reply to RTA with the binding between prefix 128.89.0.0/16 and the VCI 40 label.

8 RTA then creates an entry in its LFIB and sets the outgoing label to VCI 40.

Optimistic mode operation is similar to that shown in Figure 19-3, except that the events labeled 7 and 8 in the figure may occur concurrently with event 3.

Figure 19-3 Downstream on Demand Label Allocation, Conservative Mode Shown



Label Switching and the BPX 8650

With label switching, the router function can be accomplished by either integrating the routing engine into the switch or by using a separate routing controller (associated router). The BPX 8650 label switch combines a BPX switch with a separate router controller (Cisco Series 7200 or 7500 router). This has the advantage of separating the various services (such as, AutoRoute, SVCs and label switching) into separate logical spaces that do not interfere with one another.

Note The current version of Cisco MPLS software uses an early version of LDP called the Tag Distribution Protocol (TDP). TDP and LDP are virtually identical in function, but use incompatible message formats. Once the MPLS standard is complete, Cisco will provide standard LDP in its MPLS implementation.

Two scenarios are shown in Figure 19-3. In the first, IP packets are applied to the network via the edge routers (either part of the BPX 8650 Label Switches or independent 7500 Label Edge Routers). In the second, IP packets are routed via Frame Relay to an MGX 8220 which in turn sends ATM cells via a BPX 8620 to a BPX 8650 in the interior of the network.

Example 1: An IP packet is applied to the network via BPX 8650s on the edge of the network and then label switching is used to forward the packet across the network via BPX 8650s. In this example the shortest path is not used, but rather the label switch connection is routed across BPX 8650 ATM-LSR-A, BPX 8650 ATM-LSR-B, BPX 8650 ATM-LSR-C, BPX 8650 ATM-LSR-D, and 7500 LER-S. This particular routing path might, for example, have been selected with administrative weights set by the network operator. The designated labels for the cells transmitted across the network in this example are shown as 40, 60, 70, and 50, respectively.

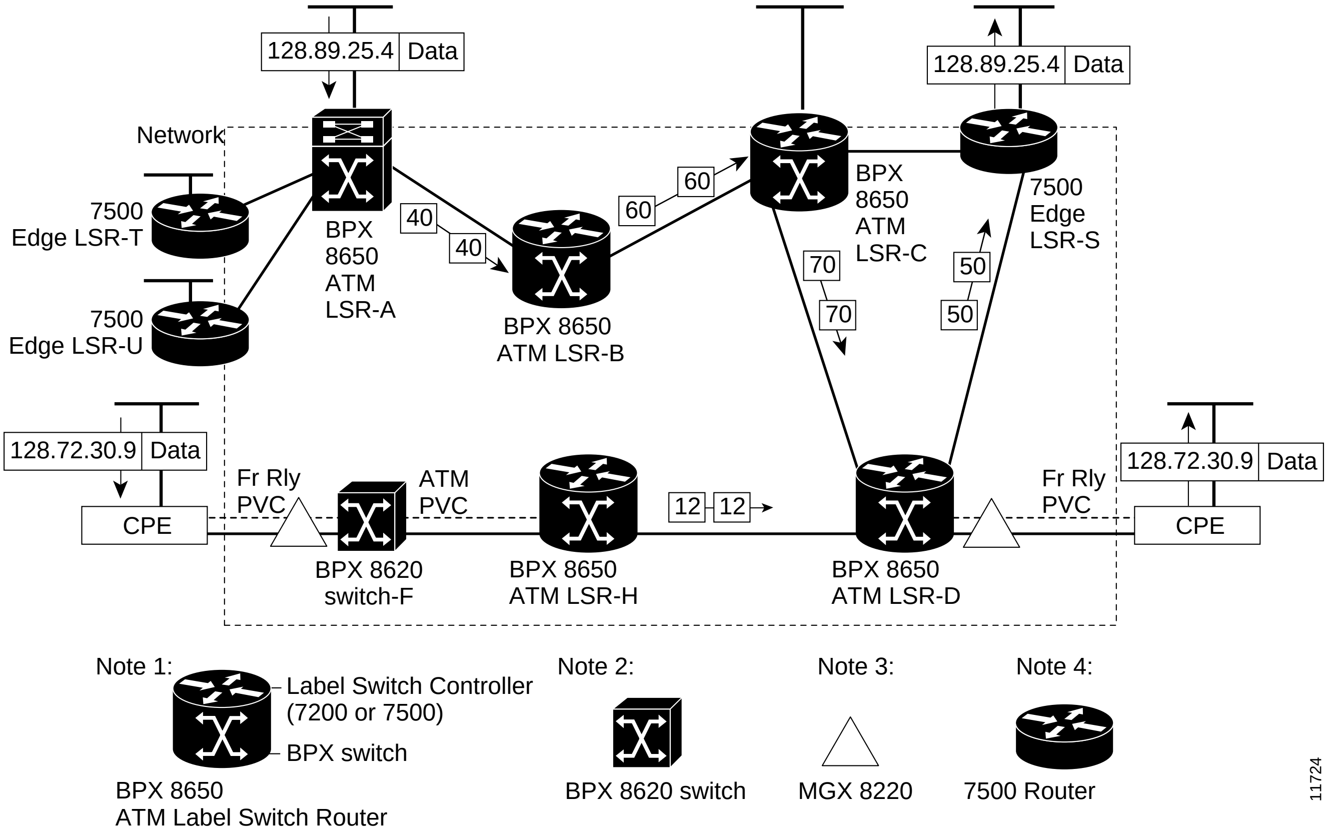
The router component of the label switches that are located at the boundaries of the network (BPX 8650 ATM-LSR-A, BPX 8650 ATM-LSR-C, BPX 8650 ATM-LSR-H), perform edge-routing network layer services including the application of labels to incoming packets. The edge label switch routers, 7500 edge LSR-S, 7500 edge LSR-T, and 7500 edge LSR-U, perform the same edge-routing network layer services in this example.

Example 2: An IP packet is routed to BPX 8650 ATM-LSR-H at the interior of the network via BPX 8620 switch-F. The Frame Relay to ATM interface for BPX 8620 switch-F might be an MGX 8220 as shown. BPX 8650 ATM-LSR-H then acts as an edge LSR as well as a label switch. When the ATM cells arrive at BPX 8650 ATM-LSR-H, they are routed to an ATM interface on the associated Label Switch Controller. (Note: This is a different physical line than the ATM control link between the BPX and the Label Switch Controller.) The Label Switch Controller applies the applicable label and routes the ATM cells back to the BPX on the same ATM interface. These labeled cells are then handled as a standard MPLS label input to the BPX and transmitted across the network with a label shown as 12 in this example. These label switching cells are then forwarded to BPX 8650 ATM-LSR-D where they are converted back to an IP packet and routed to the CPE at the edge of the network as a Frame Relay PVC via an MGX 8220.

Edge label router functionality is necessary to add and remove labels from IP packets, but not to switch labeled packets. Figure 19-4 shows 3 stand-alone edge LSRs (edge LSRs S, T, and U). These would typically be co-located with BPX 8650 Label Switches in Points of Presence. However the Label Switch Controller in a BPX 8650 can also act as an edge LSR if required.

In Figure 19-4, ATM Label Switch Routers A, C, D and H use this combined Label Switch/Label Edge Router functionality. Only ATM-LSR-B acts purely as a Label Switch. Note also that the edge label router performance of a BPX 8650 Label Switch is significantly lower than its Label Switching performance. Typically there will be several edge Label Routers (or combined LSR/edge LSRs) for each BPX 8650 ATM-LSR acting purely as a label switch.

Figure 19-4 BPX Label Switching

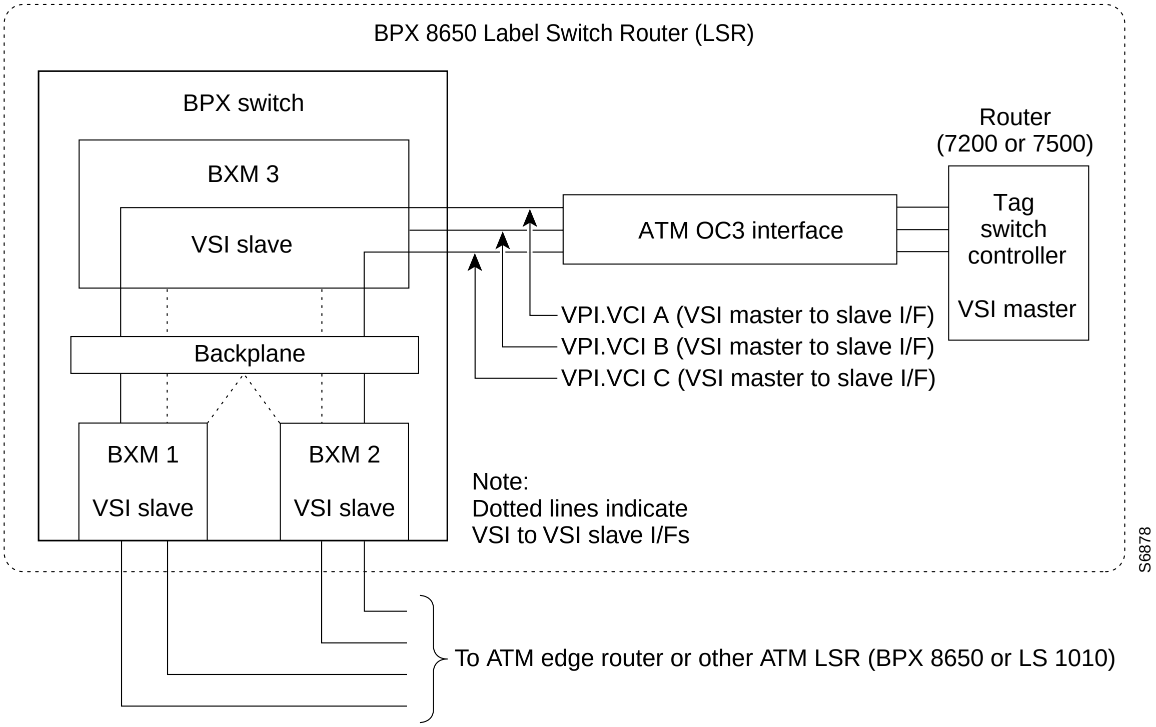


Virtual Switch Interfaces

Figure 19-5 shows how virtual switch interfaces are implemented by the BPX switch in order to facilitate label switching. A virtual switch interface (VSI) provides a standard interface so that a resource in the BPX switch can be controlled by additional controllers other than the BPX controller card such as a label switch controller.

The label switch controller is connected to the BPX switch using ATM T3/E3/OC-3 interfaces on the LSC device (an Cisco 6400 or a 7200 or 7500 series router) and on a BXM card. The ATM OC-3 interface on the 7200 router is provided by an ATM port adapter, on the 7500 router by an AIP or a VIP with ATM Port Adapter, and for the BXM front card by an ATM OC-3 4-port or 8-port back card.

Figure 19-5 BPX Switch VSI Interfaces


BPX 8650 Label Switch Router (LSR)
BPX switch
BXM 3
VSI slave
Backplane
BXM 1
VSI slave
BXM 2
VSI slave
Router
(7200 or 7500)
ATM OC3 interface
Tag
switch
controller
VSI master
VPI.VCI A (VSI master to slave I/F)
VPI.VCI B (VSI master to slave I/F)
VPI.VCI C (VSI master to slave I/F)
Note:
Dotted lines indicate
VSI to VSI slave I/Fs
S6878
To ATM edge router or other ATM LSR (BPX 8650 or LS 1010)

A distributed slave model is used for implementing VSI in a BPX switch. Each BXM in a BPX switch is a VSI slave and communicates with the controller and other slaves, if needed, when processing VSI commands. The VSI master sends a VSI message to one slave. Depending on the command, the slave either handles the command entirely by itself, or communicates with a remote slave to complete the command. For example, a command to obtain configuration information would be processed by one slave only. A command for connection setup would cause the local slave to communicate with the remote slave in order to coordinate with both endpoints of the connection.

Figure 19-6 shows a simplified example of a connection setup with endpoints on the same slave (BXM VSI), and an example of a connection setup with endpoints on different slaves (BXM VSIs) is shown in Figure 19-7.

Figure 19-6 Connection Setup, End Points on same VSI Slave

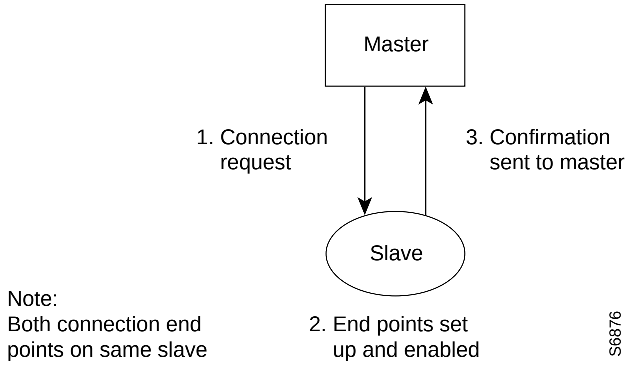
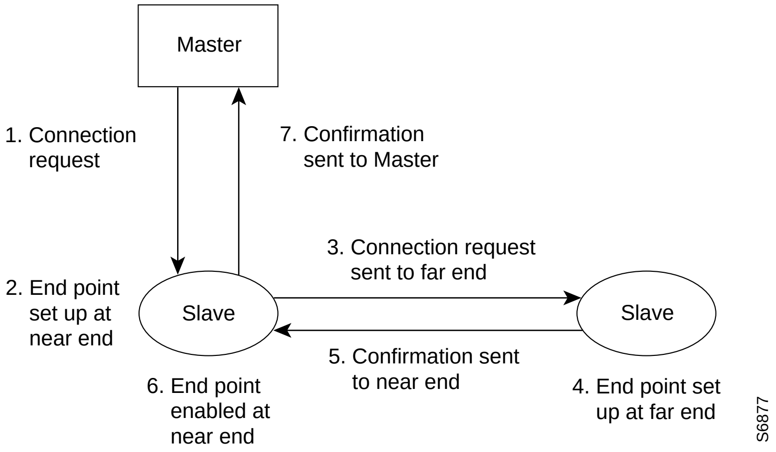

Master
1. Connection request
3. Confirmation sent to master
Slave
Note:
Both connection end points on same slave
2. End points set up and enabled
S6876

Figure 19-7 Connection Setup, End Points on Different VSI Slaves


Master
1. Connection request
7. Confirmation sent to Master
3. Connection request sent to far end
2. End point set up at near end
Slave
Slave
5. Confirmation sent to near end
6. End point enabled at near end
4. End point set up at far end
S6877

Label Switching Resource Configuration Parameters

This section describes resource partitioning for label switching. It includes the following:

- Summary
- Configuring VSI LCNS
- Useful Default Allocations
- Details of More Rigorous Allocations

Summary

Most label switching configuration, including the provisioning of connections, is performed directly by the Label Switch Controller. This is discussed separately; refer to the *Label Switching for the Cisco 7500/7200 Series Routers* documentation. Configuration for label switching on the BPX 8650 itself, consists of basic VSI configuration, including resource partitioning.

The following items need to be configured or checked on the BPX 8650:

- Partitioning

  On each interface (port or trunk) on the BXM cards used for label switching, two sets of resources must be divided up between traditional PVC connections and label switching connections. The traditional PVC connections are configured directly on the BPX platform, and label switching connections are set up by the LSC using the VSI. The following resources are partitioned on each interface:

  — Bandwidth

  — Connections

  As with all ATM switches, the BPX switch supports up to a specified number of connections. On the BPX switch, the number of connections supported depends on the number of port/trunk cards installed. On each interface, space for connections is divided up between traditional BPX switch permanent virtual circuit (PVC) connections, and Label Switching VCs (LVCs). The details of connection partitioning using the **cnfrsrc** command are discussed later in this section.

- Queues for Label Switching traffic

  These should be automatically configured correctly, but it is possible to change the configuration manually. Consequently, the configuration of the queues should be checked as part of the process of enabling label switching. Configuration of these parameters using the **cnfqbin** command is discussed later in this chapter. (Refer also to the VSI chapter.)

- VSI Control Interface

  A trunk must be enabled as VSI control interface, to allow a LSC to be connected. This is done using the **addshelf** command and selecting the VSI option.

Configuring VSI LCNS

In the first release of label switching, each BXM card supports 16k connections in total, including PVCs, label switching VSI connections, and connections used for internal signaling.

Note The number of connections that the BXM can support is referred to as connection spaces, or logical connection numbers (LCNs).

On the BXM, the ports are grouped into port groups, and a certain number of connections is available to each port group. For example, an 8-port-OC-3 BXM has two port groups, consisting of ports 1-4 and 5-8, respectively.

Note Newer BXMs support 32k connections in total.

Each port group for the various versions of the BXM cards has a separate connection pool as specified in Table 19-1.

Table 19-1 BXM Port Groups

BXM Card Type	Number of Port Groups	Port Group Size	LCN Limit per Port Group	Average Connections per Port
8–T3/E3	1	8 ports	16k	2048
12–T3/E3	1	12 ports	16k	1365
4–OC-3	2	2 ports	8k	4096
8–OC-3	2	4 ports	8k	2048
1–OC-12	1	1 port	16k	16384
2–OC-12	2	1 port	8k	8192

For label switching, connections are allocated to VSI partitions. On the BPX 8650, for Release 9.2, only one VSI partition is used. In Release 9.2.3, up to two VSI partitions may be used to support controllers other than the Label Switch Controller (such as, Cisco 6400 or 7200 and 7500 series routers).

When configuring connection partitioning for a BXM card, with one VSI partition per port, a number of connection spaces (LCNs) are assigned to each port as listed in Table 19-2. The **cnfrsrc** command is used to configure partition resources.

Note When the configuring the port using the **cnfrsrc** command, the term LCN is used in place of connection.

Table 19-2 Port Connection Allocations

Connection Type	cnfrsrc cmd parameter	Variable	Description
AutoRoute LCNs	maxpvclcns	a(x)	Represents the number of AutoRoute (PVC) LCNs configured for a port.
Minimum VSI LCNs for partition 1	minvsilcns	$n_1(x)$	Represents the guaranteed minimum number of LCNs configured for the port VSI partition. This value is not necessarily always available. Reaching it is dependent on FIFO access to the unallocated LCNs in the port group common pool.
Maximum VSI LCNs for partition 1	maxvsilcns	$m_1(x)$	Represents the maximum number of LCNs configured for the port VSI partition. This value is not necessarily reached. It is dependent on FIFO access to the unallocated LCNs in the port group common pool.

Note In the previous table, x is the port number and subscript “$_1$” is the partition number.

AutoRoute is guaranteed to have its assigned connection spaces (LCNs) available. Label switching, uses one connection space (LCN) per Label VC (LVC). This is usually one connection space (LCN) per source-destination pair using the port where the sources and destinations are label edge routers.

Beyond the guaranteed minimum number of connection spaces (LCNs) configured for a port VSI partition, a label switching partition uses unallocated LCNs on a FIFO basis from the common pool shared by all ports in the port group. These unallocated LCNs are accessed only after a port partition has reached its guaranteed minimum limit, “minvsilcns”, as configured by the **cnfrsrc** command.

Useful Default Allocations

Reasonable default values for all ports on all cards are listed in Table 19-3. If these values are not applicable, then other values may be configured using the **cnfrsrc** command.

Table 19-3 Port Connection Allocations, Useful Default Values

Connection Type	Variable	Useful Default Value	cnfrsrc cmd parameter
AutoRoute LCNs	a(x)	256	maxpvclcns
Minimum VSI LCNs for partition 1	$n_1(x)$	512	minvsilcns
Maximum VSI LCNs for partition 1	$m_1(x)$	16384	maxvsilcns Different types of BXM cards support different maximums. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum.

Here, a(x) = 256, $n_1(x) = 512$, and $m_1(x) = 16384$.

The next section describes more rigorous allocations which may be configured in place of using these default allocations.

Details of More Rigorous Allocations

More rigorous allocations are possible as may be desired when the default values are not applicable. For example, the LCN allocations for a port group must satisfy the following limit:

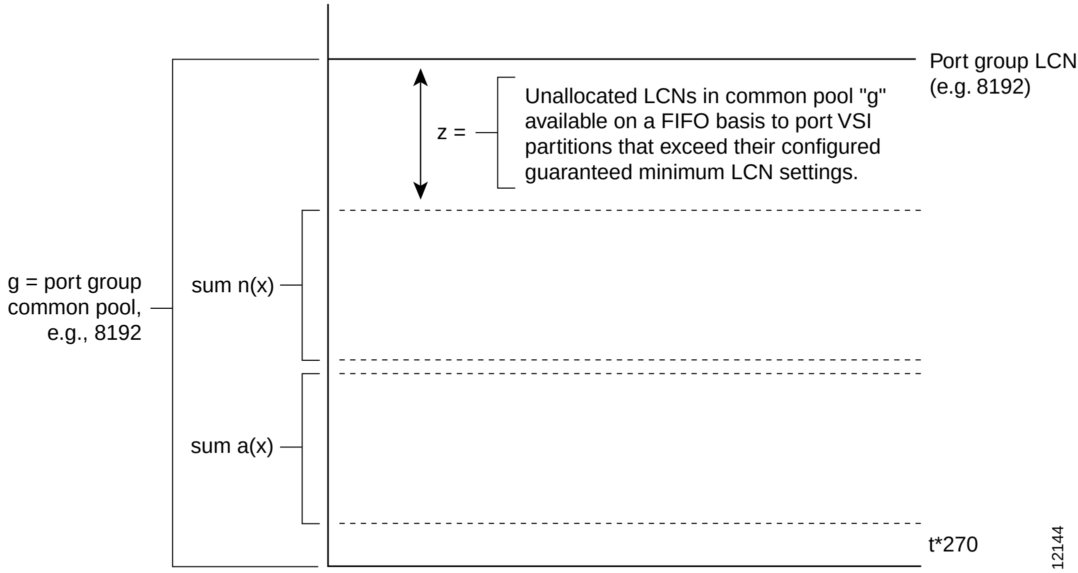
$\text{sum} (a (x)) + \text{sum} (n_1 (x)) + t * 270 <= g$

In this expression, “a (x)” represents AutoRoute LCNs, “n_1 (x)” represents the guaranteed minimum number of VSI LCNs, “t” is the number of ports in the port group that are configured as AutoRoute trunks, and “g” is the total number of LCNs available to the port group. Figure 19-8 shows the relationship of these elements.

The “270” value reflects the number of LCNs which are reserved on each AutoRoute trunk for internal purposes. If the none of the interfaces in this port group is configured in trunk mode, “t” = 0, and t*270 drops out of the expression.

For detailed information on the allocation of resources for VSI partitions, refer to the **cnfrsrc** command description in the section, *Command Reference* in this chapter.

Figure 19-8 Port VSI Partition LCN Allocation Elements


Port group LCNs
(e.g. 8192)
z =
Unallocated LCNs in common pool "g" available on a FIFO basis to port VSI partitions that exceed their configured guaranteed minimum LCN settings.
g = port group common pool, e.g., 8192
sum n(x)
sum a(x)
t*270
12144

Note Label switching can operate on a BXM card configured for either trunk (network) or port (service) mode. In Release 9.2, ports on the card can be configured either as port or trunks in any combination, they don’t all have to be configured as trunks or ports. When the card is configured for trunk mode, the trunks reserve some connection bandwidth.

Requirements

- BCC cards of one of the following versions:
  - BCC-3-64
  - BCC-4-64
  - BCC-4-128
- BPX switches require BXM cards to originate, terminate, or transfer label switching connections.

List of Terms

The following terms are defined for a label switching context only, not for general situations:

ATM-LSR—A label switching router with a number of TC-ATM interfaces. The router forwards the cells from these interfaces using labels carried in the VPI and/or VCI field.

BPX switch—The BPX switch is a carrier quality switch, with trunk and CPU hot standby redundancy.

BPX-LSR—An ATM label switch router consisting a label switch controller (a Cisco 6400 or series 7200 or 7500 router) and a label controlled switch (BPX switch).

BXM—Broadband Switch Module. ATM port and trunk card for the BPX switch.

CLI—Command line interface.

edge ATM LSR—A label switching router that is connected to the ATM-LSR cloud through TC-ATM interfaces. The ATM edge LSR adds labels to unlabeled packets and strips labels from labeled packets.

extended label ATM interface—A new type of interface supported by the remote ATM switch driver and a particular switch-specific driver that supports label switching over an ATM interface on a remotely controlled switch.

external ATM interface—One of the interfaces on the slave ATM switch other than the slave control port. It is also referred to as an exposed ATM interface, because it is available for connections outside of the label controlled switch.

LCNs—A common pool of logical connection numbers is defined per port group. The partitions in the same port group share these LCNs. New connections are assigned LCNs from the common pool.

master control port—A physical interface on a LSC that is connected to one end of a slave control link.

Ships in the Night (SIN)—The ability to support both label switching procedures and ATM Forum protocols on the same physical interface, or on the same router or switch platform. In this mode, the two protocol stacks operate independently.

slave ATM switch—An ATM switch that is being controlled by a LSC.

slave control link—A physical connection, such as an ATM link, between the LSC and the slave switch, that runs a slave control protocol such as VSI.

slave control port—An interface that uses a LSC to control the operation of a slave ATM switch (for example, VSI). The protocol runs on the slave control link.

remote ATM switch driver—A set of interfaces that allow IOS software to control the operation of a remote ATM switch through a control protocol, such as VSI.

label controlled switch—The label switch controller and slave ATM switch that it controls, viewed together as a unit.

label switch controller (LSC)—An IOS platform that runs the generic label switching software and is capable of controlling the operation of an external ATM (or other type of) switch, making the interfaces of the latter appear externally as TC-ATM interfaces.

label switching router (LSR)—A Layer 3 router that forwards packets based on the value of a label encapsulated in the packets.

TC-ATM interface—A label switching interface where labels are carried in the VPI/VCI bits of ATM cells and where VC connections are established under the control of label switching control software.

LFIB—Label Forwarding Information Base (LFIB). A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

LVC—Label switched controlled virtual circuit (LVC). A virtual circuit (VC) established under the control of label switching. A LVC is not a PVC or an SVC. It must traverse only a single hop in a label-switched path (LSP), but may traverse several ATM hops only if it exists within a VP tunnel.

VP tunnel—In the context of ATM label switching, a VP tunnel is a TC-ATM interface that traverses one or more ATM switches that do not act as ATM-LSRs.

VSI—Virtual Switch Interface. The protocol that enables an LSC to control an ATM switch over an ATM link.

VSI slave—In a hardware context, a switch or a port card that implements the VSI. In a software context, a process that implements the slave side of the VSI protocol.

VSI master—In a hardware context, a device that controls a VSI switch (for example, a VSI label switch controller). In a software context, a process that implements the master side of the VSI protocol.

Related Documents

- *Label Switching for the Cisco 7500/7200 Series Routers*
- *Cisco BPX 8600 Series Installation and Configuration*
- *Cisco BPX 8600 Series Reference*
- *Cisco WAN Switch Command Reference*

Configuration Management

The BPX switch must be initially installed, configured, and connected to a network. Following this, connections can be added to the BPX switch.

For label switching, the BPX node must be enabled for label switching.The BXM cards that will be used to support label switching connections must also be configured properly, including setting up resources for the label switching VSIs. In addition, a Label Switch Controller (6400, 7200 or 7500 series router) must be connected to one of the BXM cards configured for label switching.

Instructions for configuring the BPX switch and BXM cards for label switching are provided in the next section.

Instructions for configuring the router are provided in the applicable label switch controller documents, such as the *Label Switch Controller Documentation*.

Configuration Criteria

Label switching for VSIs on a BXM card is configured using the **cnfrsrc** and **cnfqbin** commands. Qbin 10 is assigned to label switching. (Refer also to the VSI chapter.)

The cnfqbin Command

The **cnfqbin** command is used to adjust the threshold for the traffic arriving in Qbin 10 of a given VSI interface as away of fine tuning traffic delay.

If the **cnfqbin** command is used to set an existing Qbin to disabled, the egress of the connection traffic to the network is disabled. Re-enabling the Qbin restores the egress traffic.

The cnfrsrc Command

The **cnfrsrc** command is used to enable a VSI partition and to allocate resources to the partition. An example of a **cnfrsrc** command is shown in the following example. If the **cnfrsrc** command is used to disable a partition, those connections are deleted.

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000



Last Command: cnfrsrc 4.1 256 26000 y 1 e 512 7048 2 15 26000 100000


Next Command:
```

A detailed description of the **cnfrsrc** parameters is provided later in this chapter in the *Command Reference* section under the heading **cnfrsrc**. A brief summary of the parameters and their use is provided in Table 19-4.

Table 19-4 cnfrsrc Parameter Summary

Parameter (cnfrsrc)	Example Value	Description
slot.port	4.1	Specifies the slot and port number for the BXM.
maxpvclcns	256	The maximum number of LCNs allocated for AutoRoute PVCs for this port.
maxpvcbw	26000	The maximum bandwidth of the port allocated for AutoRoute use.
partition	1	Partition number.
e/d	e	Enables or disables the VSI partition.
minvsilcns	512	The minimum number of LCNs guaranteed for this partition.
maxvsilcns	7048	The total number of LCNs the partition is allowed for setting up connections. Cannot exceed the port group max shown by the **dspcd** command.
vsistartvpi	240	VSI starting VPI: 240 and VSI ending VPI: 255. Reserves VPIs in the range of 240-255 for MPLS. Only one VP is really required, but a few more can be reserved to save for future use. AutoRoute uses a VPI range starting at 0, so MPLS should use higher values. It is best to always avoid using VPIs “0” and “1” for MPLS on the BPX 8650.The range of 240-255 is the range most compatible with a range of equipment.
vsiendvpi	255	Two VPIs are sufficient for the current release, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 240-255.
vsiminbw	26000	The minimum port bandwidth allocated to this partition in cells/sec. Entered values are ignored.
vsimaxbw	100000	The maximum port bandwidth guaranteed to this partition. The actual bw may be as high as the line rate. This value is used for VSI QBIN bandwidth scaling.

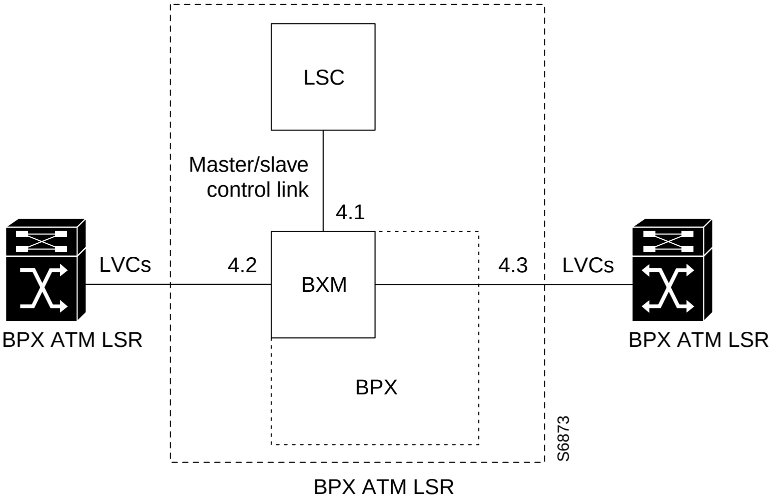
Configuration Example

The following initial configuration example for a BPX label switching router is with respect to a BXM OC-3 card located in slot 4 of the BPX switch, a Label Switch Controller (6400, 7500 or 7200 series router) connected to BXM port 4.1, and with connections to two label switching routers in the network at BXM ports 4.2 and 4.3, respectively, as shown in Figure 19-9.

For a detailed configuration example including label switch controller configuration, refer to *Chapter 20, Configuring the BPX Switch, 7200, and 7500 Routers for MPLS.*

Note For label switching, the BXM may operate in either trunk or port mode. With Release 9.2, ports may be configured as either trunks or ports at the same time. They don't all have to be configured as either trunks or ports (service).

Figure 19-9 BPX Label Switching Router with BXM in Slot 4



Step 1 Log in to the BPX switch.

Step 2 Check the card status by entering the command:

dspcds

The card status, for card in slot 4 in this example, should be "standby".

If the card status is OK, proceed to step 4, otherwise, proceed to step 3.

Step 3 If the card does not come up in standby, perform the following actions as required:

(a) Enter the command.

resetcd 4 h

(b) If the **resetcd** command does not work, pull the card and re-insert it.

(c) If reseating the card does not work, call Customer Service.

Step 4 Enter the **dspcd** command to check the port group max that can be entered for the maxvsilcn parameter of the **cnfrsrc** command. In this example, the maximum value for a port group is 7048.

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Detailed Card Display for BXM-155 in slot 4

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

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

Last Command: dspcd 4

Next Command:
```

Step 5 On the BXM in slot 4, bring up the ports 4.1, 4.2, and 4.3, as follows:

Note The following example enables ports 4.1, 4.2, and 4.3 in trunk mode with the **uptrk** command, they could also all be upped in port mode using the **upport** command. This is because label switching and the VSI make no distinction between a “port” and a “trunk”.

uptrk 4.1

uptrk 4.2

uptrk 4.3

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:39 PST

TRK     Type     Current Line Alarm Status               Other End
 2.1    OC-3      Clear - OK                              j4a/2.1
 3.1    E3       Clear - OK                              j6c(AXIS)
 5.1    E3       Clear - OK                              j6a/5.2
 5.2    E3       Clear - OK                              j3b/3
 5.3    E3       Clear - OK                              j5c(IPX/AF)
 6.1    T3       Clear - OK                              j4a/4.1
 6.2    T3       Clear - OK                              j3b/4
 4.1    OC-3      Clear - OK                              VSI(VSI)



Last Command: uptrk 4.1

Next Command:
```

Step 6 Port 4.1 is the slave interface to the label switch controller. Configure the VSI partitions for port 4.1 as follows:

cnfrsrc 4.1

PVC LCNs: [256] {accept default value}

max PVC bandwidth: 26000

y

partition: 1

enabled: e

VSI min LCNs: 512

VSI max LCNs: 7048 {varies with BXM type

VSI start VPI: 2

VSI end VPI: 15

VSI min b/w: 26000

VSI max b/w: 100000

or with one entry as follows:

cnfrsrc 4.1 256 26000 y 1 e 512 7048 2 15 26000 100000

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000



Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000


Next Command:
```

Note It is possible to have PVCs terminating on the Label Switch Controller itself, as shown in Figure 19-3. This example reserves approximately 10 Mbps (26000 cells/sec) for PVCs, and allows up to 256 PVCs on the switch port connected to the LSC.

Note The VSI max and min logical connections (LCNs) will determine the maximum number of label virtual connections (LVCs) that can be supported on the interface. The number of LVCs required on the interface depends on the routing topology of the label switch.

Note VSI starting VPI: 240 and VSI ending VPI: 255. Reserves VPIs in the range of 240-255 for MPLS. Only one VP is really required, but a few more can be reserved to save for future use. AutoRoute uses a VPI range starting at 0, so MPLS should use higher values. It is best to always avoid using VPIs “0” and “1” for MPLS on the BPX 8650. The label switching VPI interface configuration command can be used on the LSC to override the default values.

Note the label switching VPI interface configuration command can be used on the LSC to override the defaults.

Note The VSI range for label switching on the BPX switch is configured as a VSI partition, usually VSI partition number 1. VSI VPI 1 is reserved for autoroute, so the VSI partition for label switching should start at VPI 2. Two VPIs are sufficient for the current release, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 2-15.

Step 7 Ports 4.2 and 4.3 are connected to other label switch router ports in this example and support LVCs across the network. Configure the VSI partitions for ports 4.2 and 4.3 by repeating the procedures in the previous step, but entering 4.2 and 4.3, where applicable.

cnfrsrc 4.2 256 26000 y 1 e 512 7048 2 15 26000 100000

cnfrsrc 4.3 256 26000 y 1 e 512 7048 2 15 26000 100000

Maximum VSI LCNs (logical connection numbers) determine the number of connections that can be made to each port. For a description of how the LCNs may be assigned to a port, refer to *Configuring VSI LCNS on page 13*.

If the interfaces require other than a max PVC bandwidth of 10 Mbps or require other than a PVC LCN configuration of 256, adjust the configuration accordingly.

Step 8 MPLS uses Class of Service buffers 10 through 14 for label switching connections. Check the queue buffer configurations for port 4.1, for qbin 10 for example, as follows:

dspqbin 4.1 10

The qbin configuration should be as shown in the following example:

Note VC connections are grouped into large buffers called qbins. (per-VC queues can be specified on a connection-by connection basis also). In this release, all VSI connections use qbin 10 on each interface.

Sample Display:

```
Sample Display:
n4          TN    superuser       BPX 8620  9.2.20    July 26 1999 23:53 PDT

Qbin Database 2.2 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       65536 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          40%




Last Command: dspqbin 4.1 10


Next Command:
```

If the qbin is not configured as shown in the example, configure the queues on the ports using the **cnfqbin** command:

cnfqbin 4.1 10

enable/disable: e

For all other parameters, accept the (default).

The previous parameters can also be set for qbin 10 as follows:

cnfqbin 4.1 10 e n 65536 95 100 40

Sample Display:

```
Sample Display:

n4       TN     superuser       BPX 8620  9.2.2G    July 26 1999 23:57 PDT

Qbin Database 2.2 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       105920 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          40%







Last Command: cnfqbin 4.1 10 e n 65536 95 100 40


Next Command:
```

Step 9 Configure the Qbin 10 for ports 4.2 and 4.3 by performing the procedures in the previous step, but entering port 4.2 and 4.3 where applicable.

