Cisco BPX 8600 Series Reference

Release 9.2
October 1999

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: 78-6325-03

Cisco BPX 8600 Series Reference, Release 9.2

Feedback on the Cisco BPX 8600 Series Reference, Release 9.2, October 1999, Part No. 78-6325-04

78-6721-02

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 Reference, Release 9.2, October 1999, Part No. 78-6325-04

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 2

General Description

Chapter 3

PART 3

Service and Trunk Cards

Chapter 4

Chapter 8

PART 7

Reference

Appendix A

BPX Node Specifications A-1

Appendix B

BPX Switch Cabling Summary B-1

Appendix C

BPX Switch Peripherals C-1

LIST OF FIGURES

LIST OF TABLES

About This Manual

This publication provides an overview of the operation of the BPX 8600 Series wide-area switches which include the BPX 8620 switch and the BPX 8650 tag switch. Refer to 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 up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

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

Objectives

This publication is intended to provide reference information useful during installation, configuration, operation, and maintenance of the BPX 8600 Series.

Audience

This publication is intended for installers, operators, network designers, and system administrators.

Cisco WAN Switching Product Name Change

The Cisco WAN Switching products have new names. A switch in the BPX family is now part of the Cisco BPX® 8600 Series wide area switch family. 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-wide area switch. The IGX 8 switch is now called the Cisco IGX™ 8410 wide-area switch. The IGX 16 switch is now called the Cisco IGX™ 8420 wide-area switch, and the IGX 32 switch is now called the Cisco IGX™ 8430 wide-area switch.

Organization

This publication is organized as follows:

PART 1 **Overview**

Chapter 1 **Introduction**

Describes the overall operation of the BPX 8600 Series wide-area switches and associated peripherals.

Chapter 2 **BPX Switch**

Provides an overall physical and functional description of the BPX switch. The physical description includes the BPX enclosure, power, and cooling subsystems. The functional description includes an overview of BPX switch operation.

PART 2 **General Description**

Chapter 3 **BPX Switch Common Core**

Describes the common core group, comprising the Broadband Controller Cards (BCCs), the Alarm/Status Monitor (ASM) card, associated backcards, and the StrataBus backplane.

PART 3 **Service and Trunk Cards**

Chapter 4 **BNI (Trunk) Cards**

Describes the Broadband Network Interface (BNI) trunk card and associated backcards.

Chapter 5 **ASI Service Interface (Line) Cards**

Describes the ATM Service Interface (ASI) line card and associated backcards.

Chapter 6 **BXM T3/E3, 155, and 622**

Describes the BXM card group which includes the BXM-T3/E3, BXM-155, and BXM-622 card sets. Describes the operation of these cards in either trunk or service mode.

PART 4 **Functional Descriptions, General**

Chapter 7 **BXM Virtual Trunks**

Provides a description of BXM virtual trunks, a feature supported by the BXM cards beginning with switch software Release 9.2

Chapter 8 **ATM Connections**

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.

Chapter 9 **SONET APS**

Provides a description of the SONET Automatic Protection System (APS) which may be used to provide line and card redundancy for BXM SMF and SMF LR OC-3 and OC-12 cards.

Chapter 10 **ATM and Frame Relay SVCs, and SPVCs**

Provides a summary of switched virtual circuits and soft permanent virtual circuits with respect to the BPX switch and co-located Extended Services Processor. For additional information, refer to the *Cisco WAN Service Node Extended Processor Installation and Operation Release 2.2* document.

Chapter 11 **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

Chapter 12 **BME Multicasting**

Provides a description of BME multicasting and configuration examples.

Chapter 13 **Frame Relay to ATM Network and Service Interworking**

Describes Frame Relay to ATM interworking which allows users to retain their existing Frame Relay services, and as their needs expand, migrate to the higher bandwidth capabilities provided by BPX ATM networks. Frame Relay to ATM Interworking enables Frame Relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking.

Chapter 14 **Tiered Networks**

Describes the tiered network configuration that provides the capability of adding interface shelves/feeders (non-routing nodes) to an IPX/IGX/BPX routing network.

Chapter 15 **BPX SNMP Agent**

Introduces the functions of the Simple Network Management Protocol (SNMP) agent and MIBs that are embedded in each BPX switch.

PART 5 **MPLS**

Chapter 16 **MPLS on BPX Switch**

Provides a summary of label switching on the BPX 8650 where the BPX switch and associated series 7200 or 7500 router comprise a BPX 8650 Label Switch Router. Also provides configuration examples.

Chapter 18 **MPLS CoS with BPX 8650**

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

Related Documentation

The following Cisco WAN Switching publications contain additional information related to the installation and operation of the BPX switch and associated equipment:

- *Cisco WAN Manager Guide* provides 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/IPX/BPX Documentation Set, includes:
    - *Cisco BPX 8600 Series Installation and Configuration* provides installation and configuration instructions for the BPX broadband node.
    - *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 the command line interface 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

Overview

Introduction

This chapter contains an overall description of the BPX 8600 Series. For installation information, refer to the *Cisco BPX 8600 Series Installation and Configuration* publication. Also, refer to the *Cisco WAN Switching Command Reference* publications. Refer to 9.2 Release Notes for supported features.

This chapter contains the following:

- General Description
- New with Release 9.2
- Continuing Features with Release 9.2
- BPX Switch Operation
- Traffic and Congestion Management
- Network Management
- Switch Software Description
- Network Synchronization
- Switch Availability

General Description

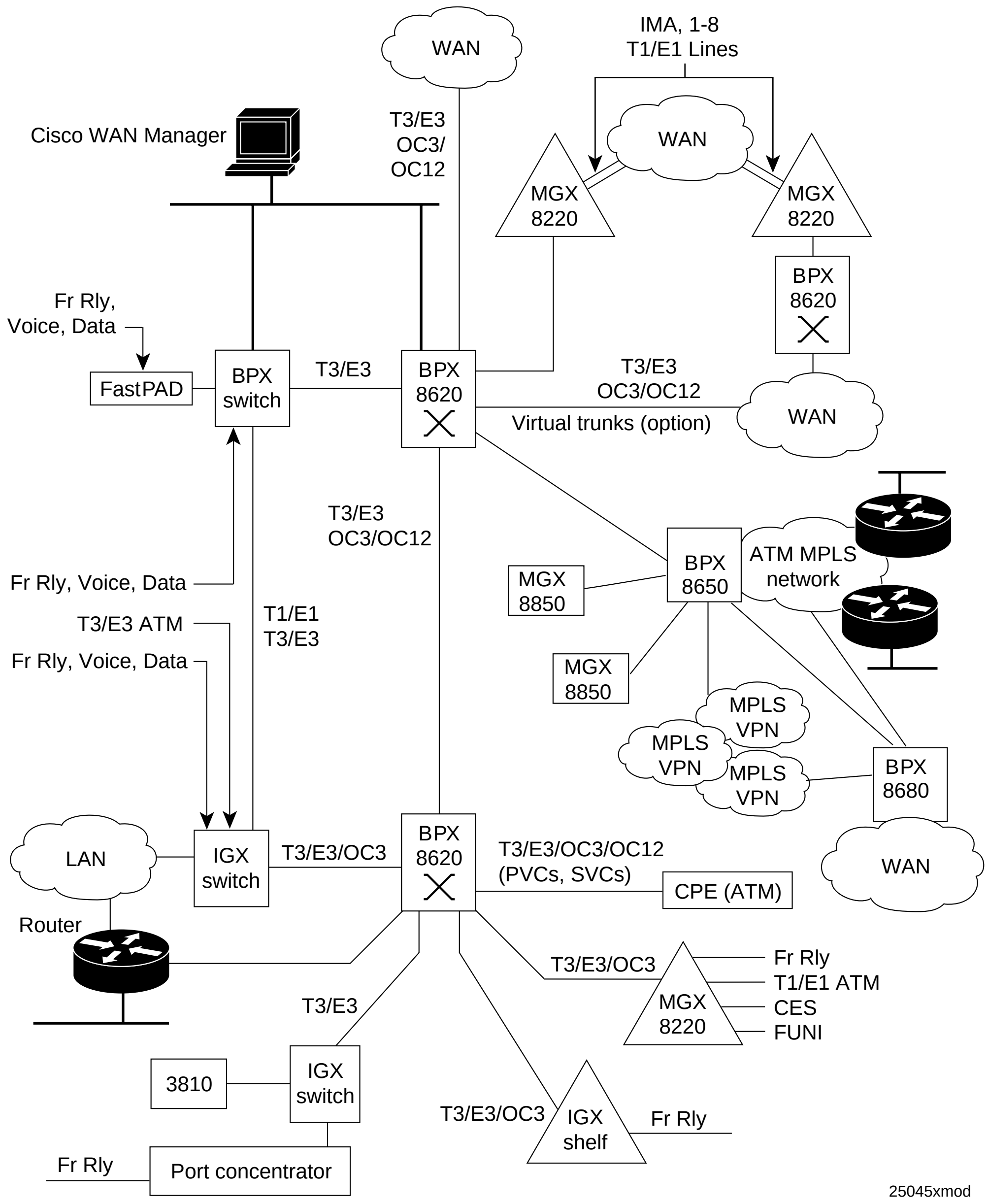
The Cisco BPX® 8600 Series wide-area switches are standards based high-capacity broadband ATM switches that provide backbone ATM switching, IP + ATM services including Multiprotocol Label Switching (MPLS) and deliver a wide range of other user services (see Figure 1-1). The BPX 8600 Series includes the BPX 8620 wide-area switch, the BPX 8650 IP + ATM switch, and the BPX 8680 universal service switch.

BPX 8620

Fully compatible with the Cisco MGX™ 8800 series wide area edge switch, MGX 8220 edge concentrator, the Cisco IGX™ 8400 series wide-area switch, the BPX 8620 switch is a scalable, standards-compliant unit. Using a multi-shelf architecture, the BPX switch supports both narrowband and broadband user services. The modular, multi-shelf architecture enables users to incrementally expand the capacity of the system as needed. The BPX switch consists of the BPX shelf with fifteen card slots which may be co-located with the MGX 8220 and Extended Services Processor (ESP), as required.

Three of the slots on the BPX switch shelf are reserved for common equipment cards. The other twelve are general purpose slots used for network interface cards or service interface cards. The cards are provided in sets, consisting of a front card and associated back card. The BPX shelf can be mounted in a rack enclosure which provides mounting for a co-located ESP and the MGX 8220 interface shelves.

Figure 1-1 BPX Switch General Configuration Example



BPX 8650

The BPX® 8650 is an IP+ATM switch that provides ATM-based broadband services and integrates Cisco IOS® software via Cisco 7200 series routers to deliver Multiprotocol Label Switching (MPLS) services. The BPX 8650 provides the core Internet requirements of scalability, advanced IP services, Layer 2 virtual circuit switching advantages, and Layer 2/Layer 3 interoperability. In addition to scaling Internet services, the BPX 8650 switch enables the user to provision new integrated IP+ATM services such as voice over IP, MPLS virtual private networks (VPNs), and Web hosting services across the ATM backbone.

BPX 8680

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

The BPX 8680 switch incorporates a modular, multishelf architecture that scales from small sites to very large sites and enables service providers to meet the rapidly growing demand for IP applications while cost-effectively delivering today's services. The BPX 8680 consists of one or more MGX 8850s connected as feeders to a BPX 8620. Designed for very large installations, the BPX 8680 can scale to 16,000 DS1s by adding up to 16 MGX 8850 concentrator shelves while still being managed as a single node.

New with Release 9.2

With Release 9.2, the BPX supports a number of new features:

VSI Enhancements

With Release 9.2, virtual switch interfaces (VSIs) can be configured on a BXM virtual trunk. The BXM previously did not support virtual trunks. MPLS switching can be enabled on a virtual trunk VSI in a similar manner to a standard trunk or port.

MPLS Class of Service (CoS) templates simplify bandwidth allocation on a class-by-class basis for end-to-end IP CoS in a routed ATM environment. An MPLS switching CoS template is assigned to a VSI when the VSI is enabled. Each templates links to two types of tables. One table type defines, on a per VC basis, bandwidth related parameters and UPC actions. The other table type defines the parameters required to configure qbins that provide Quality of Service (QoS) support.

With the implementation of VSI 2.0, MPLS supports master VSI controller redundancy and VSI slave controller redundancy.

MPLS Enhancements

MLPS based enhancements include the use of MPLS Class of Service (CoS) templates supported by VSI, and MPLS VSI master and VSI slave redundancy. In addition, MPLS supports Virtual Private Network (VPNs) via the use of virtual trunks. For additional information, refer to *PART 5, MPLS*.

rt-VBR

Either rt-VBR or nrt-VBR connections are supported. Separate queuing and traffic control features enhance the performance of connections added as rt-VBR connections. For additional information, refer to *Chapter 8, **ATM Connections***.

Ports or Trunks Concurrently Configurable on BXM

With Release 9.2, individual ports can be enabled in either trunk (network) or line (service) mode independent of how other ports on the card are enabled. So the ports on the same BXM card can be active in either trunk or line mode. In previous releases, once a port was upped, all ports had to be upped in the same mode.

Virtual Trunking on BXM

Virtual trunking is now available on the BXM. Virtual trunks typically are used to connect private virtual networks (PVNs) across a public ATM cloud, taking advantage of the full mesh capabilities of the public network. The virtual trunks can be used for standard ATM Forum traffic or for MPLS traffic.

The BXM card can support up to 31 virtual trunks. The 31 virtual trunks can be configured all on one physical port or distributed across the physical ports on the BXM. Each virtual trunk is associated with a virtual interface which in turn has 16 qbins available to provide traffic engineering VC differentiation. For additional information, refer to *Chapter 7, BXM Virtual Trunks*.

Virtual Private Networks

Virtual private networks using IP over the network allow such groups as companies, campuses, and enterprises, to use the capabilities and flexibility of the internet for employee communication, employee telecommuting, remote site access, and branch office data exchange. The standard Web applications available, make for easy and quick site access and utilization.

Cisco's implementation of virtual privates networks using MPLS provides scalability through integrated support of ATM switches within an IP core, supports advanced IP services on ATM switches, and delivers traffic engineering and IP based VPN capabilities on both ATM switches and on standard layer 3 routers. For additional information, refer to *Chapter 19, MPLS VPNS with BPX 8650*.

APS Redundancy on BXM Fiber Interfaces

Automatic protection switching (APS) provides redundancy for fiber optic line interface connections on BXM cards with SMF and SMFLR OC-3 or OC-12 interfaces.

Sonet Automatic Protection Switching provides the ability to configure a pair of SONET lines for line redundancy so that the hardware automatically switches from the active line to the standby line when the active line fails.

Each redundant line pair consists of a working line and a protection line. The hardware is set up to switch automatically. Upon detection of a signal fail condition (e.g., LOS, LOF, Line AIS, or Bit Error Rate exceeding a configured limit) or a signal degrade condition (BER exceeding a configured limit) the hardware switches from a working line to the protection line.

The following APS types of redundancy are supported, APS 1+1, APS 1:1, and APS 1+1 (Annex B).

To support line redundancy only, no additional hardware is required other than cabling. To support card and line redundancy, APS 1+1 requires a new paired backcard. When used with the current BPX chassis, the APS card locations are restricted to slots 2-5 and 10-13. WIth the new BPX chassis (post Rel. 9.1) this card location restriction is removed. For additional information, refer to *Chapter 9, SONET APS.*

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. 9.2.30 Cisco WAN Switching Command Reference*.

Cisco WAN Manager (CWM) and Cisco View Enhancements

The Cisco WAN Manager (formerly StrataView Plus) and Cisco View add additional topology and management functions.

MGX 8220

Rel. 5.0 supported.

Continuing Features with Current Release

The following is a list of previously provided features that are included in this release along with the new features previously listed:

Cisco WAN Manager Network Management

- NMS enhancements including additional management and provisioning capabilities including support of IGX switch tiered network voice and data applications
- Support for 12 Cisco WAN Manager workstations
- Multi-network Cisco WAN Manager capability

Network

- Support for IGX switch hubs and associated interface shelves in tiered network
- The number of nodes supported in a network is increased to over 1100, of which 223 can be routing nodes.
- Inverse Multiplexing ATM (IMA)
- Frame Relay to ATM Network Interworking (Supported by FRM on IGX switch, and FRSM on MGX 8220
- Frame Relay to ATM Service Interworking (Supported by FRSM on MGX 8220)
- Tiered networks
- VSVD standards based, closed-loop, rate-based congestion management for ABR
- Automatic end-to-end routing of virtual connections (AutoRoute)
- Closed-loop, rate-based congestion management (using Optimized Bandwidth Management (ForeSight) for ABR)
- Effective management of quality of service (Advanced CoS Management)
- Per -VC queueing and per-VC scheduling (Advance Cos Management)

BPX Switch

- MPLS with the BXM
- BME Multicasting for PVCs
- Traffic shaping for BXM for UBR, VBR, and CBR per VC scheduling policies. Prior to Rel. 9.1, this was previously supported for ABR only.
- Extended Services Processor (ESP) Release 2.2
  - Support for SPVCs, including auto-grooming of SPVCs
  - Dynamic resource partitioning for migration of PVCs to SPVCs
  - Interworking with the LS1010 ATM switch to provide point-to-multipoint SVC connections.

  Continued ESP features that were available in Release 2.0 including:

  - ATM switched virtual circuits (ATM SVCs)
  - Frame Relay switched virtual circuits (Frame Relay SVCs)

- ESP redundancy
- Call billing and call detail records (for ATM, Frame Relay, and SVCs only)

- The BXM cards provide a range of trunk and service interfaces and support ATM Forum Standards UNI 3.1 and ATM Traffic Management 4.0 including ABR connections with VSVD congestion control. The BXM cards are implemented with Stratm technology which uses a family of custom Application Specific Integrated Circuits (ASICs) to provide high-density, high-speed operation. The three types of BXM cards are:
  - The BXM T3/E3 is available as an eight or twelve port card that provides T3/E3 interfaces at 44.736 or 34.368 Mbps rates, respectively. The BXM-T3/E3 can be configured for either trunk or access applications.
  - The BXM 155 is available as a four or eight port card that provides OC-3/STM-1 interfaces at 155.52 Mbps rates. The BXM-155 can be configured for either trunk or access applications.
  - The BXM 622 is available as a one or two port card that provides OC-12/STM-4 interfaces at 622.08 Mbps rates. The BXM-622 can be configured for either trunk or access applications.
- Enhanced network scaling:
  - 50/64 trunks per BPX switch equipped with BCC-32 or BCC-64, respectively
  - 72/144 lines per node equipped with BCC-32 or BCC-64, respectively
  - 223 routing nodes (with BPX switch or IGX switch)
  - trunk based loading
  - BCC-3-64 supported on BPX switch
  - BCC-3-32, 7000 virtual connections
  - BCC-3-64, supports VSI, 12000 virtual connections
  - BCC-4, supports VSI, and supports up to 19.2 Gbps peak switching with the BXM cards supporting egress at up to 1600 Mbps and ingress at up to 800 Mbps.
  - de-route delay timer
  - connection routing groups by cell loading
- ATM and Frame Relay SVCs, and Soft Permanent Virtual Circuits (SPVCs) with Extended Services Processor

  ESP is an adjunct processor that is co-located with a BPX switch shelf. The ESP provides the signaling and Private Network to Network Interface (PNNI) routing for ATM and Frame Relay SVCs via BXM cards in the BPX switch and AUSM and FRSM cards in the MGX 8220.
- Cisco WAN Manager NMS enhancements including additional management and provisioning capabilities.
- Hot Standby Redundancy
- MGX 8220 Release 4.1, which includes:
  - BNM-155 interface to BXM on BPX switch
  - FRSM support for both SVC and PVC Frame Relay connections with ESP
  - AUSM support for both SVC and PVC ATM connections with ESP
  - FRSM-8 with ELMI

- IMATM-B
- AUSM-8
- CESM/4T1E1
- FRSM-HS1 (HSSI and X.21 interfaces)
- SRM 3T3

- Virtual Trunking on the BNI cards.
- Inverse Multiplexing ATM (IMA).
- Enhanced Ingress buffers for ASI-155 and BNI-155 to 8K cells for Release 8.1 and up.
- BPX switch OC-3 network and service interfaces on the BNI and ASI cards.
- High-speed switching capacity.
- Powerful crosspoint switching architecture.
- 53-byte cell-based ATM transmission protocol.
- Twelve 800 Mbps switch ports for network or access interfaces with BNI and ASI cards.
- Three DS3 or E3 ATM network interface ports per card (BNI).
- Totally redundant common control and switch fabric.
- Up to 20 million point-to-point cell connections per second between slots.
- Switches individual connections rather than merely serving as a virtual path switch.
- Easy integration into existing IGX switch networks.
- Internal diagnostics and self-test routines on all cards and backplane, status indication on each card.
- Collection of many ATM and other network statistics and transfer of the data collected to Cisco WAN Manager over high-speed Ethernet LAN interface.
- Integration with the Cisco WAN Manager Network Management System to provide configuration, control, and maintenance.
- Conformation to recommendations from all current ATM standards bodies: ATM Forum, ITU, ETSI, and ANSI.
- Compliant with all applicable safety, emissions, and interface regulations. Meets requirements of NEBS for Central Office equipment.

MGX 8220

- With Release 9.1, MGX 8220, Rel. 4.1, supported (with Rel. 9.2, MGX 8220 Rel. 5.0 is supported)
- Inverse Multiplexing ATM (IMA) support for the BPX switch with Rel. 3 MGX 8220
- CES T1/E1
- MGX 8220 T1/E1 Frame Relay and T1/E1 ATM service interfaces
- FUNI (Frame Based UNI over ATM)

IGX Switch

- With Rel. 9.1, UXM added native ATM trunks and ports (UNI)
- The IGX switch is configurable as a tiered network routing hub supporting voice and data over IGX switch interface shelves.

BPX Switch Operation

BPX Switch Operation

With the BCC-4, the BPX switch employs an up to 19.2 Gbps peak non-blocking crosspoint switch matrix for cell switching. The switch matrix can establish up to 20 million point-to-point connections per second between ports. A single BPX switch provides twelve card slots, with each card capable of operating at 800 Mbps for ASI and BNI cards. The BXM cards support egress at up to 1600 Mbps and ingress at up to 800 Mbps. The enhanced egress rate enhance operations such as multicast. Access to and from the crosspoint switch matrix on the BCC is through multi-port network and user access cards. It is designed to easily meet current requirements with scalability to higher capacity for future growth.

A BPX switch shelf is a self-contained chassis which may be rack-mounted in a standard 19-inch rack or open enclosure. All control functions, switching matrix, backplane connections, and power supplies are redundant, and non-disruptive diagnostics continuously monitor system operation to detect any system or transmission failure. Hot-standby hardware and alternate routing capability combine to provide maximum system availability.

The BPX Switch with MGX 8220 Shelves

Many network locations have increasing bandwidth requirements due to emerging applications. To meet these requirements, users can overlay their existing narrowband networks with a backbone of BPX switches to utilize the high-speed connectivity of the BPX switch operating at up to 19.2 Gbps with its T3/E3/OC-3/OC-12 network and service interfaces. The BPX switch service interfaces include BXM and ASI ports on the BPX switch and service ports on MGX 8220 shelves. The MGX 8220 shelves may be co-located in the same cabinet as the BPX switch, providing economical port concentration for T1/E1 Frame Relay, T1/E1 ATM, CES, and FUNI connections.

Multiprotocol Label Switching

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

By integrating the switching and routing functions, MPLS combines the reachability, scalability, and flexibility provided by the router function with the traffic engineering optimizing capabilities of the switch. The BPX 8650 MPLS switch combines a BPX switch with a separate MPLS controller (Cisco Series 7200 or 7500 router).

The BPX Switch with Extended Services Processor

With a co-located ESP, the BPX Switch adds the capability to support ATM and Frame Relay switched virtual circuits (SVCs), and also soft permanent virtual circuits (SPVCs). Refer to the *Cisco WAN Service Node Extended Services Processor Installation and Operation* document for detailed information abut the ESP.

Virtual Private Networks

The following paragrap;hs provide a brief description of VPNs. For additional information, refer to *Chapter 19, MPLS VPNS with BPX 8650*.

Conventional Virtual Private Networks

Conventional Virtual Private Networks using dedicated lease lines or Frame Relay PVCs and a meshed network (Figure 1-2), while providing many advantages, have typically been limited in efficiency and flexibility.

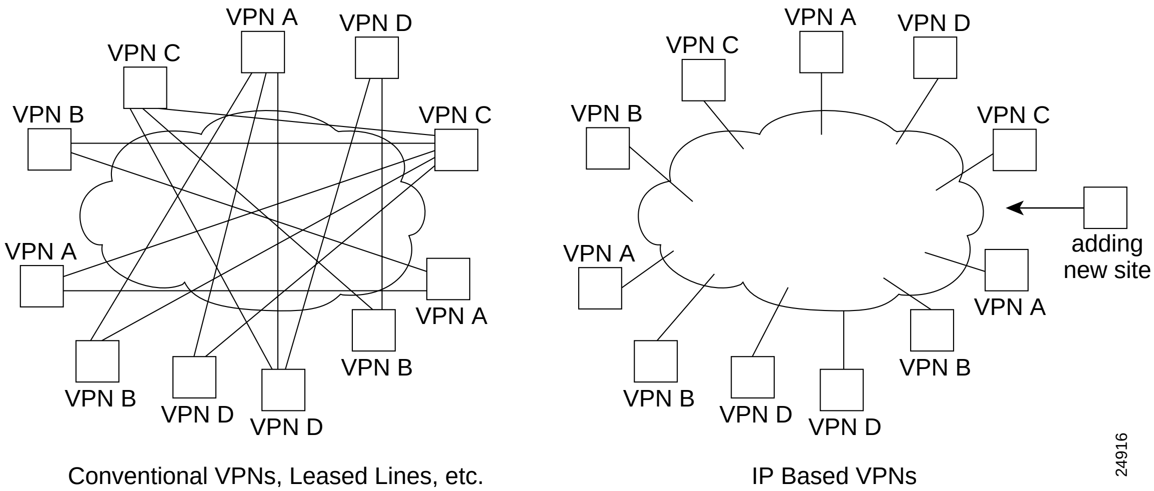
IP Virtual Private Networks

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

An IP virtual private network offers the following benefits:

- Scalability
  - — Avoids VC mesh configuration
  - — Easy to add a new site since IP is connectionless
  - — Service provider handles router service management
- Efficient
  - — Rapid provisioning for networks
  - — Supports any to any intranets

Figure 1-2 IP VPN Service Example



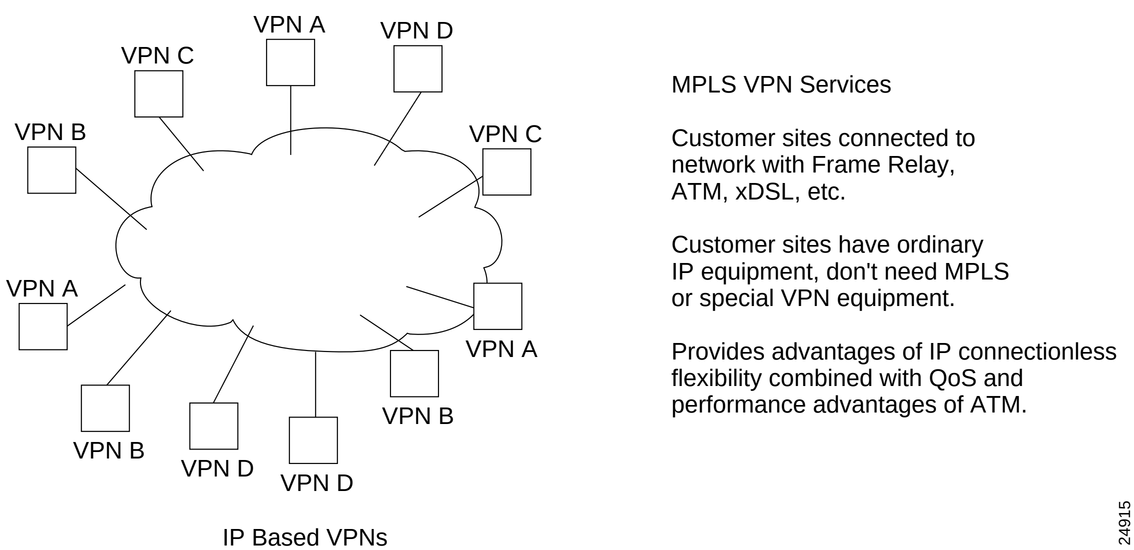
MPLS Virtual Private Networks

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

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

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

Figure 1-3 MPLS VPNs Example



Frame Relay to ATM Interworking

Interworking allows users to retain their existing services, and as their needs expand, migrate to the higher bandwidth capabilities provided by BPX switch networks. Frame Relay to ATM Interworking enables Frame Relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking. For additional information, refer to *Chapter 13, Frame Relay to ATM Network and Service Interworking.*

Two types of Frame Relay to ATM interworking are supported, Network Interworking (see Figure 1-4) and Service Interworking (see Figure 1-5). The Network Interworking function is performed by the BTM card on the IGX switch, and the FRSM card on the MGX 8220. The FRSM card on the MGX 8220 and the UFM cards on the IGX switch also support Service Interworking.

The Frame Relay to ATM network and service interworking functions are available as described in the following paragraphs:

Network Interworking

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

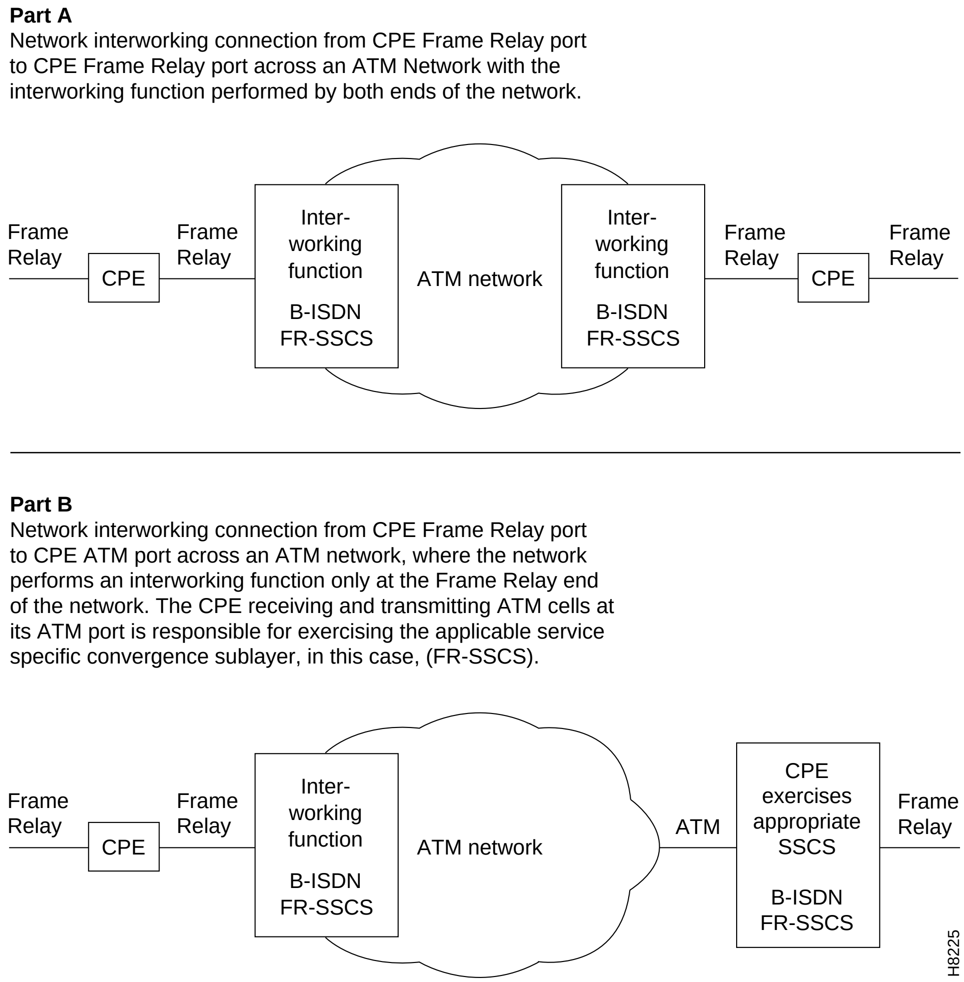
- IGX switch Frame Relay (shelf/feeder) to IGX switch Frame Relay (either routing node or shelf/feeder).
- MGX 8220 Frame Relay to MGX 8220 Frame Relay.
- MGX 8220 Frame Relay to IGX switch Frame Relay (either routing node or shelf/feeder).