Step 10 Add a VSI controller to port 4.1, controlling partition 1

addshelf 4.1 vsi 1 1

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

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:42 PST

                        BPX Interface Shelf Information

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










Last Command: addshelf 4.1 vsi 1 1


Next Command:
```

Checking and Troubleshooting

Use the following procedure as a quick checkout of the label switching configuration and operation with respect to the BPX switch. (Refer also to the VSI chapter for additional information on configuring queues.)

Step 1 Wait a while, and check whether the controller sees the interfaces correctly;

on the LSC (also referred to as TSC), enter the following command:

tsc# show controllers VSI descriptor

and an example output is:

Note Check the LSC on-line documentation for the most current information.

```
   Phys desc:   4.1
   Log intf:    0x00040100 (0.4.1.0)
   Interface:   slave control port
   IF status:   n/a                    IFC state: ACTIVE
   Min VPI:     0                      Maximum cell rate:  10000
   Max VPI:     10                     Available channels: 999
   Min VCI:     0                      Available cell rate (forward):  100000
   Max VCI:     65535                  Available cell rate (backward): 100000

   Phys desc:   4.2
   Log intf:    0x00040200 (0.4.2.0)
   Interface:   ExtTagATM2
   IF status:   up                     IFC state: ACTIVE
   Min VPI:     0                      Maximum cell rate:  10000
   Max VPI:     10                     Available channels: 999
   Min VCI:     0                      Available cell rate (forward):  100000
   Max VCI:     65535                  Available cell rate (backward): 100000

   Phys desc:   4.3
   Log intf:    0x00040300 (0.4.3.0)
   Interface:   ExtTagATM3
   IF status:   up                     IFC state: ACTIVE
   Min VPI:     0                      Maximum cell rate:  10000
   Max VPI:     10                     Available channels: 999
   Min VCI:     0                      Available cell rate (forward):  100000
   Max VCI:     65535                  Available cell rate (backward): 100000
-------
```

Step 2 If there are no interfaces present, first check that card 4 is up,

with, on the BPX switch:

dspcds

and, if the card is not up:

resetcd 4 h

and/or remove the card to get it to reset if necessary.

Note This example assumes that the controller is connected to card 4 on the switch. Substitute a different card number, as applicable.

Step 3 Check the trunk status with the following command:

dsptrks

The **dsptrks** screen should show 4.1, 4.2 and 4.3, with the “Other End” of 4.1 reading “VSI (VSI)”. A typical **dsptrks** screen example follows:

Sample Display

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:45 PST

TRK     Type     Current Line Alarm Status              Other End
 2.1    OC-3      Clear - OK                             j4a/2.1
 3.1    E3       Clear - OK                             j6c(AXIS)
 5.1    E3       Clear - OK                             j6a/5.2
 5.2    E3       Clear - OK                             j3b/3
 5.3    E3       Clear - OK                             j5c(IPX/AF)
 6.1    T3       Clear - OK                             j4a/4.1
 6.2    T3       Clear - OK                             j3b/4
 4.1    OC-3      Clear - OK                             VSI(VSI)
 4.2    OC-3      Clear - OK                             VSI(VSI)
 4.3    OC-3      Clear - OK                             VSI(VSI)



Last Command: dsptrks

Next Command:
```

Step 4 Enter the **dspnode** command.

dspnode

The resulting screens should show trunk 4.1 as type VSI. A typical **dspnode** screen follows:

Example of **dspnode** screen.

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:46 PST

                        BPX Interface Shelf Information

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







Last Command: dspnode

Next Command:
```

Step 5 Enter the **dsprsrc** command as follows:

dsprsrc 4.1 1

The resulting screen should show the settings shown in the following example:

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:47 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000



Last Command: dsprsrc 4.1 1


Next Command:
```

Step 6 Enter the **dspqbin** command as follows:

dspqbin 4.1 10

The resulting screen should show the settings shown in the following example:

Sample Display:

```
n4          TN    superuser       BPX 8620  9.2.20    July 26 1999 23:53 PDT

Qbin Database 2.2 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       65536 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          40%




Last Command: dspqbin 4.1 10


Next Command:
```

Step 7 If interfaces 4.2 and 4.3 are present, but not enabled, perform the previous debugging steps for interfaces 4.2 and 4.3 instead of 4.1, except for the **dspnode** command which does not show anything useful pertaining to ports 4.2 and 4.3.

Step 8 Try a ping on the label switch connections. If the ping doesn't work, but all the label switching and routing configuration looks correct, check that the LSC (also known as TSC) has found the VSI interfaces correctly by entering the following command at the LSC:

tsc# show tag int

Step 9 If the interfaces are not shown, re-check the configuration of port 4.1 on the BPX switch as described in the previous steps.

Step 10 If the VSI interfaces are shown, but are down, check whether the LSRs connected to the BPX switch show that the lines are up. If not, check such items as cabling and connections.

Step 11 If the LSCs and BPX switch show the interfaces are up, but the LSC doesn't, enter the following command on the LSC:

tsc# reload

Step 12 If the “show tag int” shows that the interfaces are up, but the ping doesn't work, enter the follow command at the LSC:

tsc# sho tag tdp disc

The resulting display should show something similar to the following:

```
Local TDP Identifier:
    30.30.30.30:0
TDP Discovery Sources:
    Interfaces:
        ExtTagATM2.1:   xmit/recv
        ExtTagATM3.1:   xmit/recv
-----------------
```

Step 13 If the interfaces on the display show “xmit” and not “xmit/recv”, then the LSC is sending TDP messages, but not getting responses. Enter the following command on the neighboring LSRs:

tsc# sho tag tdp disc

If resulting displays also show “xmit” and not “xmit/recv”, then one of two things is likely:

(a) The LSC is not able to set up VSI connections

(b) The LSC is able to set up VSI connections, but cells won't be transferred because they can't get into a queue

Step 14 Check the VSI configuration on the switch again, for interfaces 4.1, 4.2, and 4.3, paying particular attention to:

(a) maximum bandwidths at least a few thousands cells/sec

(b) qbins enabled

(c) all qbin thresholds non-zero

Note VSI partitioning and resources must be set up correctly on the interface connected to the LSC, interface 4.1 in this example, as well as interfaces connected to other label switching devices.

Provisioning and Managing Connections

Instructions for configuration of the BPX switch including the setting of VSI partitions for label switching are provided in this document. Adding (provisioning) and administering connections is performed from the Label Switch Controller. For further information on the Label Switch Controller, refer to *Label Switching for the Cisco 7500/7200 Series Routers*.

Statistics

Statistics are monitored via the Label Switch Controller. Refer to the *Cisco StrataView Plus Operations Guide* for information on monitoring statistics.

Command Reference

This section provides a description of the BPX switch and LSC commands referenced in this chapter on label switching. They are presented in the following order:

BPX Switch Commands

A summary of the following commands is provided in this section. For complete descriptions of user and superuser commands, refer to the *Cisco WAN Switch Command Reference* and the Ci*sco WAN Switch Superuser Command Reference* documents.

- **addshelf**
- **cnfqbin**
- **cnfrsrc**
- **dspcd**
- **dspcds**
- **dspnode**
- **dspqbin**
- **dsprsrc**
- **dsptrks**
- **resetcd**
- **upport**
- **uptrk**

LSC Commands

```
tsc# show controller vsi descriptor

tsc# show tag int

tsc# reload

tsc# sho tag tdp disc
```

For the LSC command reference information, refer to the appropriate router 7200 or 7500 source documentation.

addshelf

Adds an ATM link between a hub node and an interface shelf such as an MGX 8220, IPX shelf, or IGX shelf in a tiered network, or an ATM link between a BXM card on a BPX node and a label switch controller such as a series 7200 or 7500 router.

Syntax

Label switch controller:

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

Interface shelf:

addshelf <slot.port> <shelf-type> <vpi> <vci>

MPLS (MultiProtocol Label Switching) controller:

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

Examples

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

Interface shelf: **addshelf 12.1 A 21 200**

Attributes

Privilege	Jobs	Log	Node	Lock
1-4	Yes	Yes	BPX switch for label switch controller, BPX switch and IGX switch for IPX and IGX shelves, BPX switch for the MGX 8220	Yes

Related Commands

delshelf, **dspnode**, **dsptrk**, **dspport**

Description for Label Switching

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

Note Once a port on the BXM is upped in either trunk or port mode by either the **uptrk** or **upport** commands, respectively, all other ports can only be “upped” in the same mode.

Table 19-5 Label Switching Parameters—addshelf

Parameter	Description
slot.port	Specifies the BXM slot and port number. (The port may be configured for either trunk (network) or port (service) mode.)
device-type	vsi, which is “virtual switch interface” and specifies a virtual interface to a label switch controller (LSC) such as a 7200 or 7500 series router.
control partition	-
control ID	Control IDs must be in the range 1-32, and must be set identically on the LSC and in the **addshelf** command. A control ID of “1” is the default used by the label switch controller.

Example for Label Switching

Add a label switch controller link to a BPX node, by entering the **addshelf** command at the desired BXM port as follows:

`addshelf 4.1 vsi 1 1`

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

                        BPX Interface Shelf Information

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










Last Command: addshelf 4.1 vsi 1 1


Next Command:
```

Description for Interface Shelves

An interface shelf can be one of the following:

- An MGX 8220 connected to a BPX node.
- An IPX or IGX node connected to a BPX node that serves as a hub for the IPX/AF or IGX/AF.
- An IGX node connected to an IGX routing node that serves as a hub for the IGX/AF.

The signaling protocol that applies to the trunk on an interface shelf is Annex G.

Each IPX/AF, IGX/AF, or MGX 8220 has one trunk that connects to the BPX or IGX node serving as an access hub. A BPX hub can support up to 16 T3 trunks to the interface shelves. An IGX hub can support up to 4 trunks to the interface shelves.

Before it can carry traffic, the trunk on an interface shelf must be "upped" (using **uptrk**) on both the interface shelf and the hub node and "added" to the network (using **addshelf**). Also, a trunk must be free of major alarms before you can add it with the **addshelf** command.

Table 19-6 Interface Shelf Parameters—addshelf

Parameter	Description
slot.port (trunk)	slot.port Specifies the slot and port number of the trunk.
shelf-type	I or A or X On a BPX node, shelf type specifies the type of interface shelf when you execute **addshelf**. The choices are I for /AF or IGX/AF, A for the MGX 8220, P for EPS (Extended Services Processor, a type of Adjunct Processor Shelf), V for VSI, or X for the MGX 8800. On an IGX hub, only the IGX/AF is possible, so *shelf type* does not appear.
vpi vci	Specifies the vpi and vci (Annex G vpi and vci used). For the MGX 8220 only, the valid range for vpi is 5–14 and for vci is 16–271. For an IGX/AF interface shelf, the valid range for both vpi and vci is 1–255. On an IGX 8400 node, when using an MGX 8800 interface shelf, the following VPI/VCI limits apply: • Use the VPI/VCI combination of 3/31 for the LMI signalling channel. When adding an MGX 8800 as an interface shelf, do not use 3/31 for anything else but the LMI signalling channel. • For VCC addressing, the VPI range is 1-255 and the VCI range is 1-65535. • For VPC addressing, the interface type is significant: UNI or NNI may be supported. When the interface type is UNI, the available VPI range is 1-255 and VCI range is 1-65535. When the interface type is NNI the available VPI range is 1-4095 and VCI range is 1-65535.
control_vpi	Choose the value for <control_VPI> such that: if <control_VPI> = 0, <control_VCI_start> can be set to a value > 40. If any VSI partition exists on the interface, then control_VPI < start_VPI or control_VPI > end_VPI for all partitions on that interface. An error message appears if the control VPI falls into the VPI range belonging to a VSI partition. No Auto Route connection exists on (VPI.start_VCI to VPI.start_VCI+14). If any Auto Route connection exists on these VPI/VCI values, you are not allowed to use these VPI/VCI values. This VPI is reserved for control VCs. Default = 0

Table 19-6 Interface Shelf Parameters—addshelf (Continued)

Parameter	Description
control_vci_start	Default = 40

The (VPI.VCI) of the 15 control VCs is:
(control_VPI.control_VCI_start) to (control_VPI.control_VCI_start+14).

The control VC used for slot n (1<= n<=15) is
(control_VPI.control_VCI_start + n -1).

Example for Interface Shelves

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

addshelf 11.1 a

The sample display shows the partial execution of the command with the prompt requesting that the I/F type be entered:

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

                        BPX Interface Shelf Information

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







This Command: addshelf 11.1


Enter Interface Shelf Type: I (IPX/AF), A (AXIS)
```

cnfqbin

Label switched VC connections are grouped into large buffers called Qbins. This command configures the Qbins. For the EFT release of label switching, Qbins 10 through 14 are used for labeled switch connections.

Refer also to the VSI chapter for additional information on configuring queues.

Syntax

cnfqbin <slot.port> <Qbin_#> <e/d> y/n <Qbin discard_thr> <Low EPD thr> <CLPhi> <EFCI_thr>

Example

cnfqbin `13.4 10 E 0 65536 6095 80100 40`

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX switch	

Related Commands

dspqbin

Parameters—cnfqbin

Parameter	Description
slot.port	slot.port Specifies the slot and port number for the BXM.
Qbin number	Specifies the number of the Qbin to be configured.
e/d	Enables or disables the Qbin.
y/n	You enter “n” not to accept default values, so you can configure the following parameters.
Qbin discard threshold	
Low EPD threshold	.
High CLP threshold	Specifies a percentage of the Qbin depth. When the threshold is exceeded, the node discards cells with CLP=1 in the connection until the Qbin level falls below the depth specified by CLP Lo.
EFCI threshold	Explicit Forward Congestion Indication.The percentage of Qbin depth that causes EFCI to be set.

Description

The following example shows the configuration of a BXM Qbin on port 4.1 for label switching.

Example

Configure a qbin by enabling it and accepting the defaults for the other parameters:

cnfqbin **`4.1 10 e n 65536 95 100 40`**

```
Qbin Database 2.2 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       105920 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          40%







Last Command: cnfqbin 4.1 10 e n 65536 95 100 40


Next Command:
```

cnfrsrc

This command configures resources among AutoRoute PVCs and VSI partitions. Refer also to the VSI chapter for additional information on configuring resources.

Syntax

cnfrsrc slot.port maxpvclcns maxpvcbw partition e/d minvsilcns maxvsilcns vsistartvpi

vsiendvpi vsiminbw vsimaxbw

Example

```
cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000
```

Attributes

Privilege	**Jobs**	**Log**	**Node**	**Lock**
			BPX switch	

Related Commands

```
dsprsrc
```

Parameters-cnfrsrc

Parameter (cnfrsrc)	Description
slot.port	Specifies the slot and port number for the BXM.
maxpvclcns	The maximum number of LCNs allocated for AutoRoute PVCs for this port. For trunks there are additional LCNs allocated for AutoRoute that are not configurable. The **dspcd** <slot> command displays the maximum number of LCNs configurable via the **cnfrsrc** command for the given port. For trunks, “configurable LCNs” represent the LCNs remaining after the BCC has subtracted the “additional LCNs” needed. For a port card, a larger number is shown, as compared with a trunk card. Setting this field to zero would enable configuring all of the configurable LCNs to the VSI.
maxpvcbw	The maximum bandwidth of the port allocated for AutoRoute use.
partition	Partition number.
e/d	Enables or disables the VSI partition.

Parameter (cnfrsrc)	Description
minvsilcns	The minimum number of LCNs guaranteed for this partition. The VSI controller guarantees at least this many connection endpoints in the partition, provided that there are sufficient free LCNs in the common pool to satisfy the request at the time the partition is added. When a new partition is added or the value is increased, it may be that existing connections have depleted the common pool so that there are not enough free LCNs to satisfy the request. The BXM gives priority to the request when LCNs are freed. The net effect is that the partition may not receive all the guaranteed LCNs (min LCNs) until other LCNs are returned to the common pool. This value may not be decreased dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. The value may be increased dynamically. However, this may cause the “deficit” condition described above. The command line interface warns the user when the action is invalid, except for the “deficit” condition. To avoid this deficit condition which could occur with maximum LCN usage by a partition or partitions, it is recommended that all partitions be configured ahead of time before adding connections. Also, it is recommended that all partitions be configured before adding a VSI controller via the **addshelf** command.
maxvsilcns	The total number of LCNs the partition is allowed for setting up connections. The min LCNs is included in this calculation. If max LCNs equals min LCNs, then the max LCNs are guaranteed for the partition. Otherwise, (max - min) LCNs are allocated from the common pool on a FIFO basis. If the common pool is exhausted, new connection setup requests will be rejected for the partition, even though the max LCNs has not been reached. This value may be increased dynamically when there are enough unallocated LCNs in the port group to satisfy the increase. The value may not be decreased dynamically. All partitions in the same port group must be deleted first and reconfigured in order to reduce this value. Different types of BXM cards support different maximums. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum.
vsistartvpi	VSI starting VPI: 240 and VSI ending VPI: 255. Reserves VPIs in the range of 240-255 for MPLS. Only one VP is really required, but a few more can be reserved to save for future use. AutoRoute uses a VPI range starting at 0, so MPLS should use higher values. It is best to always avoid using VPIs “0” and “1” for MPLS on the BPX 8650. The label switching VPI interface configuration command can be used on the LSC to override the default values.
vsiendvpi	Two VPIs are sufficient for the current release, although it may be advisable to reserve a larger range of VPIs for later expansion, for example, VPIs 240-255.
vsiminbw	The minimum port bandwidth allocated to this partition in cells/sec. (Multiply by 400 based on 55 bytes per ATM cell to get approximate bits/sec.)
vsimaxbw	The maximum port bandwidth allocated to this partition. This value is used for VSI QBIN bandwidth scaling.

Description

The following paragraphs describe various configurations of BXM port resources for label switching. The first allocation example is using default allocations. The second allocation example describes more rigorous allocations where default allocations are not applicable.

Useful Default Allocations

Reasonable default values for all ports on all cards are listed in Table 19-7. If these values are not applicable, then other values may be configured using the **cnfrsrc** command.

Table 19-7 Port Connection Allocations, Useful Default Values

Connection Type	Variable	Useful Default Value	cnfrsrc cmd parameter
AutoRoute LCNs	a(x)	256	maxpvclcns
Minimum VSI LCNs for partition 1	$n_1(x)$	512	minvsilcns
Maximum VSI LCNs for partition 1	$m_1(x)$	7048	maxvsilcns Different types of BXM cards support different maximums. If you enter a value greater than the allowed maximum, a message is displayed with the allowable maximum

Here, a(x) = 256, $n_1(x)$ = 512, and $m_1(x)$ = 16384.

Example:

Configure the VSI partition for port 4.1 by entering the following command:

```
cnfrsrc 4.1 256 26000 1 e 512 16384 2 15 26000 100000
```

Sample Display:

```
n4              TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000


Last Command: cnfrsrc 4.1 256 26000 1 e 512 7048 2 15 26000 100000


Next Command:
```

Details of More Rigorous Allocations

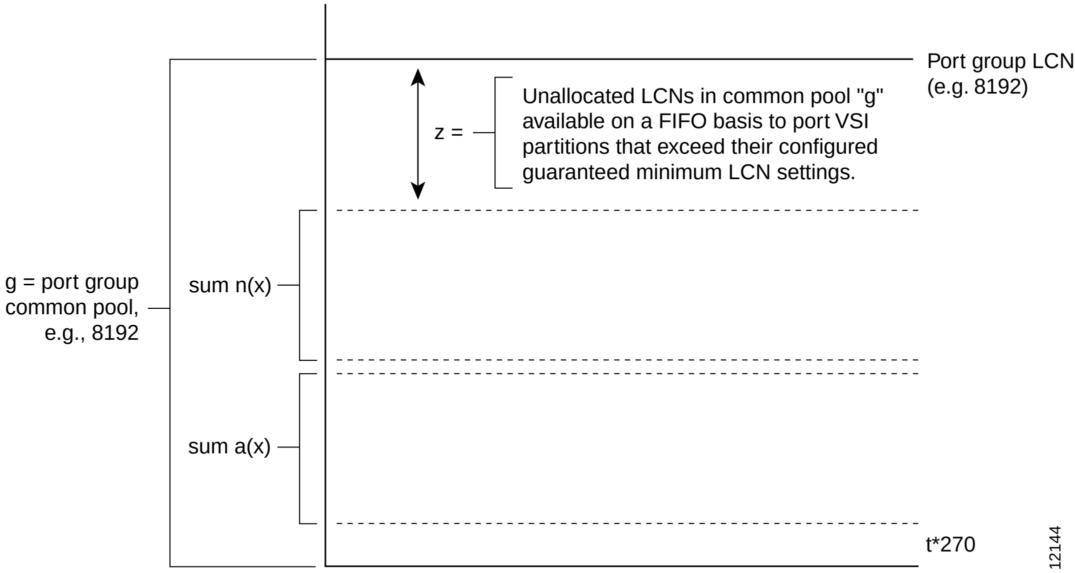
More rigorous allocations are possible when default values are not applicable. For example, the LCN allocations for a port group must satisfy the following limit:

sum (a (x)) + sum (n_1 (x)) + t *270 <= g

In this expression, “a (x)” represents AutoRoute LCNs, “n_1 (x)” represents the guaranteed minimum number of VSI LCNs, “t” is the number of ports in the port group that are configured as AutoRoute trunks, and “g” is the total number of LCNs available to the port group. Figure 19-10 shows the relationship of these elements.

The “270” value reflects the number of LCNs which are reserved on each AutoRoute trunk for internal purposes. If the port is configured in port rather than trunk mode, “t” = 0, and t*270 drops out of the expression.

Figure 19-10 Port VSI Partition LCN Allocation Elements


Port group LCNs
(e.g. 8192)
z =
Unallocated LCNs in common pool "g" available on a FIFO basis to port VSI partitions that exceed their configured guaranteed minimum LCN settings.
g = port group common pool, e.g., 8192
sum n(x)
sum a(x)
t*270
12144

Note Label switching can operate on a BXM card configured for either trunk (network) or port (service) mode. If a BXM card is configured for port (service) mode, all ports on the card are configured in port (service) mode. If a BXM card is configured for trunk (network) mode, all ports on the card are configured for trunk (network) mode. When the card is configured for trunk mode, the trunks reserve some connection bandwidth.

In the following expression, “z_1” equals the number of unallocated LCNs in the common pool of LCNs available for use by the port VSI partitions. The value of “z_1” is the number of LCNs available after subtracting the AutoRoute LCNs [sum (a (x)], VSI LCNs [sum (n_1 (x))], and LCNs for trunk use [t*270] from the total number of LCNs “g” available at the port. For a BXM card with ports configured in “port” mode, “t” = 0.

z_1 = (g - sum (a(x)) - sum (n_1(x) -t*270)

When a port partition has exhausted its configured guaranteed LCNs (min LCNs), it may draw LCNs for new connections on a FIFO basis from the unallocated LCNs, “z_1”, until its maximum number of LCNs, “$m_1(x)$”, is reached or the pool, “z1”, is exhausted.

No limit is actually placed on what may be configured for “m_1 (x)”, although “m_1 (x)” is effectively ignored if larger than “$z_1 + n_1$”.The value “m_1 (x)” is a non-guaranteed maximum value of connection spaces that may be used for a new connection or shared by a number of connections at a given time if there are a sufficient number of unallocated “LCNs available in “z_1”. The value m_1 (x) typically is not used in Release 9.2, but in future releases allows more control over how the LCNs are shared among multiple VSI partitions.

The following two examples, one for a BXM in port mode and the other for a BXM in trunk mode, provide further detail on the allocation of connections.

Example 1, 8-Port OC-3 BXM Configured in Trunk Mode

This example is for an 8-port OC-3 BXM configured for trunk mode with all ports configured as trunks. Table 19-8 lists the configured connection space (LCN) allocations for each port of “a (x)”, “n_1 (x)”, and “m_1 (x)”. It also shows the unallocated LCN pool, “z_1” for each port group and the total common pool access, “g”.

Note LCN is the variable affected when configuring connection space allocations using the **cnfrsrc** command.

The port groups in the example are ports 1-4 and 5-8, and the maximum number of connection spaces (LCNs) per port group is 8192 for this 8-port-OC-3 BXM card. The allocations for ports 1-4 are shown in Figure 19-11. The allocations for ports 5-8 are similar to that shown in Figure 19-11, but with correspondingly different values.

As shown in Figure 19-11, “g” is the total number of connection spaces (LCNs) available to port group 1-4 and is equal to 8192 LCNs in this example. To find the number of unallocated LCNs available for use by port partitions that exhaust their assigned number of LCNs, proceed as follows:

From “g”, subtract the sum of the AutoRoute connections, “a (x)”, and the sum of minimum guaranteed LCNs, “n_1 (x)”. Also, since the ports in this example are configured in trunk mode, 270 LCNs per port are subtracted from “g”. Since there are four ports, “t” equals “4” in the expression “t*270”. The resulting expression is as follows:

z_1 = (g - sum (a (x)) - sum (n_1 (x)) - t*270)

The remaining pool of unallocated LCNs is “z_1” as shown. This pool is available for use by ports 1-4 that exceed their minimum VSI LCN allocations “n1 (x)” for partition 1.

The maximum number of LCNs that a port partition can access on a FIFO basis from the unallocated pool “z_1” for new connections can only bring its total allocation up to either “(z_1 + n_1 (x)) or m_1(x)”, whichever value is smaller. Also, since “z_1” is a shared pool, the value of “z_1” will vary as the common pool is accessed by other port partitions in the group.

The values shown in Table 19-8 are obtained as follows:

- For ports 1-4:

  z_1 = (g - sum (a(x)) - sum(n_1(x) -4*270)

  and factoring in the sum of a (x) and the sum of n_1 (x), the above expression evaluates to:

  = (8192 - (185) - (3100) -4*270) = 3827 unallocated LCNs

The values shown in Table 19-8 for the port group containing ports 1-4 may be summarized as follows:

— Port 1 is guaranteed to be able to support 120 AutoRoute connections (PVCs) and 3000 label VCs (LVCs). It will not support more than 120 PVCs. It may be able to support up to 3500 LVCs, subject to availability of unallocated LCNs "z_1" on a FIFO basis. Since "m_1 (1)" of 3500 is less than "z_1" of 3827, the most LVCs that can be supported are 3500.

— Port 2 will support up to 50 PVCs, and no more. It will support no LVCs, as "m_1(2)" = 0.

— Port 3 is guaranteed to support up to 15 PVCs, and no more. It is not guaranteed to support any LVCs, but will support up to:

3827 LVCs, subject to availability of unallocated LCNs "z_1" on a FIFO basis. The configured maximum limit "m_1(3)" of 7048 LCNs is ignored, as it is greater than the unallocated LCNs, "z_1", of 3827.

— Port 4 supports no PVCS. It is guaranteed to support 100 LVCs, and no more.

- For ports 5-8:

z_1 = (g - sum (a(x)) - sum (n_1(x) -4 * 270)

and factoring in the sum of a (x) and the sum of n_1 (x), the above expression evaluates to:

= (8192 - (6100) - (310) - 4 * 270) = 702 unallocated LCNs

The values shown in Table 19-8 for the port group containing ports 5-8 may be summarized as follows:

— Port 5 will support 6000 PVCs, and at least 10 LVCs. It will support up to 712 LVCs, subject to availability of the 702 unallocated LCNs "z_1" on a FIFO basis. The configured maximum limit "m_1(5)" of 7048 is ignored, as it is greater than 712 (the unallocated 702 LCNs in the "z_1" pool plus the 10 LCN guaranteed minimum already allocated from the common pool "g" of 8192 LCNs).

— Port 6 will support no PVCs. It will support up to 100 LVCs subject to available LCNs, but is not guaranteed to be able to support any LVCs.

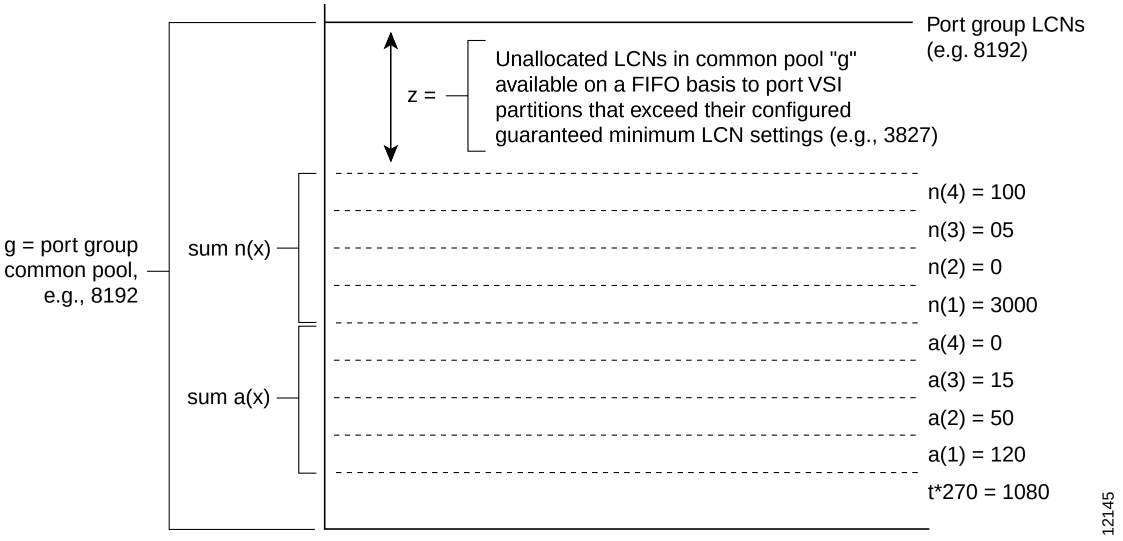
— Port 7 is guaranteed to be able to support 100 PVCs and 200 LVCs. It will not support any more.

— Port 8 will support no PVCs. It is not guaranteed to be able to support more than 100 LVCs, but will support up to 802 LVCs, subject to the availability of the 702 unallocated LCNs "z_1" on a FIFO basis. The configured maximum limit "m_1(8)" of 2100 LVCS is ignored, as it is greater than 802 (the number of unallocated 702 LCNs in the "z_1" pool plus the 100 LCN guaranteed minimum already allocated from the common pool "g" of 8192 LCNs).

Table 19-8 LCN Allocations for 8-port OC-3 BXM, Ports Configured in Trunk Mode

Port (x)	a(x)	n_1(x)	m_1(x)	z_1 = unallocated LCNs	Total LCNS available to Port VSI Partition = min (z_1 + n_1(x), max m_1 (x))
Port Group 1					
1	120	3000	3500	3827	3500
2	50	0	0	3827	0
3	15	0	7048	3827	3827
4	0	100	100	3827	100
Sum, for x =1 through 4	185	3100	N/A	N/A	
Port Group 2					
5	6000	10	7048	702	712
6	0	0	100	702	100
7	100	200	200	702	200
8	0	100	2100	702	802
Sum for x = 5 through 8	6100	310	N/A	N/A	

Figure 19-11 LCN Allocations for Ports 1-4, Ports Configured in Trunk Mode Example


Port group LCNs (e.g. 8192)
z =
Unallocated LCNs in common pool "g" available on a FIFO basis to port VSI partitions that exceed their configured guaranteed minimum LCN settings (e.g., 3827)
g = port group common pool, e.g., 8192
sum n(x)
sum a(x)
n(4) = 100
n(3) = 05
n(2) = 0
n(1) = 3000
a(4) = 0
a(3) = 15
a(2) = 50
a(1) = 120
t*270 = 1080
12145

Example 2, 8-Port OC-3 BXM Configured in Port Mode

BXM ports configured for port mode rather than trunk mode have more connection spaces available for use by the LVC connections as it is not necessary to provide connection spaces for use by the AutoRoute trunks. This example is for an 8-port OC-3 BXM configured for port mode, with all ports configured as ports. Table 19-9 lists the configured connection space (LCN) allocations for each port of “a (x)”, “n_1 (x)”, and “m_1 (x)”. It also shows the unallocated LCN pool, “z_1” for each port group and the total common pool access, “g”.

Note LCN is the variable affected when configuring connection space allocations using the **cnfrsrc** command.

The port groups in the example are ports 1-4 and 5-8, and the maximum number of connection spaces (LCNs) per port group is 8192 for this 8-port-OC-3 BXM card. The allocations for ports 1-4 are shown in Figure 19-12. The allocations for ports 5-8 are similar to that shown in Figure 19-12, but with correspondingly different values.

As shown in Figure 19-12, “g” is the total number of connection spaces (LCNs) available to port group 1-4 and is equal to 8192 LCNs in this example. To find the number of unallocated LCNs available for use by port partitions that exhaust their assigned number of LCNs, proceed as follows:

From “g”, subtract the sum of the AutoRoute connections, “a (x)”, and the sum of minimum guaranteed LCNs, “n_1 (x)”. Also, since the ports in this example are configured in port mode, “t” equals zero in the expression “t * 270”. This is indicated as follows:

z_1 = (g - sum (a (x)) - sum (n_1 (x)) - t * 270)

The remaining pool of unallocated LCNs is “z_1” as shown. This pool is available for use by ports 1-4 that exceed their minimum VSI LCN allocations “n1 (x)” for partition 1.

The maximum number of LCNs that a port partition can access on a FIFO basis from the unallocated pool “z1” for new connections can only bring its total allocation up to either “(z_1 + n_1 (x)) or m_1(x)”, whichever value is smaller. Also, since “z_1” is a shared pool, the value of “z_1” will vary as the common pool is accessed by other port partitions in the group.

The values shown in Table 19-9 are obtained as follows:

- For ports 1-4:

  z_1 = (g - sum (a(x)) - sum (n_1(x) -0*270)

  which simplifies to:

  z_1 = (g - sum (a(x)) - sum (n_1(x))

  and factoring in the sum of a (x) and the sum of n_1 (x), the above expression evaluates to:

  = (8192 - (185) - (3100)) = 4907 unallocated LCNs

  The values shown in Table 19-9 for the port group containing ports 1-4 may be summarized as follows:

  - Port 1 is guaranteed to be able to support 120 AutoRoute connections (PVCs) and 3000 label VCs (LVCs). It will not support more than 120 PVCs. It may be able to support up to 3500 LVCs, subject to availability of unallocated LCNs “z_1” on a FIFO basis. Since “m_1 (1)” of 3500 is less than “z_1” of 4907, the most LVCs that can be supported are 3500.
  - Port 2 will support up to 50 PVCs, and no more. It will support no LVCs, as “m_1(2)” = 0.

- — Port 3 is guaranteed to support up to 15 PVCs, and no more. It is not guaranteed to support any LVCs, but will support up to:

  4907 LVCs, subject to availability of unallocated LCNs “z_1” on a FIFO basis. The configured maximum limit “$m_1(3)$” of 7588 LCNs is ignored, as it is greater than the unallocated LCNs, “z_1”, of 4907.

- — Port 4 supports no PVCS. It is guaranteed to support 100 LVCs, and no more.

- For ports 5-8:

  z_1 = (g - sum (a(x)) - sum(n_1(x) -0 * 270)

  which simplifies to:

  z_1 = (g - sum (a(x)) - sum(n_1(x))

  and factoring in the sum of a (x) and the sum of n_1 (x), the above expression evaluates to:

  = (8192 - (6100) - (310)) = 1782 unallocated LCNs

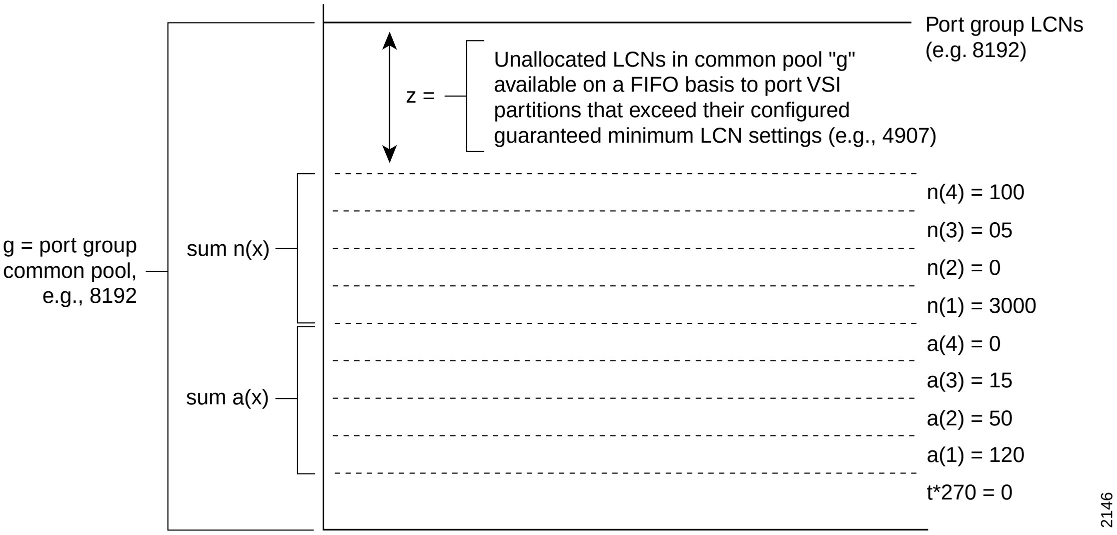
The values shown in Table 19-9 for the port group containing ports 5-8 may be summarized as follows:

- — Port 5 will support 6000 PVCs, and at least 10 LVCs. It will support up to 1792 LVCs, subject to availability of the 1782 unallocated LCNs “z_1” on a FIFO basis. The configured maximum limit “$m_1(5)$” of 7588 is ignored, as it is greater than 1792 (the unallocated 1782 LCNs in the “z_1” pool plus the 10 LCN guaranteed minimum already allocated from the common pool “g” of 8192 LCNs).
- — Port 6 will support no PVCs. It will support up to 100 LVCs subject to available LCNs, but is not guaranteed to be able to support any LVCs.
- — Port 7 is guaranteed to be able to support 100 PVCs and 200 LVCs. It will not support any more.
- — Port 8 will support no PVCs. It is not guaranteed to be able to support more than 100 LVCs, but will support up to 1882 LVCs, subject to availability of the 1782 unallocated LCNs “z_1” on a FIFO basis. The configured maximum limit “$m_1(8)$” of 2100 LVCS is ignored, as it is greater than 1882 (the number of unallocated 1782 LCNs in the “z1” pool plus the 100 LCN guaranteed minimum already allocated from the common pool “g” of 8192 LCNs).

Table 19-9 LCN Allocations for 8-Port OC-3 BXM, Ports Configured in Port Mode

Port (x)	a(x)	n_1(x)	m_1(x)	z_1 = unallocated LCNs	Total LCNS available to Port VSI Partition = min (z_1 + n_1(x), max m_1 (x))
			Port Group 1		
1	120	3000	3500	4907	3500
2	50	0	0	4907	0
3	15	0	7588	4907	4907
4	0	100	100	4907	100
Sum, for x =1 through 4	185	3100	N/A	N/A	
			Port Group 2		
5	6000	10	7588	1782	1792
6	0	0	100	1782	100
7	100	200	200	1782	200
8	0	100	2100	1782	1882
Sum for x = 5 through 8	6100	310	N/A	N/A	

Figure 19-12 LCN Allocations for Ports 1-4, Ports Configured in Port Mode Example


Port group LCNs (e.g. 8192)
z =
Unallocated LCNs in common pool "g" available on a FIFO basis to port VSI partitions that exceed their configured guaranteed minimum LCN settings (e.g., 4907)
n(4) = 100
n(3) = 05
n(2) = 0
n(1) = 3000
a(4) = 0
a(3) = 15
a(2) = 50
a(1) = 120
t*270 = 0
g = port group common pool, e.g., 8192
sum n(x)
sum a(x)
2146

dspcd

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

Syntax

dspcd <slot>

Example

dspcd 5

Attributes

Privilege	Jobs	Log	Node	Lock
1-6	No	No	IPX switch, IGX switch, BPX switch	No

Related Commands

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

Parameters—dspcd

Parameter	Description
slot	slot number of card.

Description

The following shows an example of the **dspcd** command for a BXM card.

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Detailed Card Display for BXM-155 in slot 4
Status:          Active
Revision:        CD18
Serial Number:   693313
Fab Number:      28-2158-02
Queue Size:      228300
Support:         FST, 4 Pts,OC-3,Vc
Chnls:16320,PG[1]:7588,PG[2]:7588
PG[1]:1,2,
PG[2]:3,4,
Backcard Installed
  Type:          LM-BXM
  Revision:      BA
  Serial Number: 688284
  Supports: 8 Pts, OC-3, MMF Md


Last Command: dspcd 4

Next Command:
```

dspcds

Displays the cards in a shelf, front and back, with their type, revision, and status.

Syntax

dspcds [l]

Example

dspcds

Attributes

Privilege	Jobs	Log	Node	Lock
1-6	No	No	IPX switch, IGX switch, BPX switch	No

Related Commands

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

Parameters—dspcds

Parameter	Description
l	Directs the system to display status of the cards on just the lower shelf of an IPX 32 or IGX 8430. If not entered, **dspcds** displays the top shelf by default.

Description

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

For an IPX 32 or IGX 8430, the screen initially displays only the upper shelf with a “Continue?” prompt. Typing “y” to the prompt displays the cards in the lower shelf. The command **dspcds** followed by the letter “L” (for lower shelf) displays card status for just the lower shelf. For an IPX 8 or IGX 8410, the card information appears in only the left column. The status and update messages are as follows:

- Active Card in use, no failures detected.
- Active—F Card in use, failure(s) detected.
- Active—T Card active, background test in progress.
- Active—F-T Card active, minor failures detected, background test in progress.
- Standby Card idle, no failures.

- Standby—F Card idle, failure(s) detected.
- Standby—T Card idle, background test in progress.
- Standby—F-T Card idle, failure(s) detected, background test in progress.
- Failed Card failed.
- Down Card downed by user.
- Down—F Card downed, failure(s) detected.
- Down—T Card downed, failure(s) detected, background test in progress.
- Mismatch Mismatch between front card and back card.
- Update * Configuration RAM being updated from active control card.
- Locked* Incompatible version of old software is being maintained in case it is needed.
- Dnlding* Downloading new system software from the active BCC (BPX switch), or NPC (IPX switch or IGX switch), adjacent node, or from StrataView Plus.
- Dnldr* Looking to adjacent nodes or StrataView Plus for either software to load or other software needs you have not specifically requested.

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

Example

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST



   FrontCard    BackCard                   FrontCard    BackCard
   Type    Rev  Type  Rev   Status         Type    Rev  Type  Rev   Status
1  Empty                                9  ASI-155 BE02 MMF-2 AB    Standby
2  BXM-155 BB16 MM-8  BA    Active      10 BME-622 KDJ  MM-2  FH    Active
3  Empty                                11 BXM-E3  BB16 TE3-12P04   Active
4  BNI-E3  CE08 E3-3  JY    Active      12 BXM-155 BB16 MM-8  BA    Active
5  BNI-E3  CE08 E3-3  EY    Active      13 BXM-155 AC30 SM-4  P05   Active
6  BNI-T3  CF08 T3-3  FH    Active      14 Empty
7  BCC-3   DJL  LM-2  AA    Active      15 ASM     ACB  LMASM P01   Active
8  BCC-3   DJL  LM-2  AA    Standby




Last Command: dspcds


Next Command:
```

dspnode

Displays a summary of interface devices connected to a routing node, or when executed from an IPX or IGX interface shelve shows the name of its hub node and trunk number.

Syntax:

dspnode

Related Commands

addshelf, **delshelf**, **dsptrk**

Attributes

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

Description

The command displays label switch controller devices connected to a BPX node and interface shelves connected to an IGX switch or BPX node. The command can be used to isolate the shelf or label switch controller where an alarm has originated.

The routing nodes in a network do not indicate the interface shelf or label switch controller where an alarm condition exists, so **dspnode** may be executed at a hub node to find out which interface device originated the alarm.

When executed on an IPX or IGX interface shelve, **dspnode** shows the name of the hub node and the trunk number. Note that to execute a command on an IPX or IGX interface shelf, you must either use a control terminal directly attached to the IPX or IGX switch or telnet to the IPX/AF, as the **vt** command is not applicable.

Example

Displays information about label switch controllers and interface shelves (executed on the BPX hub node).

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PSTT

                        BPX Interface Shelf Information

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




Last Command: dspnode


Next Command:
```

dspqbin

Displays the configuration of the specified Qbin on a BXM.

Syntax

dspqbin <slot.port> <qbin number>

Example

dspqbin 4.1 10

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX switch	

Related Commands

cnfqbin

Parameters-dspqbin

Parameter	Description
slot.port	The slot and port number of interest.
qbin number	The qbin number. For EFT label switching, this is Qbin number 10.

Description

The following example shows configuration of Qbin 10 on port 4.1 of a BXM card.

Example

dspqbin 4.1 10

Sample Display:

```
n4          TN    superuser       BPX 8620  9.2.20    July 26 1999 23:53 PDT

Qbin Database 2.2 on BXM qbin 10        (Configured by MPLS1 Template)
                                        (EPD Enabled on this qbin)

Qbin State:              Enabled
Discard Threshold:       65536 cells
EPD Threshold:           95%
High CLP Threshold:      100%
EFCI Threshold:          40%




Last Command: dspqbin 4.1 10


Next Command:
```

dsprsrc

Displays the label switching resource configuration of the specified partition on a BXM card.

Syntax

dsprsrc <slot.port> <partition>

Example

dsprsrc 4.1 1

Attributes

Privilege	Jobs	Log	Node	Lock
			BPX switch	

Related Commands

cnfrsrc

Parameters-dspcds

Parameter	Description
slot.port	Specifies the BXM slot and port.
partition	Specifies the vsi partition.

Description

The following example shows configuration of vsi resources for partition 1 at BXM port 4.1.

Example Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Port/Trunk : 4.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:26000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             7048
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        100000


Last Command: dsprsrc 4.1 1


Next Command:
```

dsptrks

Display information on the trunk configuration and alarm status for the trunks at a node. The trunk numbers with three places represent virtual trunks.

Syntax

dsptrks

Related Commands

addtrk, **deltrk**, **dntrk**, **uptrk**

Attributes

Privilege	Jobs	Log	Node	Lock
1-6	No	No	IPX switch, IGX switch, BPX switch	No

Description

Displays basic trunk information for all trunks on a node. This command applies to both physical only and virtual trunks. The displayed information consists of:

- Trunk number, including the virtual trunk number (three places such as 4.1.10).
- Line type (E1, T3, or OC-3, for example).
- Alarm status.
- Device type at other end of trunk, such as node, interface shelf, label switch controller.

For trunks that have been added to the network with the **addtrk** or **addshelf** command, the information includes the device name and trunk number at the other end. Trunks that have a "–" in the Other End column have been upped with **uptrk** but not yet added. For disabled trunks, the trunk numbers appear in reverse video on the screen. Virtual trunk numbers contain three parts, for example, 4.1.1.

Example

Enter the **dsptrks** command as follows to display the trunks on a BPX switch:

dsptrks

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

TRK     Type     Current Line Alarm Status               Other End
 2.1    OC-3      Clear - OK                              j4a/2.1
 3.1    E3       Clear - OK                              j6c(AXIS)
 5.1    E3       Clear - OK                              j6a/5.2
 5.2    E3       Clear - OK                              j3b/3
 5.3    E3       Clear - OK                              j5c(IPX/AF)
 6.1    T3       Clear - OK                              j4a/4.1
 6.2    T3       Clear - OK                              j3b/4
 4.1    OC-3      Clear - OK                              VSI(VSI)
 4.2    OC-3      Clear - OK                              VSI(VSI)
 4.3    OC-3      Clear - OK                              VSI(VSI)



 Last Command: dsptrks


 Next Command:
```

resetcd

The reset card command resets the hardware and software for a specified card.

Syntax

resetcd <slot_num> <reset_type>

Example

resetcd 5 H

Attributes

Privilege	Jobs	Log	Node	Lock
1-3	Yes	Yes	IPX switch, IGX switch, BPX switch	Yes

Related Commands

dspcd

Parameters—resetcds

Parameter	Description
slot number	Specifies the card number to be reset.
H/F	Specifies whether the hardware or failure history for the card is to be reset. An “H” specifies hardware; an “F” specifies failure history.

Description

A hardware reset is equivalent to physically removing and reinserting the front card of a card group and causes the card’s logic to be reset. When you reset the hardware of an active card other than a controller card (an NPC, NPM, or BCC), a standby card takes over if one is available. A failure reset clears the card failures associated with the specified slot. If a slot contains a card set, both the front and back cards are reset.

Do not use the **reset** command on an active NPC, NPM, or BCC because this causes a temporary interruption of all traffic while the card is re-booting. (Resetting a controller card does not destroy configuration information.) Where a redundant NPC, NPM, or BCC is available, the **switchcc** command is used to switch the active controller card to standby and the standby controller card to active. If a standby card is available, resetting an active card (except for a NPC, NPM, or BCC) does not cause a system failure. H/F Resetting of an active card that has no standby does disrupt service until the self-test finishes.

Example 1

resd 3 H

Sample Display:

No display is generated.

upport

Displays the cards in a shelf, front and back, with their type, revision, and status.

Syntax

upport <slot.port>

Example

upport 4.2

Attributes

Privilege	Jobs	Log	Node	Lock
1-2	Yes	Yes	BPX switch	Yes

Related Commands

dnport, **cnfport**, **upln**

Parameters-dspcds

Parameter	Description
slot.port	Specifies the slot number and port number of the port to be activated.

Related Commands

dnport, **cnfport**, **upln**

Description

The following example shows the screen that is displayed when the following command is entered to up a port on an ASI card:

upport 4.2

System Response

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

Port:       4.2     [ACTIVE  ]
Interface:          T3-2
Type:               UNI
Speed:              96000 (cps)

CBR Queue Depth:              200
CBR Queue CLP High Threshold: 80%
CBR Queue CLP Low Threshold:  60%
CBR Queue EFCI Threshold:     80%
VBR Queue Depth:              1000    ABR Queue Depth:              9800
VBR Queue CLP High Threshold: 80%     ABR Queue CLP High Threshold:  80%
VBR Queue CLP Low Threshold:  60%     ABR Queue CLP Low Threshold:   60%
VBR Queue EFCI Threshold:     80%     ABR Queue EFCI Threshold:      80%



Last Command: upport 4.2


Next Command:
```

uptrk

Activates (or “ups”) a trunk.

Syntax

uptrk <slot.port>[.vtrk]

Example

uptrk 4.1

Related Commands

addtrk, **dntrk**

Attributes

Privilege	Jobs	Log	Node	Lock
1-2	Yes	Yes	IPX switch, IGX switch, BPX switch	Yes

Parameters-uptrk

Parameter	Description
slot.port	Specifies the slot and port of the trunk to activate. If the card has only one port, the *port* parameter is not necessary. An NTM, for example, has one port.

Optional Parameters-uptrk

Parameter	Description
vtrk	Specifies the virtual trunk number. The maximum on a node is 32. The maximum on a T3 or E3 line is 32. The maximum for user traffic on an OC-3/STM1 trunk is 11 (so more than one OC-3/STM1 may be necessary).

Description

After you have upped the trunk but not yet *added* it, the trunk carries line signaling but does not yet carry live traffic. The node verifies that the trunk is operating properly. When the trunk is verified to be correct, the trunk alarm status goes to clear. The trunk is then ready to go into service, and can be added to the network.

If you need to take an active trunk between nodes out of service, the **dntrk** command may be used. However, this will result in temporary disruptions in service as connections are rerouted. The **dntrk** command causes the node to reroute any existing traffic if sufficient bandwidth is available.

Interface Shelves and Label Switch Controllers: For interface shelves or label switch controllers connected to a node, connections from those devices will also be disrupted when the links to them are deleted. For an interface shelf, the **delshelf** command is used to deactivate the trunk between the IGX or BPX routing node and the shelf.

Label Switch Controller: For a label switch controller, the **delshelf** command is also used to deactivate the link between the BPX routing node and the label switch controller. In the case of label switching, this is a link between a port on the BXM card and the label switch controller. This link can be connected to a port that has been upped by either the upport or **uptrk** command, as the label switching operation does not differentiate between these modes on the BXM.

Virtual Trunks: If you include the optional *vtrk* parameter, **uptrk** activates the trunk as a *virtual* trunk. If the front card is a BXM (in a BPX switch), **uptrk** indicates to the BXM that it is supporting a trunk rather than a UNI port. (See the **upln** description for the BXM in port mode.)

You cannot mix physical and virtual trunk specifications. For example, after you up a trunk as a standard trunk, you cannot add it as a virtual trunk when you execute **addtrk**. Furthermore, if you want to change trunk types between standard and virtual, you must first down the trunk with **dntrk** then up it as the new trunk type.

You cannot up a trunk if the required card is not available. Furthermore, if a trunk is executing self-test, a “card in test” message may appear on-screen. If this message appears, re-enter **uptrk**.

Example 1

Activate (up) trunk 21—a single-port card, in this case, so only the slot is necessary.

uptrk 21

Example 2

This example shows the screen when BXM trunk 4.1 connected to a Label Switch Controller is upped with the following command:

uptrk 4.1

Sample Display:

```
n4             TN     SuperUser       BPX 15    9.2      Apr. 4 1999  16:40 PST

TRK     Type     Current Line Alarm Status               Other End
 2.1    OC-3      Clear - OK                              j4a/2.1
 5.1    E3       Clear - OK                              j6c(AXIS)
 5.1    E3       Clear - OK                              j6a/5.2
 5.2    E3       Clear - OK                              j3b/3
 5.3    E3       Clear - OK                              j5c(IPX/AF)
 6.1    T3       Clear - OK                              j4a/4.1
 6.2    T3       Clear - OK                              j3b/4
 4.1    OC-3      Clear - OK                              VSI(VSI)




Last Command: uptrk 4.1


Next Command:
```

Example 3

Activate (up) trunk 6.1.1—a virtual trunk, in this case, which the third digit indicates.

uptrk 6.1.1

Configuring the BPX Switch, 7200, and 7500 Routers for MPLS

This chapter provides basic information for configuring BPX switches and associated label switching controllers along with edge routers for Multiprotocol Label Switching (MPLS) operation. Once MPLS is running in the network, OSPF determines the paths through the network, and MPLS sets up a label along each path. Refer to 9.2 Release Notes for supported features.

For additional information, refer to *Chapter 19, Configuration General, MPLS on BPX Switch*; for configuring CoS operation*, refer to Chapter 21, MPLS CoS with BPX 8650, Configuration*; and for information on MPLS VPNs, refer to *Chapter 22, MPLS VPNS with BPX 8650, Configuration*.

In addition, some basic procedures are provided for initial configuration of a router and its various interfaces, including ATM and Ethernet interfaces.

For further information regarding the Cisco 6400, 7200, or 7500 series, detailed software configuration information is provided in the Cisco IOS configuration guide and Cisco IOS command reference publications, which are available on the Cisco Documentation CD-ROM.

The chapter contains the following sections:

- Introduction
- MPLS/Tag Terminology
- Equipment and Software Requirements
- Configuration Preview
- Initial Setup of MPLS Switching
- Testing the MPLS Network Configuration
- Adding to the MPLS Network
- Network Management
- Basic Router Configuration
- Accessing the Router Command-Line Interface
- Booting the Router the First Time
- Configuring the Router for the First Time
- Using the System Configuration Dialog
- Configuring Port Adapter Interfaces
- Other Router Interfaces
- Checking the Configuration
- Using Configuration Mode
- Cisco IOS Software Basics

Introduction

Networks using MPLS, transport IP packets over ATM using label switching, thereby realizing the flexibility and scalability of TCP/IP along with the switching speed and reliability of ATM.

Note The current version of Cisco MPLS software uses an early version of LDP called the Tag Distribution Protocol (TDP). TDP and LDP are virtually identical in function, but use incompatible message formats. Once the MPLS standard is complete, Cisco will provide standard LDP in its MPLS implementation.

Configuring the MPLS network consists of setting up ATM router/switches for MPLS. This requires configuring the MPLS controller function on the router entity and the controlled (slave) function on the switch entity of each node.

In the example given here for BPX MPLS nodes (BPX 8650 ATM-LSRs), each MPLS node comprises an Cisco 6400 or a 7200 or 7500 router and a BPX switch shelf, where an Cisco 6400 or a 7200 or 7500 router provides the controlling function to the BPX switch shelf.

When MPLS is running in the network, the routing protocol, such as, OSPF, determines the paths through the MLPS switch network from every edge label switch router (LSR) to every IP destination. Based on this routing information, MPLS then automatically sets up a Label VC (LVC) along each path. This is done using the Label Distribution Protocol (LDP).

Consider packets arriving at the edge of the MPLS network with a particular destination IP address. The packets with that IP address will have labels applied at the edge LSR and the resulting ATM cells will be forwarded along the appropriate LVC path through the network using label swapping at each label switch until the far end edge LSR is reached. The far end edge LSR will remove the label, rebuild the frame, and forward the IP packet onto its LAN destination.

MPLS/Tag Terminology

The following lists the change of terminology to reflect the change from “label” to “mpls” terms.

Old Designation	New Designation
Tag Switching	MPLS, Multiprotocol Label Switching
Tag (short for Tag Switching)	MPLS
Tag (item or packet)	Label
TDP (Tag Distribution Protocol)	LDP (Label Distribution Protocol) **Note** Cisco TDP: and LDP (MPLS Label Distribution Protocol)) are nearly identical in function, but use incompatible message formats and some different procedures. Cisco will be changing from TDP to a fully compliant LDP.
Tag Switched	Label Switched
TFIB (Tag Forwarding Information Base)	LFIB (Label Forwarding Information Base)
TSR (Tag Switching Router)	LSR (Label Switching Router)
TSC (Tag Switch Controller)	LSC (Label Switch Controller
ATM-TSR	ATM-LSR (ATM Label Switch Router, such as, BPX 8650)
TVC (Tag VC, Tag Virtual Circuit)	LVC (Label VC, Label Virtual Circuit)
TSP (Tag Switch Protocol)	LSP (Label Switch Protocol)
TCR (Tag Core Router)	LSR (Label Switching Router)
XTag ATM (extended Tag ATM port)	XmplsATM (extended mpls ATM port)

Equipment and Software Requirements

BPX:

- BPX 8650

  BCC-3-64, BCC-4-64, BCC-4-128

BXM FW

- --

LSC Router:

- 7200 Series Router with NPE-150, NPE-200, or 7200VXR processor
- 7500 Series Router with RSP-2 or RSP-4 processor
- Cisco 6400
- 32 MB minimum, 64 MB recommended memory

IOS:

- 12.0T(5) or later, IP only release recommended

SWSW:

- 9.2.10 or later

Configuration Preview

Setting up label switching on a node involves is essentially a three-step process:

1. Configuring BPX switch
   (a) BPX switch (label switch slaves) configuration
   (b) Router (label switch controller) configuration of router extended ATM interfaces on the BPX for tag switching
2. Setting up edge routers (can include setting up policies, etc.)
3. MPLS automatically sets up LVCs across the network.

Figure 20-1 shows an example of a simplified MPLS network. The packets destined for 204.129.33.127 could be real time video, while the packets destined for 204.133.44.129 could be data files which can be transmitted when network bandwidth is available.

Once MPLS has been set up on the nodes shown in Figure 20-1, (ATM-LSR 1 thru ATM-LSR 5, Edge LSR_A, Edge LSR_B, and Edge LSR_C), automatic network discovery is thereby enabled. Then MPLS will automatically set up LVCs across the network. At each ATM LSR (label switch), label swapping is used to transport the cells across the previously set up LVC paths.

Note Label swapping is a name for VCI switching, the underlying capability of an ATM switch.

At the edge LSRs, labels are added to incoming IP packets, and labels are removed from outgoing packets. Figure 20-1 shows IP packets with host destination 204.129.33.127 being transported as labeled ATM cells across LVC 1, and IP packets with host destination 204.133.44.129 being transported as labeled ATM cells across LVC 2.

Note IP addresses shown are for example purposes only, and are assumed to be isolated from external networks. Check with your Network Administrator for appropriate IP addresses for your network.

Figure 20-1 High-Level View of Configuration of an MPLS Network

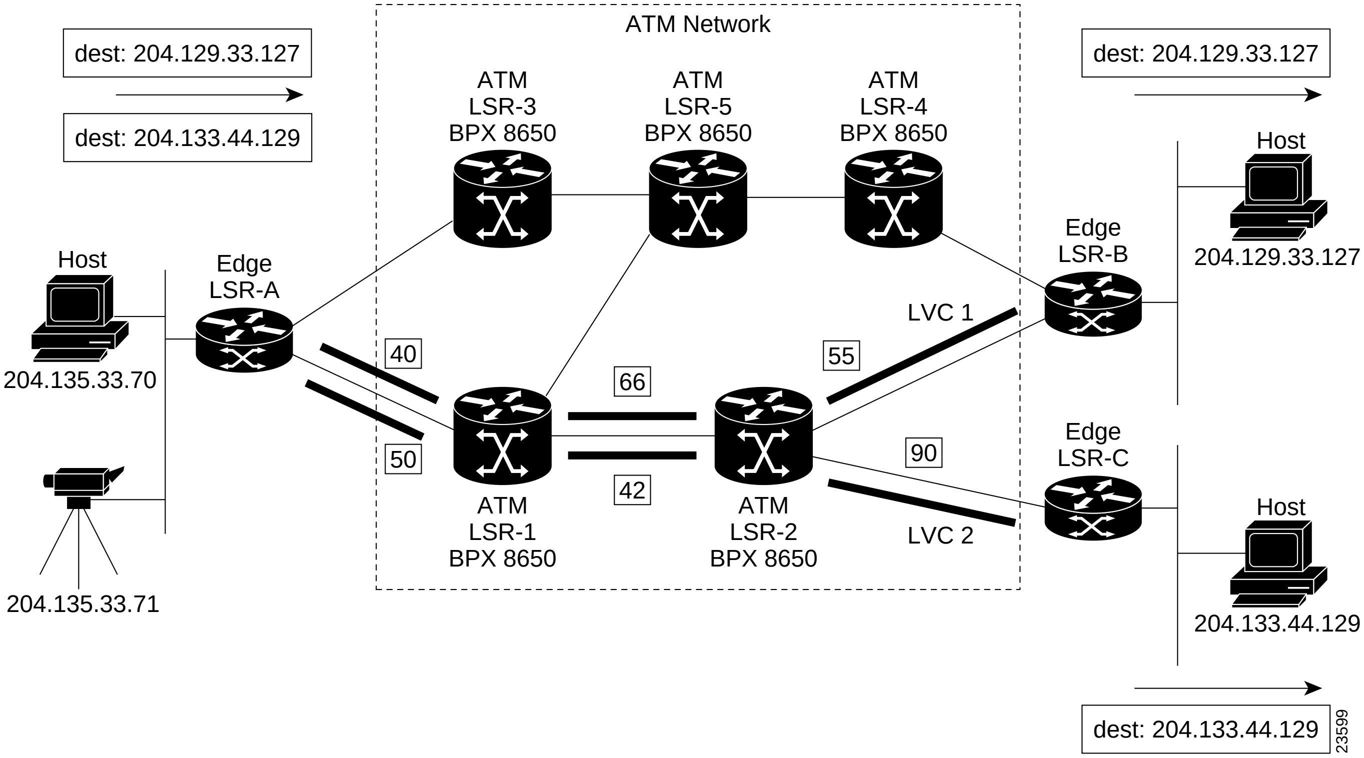
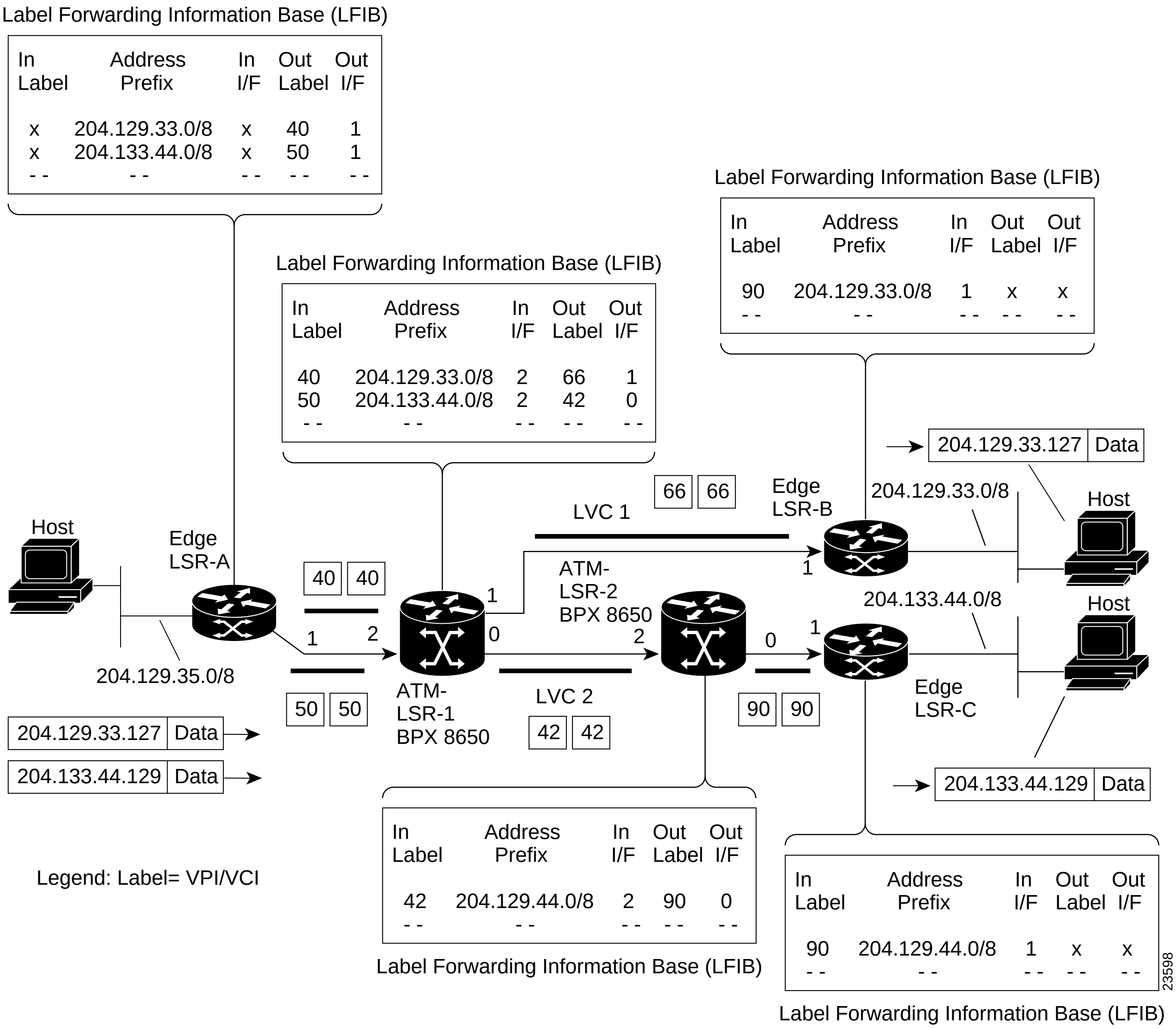


Figure 20-2 is a simplified diagram showing the MPLS label swapping that might take place in the transportation of the IP packets in the form of ATM cells across the network on the LVC1 and LVC2 virtual circuits.

For example, an unlabeled IP packet with destination 204.133.44.129 arrives at edge label switching router (LSR-A). Edge LSR-A checks its label forwarding information base (LFIB) and matches the destination with prefix 204.133.44.0/8. LSR-A converts the AAL5 frame to cells and sends the frame out as a sequence of cells on 1/VCI 50. ATM-LSR-1, which is a BPX 8650 label switch router (LSR) controlled by a routing engine (7200 or 7500 router), performs a normal switching operation by checking its LFIB and switching incoming cells on interface 2/VCI 50 to outgoing interface 0/VCI 42.

Continuing on, ATM-LSR-2 checks its LFIB and switches incoming cells on interface 2/VCI 42 to outgoing interface 0/VCI 90. Finally, Edge LSR-C receives the incoming cells on incoming interface 1/VCI 90, checks its LFIB, converts the ATM cells back to an AAL5 frame, then to an IP packet, and then sends the outgoing packet onto its LAN destination 204.133.44.129.

Figure 20-2 Label Swapping Detail



Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
x	204.129.33.0/8	x	40	1
x	204.133.44.0/8	x	50	1
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
40	204.129.33.0/8	2	66	1
50	204.133.44.0/8	2	42	0
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
90	204.129.33.0/8	1	x	x
- -	- -	- -	- -	- -

In Label	Address Prefix	In I/F	Out Label	Out I/F
42	204.129.44.0/8	2	90	0
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

In Label	Address Prefix	In I/F	Out Label	Out I/F
90	204.129.44.0/8	1	x	x
- -	- -	- -	- -	- -

Label Forwarding Information Base (LFIB)

Initial Setup of MPLS Switching

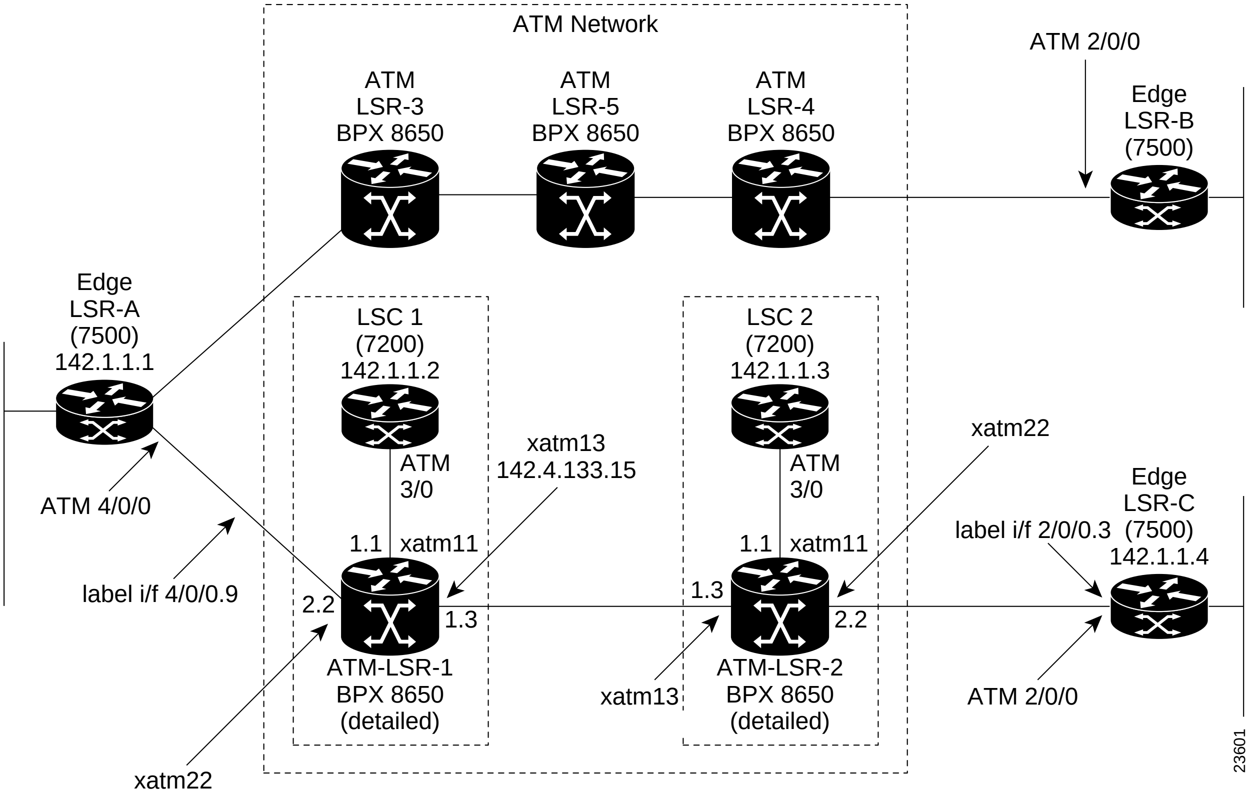
The following provides an example of configuring BPX 8650 MPLS label switches (ATM-LSRs) for MPLS switching of IP packets through an ATM network, along with configuration for 7200/7500 routers for use as Label edge routers (Edge LSRs) at the edges of the network.

See Figure 20-3 for a simplified example of the network. The following configuration example describes the configuration of Edge LSR-A (7500 router), Edge LSR-C (7500 router), ATM LSR-1 (BPX 8650 switch and controller), and ATM LSR-2 (BPX 8650 switch and controller) shown in

Figure 20-3. The configuration of ATM LSR-3, ATM LSR-4, and ATM LSR-5, is not detailed, but would be performed in a similar manner to that for ATM LSR-1 and ATM LSR-2. Also, the configuration of Edge LSR-B (7500 router) would be similar to that for Edge LSR-A and LSR-C.

The configuration of a BPX 8650 ATM-LSR, consists of two parts, configuring the BPX switch and configuring the associated label switch controller (Cisco 6400 or 7200 or 7500 router).

Figure 20-3 Simplified Example of Configuring an MPLS network.



Configuration for BPX switch portions of the BPX 8650 ATM-LSRs

The BPX nodes need to be set up and configured in the ATM network, including links to other nodes, etc. Following this, they may be configured for MPLS Operation. In configuring the BPX nodes for operation, a virtual interface and associated partition is set up with the **cnfrsrc** command. The 7200 or 7500 router is linked to the BPX with the **addshelf** command to allow the router's label switch controller function to control the MPLS operation of a node. The resources of the partition may be distributed between the associated ports. These are items such as bandwidth, vpi range, and number of logical connection spaces (LCNs). The VPIs are of local significance, so they do not have to be the same for each port in a node, but it is generally convenient from a tracking standpoint to keep them the same for a given BPX node. In this example, it is assumed that a single external controller per node is supported, so that the partition chosen is always 1.

Note With the appropriate release of switch software, firmware, and IOS, Service Class Templates are supported.

Proceed as follows to configure the BPX 8650 label switch routers, ATM-LSR-1 and ATM-LSR-2:

Command Syntax Summary for BPX Portion of MPLS Configuration

This chapter provides an example for configuring the BPX 8650 for basic MPLS operation. For additional detail about configuring MPLS on the BPX: for general information, refer to *Chapter 19, Configuration General, MPLS on BPX Switch*; for configuring CoS operation*, refer to Chapter 21, MPLS CoS with BPX 8650, Configuration*; and for information on MPLS VPNs, refer to *Chapter 22, MPLS VPNS with BPX 8650, Configuration*.