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

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

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

Figure 1-4 Frame Relay to ATM Network Interworking



Service Interworking

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

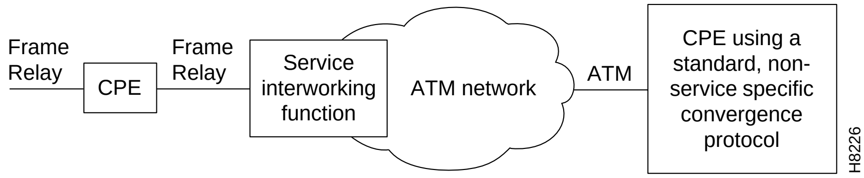
In Service Interworking, for example, for a connection between an ATM port and a Frame Relay port, unlike Network Interworking, the ATM device does not need to be aware that it is connected to an interworking function.

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

The following is a typical configuration for service interworking:

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

Figure 1-5 Frame Relay to ATM Service Interworking



Additional Information

For additional information about interworking, refer to *Chapter 13, Frame Relay to ATM Network and Service Interworking.*

Tiered Networks

Networks may be configured as flat (all nodes perform routing and communicate fully with one another), or they may be configured as tiered. In a tiered network, interface shelves are connected to routing hubs, where the interface shelves are configured as non-routing nodes. For additional information, refer to *Chapter 14, Tiered Networks*.

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

Starting with Release 8.5, in addition to BPX switch routing hubs, tiered networks now support IGX switch routing hubs. Voice and data connections originating and terminating on IGX switch interface shelves (feeders) are routed across the routing network via their associated IGX switch routing hubs. Intermediate routing nodes must be IGX switches, and IGX switch interface shelves are the only interface shelves that can be connected to an IGX switch routing hub. With this addition, a tiered network provides a multi-service capability (Frame Relay, circuit data, voice, and ATM).

Routing Hubs and Interface Shelves

In a tiered network, interface shelves at the access layer (edge) of the network are connected to routing nodes via feeder trunks (Figure 1-6). Those routing nodes with attached interface shelves are referred to as routing hubs. The interface shelves, sometimes referred to as feeders, are non-routing nodes. The routing hubs route the interface shelf connections across the core layer of the network.

The interface shelves do not need to maintain network topology nor connection routing information. This task is left to their routing hubs. This architecture provides an expanded network consisting of a number of non-routing nodes (interface shelves) at the edge of the network that are connected to the network by their routing hubs.

For detailed information about tiered networks, refer to *Chapter 14,* “*Tiered Networks*”.

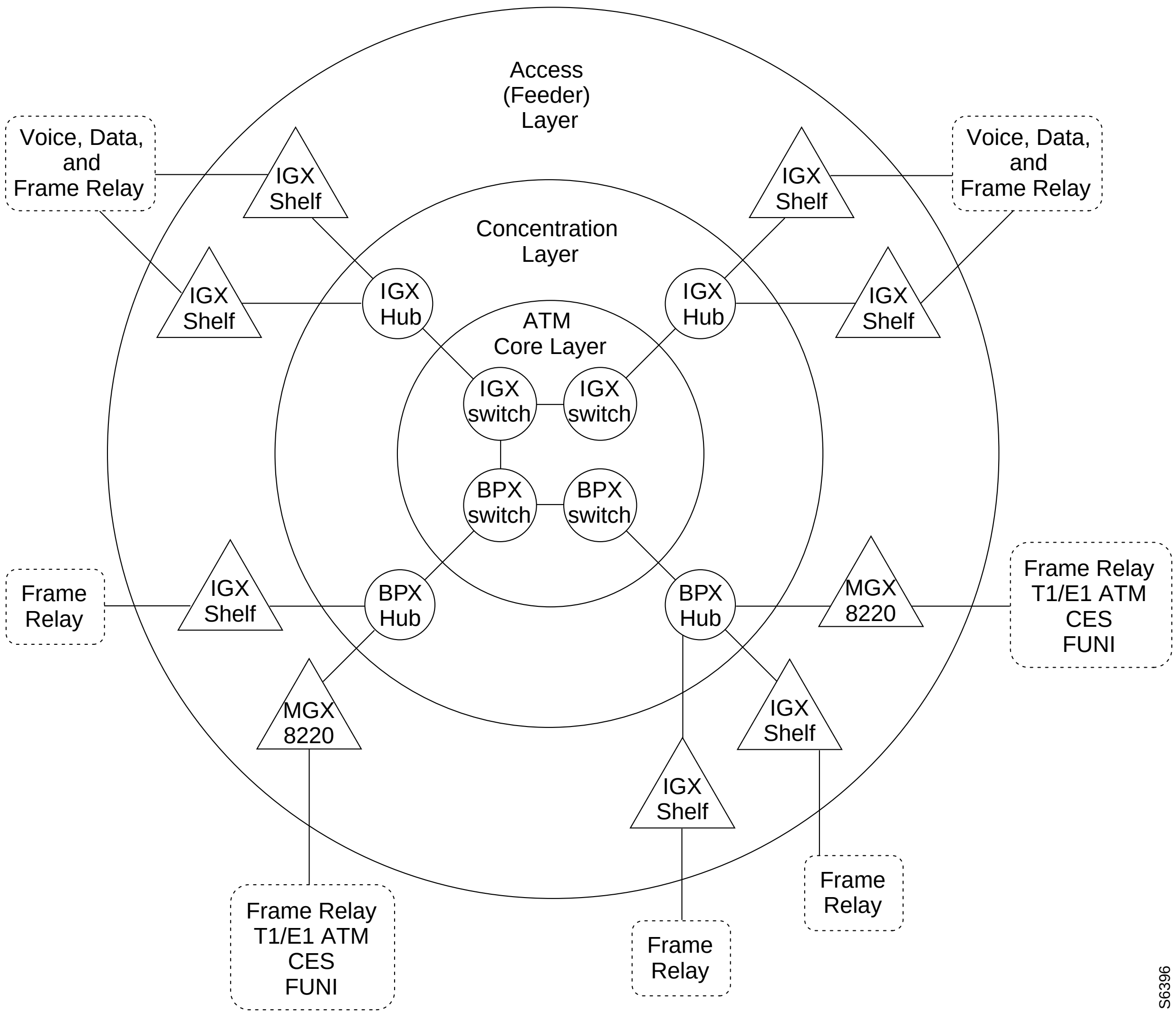
BPX Switch Routing Hubs

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

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

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

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



Inverse Multiplexing ATM

Where greater bandwidths are not needed, the Inverse Multiplexing ATM (IMA) feature provides a low cost trunk between two BPX switches. The IMA feature allows BPX switches to be connected to one another over any of the 8 T1 or E1 trunks provided by an AIMNM module on an MGX 8220 shelf. A BNI or BXM port on each BPX switch is directly connected to an AIMNM module in an MGX 8220 by a T3 or E3 trunk. The AIMNM modules are then linked together by any of the 8 T1 or E1 trunks. Refer to the *Cisco MGX 8220 Reference* and the *Cisco WAN Switching Command Reference* publications for further information.

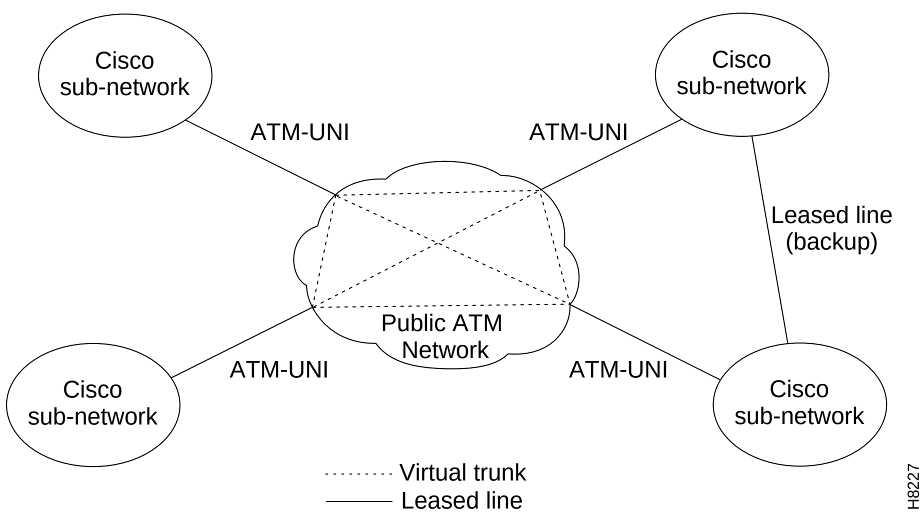
Virtual Trunking

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

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

A virtual trunk may be defined as a "trunk over a public ATM service". The trunk really doesn't exist as a physical line in the network. Rather, an additional level of reference, called a **virtual trunk number**, is used to differentiate the virtual trunks found within a physical trunk port. Figure 1-7 shows four Cisco WAN switching networks, each connected to a Public ATM Network via a physical line. The Public ATM Network is shown linking all four of these subnetworks to every other one with a full meshed network of virtual trunks. In this example, each physical line is configured with three virtual trunks.

Figure 1-7 Virtual Trunking Example



Traffic and Congestion Management

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

The Traffic Control functions include:

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

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

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

  Cisco’s Frame Relay and ATM service modules are equipped with large buffers and a dynamic buffer management technique for allocating and scaling the buffers on a per VC basis to traffic entering or leaving a node. The switch dynamically assigns buffers to individual virtual circuits based on the amount of traffic present and service level agreements. The large queues readily accommodate large bursts of traffic into the node.
- PNNI, a standards-based routing protocol for ATM and Frame Relay SVCs.
- Early and partial packet discard for AAL5 connections.

Advanced CoS Management

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

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

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

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

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

Rather than limiting the user to the five broad classes of service defined by the ATM standards committees, CoS management can provide up to 16 classes of service (service subclasses) that 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.

Automatic Routing Management

With Automatic Routing Management (formerly referred to as AutoRoute), connections in Cisco WAN switching networks are added if there is sufficient bandwidth across the network and are automatically routed when they are added. The user only needs to enter the endpoints of the connection at one end of the connection and the IGX switch, and BPX switch software automatically set up a route based on a sophisticated routing algorithm. This feature is called *Automatic Routing Management*. It is a standard feature on the IGX switch, BPX switch, and MGX 8220.

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

Cost-Based Routing Management

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

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

The section, Cost-Based Connection Routing, contains more detailed information about cost-based AutoRoute.

ABR Standard with VSVD Congestion Control

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

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

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

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

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

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

Optimized Bandwidth Management (ForeSight) Congestion Control

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

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

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

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

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

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

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

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

PNNI

The Private Network to Network Interface (PNNI) protocol provides a standards-based dynamic routing protocol for ATM and Frame Relay SVCs. PNNI is an ATM-Forum-defined interface and routing protocol which is responsive to changes in network resources, availability, and will scale to large networks. PNNI is available on the BPX switch when an ESP or SES PNNI is installed. For further information about PNNI and the ESP, refer to the *Cisco WAN Service Node Series Extended Services Processor Installation and Operation* publication.

Network Management

BPX switches provide one high-speed and two low-speed data interfaces for data collection and network management. The high-speed interface is an Ethernet 802.3 LAN interface port for communicating with a Cisco WAN Manager NMS workstation. TCP/IP provides the transport and network layer, Logical Link Control 1 is the protocol across the Ethernet port.

The low-speed interfaces are two RS-232 ports, one for a network printer and the second for either a modem connection or a connection to an external control terminal. These low-speed interfaces are the same as provided by the IGX switch.

A Cisco WAN Manager NMS workstation connects via the Ethernet to the LAN port on the BPX and provides network management via SNMP. Statistics are collected by Cisco WAN Manager using the TFTP protocol. On IGX switch shelves, Frame Relay connections are managed via the Cisco WAN Manager Connection Manager. On MGX 8220 shelves, the Cisco WAN Manager Connection Manager manages Frame Relay and ATM connections, and the Connection Manager is used for MGX 8220 shelf configuration.

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

Network Interfaces

Network interfaces connect the BPX switch to other BPX or IGX switches to form a wide-area network.

The BPX switch provides T3, E3, OC-3/STM-1, and OC-12/STM-4 trunk interfaces. The T3 physical interface utilizes DS3 C-bit parity and the 53-byte ATM physical layer cell relay transmission using the Physical Layer Convergence Protocol. The E3 physical interface uses G.804 for cell delineation and HDB3 line coding. The BNI-155 card supports single-mode fiber (SMF), single-mode fiber long reach (SMF-LR), and multi-mode fiber (MMF) physical interfaces. The BXM-155 cards support SMF, SMFLR, and MMF physical interfaces. The BXM-622 cards support SMF and SMFLR physical interfaces.

The design of the BPX switch permits it to support network interfaces up to 622 Mbps in the current release while providing the architecture to support higher broadband network interfaces as the need arises.

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

Service Interfaces

Service interfaces connect ATM customer equipment to the BPX switch. ATM User-to-Network Interfaces (UNI) and ATM Network-to-Network Interfaces (NNI) terminate on the ATM Service Interface (ASI) cards and on BXM T3/E3, OC-3, and OC-12 cards configured for as service interfaces (UNI access mode). The ASI-1 card provides two T3 or E3 ports. The ASI-155 card OC-3/STM-1 trunk interfaces are single-mode fiber (SMF), single-mode fiber long reach (SMF-LR), and multi-mode fiber (MMF) physical interfaces. The BXM T3/E3 card supports the standard T3/E3 interfaces. The BXM-155 cards support SMF, SMFLR, and MMF physical interfaces. The BXM-622 cards support SMF and SMFLR physical interfaces. The ASI and BXM cards support cell relay connections that are compliant with both the physical layer and ATM layer standards.

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

Statistical Alarms and Network Statistics

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

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

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

These statistics are collected in real-time throughout the network and forwarded to the WAN Manager workstation for logging and display. The link from the node to the Cisco WAN Manager workstation uses a protocol to acknowledge receipt of each statistics data packet. Refer to the *Cisco WAN Manager Operations* publication, for more details on statistics and statistical alarms.

Node Synchronization

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

Since the BPX switch is designed to be part of a larger communications network, it is capable of synchronizing to higher-level network clocks as well as providing synchronization to lower-level devices. Any network access input can be configured to synchronize the node. Any external T1 or E1 input can also be configured to synchronize network timing. A clock output allows synchronizing an adjacent IGX switch or other network device to the BPX switch and the network. In nodes equipped with optional redundancy, the standby hardware is locked to the active hardware to minimize system disruption during system switchovers.

The BPX Service Node can be configured to select clock from the following sources:

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

Switch Software Description

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

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

Software among multiple nodes cooperates to perform network-wide functions such as trunk and connection management. This multi-processor approach ensures rapid response with no single point of failure. System software applications provide advanced features that may be installed and configured as required by the user.

Some of the many software features are:

- Automatic routing of connections (Automatic Routing Management feature).
- Various classes of service that may be assigned to each connection type (Advanced CoS Management).
- Bandwidth reservation on a time-of-day basis.
- Detection and control of network congestion with ABR with VSVD or Optimized Bandwidth Management (ForeSight) algorithms.
- Automatic self-testing of each component of the node.
- Automatic collecting and reporting of many network-wide statistics, such as trunk loading, connection usage, and trunk error rates, as specified by the user.

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

Connections and Connection Routing

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

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

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

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

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

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

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

Connection Routing Groups

The re-routing mechanism is enhanced so that connections are presorted in order of cell loading when they are added. Rerouting takes place by rerouting the group containing the connections with the largest cell loadings first on down to the last group which contains the connections with the smallest cell loadings. These groups are referred to as routing groups. Each routing group contains connections with loading in a particular range.

There are three configurable parameters for configuring the rerouting groups,

— total number of rerouting groups

— starting load size of first group

— load size range of each group

The three routing group parameters are configured with the **cnfcmparm** command.

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

Table 1-1 Routing Group Configuration Example

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

Cost-Based Connection Routing

In standard AutoRoute, the path with the fewest number of hops to the destination node is chosen as the best route. Cost-based route selection uses an administrative trunk cost routing metric. The path with the lowest total trunk cost is chosen as the best route. Cost-based route selection is based on Dijkstra’s Shortest Path Algorithm, which is widely used in network routing environments. You can use cost-based route selection (that is, cost-based AutoRoute) to give preference to slower privately owned trunks over faster public trunks which charge based on usage time. This gives network operators more control over the usability of their network trunks, while providing a more standard algorithm for route selection.

Major Features of Cost-Based AutoRoute

The following list gives a short description of the major functional elements of Cost-Based Route Selection.

- Enabling Cost-Based Route Selection.
  Cost-based route selection is selectively enabled by the user as the route selection algorithm per node. The feature is not a chargeable feature and does not require special password access. The default algorithm is the hop-based algorithm. cost-based route selection can be enabled or disabled at any time.

- Configuring Trunk Cost
  A trunk cost is assigned by the user to each trunk (physical and virtual) in the network. One cost is assigned per trunk - no separate costs are used for different connection or service types. The valid range of trunk costs is 1 (lowest cost) to 50 (highest cost). A trunk has a default cost of 10 upon activation. The cost of a trunk can be changed before or after the trunk has been added to the network topology.

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

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

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

  Enabling cost-based route selection automatically enables cache usage. Enabling Hop-Based Route Selection automatically disables cache usage. Cache usage can also be independently enabled or disabled for both types of route selection.

- On-Demand Lowest Cost Route Determination
  On-demand routing chooses the current lowest cost route to the destination node. This lowest cost route is bounded by the maximum route length of 10 hops. If more than one route of similar cost and distance is available, the route with most available resources is chosen. No route grooming occurs after the initial routing. A connection does not automatically reroute if its route cost changes over time. A connection also does not automatically reroute if a lower cost route becomes available after the initial routing. However, a forced reroute or a preferred route can be used to move the connection to a lower cost route.

- Delay Sensitive Routes
  Delay sensitive IGX connection types (Voice and Non-Timestamped Data) may be configured to use the worst case queueing delay per trunk, rather than the configured trunk cost, in the

lowest-cost route determination. The trunk delay acts as the cost attribute in the Dijkstra algorithm. The default mode for the delay sensitive connections is to use the trunk cost. All other connection types always use the trunk cost in the route determination.

AutoRoute currently does not use the worst case end-to-end queueing delay in route selection for delay sensitive BPX connection types (ATM CBR). Cost-based route selection does not change this.

- Cost Cap
  A maximum allowable cost value (cost cap) is used during route determination to prevent selection of a route which exceeds an acceptable cost. For routing based on delay, the cost cap is the acceptable end-to-end delay for the connection type. This cap is configured network-wide per delay sensitive connection type.

  For routing based on trunk cost, the cost cap is the acceptable end-to-end cost. This cap is configured per connection. The default cost cap is 100, which is derived from the maximum hops per route (10) and default cost per trunk (10). The cost cap can be changed at any time. If the cost cap is decreased below the current route cost, the connection is not automatically rerouted. A manual reroute is required to route the connection to fit under the new cost cap. This gives the user more control over the connection reroute outage.
- Software Upgrades
  A software upgrade to Release 9.0 set AutoRoute to use Hop-Based Route Selection. The cost of all trunks is set to the default cost (10). The cost cap of all connections is set to the maximum allowable cost (100). All other new cost-based routing parameters are set to regular default values.
- AutoRoute Interoperability
  Because AutoRoute is source-based, nodes can interoperate using different route selection algorithms. The originating node computes the full end-to-end route based on its own knowledge of the network topology. The route is then passed to the subsequent nodes on the route. This source routing allows a mix of Cost-Based and Hop-Based Route Selection to run in a network.

Cost-Based AutoRoute Commands

The following switched software Command Line Interface (CLI) commands are used for cost-based route selection:

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

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

The cost can be configured from either end of the trunk. The cost can be changed before or after the trunk has been added to the network. The cost can also be changed after connections have been routed over the trunk. Any cost change is updated network-wide. Every node in the network stores the cost of every trunk in the network. This knowledge is required for successful source-based routing.

- **cnfrtcost**
  New command which configures the cost cap for a connection. This command is valid only at the node where the connection is added.
- **cnfsysparm**
  Configures the delay cost cap for all delay sensitive connections in the network. This command was not modified in Release 9.0.
- **dspcon**
  Displays the maximum and current costs for a connection route
- **dspload**
  Displays the administrative cost and queue delay for a network trunk
- **dsprts**
  Displays the current costs for all connection routes
- **dsptrkcnf**
  Displays the configured cost of a trunk

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

Network Synchronization

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

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

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

Switch Availability

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

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

Node Redundancy

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

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

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

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

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

Node Alarms

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

Each card in the node has front-panel LEDs to indicate active, failed, or standby status. Each power supply has green LEDs to indicate proper voltage input and output. An Alarm, Status, and Monitor card collects all the node hardware status conditions and reports it using front panel LED indicators and alarm closures. Indicators are provided for major alarm, minor alarm, ACO, power supply status, and alarm history. Alarm relay contact closures for major and minor alarms are available from each node through a 15-pin D-type connector for forwarding to a site alarm system.

BPX switches are completely compatible with the network status and alarm display provided by the Cisco WAN Manager NMS workstation. In addition to providing network management capabilities, it displays major and minor alarm status on its topology screen for all nodes in a network. The Cisco WAN Manager NMS also provides a maintenance log capability with configurable filtering of the maintenance log output by node name, start time, end time, alarm type, and user specified search string.

BPX Switch

This chapter contains an overall physical and functional description of the BPX switch. The physical description includes the BPX switch enclosure, power, and cooling subsystems. The functional description includes an overview of BPX switch operation.

This chapter contains the following:

- Physical Description
- Functional Description
- BPX Switch Major Groups
- Optional Peripherals

Physical Description

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

BPX Switch Enclosure

The BPX switch enclosure is a self-contained chassis which may be rack mounted in any standard 19 inch rack or enclosure with adequate ventilation. It contains a single shelf which provides fifteen slots for vertically mounting the BPX switch cards front and rear. Refer to Figure 2-1 which illustrate the front view of the BPX switch Shelf.

At the front of the enclosure (see Figure 2-1) are 15 slots for mounting the BPX switch front cards. Once inserted, the cards are locked in place by the air intake grille at the bottom of the enclosure. A mechanical latch on the air intake grille must be released by using a screwdriver and the grille must be tilted forward in order to remove or insert cards.

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

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

Figure 2-1 BPX Switch Exterior Front View

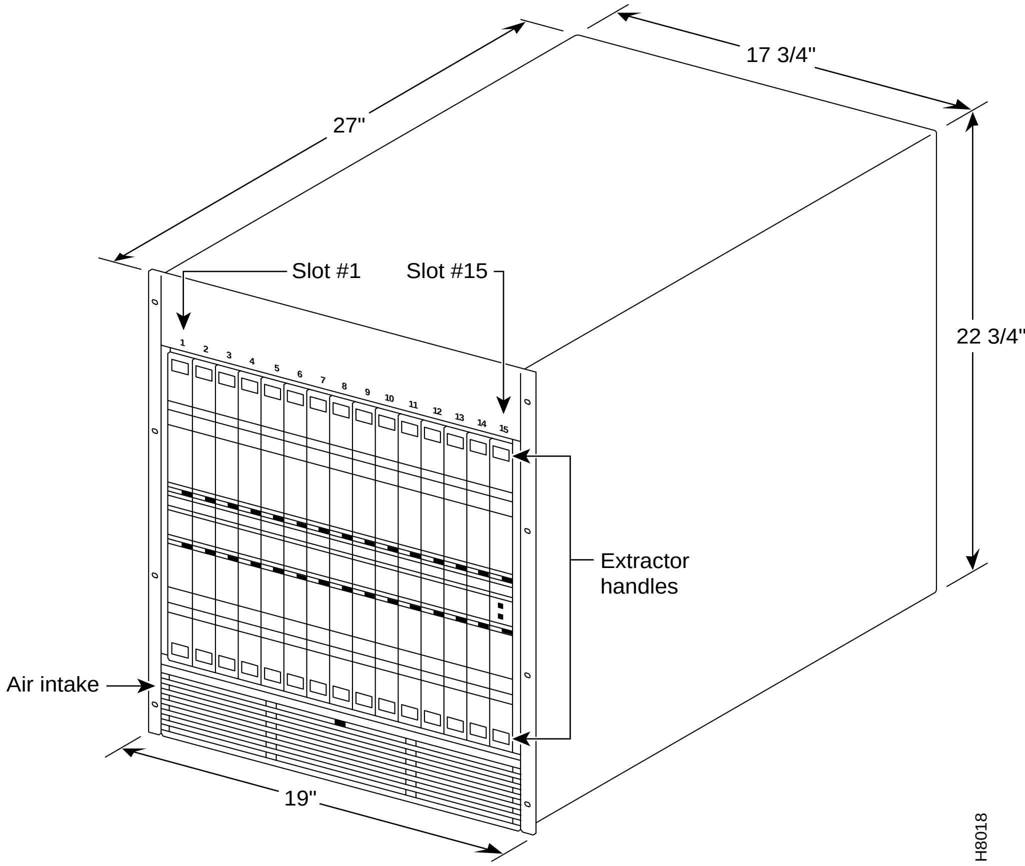
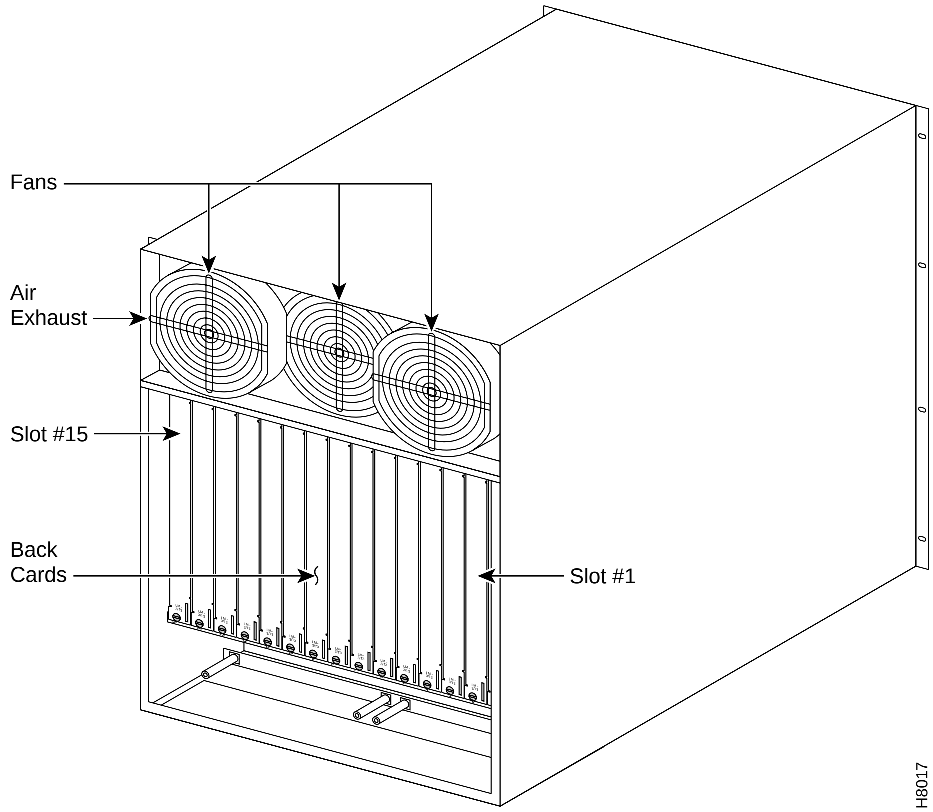


Figure 2-2 BPX Switch Exterior Rear View



Node Cooling

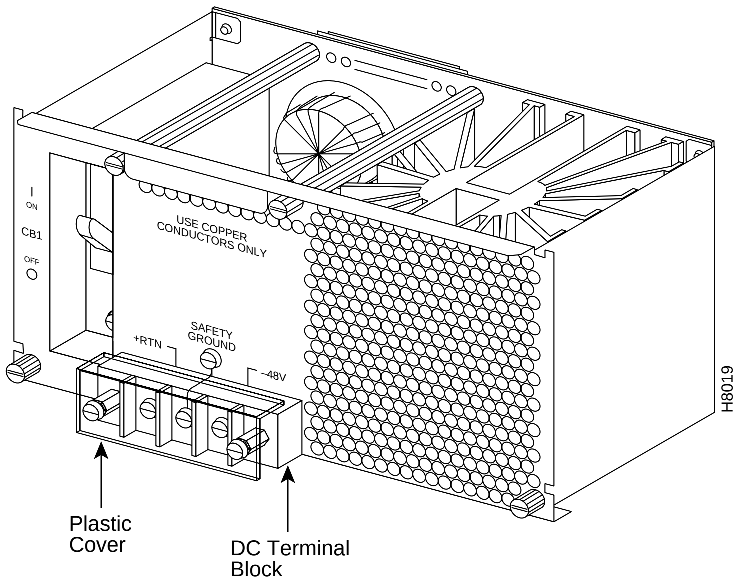
A fan assembly, with three six-inch 48 VDC fans is mounted on a tray at the rear of the BPX switch shelf (see Figure 2-2). Air for cooling the cards is drawn through an air intake grille located at the bottom in the front of the enclosure. Air passes up between the vertically-mounted cards and exhausts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

Node DC Powering

The primary power for a BPX switch node is -48 VDC which is bused across the backplane for use by all card slots. DC-to-DC converters on each card convert the -48V to lower voltages for use by the card. The -48 VDC input connects directly to the DC Power Entry Module (PEM). The DC Power Entry Module (see Figure 2-3) provides a circuit breaker and line filter for the DC input.