Syntax for associated commands, **cnfrsrc, cnfqbin, addshelf** are as follows:

cnfrsrc slot.port.{virtual trk} maxpvclcns maxpvcbw [Edit parms ? y/n] partitionID e/d minvsilcns maxvsilcns vsistartvpi vsiendvpi vsiminbw vsimaxbw {if you enter "y", to Edit parms?

cnfrsrc slot.port.{virtual trk} maxpvclcns maxpvcbw [Edit parms ? y/n] {accepts defaults if you enter "n" to Edit parms

cnfqbin <slot.port> <Qbin_#> <e/d> y/n <Qbin discard_thr> <Low EPD threshold> <CLPhi> <EFCI_thr> {If you enter "n" to not accept template values

cnfqbin <slot.port.[virtual trk}> <Qbin_#> <e/d> y/n {If you enter "y" to accept template values.

addshelf <slot.port [virtual trk]> <device-type> <control ID> <control partition ID>

Configuration for BPX 1 Portion of ATM-LSR-1

Proceed with configuration as follows:.

Step	Command	Description
Step 1	Check card status: **dspcds**	Display status of all cards, BXM cards that you are configuring should be "Standby" or "Active". If not perform a hard reset, "resetcd 1 h", resets card 1, for example.
Step 2	Check card connection capabilities: **dspcd 1** Chnls:16320, PG[1} :7048, PG[2] : 7048 PG [1} : 1, 2 PG [2] : 3, 4 **dspcd 2** Chnls:16320, PG[1} :7048, PG[2] : 7048 PG [1} : 1, 2 PG [2] : 3, 4	This example shows that ports 1 and 2 together have a total of 7048 connections or "channels" available for use Ports 1 and 2 form a port group (PG). Similarly, ports 3 and 4 are a port group with a limit of 7048 connections. Unless there is a good reason to do otherwise, it is best to leave many of the LCNs as spares. In this example, we will allocate 1500 LCNs to MPLS on each port using the **cnfrsrc** command. More detailed calculations for LCNs are described in *Chapter 19, Configuration General, MPLS on BPX Switch*.

continued:

Step	Command	Description
Step 3	Enable BXM interfaces: **uptrk 1.1** **uptrk 1.3** **uptrk 2.2**	In this example, trunk 1.1 is the link to the LSC controller, and trunks 1.3 and 2.2 are being set up as cross-connects for use by LVCs. **Note** A BXM interface is a “trunk” if it connects to another switch or MGX 8220 feeder. The VSI connection to an LSC is also a “trunk”. Other interfaces are ports, typically to service interfaces. **Note** **`uptrk`** and related commands are of form **`uptrk <slot.port. [<virtual trk}>`**, so if a virtual trunk is being configured (available in Release 9.2), the **`uptrk`** command for example, would be of the form, **`uptrk 1.1.1, uptrk 1.1.2,`** etc. Also, starting with Release 9.2, either ports or trunks can be active simultaneously on the same BXM.
Step 4	Configure VSI partitions on the BXM interfaces: **cnfrsrc 1.1 256 26000 y 1 e 512 1500 240 255 26000 105000** or if entered individually: **cnfrsrc 1.1** **256** {PVC LCNs, accept default value **26000** **y** {to edit VSI parameters **1** {partition **e** {enable partition **512** {VSI min LCNs **1500** {VSI max LCNs **240** {VSI starting VPI **255** {VSI ending VPI **26000** {VSI min bandwidth **105000** {VSI max bandwidth Repeat for BXM interfaces 1.3 and 2.2 **cnfrsrc 1.3 256 26000 y 1 e 512 1500 240 255 26000 105000** **cnfrsrc 2.2 256 26000 y 1 e 512 1500 240 255 26000 105000**	**Note** PVC LCNs: [256] default value. Reserves space on this link for 256 AutoRoute PVCs (LCNs = Logical Connection Numbers). One VSI partition is supported and it must be numbered “1”. VSI min LCNs: 512 and VSI max LCNs: 1500. Guarantees that MPLS can set up 512 LVCs on this link, but is allowed to use up to 1500, subject to availability of LCNs. VSI starting VPI: 240 and VSI ending VPI: 255. Reserves VPIs in the range of 240-255 for MPLS. Only one VP is really required, but a few more can be reserved to save for future use. AutoRoute uses a VPI range starting at 0, so MPLS should use higher values. It is best to always avoid using VPIs “0” and “1” for MPLS on the BPX 8650. **Note** VPIs are locally significant. In this example 240 is shown as the starting VPI for each port. A different value could be used for each of the three ports shown, 1.1, 1.3, and 2.2. However, at each end of a trunk, such as, between port 1.3 on ATM-LSR-1 and port 1.3 on ATM-LSR-2, the same VPI must be assigned. VSI min bandwidth: 26000 and VSI maximum 105000. Guarantees that MPLS can use 26000 cells/second (about 10 Mbps) on this link, but allows it to use up to 105000 cells/sec (about 40 Mbps) if bandwidth is available. More can be allocated if required. VSI maximum bandwidth: 26000. Guarantees that PVCs can always use up to 26000 cells per second (about 10 Mbps) on this link.

continued:

Step	Command	Description

Step 5	Enable MPLS queues on BXM:
	dsqbin 1.1 10
	and verify that it matches the following:
	`Qbin Database 1.1 on BXM qbin 10`
	`Qbin State: Enable`
	`Qbin discard threshold: 65536`
	`EPD threshold: 95%`
	`High CLP threshold: 100%`
	`EFCI threshold: 40%`
	If configuration is not correct, enter
	cnfqbin 1.1 10 e n 65536 95 100 40
	Repeat as necessary for BXM interfaces 1.3 and 2.2:
	cnfqbin 1.3 10 e n 65536 95 100 40
	cnfqbin 2.2 10 e n 65536 95 100 40
		MPLS CoS uses qbins 10-14

Step 6	Enable the VSI control interface: **addshelf 1.1 vsi 1 1** {link to controller, ID = 1, partition = 1	The first “1” after “vsi” is the vsi controller ID, which must be set the same on both the BPX 8650 and the LSC. The default controller ID on the LSC is “1”. The second “1” after “vsi” indicates that this is a controller for partition 1.

Configuration for BPX 2 portion of ATM-LSR-2

Proceed with configuration as follows:.

Step	Command	Description
Step 1	Check card status**:** **dspcds**	Display status of all cards, BXM cards that you are configuring should be “Standby” or “Active”. If not perform a hard reset, “resetcd 1 h”, resets card 1, for example.
Step 2	Check card connection capabilities: **dspcd 1** Chnls:16320, PG[1} :7048, PG[2] : 7048 PG [1} : 1, 2 PG [2] : 3, 4 **dspcd 2** Chnls:16320, PG[1} :7048, PG[2] : 7048 PG [1} : 1, 2 PG [2] : 3, 4	This example shows that ports 1 and 2 together have a total of 7048 connections or “channels” available for use Ports 1 and 2 form a port group (PG). Similarly, ports 3 and 4 are a port group with a limit of 7048 connections. Unless there is a good reason to do otherwise, it is best to leave many of the LCNs as spares. In this example, we will allocate 1500 LCNs to MPLS on each port using the **cnfrsrc** command. More detailed calculations for LCNs are described in *Chapter 19, Configuration General, MPLS on BPX Switch*.

continued:

Step	Command	Description
Step 3	Enable BXM interfaces: **uptrk 1.1** **uptrk 1.3** **uptrk 2.2**	In this example, trunk 1.1 is the link to the LSC controller, and trunks 1.3 and 2.2 are being set up as cross-connects for use by LVCs.
Step 4	Configure VSI partitions on the BXM interfaces: **cnfrsrc 1.1 256 26000 y 1 e 512 1500 240 255 26000 105000** or if entered individually: **cnfrsrc 1.1** **256** {PVC LCNs, accept default value **26000** **y** {to edit VSI parameters **1** {partition **e** {enable partition **512** {VSI min LCNs **1500** {VSI max LCNs **240** {VSI starting VPI **255** {VSI ending VPI **26000** {VSI min bandwidth **105000** {VSI max bandwidth Repeat for BXM interfaces 1.3 and 2.2 **cnfrsrc 1.3 256 26000 y 1 e 512 1500 240 255 26000 105000** **cnfrsrc 2.2 256 26000 y 1 e 512 1500 240 255 26000 105000**	

Step 5	Enable MPLS queues on BXM:
	dspqbin 1.1 10
	and verify that it matches the following:
	`Qbin Database 1.1 on BXM qbin 10`
	`Qbin State: Enable`
	`Qbin discard threshold: 65536`
	`EPD threshold: 95%`
	`High CLP threshold: 100%`
	`EFCI threshold: 40%`
	If configuration is not correct, enter
	cnfqbin 1.1 10 e n 65536 95 100 40
	Repeat as necessary for BXM interfaces 1.3 and 2.2:
	cnfqbin 1.3 10 e n 65536 95 100 40
	cnfqbin 2.2 10 e n 65536 95 100 40
		MPLS CoS uses qbins 10-14

Step 6	Enable the VSI control interface: **addshelf 1.1 vsi 1 1** {link to controller, ID = 1, partition = 1	The first “1” after “vsi” is the vsi controller ID, which must be set the same on both the BPX 8650 and the LSC. The default controller ID on the LSC is “1”. The second “1” after “vsi” is the partition ID that indicates this is a controller for partition 1.

Configuration for LSC 1 and LSC 2 portions of the BPX 8650

Before configuring the routers for the label switch (MPLS) controlling function, it is necessary to perform the initial router configuration if this has not been done.

As part of this configuration, it is necessary to enable and configure the ATM Adapter interface as described in “Configuring ATM Interfaces” section on page 20-28.

Then the extended ATM interface can be set up for Label Switching, and the BPX ports configured by the router as extended ATM ports of the router physical ATM interface according to the following procedures for LSC1 and LSC2.

Configuration for LSC1 portion of ATM-LSR-1

Step	Command	Description
	Preliminary	
1	Router LSC1(config)# ip routing	{enable IP routing protocol.
2	Router LSC1(config)# ip cef switch	{enable cisco express forwarding protocol.
3	Router LSC1(config)# interface ATM3/0	{enable physical interface link to BPX.
4	Router LSC1(config-if)# no ip address	
5	Router LSC1(config-if)# tag-control-protocol vsi [controller ID}	{enable router ATM port ATM3/0 as tag switching controller. Controller ID default is 1, optional values up to 32 for BPX.
	Setting up interslave control link	
6	Router LSC1(config-if)# interface XtagATM13	{interslave link on 1.3 port of BPX (port 3 os BXM in slot 1). This is an extended port of the router ATM3/0 port.
7	Router LSC1(config-if)# extended-port ATM3/0 bpx 1.3	{binding extended port xtagATM13 to bpx slave port 1.3.
8	Router LSC1(config-if)# ip address 142.4.133.13 255.255.0.0	{assigning ip address to xtagATM13.
9	Router LSC1(config-if)# tag-switching ip	{enable MPLS for xtag interface xtagATM13.
	Setting up interslave port	
10	Router LSC1(config-if)# interface XtagATM22	{interslave link on 2.2 port of BPX (port 2 os BXM in slot 2). This is an extended port of the router ATM3/0 port.
11	Router LSC1(config-if)# extended-port ATM3/0 bpx 2.2	{binding extended port xtagATM22 to bpx slave port 2.2
12	Router LSC1(config-if)# ip address 142.6.133.22 255.255.0.0	{assigning ip address to xtagATM22.
13	Router LSC1(config-if)# tag-switching ip	{enable MPLS for xtag interface xtagATM22.
14	Router LSC1 (config-if)# exit	
	Configuring routing protocol	{Configuring Open Shortest Path FIrst (OSPF) routing protocol or Enhanced Interior Gateway Routing Protocol (EIGRP).
15	Router LSC1 (config-if)# Router OSPF 5	{Setting up OSPF routing and assigning a process ID of 5 which is locally significant. The ID may be chosen from a wide range of available process ID up to approximately 32,000.
16	Router LSC1 (config-router)# network 142.4.0.0 0.0.255.255 area 10	
17	Router LSC1 (config-router)# network 142.6.0.0 0.0.255.255 area 10	

Configuration for LSC2 portion of ATM-LSR-2

Step	Command	Description
	Preliminary	
1	Router LSC2(config)# ip routing	{enable IP routing protocol.
2	Router LSC2(config)# ip cef switch	{enable cisco express forwarding protocol.
3	Router LSC2(config)# interface ATM3/0	{enable physical interface link to BPX.
4	Router LSC2(config-if)# no ip address	
5	Router LSC2(config-if)# tag-control-protocol vsi [controller ID]	{enable router ATM port ATM3/0 as tag switching controller. Controller ID default is 1, optional values up to 32 for BPX.
	Setting up interslave control link	
6	Router LSC2(config-if)# interface XtagATM13	{interslave link on 1.3 port of BPX (port 3 os BXM in slot 1). This is an extended port of the router ATM3/0 port.
7	Router LSC2(config-if)# extended-port ATM3/0 bpx 1.3	{binding extended port xtagATM13 to bpx slave port 1.3.
8	Router LSC2(config-if)# ip address 142.4.133.15 255.255.0.0	{assigning ip address to xtagATM1.
9	Router LSC2(config-if)# tag-switching ip	{enable MPLS for xtag interface xtagATM1.
	Setting up interslave port	
10	Router LSC2(config-if)# interface XtagATM22	{interslave link on 2.2 port of BPX (port 2 os BXM in slot 2). This is an extended port of the router ATM3/0 port.
11	Router LSC2(config-if)# extended-port ATM3/0 bpx 2.2	{binding extended port xtagATM22 to bpx slave port 2.
12	Router LSC2(config-if)# ip address 142.7.133.22 255.255.0.0	{assigning ip address to xtagATM22.
13	Router LSC2(config-if)# tag-switching ip	{enable MPLS for xtag interface xtagATM22.
14	Router LSC2 (config-if)# exit	
	Configuring routing protocol	{Configuring Open Shortest Path FIrst (OSPF) routing protocol or Enhanced Interior Gateway Routing Protocol (EIGRP).
15	Router LSC2 (config-if)# Router OSPF 5	{Setting up OSPF routing and assigning a process ID of 5 which is locally significant. The ID may be chosen from a wide range of available process ID up to approximately 32,000.
16	Router LSC2 (config-router)# network 142.4.0.0 0.0.255.255 area 10	
17	Router LSC2 (config-router)# network 142.7.0.0 0.0.255.255 area 10	

Configuration for Edge Label Switch Routers, LSR-A and LSR-B

Before configuring the routers for the label switch (MPLS) controlling function, it is necessary to perform the initial router configuration if this has not been done.

As part of this configuration, it is necessary to enable and configure the ATM Adapter interface as described in “Configuring ATM Interfaces” section on page 20-28.

Then the extended ATM interface can be set up for Label Switching, and the BPX ports configured by the router as extended ATM ports of the router physical ATM interface according to the following procedures for LSR-A and LSR-C. Configuration of the 7500 routers performing as label edge routers is provided in the following:

Configuration of Cisco 7500 as an Edge Router, Edge LSR-A

Step	Command	Description
1	Router LSR-A (config)# ip routing	{enable IP routing protocol.
2	Router LSR-A(config)# ip cef distributed switch	{enable label switching for ATM subinterface.
3	Router LSR-A(config)# interface ATM4/0/0	
4	Router LSR-A(config-if)# no ip address	
5	Router LSR-A(config-if)# interface ATM4/0/0.9 tag-switching	[interface can be basically any number within range limits ATM4/0/0.1, ATM 4/0/0.2, etc.
6	Router LSR-A(config-if)# ip address 142.6.133.142 255.255.0.0	
7	Router LSR-A(config-if)# tag-switching ip	
	Configuring routing protocol	{Configuring Open Shortest Path FIrst (OSPF) routing protocol or Enhanced Interior Gateway Routing Protocol (EIGRP).
8	Router LSR-A (config-if)# Router OSPF 5	{Setting up OSPF routing and assigning a process ID of 5 which is locally significant. The ID may be chosen from a wide range of available process IDs up to approximately 32,000.
9	Router LSR-A (config-router)# network 142.6.0.0 0.0.255.255 area 10	

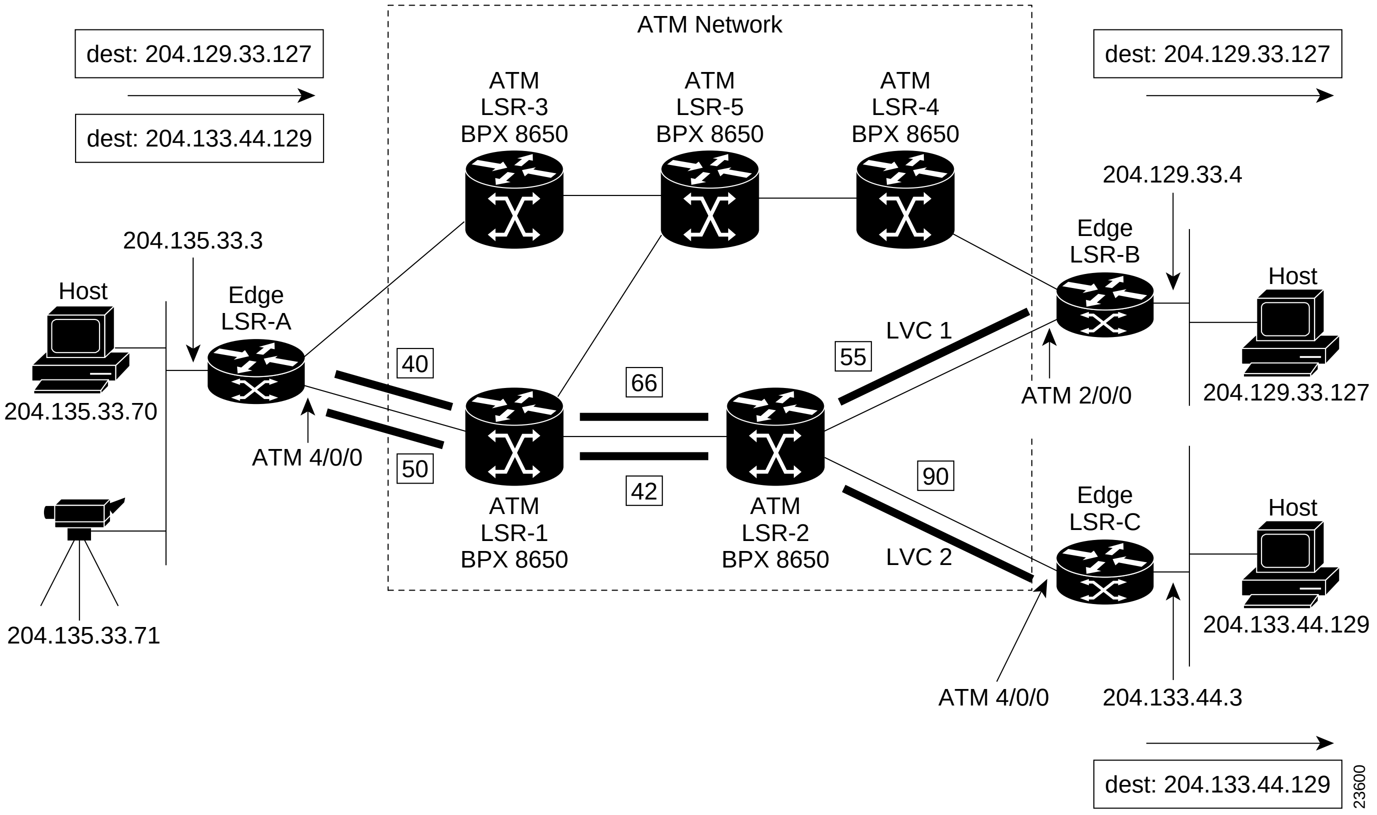
Configuration of Cisco 7500 as an Edge Router, Edge LSR-C

Step	Command	Description
1	Router LSR-C (config)# ip routing	{enable IP routing protocol.
2	Router LSR-C(config)# ip cef distributed switch	{enable label switching for ATM subinterface.
3	Router LSR-C(config)# interface ATM2/0/0	
4	Router LSR-C(config-if)# no ip address	
5	Router LSR-C(config-if)# interface ATM2/0/0.3 tag-switching	
6	Router LSR-C(config-if)# ip address 142.7.133.23 255.255.0.0	
7	Router LSR-C(config-if)# tag-switching ip	
	Configuring routing protocol	{Configuring Open Shortest Path FIrst (OSPF) routing protocol or Enhanced Interior Gateway Routing Protocol (EIGRP).
8	Router LSR-C (config-if)# Router OSPF 5	{Setting up OSPF routing and assigning a process ID of 5 which is locally significant. The ID may be chosen from a wide range of available process IDs up to approximately 32,000.
9	Router LSR-C (config-router)# network 142.7.0.0 0.0.255.255 area 10	

Routing Protocol Configures LVCs via MPLS

After the initial configuration procedures for the BPX 8650 and Edge Routers has been performed as described in the previous paragraphs, the routing protocol, such as, OSPF, sets up the LVCs via MPLS as shown in Figure 20-4.

Figure 20-4 Example of LVCs in an MPLS Switched Network



Testing the MPLS Network Configuration

Preliminary testing of the MPLS network starts with checking VSI status, the MPLS interfaces, and MPLS discovery process.

Useful LSC Commands

The following are some of the useful LSC (also referred to as TSC) commands for monitoring and troubleshooting an MPLS network:

show controllers VSI descriptor [descriptor]

show tag int

show tag tdp disc

For a complete description of these LSC commands refer to the related IOS MPLS documentation. For Release 9.1, these are Cisco IOS 11.1 CT documents:

- Tag Switching on Cisco 7000 Family
- Tag Switch Controller

Checking the BPX Extended ATM Interfaces

Use the following procedure as a quick checkout of the tag switching configuration and operation with respect to the BPX switch, for example ATM-LSR-1.

Step 1 Wait a while, and check whether the controller sees the interfaces correctly; on LSC1, for example, enter the following command:

Command	Description
Router LSC1# show controllers VSI ATM3/0	shows VSI information for extended ATM interfaces.

The example output for ATM-LSC-1 (BPX 8650 shelf) is:

Note Check the LSC on-line documentation for the most current information.

```
Phys desc:   1.1
Log intf:    0x00040100 (0.4.1.0)
Interface:   slave control port
IF status:   n/a                    IFC state: ACTIVE
Min VPI:     0                      Maximum cell rate:  10000
Max VPI:     10                     Available channels: xxx
Min VCI:     0                      Available cell rate (forward):  xxxxxx
Max VCI:     65535                  Available cell rate (backward): xxxxxx
```

```
   Phys desc:   1.3
   Log intf:    0x00040200 (0.4.2.0)
   Interface:   ExtTagATM13
   IF status:   up                     IFC state: ACTIVE
   Min VPI:     0                      Maximum cell rate:  10000
   Max VPI:     10                     Available channels: xxx
   Min VCI:     0                      Available cell rate (forward):  xxxxxx
   Max VCI:     65535                  Available cell rate (backward): xxxxxx


   Phys desc:   2.2
   Log intf:    0x00040300 (0.4.3.0)
   Interface:   ExtTagATM22
   IF status:   up                     IFC state: ACTIVE
   Min VPI:     0                      Maximum cell rate:  10000
   Max VPI:     10                     Available channels: xxx
   Min VCI:     0                      Available cell rate (forward):  xxxxxx
   Max VCI:     65535                  Available cell rate (backward): xxxxxx
-------
```

Step 2 If there are no interfaces present, first check that card 1 is up,

with, on the BPX switch:

dspcds

and, if the card is not up, in this example BXM in slot 1 of the BPX shelf:

resetcd 1 h

and/or remove the card to get it to reset if necessary.

Note This example assumes that the controller is connected to card 1 on the switch. Substitute a different card number, as applicable.

Step 3 Check the trunk status with the following command:

dsptrks

The **dsptrks** screen for ATM-LSR-1 should show the 1.1, 1.3 and 2.2 MPLS interfaces, with the “Other End” of 1.1 reading “VSI (VSI)”. A typical **dsptrks** screen example follows:

Sample Display

```
n4             TN    SuperUser       BPX 15    9.2      Dec. 4 1998  16:45 PST

TRK     Type     Current Line Alarm Status               Other End
 2.1    OC3      Clear - OK                              j4a/2.1
 3.1    E3       Clear - OK                              j6c(AXIS)
 5.1    E3       Clear - OK                              j6a/5.2
 5.2    E3       Clear - OK                              j3b/3
 5.3    E3       Clear - OK                              j5c(IPX/AF)
 6.1    T3       Clear - OK                              j4a/4.1
 6.2    T3       Clear - OK                              j3b/4
 1.1    OC3      Clear - OK                              VSI(VSI)
 1.3    OC3      Clear - OK
 2.2    OC3      Clear - OK



Last Command: dsptrks

Next Command:
```

Step 4 Enter the **dspnode** command.

dspnode

The resulting screens should show trunk 1.1 (link to LSC on ATM-LSR-1) as type VSI. A typical **dspnode** screen follows:

Example of **dspnode** screen.

```
n4             TN    SuperUser       BPX 15    9.2    Dec. 4 1998  16:46 PST

                        BPX Interface Shelf Information

Trunk    Name      Type      Alarm
 3.1     j6c       AXIS      MIN
 5.3     j5c       IPX/AF    MIN
 1.1     VSI       VSI       OK






Last Command: dspnode

Next Command:
```

Step 5 Enter the **dsprsrc** command as follows:

dsprsrc 1.1 1

The resulting screen should show the settings shown in the following example:

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Dec. 4 1998  16:47 PST

Port/Trunk : 1.1

Maximum PVC LCNS:             256     Maximum PVC Bandwidth:105000

Min Lcn(1) : 0 Min Lcn(2) : 0
Partition 1

Partition State :             Enabled
Minimum VSI LCNS:             512
Maximum VSI LCNS:             1500
Start VSI VPI:                240
End VSI VPI :                 255
Minimum VSI Bandwidth :       26000       Maximum VSI Bandwidth :        105000



Last Command: dsprsrc 1.1 1


Next Command:
```

Step 6 Enter the **dspqbin** command as follows:

dspqbin 1.1 10

The resulting screen should show the settings shown in the following example:

Sample Display:

```
n4             TN    SuperUser       BPX 15    9.2      Dec. 4 1998  16:48 PST

Qbin Database 1.1 on BXM qbin 10

Qbin State:                   Enabled

Minimum Bandwidth:             0
Qbin Discard threshold:       65536
Low CLP threshold:            95%
High CLP threshold:           100%
EFCI threshold:               40%






Last Command: dspqbin 1.1 10


Next Command:
```

Step 7 If interfaces 1.3 and 2.2 are present, but not enabled, perform the previous debugging steps for interfaces 1.3 and 2.2 instead of 1.1, except for the **dspnode** command which does not show anything useful pertaining to ports 1.3 and 2.2.

Step 8 Try a ping on the label switch connections. If the ping doesn't work, but all the label switching and routing configuration looks correct, check that the TSC has found the VSI interfaces correctly by entering the following command at the TSC:

Command	Description
Router LSC1# show tag int	shows the label interfaces.

If the interfaces are not shown, re-check the configuration of port 1.1 on the BPX switch as described in the previous steps.

Step 9 If the VSI interfaces are shown, but are down, check whether the LSRs connected to the BPX switch show that the lines are up. If not, check such items as cabling and connections.

Step 10 If the LSCs and BPX switches show the interfaces are up, but the LSC doesn't show this, enter the following command on the LSC:

```
Router LSC1# reload
```

If the "show tag int" command shows that the interfaces are up, but the ping doesn't work, enter the follow command at the LSC:

```
Router LSC1# tag tdp disc
```

The resulting display should show something similar to the following:

```
Local TDP Identifier:
    30.30.30.30:0
TDP Discovery Sources:
    Interfaces:
        ExtTagATM1.3:   xmit/recv
        ExtTagATM2.2:   xmit/recv
-----------------
```

Step 11 If the interfaces on the display show "xmit" and not "xmit/recv", then the LSC is sending LDP messages, but not getting responses. Enter the following command on the neighboring LSRs.

```
Router LSC1# tag tdp disc
```

If resulting displays also show "xmit" and not "xmit/recv", then one of two things is likely:

(a) The LSC is not able to set up VSI connections

(b) The LSC is able to set up VSI connections, but cells won't be transferred because they can't get into a queue

Step 12 Check the VSI configuration on the switch again, for interfaces 1.1, 1.3, and 2.2, paying particular attention to:

(a) maximum bandwidths at least a few thousands cells/sec

(b) qbins enabled

(c) all qbin thresholds non-zero

Note VSI partitioning and resources must be set up correctly on the interface connected to the TSC, interface 1.1 in this example, as well as interfaces connected to other tag switching devices.

Basic Router Configuration

The following paragraphs in this chapter provide basic configuration information for the Cisco 6400, or Cisco 7200 or 7500 routers used as the Label Switch Controller for the BPX 8650. The following topics are included:

- Accessing the Router Command-Line Interface
- Booting the Router for the First Time
- Configuring the Router for the First Time

Accessing the Router Command-Line Interface

To configure a router, you must access its command-line interface (CLI).

If you will be configuring the router on site, connect a console terminal (an ASCII terminal or a PC running terminal emulation software) to the console port on the router.

For remote access, connect a modem to the auxiliary port on the router.

Booting the Router for the First Time

Each time you turn on power to the router, it goes through the following boot sequence:

1. The router goes through power-on self-test diagnostics to verify basic operation of the CPU, memory, and interfaces.
2. The system bootstrap software (boot image) executes and searches for a valid Cisco IOS image The factory-default setting for the configuration register is 0x2102, which indicates that the router should attempt to load a Cisco IOS image from Flash memory.
3. If after five attempts a valid Cisco IOS image is not found in Flash memory, the Cisco router reverts to boot ROM mode (which is used to install or upgrade a Cisco IOS image).
4. If a valid Cisco IOS image is found, then the Cisco router searches for a valid configuration file.
5. If a valid configuration file is not found in NVRAM, the Cisco router runs the System Configuration Dialog so you can configure it manually. For normal router operation, there must be a valid Cisco IOS image in Flash memory and a configuration file in NVRAM.

The first time you boot the router, you need to configure the router interfaces and then save the configuration to a file in NVRAM. Proceed to the next section, “Configuring the Router for the First Time,” for configuration instructions.

Configuring the Router for the First Time

You can configure the Cisco router using one of the following procedures, which are described in this section:

1. Using the System Configuration Dialog—Recommended if you are not familiar with Cisco IOS commands.

2. Using Configuration Mode—Recommended if you are familiar with Cisco IOS commands.
3. Using Auto Install—Recommended for automatic installation if another router running Cisco IOS software is installed on the network. This configuration method must be set up by someone with experience using Cisco IOS software.

Timesaver Obtain the correct network addresses from your system administrator or consult your network plan to determine correct addresses before you begin to configure the router.

Use the procedure that best meets the needs of your network configuration and level of experience using Cisco IOS software. If you use configuration mode or Auto Install to configure the router and you would like a quick review of the Cisco IOS software, refer to the section "Cisco IOS Software Basics" later in this chapter. Otherwise, proceed to the next section, "Using the System Configuration Dialog."

Using the System Configuration Dialog

If your router does not have a configuration (setup) file and you are not using AutoInstall, the router will automatically start the setup command facility. An interactive dialog called the System Configuration Dialog appears on the console screen. This dialog helps you navigate through the configuration process by prompting you for the configuration information necessary for the Cisco router to operate.

Note Many prompts in the System Configuration Dialog include default answers, which are included in square brackets following the question. To accept a default answer, press **Return**; otherwise, enter your response.

This section gives an example configuration using the System Configuration Dialog. When you are configuring your router, respond as appropriate for your network.

At any time during the System Configuration Dialog, you can request help by entering a question mark (?) at a prompt.

Before proceeding with the System Configuration Dialog, obtain from your system administrator the node addresses and the number of bits in the subnet field (if applicable) of the Ethernet and synchronous serial ports.

Take the following steps to configure the router using the System Configuration Dialog:

Step 1 After connecting a console terminal or modem to the router and powering ON the router, wait about 30 seconds for messages to be displayed, corresponding to the Cisco IOS release and feature set you selected. The screen displays in this section are for reference only and might not exactly reflect the screen displays on your console. Following is an example of the messages displayed:

```
System Bootstrap, Version 11.1(13)CA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(24)CC, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)

cisco 7206 (NPE200) processor with 122880K/8192K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
6 slot midplane, Version 1.3

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-P-M), Version 12.0(5.0.2)T2,  MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Sun 11-Jul-99 08:26 by kpma
Image text-base: 0x60008900, data-base: 0x60D64000


4 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
125K bytes of non-volatile configuration memory.
4096K bytes of packet SRAM memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
107520K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x102

 --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]:
```

Step 2 Press **Return** or enter **yes** to begin the configuration process.

Step 3 When the System Configuration Dialog asks whether you want to view the current interface summary, press **Return** or enter **yes**:

```
First, would you like to see the current interface summary? yes

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Ethernet0              unassigned      NO  unset  up                    down
Serial0                unassigned      NO  unset  down                  down
TokenRing0             unassigned      NO  unset  reset                 down
ATM 0                  unassigned      NO  unset  reset                 down
```

Step 4 Configure the global parameters. A typical configuration follows:

```
Enter host name [7200router]: aries
```

Step 5 Next, you are prompted to enter an enable secret password. There are two types of privileged-level passwords:

- Enable secret password (a secure, encrypted password).
- Enable password (a less secure, nonencrypted password).

The enable password is used when the enable secret password does not exist. For maximum security, be sure the passwords are different. If you enter the same password for both, the Cisco router will accept your entry, but will display a warning message indicating that you should enter a different password.

Step 6 Enter an enable secret password:

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

Enter enable secret: orca

The enable password is used when there is no enable secret and when using older
software and some boot images.
```

Step 7 Enter the enable and virtual terminal passwords:

```
     Enter enable password: xxxx
     Enter virtual terminal password: yyyy
```

Step 8 Press **Return** to accept Simple Network Management Protocol management, or enter **no** to refuse it:

```
     Configure SNMP Network Management? [yes]: no
```

Step 9 In the following example, the Cisco router is configured for AppleTalk, IP, MPLS, and Internetwork Packet Exchange. Configure the appropriate protocols for your router:

```
Configure Vines? [no]:
Configure LAT? [no]:
Configure AppleTalk? [no]:
Multizone networks? [no]: yes
Configure DECnet? [no]:
Configure IP? [yes]:
Configure MPLS? [no]: yes
Configure IGRP routing? [yes]: no
Your IGRP autonomous system number [1]: 15
Configure CLNS? [no]:
Configure bridging? [no]:
Configure IPX? [no]:
Configure XNS? [no]:
Configure Apollo? [no]:
```

Note It is recommended that an MPLS network use either OSPF or IS-IS routing as its routing protocol. EIGRP will also work, but it does not support the useful MPLS feature referred to as Traffic Engineering. IGRP and RIP protocols are not recommended.

Configuring Port Adapter Interfaces

Once port adapter cable connections have been made, and basic configuration on the router is completed, the applicable port adapter interfaces on the router, Ethernet, Fast Ethernet, ATM, FDDI, etc., must be configured, followed by configuration of the router for MPLS operation, and addition of permanent virtual circuits (PVCs), as applicable.

Preparing to Configure Port Adapter Interfaces

If you want to configure interfaces in a new Cisco 7200 or 7500 Series router, or if you want to change the configuration of an existing interface, be prepared with the information you will need, such as the following:

- Protocols you plan to route on each new interface.
- Internet protocol (IP) addresses if you plan to configure the interfaces for IP routing.
- The types of interfaces that will be used.

The **configure** command requires privileged-level access to the EXEC command interpreter, which usually requires a password. Contact your system administrator if necessary to obtain EXEC-level access.

Identifying Chassis Slot, Port Adapter Slot, and Interface Port Numbers

The following section describes how to identify chassis slot, port adapter slot, and interface port numbers on the 7200 or 7500 Series routers for all port adapter interface types.

Cisco 7200 or 7500 Port Adapter Interface Ports

Physical port addresses specify the actual physical location of each interface port, regardless of the type.

You can also identify port adapter interface ports by physically checking the slot/interface port location on the 7200 or 7500 Series routers, or by using **show** commands to display information about a specific interface or all interfaces.

Configuring ATM Interfaces

This section provides the procedure for a basic interface configuration.

Press the **Return** key after each step unless otherwise noted. At any time you can exit the privileged level and return to the user level by entering **disable** at the prompt as follows:

```
Cisco 7200 Router# disable

Cisco 7200 Router>
```

Use the following procedure to perform a basic configuration:

Step 1 At the privileged-level prompt, enter configuration mode and specify that the console terminal will be the source of the configuration subcommands, as follows:

```
Cisco 7200 Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco 7200 Router (config)#
```

Step 2 At the prompt, enter the subcommand **interface** to specify the interface to be configured, then **atm** to specify port adapter type, then *slot/port* (port adapter slot number and interface port number). The example that follows is the 1/0 interface of the atm port adapter in a 7200 Series router:

```
Cisco 7200 Router (config)# interface switch atm 1/0
```

Step 3 If IP routing is enabled on the system, you can assign an IP address and subnet mask to the interface with the **ip address** configuration subcommand, as in the following example:

```
Cisco 7200 Router (config-if)# ip address 224.135.128.44 255.255.255.0
```

Step 4 Add any additional configuration subcommands required to enable routing protocols and set the interface characteristics.

Step 5 Change the shutdown state to up and enable the interface as follows:

```
Cisco 7200 Router (config-if)# no shutdown
```

Step 6 Repeat Step 2 through Step 5 to configure additional interfaces as required.

Step 7 When you have completed the configuration, press **Ctrl-Z** to exit configuration mode.

Step 8 Write the new configuration to nonvolatile memory as follows:

```
Cisco Router 7200# copy running-config startup-config
[OK]
Cisco Router 7200#
```

Note If you are going to unattach/reconfigure the ATM interface cable, use the **shutdown** command prior to this action. After re-attaching the ATM interface cable, use the **no shutdown** command to bring the ATM interface into an up state.

Other Router Interfaces

The router has other interfaces for carrying IP traffic. Refer to the Cisco 7200 or 7500 Series Router documentation, as applicable.

Checking the Configuration

After configuring the new interface, use the **show** commands to display the status of the new interface or all interfaces and the **ping** command to check connectivity.

Using Show Commands to Verify the New Interface Status

The following steps use **show** commands to verify that the new interfaces are configured and operating correctly.

Step 1 Use the **show version** command to display the system hardware configuration. Ensure that the list includes the new interfaces.

Step 2 Display all the current port adapters and their interfaces with the **show controllers** command. Verify that the new port adapter appears in the correct slot.

Step 3 Specify one of the new interfaces with the **show interfaces** *port adapter type slot/interface* command and verify that the first line of the display specifies the interface with the correct slot number. Also verify that the interface and line protocol are in the correct state: up or down.

Step 4 Display the protocols configured for the entire system and specific interfaces with the **show protocols** command. If necessary, return to configuration mode to add or remove protocol routing on the system or specific interfaces.

Step 5 Display the running configuration file with the **show running-config** command. Display the configuration stored in NVRAM using the **show startup-config** command. Verify that the configuration is accurate for the system and each interface.

If the interface is down and you configured it as up, or if the displays indicate that the hardware is not functioning properly, ensure that the network interface is properly connected and terminated. If you still have problems bringing the interface up, contact a service representative for assistance.

Using Show Commands to Display Interface Information

To display information about a specific interface, use the **show interfaces** command with the interface type and port address in the format **show interfaces** [*type slot/port*] for the Cisco router.

Note For complete command descriptions and examples for all of the supported platforms, refer to the publications listed in the first paragraph “About this Guide” at the beginning of this document.

Cisco Show Interfaces Command

Following is an example of how the **show interfaces** [*type slot/port*] command displays status information (including the physical slot and port address) for the interfaces you specify.(Interfaces are administratively shut down until you enable them.)

```
Cisco 7200 Router 3# sh int e 2/0
Ethernet2/0 is administratively down, line protocol is down
  Hardware is AmdP2 Ethernet, address is x.x.x.x (bia 0000.0ca5.2389)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
(display text omitted]
```

With the **show interfaces** *type slot/port* command, use arguments such as the interface type (ethernet, and so forth) slot, and the port number (slot/port) to display information about a specific Ethernet 10BASE-T interface only.

The **show version** (or **show hardware**) command displays the configuration of the system hardware (the number of each port adapter type installed), the software version, the names and sources of configuration files, and the boot images. Following is an example of the **show version** command:

```
7200 router 1>show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-P-M), Version 12.0(5.0.2)T2,  MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Sun 11-Jul-99 08:26 by kpma
Image text-base: 0x60008900, data-base: 0x60D64000

ROM: System Bootstrap, Version 11.1(13)CA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(24)CC, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)

7200 router 1 uptime is 2 weeks, 2 hours, 38 minutes


System returned to ROM by reload
System image file is "tftp://173.xx.xx.xx/c7200-p-mz.120-5.0.2.T2"

cisco 7206 (NPE200) processor with 122880K/8192K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
6 slot midplane, Version 1.3

Last reset from power-on
X.25 software, Version 3.0.0.
4 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
125K bytes of non-volatile configuration memory.
4096K bytes of packet SRAM memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
107520K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x102

7200 router 1>
```

To determine which typew of port adapter are installed in your system, use the **show diag** command. Specific port adapter information is displayed, as shown in the following example: o:

```
7200 router 1>show diag
Slot 0:
        Fast-ethernet on C7200 I/O card with MII or RJ45 port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 2w0d ago
        EEPROM contents at hardware discovery:
        Hardware revision 1.3           Board revision C0
        Serial number     12635836      Part number    73-2956-02
        Test history      0x0           RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 83 01 03 00 C0 CE BC 49 0B 8C 02 00 00 00 00
          0x30: 60 00 00 00 99 05 10 00 00 FF FF FF FF FF FF FF

Slot 3:
        Ethernet port adapter, 4 ports
        Port adapter is analyzed
        Port adapter insertion time 2w0d ago
        EEPROM contents at hardware discovery:
        Hardware revision 1.14          Board revision A0
        Serial number     12275103      Part number    73-1556-08
        Test history      0x0           RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 02 01 0E 00 BB 4D 9F 49 06 14 08 00 00 00 00
          0x30: 50 00 00 00 99 03 30 00 FF FF FF FF FF FF FF FF

Slot 6:
        ATM WAN DS3 port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 2w0d ago
        EEPROM contents at hardware discovery:
        Hardware revision 2.0           Board revision A0
        Serial number     14077539      Part number    73-2432-04
        Test history      0x0           RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 5B 02 00 00 D6 CE 63 49 09 80 04 00 00 00 00
          0x30: 50 00 00 00 99 04 26 00 FF FF FF FF FF FF FF FF

7200 router 1>
```

Proceed to the “Using the ping Command” section on page 20-32 to verify that each interface port is functioning properly.

Using the ping Command

The *packet internet groper* (**ping**) command allows you to verify that an interface port is functioning properly and to check the path between a specific port and connected devices at various locations on the network. This section provides brief descriptions of the **ping** command. After you verify that the system has booted successfully and is operational, you can use this command to verify the status of interface ports.

The **ping** command sends an echo request out to a remote device at an IP address that you specify. After sending a series of signals, the command waits a specified time for the remote device to echo the signals. Each returned signal is displayed as an exclamation point (!) on the console terminal;

each signal that is not returned before the specified time-out is displayed as a period (.). A series of exclamation points (!!!!!) indicates a good connection; a series of periods (.....) or the messages [timed out] or [failed] indicate that the connection failed.

Following is an example of a successful **ping** command to a remote server with the address 1.1.1.10:

```
Cisco 7200 Router # ping 1.1.1.10 <Return>
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 1.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/64 ms
Cisco 7200 Router #
```

If the connection fails, verify that you have the correct IP address for the server and that the server is active (powered on), and repeat the **ping** command.

Using Configuration Mode

You can configure the 7200 Router manually if you prefer not to use AutoInstall or the prompt-driven System Configuration Dialog.

Note Refer to the section “Cisco IOS Software Basics” later in this chapter for basic information about Cisco IOS software, getting context-sensitive help, and saving configuration changes.

Take the following steps to configure the Cisco 7200 router manually:

Step 1 Connect a console terminal.Then power ON the Cisco 7200 router.

Step 2 When you are prompted to enter the initial dialog, enter **no** to go into the normal operating mode of the Cisco 7200 router:

```
Would you like to enter the initial dialog? [yes]: no
```

Step 3 After a few seconds you will see the user EXEC prompt (Router>). By default, the host name is Router, but the prompt will match the current host name. In the following examples, the host name is **aries** Enter the **enable** command to enter enable mode. You can only make configuration changes in enable mode:

```
Router > enable
```

The prompt will change to the privileged EXEC (enable) prompt, **`7200 Router aries`**#.

Step 4 Enter the **configure terminal** command at the enable prompt to enter configuration mode:

```
Router# config terminal
```

You can now enter any changes you want to the configuration. You will probably want to perform the following tasks:

(a) Assign a host name for the Cisco 7200 router using the **hostname** command.

(b) Enter an enable secret password using the **enable password** command.

(c) Assign addresses to the interfaces using the *protocol* **address** command.

(d) Specify which protocols to support on the interfaces.

Refer to the Cisco IOS configuration guide and command reference publications for more information about the commands you can use to configure the 7200 or 7500 series routers.

Step 5 When you finish configuring the router, enter the **exit** command until you return to the privileged EXEC prompt (7200 router aries#).

Step 6 To save the configuration changes to NVRAM, enter the **copy running-config startup-config** command at the privileged EXEC prompt:

```
7200 router aries# copy running-config startup-config
********
```

The Cisco router is now configured and will boot with the configuration you entered.

Cisco IOS Software Basics

The section provides you with some basic information about the Cisco IOS software and includes the following sections:

- Cisco IOS Modes of Operation
- Getting Context-Sensitive Help

Cisco IOS Modes of Operation

Cisco IOS software provides access to several different command modes. Each command mode provides a different group of related commands.

For security purposes, Cisco IOS software provides two levels of access to commands: user and privileged. The unprivileged user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.

Table 20-1 describes some of the most commonly used modes, how to enter the modes, and the resulting prompts. The prompt helps you identify which mode you are in and, therefore, which commands are available to you.

Table 20-1 Cisco IOS Operating Modes

Mode of Operation	Usage	How to Enter the Mode	Prompt
User EXEC	User EXEC commands allow you to connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information. The EXEC commands available at the user level are a subset of those available at the privileged level.	Log in.	7200 Router
Privileged EXEC	Privileged EXEC commands set operating parameters. The privileged command set includes those commands contained in user EXEC mode, and also the **configure** command through which you can access the remaining command modes. Privileged EXEC mode also includes high-level testing commands, such as **debug**.	From user EXEC mode, enter the **enable** EXEC command.	7200 Router#

Table 20-1 Cisco IOS Operating Modes (Continued)

Mode of Operation	Usage	How to Enter the Mode	Prompt
Global configuration	Global configuration commands apply to features that affect the system as a whole.	From global configuration mode, enter the **configure** privileged EXEC command.	7200 Router#config)#
Interface configuration	Interface configuration commands modify the operation of an interface such as an ATM, Ethernet, or serial port. Many features are enabled on a per-interface basis. Interface configuration commands always follow an interface global configuration command, which defines the interface type.	From global configuration mode, enter the **interface** *type number* command. For example, enter the **interface serial 0** command to configure the serial 0 interface.	7200 Router#(config-if)#
ROM monitor	ROM monitor commands are used to perform low-level diagnostics. You can also use the ROM monitor commands to recover from a system failure and stop the boot process in a specific operating environment.	From privileged EXEC mode, enter the **reload** EXEC command. Press Break during the first 60 seconds while the system is booting.	>

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, enter the **no ip routing** command and enter **ip routing** to reenable it. The Cisco IOS software command reference publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Getting Context-Sensitive Help

In any command mode, you can get a list of available commands by entering a question mark (?).

```
7200 Router> ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called word help, because it completes a word for you.

```
7200 Router# co?
configure  connect  copy
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
7200 Router# configure ?
  memory    Configure from NV memory
  network   Configure from a TFTP network host
  terminal  Configure from the terminal
  <cr>
```

You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

Saving Configuration Changes

Whenever you make changes to the Cisco 7200 Router configuration, you must save the changes to memory so they will not be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration. The running configuration is stored in RAM; the startup configuration is stored in NVRAM.

To display the current running configuration, enter the **show running-config** command. Enter the **copy running-config startup-config** command to save the current running configuration to the startup configuration file in NVRAM.

```
7200 Router> enable
7200 Router# copy running-config startup-config
```

To display the startup configuration, enter the **show startup-config** command. Enter the **copy startup-config running-config** command to write the startup configuration to the running configuration.

```
7200 Router> enable
7200 Router# copy startup-config running-config
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
7200 Router# configure ?
  memory    Configure from NV memory
  network   Configure from a TFTP network host
  terminal  Configure from the terminal
  <cr>
```

You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

MPLS CoS with BPX 8650, Configuration

This chapter provides a description of MPLS CoS with the use of the BPX 8650 ATM Label Switch Router (ATM LSR). It also contains a summary example for configuring BPX 8650 ATM LSRs, their associated LSCs (7200 or 7500 series), and Edge Label Switch Routers. For additional information, refer to Cisco 7200 or 7500 series router and MPLS related IOS documentation. Refer to 9.2 Release notes for supported features.

The chapter contains the following:

- MPLS CoS Summary
- Related Features and Technologies
- Related Documents
- Prerequisites
- List of Terms and Acronyms
- MPLS CoS with IP+ATM Overview
- MPLS CoS in an IP+ATM Network
- ATM CoS Service Templates and Qbins on the BPX 8650
- MPLS CoS over IP+ATM Operation
- Configuration Example

MPLS CoS Summary

The MPLS CoS feature enables network administrators to provide differentiated types of service across an MPLS Switching network. Differentiated service satisfies a range of requirements by supplying the particular kind of service specified for each packet by its CoS. Service can be specified in different ways—for example, through use of the IP precedence bit settings in IP packets or in source and destination addresses.

In supplying differentiated service, MPLS CoS offers packet classification, congestion avoidance, and congestion management. Table 21-1 lists these functions and the means by which they are delivered.

Table 21-1 CoS Services and Features

Service	CoS Function	Description
Packet classification	Committed access rate (CAR). Packets are classified at the edge of the network before labels are assigned.	CAR uses the type of service (TOS) bits in the IP header to classify packets according to input and output transmission rates. CAR is often configured on interfaces at the edge of a network in order to control traffic into or out of the network. You can use CAR classification commands to classify or reclassify a packet.
Congestion avoidance	Weighted random early detection (WRED). Packet classes are differentiated based on drop probability.	WRED monitors network traffic, trying to anticipate and prevent congestion at common network and internetwork bottlenecks. WRED can selectively discard lower priority traffic when an interface begins to get congested. It can also provide differentiated performance characteristics for different classes of service.
Congestion management	Weighted fair queueing (WFQ). Packet classes are differentiated based on bandwidth and bounded delay.	WFQ is an automated scheduling system that provides fair bandwidth allocation to all network traffic. WFQ classifies traffic into conversations and uses weights (priorities) to determine how much bandwidth each conversation is allocated, relative to other conversations.

MPLS CoS lets you duplicate Cisco IOS IP CoS (Layer 3) features as closely as possible in MPLS switching devices, including label switching routers (LSRs), edge LSRS, and ATM label switching routers (ATM LSRs). MPLS CoS functions map nearly one-for-one to IP CoS functions on all interface types.

Related Features and Technologies

The MPLS CoS feature can be used optionally with MPLS Virtual Private Networks. MPLS CoS can also be used in any MPLS switching network.

Related Documents

For more information on configuration of the CoS functions (CAR, WRED, and WFQ), refer to the *Cisco IOS Class of Service for Tag Switching Feature Guid*e, and the *Cisco IOS Quality of Service Solutions Configuration Guide*.

For complete command syntax information for CAR, WRED, and WFQ, refer to the Cisco IOS *Quality of Service Solutions Command Reference*.

For additional information on BPX 8650 CLI commands, refer to the *Cisco WAN Switch Command Reference*.

Prerequisites

In order to use the MPLS CoS feature, your network must be running the following Cisco IOS features:

- CEF switching in every MPLS enabled router
- MPLS
- ATM functionality

Also, the BPX 8650 must have:

- the appropriate switch software associated with the Cisco IOS
- the appropriate firmware loaded in the associated BXM cards.

List of Terms and Acronyms

ATM-LSR—An ATM label switching router with a number of LC-ATM interfaces. The router forwards the cells among these interfaces using labels carried in the VPI/VCI field.

CAR—Committed Access Rate (packet classification). CAR is the main feature supporting packet classification. CAR uses the type of service (TOS) bits in the IP header to classify packets. You can use the CAR classification commands to classify and reclassify a packet.

CoS—Class of service. A feature that provides scalable, differentiated types of service across a label switched network.

DWFQ—VIP-Distributed WFQ.

DWRED—VIP-Distributed WRED.

edge ATM LSR—A switch router that is connected to the ATM-LSR cloud through LC-ATM interfaces. The edge ATM LSR adds labels to unlabeled packets and strips labels from unlabeled packets.

IP Precedence—3-bit value in TOS byte used for assigning Precedence to IP packets.

MPLS—Multiprotocol Label Switching. Networks using MPLS, transport IP packets over ATM using label switching, thereby realizing the flexibility and scalability of TCP/IP along with the switching speed and reliability of ATM.

QoS—Quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

RED—Random early detection. Congestion avoidance algorithm in which a small percentage of packets are dropped when congestion is detected and before the queue in question overflows completely.

label—A label is a header used by an LSR to forward packets. The header format depends upon network characteristics. In router networks, the label is a separate, 32-bit header. In ATM networks, the label is placed into the virtual channel identifier/virtual path identifier (VCI/VPI) cell header. In the core, LSRs read only the label, not the packet header. One key to the scalability of MPLS is that labels have only local significance between two devices that are communicating.

label imposition—The act of putting the first label on a packet.

edge label switch router (LSR)—The edge device that performs initial packet processing and classification and applies the first label. This device can be either a router, such as the Cisco 7500, or a switch with built-in routing, such as the Cisco BPX 8650.

label switch router (LSR)—The core device that switches labeled packets according to precomputed switching tables. It can also be a switch or a router.

Label VC (LVC)—An ATM virtual circuit that is set up through ATM LSR label distribution procedures.

label-controlled ATM interface (LC-ATM interface)—An interface on a router or switch that uses label distribution procedures to negotiate label VCs.

Label Switched Path (LSP)—Path defined by all labels assigned between end points. An LSP can be dynamic or static

TOS—Type of Service. A byte in the IPv4 header.

VPN—Virtual private network. A secure network that shares resources with one or more physical networks. A VPN can contain one or more geographically dispersed sites that can communicate securely over a shared backbone.

WEPD—Weighted Early Packet Discard

WRED—Weighted RED. A variant of RED in which the probability of a packet being dropped depends on either, its IP Precedence, CAR marking, or Label Switching CoS (as well as the other factors in the RED algorithm).

WFQ—Weighted Fair Queueing. A queue management algorithm that provides a certain fraction of link bandwidth to each of several queues, based on a relative bandwidth applied to each of the queues.

MPLS CoS with IP+ATM Overview

As part of their VPN services, service providers may wish to offer premium services defined by Service Level Agreements (SLAs) to expedite traffic from certain customers or applications. QoS in IP networks gives devices the intelligence to preferentially handle traffic as dictated by network policy. QoS is defined as those mechanisms that give network managers the ability to control the mix of bandwidth, delay, jitter, and packet loss in the network. QoS is not a device feature, it is an end-to-end system architecture. A robust QoS solution includes a variety of technologies that interoperate to deliver scalable, media-independent services throughout the network, with system-wide performance monitoring capabilities.

The actual deployment of QoS in a network requires a division of labor for greatest efficiency. Because QoS requires intensive processing, the Cisco model distributes QoS duties between edge and core devices, which can be multilayer switches or routers. Edge devices do most of the processor-intensive work, performing application recognition to identify flows and classify packets according to unique customer policies. Edge devices also provide bandwidth management. Core devices expedite forwarding while enforcing QoS levels assigned at the edge.

MPLS-enabled networks make use of Cisco IOS QoS features to build an end-to-end QoS architecture:

- IP Precedence---This feature uses three bits in the IP header to indicate the service class of a packet (up to eight classes). This value is set at the edge and enforced in the core. In IP+ATM networks, different labels are used to indicate precedence levels.
- Committed Access Rate (CAR)---CAR manages bandwidth allocation for certain traffic types. To enforce customer network policies, managers can configure multiple Layer 3 thresholds based on the desired parameters, such as application or protocol. If a flow exceeds a given threshold, managers can provision a variety of responses, from dropping excess packets to sending them at a lower service class.
- Weighted Random Early Detection (WRED)---This feature prevents network congestion by detecting and slowing flows (according to service class) before congestion occurs.
- Class-Based Weighted Fair Queuing (CBWFQ)---This feature provides the ability to reorder packets and control latency at the edge and in the core. By assigning different weights to different service classes, a switch can manage buffering and bandwidth for each service class. Because weights are relative and not absolute, under utilized resources can be shared between service classes for optimal bandwidth efficiency.

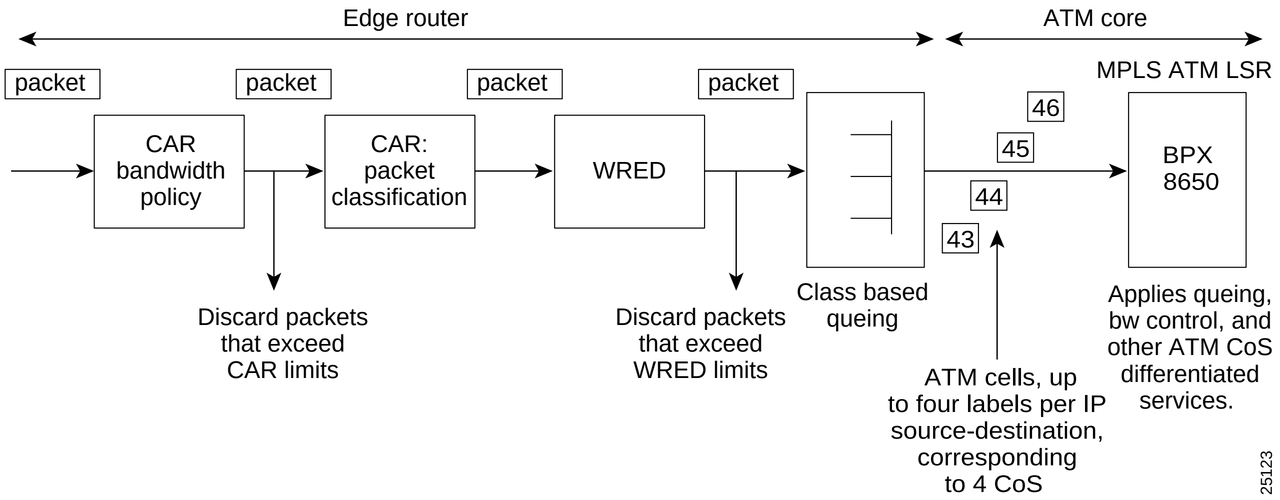
The key to an effective, network-wide IP QoS plan is scalability. Applying QoS on a flow-by-flow basis is not practical because of the huge numbers of IP traffic flows in carrier-sized networks. A scalable way to provide higher levels of service quality with minimal loss in granularity is to implement multiple service classes, or classes of service (CoSs). For example, a service provider network may implement three service classes: a high-priority, low-latency class, a guaranteed-delivery “mission-critical” service, and a low-priority “best-effort” class. Subscribers can use the mix of services that suits their needs. For example, subscribers may wish to use a guaranteed-delivery, low-latency service for their video conferencing applications, and best-effort service for e-mail traffic.

MPLS makes it possible to apply scalable QoS across very large routed networks and Layer 3 IP QoS in ATM networks, because providers can designate sets of labels that correspond to service classes. In routed networks, MPLS-enabled QoS substantially reduces processing throughout the core for optimal performance. In ATM networks, MPLS makes end-to-end Layer 3-type services possible. Traditional ATM and Frame Relay networks implement CoS with point-to-point virtual circuits, but this is not scalable because of high provisioning and management overhead. Placing traffic into service classes at the edge enables providers to engineer and manage classes throughout the network. If service providers manage networks based on service classes, not point-to-point connections, they can substantially reduce the amount of detail they must track and increase efficiency without losing functionality. Compared to per-circuit management, MPLS-enabled CoS in ATM networks provides virtually all the benefits of point-to-point meshes with far less complexity. Using MPLS to establish IP CoS in ATM networks eliminates per-VC configuration. The entire network is easier to provision and engineer.

MPLS CoS in an IP+ATM Network

In IP+ATM networks, MPLS uses predefined sets of labels for each service class, so switches automatically know which traffic requires priority queuing. A different label is used per destination to designate each service class (see Figure 21-1). There can be up to four labels per IP source-destination. Using these labels, core LSRs implement class based WFQ to allocate specific amounts of bandwidth and buffer to each service class. Cells are queued by class to implement latency guarantees. On a Cisco IP+ATM LSR, the weights assigned to each service class are relative, not absolute. The switch can therefore “borrow” unused bandwidth from one class and allocate it to other classes (according to weight). This scenario enables very efficient bandwidth utilization. The class based WFQ solution ensures that customer traffic is sent whenever unused bandwidth is available, whereas ordinary ATM VCs drop cells in oversubscribed classes even when bandwidth is available.

Figure 21-1 Multiple LVCs for IP QoS Services


Edge router
ATM core
packet
packet
packet
packet
MPLS ATM LSR
CAR bandwidth policy
CAR: packet classification
WRED
46
45
44
43
BPX 8650
Discard packets that exceed CAR limits
Discard packets that exceed WRED limits
Class based queing
ATM cells, up to four labels per IP source-destination, corresponding to 4 CoS
Applies queing, bw control, and other ATM CoS differentiated services.
25123

Packets have their precedence bits in the Type of Service field of the IP header, set at either the host or an intermediate router, which could be the edge Label Switch Router (LSR). The precedence bits define a Class of Service (CoS) 0-3, corresponding for to premium, standard, available, or control, for example.

To establish CoS operation when the BPX and the associated LSC router (7200 or 7500 series) are initially configured, the binding type assigned each LVC interface on the BPX is configured to be multiple LVCs.

Then under the routing protocol (OSPF, for example), four LVCs are set up across the network for each IP source to destination requirement. Depending on the precedence bits set in the packets that are received by the edge LSR, the packet ATM cells that are sent to the ATM LSR will be one four classes (as determined by the cell label, that is, VPI.VCI). Furthermore, two subclasses are distinguishable within each class by the use of the Cell Loss Priority (CLP) bit in the cells.

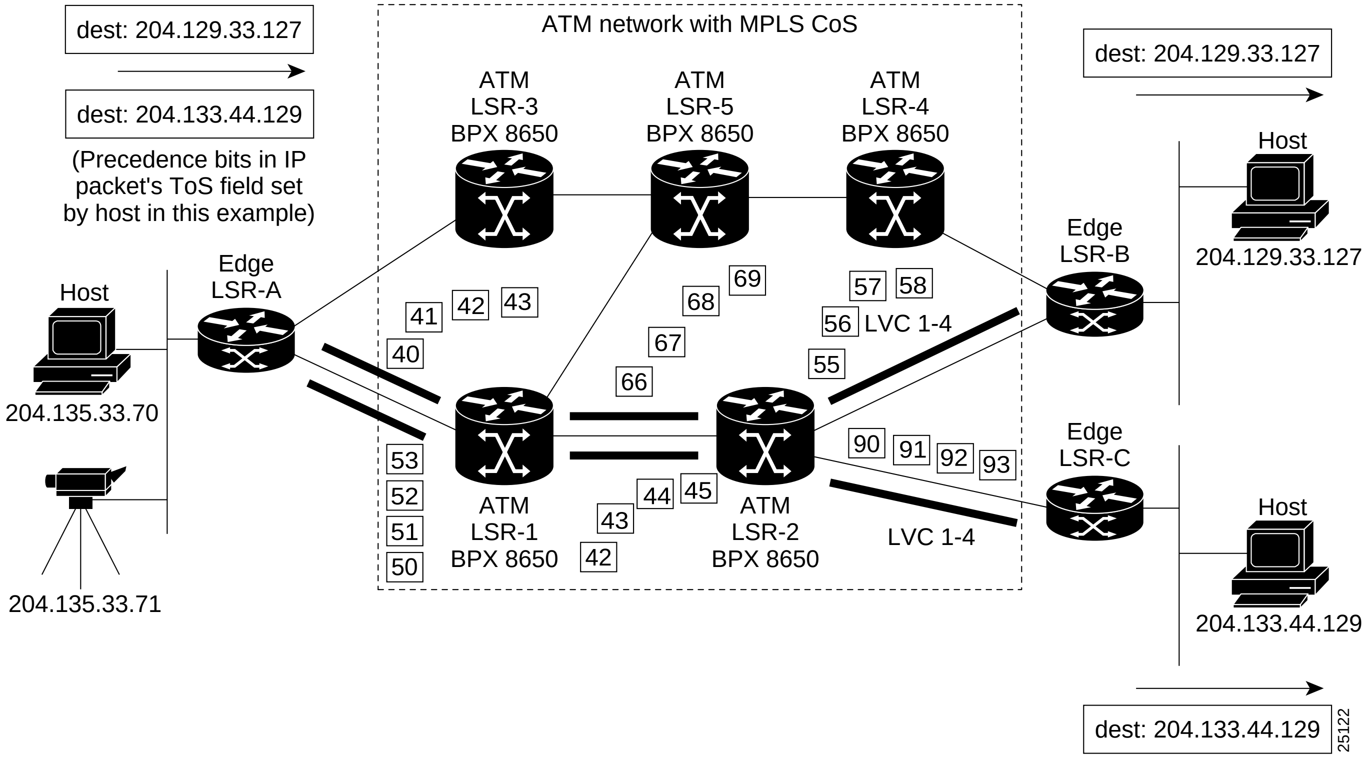
Then the ATM LSR performs a MPLS data table lookup and assigns the appropriate template class of service template and qbin characteristics. The default mapping for CoS is listed in Table 21-2.

Table 21-2 Type of Service and Related CoS

Class of Service Mapping	Class of Service	IP ToS
Available	0	ToS 0/4
Standard	1	ToS 1/5
Premium	2	ToS 2/6
Control	3	ToS 3/7

Figure 21-2 shows an example of IP traffic across an ATM core consisting of BPX 8650 ATM LSRs. The host is seen to be sending two types of traffic across the network, interactive video and non-time critical data. Since multiple LVCs have automatically been generated for all IP source-destination paths, traffic for each source destination is assigned to 1 of 4 LVCs, based on the precedence bit setting in the IP packet header. In this case, the video traffic might be assigned to the premium CoS, and transmitted across the network starting with the cell label “51” out of the Edge LSR-A, and continuing across the network with the cell label “91” applied to the Edge LSR-C. In each BPX 8650 ATM LSR, the cells are processed with the pre-assigned bandwidth, queuing, and other ATM QoS functions suitable to “premium” traffic. In a similar fashion, low priority data traffic cells with the same IP source-destination might be assigned label “53 out of Edge LSR-A and arrive at Edge LSR-C with the label “93”, receiving pre-assigned bandwidth, queuing and other ATM QoS functions suitable to “available” traffic.

Figure 21-2 Example of Multiple LVCs CoS with BPX 8650s



ATM CoS Service Templates and Qbins on the BPX 8650

The service class template 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 in a BXM port interface during initial setup of the interface.

A set of service templates is stored in each switch (BPX 8650) 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.

For MPLS, an MPLS service termplate is assigned to the VSI interface when the trunk or port is initialized The label switch controller (LSC) automatically sets up LVCs via a routing protocol (e.g., OSPF) and the Label Distribution Protocol (LDP), when the class of service Multiple LVC option is enabled at the edge label switch routers (LSRs). With the Multiple VC option enabled (at edge LSRs), four LVCs are configured for each IP source-destination. Each of the four LVCs is assigned a service template type. For example, one of the four cell labels might be assigned to label cos2 service type category. Each service template type has an associated qbin (see Figure 21-3). The qbins provide the ability to manage bandwidth by temporarily storing cells and then serving them out as bandwidth is available 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 celsl are processed based on their connection classification. Based on its label, a cell receives the ATM differentiated service associated with its template type, that is, MPLS1 template, and service type, for example., label cos2 bw, associated qbin characteristics, and other associated ATM parameters.

Initial Setup of LVCs

The service template contains two classes of data. One class consists of parameters necessary to establish a connection (that is, per LVC) and includes entries such as UPC actions, various bandwidth related items, per LVC thresholds, etc. The second class of data items includes those necessary to configure the associated class of service buffers (qbins) that provide CoS support.

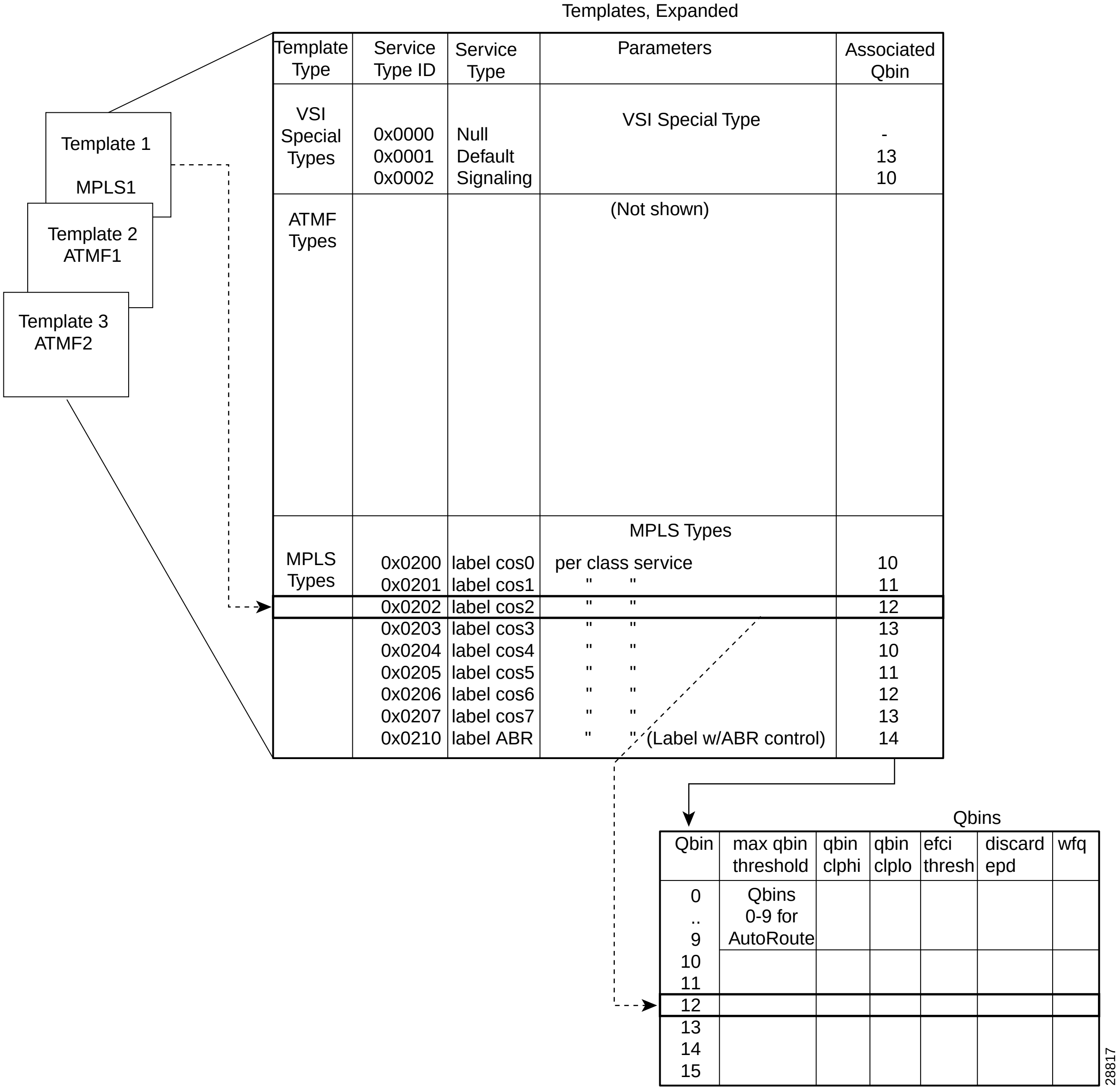
When a connection setup request is received from the VSI master in the Label Switch Controller, the VSI slave (in the BXM, for example) uses the service type identifier to index into a Service Class Template database (Figure 21-3) containing extended parameter settings for connections matching that index. The slave uses these values to complete the connection setup and program the hardware.

Structure

When the **upport** or **uptrk** command is used to activate an interface on the BXM card, the default service template, which is MPLS1, is assigned to the interface (Figure 21-3). 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.

Qbin templates are used only with qbins that are available to VSI partitions, namely qbins 10 through 15. Qbins 10 through 15 are used by the VSI on interfaces configured as trunks or ports. The rest of the qbins (0-9) are reserved for and configured by Autoroute.

Figure 21-3 Service Template and Associated Qbin Selection



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			(Not shown)	
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

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						

MPLS CoS over IP+ATM Operation

The basic functions that are applied to a packet, as it makes its way from on host on the left side of a network (see Figure 21-4), through the network consisting of conventional routers, label edge routers (LSRs), Label Switch Routers (LSRs), and ATM LSRs such as a BPX 8650 are as follows:

Note In the figure, the functions are shown being performed by separate entities. In general, one or more functions can be performed by the same entity. For example, the setting of precedence and labeling could all be performed in a single Label Edge Router if the Host was not participating.

The typical operation for MPLS CoS in the network shown in Figure 21-4 is as follows:

Step 1 Set the IP Type of Service (ToS) for a packet in the host (or router).

Step 2 Apply one or more labels, and copy the IP ToS to Label CoS in the label header at the edge label switch router (LSR).

Step 3 Queue the packet in a Label Switch Router (LSR) according to its CoS.

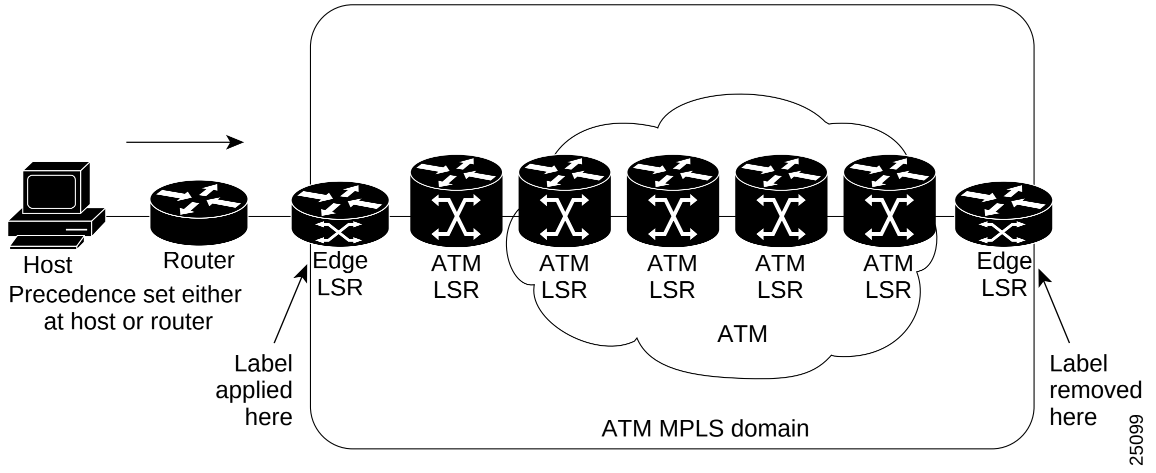
Step 4 Map the MPLS and MPLS CoS bits to an ATM Label-VC in (LSR at edge of ATM cloud).

Step 5 Apply ATM CoS bandwidth and queuing to ATM cells based on their class of service in the ATM LSR (BPX 8650, for example).

Step 6 Receive the packet from the ATM cloud and forward it with appropriate Label CoS through a LSR (could be frame-based LSR) at the edge of the ATM cloud.

Step 7 Receive the labeled packet, remove the label, and forward the IP packet with appropriate CoS towards its destination (edge LSR).

Figure 21-4 MPLS CoS over IP+ ATM with BPX 8650 LSRs



Configuration Example

There are four default policy types for MPLS CoS. The default relative bandwidth per xtagatm interface are listed in Table 21-3. The relative bandwidth weights determine the proportion of bandwidth available to MPLS which is given to each class of service on each link. If a CoS does not use the bandwidth given to it, then the bandwidth may be shared among the other CoSes.

Table 21-3 Class of Service and Relative Bandwidth Weighting

Class of Service Mapping	Class of Service	IP ToS	Default Bandwidth Weight
Available	0	ToS 0/4	50
Standard	1	ToS 1/5	50
Premium	2	ToS 2/6	0
Control	3	ToS 3/7	1

It is important to reserve a small amount of bandwidth for the Control CoS. This CoS is used for MPLS control traffic, and it is important to guarantee a good quality of service for this traffic. For this reason, it is desirable to reserve a small amount of bandwidth for the Control CoS as shown in Table 21-4.

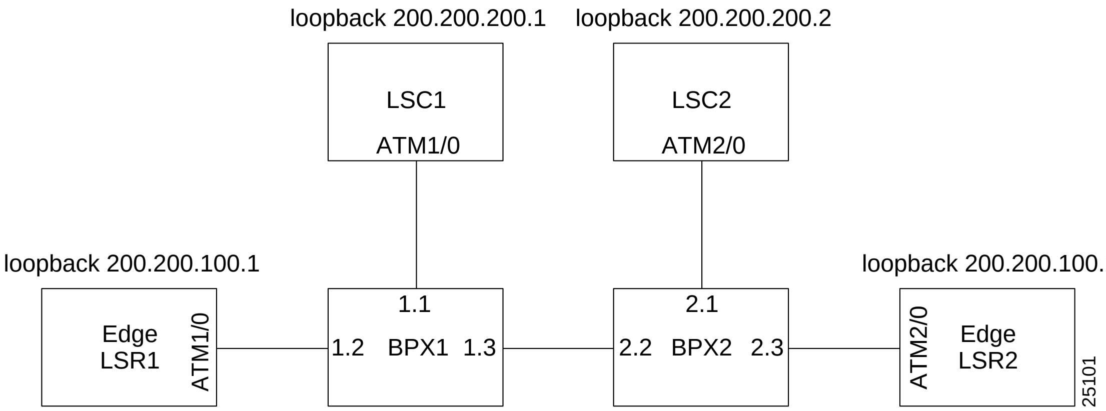
Table 21-4 Class of Service and Relative Bandwidth Weighting Setup

Class of Service Mapping	Class of Service	IP ToS	Bandwidth Weight
Available	0	ToS 0/4	49
Standard	1	ToS 1/5	50
Premium	2	ToS 2/6	0
Control	3	ToS 3/7	1

To verify an xtagatm interface after configuration on the LSC, perform a show xtagatm cos-bandwidth-allocation xtagatmxx, where xx is the interface number. The maximum value for cos bandwidth is 100.

The setup for the configuration example is shown in Figure 21-5.

Figure 21-5 MPLS CoS with BPX 8650 LSRs, Configuration Example



Configuration

Configure the following resources according to the example setup shown in Figure 21-5:

When configuring BPX1 and BPX1 verify that no software, card, and trunk errors are reported on the console. In this example, all VSI resources are allocated to maximum value.

BPX configurations:

BPX1