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

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

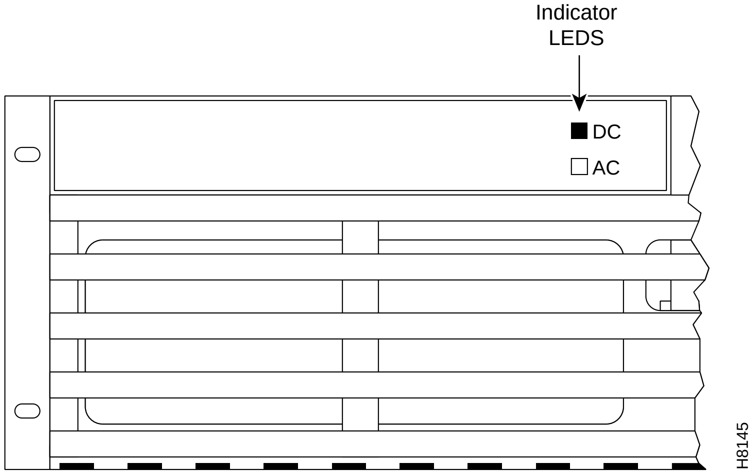


Optional AC Power Supply Assembly

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

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

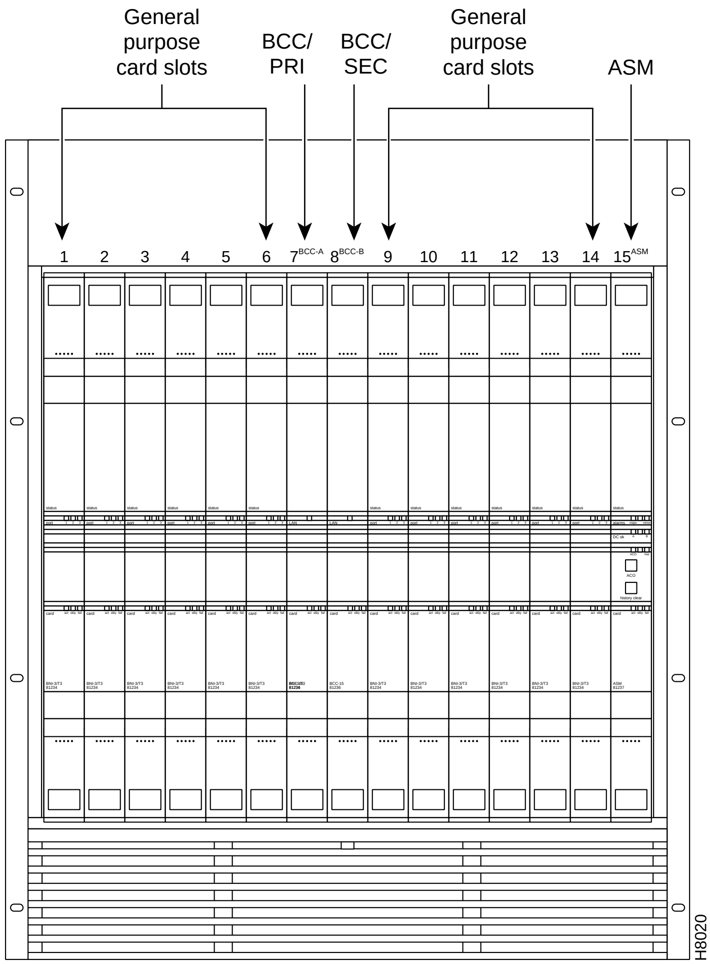
Figure 2-4 AC Power Supply Assembly Front View



Card Shelf Configuration

There are fifteen vertical slots in the front of the BPX switch enclosure to hold plug-in cards (see Figure 2-5). The middle two slots, slots number 7 and number 8, are used for the primary and secondary Broadband Controller Cards (BCC). The right-most slot, number 15, is used to hold the single Alarm/Status Monitor Card. The other twelve slots, number 1 through number 6 and number 8 through number 14, can be used for the Network Interface and Service Interface cards.

Figure 2-5 BPX Switch Card Shelf Front View



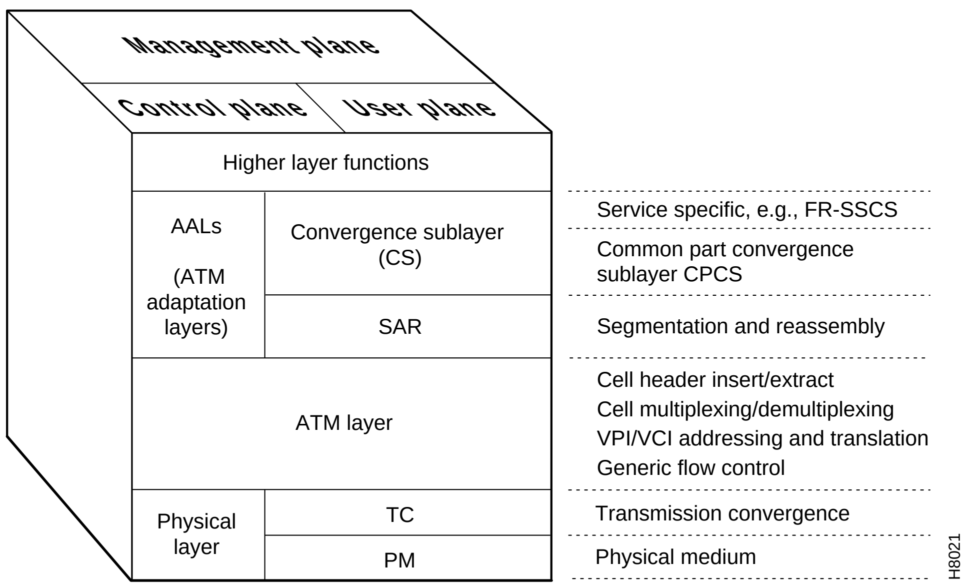
Functional Description

ATM

ATM transmits broadband information using fixed length, relatively small, 53-byte cells which are suitable for carrying both constant rate data (e.g., voice and video) as well as bursty data.

ATM evolved from the Broadband Integrated Services Digital Network (B-ISDN) standard, which in turn is an extension of ISDN. ISDN defines service and interfaces for public telecommunications networks. B-ISDN utilizes a 7-layer reference model similar to the Open Systems Interconnection (OSI) 7-layer architecture. ATM redefines the lower three levels as shown in Figure 2-6. These are the Physical Layer, the ATM layer, and the ATM Adaptation Layer (AAL).

Figure 2-6 B-ISDN Model



Physical Layer

The physical layer is divided into two parts, the Transmission Convergence sub-layer and the Physical Medium sub-layer.

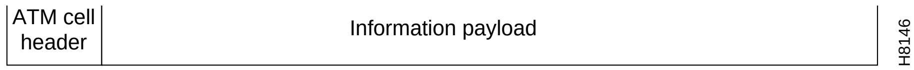
The Physical Medium sub-layer (PMD) handles processing specific to a particular physical layer, such as transmission rate, clock extractions, etc.

The Transmission Convergence sub-layer (TC) extracts the information content from the physical layer data format. This includes HEC generation and checking, extraction of cells from the data stream, processing of idle cells, etc.

ATM Layer

The ATM layer processes ATM cells. The ATM cell consists of a 5-byte header and a 48-byte payload. The header contains the ATM cell address and other management information Figure 2-7.

Figure 2-7 ATM Cell Format



ATM Cell Headers

There are two basic header types defined by the standards committees, a UNI header and a NNI header; both are quite similar. Cisco has expanded on these header types to provide additional features beyond those proposed for basic ATM service. Usage of each of the various cell header types is described as follows:

- The UNI header (see Figure 2-8) must be specified for each *User-to-Network Interface*. A UNI is any interface between a user device, such as an ATM router, and an ATM network.
- The NNI header (see Figure 2-9) must be specified for each *Network-to-Network Interface*. This is used, for example, at the interface between a user's private ATM network and a service provider's public ATM network.
- The STI header (see Figure 2-10) is an extension of these two header types and is used between Cisco switching nodes to provide advanced network features, including ForeSight, that improve performance, efficiency, and congestion control.

Figure 2-8 UNI Header

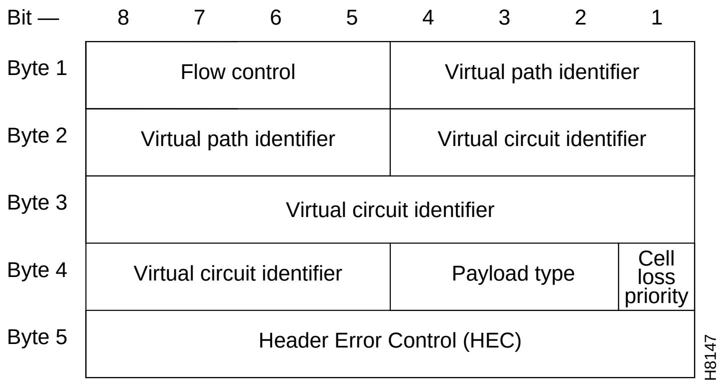


Figure 2-9 NNI Header

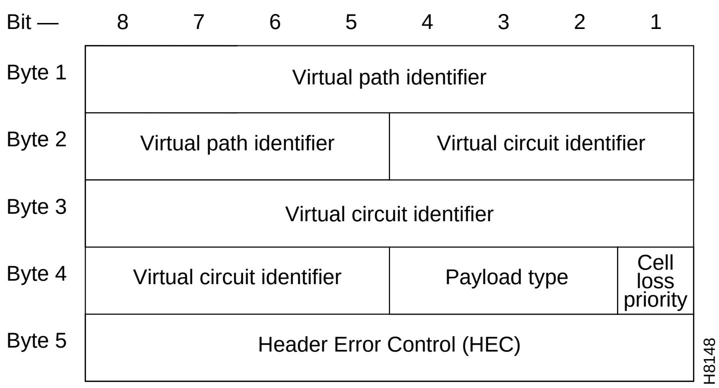


Figure 2-10 STI Header

STI Header

8	7	6	5	4	3	2	1
HCF		VPI					
VPI				VCI			
VCI				Payload class			
CC		F	R	PTI			CLP
HCS							

HCF: Header Control Field, a 01 indicates an STI Cell
VPI/VCI: Virtual Path/Virtual Channel Identifiers, same as UNI and NNI.

Payload Class:

- 0001 Non-Timestamped Data/Constant BIt Rate
- 0010 High Priority/Variable Bit Rate
- 0011 Voice/Constant BIt Rate
- 0100 Bursty Data A/Variable BIt Rate
- 0101 Time-Stamped Data/Constant BIt Rate
- 0110 Bursty Data B/Variable BIt Rate

CC: Congestion Control

- 00: No report
- 01: Uncongested
- 10: Congestion
- 11: Severe Congestion

F: ForeSIght Forward Congestion Indication (FFCI).

Set to 1 if FECN in Frame is a 1. or if incoming cell FFCI is a 1, or egress queue experiences congestion.

R: Reserved

PTI: Payload Type Indicator

CLP: Cell Loss Priority. Same as for UNI or NNI. The CLP bit is set to 1 if the DE is set for a frame, or if the first FastPacket in a frame has its CLP set.

PTI, bits 4,3, and 2:
- bit 4 = 0, user data cell;
- bit 4 = 1, connection management cell
- bit 3 = 0, No congestion experienced
- bit 3 = 1, Congestion experienced
- bit 2 = 0, for user data cell, indicates CPE information
- bit 2 = 1, not used

PTI Bits 432	Description		
000	User Data Cell	no congestion experienced	SDU Type 0 (CPE information)
001	User Data Cell	no congestion experienced	SDU Type 1
010	User Data Cell	congestion experienced,	SDU Type 0 (CPE information)
011	User Data Cell	congestion experienced,	SDU Type 1
100	Connection Management Cell, OAM F5 Segment Flow Related cell		
101	Congestion Management Cell, OAM F5 End-to-End Flow related cell		
110	Connection Management Cell, reserved for future use.		
111	Connection Management Cell, reserved for future use.		

H8149

The most important fields in all three ATM cell header types are the *Virtual Path Identifier* (VPI) and a *Virtual Circuit Identifier* (VCI). The VPI identifies the route (path) to be taken by the ATM cell while the VCI identifies the circuit or connection number on that path. The VPI and VCI are translated at each ATM switch, they are unique only for a given physical link.

A 4-bit *Generic Flow Control* (GFC) field in the UNI header is intended to be used for controlling user access and flow control. At present, it is not defined by the standards committees and is generally set to all zeros.

A 3-bit *Payload Type Indicator* (PTI) field indicates the type of data being carried in the payload. The high-order bit is a “0” if the payload contains user information and is a “1” if it carries connection management information. The second bit indicates if the cell experienced congestion over a path. If the payload is user information, the third bit indicates if the information is from Customer Premises Equipment. The PTI field is identical for UNI/NNI/STI.

In the STI header (see Figure 2-10), the *Payload Class* is used to indicate various classes of service and BPX switch queues, e.g., Opticlass, the enhanced class of service feature of the BPX switch. The *ForeSight Forward Congestion Indication*, the F bit, is used by ForeSight for congestion status.

The *Cell Loss Priority* (CLP) bit follows the PTI bits in all header types. When set, it indicates that the cell is subject to discard if congestion is encountered in the network. For Frame Relay connections, depending on mapping considerations, the frame Discard Eligibility status is carried by the CLP bit in the ATM Cell. The CLP bit is also set at the ingress to the network for all cells carrying user data transmitted above the minimum rate guaranteed to the user.

ATM Cell Addressing

Each ATM cell contains a two-part address, VPI/VCI, in the cell header. This address uniquely identifies an individual ATM virtual connection on a physical interface. VCI bits are used to identify the individual circuit or connection. Multiple virtual circuits that traverse the same physical layer connection between nodes are grouped together in a virtual path. The virtual path address is given by the VPI bits. The Virtual Path can be viewed as a trunk that carries multiple circuits all routed the same between switches

The VPI and VCI addresses may be translated at each ATM switch in the network connection route. They are unique only for a given physical link. Therefore, they may be reused in other parts of the network as long as care is taken to avoid conflicts.

The VCI field is 16 bits wide with UNI and NNI header types described earlier. This allows for a total possible 65, 535 unique circuit numbers. The UNI header reserves 8 bits for VPI (256 unique paths) while the NNI reserves 12 bits (4,096 unique paths) as it is likely that more virtual paths will be routed between networks than between a user and the network. The STI header reserves 8 bits for VCI and 10 bits for VPI addresses.

ATM Adaptation Layer

The purpose of the ATM Adaptation Layer (AAL) is to receive the data from the various sources or applications and convert, or adapt, it to 48-byte segments that will fit into the payload of an ATM cell. Since ATM benefits from its ability to accommodate data from various sources with differing characteristics, the Adaptation Layer must be flexible.

Traffic from the various sources have been categorized by the standards committees into four general classifications, Class A through Class D, as indicated in Table 2-1. This categorization is somewhat preliminary and initial developments have indicated that it may be desirable to have more than these initial four classes of service.

Table 2-1 Classes of Traffic and Associated AAL Layers

Traffic Class	Class A	Class B	Class C	Class D
Adaptation Layer (AAL)	AAL-1	AAL-2	AAL-3/4 AAL-5	AAL-3/4
Connection Mode	Connection-oriented	Connection-oriented	Connection-oriented	Connectionless
End-to-End Timing Relationship	Yes	Yes	No	No
Bit Rate	Constant	Variable	Variable	Variable
Examples	Uncompressed voice, constant bit-rate video	Compressed voice and video	Frame relay, SNA, TCP-IP, E-mail	SMDS

Initially, four different adaptation layers (AAL1 through AAL4) were envisioned for the four classes of traffic. However, since AAL3 and AAL4 both could carry Class C as well as Class D traffic and since the differences between AAL3 and AAL4 were so slight, the two have been combined into one AAL3/4.

AAL3/4 is quite complex and carries a considerable overhead. Therefore, a fifth adaptation layer, AAL5, has been adopted for carrying Class C traffic, which is simpler and eliminates much of the overhead of the proposed AAL3/4. AAL5 is referred to as the Simple and Efficient Adaptation Layer, or SEAL, and is used for Frame Relay data.

Since ATM is inherently a connection-oriented transport mechanism and since the early applications of ATM will be heavily oriented towards LAN traffic, many of the initial ATM products are implemented supporting the Class C Adaptation Layer with AAL5 Adaptation Layer processing for carrying Frame Relay traffic.

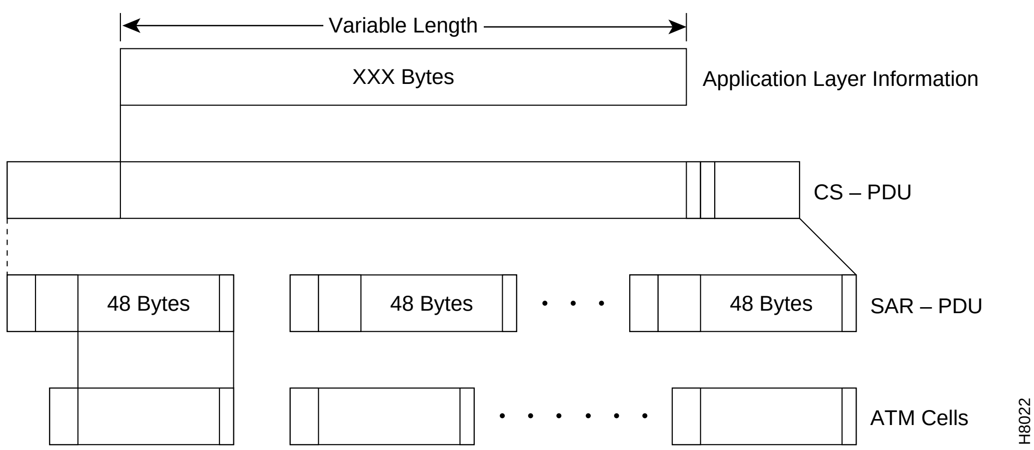
Referring back to Figure 2-6, the ATM Adaptation Layer consists of two sub-layers:

- Convergence Sub-Layer (CS)
- Segmentation and Reassembly Sub-Layer (SAR)

Data is received from the various applications layers by the Convergence Sub-Layer and mapped into the Segmentation and Reassembly Sub-Layer. User information, typically of variable length, is packetized into data packets called Convergence Sublayer Protocol Data Units (CS-PDUs). Depending on the Adaptation Layer, these variable length CS-PDUs will have a short header, trailer, a small amount of padding, and may have a checksum.

The Segmentation and Reassembly Sub-Layer receives the CS-PDUs from the Convergence Sub-Layer and segments them into one or more 48-byte SAR-PDUs, which can be carried in the 48-byte ATM information payload bucket. The SAR-PDU maps directly into the 48-byte payload of the ATM cell transmitted by the Physical Layer. Figure 2-11 illustrates an example of the Adaptation Process.

Figure 2-11 SAR Adaptation Process



IPX and IGX Switch Trunk Interfaces to ATM

The IPX switch connects to a BPX switch or other ATM switch via an AIT/BTM T3 or E3 trunk. the IGX switch also connects to an ATM trunk via the UXM card. The AIT(IPX switch) or BTM (IGX switch) can operate in several different addressing modes selected by the user (see Table 2-2 and

Figure 2-12). To allow the IPX switch or IGX switch to be used in mixed networks with other ATM switches, there are two other addressing modes available, Cloud Addressing Mode (CAM) and Simple Addressing Mode (SAM).

BAM

In the BPX switch Addressing Mode (BAM), used for all Cisco WAN switching networks, the system software determines VPI and VCI values for each connection that is added to the network. The user enters the beginning and end points of the connection and the software automatically programs routing tables in each node that will carry the connection to translate the VPI/VCI address. The user does not need to enter anything more. This mode uses the STI header format and can support all of the optional Cisco WAN switching features.

SAM

In the Simple Addressing Mode (SAM), the user must manually program the path whole address, both VPI and VCI values.

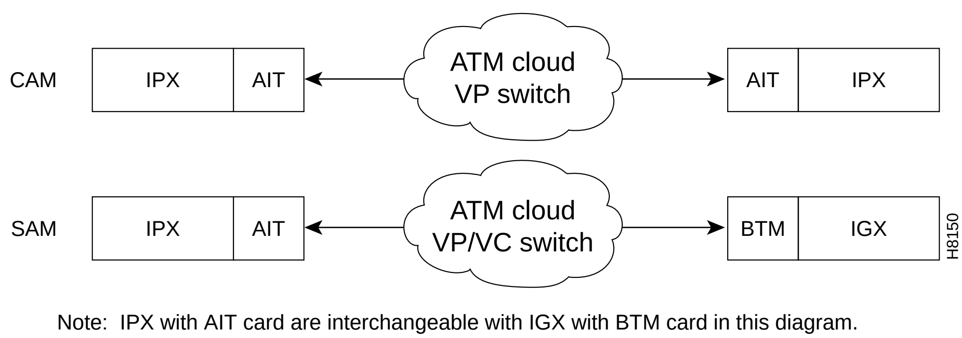
CAM

The Cloud Addressing Mode (CAM) is used in mixed networks where the virtual path addresses are programmed by the user and the switch decodes the VCI address. Both CAM and SAM utilize the UNI header type.

Table 2-2 ATM Cell Addressing Modes

Addressing Mode	Hdr. Type	Derivation of VPI/VCI	Where Used
BAM-BPX switch Addressing Mode	STI	VPI/VCI = Node Derived Address	Between IPX switch (or IGX switch) and BPX switches, or between IPX switch (or IGX switch) nodes.
CAM— Cloud Addressing Mode	UNI	VPI = User Programmed VCI = Node Derived Address	IPX switch to IPX switch (or IGX switch) connections over networks using ATM switches that switch on VPI only. VPI is manually programmed by user. Terminating IPX switch converts VCI address to FastPacket address.
SAM— Simple Addressing Mode	UNI	VPI/VCI = User Programmed	IPX switch to IPX switch (or IGX switch) connections over networks using ATM switches that switch where all routing is manually programmed by user, both VPI and VCI.

Figure 2-12 BAM, CAM, and SAM Configurations



FastPacket Adaptation to ATM

A specialized adaptation that is of particular interest to users of Cisco equipment is the adaptation of IPX switch FastPackets to ATM cells. There are a large number of narrowband IPX switch networks currently in existence that are efficiently carrying voice, video, data, and Frame Relay. A means must be provided to allow these networks to grow by providing a migration path to broadband.

Since FastPackets are already a form of cell relay, the adaptation of FastPackets to ATM cells is relatively simple.

Simple Gateway

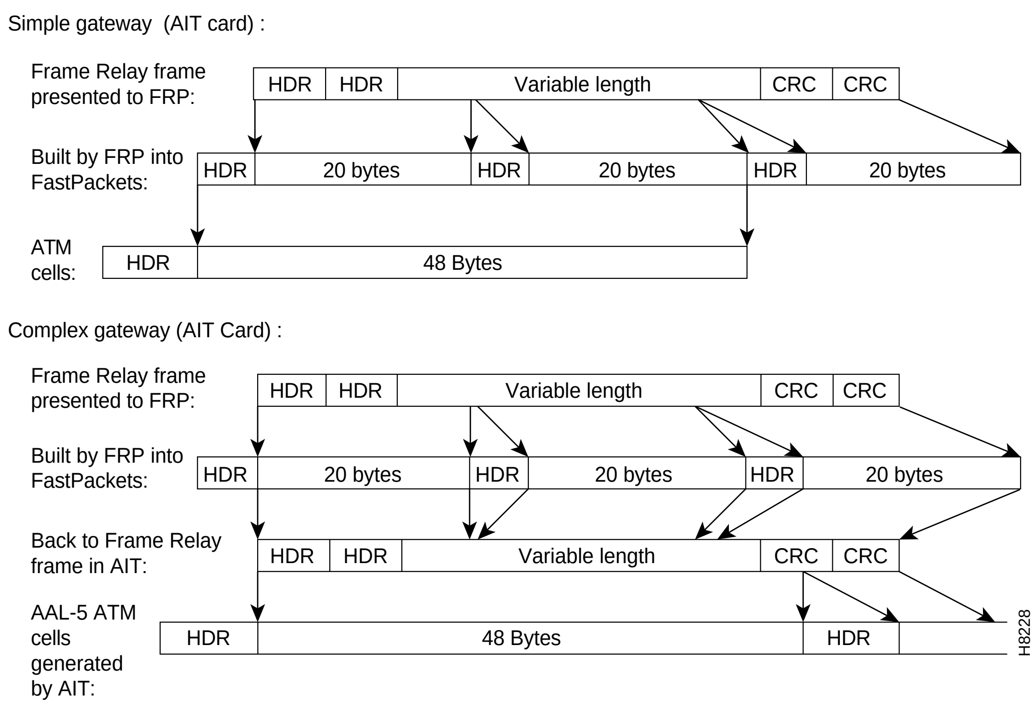
With the Simple Gateway protocol, the AIT card in the IPX switch (or BTM in the IGX switch) loads 24-byte FastPacket cells into ATM cells in ways that are consistent with each application. (Each of the two FastPacket cells loaded into the ATM Cell is loaded in its entirety, including the FastPacket header.) For example, two FastPackets can be loaded into one ATM cell provided they both have the same destination. This adaptation is performed by the IPX switch AIT card or the IGX switch BTM card.

The AIT (or BTM) is configured to wait a given interval for a second FastPacket to combine in one ATM cell for each FastPacket type. The cell is transmitted half full if the wait interval expires. High priority and non-time stamped packets are given a short wait interval. High priority FastPackets will not wait for a second FastPacket. The ATM trunk interface will always wait for Frame Relay data (bursty data) to send two packets. NPC traffic will always have two FastPackets in an ATM cell.

Complex Gateway, Frame Relay to ATM Network Interworking

Starting with Release 8.1, with the Complex Gateway capability, the FRSM card in the MGX 8220, the AIT card in the IPX switch (or BTM card in the IGX switch) streams the Frame Relay data into ATM cells, cell after cell, until the frame has been completely transmitted. Since only the data from the FastPacket is loaded, the Complex Gateway is an efficient mechanism. Also, discard eligibility information carried by the Frame Relay bit is mapped to the ATM cell CLP bit, and vice versa. See Chapter 13 for further information on Frame Relay to ATM interworking. A comparison of the simple gateway and complex gateway formats is shown in Figure 2-13.

Figure 2-13 Simple and Complex Gateway Formats



BPX Switch Major Groups

There are four major groups in the BPX switch. These are listed in Table 2-3.

- Common Core
- Network Interface
- Service Interface
- Power Supplies

Table 2-3 lists these groups and their components along with a brief description of each.

Table 2-3 BPX Switch Plug-In Card Summary

Card	Card Name	Where
BPX-	**Common Core Group**	
BPX-BCC-32	Broadband Controller Card, operates with versions of System Software Rel. 7.0 and above, and requires 32 Mbyte RAM for 8.1 and later software. For redundancy configuration, installed as a pair of BCC-32s. (System operation equivalent to BCC-3.)	Front
BPX-BCC-bc	Back card (also known as LM-BCC) used only with the BCC-32.	Back
BPX-BCC-3	Broadband Controller Card, operates with 7.X software versions 7.2.84 and above, and with 8.X System Software versions 8.1.12 and above. For redundancy configuration, installed as a pair of BCC-3s. (System operation equivalent to BCC-32.)	Front
BPX-BCC-3-64	Broadband Controller Card, enhanced BCC-3. Note: BCC-3-64 or BCC-4 required to support VSI and MPLS.	
BPX-BCC-4	Broadband Controller Card, operates with 8.4 software and above. For redundancy configuration, installed as a pair of BCC-4s. Provides 64 Mbyte of RAM and above. Supports up to 19.2 Gbps performance of BXM cards. Note: BCC-3-64 or BCC-4 required to support VSI and MPLS	Front
BPX-BCC-3-bc	Back card (also known as LM-BCC) used with BCC-3 or BCC-4.	Back
BPX-ASM	Alarm/Status Monitor Card.	Front
BPX-ASM-BC	Line Module - Alarm/Status Monitor.	Back
	Network Interface Group	
BPX-BXM-T3-8 BPX-BXM-E3-8 BP:X-BXM-T3-12 BPX-BXM-E3-12	T3/E3 card with 8 or 12 ports. Card is configured for use in either network interface or service access (UNI) mode and with either a T3 or E3 interface.	Front
BPX-T3/E3-BC	Backcard for use with a BXM-T3/E3-8 or BXM-T3/E3-12	Back
BPX-BXM-155-4 BPX-BXM-155-8	BXM OC-3 cards with 4 or 8 OC-3/STM-1ports, respectively. Card is configured for use in either network interface or service access (UNI) mode.	Front
BPX-MMF-155-4-BC BPX-SMF-155-4-BC BPX-SMFLR-155-4-BC	Backcards for BXM-155-4.	Back
BPX-MMF-155-8-BC BPX-SMF-155-8-BC BPX-SMFLR-155-8-BC	Backcards for BXM-155-8.	Back

Table 2-3 BPX Switch Plug-In Card Summary (Continued)

Card	Card Name	Where
BPX-BXM-622 BPX-BXM-622-2	OC-12 card with 1or 2 OC-12/STM-4ports. Card is configured for use in either network interface or service access (UNI) mode.	Front
BPX-BME	Used for multicast connections. Used with SMF-622-2 backcard with port 1 looped to port 2, transmit to receive, and receive to transmit.	
BPX-SMF-622 BPX-SMFLR-622 BPX-XLR-622-BC	Backcards for BXM-622. The XLR card supports a 1500nm interface	Back
BPX-SMF-622-2-BC BPX-SMFLR-622-2-BC BPX-SMFLR-622-2-BC	Backcards for BXM-622-2 and BME (BME typically would use SMF-622-2).	Back
BPX-BME	Used for multicast connections. Used with SMF-622-2 backcard with port 1 looped to port 2, transmit to receive, and receive to transmit.	Back
BPX-BNI-3-T3	Broadband Network Interface Card (with 3 T3 Ports).	Front
BPX-T3-BC	Line Module - used with BNI-T3 for 3 physical T3 ports. (Configured for 3 ports)	Back
BPX-BNI-3-E3	Broadband Network Interface Card (with 3 E3 Ports).	Front
BPX-E3-BC	Line Module - used with BNI-E3 for 3 physical E3 ports. (Configured for 3 ports).	Back
BPX-BNI-155	Broadband Network Interface Card (with 2 OC3c/STM-1 ports).	Front
BPX-SMF-2-BC	OC3/STM-1 Interface Card, single mode fiber optic, used with either BNI-155 or ASI-155 front card.	Back
BPX-SMFLR-2-BC	OC3/STM-1 Interface Card, single mode fiber optic long range, used with either BNI-155 or ASI-155.	Back
BPX-MMF-2-BC	OC3/STM-1 Interface Card, multi-mode fiber optic (1 x 9 LED), used with either BNI-155 or ASI-155 front card.	Back
	APS Backcards and APS Redundant Backplane	

The APS 1+1 feature requires two BXM front cards, an APS redundant frame assembly, and two redundant type BXM backcards. The types of redundant backcard and backplane sets are:

- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622 (single port, long reach, SMF, FC connector)
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- BPX-RDNT-SM-622-2 (2 port, medium reach, SMF, FC connector)

Each of the listed model numbers includes two single backcards and one mini-backplane.