```
uptrk 1.1//LSC1 control port
uptrk 1.3//trunk via BPX1
upln 1.2//up line for LER1
cnfrsrc 1.1 0 352207 y 1 e 0 3000 1 20 0 352207//LSC1
cnfrsrc 1.3 0 352207 y 1 e 0 3000 1 20 0 352207//trunk
cnfrsrc 1.2 0 353207 y 1 e 0 3000 1 20 0 352307//LER1 port
addshelf v 1 1//control-id=1;partition number=1
```

BPX2

```
uptrk 2.1//LSC2 control port
uptrk 2.3//trunk via BPX1
upln 2.2//up line for LER2
cnfrsrc 2.1 0 352207 y 1 e 0 3000 1 20 0 352207//LSC2
cnfrsrc 2.3 0 352207 y 1 e 0 3000 1 20 0 352207//trunk
cnfrsrc 2.2 0 353207 y 1 e 0 3000 1 20 0 352307//LER2 port
addshelf v 2 1//control-id=2;partition number=1
```

Check that VSI resources have been allocated and that the LSC controller was added successfully.

```
dsptrks//successful with no alarms
dspvsipartinfo //verify lcns and bandwidth are allocated successfully
dsplns//no alarm
```

```
dspctrlrs//controller ID is  added successfully
```

There are four default policy parameters for MPLS CoS. The default relative bandwidth per xtagatm interface are as follows: 50 percent for available (0/4 IP ToS), 50 percent for standard (1/5), zero for premium (2/6), and zero for control (3/7) Class of Service. Once xtagatm interface have been defined for each LSC, do a '***show xtagatm cos-bandwidth-allocation xtagatmxx***', where xx is interface number. Verify that default relative bandwidth are properly assigned in percentage value. The maximum value for cos-bandwidth is 100.

LSC configurations:

LSC1

```
LSC11-1#config t
LSC1(config)#int atm1/0//LSC1LSC1 control port
LSC1(config-if)#no shut
LSC1(config-if)#tag-control-protocol vsi
LSC1(config-if)#exit

LSC1(config)#int xtagatm12//LSR1 port 1.2
LSC1(config-if)#extended-port atm1/0 bpx 1.2
LSC1(config-if)#tag-switching ip
LSC1(config-if)#tag-switching atm cos available 49
LSC1(config-if)#tag-switching atm cos standard 50
LSC1(config-if)#tag-switching atm cos premium 0
LSC1(config-if)#tag-switching atm cos control 1
LSC1(config-if)ip unnumbered loopback0
LSC1(config-if)#exit

LSC1(config)#int xtagatm13//LSR1 port 1.3
LSC1(config-if)#extended-port atm1/0 bpx 1.3
LSC1(config-if)#tag-switching ip
LSC1(config-if)#tag-switching atm cos available 49
LSC1(config-if)#tag-switching atm cos standard 50
LSC1(config-if)#tag-switching atm cos premium 0
LSC1(config-if)#tag-switching atm cos control 1
LSC1(config-if)ip unnumbered loopback0
LSC1(config-if)#exit

LSC1(config)#int loopback0//configure loopback0 interface
LSC1(config-if)#ip address 200.200.200.1 255.255.255.255
LSC1(config-if)#exit

LSC1(config)#ip routing//enable IP routing
LSC1(config)#ip cef//enable Cisco Express Forwarding Protocol
LSC1(config)#router ospf 10
LSC1(config-router)#network 200.200.200.1 0.0.0.0 area 0
LSC1(config-router)#end
```

LSC2

```
LSC2#config t
LSC2(config)#int atm2/0//LSC2 control port
```

```
 LSC2(config-if)#no shut
 LSC2(config-if)#tag-control-protocol vsi id 2
 LSC2(config-if)#exit

 LSC2(config)#int xtagatm22//LSR2 port 2.2
 LSC2(config-if)#extended-port atm1/0 bpx 2.2
 LSC2(config-if)#tag-switching ip
 LSC2(config-if)#tag-switching atm cos available 49
 LSC2(config-if)#tag-switching atm cos standard 50
 LSC2(config-if)#tag-switching atm cos premium 0
 LSC2(config-if)#tag-switching atm cos control 1
LSC2(config-if)ip unnumbered loopback0
 LSC2(config-if)#exit

 LSC2(config)#int xtagatm23//LSR2 port 2.3
 LSC2(config-if)#extended-port atm1/0 bpx 2.3
 LSC2(config-if)#tag-switching ip
 LSC2(config-if)#tag-switching atm cos available 49
 LSC1(config-if)#tag-switching atm cos standard 50
 LSC1(config-if)#tag-switching atm cos premium 0
 LSC1(config-if)#tag-switching atm cos control 1
 LSC2(config-if)ip unnumbered loopback0
 LSC2(config-if)#exit

 LSC2(config)#int loopback0//configure loopback0 interface
 LSC2(config-if)#ip address 200.200.200.2 255.255.255.255
 LSC2(config-if)#exit

 LSC2(config)#ip routing//enable IP routing
 LSC2(config)#ip cef//enable Cisco Express Forwarding Protocol
 LSC2(config)#router ospf 10
 LSC2(config-router)#network 200.200.200.2 0.0.0.0 area 0
 LSC2(config-router)#end
```

Edge LSR configurations:

LSR1

```
LSR1LSR1#config t
LSR1(config)#int atm1/0//LSR1 interface
LSR1(config-if)#no shut
LSR1(config-if)#exit
LSR1(config)#interface atm1/0.1 tag-switching//create tag sub-interface
LSR1(config-subif)#ip unnumbered loopback0
LSR1(config-subif)#tag-switching atm multi-vc//enable multi-vc mode (4 VCs)
LSR1(config-subif)#tag-switching ip

LSR1(config)#int loopback0//configure loopback0 interface
LSR1(config-if)#ip address 200.200.100.1 255.255.255.255

LSR1(config)#ip routing//enable IP routing
LSR1(config)#ip cef//enable Cisco Express Forwarding Protocol
LSR1(config)#router ospf 10
LSR1(config-router)#network 200.200.100.1 0.0.0.0 area 0
LSR1(config-router)#exit
```

In default multiple LVC mode, there are four MPLS Cos LVCs created by cos-map with clp set to off. The four classes of service are available (0/4), standard (1/5), premium (2/6), and control (3/7).

LSR2

```
LSR2#config t
LSR2LSR2(config)#int atm2/0//LSR2 interface
LSR2(config-if)#no shut
LSR2(config-if)#exit
LSR2(config)#interface atm2/0.1 tag-switching//create tag sub-interface
LSR2(config-if)#ip unnumbered loopback0
LSR2(config-if)#tag-switching ip

LSR2(config)#int loopback0//configure loopback0 interface
LSR2(config-if)#ip address 200.200.100.2 255.255.255.255

LSR2(config)#ip routing//enable IP routing
LSR2(config)#ip cef//enable Cisco Express Forwarding Protocol
LSR2(config)#router ospf 10
LSR2(config-router)#network 200.200.100.2 0.0.0.0 area 0
LSR2(config-router)#end

LSR2(config)#tag-switching cos-map 1//configure Cos-Map
LSR2(config-tag-cos-map)#end//for now use default 4 VCs
LSR2#sho tag-switching cos-map//there should be 4 VCs w/ clp off
LSR2#config t
LSR2(config)#access-list 1 permit 200.200.100.1 0.0.0.0 //create access list for network
200.200.100.1
LSR2(config)#tag-switching prefix-map 1 access-list 1 cos-map 1//map access-list to cos-map 1
LSR2(config)#show tag forward 200.200.100.1 32 detail//verify forwarding table
```

Verify that the LSC/LSR is operational and BPXs have clear alarms. LSR1 should be able to ping to LSR2 successfully.

Check that VSI resources have been allocated and controller was added successfully. BPXs should have clear alarms and no software log and trunk errors.

BPX1/BPX1

```
dsptrks//successful with no alarms
dspvsipartinfo //verify lcns and bandwidth are allocated successfully
dsplns//no alarm
dspctrlrs//controller ID is added successfully
```

Check that LSC/edge LSR interfaces are operational and TDP bindings are successful.

LSC1 and LSC2

```
LSC1#sho tag interface //xtagatm interfaces are operational
LSC1#sho xtag cross-connect//verify crosss-connect
LSC1#sho xtag vc//verify tag vc
```

```
LSC1#sho control vsi descriptor//verify VSI VPI range and Bw
LSC1#sho control vsi control-interface//verify number of connections for each cross-connect
LSC1#sho control vsi traffic//verify traffic statistics
LSC1#sho tag atm bind            //verify tag atm bindings
LSC1#sho tag atm sum//verify local/remote connections
```

LSR1 and LSR2

```
LSR1#sho tag interface //xtagatm interfaces are operational
LSC2#sho tag tdp disc//verify tdp session rx/tx
LSC2#sho atm  vc//verify atm pvc and tvc
```

Note MPLS CoS Multiple LVC mode allows users to reconfigure the classes for different traffic configurations. Users have the flexibility to modify the four LVCs for any CoS. For example, the user has the choice of assigning a “high” weight to a low class (that is, available CoS =60 and control CoS = 20).

MPLS VPNS with BPX 8650, Configuration

This chapter provides a description of MPLS VPNs with the use of the BPX 8650 ATM Label Switch Router (ATM LSR). It also contains a summary example of the configuration of IOS to support VPNs, and references to relevant IOS documentation. Refer to 9.2 Release notes for supported features.

The chapter contains the following:

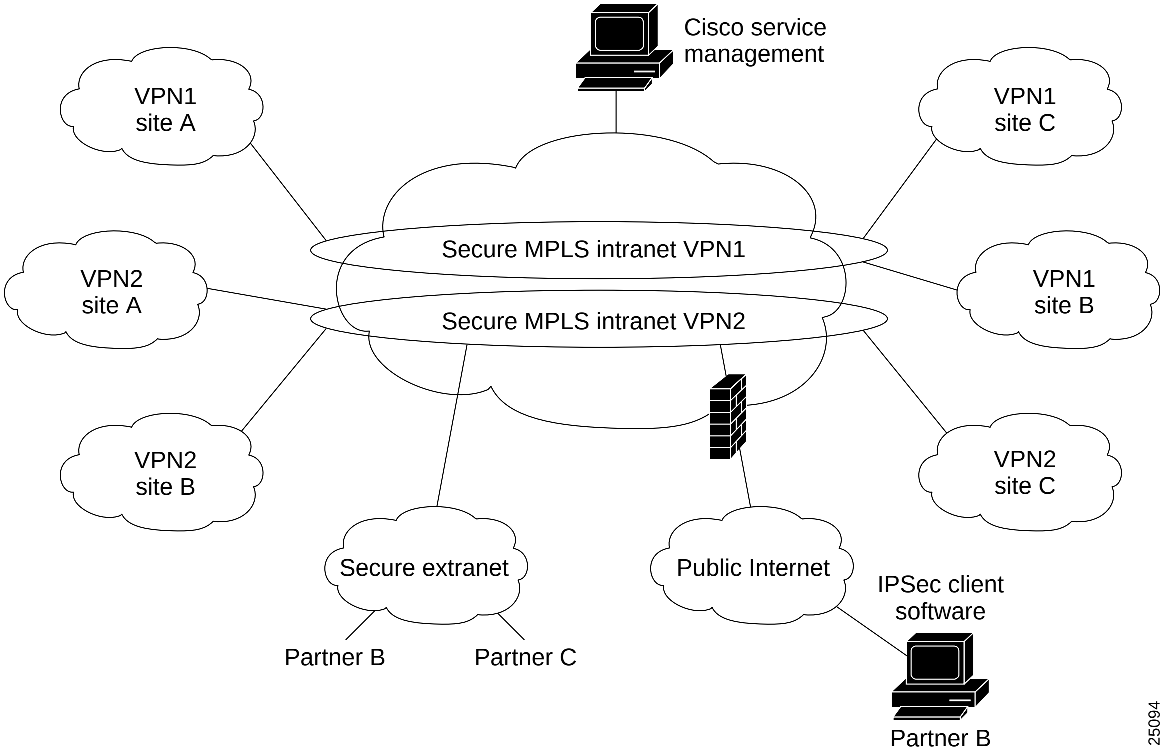
Introduction

MPLS VPNs, which are created in Layer 3, are connectionless, and therefore substantially more scalable and easier to build and manage than conventional VPNs. In addition, value-added services, such as application and data hosting, network commerce, and telephony services, can easily be added to a particular MPLS VPN because the service provider's backbone recognizes each MPLS VPN as a separate, connectionless IP network. MPLS over IP+ATM VPN networks combine the scalability and flexibility of IP networks with the performance and QoS capabilities of ATM.

MPLS-enabled IP VPN networks provide the foundation for delivering value-added IP services, such as multimedia application support, packet voice, and application hosting, all of which require specific service quality and privacy. Because QoS and privacy are an integral part of MPLS, they no longer require separate network engineering. From a single access point, it is now possible to deploy multiple VPNs, each of which designates a different set of services (Figure 22-1). This flexible way of grouping users and services makes it possible to deliver new services more quickly and at a much lower cost. The ability to associate closed groups of users with specific services is critical to service provider value-added service strategies.

The VPN network must be able to "see" traffic by application type, such as voice, mission-critical applications, or e-mail, for example. The network should easily separate traffic based on which VPN it belongs to, without configuring complex, point-to-point meshes. Further, the network needs to be "VPN aware" so that the service provider can easily group users and services into Intranets or Extranets with the services they need. In such networks, VPNs are a fundamental capability. VPNs offer service providers a technology that is highly scalable and allows subscribers to quickly and securely provision Extranets to new partners. MPLS is the technology that brings "VPN awareness" to switched or routed networks. It enables service providers to quickly and cost-effectively deploy secure VPNs of all sizes---all over the same infrastructure.

Figure 22-1 VPN Network



MPLS VPN Benefits Summary

MPLS VPN benefits and capabilities include:

- A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce
- Privacy and security equal to Layer-2 VPNs by limiting the distribution of a VPN's routes to only those routers that are members of the VPN
- Seamless integration with customer intranets
- Increased scalability over current VPN implementations, with thousands of sites per VPN and hundreds of thousands of VPNs per service provider
- IP Class of Service (CoS), with support for multiple classes of service and priorities within a VPN, as well as between VPNs
- Easy management of VPN membership and easy provisioning of new VPNs for rapid deployment
- Scalable any-to-any connectivity for extended intranets and extranets that encompass multiple businesses
- MPLS enables business IP services
  - VPNs with strong SLAs for QoS
  - privacy and QOS of ATM without tunneling or encryption
  - enabled by Cisco's unique combination of MPLS and open standards routing
- Lower operating costs
  - enables low cost managed services to increase SP market share
  - increases profits though lower marginal cost for new services
  - network establishes VPN connectivity - no provisioning
  - build once/sell many - single routing image for all VPNs
- The first transport-independent VPN
  - universal VPN:one VPN, any access/transport:dial, xDSL, ATM, ...
  - service delivery independent of transport/access technology
- Simpler for the customer
  - VPN managed by the service provider
  - transparent support for private IP addresses
  - multiple QoS service classes to implement business net policy
- Revenue and growth
  - revenue from today's transport services, growth from IP
- Business IP services enabled by MPLS/IOS
  - MPLS brings IOS to service provider ATM networks
  - MPLS is the new industry standard for bringing IP and ATM together

- Seamless service delivery
  - wide breadth of services:circuit emulation to IP VPNs
  - single pipe - multiple services (any service, any port)
- lower cost of operation - competitive advantages
  - ROI, TTM, economies of a multiservice network

MPLS VPN Features

The VPN feature for MPLS Switching allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone services. MPLS Switching VPNs provide essential characteristics and benefits that service providers require to deploy scalable VPNs and build the foundation to deliver value-added services including:

Performance—When MPLS VPNs are set up using ATM LSRs such as the BPX 8650, the combined benefits of scalable connectionless service of IP is combined with the performance and traffic management capabilities of ATM.

Connectionless Service—A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, today's VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. By creating a connectionless VPN, tunnels and encryption are not required for network privacy, thus eliminating significant complexity.

Centralized Service—Building VPNs in layer 3 has the additional advantage of allowing delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services.It must also provide a way to flexibly deliver value-added services to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS Switching VPNs are seen as private intranets, it's easy to leverage new IP services such as multicast, QoS, and telephony support within a VPN, as well as, centralized services such as content and web hosting to a VPN. Now myriad combinations of specialized services can be customized for individual customers. For example, a service that combines IP multicast with a low-latency service class to enable video conferencing within an intranet.

Scalability—The key deficiency of VPNs that are created using connection-oriented, point-to-point overlays, Frame Relay, or ATM VCs. Specifically, connection-oriented VPNs require a full N^2 mesh of connections between customer sites to support any-to-any communication. MPLS Switching based VPNs instead use the peer model and layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to only peer with one provider edge (PE) router as opposed to all other CPE or customer edge (CE) routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in layer 3, eliminating the need for tunnels or VCs.

Other scalability issues of MPLS Switching VPNs are due to the partitioning of VPN routes between PE routers and the further partitioning of VPN and IGP routes between PE routers and provider (P) routers in a core network. PE routers must maintain VPN routes for those VPNs who are members. P routers do not maintain any VPN routes. This increases the scalability of the providers core and insures that no one device is a scalability bottleneck.

Security—MPLS Switching VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN will not inadvertently go to another VPN. Security is provided at the edge and core a of a provider network:

- at the edge security ensures that packets received from a customer are placed on the correct VPN
- at the backbone, VPN traffic is kept separate.

Malicious spoofing of a provider edge (PE) router is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

Easy to Create—To take full advantage of VPNs, it must be easy to create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. Now it is easy to add sites to intranets and extranets and to easily form closed user groups. Managing VPNs in this manner enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.

Flexible Addressing—To make a VPN service more accessible, customers should be able to design their own addressing plan, independent of addressing plans for other VPN customers supported by a common service provider. Many customers use private address spaces, as defined in RFC 1918 today, and do not want to undertake the time and expense of implementing registered IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without network address translation (NAT) by providing a public and private view of the address. If two VPNs want to communicate and both have overlapping addresses, that communication requires NAT at one endpoint. This enables customers to use their own unregistered private addresses, and communicate freely across a public IP network.

Integrated Class of Service (CoS) Support—CoS is an essential ingredient of an IP VPN, it provides the ability to address two fundamental VPN requirements:

- predictable performance and policy implementation.
- support for multiple classes of service in a MPLS Switching VPN.

Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

Straightforward Migration—For service providers to quickly deploy these VPN services, a straightforward migration path is required. MPLS VPNs are unique because they can be built over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks.

Migration for the end customer is also simplified because there is no requirement to support MPLS on the customer edge (CE) router and no modifications are required to a customer’s intranet.

MPLS VPN Description

VPNs deliver enterprise-scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. A VPN can be built on the Internet or on a service provider's IP, Frame Relay, or ATM infrastructure. Businesses that run their intranets over a VPN service enjoy the same security, prioritization, reliability, and manageability as they do in their own private networks.

VPNs based on IP can extend intranets over wide-area links to remote offices, mobile users, and telecommuters. Further, they can support extranets linking business partners, customers, and suppliers to provide better customer satisfaction and reduced manufacturing costs. Alternatively, VPNs can connect communities of interest, providing a secure forum for common topics of discussion.

MPLS uses a label-based forwarding paradigm. Labels indicate both routes and service attributes. At the ingress edge, incoming packets are processed and labels selected and applied. The core merely reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification, and filtering happens only once, at the ingress edge. At the egress edge, labels are stripped, and packets forwarded to their final destination.

New Business Opportunities for Service Providers

New IP-based services such as video conferencing, packet telephony, distance learning, and information-rich applications offer businesses the promise of improved productivity at reduced costs. As these networked applications become more prevalent, businesses increasingly look to their service providers for intelligent services based on a rich set of controls that go beyond transport to optimize the delivery of applications end to end. Business customers want their applications to traverse a network in a secure, prioritized environment, and they want the opportunity to reduce costs, improve connectivity, and gain access to networking expertise.

Intranet and Extranet VPNs

Intranet VPN services link employees, telecommuters, mobile workers, remote offices, etc., to each other with the same privacy as a private network.

Extranet VPN services link suppliers, partners, customers, or communities of interest over a shared infrastructure with the same policies as a private network.

Cisco provides a range of ATM- and IP-based choices for deploying large-scale Intranet and Extranet VPN services, including Multiprotocol Label Switching (MPLS)-based services which provide secure, business-quality VPN solutions that scale to support tens of thousands of VPN customers over IP or IP+ATM technologies

A VPN built with MPLS affords broad scalability and flexibility across any IP, IP+ATM, or multivendor backbone. MPLS forwards packets using labels. The VPN identifier in the label isolates traffic to a specific VPN. In contrast with IP tunnel and virtual-circuit architectures, MPLS-based VPNs enable connectionless routing within each VPN community. Subsequently, service providers can easily scale their services to support tens of thousands of VPNs on the same infrastructure, with full QoS benefits across IP and ATM environments.

Cisco MPLS-based VPN solutions are supported on its IP+ATM WAN switch platforms including the BPX 8650 and MGX families, and on its high-end router platforms such as the Cisco 12000 series GSR and 7000 series routers.

List of Terms

ATM LSR—An ATM label switching router with a number of LC-ATM interfaces. The ATM LSR forwards the cells among these interfaces using labels carried in the VPI/VCI field. This device can be either a router, such as the Cisco 7500, or a switch with built-in routing, such as the Cisco BPX 8650.

xBGP—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined in RFC 1163.

CEF—Cisco Express Forwarding. An advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns.

CE router—Customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

CoS—Class of service. A feature that provides scalable, differentiated types of service across a MPLS switched network.

Edge ATM Edge LSR—A router that is connected to the ATM-LSR cloud through LC-ATM interfaces. The edge ATM LSR adds labels to unlabeled packets and removes labels from unlabeled packets.

GRE—Generic routing encapsulation. A tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment.

IGP—Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include IGRP, OSPF, and RIP.

IS-IS—Intermediate system-to-intermediate system. OSI link-state hierarchical routing protocol in which ISs (routers) exchange routing information based on a single metric in order to determine network topology.

Label Distribution Protocol (LDP)—Provides communication between edge and core devices. It assigns labels in edge and core devices to establish Label Switched Paths (LSPs) in conjunction with routing protocols such as OSPF, IS-IS, Enhanced Interior Gateway Routing Protocol (EIGRP), or BGP.

Label-switched path (LSP)—A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through MPLS Switching mechanisms. A label-switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

Edge Label Switch Router (LSR)—The edge device that performs initial packet processing and classification and applies the first label. This device can be either a router, such as the Cisco 7500, or a switch with built-in routing, such as the Cisco BPX 8650.

Label-switched path (LSP) tunnel—A configured connection between two routers, in which label Switching is used to carry the packet.

Label Switch Router (LSR)—The core device that switches labeled packets according to precomputed switching tables. It can also be a switch or a router

LSA—Link-state advertisement. A broadcast packet used by link-state protocols. The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

MPLS—Multiprotocol Label Switching. An emerging industry standard upon which MPLS is based.

NLRI—Network layer reachability information. BGP sends routing update messages containing NLRI to describe a route and how to get there. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes; the route attributes include a BGP next hop gateway address, community values, and other information.

PE router—Provider edge router. A router that is part of a service provider's network and that is connected to a customer edge (CE) router. The PE router function is a combination of an MLS edge label switch router (LSR) function with some additional functions to support VPNs.

RD—Route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.

RIP—Routing Information Protocol. Used to exchange routing information within an autonomous system, RIP uses hop count as a routing metric.

traffic engineering—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

traffic engineering tunnel—A label-switched path tunnel that is used for engineering traffic. It is set up through means other than normal Layer 3 routing and is used to direct traffic over a path different from the one that Layer 3 routing would cause it to take.

tunneling—Architecture providing the services necessary to implement any standard point-to-point data encapsulation scheme.

VPN—Virtual private network. A secure network that shares resources with one or more physical networks. A VPN can contain one or more geographically dispersed sites that can communicate securely over a shared backbone.

vpnv4—Used as a keyword in commands to indicate VPN-IPv4 prefixes. These prefixes are customer VPN addresses, each of which has been made unique by the addition of an 8-byte route distinguisher.

VRF—VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

Related Features and Technologies

VPNs are used with the Class of Service (CoS) feature for Label Switching.

Related Documents

- *MPLS VPNs Feature Module*
- C*isco IOS Network Protocols Command Reference, Part 1*

Prerequisites

Your network must be running the following Cisco IOS services before configuring VPN operation:

Label Switching connectivity with generic routing encapsulation (GRE) tunnels configured among all provider (PE) routers with VPN service, or label switching in all provider backbone (P) routers

Label Switching with VPN code in all provider routers with a VPN edge service (PE) routers

BGP in all routers providing a VPN service

CEF switching in every label-enable router

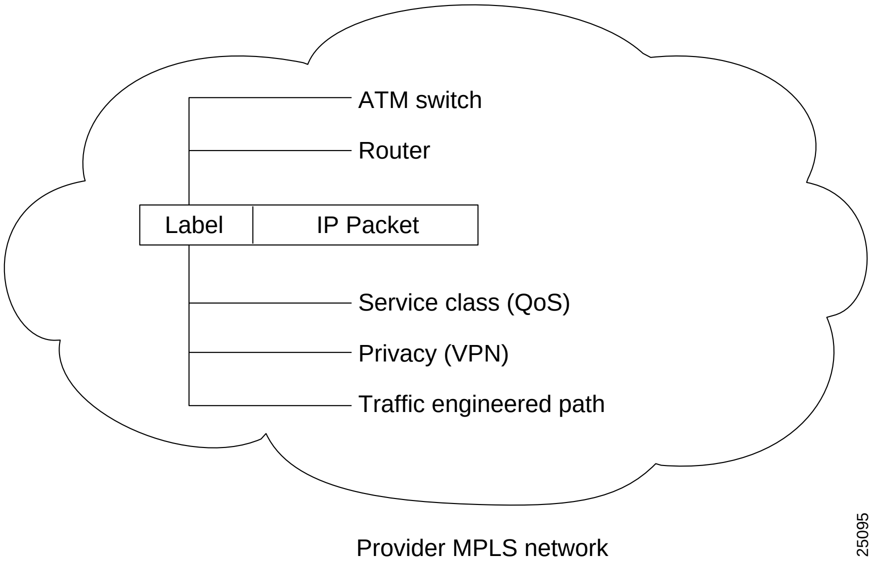
GRE

CoS enabled on all routers

MPLS Labeling Criteria

For enabling business IP services, the most significant benefit of MPLS is the ability to assign labels that have special meanings. Sets of labels distinguish destination address as well as application type or service class, as discussed in the following sections (see Figure 22-2).

Figure 22-2 Benefits of MPLS Labels



The MPLS label is compared to pre-computed switching tables in core devices, such as the BPX ATM LSR, allowing each switch to automatically apply the correct IP services to each packet. Tables are pre-calculated, so there is no need to reprocess packets at every hop. This scenario not only makes it possible to separate types of traffic, such as best-effort traffic from mission-critical traffic, it also renders an MPLS solution highly scalable.

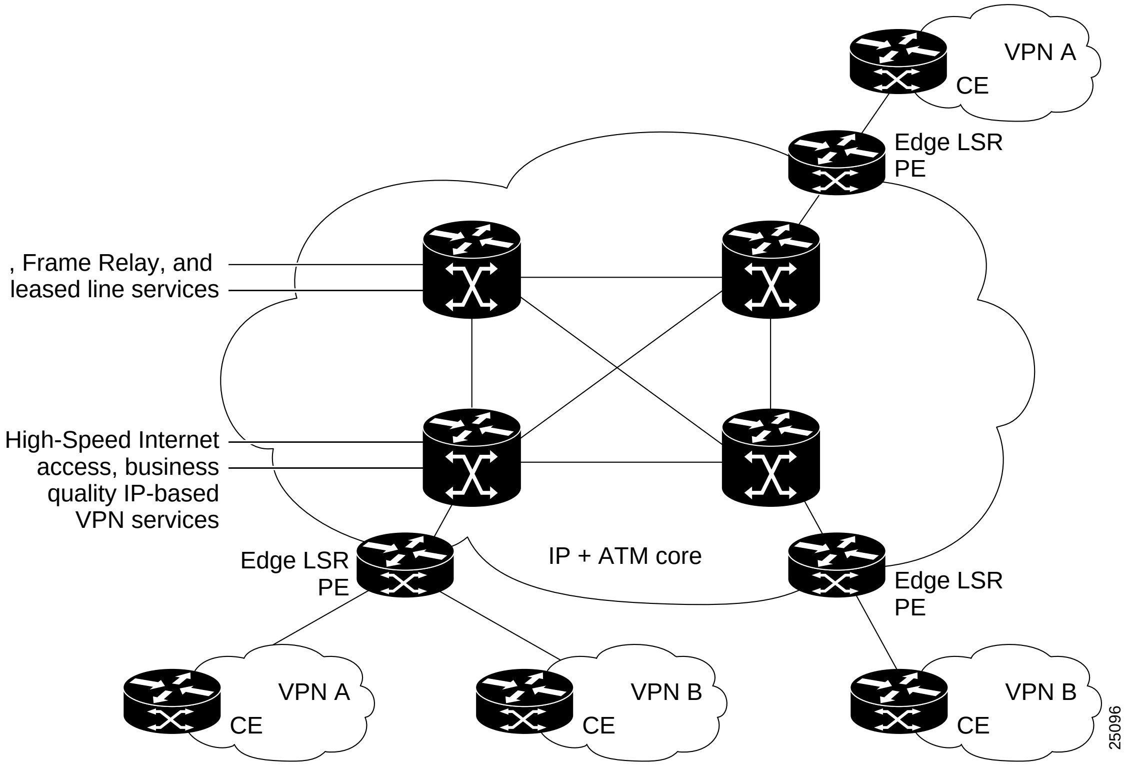
Because MPLS uses different policy mechanisms to assign labels to packets, it decouples packet forwarding from the content of IP headers. Labels have local significance, and they are used many times in large networks; therefore, it's nearly impossible to run out of labels. This characteristic is essential to implementing advanced IP services such as QoS, large-scale VPNs, and traffic engineering.

MPLS VPNs over IP+ATM Backbones Description

Service providers can use MPLS to build intelligent IP VPNs across their existing ATM networks. Because all routing decisions are pre-computed into switching tables, MPLS both expedites IP forwarding in large ATM networks at the provider edge and makes it possible to apply rich Layer 3 services via Cisco IOS technologies in Layer 2 cores. A service provider with an existing ATM core can deploy MPLS-enabled edge switches or routers (LSRs) to enable the delivery of differentiated business IP services. The service provider needs only a small number of VCs to interconnect provider edge switches or routers to deliver extremely large numbers of secure VPNs.

Cisco IP+ATM solutions give ATM networks the ability to intelligently "see" IP application traffic as distinct from ATM/Frame Relay traffic. By harnessing the attributes of both IP and ATM, service providers can provision Intranet or Extranet VPNs. Cisco enables IP+ATM solutions with MPLS, uniting the application richness of Cisco IOS software with carrier-class ATM switches (see Figure 22-3).

Figure 22-3 MPLS VPNs in Cisco IP+ATM Network



Without MPLS, IP transport over ATM networks requires a complex hierarchy of translation protocols to map IP addresses and routing into ATM addressing and routing. MPLS eliminates complexity by mapping IP addressing and routing information directly into ATM switching tables. The MPLS label-swapping paradigm is the same mechanism that ATM switches use to forward ATM cells. This solution has the added benefit of allowing service providers to continue to offer their current Frame Relay, leased-line, and ATM services portfolio while enabling them to offer differentiated business-quality IP services.

MPLS-Enabled Virtual Private Networks

Service providers can use MPLS to build an entirely new class of IP VPNs. MPLS-enabled IP VPNs are connectionless networks with the same privacy as VPNs built using Frame Relay or ATM VCs. Cisco MPLS solutions offer multiple IP service classes to enforce business-based policies. Providers can offer low-cost managed IP services because they can consolidate services over common infrastructure and make provisioning and network operations much more efficient.

Although Frame Relay and multiservice ATM deliver privacy and class of service, IP delivers any-to-any connectivity, and MPLS on Cisco IP+ATM switches, such as the BPX 8650 ATM LSR, enables providers to offer the benefits of business-quality IP services over their ATM infrastructures.

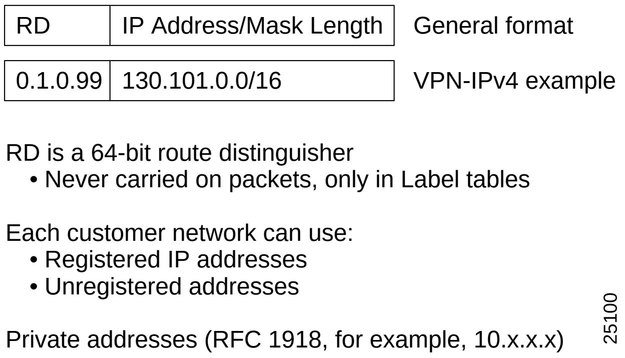
Built-In VPN Visibility

To cost-effectively provision feature-rich IP VPNs, providers need features that distinguish between different types of application traffic and apply privacy and QoS—with far less complexity than an overlay IP tunnel, Frame Relay, or ATM “mesh.”

Compared to an overlay solution, an MPLS-enabled network can separate traffic and provide privacy without tunneling or encryption. MPLS-enabled networks provide privacy on a network-by-network basis, much as Frame Relay or ATM provides it on a connection-by-connection basis. The Frame Relay or ATM VPN offers basic transport, whereas an MPLS-enabled network supports scalable VPN services and IP-based value added applications. This scenario upholds the shift in service provider business from a transport-oriented model to a service-focused one.

In MPLS-enabled VPNs, whether over an IP switched core or an ATM LSR switch core, the provider assigns each VPN a unique identifier called a route distinguisher (RD) that is different for each Intranet or Extranet within the provider network. Forwarding tables contain unique addresses, called VPN-IP addresses (see Figure 22-4), constructed by concatenating the RD with the customer IP address. VPN-IP addresses are unique for each endpoint in the network, and entries are stored in forwarding tables for each node in the VPN.

Figure 22-4 VPN-IP Address Format



RD	IP Address/Mask Length	General format
0.1.0.99	130.101.0.0/16	VPN-IPv4 example

RD is a 64-bit route distinguisher

- Never carried on packets, only in Label tables

Each customer network can use:

- Registered IP addresses
- Unregistered addresses

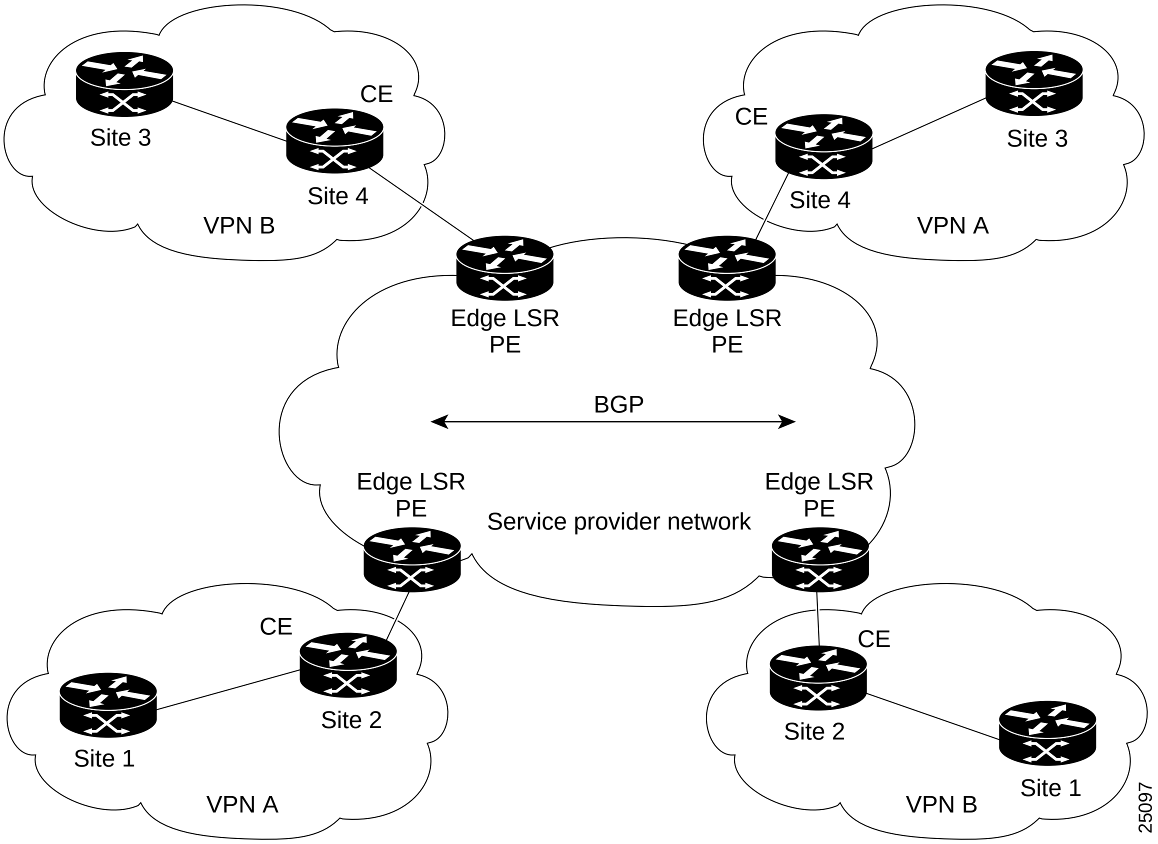
Private addresses (RFC 1918, for example, 10.x.x.x)

BGP Protocol

Border Gateway Protocol **(**BGP) is a routing information distribution protocol that defines who can talk to whom using multiprotocol extensions and community attributes. In an MPLS-enabled VPN, BGP distributes information about VPNs only to members of the same VPN, providing native security through traffic separation. Figure 22-5 shows an example of a service provider network with ATM backbone switches (P), service provider edge label switch routers (PE), and customer edge routers (CE).

Additional security is assured because all traffic is forwarded using LSPs, which define a specific path through the network that cannot be altered. This label-based paradigm is the same property that assures privacy in Frame Relay and ATM connections.

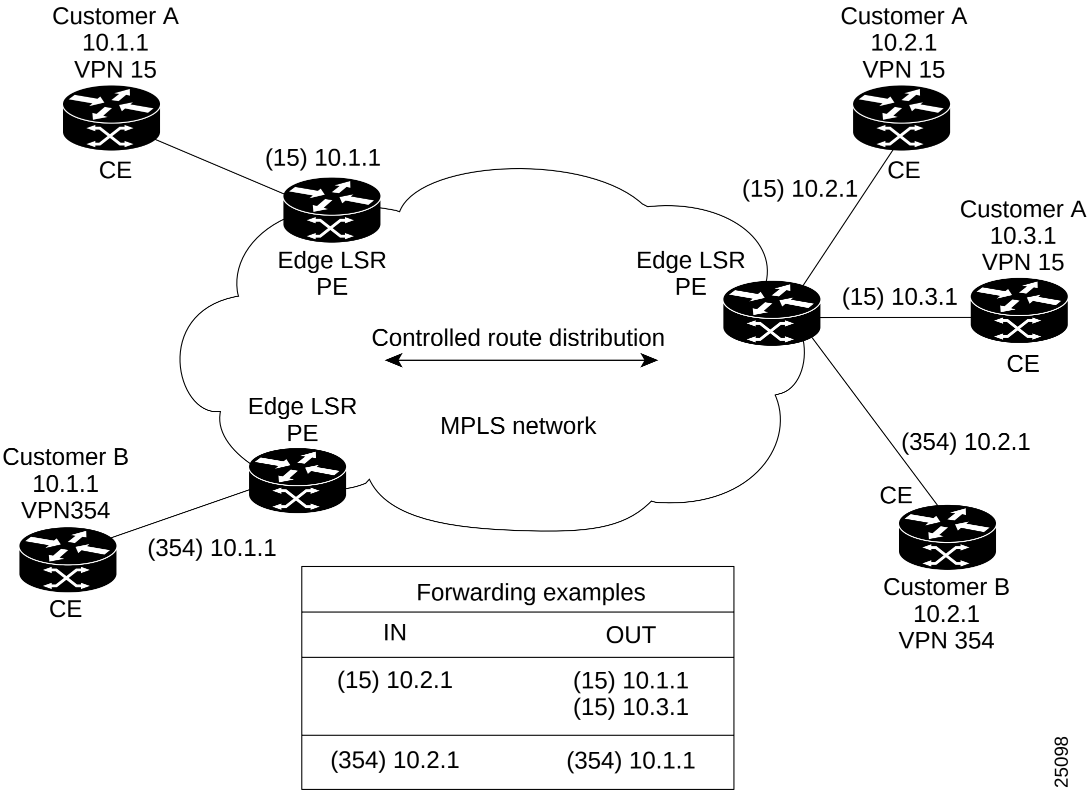
Figure 22-5 VPN with Service Provider Backbone



The provider, not the customer, associates a specific VPN with each interface when the VPN is provisioned. Within the provider network, RDs are associated with every packet, so VPNs cannot be penetrated by attempting to “spoof” a flow or packet. Users can participate in an Intranet or Extranet only if they reside on the correct physical port and have the proper RD. This setup makes Cisco MPLS-enabled VPNs virtually impossible to enter, and provides the same security levels users are accustomed to in a Frame Relay, leased-line, or ATM service.

PN-IP forwarding tables contain labels that correspond to VPN-IP addresses. These labels route traffic to each site in a VPN (see Figure 22-6). Because labels are used instead of IP addresses, customers can keep their private addressing schemes, within the corporate Internet, without requiring Network Address Translation (NAT) to pass traffic through the provider network. Traffic is separated between VPNs using a logically distinct forwarding table for each VPN. Based on the incoming interface, the switch selects a specific forwarding table, which lists only valid destinations in the VPN, as specified by BGP. To create Extranets, a provider explicitly configures reachability between VPNs. (NAT configurations may be required.)

Figure 22-6 Using MPLS to Build VPNs



Forwarding examples	
IN	OUT
(15) 10.2.1	(15) 10.1.1 (15) 10.3.1
(354) 10.2.1	(354) 10.1.1

One strength of MPLS is that providers can use the same infrastructure to support many VPNs, and do not need to build separate networks for each customer. VPNs loosely correspond to "subnets" of the provider network. Further, this solution has IP VPN capabilities built into the network itself, so providers can configure one network for all subscribers that delivers private IP network services such as Intranets and Extranets without complex management, tunnels, or VC meshes. Application-aware QoS makes it possible to apply customer-specific business policies to each VPN. Adding QoS services to MPLS-based VPNs works seamlessly, and the provider Edge LSR assigns correct priorities for each application within a VPN.

MPLS-enabled IP VPN networks are easier to integrate with IP-based customer networks. Subscribers can seamlessly interconnect with a provider service without changing their Intranet applications, because these networks have application awareness built in, for privacy, QoS, and any-to-any networking. Customers can even transparently use their private IP addresses without NAT.

The same infrastructure can support many VPNs for many customers, removing the burden of separately engineering a new network for each customer, as with overlay VPNs. It's also much easier to perform adds, moves, and changes. If a company wants to add a new site to a VPN, the service provider only has to tell the CPE router how to reach the network, and configure the LSR to recognize VPN membership of the CPE. BGP updates all VPN members automatically. This scenario is far easier, faster, and less expensive than building a new point-to-point VC mesh for each new site. Adding a new site to an overlay VPN entails updating the traffic matrix, provisioning point-to-point VCs from the new site to all existing sites, updating OSPF design for every site, and reconfiguring each CPE for the new topology.

MPLS VPN Operation

VRFs

Each VPN is associated with one or more VPN routing/forwarding instances (VRFs). A VRF table defines a VPN at a customer site attached to a PE router. A VRF table consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol variables that determine what goes into the forwarding table.

A 1 to 1 relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can be associated with one (and only one) VRF. A customer site's VRF contains all the routes available to the site from the VPNs of which it is a member.

Packet forwarding information is stored in the IP routing table and the CEF table for each VRF. (Together, these tables are analogous to the forwarding information base (FIB) used in Label Switching.) A logically separate set of routing and CEF tables is constructed for each VRF. These tables prevent information from being forwarded outside a VPN, and also prevents packets that are outside a VPN from being forwarded to a router within the VPN.

VPN Route Target Communities

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. Here is how distribution works:

- When a VPN route is injected into BGP, it is associated with a list of VPN route target extended communities. Typically the list of VPN communities is set through an export list of extended community-distinguishers associated with the VRF from which the route was learned.
- Associated with each VRF is an import list of route-target communities. This list defines the values to be verified by the VRF table before a route is eligible to be imported into the VPN routing instance. For example, if the import list for a particular VRF includes community-destinguishers of A, B, and C, then any VPN route that carries any of those extended community-destinguishers—A, B, *or* C—will be imported into the VRF.

IBGP Distribution of VPN Routing Information

A service provider edge (PE) router can learn an IP prefix from a customer edge (CE) router (by static configuration, through a Border Gateway Protocol (BGP) session with the CE router, or through the routing information protocol (RIP) with the CE router). Once it learns the prefix, the router generates a VPN-IPv4 (vpnv4) prefix based on the IP prefix by linking an 8-byte route distinguisher to the IP prefix. This extended VPN-IPv4 address uniquely identifies hosts within each VPN site, even if the site is using globally nonunique (unregistered private) IP addresses.

The route distinguisher (RD) used to generate the VPN-IPv4 prefix is specified by a configuration command on the PE.

BGP uses VPN-IPv4 addresses to distribute network reachability information for each VPN within the service provider network. BGP distributes routing information between IP domains (known as autonomous systems) using messages to build and maintain routing tables. BGP communication takes place at two levels: within the domain (interior BGP or IBGP) and between domains (external BGP or EBGP).

BGP propagates vpnv4 information using the BGP multiprotocol extensions for handling these extended addresses. (See RFC 2283, *Multiprotocol Extensions for BGP-4.)* BGP propagates reachability information (expressed as VPN-IPv4 addresses) among PE routers; the reachability information for a given VPN is propagated only to other members of that VPN. The BGP multiprotocol extensions identify the valid recipients for VPN routing information. All the members of the VPN learn routes to other members.

Label Forwarding

Based on the routing information stored in the IP routing table and the CEF table for each VRF, Cisco Label Switching uses extended VPN-IPv4 addresses to forward packets to their destinations.

A MPLS label is associated with each customer route. The PE router assigns the label that originated the route, and directs the data packets to the correct CE router. Label forwarding across the provider backbone, is based on either dynamic IP paths or Traffic Engineered paths. A customer data packet has two levels of labels attached when it is forwarded across the backbone: the top label directs the packet to the correct PE router, and the second label indicates how that PE router should forward the packet. The PE router associates each CE router with a forwarding table that contains only the set of routes that should be available to that CE router.

Quality of Service

As part of their VPN services, service providers may wish to offer premium services defined by SLAs to expedite traffic from certain customers or applications. QoS in IP networks gives devices the intelligence to preferentially handle traffic as dictated by network policy. QoS is defined as those mechanisms that give network managers the ability to control the mix of bandwidth, delay, jitter, and packet loss in the network. QoS is not a device feature, it is an end-to-end system architecture. A robust QoS solution includes a variety of technologies that interoperate to deliver scalable, media-independent services throughout the network, with system-wide performance monitoring capabilities.

Cisco’s comprehensive set of QoS capabilities enable providers to prioritize service classes, allocate bandwidth, avoid congestion, and link Layer 2 and Layer 3 QoS mechanisms. One of the best examples is committed access rate (CAR), which classifies packets by application and protocol, and specifies bandwidth allocation. Weighted fair queuing (WFQ) and class-based queuing (CBQ) techniques implement efficient bandwidth usage by always delivering mission-critical application traffic and deferring noncritical application traffic when necessary. Weighted random early detection (WRED) provides congestion avoidance to slow transmission rates before congestion occurs and ensures predictable service for mission-critical applications that require specific delivery guarantees.

MPLS makes it possible to apply scalable QoS across very large routed networks and Layer 3 IP QoS in ATM networks, because providers can designate sets of labels that correspond to service classes. In routed networks, MPLS-enabled QoS substantially reduces processing throughout the core for optimal performance. In ATM networks, MPLS makes end-to-end Layer 3-type services possible. Traditional ATM and Frame Relay networks implement CoS with point-to-point virtual circuits, but this is not scalable because of high provisioning and management overhead. Placing traffic into service classes at the edge enables providers to engineer and manage classes throughout the network. If service providers manage networks based on service classes, not point-to-point connections, they can substantially reduce the amount of detail they must track and increase efficiency without losing functionality. Compared to per-circuit management, MPLS-enabled CoS in ATM networks provides virtually all the benefits of point-to-point meshes with far less complexity. Using MPLS to establish IP CoS in ATM networks eliminates per-VC configuration. The entire network is easier to provision and engineer.

Security

Subscribers want assurance that their VPNs are in fact private and that their applications and communications are isolated and secure. Many robust security measures are available from Cisco to keep information confidential such as encrypted data, restricted access to authorized users, user tracking after they are connected to the network, and real-time intrusion auditing.

In Intranet and Extranet VPNs based on Cisco MPLS, packets are forwarded using a unique route distinguisher (RD). RDs are unknown to end users and uniquely assigned automatically when the VPN is provisioned. To participate in a VPN, a user must be attached to its associated logical port and have the correct RD. The RD is placed in packet headers to isolate traffic to specific VPN communities. MPLS packets are forwarded using labels attached in front of the IP header. Because the MPLS network does not read IP addresses in the packet header, it allows the same IP address space to be shared among different customers, simplifying IP address management. Service providers can deliver fully managed MPLS-based VPNs with the same level of security that users are accustomed to in Frame Relay/ATM services, without the complex provisioning associated with manually establishing PVCs and performing per-VPN customer premises equipment (CPE) router configuration. QoS addresses two fundamental requirements for applications that run on a VPN: predictable performance and policy implementation. Policies are used to assign resources to applications, project groups, or servers in a prioritized way. The increasing volume of network traffic, along with project-based requirements, results in the need for service providers to offer bandwidth control and to align their network policies with business policies in a dynamic, flexible way.

Manageability

As service providers build VPNs that include WAN switches, routers, firewalls, and Cisco IOS software, they need to seamlessly manage these devices across the network infrastructure and provide service-level agreements to their customers. They also need to enable business customers to personalize their access to network services and applications.

The Cisco Service Management System (CSM) addresses these needs with a suite of service management solutions to enable service providers to effectively plan, provision, operate, and bill VPN services.

Scalability

VPNs based on Cisco MPLS technology scale to support tens of thousands of business-quality VPNs over the same infrastructure. MPLS-based VPN services solve peer adjacency and scalability issues common to large virtual circuit (VC) and IP tunnel topologies. Complex permanent virtual circuit/switched virtual circuit (PVC/SVC) meshes are no longer needed, and providers can use new, sophisticated traffic engineering methods to select predetermined paths and deliver IP QoS to premium business applications and services.

Configuration, Example, and Commands

Perform the following tasks to configure and verify VPNs:

- Configuring BPX ATM LSR
- Configuring VRFs
- Configuring BGPs
- Configuring Import and Export Routes
- Verifying VPN Operation

Configuring the BPX 8650 ATM LSR

For MPLS VPN operation, the BPX 8650 ATM LSR, including its associated 7200 or 7500 LSC, are first configured for MPLS or for MPLS QoS. Configuration for network VPN operation takes place on the edge LSRs which act as PE routers. The BPX 8650, including its LSC, requires no configuration beyond enabling MPLS and QoS.

Configuring VRFs

To configure a VRF and associated interfaces, perform the following steps on the PE router:

Step	Command	Purpose
1	`Router(config)#` **`ip vrf`** *`vrf-name`*	Enter VRF configuration mode and specify the VRF name to which subsequent commands apply.
2	`Router(config-vrf)#` **`rd`** *`route-distinguisher`*	Define the instance by assigning a name and an 8-byte route distinguisher.
3	`Router(config-if)#` **`ip vrf`** *`forwarding vrf-name`*	Associate interfaces with the VRF.
4	`Router(config-router)#` **`address-family ipv4 vrf`** *`vrf-name`*	Configure BGP parameters for the VRF CE session to use BGP between the PE and VRF CE. **Note** The default setting is off for auto-summary and synchronization in the VRF address-family submode. **Note** To ensure that addresses learned through BGJP on a PE router from a CE router are properly treated as VPN IPv4 addresses, you must enter the command no bgp default ipv4-activate before configuring and CE neighbors.
5	`Router(config-router)#` **`address-family ipv4 vrf`** *`vrf-name`*	Configure RIP parameters for use between the PE and VRF CEs.
6	`Router(config-router-af)#` **`exit-address-family`**	Exit from address-family configuration mode.
7	`Router(config)# ip route [`**`vrf`** *`vrf-name`*`]`	Configure static routes for the VRF.

Configuring BGPs

To configure a BGP between provider routes for distribution of VPN routing information, perform the following steps on the PE router:

Step	Command	Purpose
1	Router(config-router)# **address-family** {**ipv4**|**vpn4**} [**unicast**|**multicast]**	Configure BGP address families.
2	Router(config-router-af)# **neighbor** {*address*|*peer-group*} **remote-as** *as-number*	Define a BGP session.
3	Router(config-router)# **no bgp default ipv4-activate**	Activate a BGP session. Prevents automatic advertisement of address family IPv4 for all neighbor.
4	Router(config-router)# **neighbor** *address* **remote-as** as-number	Configure a IBGP to exchange VPNv4 NLRIs.
5	Router(config-router)# **neighbor** *address* **update-source** *interface*	Define a IBGP session.
6	Router(config-router-af)# **neighbor** *address* **activate**	Activate the advertisement of VPNv4 NLRIs.

Configuring Import and Export Routes

To configure import and export routes to control the distribution of routing information, perform the following steps on the PE router:

Step	Command	Purpose
1	Router(config)# **ip vrf** *vrf-name*	Enter VRF configuration mode and specify a VRF.
2	Router(config-vrf)# **route-target import** *community-distinguisher*	Import routing information to the specified extended community.
3	Router(config-vrf)# **route-target export** *community-distinguisher*	Export routing information to the specified extended community.
4	Router(config-vrf)# **import map** *route-map*	Associate the specified route map with the VRF.

Verifying VPN Operation

To verify VPN operation, perform the following steps:

Step	Command	Purpose
1	Router# **show ip vrf**	Display the set of defined VRFs and interfaces.
2	Router# **show ip vrf detail**	Display VRF information including import and export community lists.
3	Router# **show ip route vrf** *vrf-name*	Display the IP routing table for a VRF.
4	Router# **show ip protocols vrf** *vrf-name*	Display the routing protocol information for a VRF.
5	Router# **show ip cef vrf** *vrf-name*	Display the CEF forwarding table associated with a VRF.
6	Router# **show ip interface** *interface-number*	Display the VRF table associated with an interface.
7	Router# **show ip bgp vpnv4 all** [**tags**]	Display VPNv4 NLRI information.
8	Router# **show tag-switching forwarding vrf** *vrf-name* [*prefix mask/length*][**detail**]	Display label forwarding entries that correspond to VRF routes advertised by this router.

Configuration Example

This section provides a sample configuration file from a PE router.

```
! CEF switching is a pre-requisite for Tag
ip cef distributed
frame-relay switching
!
! Define two VPN Routing instances, named ‘vrf1’ and ‘vrf2’
ip vrf vrf1 rd 100:1
ip vrf vrf2 rd 100:2
!
! Configure the import and export VPN route-target list for each VRF
ip vrf vrf1 route-target both 100:1
ip vrf vrf2 route-target both 100:2
ip vrf vrf2 route-target import 100:1
! Configure an import route-map for vrf2
ip vrf vrf2 import map vrf2_import
! ‘vrf2’ should not install PE-CE addresses in the global routing table
no ip vrf vrf2 global-connected-addresses
!
interface lo0
  ip address 10.13.0.13 255.255.255.255
 no shut
! Backbone link to another Provider router
interface atm9/0/0
 !
interface atm9/0/0.1 tag-switching
 tag-switching ip
ip unnumbered lo0
!
! Set up an Ethernet interface as a VRF link to a CE router
interface Ethernet5/0/1
 ip vrf forwarding vrf1
 ip address 10.20.0.13 255.255.255.0
 !
! Set up a Frame-Relay PVC sub-interface a link to another CE router
interface hssi 10/1/0
  hssi internal-clock
  encaps fr
  frame-relay intf-type dce
  frame-relay lmi-type ansi
!
interface hssi 10/1/0.16 point-to-point
  ip vrf forwarding vrf2
  ip address 10.20.1.13 255.255.255.0
  frame-relay interface-dlci 16
  !
! Configure BGP sessions
router bgp 1
! Define an IBGP session with another PE
  no bgp default ipv4-activate
  neighbor 10.15.0.15 remote-as 1
  neighbor 10.15.0.15 update-source lo0
  no synchronization
! Define some VRF (CE) sessions.
neighbor 10.20.1.11 remote-as 65535
  neighbor 10.20.1.11 update-source h10/1/0.16
! Deactivate the default IPv4 session
    neighbor 10.20.0.60 remote-as 65535
  neighbor 10.20.0.60 update-source e5/0/1
!
! Activate PE peer for exchange of VPNv4 NLRIs
  address-family vpnv4 unicast
```

```
   neighbor 10.15.0.15 activate
   exit-address-family
!
! If exchange of IPv4 NLRI with 10.15.0.15 is desired, activate it:
  address-family ipv4 unicast
   neighbor 10.15.0.15 activate
   exit-address-family
!
! Define BGP parameters for PE - CE sessions
! Activate sessions with peers in VRFs vrf1 and vrf2.
  address-family ipv4 unicast vrf vrf1
   neighbor 10.20.0.60 activate
   no auto-summary
   redistribute static
  exit-address-family
!
  address-family ipv4 unicast vrf vrf2
   neighbor 10.20.1.11 activate
   no auto-summary
   redistribute static
  exit-address-family
!
! Define a VRF static route
ip route vrf vrf1 12.0.0.0 255.0.0.0 e5/0/1 10.20.0.60
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS command references, for Cisco IOS commands, and in the *Cisco WAN Switch Command Reference* for BPX 8650 CLI commands. For information on using the following commands, refer to the *Cisco MPLS VPN Feature Guide*.

- address-family
- clear ip route vrf
- exit-address-family
- ip route vrf
- ip vrf forwarding
- ip vrf global-connected-addresses
- ip vrf
- neighbor activate
- show ip bgp vpnv4
- show ip cef vrf
- show ip protocols vrf
- show ip route vrf
- show ip vrf
- show tag-switching forwarding vrf

PART 6

Operation and Management

Cisco WAN Manager

The Cisco WAN Manager provides network management including, provisioning and monitoring, and statistis collection capabilities. The Cisco WAN Manager, also referred to as CWM, was formerly known as Cisco StrataView Plus. For further information, refer to the *Cisco WAN Manager Operations, Release 9.2* publication.

CiscoView

CiscoView provides network provisioning capabilites via a graphics user interface. For additional information, refer to the *WAN CiscoView for BPX 8600 Switches, Release 2.0* publication.

PART 7

Upgrades

Upgrading MPLS Networks to Switch SW Rel. 9.2 and BXM FW Rel. E

This chapter provides procedures to upgrade MPLS networks from BPX switch software Release 9.1 and BXM firmware Release C, to switch software Release 9.2.x and BXM Firmware Release E. The chapter contains the following:

- Introduction
- Upgrade Steps Required
- Compatibility
- Capabilities

Introduction

The procedure for upgrading Multiprotocol Label Switching (MPLS) (also referred to as *tag switching*) networks from BPX switch software Release 9.1 and BXM firmware Release C, to software Release 9.2.x and firmware Release E is not as automatic for this release as it is for other BPX 8600-series software and firmware upgrades. There is no backward compatibility between BXM firmware Release E and BXM firmware Release C with respect to Virtual Switch Interface (VSI) functionality. Therefore, for this release, a number of upgrade steps are required.

Upgrade Steps Required

The steps to upgrade from switch software Release 9.1 to Release 9.2 and the VSI configuration upgrade are described.

Upgrading from 9.1 to 9.2

1. Upgrade the Tag Switch Controller (TSC)

   The TSC is upgraded to CoS VSI Version capable release (IOS 12.XX). This image is VSI bilingual, meaning it understands both VSI Version 1 and Version 2.

2. Upgrade the BXMs

   All the BXM cards in the node are upgraded to Revision E, which is VSI Version 2 and CoS capable. After each BXM card is downloaded with the Revision E image, it temporarily experiences VSI outage until the BCC software is upgraded to the 9.2.x image. The VSI outage during the upgrade is caused by the Revision E firmware not being backward compatible with VSI Version 1 features.

   Note that from the TSC perspective, after a BXM is upgraded to Revision E image the interfaces that used to be on the card will “disappear.” The TDP sessions that were on the interfaces will be lost. When all the BXMs are upgraded to the Revision E while still running Release 9.1 software on the BCC, the node will experience a complete outage of MPLS traffic. Autoroute will have a hitless upgrade.

3. Upgrade the BCC

   As the BCC is upgraded from software Release 9.1 to Release 9.2.x, the BCC recognizes the Revision E BXMs and downloads the VSI partition configuration. This causes the BXMs to issue ifc cfg traps to the TSC, allowing the TSC to rediscover all the BPLS interfaces on the BPX. The TDP sessions are reestablished and BPLS traffic starts flowing again through the BPX.

VSI Configuration Upgrade

VSI configuration (VSI partition information and controllers) is maintained across the switch sw upgrade. A MPLS template is assigned to all interfaces in the switch, allowing the TSC to reassert the pre-upgrade connections without changes in the switch configuration. The MPLS template has the service-class to qbin mapping shown in Table 25-1.

Table 25-1 MPLS Template Service Class to Qbin Mapping

Service Class	VSI_ID	qbin
signalling	0x002	10
default	0x001	13
tag 0	0x200	10
tag 1	0x201	11
tag 2	0x202	12
tag 3	0x203	13
tag 4	0x204	10
tag 5	0x205	11
tag 6	0x206	12
tag 7	0x207	13
tag abr	0x210	14

In software Release 9.1, a qbin value of 10 was used for all VSI connections. The upgrade code specifically keeps the configuration of qbin=10 unchanged. This preserves the working configuration set up by the user using the **cnfqbin** command in Release 9.1. If the user wants to modify the configuration after the upgrade it can continue to use **cnfqbin** to do it. The command has been enhanced by the addition of an option to force the load of the values of the interface template to the given qbin configuration. All other qbins will be configured with qbin=10. In order to start using the qbin template, the user will need to execute **cnfqbin** to force the load of the values of the interface template.

Compatibility

Support for the VSI features in the BPX requires BCC-3-64 or BCC-4 (4 MB BRAM BCCs). VSI 9.2 features are first supported in Release 9.2.x. Support for the VSI 9.2 features requires switch software Release 9.2.x and firmware Release E. Firmware Release E is not backward compatible with respect to 9.1 VSI functionality. Since there is no backward compatibility with 9.1, and VSI 9.2 features are only available in 9.2.x. VSI 9.1 networks cannot be upgraded to 9.2 until the upgrade to 9.2.x is performed.

All BXMs slated for 9.2.x switch software must be first upgraded to use Revision E firmware. The BXM cards use the VSI protocol to communicate both with the VSI controller and among themselves. The BXM firmware Revision C supports VSI version 1 and Revision E supports VSI version 2. Both versions can communicate with the VSI controller that supports version 2, because the controller supports both versions simultaneously. However Revision E BXM firmware is *not* backward compatible and is therefore not able to interoperate with Revision C firmware. For this reason VSI connections cannot be established between BXMs running Revision C and Revision E. Switch software Release 9.2.x will mismatch BXM cards with firmware Revision C if VSI is configured on the slot. Switch software Release 9.2.x will block the user from enabling VSI on cards with firmware Revision C. Different nodes in the Multi Protocol Layer Switch Network may be running different switch software versions and therefore be operating with different VSI versions and different VSI features supported. The network application defines the limitations that must be enforced in a hybrid network of this kind.

Capabilities

VSI is considered configured on a given slot if at least one partition is enabled in the slot, or if a VSI controller is connected to a port in the slot. A summary of the firmware and switch software capabilities is shown in Table 25-2.

Table 25-2 Summary of Firmware and Switch Software Capabilities

Firmware Version	Switch Software	Release	Capabilities
C	9.1	9.1	Supports VSI 9.1 features and VSI protocol version 1
D	9.2.0	9.2	AutoRoute only release
E	9.2.X	9.2.X	Supports VSI 9.2 features and VSI protocol version 2

VSI 9.2 features refer to:

- VSI 2.x protocol
- Service templates
- Full QoS for MPLS and ATM Forum service classes
- Master redundancy
- VSI support on virtual trunk interfaces
- CWM support for VSI on BPX slave redundancy

PART 8

Reference

Cisco Cabinet Dimensions

This appendix illustrates typical cable management and space requirements for various system configurations in the Cisco cabinet. It also contains a table with the height of Cisco components in inches, centimeters, and rack-mount units (RMUs). This can help in the calculation of height requirements for individual setups. The last illustration shows the bracket installation in the Cisco (for a BPX switch, in this case). The information is grouped as follows:

- Cisco Cabinet and Component Heights
- Cisco Cabinet
- Cable Management
- Examples of BPX 8600 Series Switch Configurations
- Examples of IGX 8400 Series Switch Configurations

Cisco Cabinet and Component Heights

Table A-1 lists Cisco cabinet dimensions and the heights of components that may be installed in the cabinet.

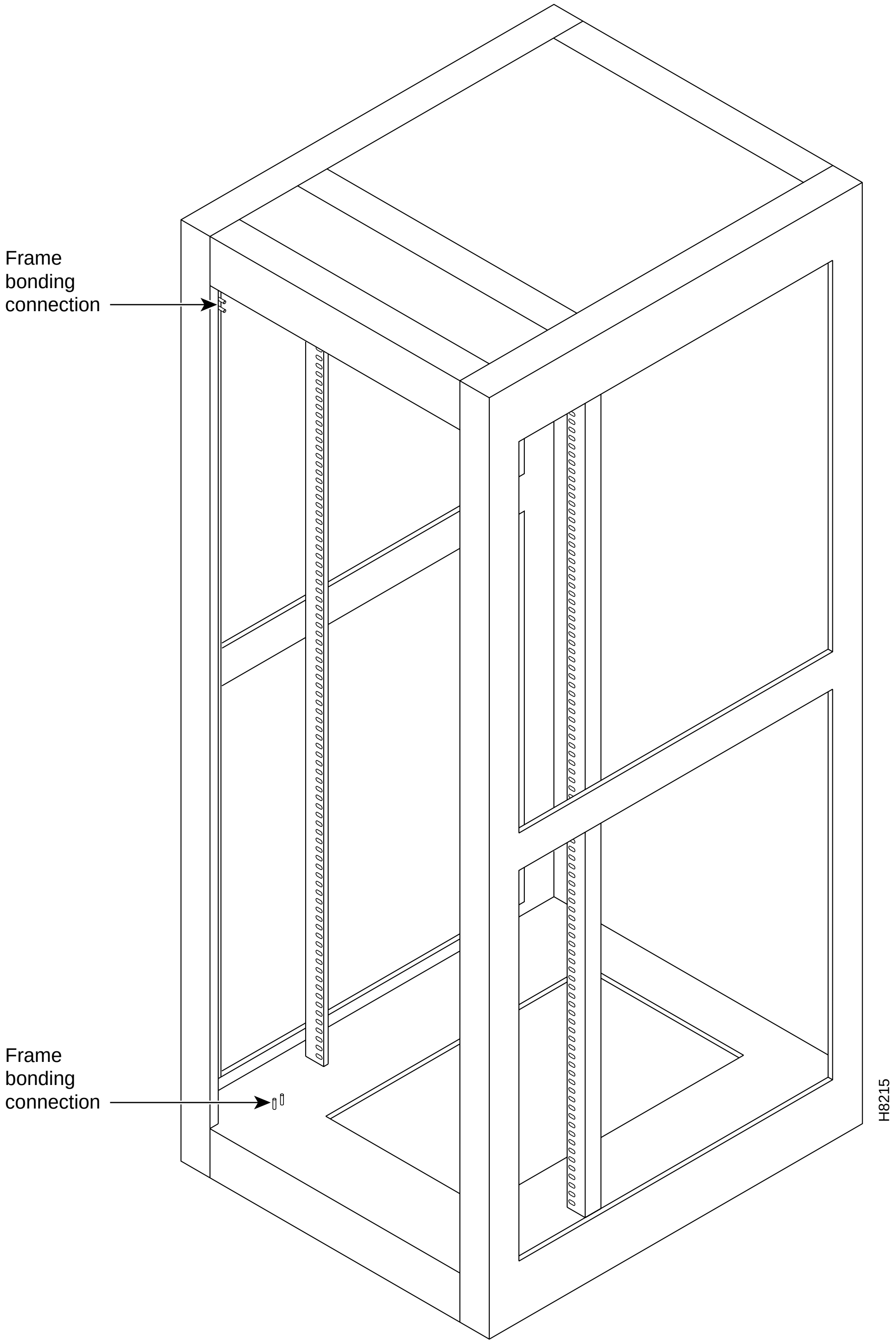
Table A-1 Table of Cisco Cabinet and Component Heights

	Unit Height		
Components	**Inches**	**CM**	**RMUs**
MGX 8220 Card Cage	8.75	22.225	5
MGX 8220 AC Power Supply shelf	5.25	13.335	3
MGX 8220 Booster Fan Assembly	3.5	8.89	2
MGX 8220 Cooling Assembly	5.25	13.335	3
MGX 8220 Exhaust Plenum	3.5	8.89	2
BPX switch AC Power Supply shelf	5.25	13.335	3
BPX switch Card Cage	22.75	57.785	13
IGX switch AC Power Supply shelf	5.25	13.335	3
IGX switch Booster Fan Assembly	3.5	8.89	2
IGX switch Card Cage	17.5	44.45	10
IGX switch Cooling Assembly	5.25	13.335	3
IGX switch Exhaust Plenum	3.5	8.89	2
IGX 8410 switch	24.5	62.23	14
DAS, VNS, and ESP	5.25	13.335	3
	Unit Height		
Cabinet	**Inches**	**CM**	**RMUs**
Cisco Cabinet	71.75	1822.45	41

Cisco Cabinet

Figure A-1 shows a back view of an empty Cisco cabinet.