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

BPX-RDNT-BP= (common backplane for all redundant APS backcards)

BPX-LR-155-8R-BC= (for BPX-RDNT-LR-155-8)

BPX-LR-622-R-BC= (for BPX-RDNT-LR-622

BPX-SMF-155-4R-BC= (for BPX-RDNT-SM-155-4)

BPX-SMF-155-8R-BC= (for BPX-RDNT-SM-155-8)

BPX-SMF-622-R-BC= (for BPX-RDNT-SM-622)

BPX-SMF-622-2R-BC= (for BPX-RDNT-SM-622-2

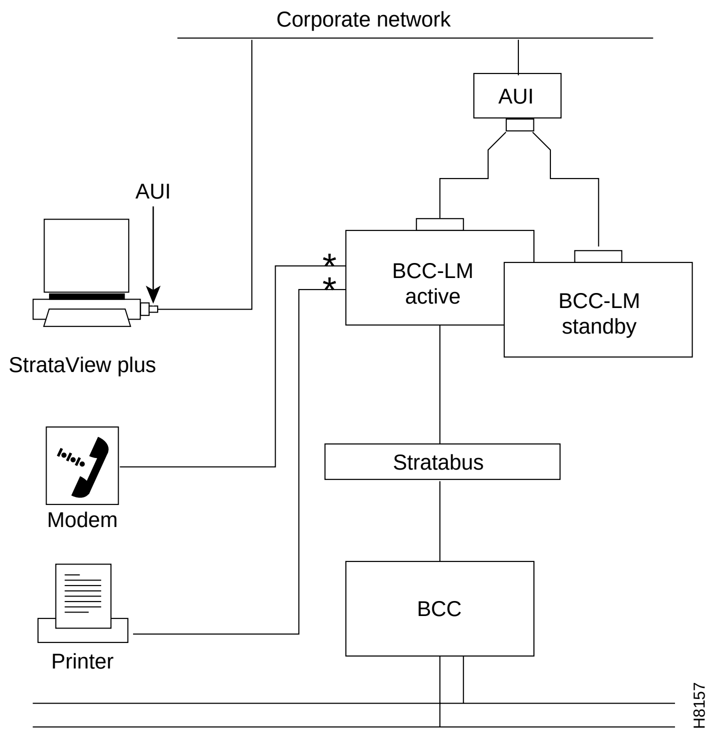
Table 2-3 BPX Switch Plug-In Card Summary (Continued)

Card	Card Name	Where
	Service Interface Group	
BPX-ASI-1-2T3	ATM Service Interface Card (with 2 usable T3 ports).	Front
BPX-T3-BC	Line Module - used with ASI-1-2T3 for 2 physical T3 ports. (Configured for 2 ports)	Back
BPX-ASI-1-2E3	ATM Service Interface Card (with 2 usableE3 ports).	Front
BPX-E3-BC	Line Module - used with BNI-E3 for 2 physical E3 ports. (Configured for 2 ports)	Back
BPX-ASI-155	ATM Service Interface Card (with 2 OC3c/STM-1 ports).	Front
BPX-SMF-2-BC	OC3/STM-1 Interface Card, SMF (single mode fiber optic) MMF (1x9 LED), used with either BNI-155 or ASI-155 front card.	Back
BPX-MMF-2-BC	OC3/STM-1 Interface Card, multi-fiber mode (1 x 9 LED), used with BNI-155 or ASI-155.	Back
BPX-SMFLR-2-BC	OC3/STM-1 Interface Card, single mode fiber optic long range, used with either BNI-155 or ASI-155.	Back
	Power Supply Group	
	48 Volt DC Power Supply	
	Optional AC Power Supply	

Optional Peripherals

At least one node in the network (or network domain if a structured network) must include a Strata-View Plus network management station (see Figure 2-14). A Y-cable may be used to connect the LAN ports on the primary and secondary BCC Line Modules, through an AUI to the LAN network, as only one BCC is active at a time. The serial Control port may be connected to a dial-in modem for remote service support or other dial-up network management access. The serial Auxiliary port is used for outgoing data only, for example, for connection to a printer.

Figure 2-14 Optional Peripherals Connected to BPX Switch



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

PART 2

General Description

BPX Switch Common Core

This chapter contains a description of the common core group, comprising the Broadband Controller Cards (BCCs), the Alarm/Status Monitor (ASM), associated backcards, and StrataBus backplane.

This chapter contains the following:

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

BPX Switch Common Core Group

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

- Broadband Controller Cards:
  - — BCC-4, BCC-3-32M or BCC-3-64M and associated BCC-3-BC backcard
  - — or BCC-32 and associated BCC15-BC backcard

Note The BCC-3-64 or BCC-4 is required for VSI and MPLS features operation

---

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

The BCC-3-32M, BC-3-64M, and BCC-32 are functionally equivalent except for performance and support 9.6 Gbps operation, but use different backcards. The BCC-4V provides a new 16 x 32 crosspoint switch architecture to extend the BPX peak switching capability from 9.6 up to 19.2 Gbps peak. The BCC-4V also provides 4 MBytes of BRAM and 128 MBytes of DRAM.

The common core group functions include:

- ATM cell switching.
- Internal node communication.
- Remote node communication.
- Node synchronization.

- Network management communications (Ethernet), local management (RS-232).
- Alarm and status monitoring functions.

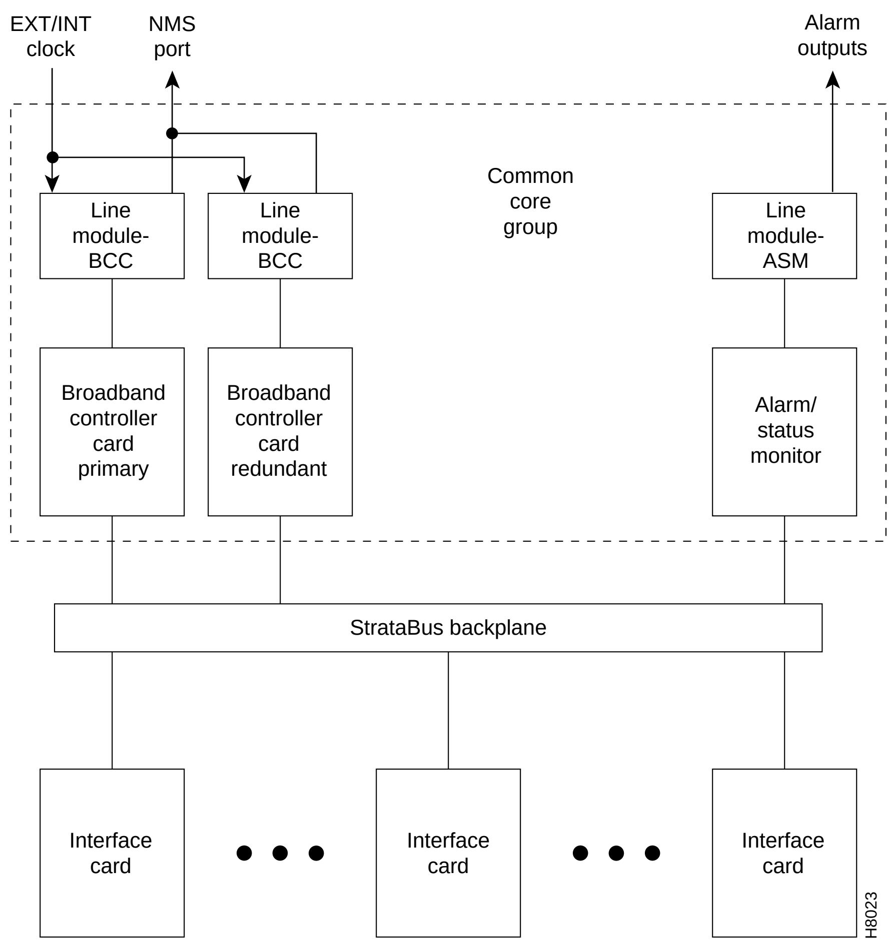
Broadband Controller Card (BCCs)

The Broadband Controller Card is a microprocessor-based system controller and is used to control the overall operation of the BPX switch. The controller card is a front card that is usually equipped as a redundant pair. Slots number 7 and number 8 are reserved for the primary and secondary (standby) broadband controller cards. Each broadband controller front card requires a corresponding back card.

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

Note The three types of BCCs with their proper backcards may be operated together temporarily for maintenance purposes, e.g., replacing a failed controller card. Throughout a network, individual BPX switches may have either a single BCC-32, BCC-3-32M, BCC-3-64M, or BCC-4V controller card or a pair of the identical type of BCC.

Figure 3-1 Common Core Group Block Diagram



The BCC-3-32M, BCC-3-64M, and BCC-32 are functionally equivalent except for performance. However, the BCC-4V provides a new 16 x 32 cross-point architecture that increases the peak switching capacity of the BPX switch to 19.2 Gbps, with a sustained non-blocking throughput of 9.6 Gbps. The term BCC is used in this manual to refer to the functional operation of the Broadband Controller Card. When a difference in operation does occur, the specific type of BCC is specified. This card group (see Figure 3-1) provides the following functions:

Features

The Broadband Controller Card performs the following major system functions:

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

Each Broadband Controller Card includes the following:

- 68EC040 processor operating at 33 MHz.
- 32 Mb of DRAM for running system software (BCC-32), 32 Mb or 64 MB option for BCC-3 and BCC-4.
- 4 Mb of Flash EEPROM for downloading system software.
- 512 Kbytes of BRAM for storing configuration data.
- EPROM for firmware routines.
- 68302 Utility processor.
- SAR engine processor operating at 33 MHz.
- Communication bus interface.
- HDLC processor for the LAN connection interface.
- Two RS-232 serial port interfaces.

Functional Description

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

- Central Arbiter on each BCC.
- Crosspoint Switch.
  - 16 X 16 Crosspoint Switching Matrix on each BCC (12 X 12 used) for BCC-32 and BCC-3-32M and BCC-3-64M.
  - 16 X 32 Crosspoint Switching Matrix on each BCC (2 X [12 X 12]) used for BCC-4V.
- Serial Interface and LAN Interface Modules on each BCC and on each Function Module.

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

Since there are 16 X 16 (BCC-32 or BCC-3-32M, or BCC-3-64M) or 16 X 32 (BCC-4V) independent crosspoints and only 15 cards, the switch fabric is non-blocking. However, only one connection at a time is allowed to an individual card. The BPX switch cell switching is not synchronized to any external clocks; it runs at its own rate. No switch fabric clocks are used to derive synchronization nor are these signals synchronized to any external sources.

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

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

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

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

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

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

Figure 3-2 BCC-32, BCC-3-32M, or BCC-3-64M Block Diagram

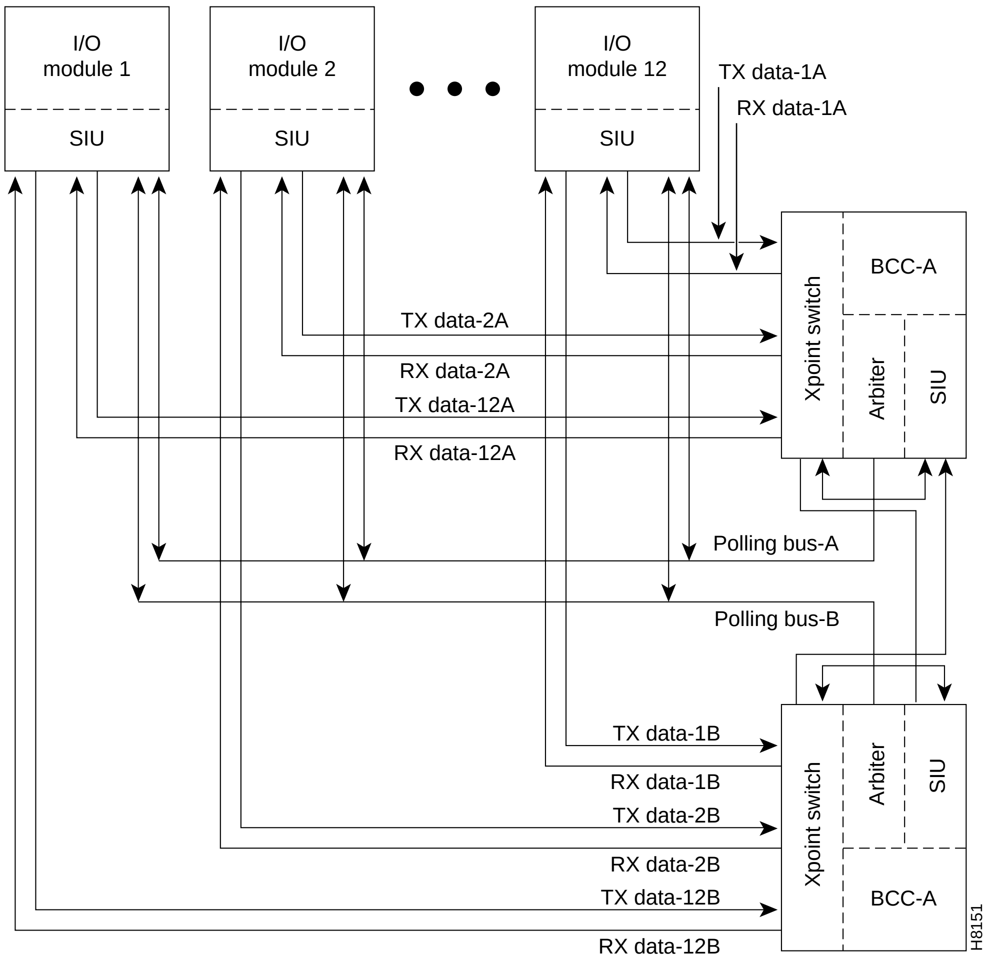
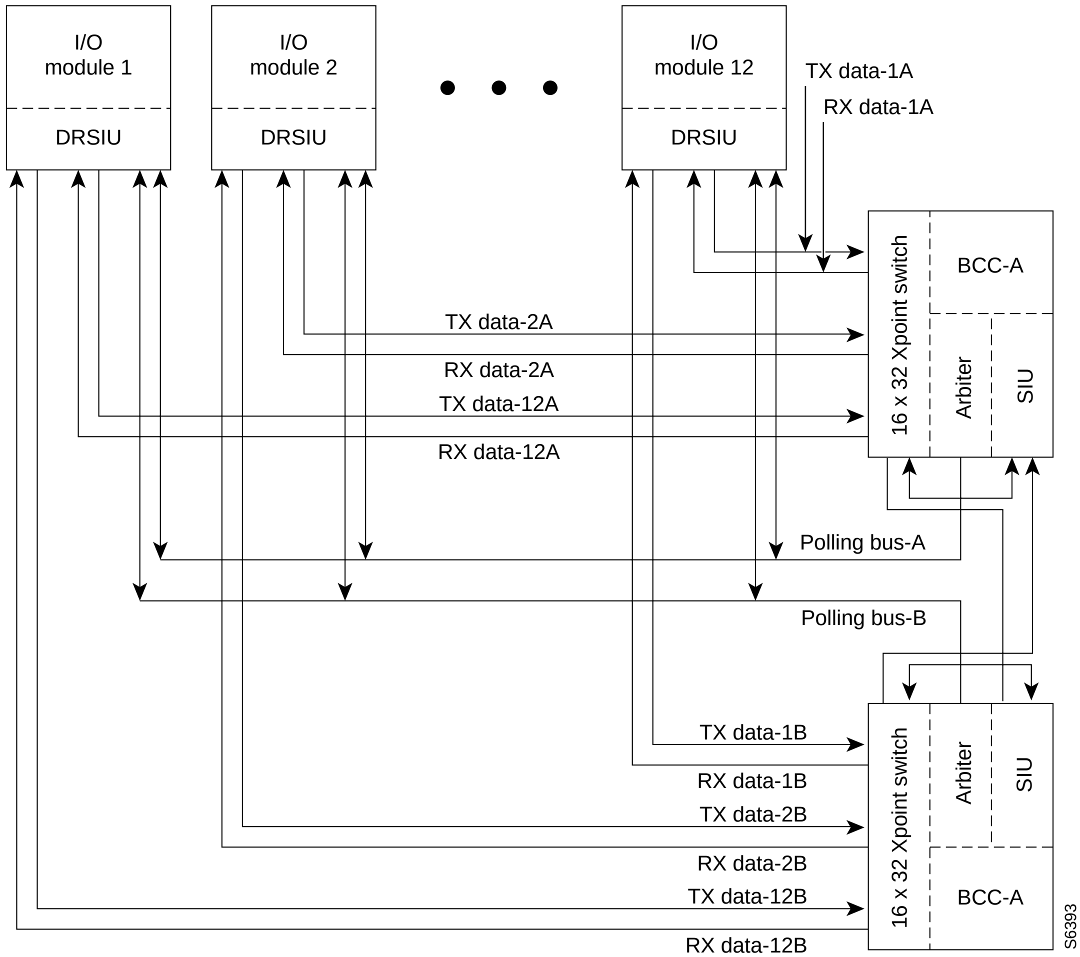


Figure 3-3 BCC4V Block Diagram



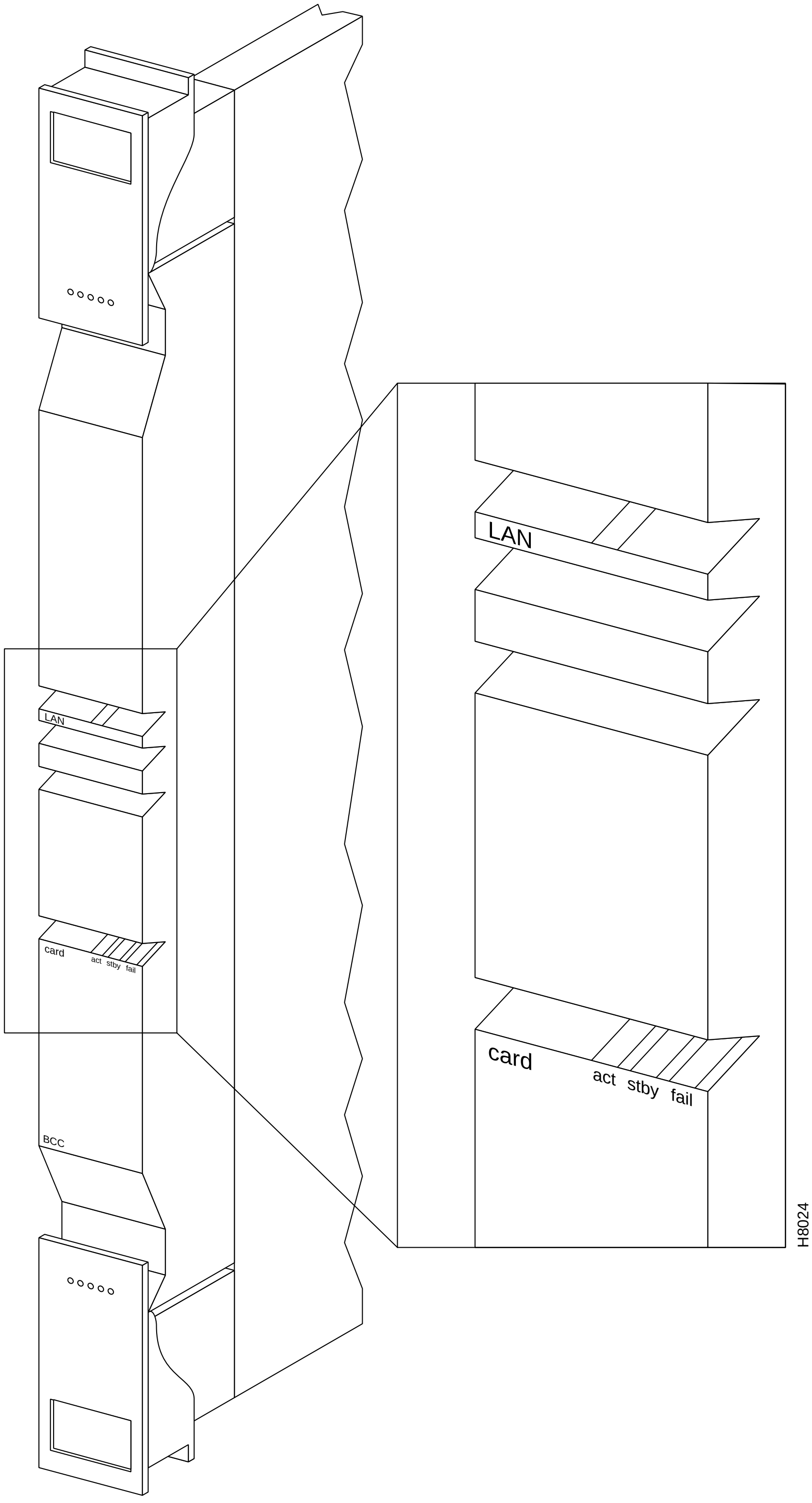
Front Panel Description

The BCC front panel has four Led, three card status LEDs, and a LAN LED. (See Figure 3-4 and Table 3-1.)

Table 3-1 BCC Front Panel Indicators

No	Indicator	Function
1	LAN	Indicates there is data activity over the Ethernet LAN port.
2	card - act	Card active LED indicates this BCC is on-line and actively controlling the node.
3	card - stby	Card standby LED indicates this BCC is off-line but is ready to take over control of the node at a moments notice.
4	card - fail	Card fail LED indicates this BCC has failed the internal self-test routine and needs to be reset or replaced.

Figure 3-4 BCC Front Panel



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

19.2 Gbps Operation with the BCC-4V

In order to operate the BPX switch at up to a 19.2 Gbps peak throughput, the following is required:

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

  Switch software 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 **despond** command which will display “Word #2 =0001” if the backplane NOVRAM has been programmed. If anything else is displayed, visually check the backplane for the fuses.

If the backplane is a 19.2 Gbps backplane, but the backplane NOVRAM has not been set to display Word #2 =0001, then 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.

Back Cards for the BCC-32, BCC-3-32M, BCC-3-64M, and BCC-4V

The backcards for the Broadband Controller Card serve as an interface between the BPX switch and the BPX switch network management system. For the BCC-32, the backcard is the BCC15-BC. For the BCC-3-32M, BCC-3-64M, and BCC-4V, the backcard is the BCC-3-BC. (These backcards are also known as the BCC backcards). The BCC-3-32M, BCC-3-64M,and the BCC-32 are functionally interchangeable except for performance, while the BCC-4V provides additional important features such as support for up to 19.2 Mbps peak operation with BXM cards. Both BCCs in a node should be of the same type. The backcard provides the following interfaces:

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

The face plate connectors are described in Table 3-2 and Table 3-3 and shown in Figure 3-5. The BCC15-BC is shown on the left and the BCC-3-BCC is shown on the right of Appendix Figure 3-5. For information on cabling, refer to Appendix B, BPX Switch Cabling Summary.

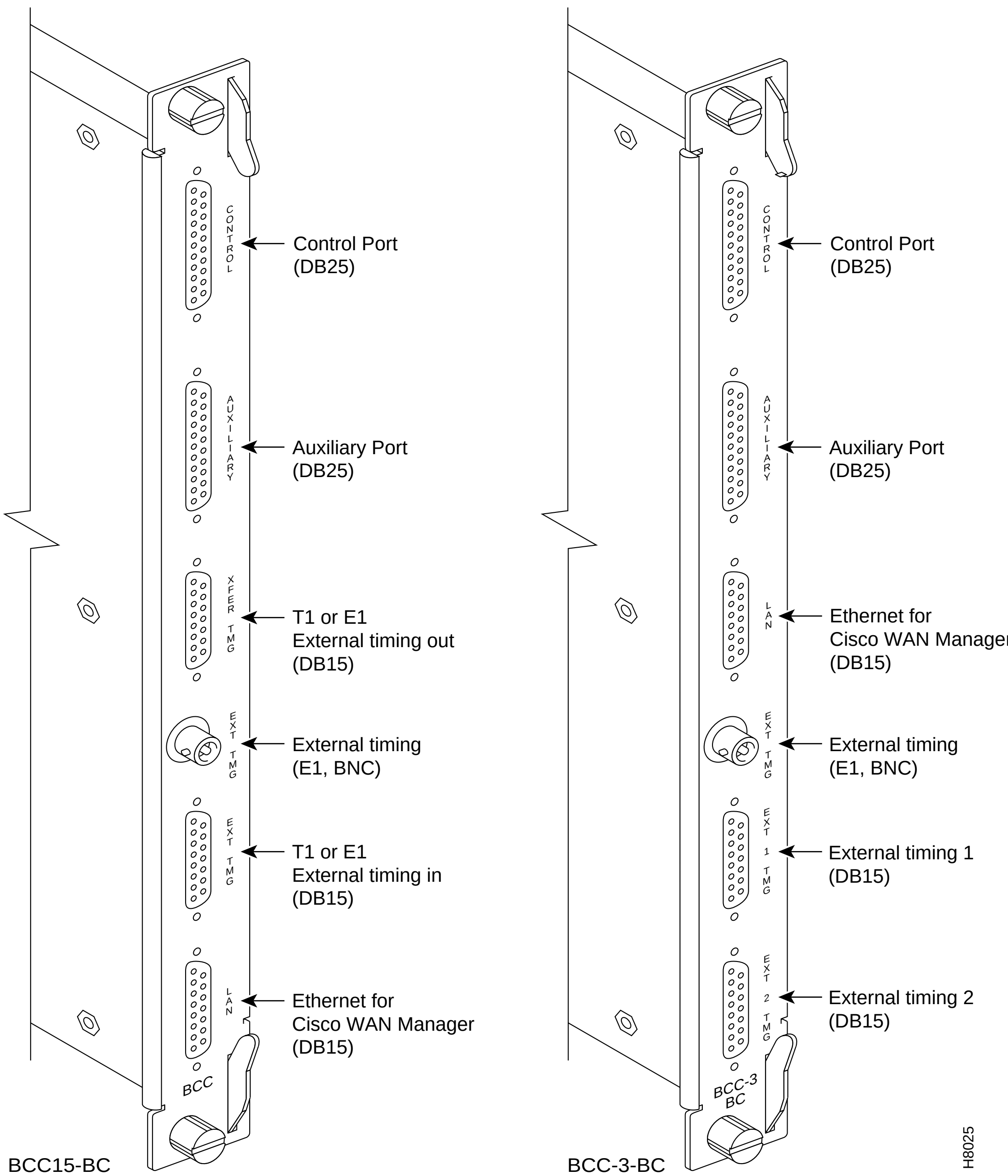
Table 3-2 BCC15-BC Backcard for BCC-32, Connectors

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

Table 3-3 BCC-3-BC Back Card for BCC-3-32, BCC-3-64, and BCC-4V

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

Figure 3-5 BCC15-BC and BCC-3-BC Backcard Face Plate Connectors



Another function of the line module back card is to provide two low-speed, serial communications ports. (Refer to Table 3-3.) The first port (CONTROL) is a bidirectional port used for connecting the BPX switch to a local terminal or to a modem for a remote terminal "dial-in" connection. The second port (AUXILIARY) is an output only and is typically used to connect to a log printer.

The CWM NMS is connected to the LAN port on the BCC backcards. When control is provided via an Ethernet interface, the node IP address is configured with the **cnflan** command for the BPX switch, and the for redundancy the LAN ports on both BCC back cards each connected to an AUI adapter. The LAN port of the primary Broadband Control Card is active. If the secondary Broadband

Control Card becomes primary (active), then its LAN port becomes active. The CWM workstation will automatically try to restore communications over the LAN and will interface with the newly active Broadband Controller Card.

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

Alarm/Status Monitor Card

The Alarm/Status Monitor (ASM) card is a front card and a member of the BPX switch Common Core group. Only one is required per node and it is installed in slot 15 of the BPX switch. It is used in conjunction with an associated back card, the Line Module for the ASM (LM-ASM) card. The ASM and LM-ASM cards are non-critical cards used for monitoring the operation of the node and not directly involved in system operation. Therefore, there is no provision or requirement for card redundancy.

Features

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

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

Functional Description

There are four significant circuits controlled by the ASM processor: alarm, power supply monitor, fan and temperature monitor, and card detection. The alarm monitor controls the operation of the front panel alarm LEDs and ACO and history pushbuttons as well as the alarm relays which provide dry contact closures for alarm outputs to customer connections. BPX switch system software commands the ASM card to activate the major and minor alarm indicators and relays.

The power supply monitor circuit monitors the status of the -48V input to the shelf on each of the two power buses, A and B. The status of both the A bus and B power bus is displayed on the ASM front panel.

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

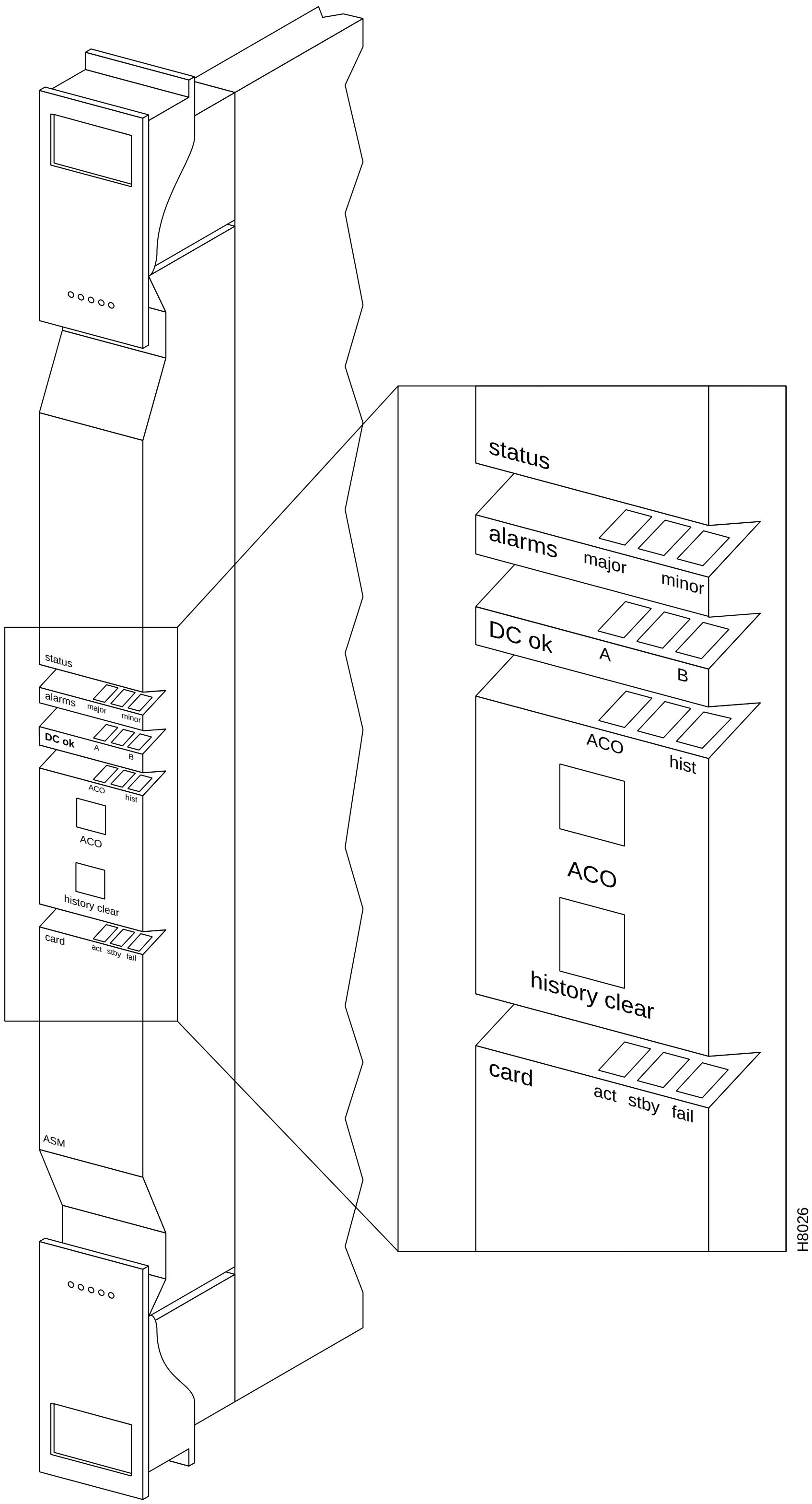
Front Panel Description

The front panel displays the status of the node and any major or minor alarms that may be present. Figure 3-6 illustrates the front panel of the ASM card. Each front panel feature is described in Table 3-4.

Table 3-4 ASM Front Panel Controls and Indicators

No	Controls/ Indicator	Function
1	alarms LEDs	A red major alarm and a yellow minor alarm indicator to display the status of the local node. In general, a major alarm is service-affecting whereas a minor alarm is a non-service affecting failure.
2	dc LEDs	Two green LEDs displaying the status of the two dc power busses on the Stratabus backplane. On–indicates voltage within tolerance. Off–indicates an out-of-tolerance voltage.
3	ACO/hist LEDs	ACO LED (yellow) lights when the front panel ACO pushbutton is operated. History LED (green) indicates an alarm has been detected by the ASM at some time in the past but may or may not be clear at present time.
4	ACO switch	When operated, releases the audible alarm relay.
5	history clear switch	Extinguishes the history LED if the alarm condition has cleared. If the alarm is still present when the history clear switch is thrown, the history LED will stay lit.
6	card status LEDs	Active (green) indicates card is on-line and clear of alarms. Standby (yellow) indicates card is off-line. Fault (red) indicates a card failure is detected by the card self-test diagnostics.

Figure 3-6 ASM Front Panel Controls and Indicators



Line Module for the Alarm/Status Monitor Card

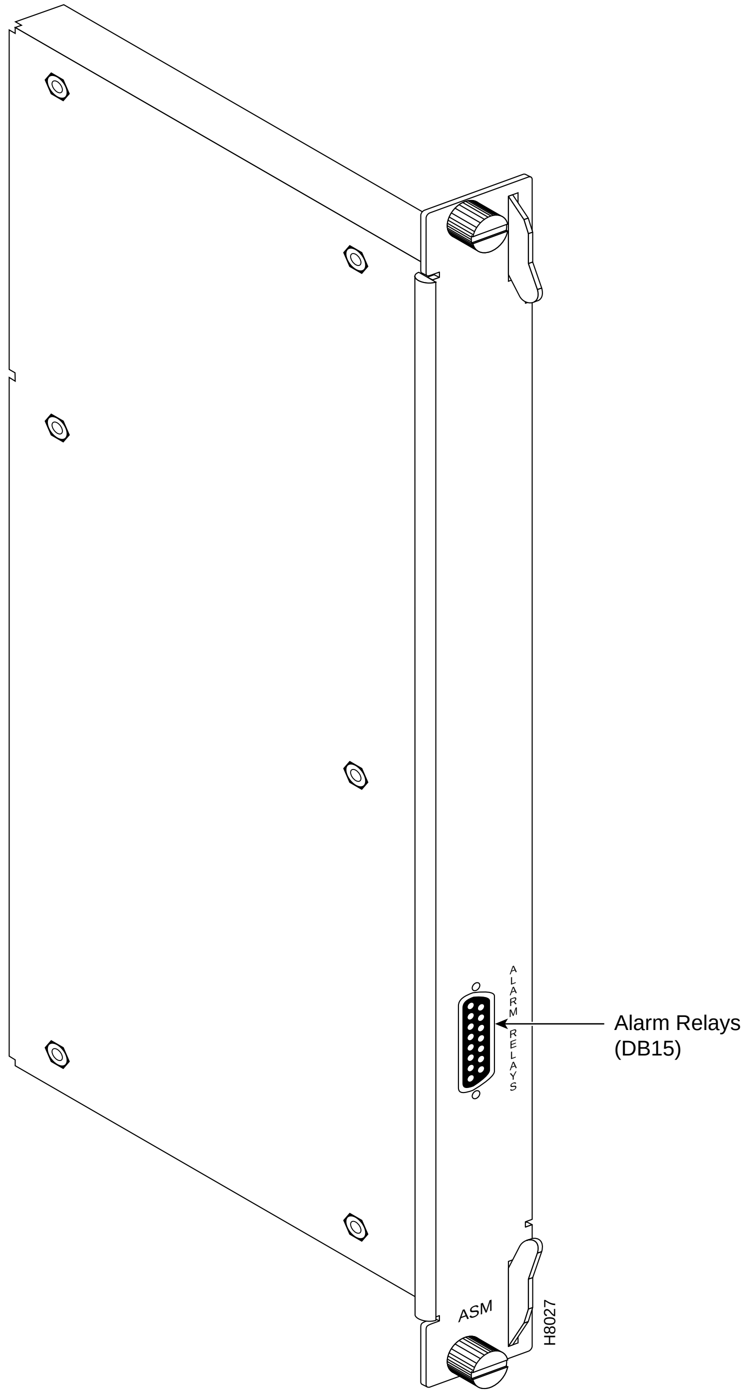
The Line Module for the Alarm/Status Monitor Card (LM-ASM) is a back card to the ASM card. It provides a simple connector panel for interfacing to the customer alarm system. It is not required for system and ASM operation and must be installed in back slot number 15.

Figure 3-7 illustrates the face plate of the LM-ASM which contains a single subminiature connector (see Table 3-5). The Alarm Relay connector provides dry-closure (no voltage) relay contact outputs.

Table 3-5 LM-ASM Face Plate Connectors

No	Connector/ Indicator	Function
1	ALARM RELAYS	A DB15 connector for alarm relay outputs. Refer to Chapter 3 or Appendix C for pinouts.

Figure 3-7 LMI-ASM Face Plate



BPX Switch StrataBus 9.6 and 19.2 Gbps Backplanes

The BPX switch may be equipped with a backplane that supports either a 9.6 or up to 19.2 Gbps operation. The 19.2 Gbps backplane can physically be identified by the card slot fuses on the bottom rear of the backplane. All BPX switch modules are interconnected by the BPX switch StrataBus backplane physically located between the front card slots and the back card slots. Even though the ATM data paths to/from the switching fabric and the interface modules are individual data connections, there are also a number of system bus paths used for controlling the operation of the BPX switch. The StrataBus backplane, in addition to the 15 card connectors, contains the following signal paths:

- ATM crosspoint wiring—individual paths used to carry ATM trunk data between both the network interface and service interface module(s) and the crosspoint switching fabric.
- Polling bus—used to carry enable signals between the BCC and all network interface modules.
- Communications bus—used for internal communications between the BCC and all other cards in the node.
- Clock bus—used to carry timing signals between the BCC and all other system cards.
- Control bus—enables either the A bus wiring or B bus wiring.

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

PART 3

Service and Trunk Cards

BNI (Trunk) Cards

This chapter contains a description of the Broadband Network Interface (BNI) card and associated backcards. For a description of the BXM cards which provide both service interfaces (line) and network interfaces (trunk), refer to *Chapter 6, BXM T3/E3, 155, and 622*.

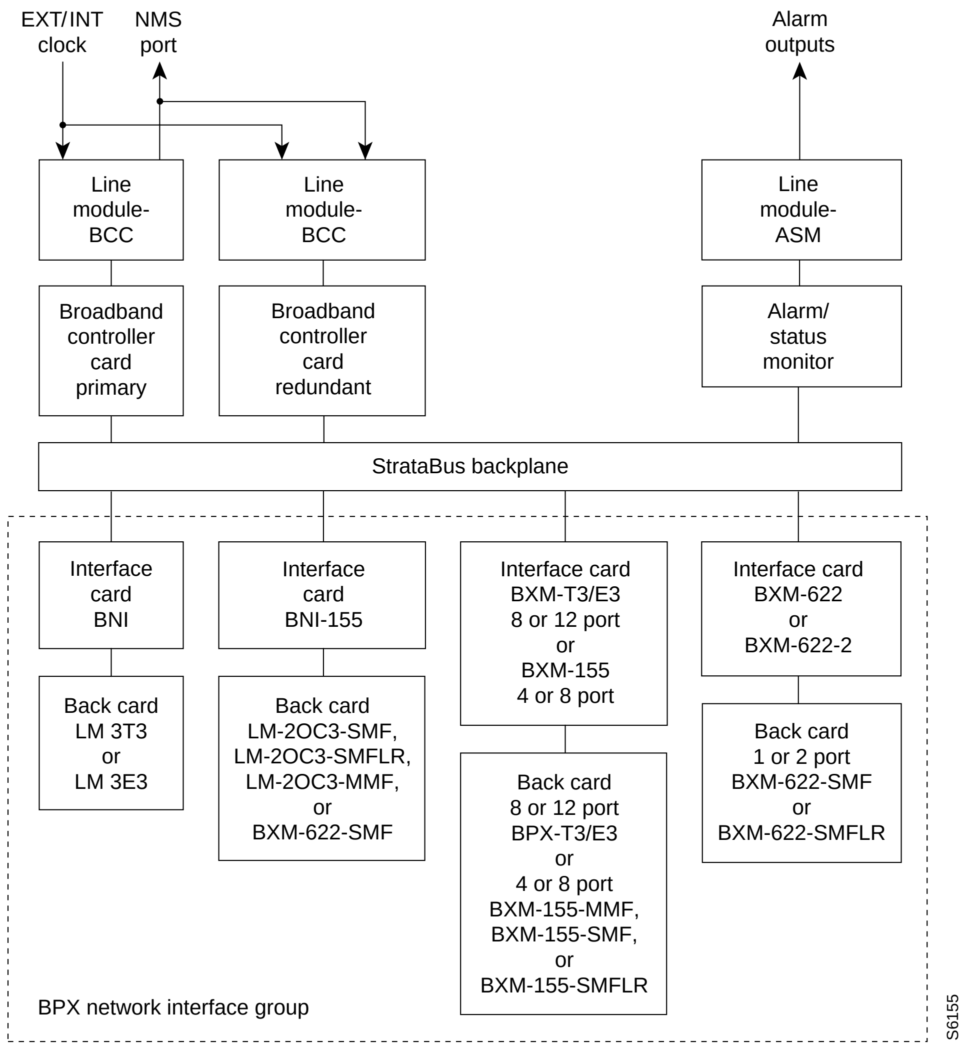
This chapter contains the following:

- BPX Switch Network Interface Group
- Broadband Network Interface Cards (BNI-T3 and BNI-E3)
- T3 and E3 Line Modules (LM-3T3 and LM-3E3)
- Broadband Network Interface Cards, BNI-155
- OC-3, Line Modules (SMF, SMFLR, & MMF)
- Y-Cabling of BNI Backcard, SMF-2-BC9

BPX Switch Network Interface Group

The BPX switch network interface group of cards provides the interface between the BPX switch and the ATM network (see Figure 4-1). The BNI series of cards (DS3, E3, and OC-3) are described in this chapter.

Figure 4-1 BPX Switch Network Interface Group



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

The BNI-T3 and BNI-E3 interface the BPX switch with ATM T3 and E3 broadband trunks, respectively. These ATM trunks may connect to either another BPX, an IPX switch equipped with an AIT card, or an MGX 8220.

The BNI-3T3 back card provides three DS3 interfaces on one card while the BNI-E3 back card provides three E3 interface ports. The BNI back card types are very similar differing only in the electrical interface and framing. Any of the 12 general purpose slots can be used to hold these cards. Each BNI operates as a pair with a corresponding Line Module back card.

Features

A summary of features for the BNI cards include:

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

Functional Description

The BNI T3 and E3 cards are functionally alike except for the two different electrical interfaces. Refer to Figure 4-2 illustrating the main functional blocks in the BNI-3T3 card.

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

Egress

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

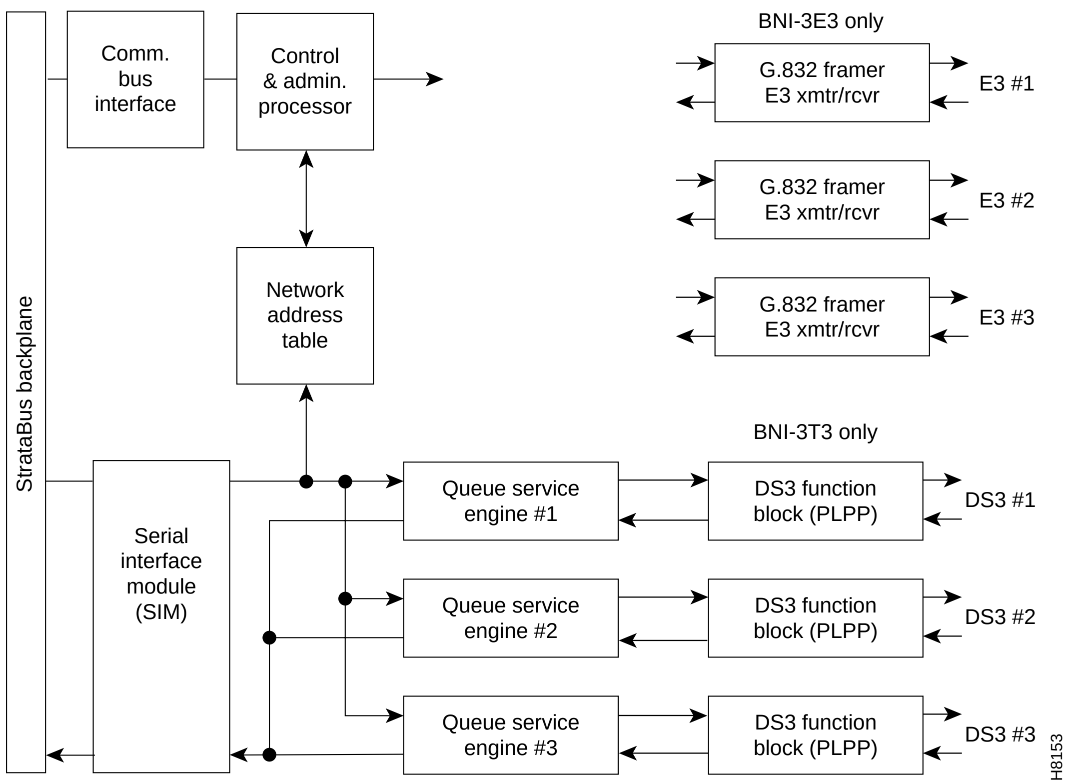
- Software controlled line buildout to match up to 900 feet (275 meters) of ABAM cable.
- Receives incoming cells from the switch matrix on the BCC.
- Queues and serves the cells based on the class-of-service algorithm.
- Sets congestion indication (EFCN) in cell header when necessary.
- Adds frame sync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

Ingress

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

- Receives incoming ATM cells from the DS3 transmission facility, stripping the framing and overhead from the received bit stream.
- Determines the address of the incoming cells by scanning the Virtual Path Identifier (VPI)/Virtual Circuit Identifier (VCI) in the cell header.
- Queues the cells for transmission through the switch matrix.
- Extracts receive timing from the input framing and makes it available for node timing. Line can operate in looped timing mode.
- Recovers clock and data from the bipolar B3ZS (T3) or HDB3 (E3) line signal and converts data to unipolar.

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



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

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

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

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

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

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

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

Bandwidth Control

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

Loopbacks and Diagnostics

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

Several loopback paths are provided. A digital card loopback path, used by the node for self-test, loops the data at the serial DS3 or E3 interface back towards the node. A digital line loopback loops the data at the electrical transmitter/receiver at the card output. Internally, the PLPP circuit in the BNI-T3 has several loopbacks for use by diagnostic routines.

There are several loopback paths within the BNI for testing. A digital loopback at the DS3 or E3 transmitter/receiver to check both the transmit and receive signal paths in the near-end BNI card. These loopbacks loop the signal in both directions, towards the StrataBus as well as towards the output. Therefore, they can be used to support both near end and far end maintenance loopback testing. On the BNI-3T3, there is a digital loopback capability to the PLPP processor used for the internal self test to basically check the operation of the signal processor.

Once a trunk has been assigned to a BNI card but before it is made active (upped), it is put in a loopback mode and a diagnostic test is continuously performed. This loopback is disruptive so it cannot be performed on a card that has an active trunk. This diagnostic test checks the data path through the BNI out to the BCC, through the switch matrix, and back to the BNI. Active trunks are constantly checked by the Communications Fail test routine which is part of system software.

Front Panel Indicators

The lower section of the BNI front panel (see Figure 4-3) has a three-section, multicolored LED to indicate the card status. The card status LED is color-coded as indicated in Table 4-1. At the upper portion of the front panel, there is a three-section multicolored LED to indicate the status of the three ports on the BNI. Types of failures are indicated by various combinations of the card status indicators as indicated in Table 4-2.

Table 4-1 BNI Front Panel Status Indicators

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

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

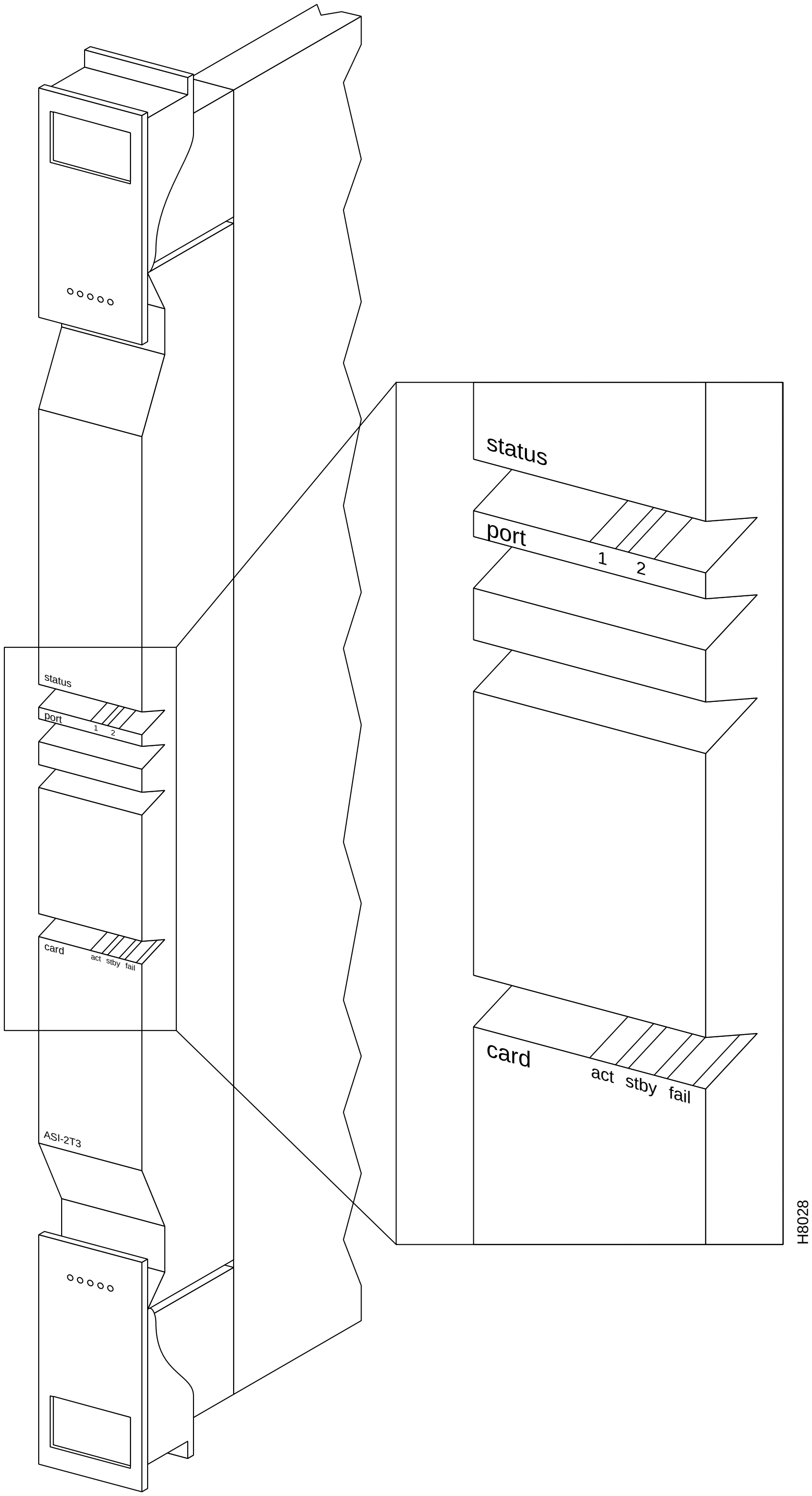


Table 4-2 BNI Front Panel Card Failure Indications

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

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

The Line Modules for the BNI-T3 and BNI-E3 front cards are back cards used to provide a physical interface to the transmission facility. The LM-3T3 is used with the BNI-T3 and the LM-3E3 with the BNI-3E3. The Line Module connects to the BNI through the StrataBus midplane. Two adjacent cards of the same type can be made redundant by using a Y-cable at the port connectors. All three ports on a card must be configured the same.

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

The LM-3T3 and LM-3E3 provides the following features:

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

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

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

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

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

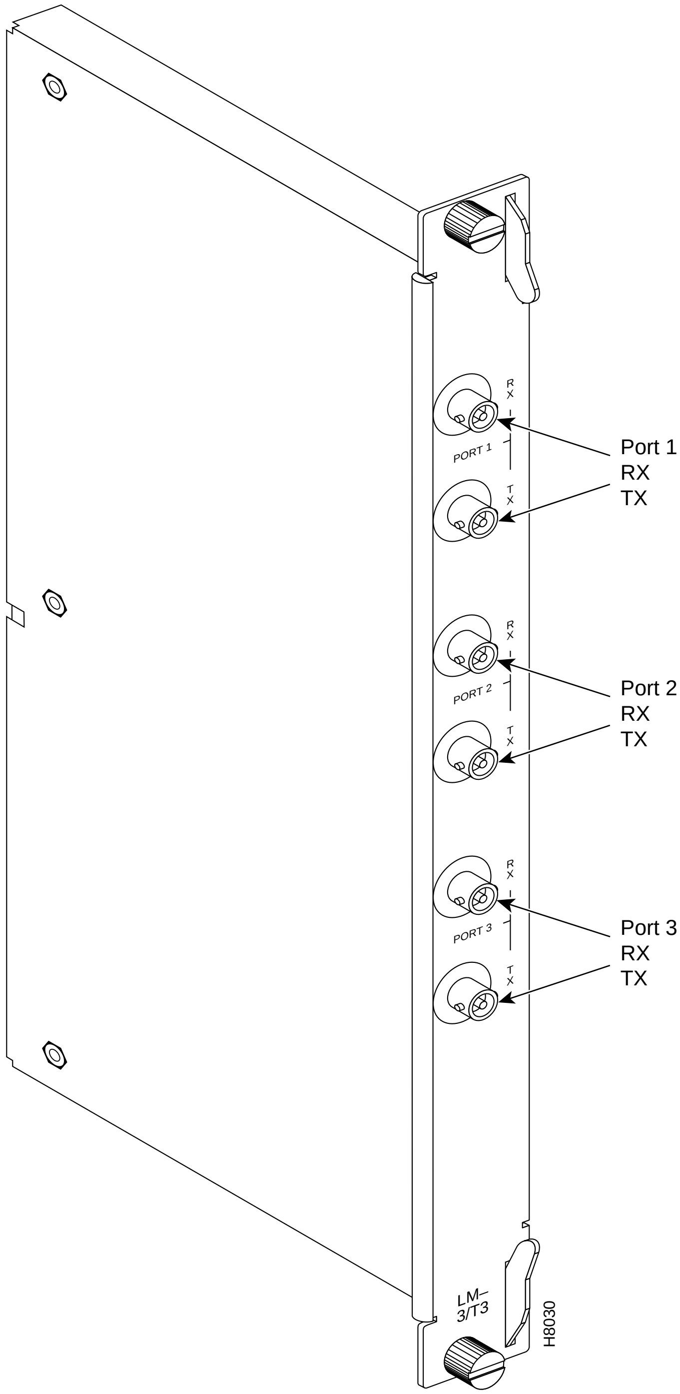
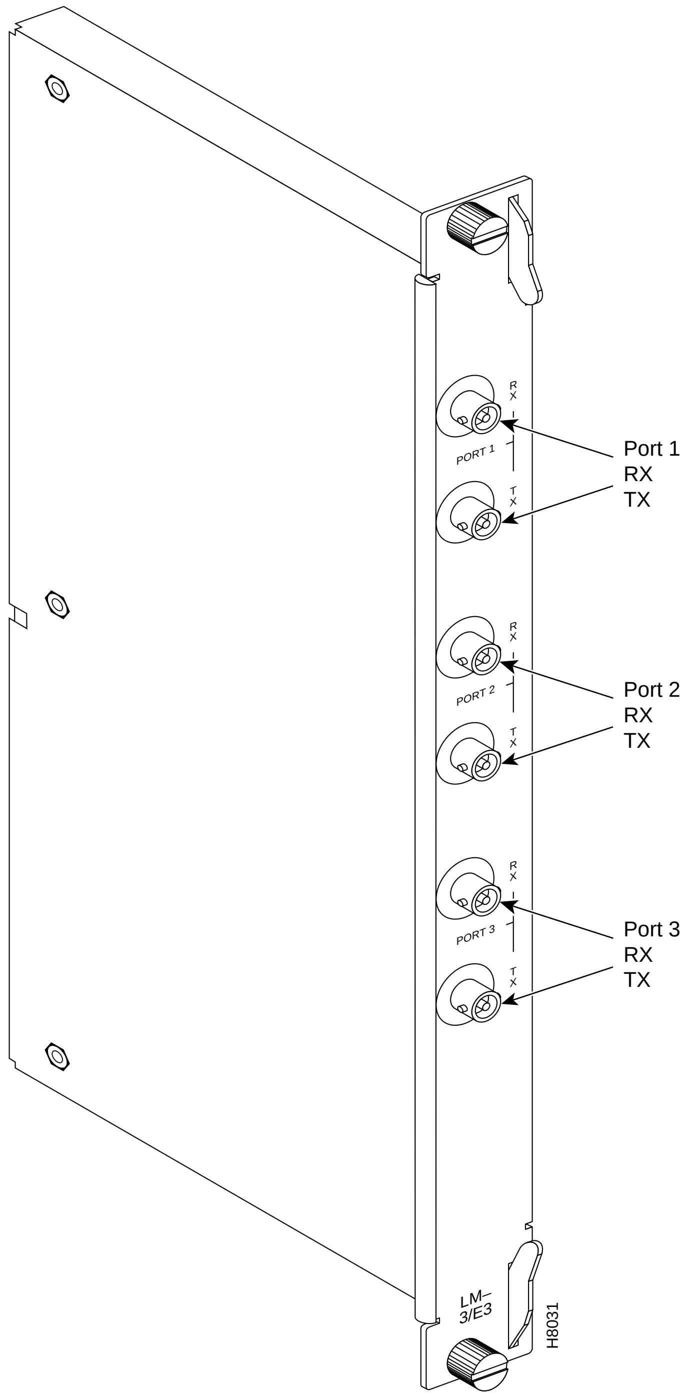


Figure 4-5 LM-3E3 Face Plate, Typical



Broadband Network Interface Cards, BNI-155

The BNI-155 interfaces the BPX switch with ATM OC-3/STM-1 broadband trunks. The ATM trunk may connect to either another BPX switch or customer CPE equipped with an ATM OC-3/STM-1 interface.

There are three BNI-155 back cards, the LM-2OC-3-SMF for single-mode fiber intermediate range, the LM-2OC-3-SMFLR for single-mode fiber long range, and the LM-2OC-3-MMF for multi-mode fiber. Any of the 12 general purpose slots can be used to hold these cards. These backcards may also be used with the ASI-155.

Features

A summary of features for the BNI-155 cards include:

- LM-OC-3-SMF and LM-OC-3-MMF cards provide two ports, each operating at 155.52 Mbps.
- Up to 353,208 cells per second.
- Up to 12 class-based queues for each port.
- 8 K cell ingress (receive) VBR buffer.
- 32 K cell egress (transmit) buffers.
- 800 Mbps backplane speed.
- Two-stage priority scheme for serving cells.
- Accumulates trunk statistics for OC-3/STM-1.
- Optional 1:1 card redundancy using Y-cable configuration for BNI-155.

Overview

Egress

In the transmit direction (from the BPX switching matrix towards the transmission facility, referred to as egress), the BNI performs the following functions (see Figure 4-6):

- Receives incoming cells from the switch matrix on the BCC.
- Serves the cells based on the class-of-service algorithm.
- Sets congestion indication (EFCN) in cell header when necessary.

Ingress

In the receive direction (from the transmission facility towards the BPX switching matrix, referred to as ingress), the BNI performs the following functions (see Figure 4-6):

- Receives incoming ATM cells from the OC-3 transmission facility, stripping the framing and overhead from the received bit stream.
- Determines the address of the incoming cells by scanning the Virtual Path Identifier/Virtual Circuit Identifier (VPI/VCI) in the cell header.

Functional Description

In the egress direction, the BNI-155 has 2 Queue Service Engine (QSEs) which provide each of the ports with up to 12 programmable queues with selectable parameters such as minimum bandwidth, priority, and maximum bandwidth. The BNI queues are based on a class of service algorithm. The BNI supports the following trunk queues:

- Voice
- Non-Time Stamped
- Time Stamped
- Bursty Data A
- Bursty Data B
- High Priority (Network Management Traffic)
- CBR
- VBR

In the ingress direction, the BNI-155 has 2 Cell Input Engines (CIEs) that convert the incoming cell headers to the appropriate connection ID based on input from a Network Address Table.

The Serial Interface Unit (SIU) provides the BNI with an 800 Mbps cell interface to the StrataBus. It provides serial-to-parallel conversion of data, along with loopback and test signal generation capabilities.

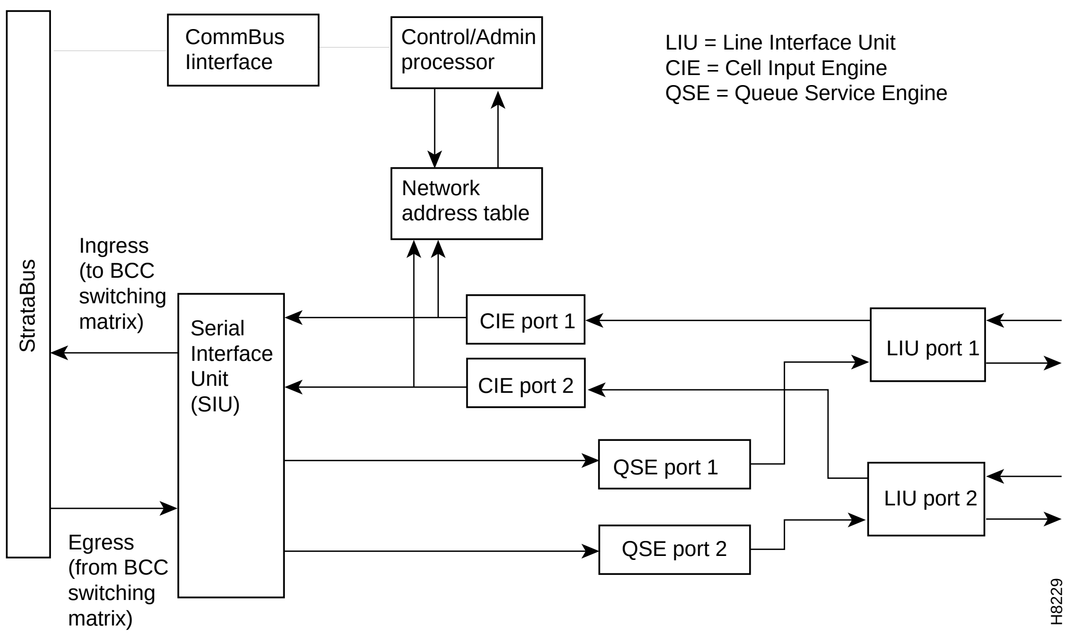
The Line Interface Unit (LIU) performs the following ingress functions:

- Provides framing detection and synchronization.
- Provides the ability to extract timing from the incoming signal, and use it as a receive clock for incoming data, while providing transmit clock in the other direction. Alternatively, loop timing can be used to turn the receive clock back around to be used as a transmit clock. The receive clock may also be used to synchronize the node.
- Detects alarms, frame errors, and parity errors.
- Detects far end errors, including framing errors, and yellow alarm indications.
- Provides optional cell descrambling, header error check (HEC), and idle cell filtering.
- Provides a small FIFO buffer for incoming cells.
- Provides optical to electrical conversion.