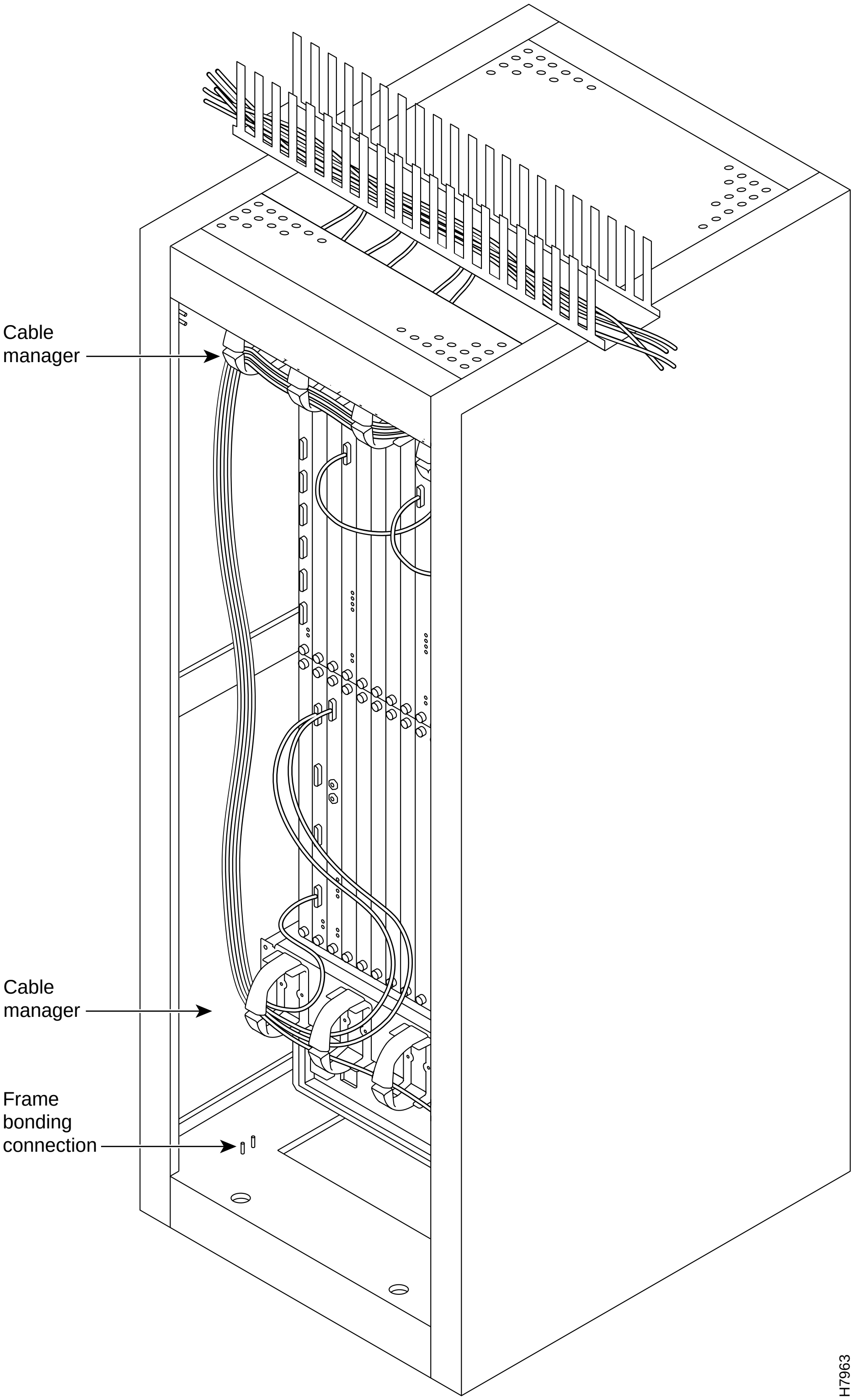
Figure A-1 Back View of Empty Cisco Cabinet



Cable Management

Figure A-2 shows a typical cable management configuration for an IGX-32 switch in a Cisco cabinet.

Figure A-2 Typical Cable Management, IGX-32 Switch in Cisco Cabinet



Examples of BPX 8600 Series Switch Configurations

Figure A-3 through Figure A-9 show various BPX switch configurations.

Figure A-3 Single BPX Switch, DC and AC Systems

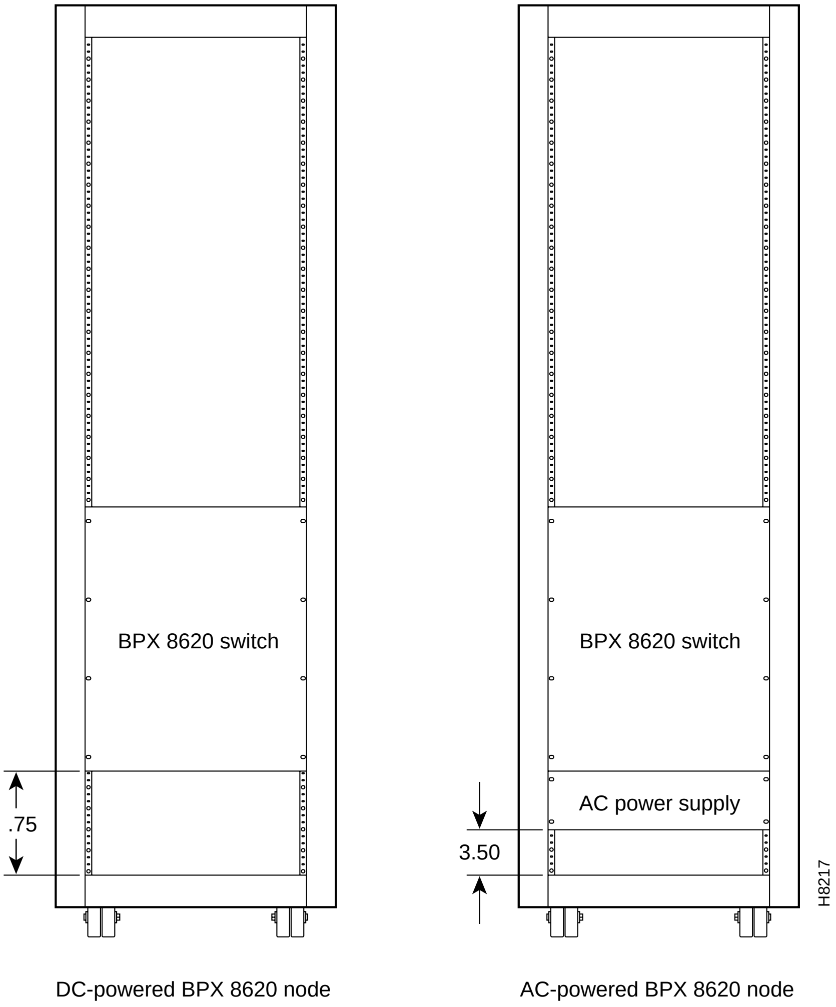


Figure A-4 Single BPX Switch and MGX 8220, DC and AC Systems

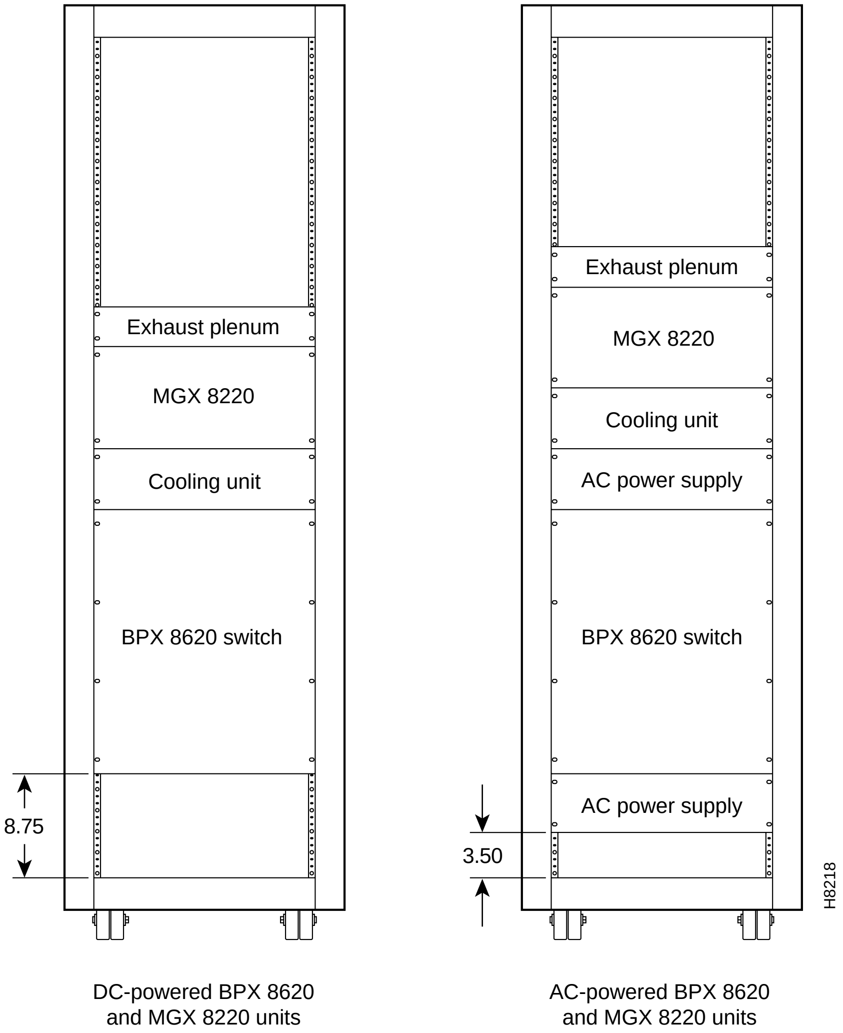


Figure A-5 BPX Switch, MGX 8220, and ESP, DC and AC Systems

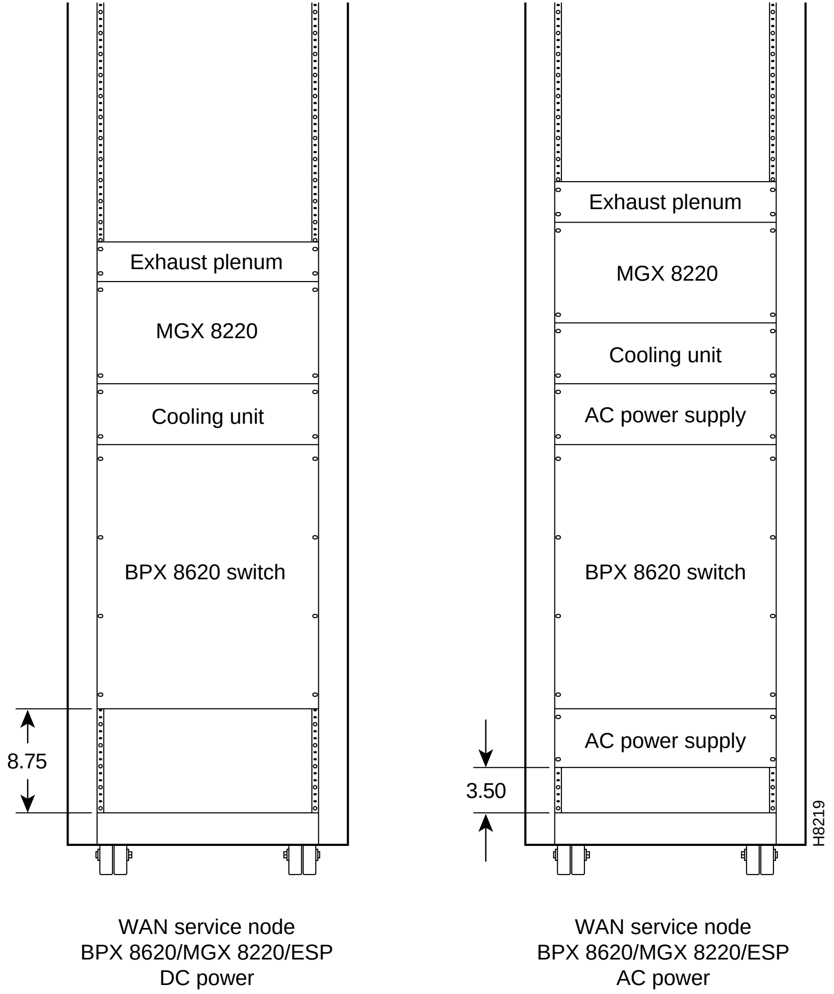
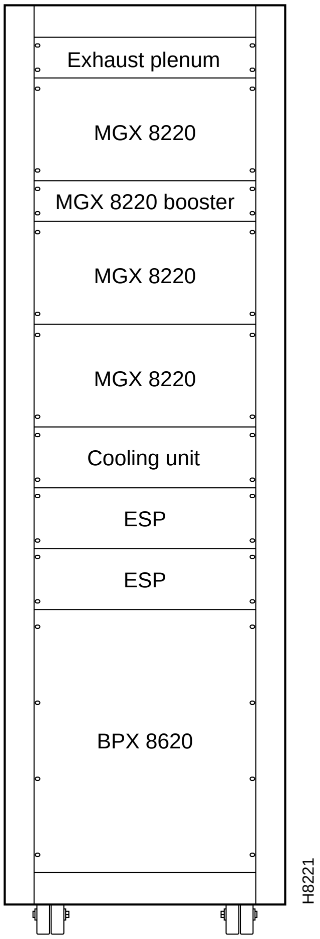
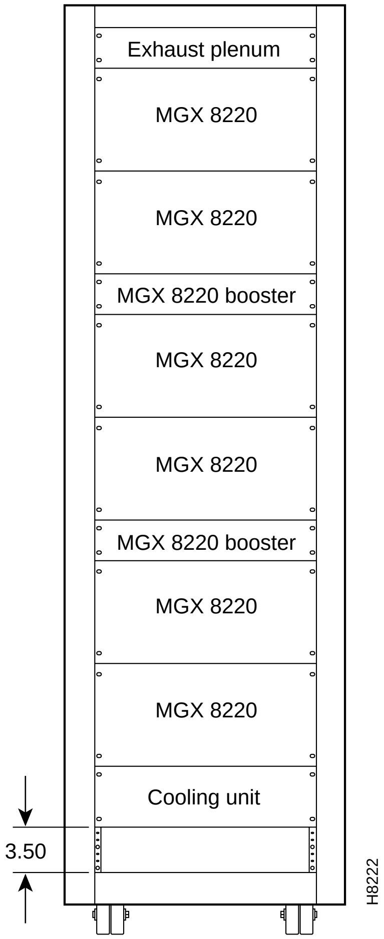


Figure A-6 BPX Switch With 2 ESP and 3 MGX 8220, DC System



WAN Service Node
BPX 8620/MGX 8220/ESP
DC power

Figure A-7 Six MGX 8220, DC System



Six MGX 8220 edge concentrators

Figure A-8 BPX Switch with Three MGX 8220s, DC System

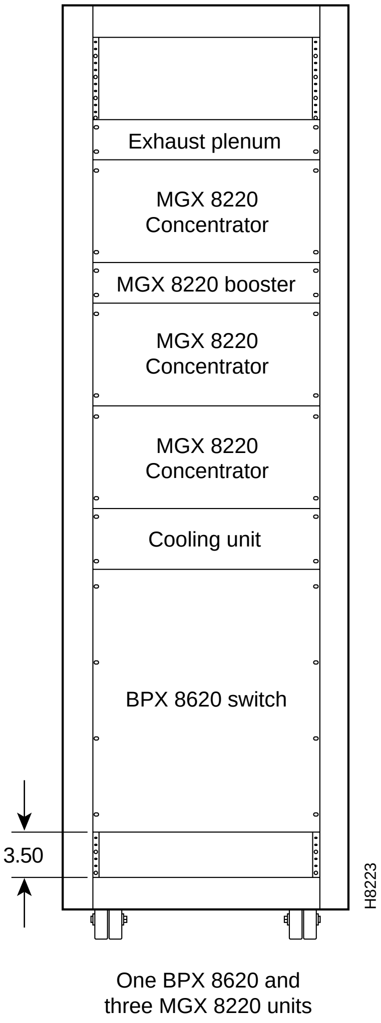
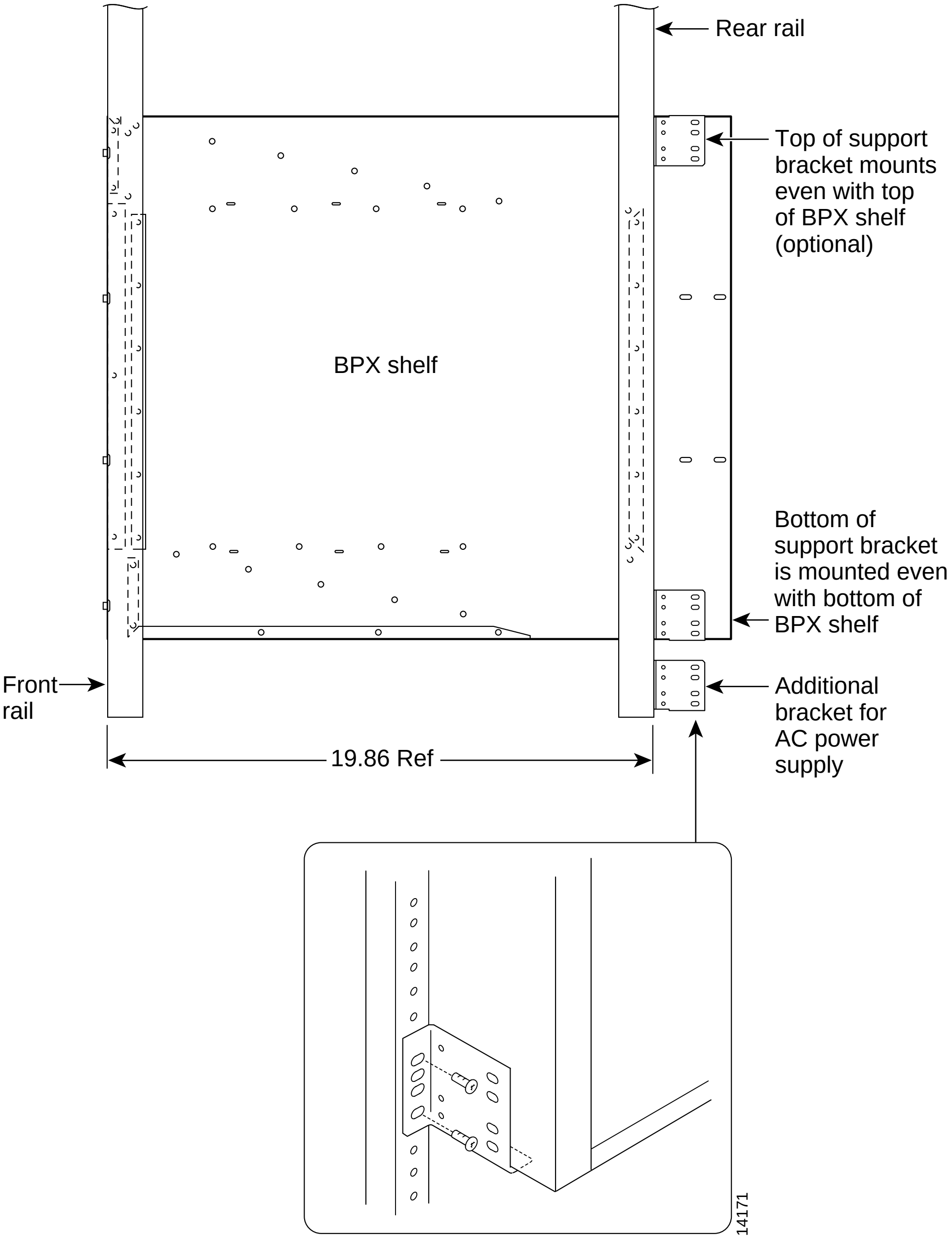


Figure A-9 Mounting Brackets (BPX switch), Standard Configuration


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

Examples of IGX 8400 Series Switch Configurations

Figure A-10 through Figure A-12 show various IGX switch configurations.

Figure A-10 IGX 8430 Switch, DC and AC Systems

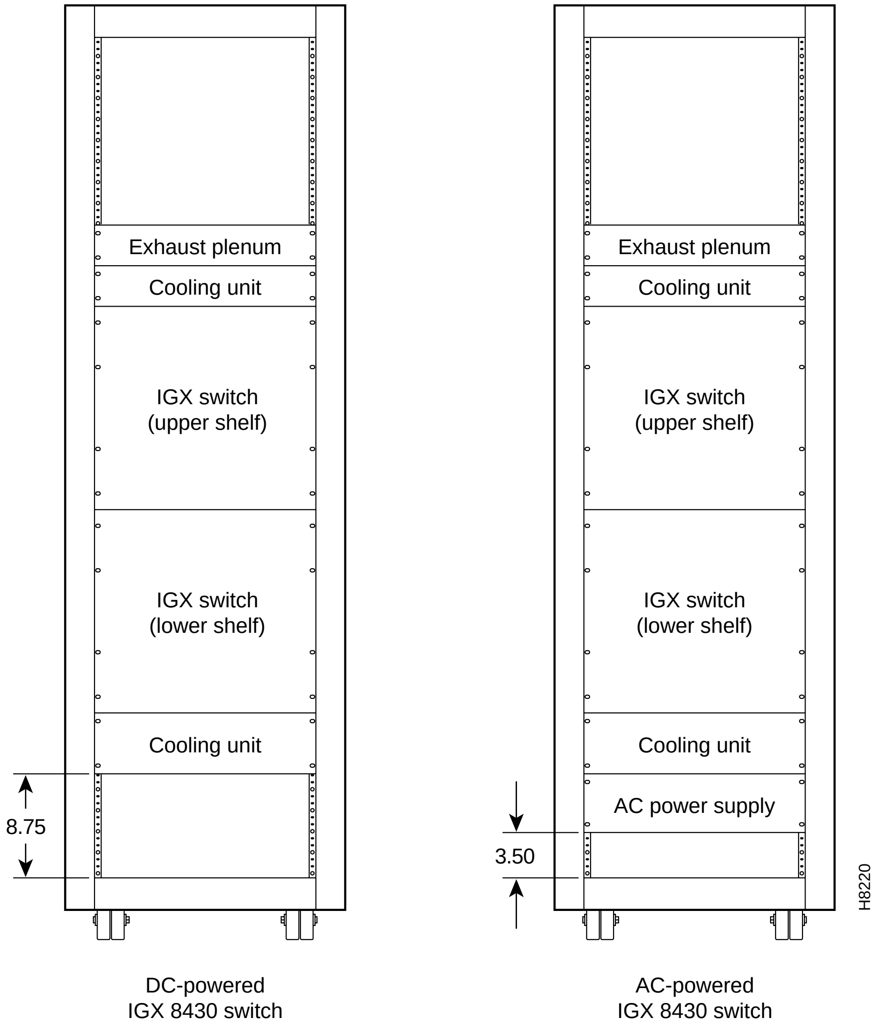


Figure A-11 Single IGX 8420 Switch, DC and AC Systems

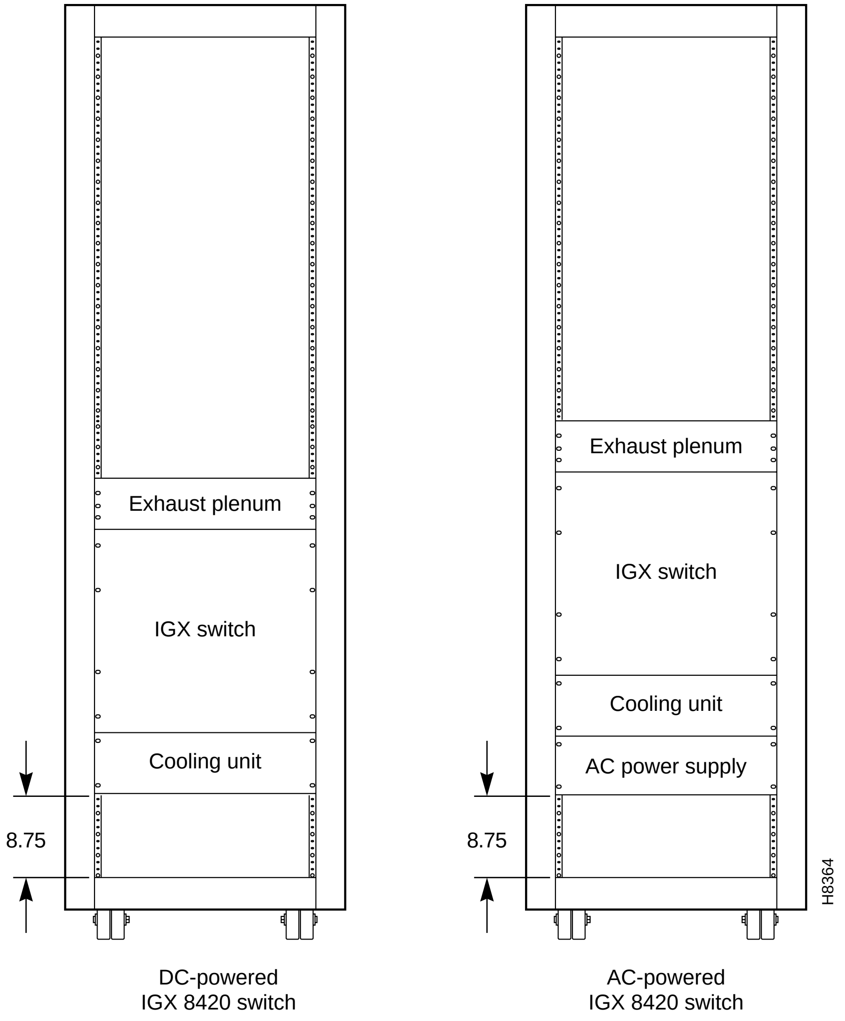
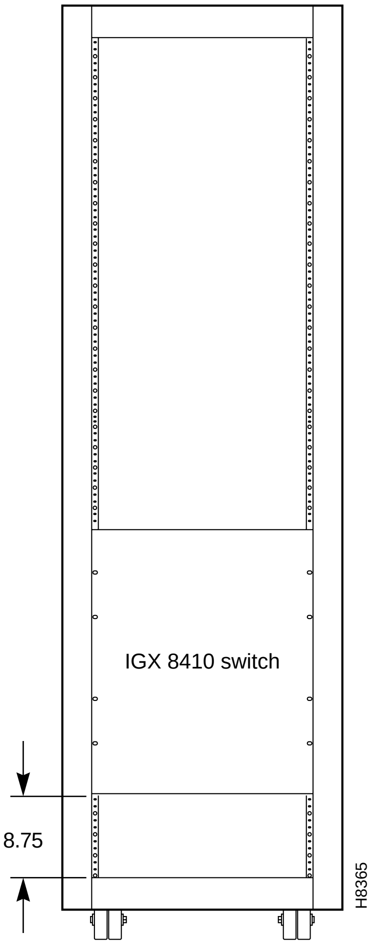


Figure A-12 Single IGX 8410 switch, DC or AC System



AC or DC-powered
IGX 8410 switch

BPX Switch Cabling Summary

This appendix provides details on the cabling required to install the BPX switch.

Note In all cable references, the transmit direction is from the BPX switch, receive 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. Refer to Table B-1 for details.

Table B-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. Refer to Table B-2 and Table B-3 for acceptable cable and wire types.

AC Powered Nodes

AC power cables may be provided by the customer or ordered from Cisco. Several standard cables are available (see Table B-2). AC cables with other plugs or different lengths may be special ordered. For users who wish to construct their own power cable, the cable must mate with an IEC320 16/20A male receptacle on rear of the AC Power Supply Assembly.

Table B-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) 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 (see Table B-3) is generally provided by the customer.

Table B-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

This cabling connects data ports on the LM-BCC to control terminals and modems. It is also used for external clock inputs from a clock source. See *Appendix C, BPX Switch Cabling Summary*, 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 or modem connections for remote alarm reporting or system monitoring. Refer to Table B-4 and Table B-5 for details on this cable.

Table B-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 B-5 contains a list of the port pin assignments.
Max. Cable Length:	50 feet (15 m.)

Table B-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 B-6 and Table B-7 for details.

Table B-6 LAN Port Cabling

Cable Parameter	Description
Interface:	Ethernet DCE port.
Cable Connector:	DB-15, subminiature, male. Table B-7 contains a list of the port pin assignments.
Max. Cable Length:	50 feet (15 m.) max. to interface adapter.

Table B-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 *Appendix C, BPX Switch Peripherals*, for modem cabling information.

External Clock Input Cabling

This cabling is for making external clock connections for use by the BCC-32, BCC-3, and BCC-4 backcards. The BCC-32 uses the BCC-bc backcard, and the BCC-3 and BCC-4 both use the BCC-3-bc backcard.

T1 Clock Cabling

Table B-8 through Table B-11 lists T1 clock cabling details.

Table B-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 B-10 through Table B-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 B-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 B-10 T1 Connection to EXT TMG on BCC-bc

Pin #	Description
2	Receive pair shield
3	Receive tip
11	Receive Ring

Table B-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 B-12 through Table B-15 lists E1 clock cabling details.

Table B-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 B-13 and Table B-15 for pinouts.
Max. Cable Length:	Approx. 100 meters maximum between the BPX switch and the first repeater or CSU. Equalizer for cable length.

Table B-13 E1 Connection 75 Ohm to EXT TMG on BCC-bc or BCC-3-bc

Connector	Description
BNC	Receive E1 from trunk

Table B-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 B-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 (see Table B-16) is for connecting network alarm outputs to the LM-ASM ALARM OUTPUT connector only. Table B-17 lists the pinouts for the network alarm outputs.

Table B-16 External Alarm Cabling

Cable Parameter	Description
Interface:	Dry-contact relay closure
Wire:	24 AWG, shielded, 6-pair
Connector:	DB-15, Subminiature, male

Table B-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 B-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.) and 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) will be 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 B-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 B-19 lists the Y-cables used with various BPX switch back cards.

Table B-19 Redundancy Y-Cables

Y - Cable	Used On
T3 trunk	LM-3T3
E3 trunk	LM-3E3
Aux./Cont. ports	LM-BCC
Ext. Clk. In	LM-BCC
Ext. Clk. Out	LM-BCC

BPX Switch Peripherals

This appendix provide details on BPX switch peripheral equipment, including printers and modems. The appendix includes the following sections:

- Network Management
- Printer
- Modems, Dial-In and Dial-Out

Network Management

StrataView Plus Terminal

A StrataView Plus workstation is recommended for managing a network containing IPX, IGX, and BPX switch. Refer to the *StrataView Plus Operation Manual* and *StrataView Plus Installation Manual* for setup instructions and specifications for the StrataView Plus NMS, which is required to provide network alarm, control, and statistics monitoring. Connection of a StrataView Plus workstation for network management is described in *Chapter 9, Finishing the Installation and Power-Up*.

Note For network management, a StrataView Plus workstation is connected to the LAN port of one or more network nodes, typically BPX switches because of their processing power, to provide network management.

Control Port, Local Control

A terminal (pc or workstation, including a StrataView Plus workstation) can be connected to the CONTROL port of a BPX switch for temporary or local control. This can be especially useful during installation, initial power-up, and configuration. Refer to Table C-1 for configuration data for the BPX CONTROL port.

Table C-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.

Printer

An optional maintenance printer for the BPX switch is the Okidata Model 184 dot matrix printer. This printer may be connected to any node. Refer to Table C-2 and Table C-3 for printer configuration requirements. Note that this is not the same as the printer that may be provided with the StrataView Plus NMS terminal but in addition to it.

Table C-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. Access to the configuration switches is made by sliding back the switch cover at the top, rear of the printer case. Set Switch A as indicated in Table C-3.

Table C-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.

Table C-3 Switch A Settings —Okidata 184 Printer

Switch A	Setting	Description
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 that is attached to the printer's main board. Set switches 1 and 2 as indicated in Table C-4 and Table C-5.

Table C-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 C-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.

Modems, Dial-In and Dial-Out

Customer service uses modems for diagnosing and correcting customer problems with installed BPX switches. The modem that is currently recommended for use with the BPX switch is the Codex Model V.34R.

A dial-in connection to a BPX switch RS-232 from customer service via a modem uses the CONTROL port of the BPX switch. A dial-out connection from a BPX switch via a modem to customer service uses the AUXILIARY port of the BPX switch. See Table C-6 for interface requirements.

Table C-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.

Motorola V.34R BPX Switch Dial-In Configuration

BPX Switch Auto-Answer (Dial-In to BPX switch)

The following is a setup procedure that allows customer service to dial in to the customer's 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 C-7 to set up the modem for proper operation.

Note Consult the manual that is supplied with your modem for specific information concerning the modem configuration. Call customer service for latest modem configuration information.

Step 5 Disconnect the terminal and the straight-through cable from the BPX CONTROL port.

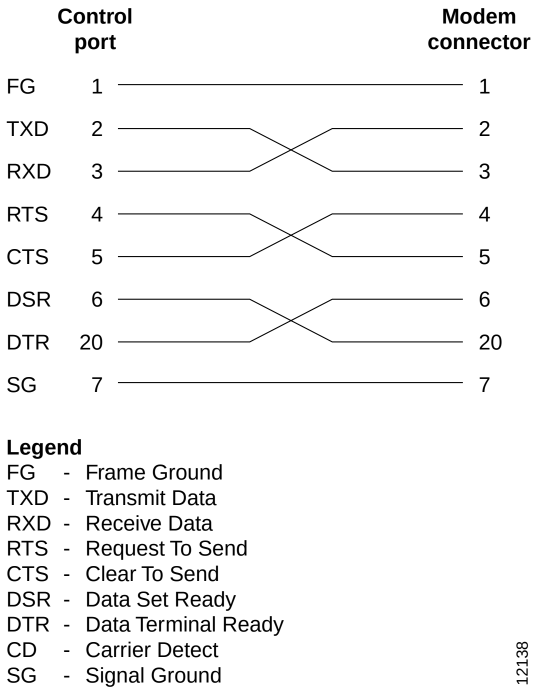
Step 6 Connect the modem to the BPX CONTROL port using a null-modem cables Figure C-1. A null modem cable is used, as the connection is essentially a DCE to DCE rather than a DTE to DCE connection.

Step 7 Ask customer service to assist in testing the operation of the modem setup.

Table C-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 C-1 Dial-Modem Cabling for Auto Answer (Dial-In to BPX)



IPX Auto-Dial to Customer Service

The following is a setup procedure for the customer's BPX to dial up customer service.

Step 1 Using the **cnfterm** command, set the BPX AUXILIARY port speed to 9600 bps and enable XON/XOFF flow control.

Step 2 Using the **cnftermfunc** command, select option 7, "Autodial Modem" and enter the customer service-designated Network ID, and the customer service modem phone number.

Step 3 Attach a 9600 bps terminal to the modem 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 C-8 (V.34R modem without talk/data pushbutton) or Table C-9 (V.34R modem with talk/data pushbutton), to set up the modem for proper operation.

Note Consult the manual that is supplied with your modem for specific information concerning the modem configuration. Call customer service for latest modem configuration information.

Step 5 Disconnect the terminal and the straight-through cable from the IPX CONTROL port.

Step 6 Connect the modem to the IPX AUX port using a null modem cable (see Figure C-2).

Step 7 Ask customer service to assist in testing the operation of the modem setup.

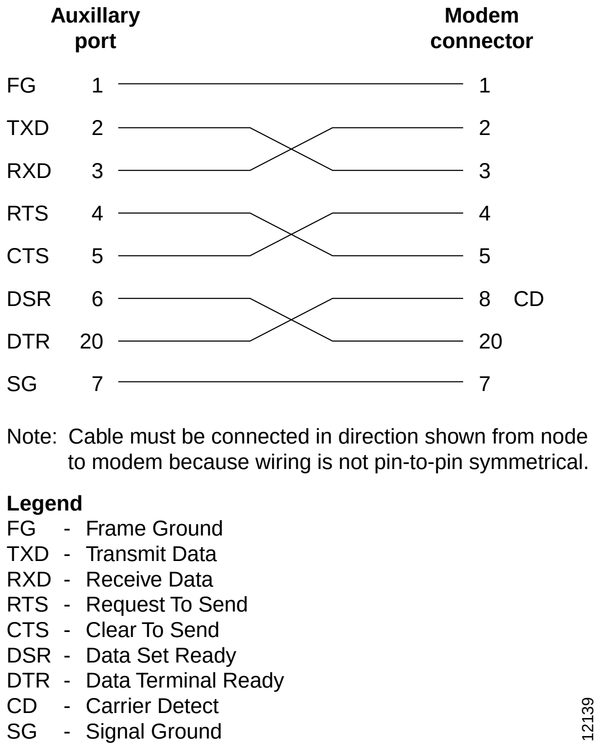
Table C-8 V.34R Auto-Dial Configuration (dial-out to customer service)*

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 IPX toggles DTR.
10.	AT&V	Verify entries.
11.	AT&W	Saves current settings to non-volatile memory.

Table C-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 IPX toggles DTR.
10.	AT&V	Verify entries. *(shows current configuration)*
11.	AT&W	Saves current settings to non-volatile memory.

Figure C-2 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