The Line Interface Unit (LIU) performs the following egress functions:

- Inserts the appropriate framing into the outgoing bit stream.
- Inserts any alarm codes for transmission to the far end.
- Provides optional cell scrambling, HEC generation, and idle cell insertion.
- Provides a small FIFO buffer outing cells.
- Provides electrical to optical conversion.

Figure 4-6 Simplified BNI-155 Block Diagram



Front Panel Indicators

The BNI-155 front panel (see Figure 4-7) has a three-section, multicolored “card” LED to indicate the card status. The card status LED is color-coded as indicated in Table 4-4. A three-section multicolored “port” LED indicates the status of the two ports on the BNI-155. Types of failures are indicated by various combinations of the card status indicators as indicated in Table 4-5.

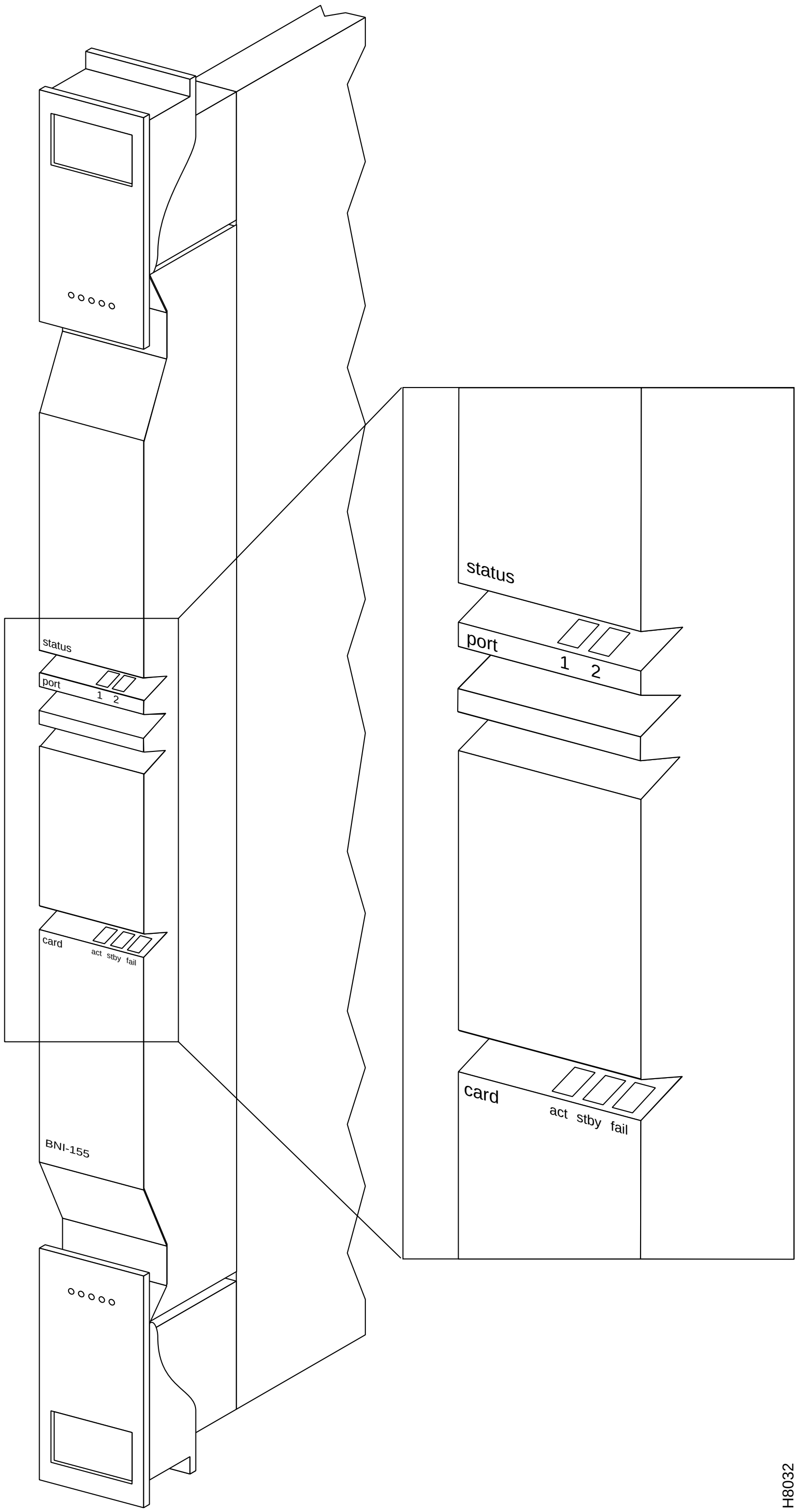
Table 4-4 BNI-155 Front Panel Status Indicators

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

Table 4-5 BNI Front Panel Card Failure Indications

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

Figure 4-7 BNI-155 Front Panel



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

The Line Modules for the OC-3 BNI cards are back cards used to provide a physical interface to the transmission facility. There are three types, a single-mode fiber intermediate range, single-mode fiber long range, and a multi-mode fiber backcard. The Line Modules connect to the BNI through the StrataBus midplane.

For connector information, refer to Figure 4-8 and Table 4-6 for the LM-OC-3-SMF and to Figure 4-9 and Table 4-7 for the LM-OC-3-MMF. The LM-OC-3-SMFLR uses the same type of connectors as the LM-OC-3-SMF.

Table 4-6 LM-OC-3-SMF and LM-OC-3-SMFLR Connectors

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

Table 4-7 LM-OC-3-MMF Connectors

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

Figure 4-8 LM-2OC-3-SMF Face Plate

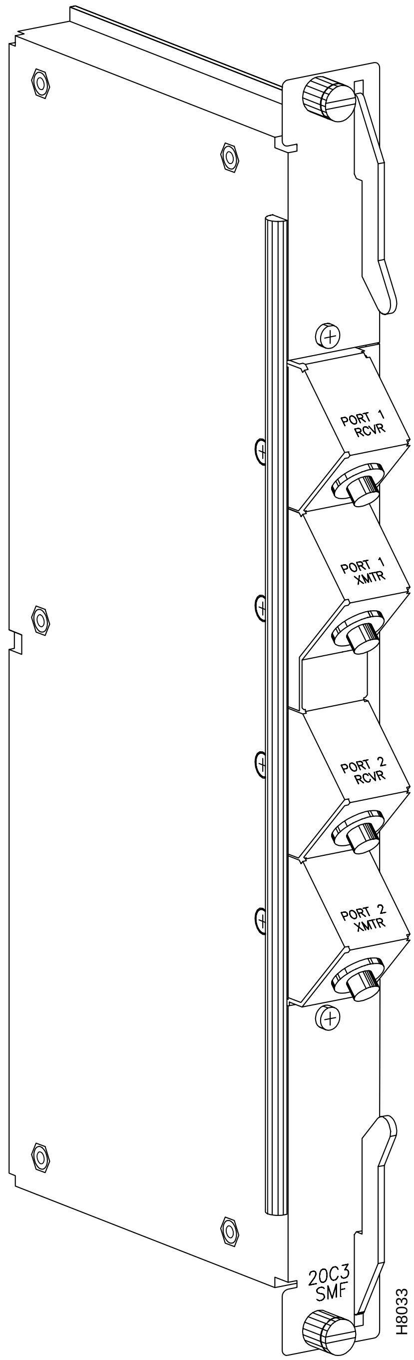
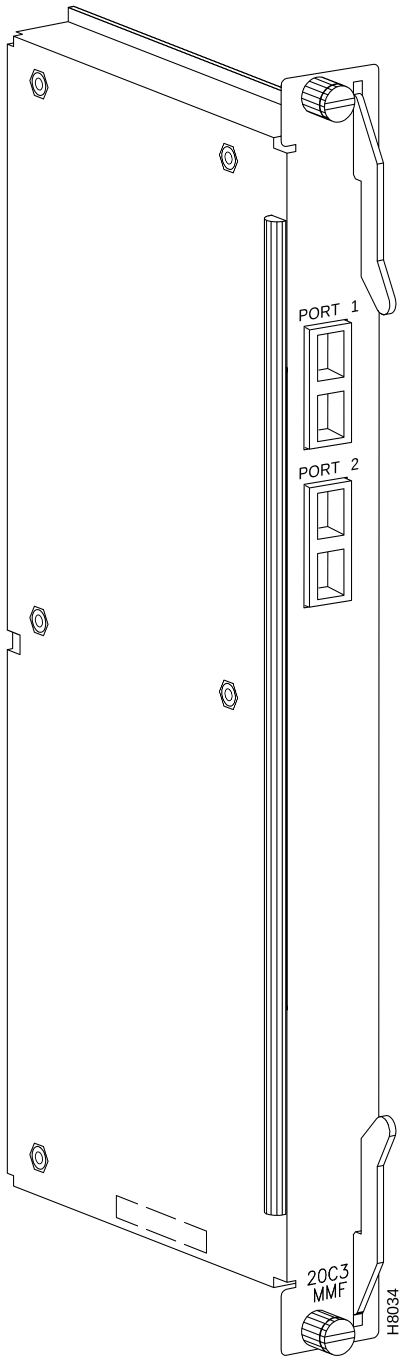


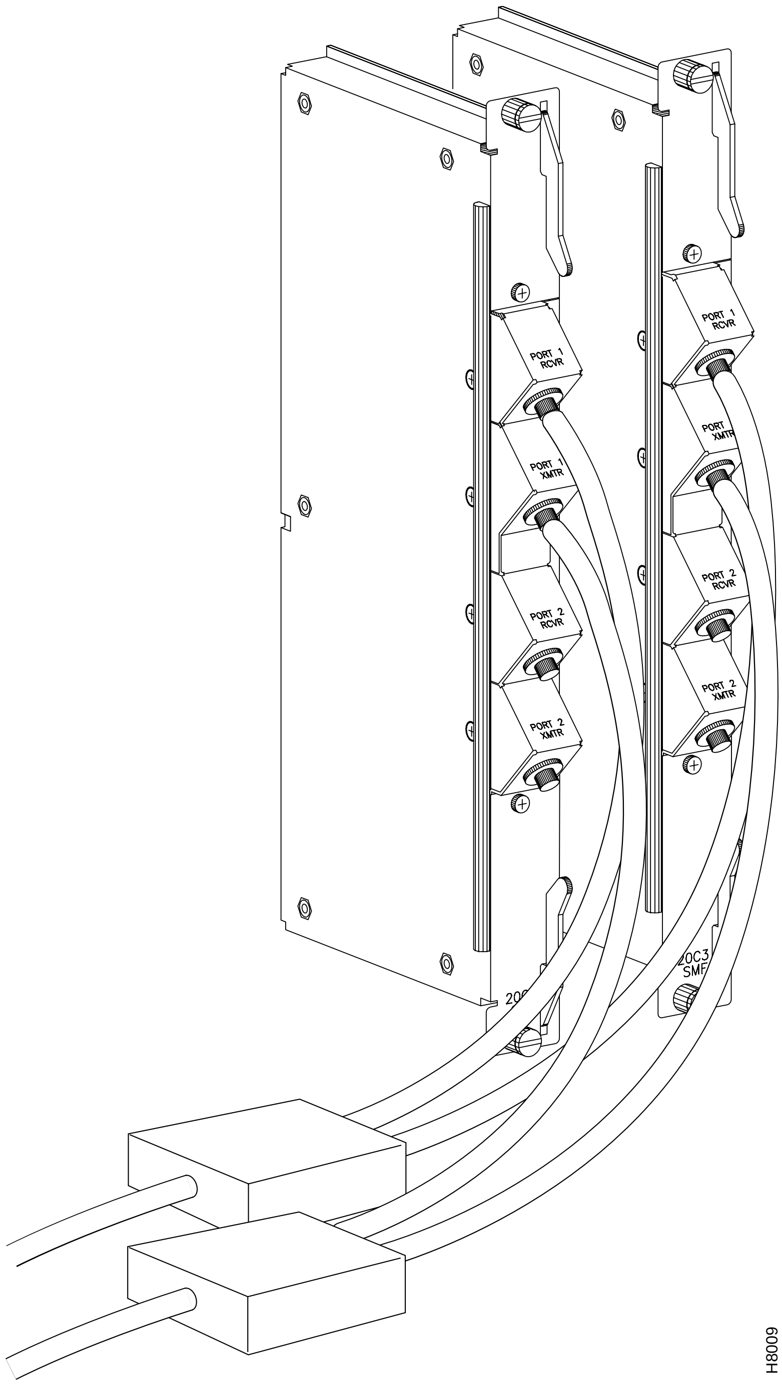
Figure 4-9 LM-2OC-3-MMF Face Plate



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

The LM-OC-3-SMF (Model SMF-2-BC) backcards may be Y-cabled for redundancy using the Y-Cable splitter shown in Figure 4-10. The cards must be configured for Y-Cable redundancy using the **addyred** command.

Figure 4-10 Y-Cable (Model SMFY), LC-OC-3-SMF (Model SMF-2-BC)



ASI Service Interface (Line) Cards

This chapter contains a description of the ATM Service Interface (ASI) and associated backcards.For a description of the BXM cards which provide both service interfaces (line) and network interfaces (trunk), refer to *Chapter 6, BXM T3/E3, 155, and 622*.

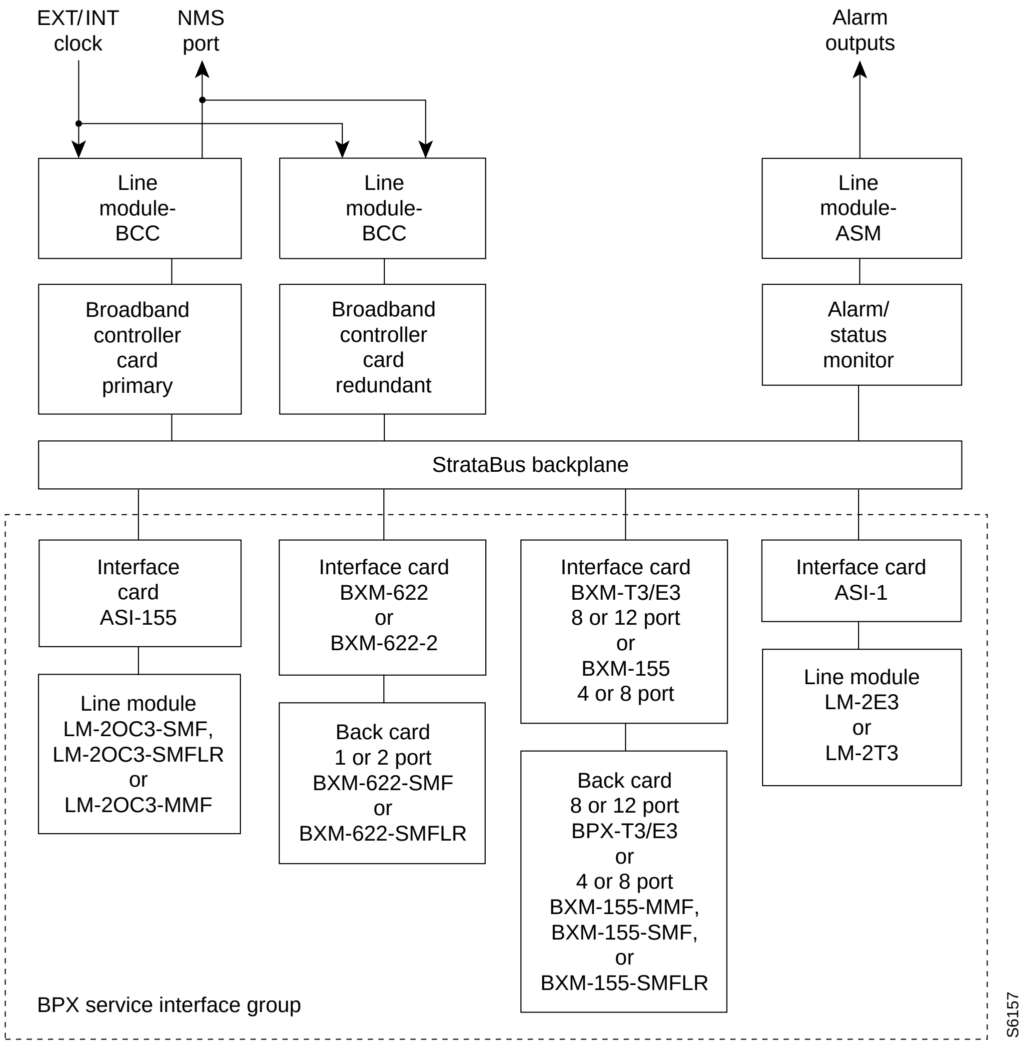
This chapter contains the following:

- BPX Switch Service Interface Group Summary
- ASI-1, ATM Service Interface Card
- LM-2T3 Module
- LM-2E3 Module
- ASI-155, ATM Service Interface Card
- ASI-155 Line Module, LM-2OC-3-SMF
- ASI-155 Line Module, LM-2OC-3-SMFLR
- ASI-155 Line Module, 2OC-3-MMF
- Y-Cabling of ASI Backcard, SMF-2-BC

BPX Switch Service Interface Group Summary

The BPX switch service interface group of cards provides an ATM interface between the BPX switch and CPE (see Figure 5-1). The ASI series of cards (DS3, E3, and OC-3) are described in this chapter.

Figure 5-1 BPX Switch Service Interface Group



ASI-1, ATM Service Interface Card

The ATM Service Interface Card for T3 and E3 interfaces (ASI-1) is a front card for use in the BPX switch to interface an ATM user device, such as, Customer Premise Equipment (CPE). The ASI provides an industry-standard ATM User-to-Network Interface (UNI) or ATM Network-to-Network Interface (NNI) to the BPX switching fabric.

Features

A summary of features for the ASI card include:

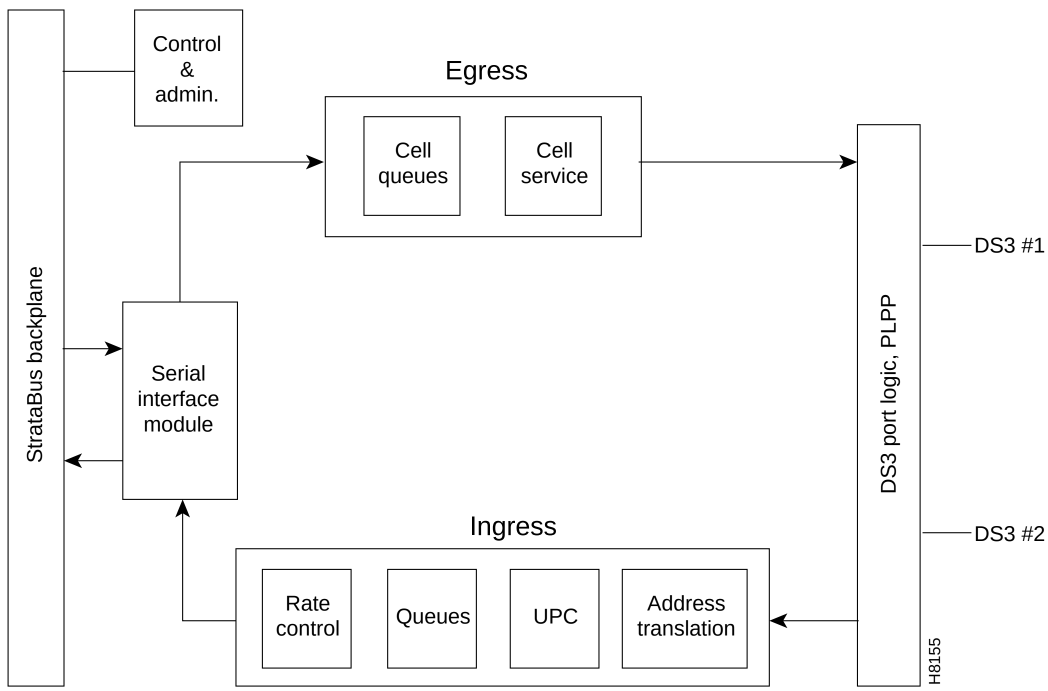
- Two 45 Mb T3 ATM UNI/NNI ports per card for connection of user devices.
- Allows connections between UNI ports on a single node, between nodes, and NNI connections between networks.
- Maximum of 1000 connections per card.

- Aggregate transport rate of 96,000 cps per port (T3) or 80,000 cps (E3).
- VCC and/or VPC addressing.
- Ingress to ASI, each PVC is assigned a separate input queue.
- Egress from ASI, sixteen fixed queues per line, including CBR, VBR, and ABR queues.
- Optional 1:1 card redundancy using Y-cable configuration.

Functional Description

Each ASI-1 card provides two ATM UNI/NNI ports, each operating at DS3 rates or E3 rates (see Figure 5-2). Any of the 12 general purpose slots can be used to hold these cards. The ASI-1 operates with a corresponding T3 or E3 Line Module back card LM-2T3 or LM-2E3, respectively. Only the first two connectors on the back card are active; the lower port is not used.

Figure 5-2 ASI-1 Simplified Block Diagram



Each port provides an aggregate ATM connection bandwidth of 96,000 cells/second (T3) or 80,000 cells/sec (E3), or 353,208 cells/sec (OC-3).

Connections are added using the **addcon** command.

Some of the functions performed by the PLPP in the ASI-1 include:

PLPP—Receiver Side

- Provides frame sync for the C-bit parity frame format.
- Provides alarm detection and accumulates B3ZS code violations framing errors, parity errors, C-bit parity errors, and far end bit error (FEBE) events.
- Detects far end alarm channel codes, yellow alarm, and loss of frame.

- Provides optional cell descrambling, header check sequence (HCS) error detection, and cell filtering.
- Small receive FIFO buffer for incoming cells.

Connections are routed using the VPI and VCI address fields in the UNI header. The allowable range for VPI is from 0 to 255 (UNI) and 0 to 1023 (NNI), while VCI can range from 1 to 65535. A total of 1000 combinations of these can be used per ASI card at any one time.

A total of 1000 logical connections (ungrouped) may be configured for the node at any one time. On the BPX switch, 5000 grouped connections can be configured. The ASI-1 supports 1000 connections per card.

Two connection addressing modes are 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.

There are sixteen egress queues per line (port), including CBR, VBR, and ABR. When a connection is added, the user selects either constant bit rate (CBR), variable bit rate (VBR), or available bit rate (ABR, which uses ForeSight). The CBR queue has higher priority. Queue depth is specified when configuring a line. Maximum depth that can be specified for any one queue is 11,000 cells. Total queue depth cannot exceed 22,000 cells.

Configuring Connections (ATM over ASI Example)

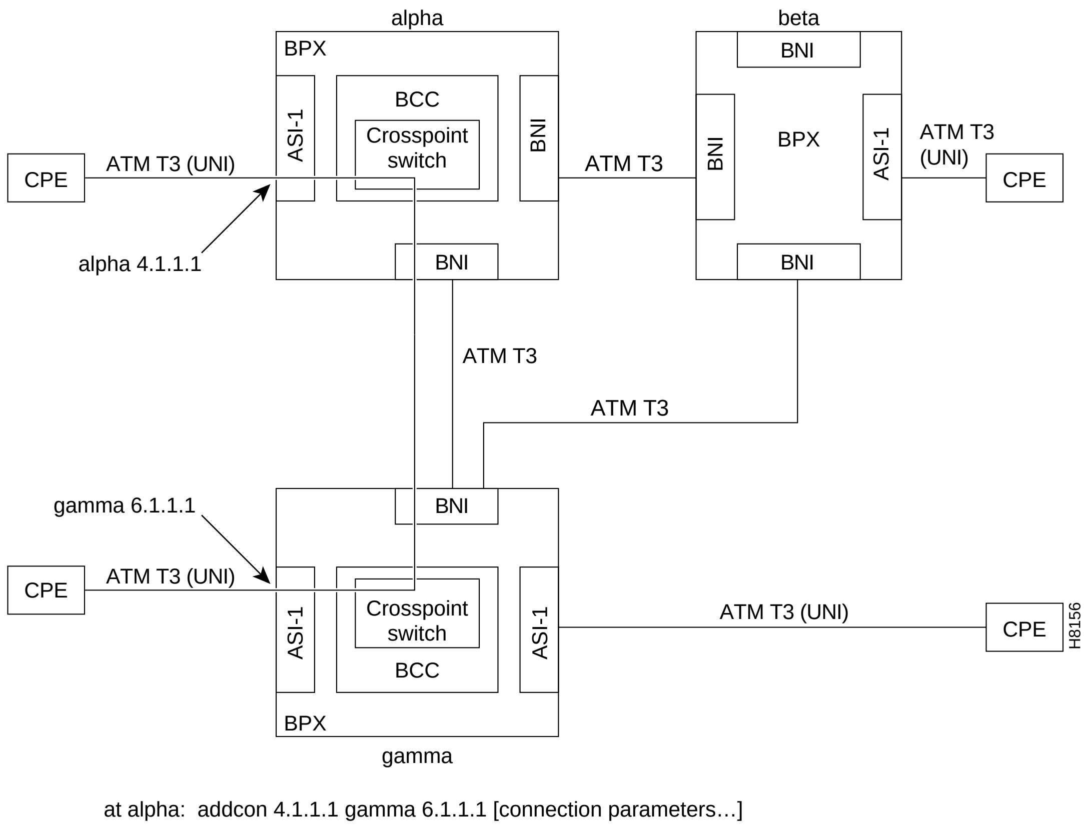
Connections are routed between CPE connected to ASI ports (see Figure 5-3). Before adding connections, an ASI line is upped with the **upln** command and configured with the **cnfln** command. Then the associated port is configured with the **cnfport** command and upped with the **upport** command. Following this, the ATM connections are added via the **addcon** command with the syntax: slot.port.vpi.vci. The example shows a connection between alpha 4.1.1.1 and gamma 6.1.1.1.

The slot number is the ASI card slot on the BPX switch. The port number is one of two ports on the ASI, the VPI is the virtual path identifier, and the VCI is the virtual circuit identifier. (The top two ports on the LM-2T3 card are used, the bottom one is not.)

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. Refer to the *Cisco WAN Switching Command Reference* for further information.

Figure 5-3 ATM Connection via ASI Ports



Monitoring Statistics

Port, line, and channel statistics are collected by the ASI-1. Refer to the *Cisco StrataView Plus Operations Guide* for a listing and description of these statistics.

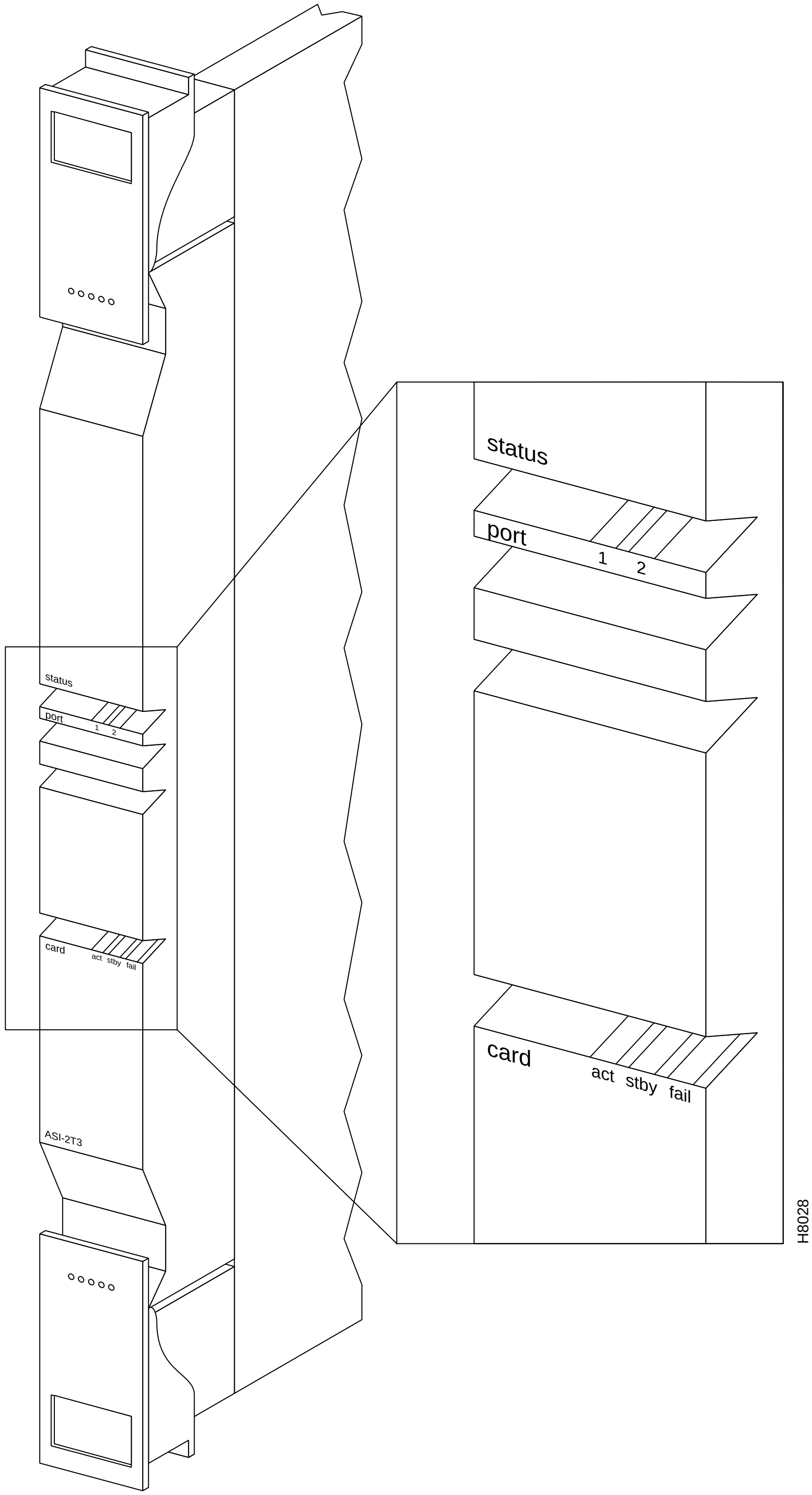
Front Panel Description

The ASI front panel (see Figure 5-4) has a three-section, multicolored “card” LED to indicate the card status. The card status LED is color-coded as indicated in Table 5-1. A two-section multicolored “port” LED indicates the status of the two ports on the ASI. The port status LED display is color-coded as indicated in Table 5-1.

Table 5-1 ASI-1 Status Indicators

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

Figure 5-4 ASI-1 Front Panel



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

The Line Modules for the ASI-T3 and ASI-E3 front cards are back cards used to provide a physical interface to the transmission facility. They are the same backcards used by the BNI-T3 and BNI-E3, except that only two ports are used by the ASI. The LM-3T3 is used with the BNI-T3 and the LM-3E3 with the BNI-3E3. The Line Module connects to the BNI through the StrataBus midplane. Two adjacent cards of the same type can be made redundant by using a Y-cable at the port connectors. All three ports on a card must be configured the same.

Refer to Figure 5-5, Figure 5-6, and Table 5-2 which describe the faceplate connectors of the LM-3T3 and LM-3E3. There are no controls or indicators.

The LM-3T3 and LM-3E3 provide the following features:

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

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

Table 5-2 LM-3T3 and LM-3E3 Connectors

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

Figure 5-5 Line Module, ASI, LM-3T3 (only two ports used)

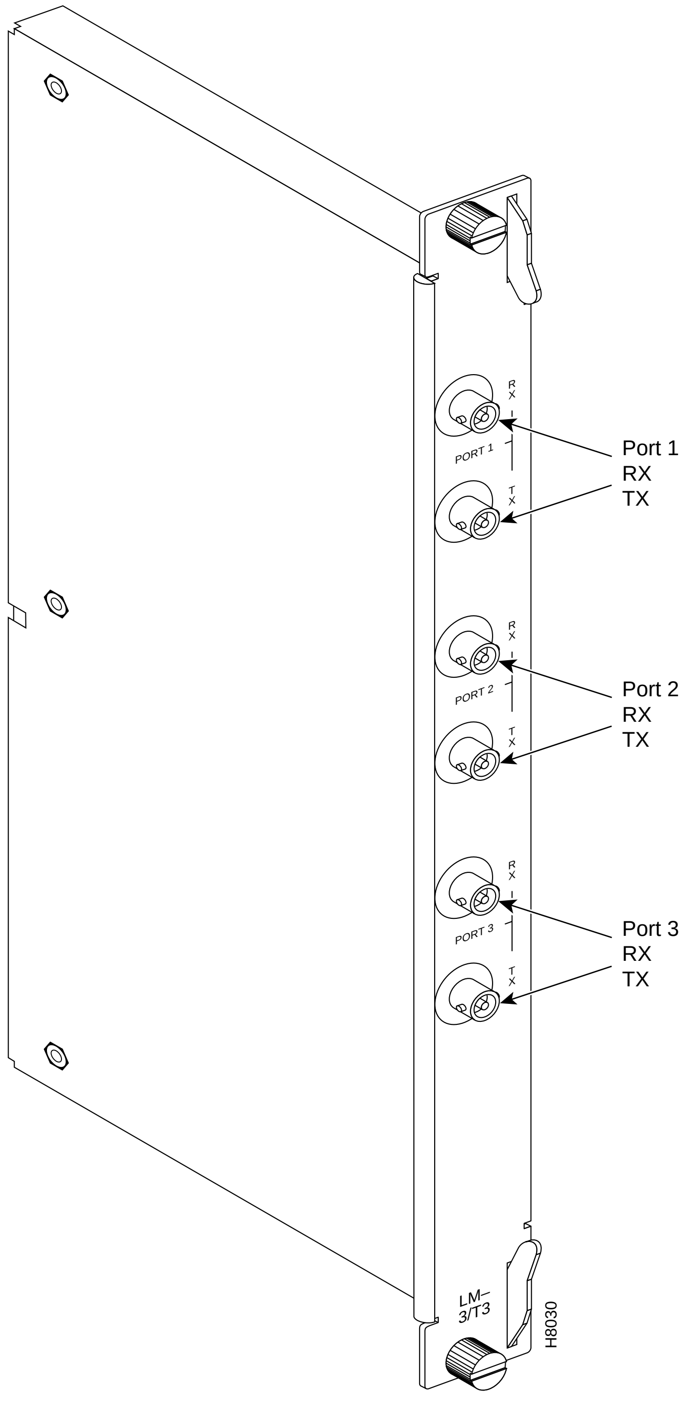
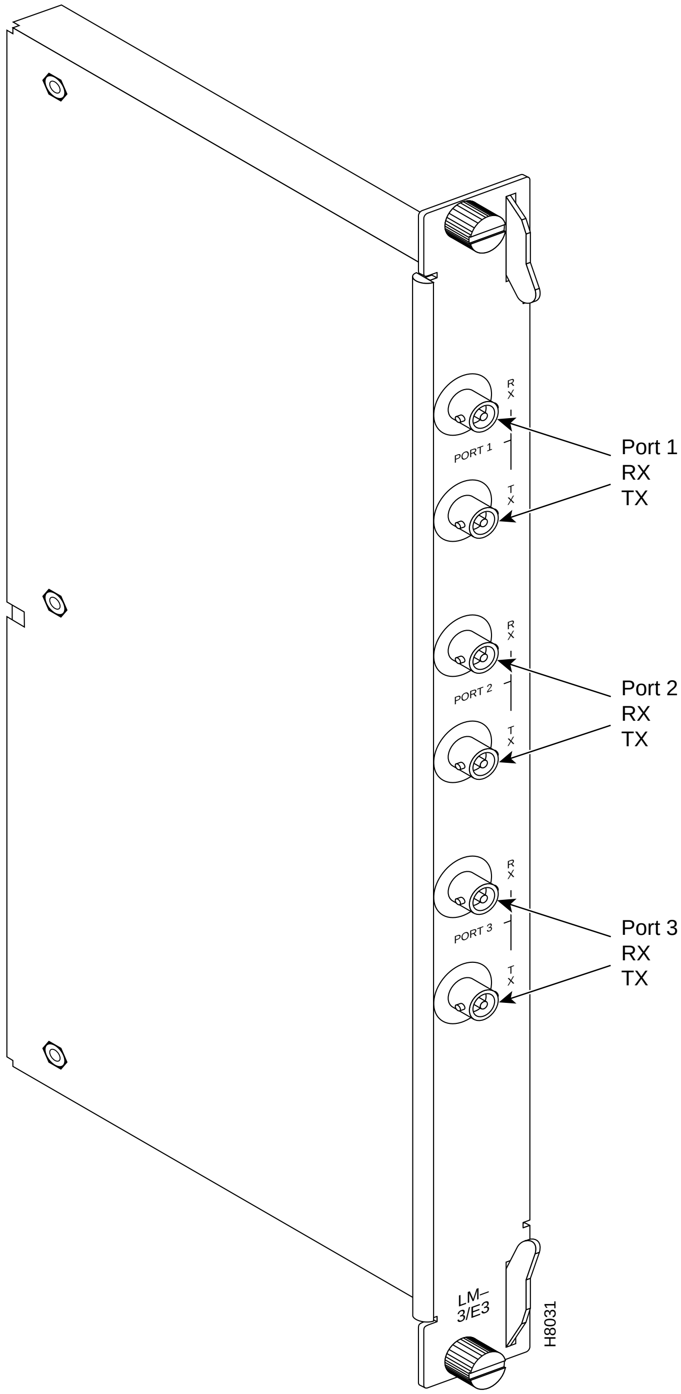


Figure 5-6 Line Module, ASI, LM-3E3 (only two ports used)



ASI-155, ATM Service Interface Card

The ATM Service Interface Card for OC-3/STM-1, the ASI-155, is a BPX switch front card used to interface with an ATM user device e.g., CPE. The ASI provides an industry-standard ATM User-to-Network Interface (UNI) or ATM Network-to-Network Interface (NNI) over OC-3 lines to the BPX switching fabric.

There are three ASI-155 back cards, the LM-2OC-3-SMF for single-mode fiber intermediate range, the LM-2OC-3-SMFLR for single-mode fiber long range, and the LM-2OC-3-MMF for multi-mode fiber. Any of the 12 general purpose slots can be used to hold these cards. These backcards may also be used with the BNI-155

Features

A summary of features for the ASI-155 card include:

- Virtual Path (VP) as well as Virtual Circuit (VC) connections.
- Support for 1000 connections per port for each of the two ports on the ASI-155 card.
- Two port OC-3 SONET/SDH ATM with each port operating at a 155.52 Mbps rate (353,208 cells per second).
- Allows connections between UNI ports on a single node, between nodes, and NNI connections between networks.
- Usage Parameter Control using leaky bucket algorithm to control admission to the network.
- Selective Cell Discard.
- 8 K cell ingress (receive) VBR buffer.
- 32 K cell egress (transmit) buffers.
- 2 connection types: CBR and VBR.
- ATM cell structure and format per ATM Forum UNI v3.1.
- End-to-end OAM flows and end-to-end loopback per ATM Forum UNI v3.1.
- External segment flows consisting of segment loopback cells per ATM Forum UNI v3.1.
- Egress from ASI, twelve fixed queues per line, including CBR and VBR queues.
- Optional 1:1 card redundancy using Y-cable configuration.

Overview

Connections are routed using the VPI and VCI address fields in the UNI header. The allowable range for VPI is from 0 to 255 (UNI) and 0 to 1023 (NNI), while VCI can range from 1 to 65535. A total of 1000 combinations of these can be used per ASI card at any one time. Future releases will support the full ATM address range.

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.

There are 12 egress queues per line (port), two of which are used. These are for CBR and VBR. When a connection is added, the user selects either a constant bit rate (CBR) or variable bit rate (VBR) connection class.

Configuring Connections

Connections are routed between CPE connected to ASI ports. Before adding connections, an ASI 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: slot.port.vpi.vci.

The slot number is the ASI card slot on the BPX switch. The port number is one of two ports on the ASI, 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.

ATM to Frame Relay Network and Service Interworking connections to the ASI are also supported. In the case of Network Interworking, the user CPE must be aware of the interworking function and provide the appropriate protocol mapping.

Refer to the *Cisco WAN Switching Command Reference* for further information.

Functional Description

For ingress traffic, the ATM Layer Interface (ALI) provides traffic management and admission controls (UPC) for the ASI-155 (see Figure 5-7). The ASI-155 supports CBR and VBR connections and employs a single leaky bucket GCRA mechanism for policing cell streams seeking entrance to the network. Each PVC (VPC.VCC) is policed separately, providing firewalling between connections, and assuring that each connection uses only a fair share of network bandwidth. The ALI also performs ingress OAM functions.

The single leaky bucket policing function is implemented using a GCRA (Generic Rate Algorithm) defined by two parameters:

- Rate (where I, expected arrival interval is defined as 1/Rate)
- Deviation (L)

In the ingress direction, the ASI-155 has 2 Cell Input Engines (CIEs) that convert the incoming cell headers to the appropriate connection ID based on input from a Network Address Table.

For egress traffic, the Supervisory Cell Filter (SCF) provides routing and direction of non-data cells, such as test cells and OAM cells.

The Serial Interface Unit (SIU) provides the ASI with an 800 Mbps cell interface to the StrataBus. It provides serial-to-parallel conversion of data, along with loopback and test signal generation capabilities.

The Line Interface Unit (LIU) performs the following ingress functions:

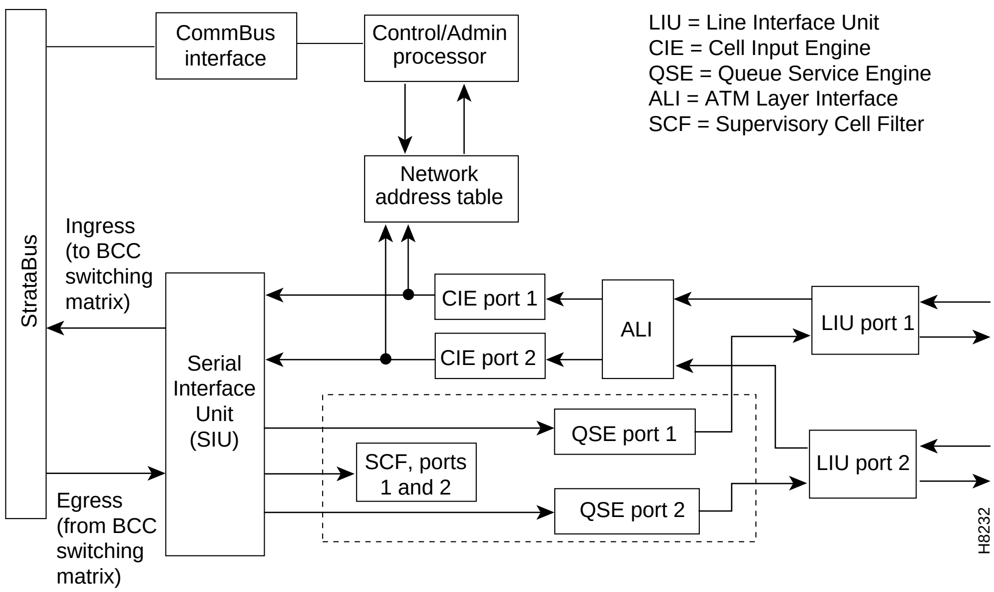
- Provides framing detection and synchronization.
- Provides the ability to extract timing from the incoming signal, and use it as a receive clock for incoming data, while providing transmit clock in the other direction. Alternatively, loop timing can be used to turn the receive clock back around to be used as a transmit clock. The receive clock may also be used to synchronize the node.
- Detects alarms, frame errors, and parity errors.
- Detects far end errors, including framing errors, and yellow alarm indications.

- Provides optional cell descrambling, header error check (HEC), and idle cell filtering.
- Provides a small FIFO buffer for incoming cells.
- Provides optical to electrical conversion.

The Line Interface Unit (LIU) performs the following egress functions:

- Inserts the appropriate framing into the outgoing bit stream.
- Inserts any alarm codes for transmission to the far end.
- Provides optional cell scrambling, HEC generation, and idle cell insertion.
- Provides a small FIFO buffer outing cells.
- Provides electrical to optical conversion.

Figure 5-7 ASI-155 Simplified Block Diagram



Monitoring Statistics

Port, line, and channel statistics are collected by the ASI-155. The StrataView Plus workstation is used to collect and monitor these statistics. For additional information regarding ASI-155 statistics refer to the *Cisco StrataView Plus Operations Guide.*

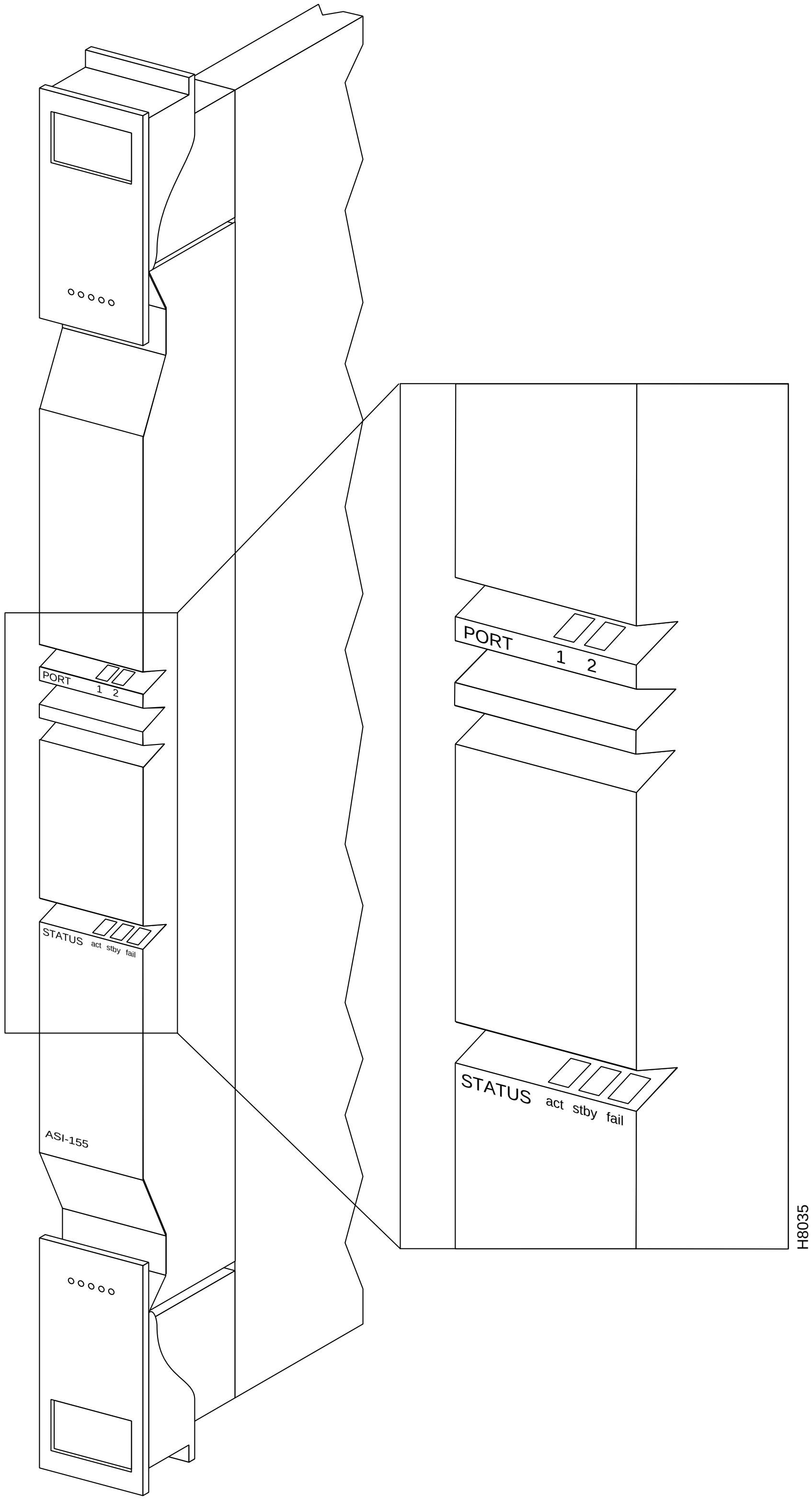
Front Panel Indicators

The ASI-155 front panel (see Figure 5-8) has a three-section, multicolored “card” LED to indicate the card status. The card status LED is color-coded as indicated in Table 5-3. A two-section multicolored “port” LED indicates the status of the two ports on the ASI-155. The port status LED display is color-coded as indicated in Table 5-3.

Table 5-3 ASI-155 Status Indicators

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

Figure 5-8 ASI-155 Front Panel



ASI-155 Line Module, LM-2OC-3-SMF

The LM- 2OC-3 -SMF (Model SMF-2-BC) line module for the ASI-155 Front Card is a backcard that provides a SMF intermediate range service interface. The line module connects to the ASI-155 through the StrataBus midplane. Two adjacent cards of the same type can be made redundant by using a Y-cable at the port connectors. This is the same LM-2OC-3-SMF backcard (Figure 4-8) that is used for the BNI-155.

ASI-155 Line Module, LM-2OC-3-SMFLR

The LM- 2OC-3 -SMFLR (Model SMFLR-2-BC) line module for the ASI-155 Front Card is a backcard that provides a SMF long range service interface. The line module connects to the ASI-155 through the StrataBus midplane. This is the same LM-2OC-3-SMFLR backcard that is used for the BNI-155.

ASI-155 Line Module, LM-2OC-3-MMF

The LM-2OC-3 -MMF (Model MMF-2-BC) line module for the ASI-155 Front Card is a backcard that provides a MMF service interface (Figure 4-9). The line module connects to the ASI-155 through the StrataBus midplane. This is the same LM-2OC-3-SMF backcard that is used for the BNI-155.

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

The LM-OC-3-SMF (Model SMF-2-BC) backcards may be Y-cabled for redundancy using the Y-Cable splitter (Model SMFY) as shown in Figure 4-10. The cards must be configured for Y-Cable redundancy using the **addyred** command

BXM T3/E3, 155, and 622

This chapter describes the BXM card sets which include the BXM T3/E3, BXM-155, and BXM-622. The BXM cards may be configured for either trunk or service (port UNI) mode. In trunk mode they provide BPX network interfaces and in service (port UNI) mode they provide service access to CPE.

The chapter includes the following:

- Label Switching
- Dynamic Resource Partitioning for SPVCs
- BXM Cards
- BXM Capabilities
- Card Operation
- BXM Functional Description
- Fault Management and Statistics
- Technical Specifications
- General SONET Notes
- 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
- Label switching virtual circuits (LVCs) and PVCs.

For information on Label Switching, refer to *Chapter 16, MPLS on BPX Switch*.

Dynamic Resource Partitioning for SPVCs

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

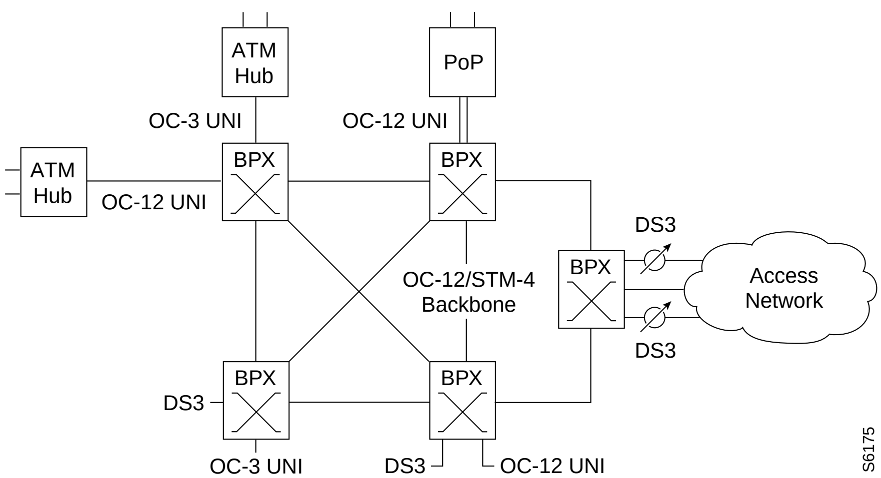
BXM Cards

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 6-1.

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 8, **ATM Connections***.

Figure 6-1 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 no-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 6-1 and Table 6-2 list the available front and back card options for the BXM-T3/E3, BXM-155, and BXM-622.

Table 6-1 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	BPX-T3/E3-BC
BXM-E3-8	8	100k/130k	16k/32k	BPX-T3/E3-BC
BXM-T3-12	12	100k/230k	16k/32k	BPX-T3/E3-BC
BXM-E3-12	12	100k/230k	16k/32k	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	SMF-622 SMFLR-622 SMFXLR-622

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

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

Table 6-2 BXM-T3/E3, BXM-155, and BXM-622 Back Cards

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

BXM Capabilities

The following lists some of the major capabilities of the BXM cards:

Features

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

- ATM cell structure and format per ATM Forum UNI v3.1.
- Loopback support.
- 1:1 card redundancy using Y-cable configuration.
- A BXM card may be configured for either network or port (access) operation.

ATM Layer

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

Service Types

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

CBR Service:

- Usage Parameter Control (UPC) and Admission Control.
- UPC: Ingress rate monitoring and discarding per I.371 for:
    - Peak Cell Rate (PCR).
    - Cell Transfer Delay Variation (CTDV).

VBR Service:

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

ABR Service:

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

      Maximum queue depth.

      Reserved queue depth.

      Congestion threshold.
- ABR congestion control.

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

UBR Service:

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

Virtual Interfaces

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

Card Operation

BXM Front Card Indicators

The BXM front panel has a three-section, multi-colored "card" LED to indicate the card status. A two-port BXM-622, an 8-port BXM-155 front card, and a 12-port BXM-T3/E3 are shown in Figure 6-2, Figure 6-3, and Figure 6-4. The card status LED is color-coded as indicated in Table 6-3. A three-section multi-colored "port" LED indicates the status of the ports. Types of failures are indicated by various combinations of the card status indicators as indicated in Table 6-4.

Table 6-3 BXM Front Panel Status Indicators

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

Table 6-4 BXM Front Panel Card Failure Indicators

act	stby	fail	Failure Description
on	off	on	Non-fatal error detected; card is still active.
off	on	on	Non-fatal error detected; card is in standby mode.
off	blinking	on	Fatal error detected; card is in a reboot mode.

act	stby	fail	Failure Description
on	on	on	Card failed boot load and operation is halted.

Figure 6-2 BXM-622 Front Panel, Two-Port Card Shown

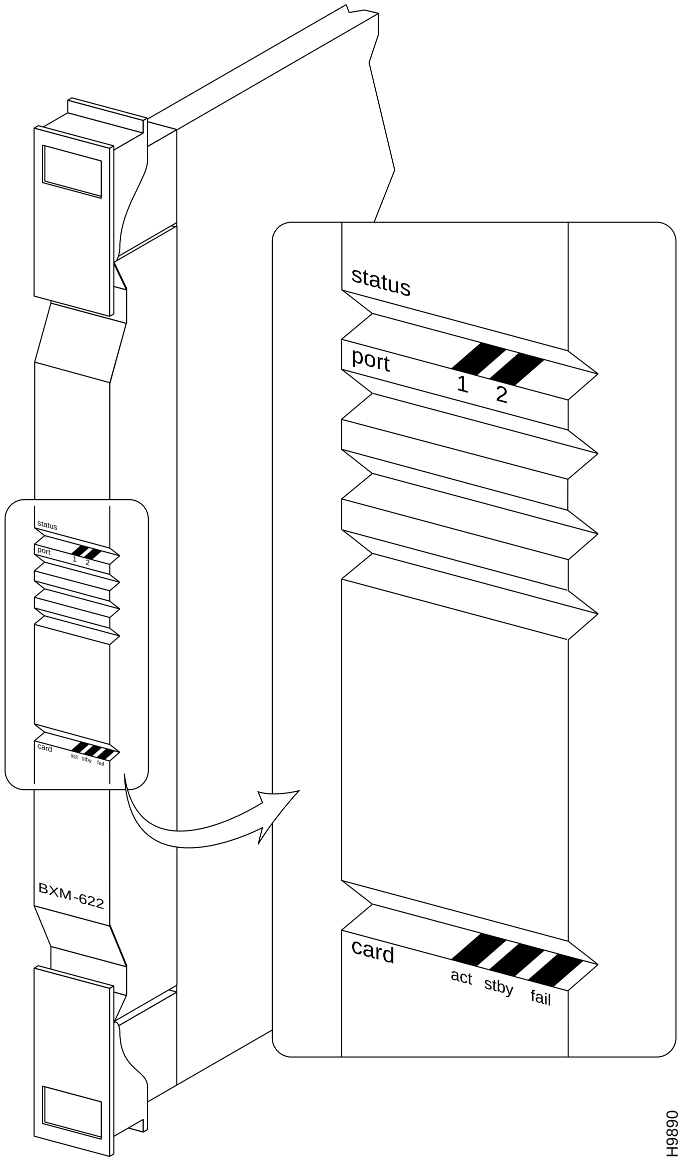


Figure 6-3 BXM-155 Front Panel, Eight-Port Card Shown

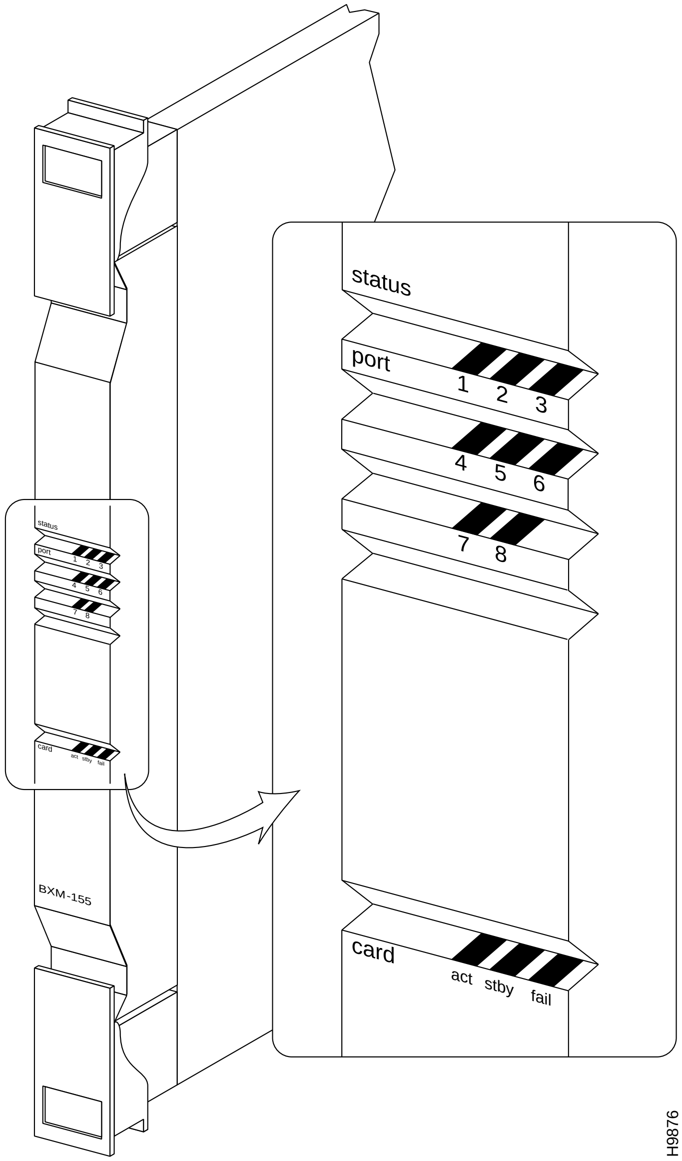
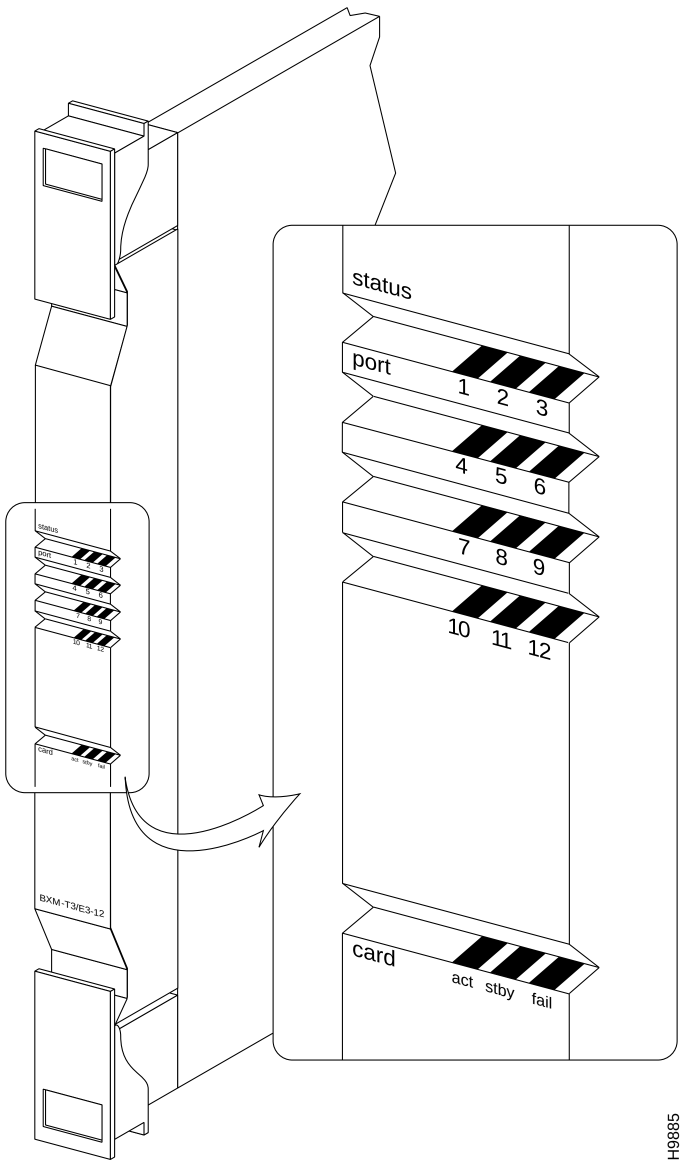


Figure 6-4 BXM-T3/E3 Front Panel, 12-Port Card Shown



BXM, Backcard Connectors

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

The BXM-622 is available in one or two port versions in either a single-mode fiber intermediate range (SMF) or a single-mode fiber long range (SMFLR) backcard. Connector information is listed in Table 6-5 and a 2-port SMF card is shown in Figure 6-5.

Table 6-5 BXM-622 Backcards

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

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

Table 6-6 BXM-155 Backcards

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

The BXM-STM1-4 is available in a four-port version that provides an electrical interface where the longer line lengths provided by the BXM optical backcards are not required. Connector information is listed in Table 6-7 and the backcard is shown in Figure 6-7.

Table 6-7 BXM-STM1-EL4 Backcard

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

The BXM-T3/E3 is available in eight or twelve port versions. Connector information is listed in Table 6-8 and a 12-port T3/E3 card is shown in Figure 6-8.

Table 6-8 BXM-T3/E3 Backcards

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

For SONET APS, card redundancy is provided by the use of two standard BXM front cards and two special backcards. The special backcards are the SMF-155-4R or -8R, SMF LR-4R or -8R, SMF -622 -1R or -2R, or SMFLR-1R or -2R. The two backcards are connected together by a BPX Redundant Backplane which mates with the BPX Midplane. The connectors are the same as for the standard backcards. An APS backcard is shown in (Figure 6-10, and the BPX Redundnant Backplane is shown in (Figure 6-11).

Figure 6-5 SMF-622-2, SMFLR-622-2, and SMFXLR-622-2 Back Card

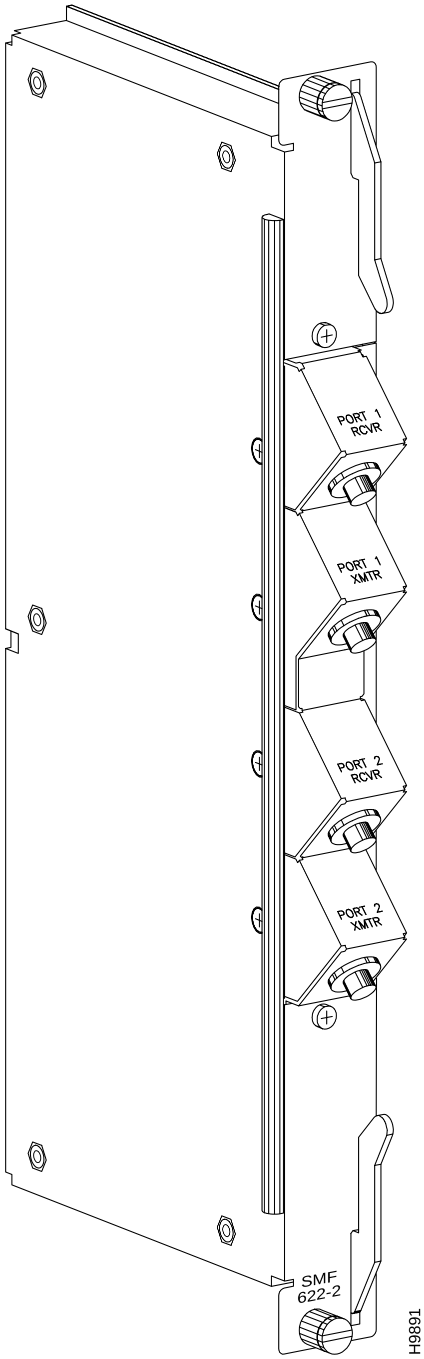


Figure 6-6 BXM-155-8 Port Backcard, MMF, SMF, or SMFLR

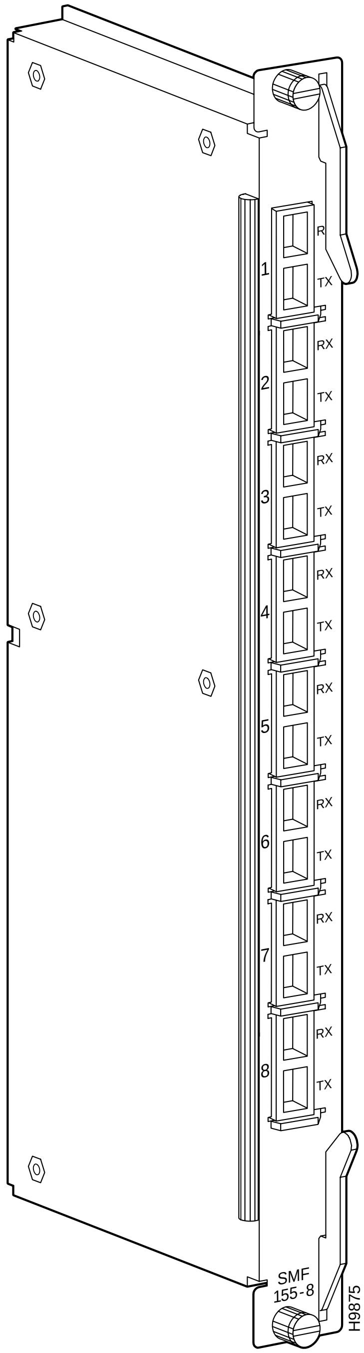


Figure 6-7 BPX-STM1-EL-4 Back Card

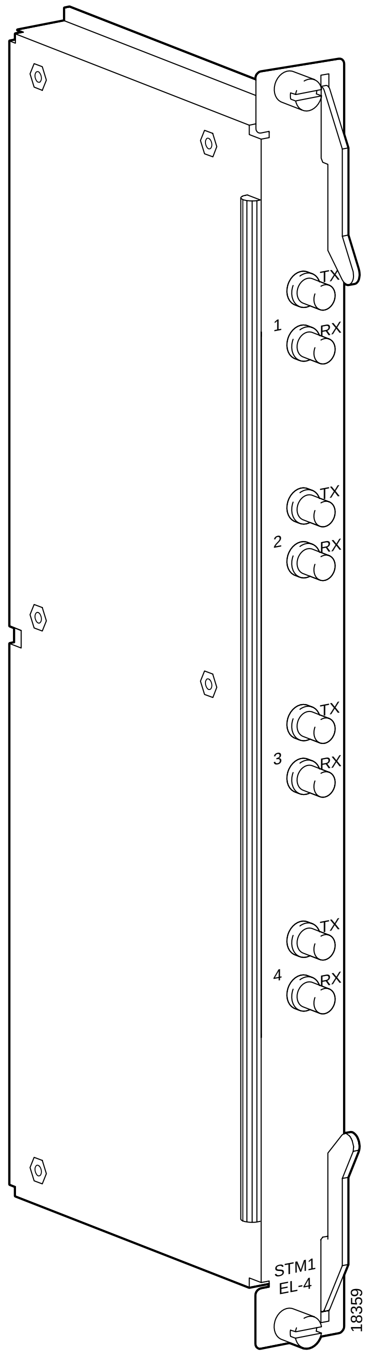
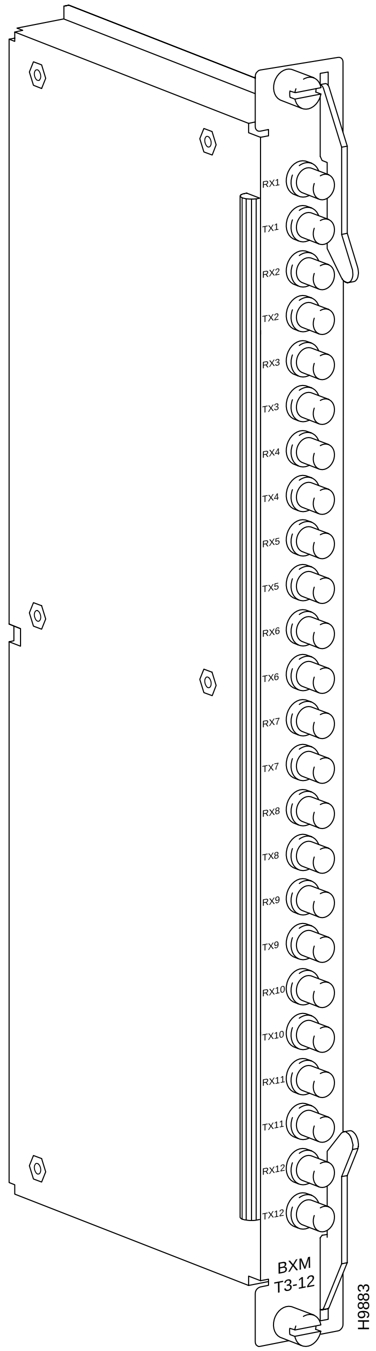


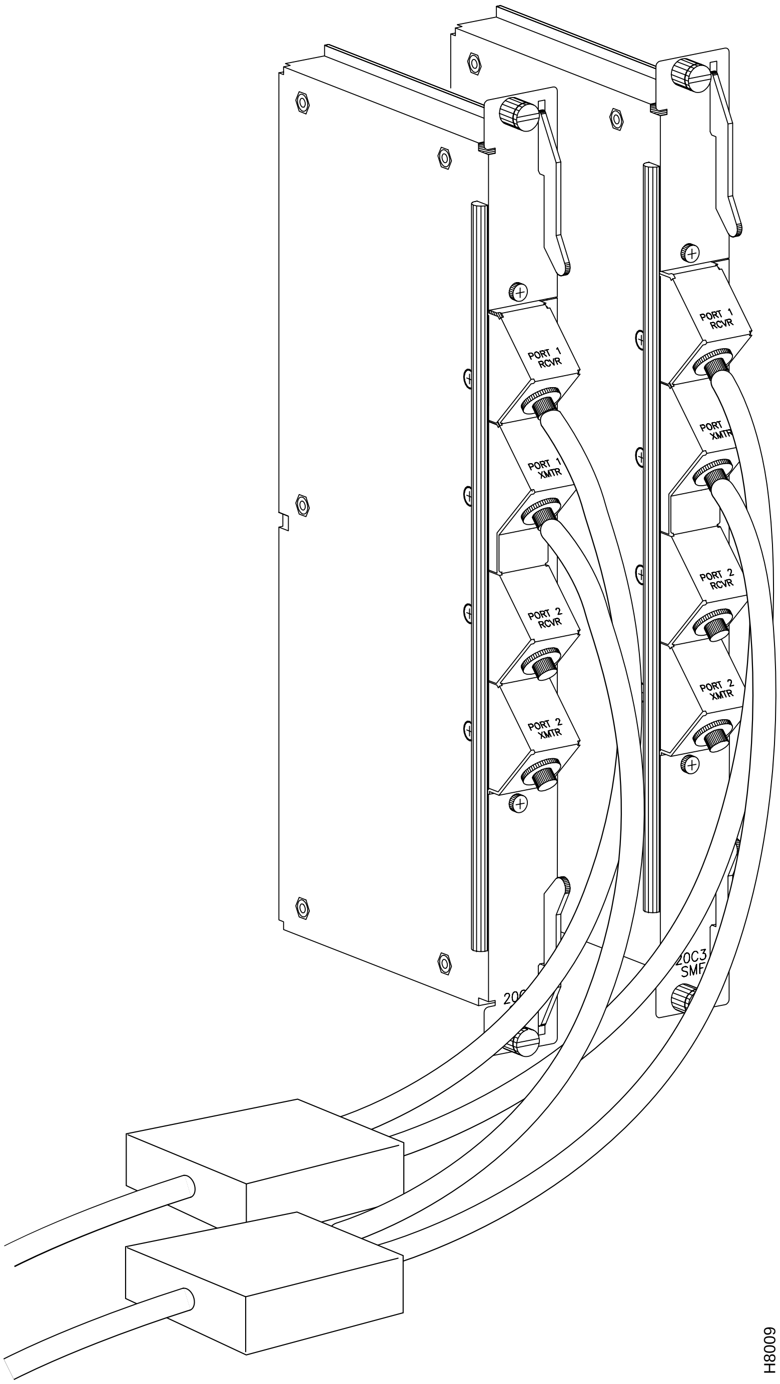
Figure 6-8 BPX-T3/E3 Back Card, 12-Port Option Shown



Y-Cabling of SMF-622 Series Backcards

The SMF-622 series backcards may be Y-cabled for redundancy using the Y-Cable splitter shown in Figure 6-9. The cards must be configured for Y-Cable redundancy using the **addyred** command.

Figure 6-9 Y-Cabling of SMF-622 Series Backcards



APS Redundancy

Automatic Protection Switching (APS) 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 following APS protocols that are supported by the BXM are listed in Table 6-9:

Table 6-9 BXM Sonet APS

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

APS 1:1 Redundancy

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

APS 1+1 Redundancy

APS 1+1 redundancy, which provides both card and line redundancy uses the standard BXM OC-3 and OC-12 front cards, but uses a special APS Redundant Frame Assembly and APS Redundant backcards. A backcard is shown in (Figure 6-10) and the APS Redundant Frame Assembly is shown in (Figure 6-11). Two redundant backcards are connected together by the APS Redundant Frame Assembly. The APS Redundant Frame Assembly with associated APS redundant backcards is inserted as a unit in two appropriate backcard slots.

Refer to Chapter 9, SONET APS, for additional information.

Figure 6-10 BXM SMF-155-8R Backcard

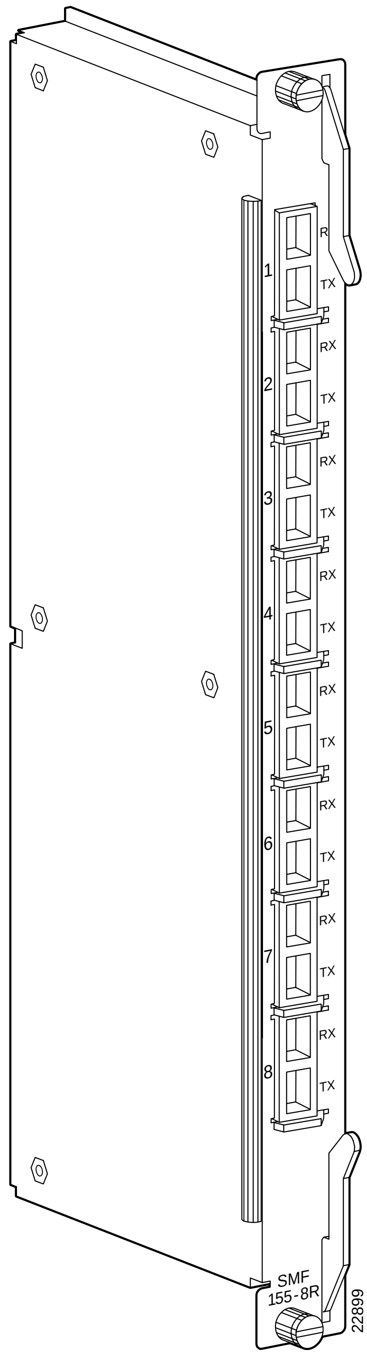
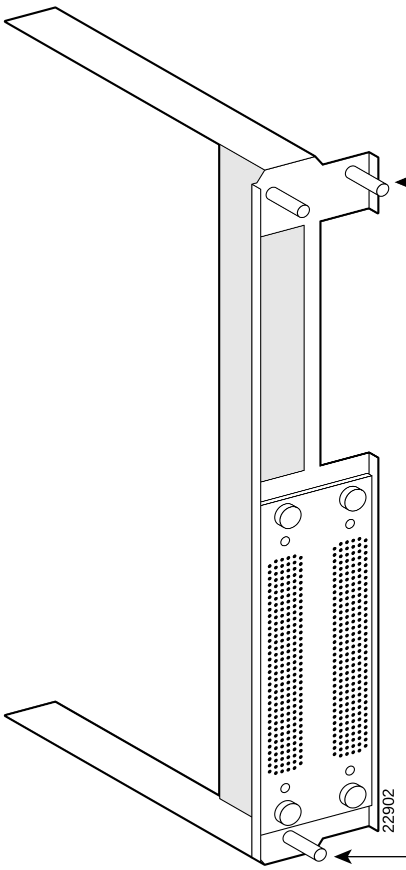


Figure 6-11 BXM APS Redundant Frame Assembly



BXM Functional Description

This functional description provides an overview of BXM operation.

Overview, Port (UNI) Mode

The following provides an overview of the operation of the BXM card when the ports are configured in port (access) mode for connection to customer equipment (CPE).

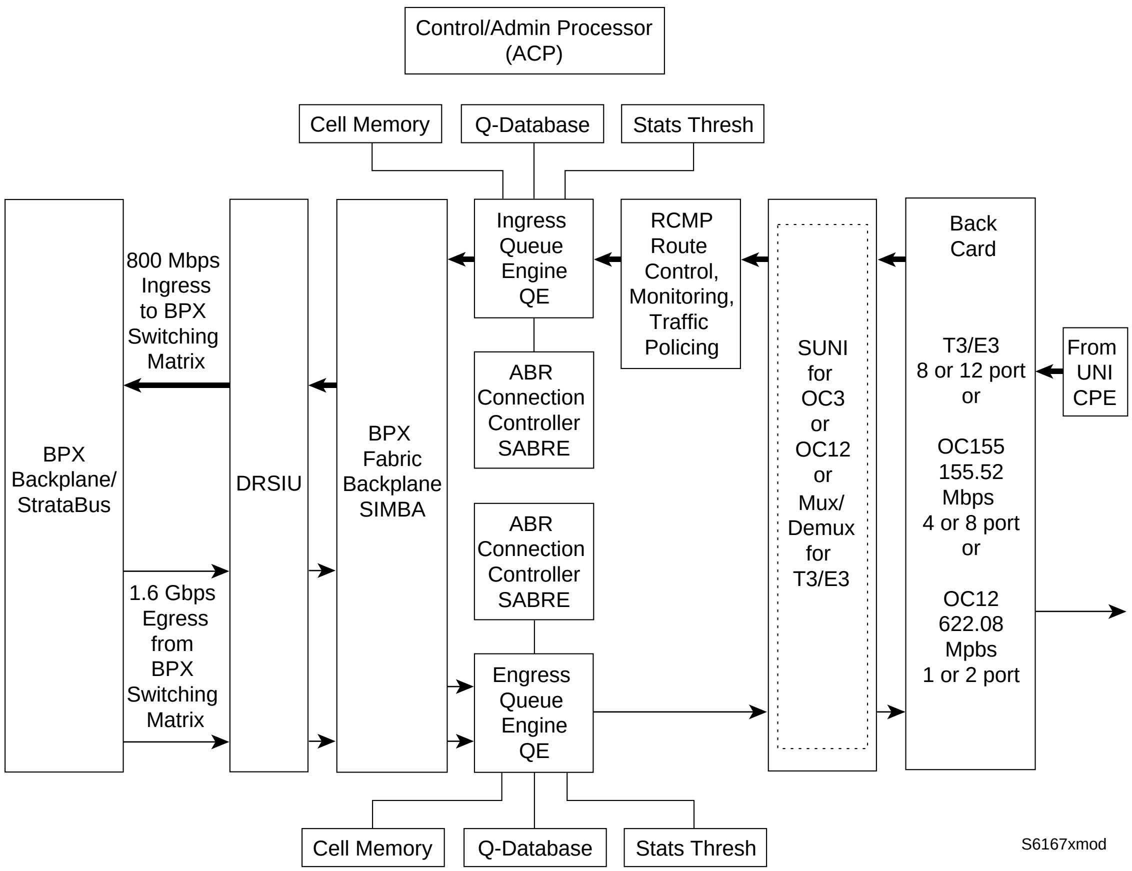
Ingress

The ingress flow of ATM cells from CPE into a BXM port when the card is configured for port (access) operation is shown in Figure 6-12.

ATM cells from the CPE are processed at the physical interface level by the SUNI (OC-3/OC-12) or Mux/Demux (T3/E3), policed per individual VC by the RCMP and routed to applicable ingress queues. In addition, for ABR cells, additional functions are performed by the SABRE ABR connection controller, including: VSVD, Foresight, and virtual connection queueing. The cells are served out via the BPX Backplane to the BPX crosspoint switch in an order of priority based on their connection type.

Figure 6-12 BXM Port (Access UNI) Ingress Operation

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



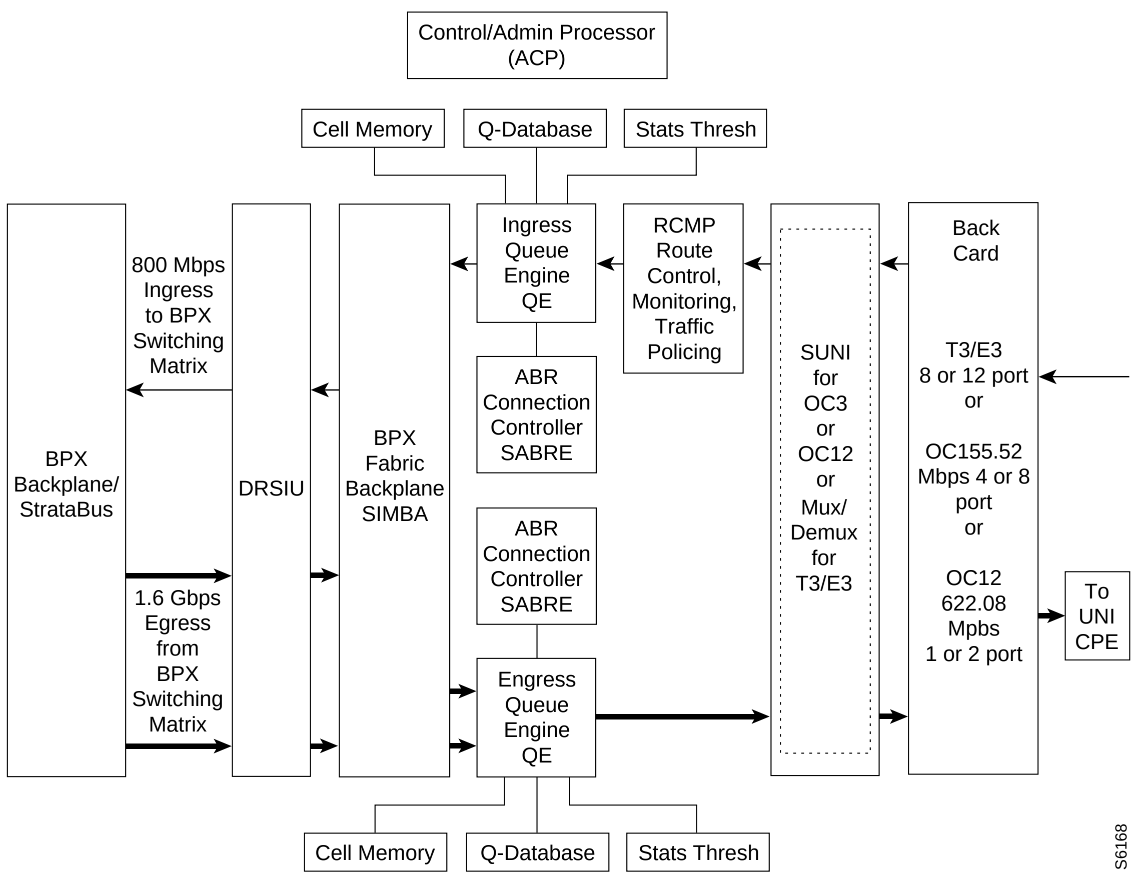
Egress

The egress flow of ATM cells out of the BXM when the card is configured for port (access) operation is shown in Figure 6-13.

ATM cells are routed to the BXM-622 via the BPX Backplane/Stratabus from the BPX crosspoint switch, applied to the DRSIU, then to an egress queue per class of service, and then served out to the SUNI (OC-3/OC-12) or Mux/Demux (T3/E3) which processes the ATM cells into frames, processing the cells from the ATM layer to the physical and on out to the CPE connected to the port(s) on the BXM backcard. For ABR cells, additional functions are performed by the SABRE ABR connection controller, including: VSVD, Foresight, and virtual connection queueing.

Figure 6-13 BXM Port (Access, UNI) Egress Operation

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



Overview, Trunk Mode

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

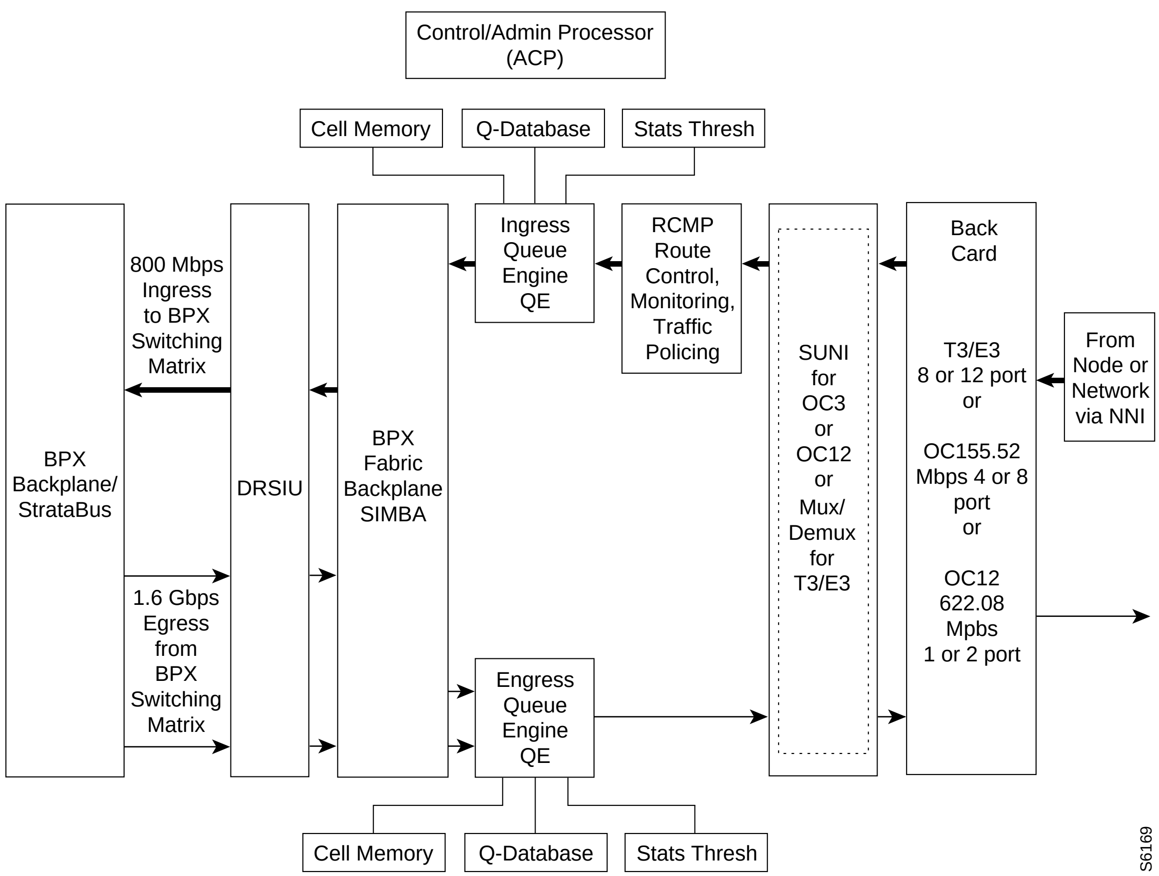
Ingress

The ingress flow of ATM cells into the BXM when the card is configured for trunk operation is shown in Figure 6-14.

ATM cells from a node or network are processed at the physical interface level by the SUNI (OC-3/OC-12) or Demux/Mux (T3/E3), routed to applicable ingress slot queues, and served out to the BPX crosspoint switch via the BPX Backplane.

Figure 6-14 BXM Trunk Ingress Operation

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



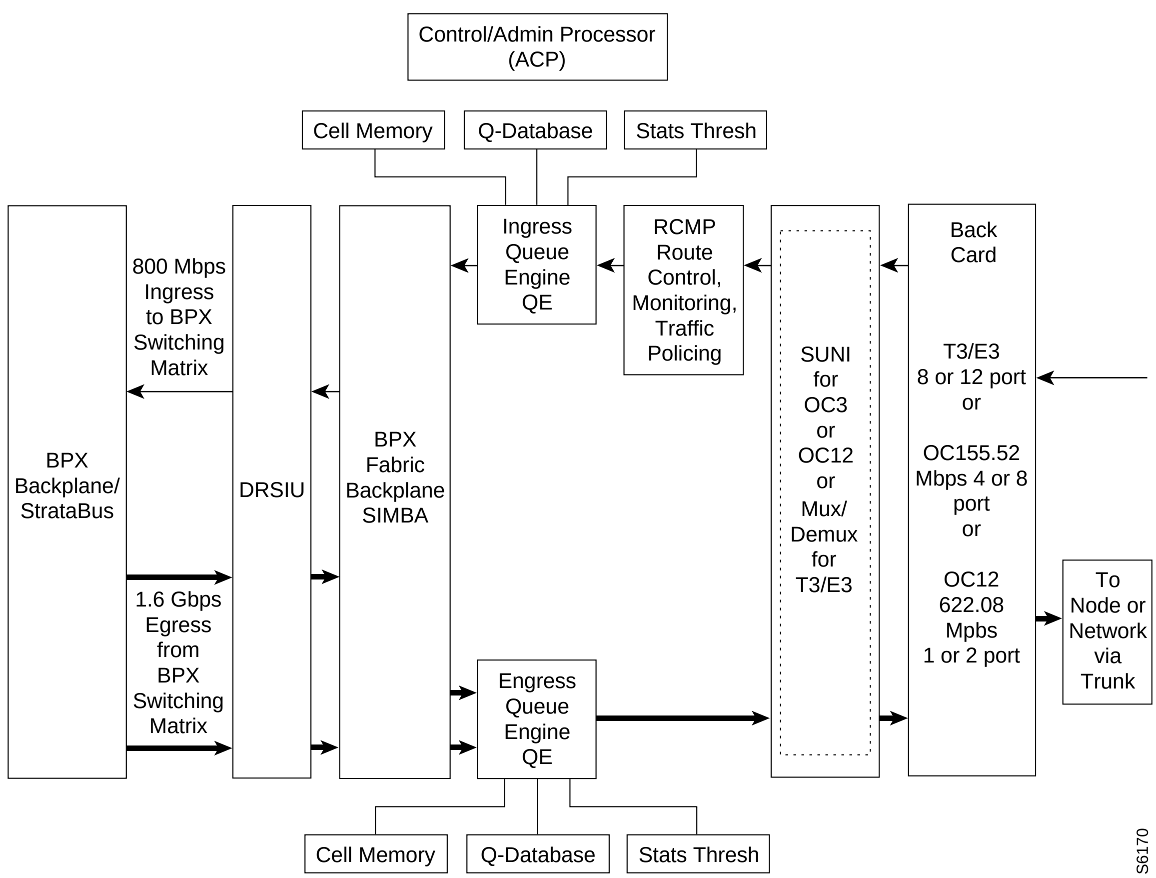
Egress

The egress flow of ATM cells out of the BXM when the card is configured for trunk operation is shown in Figure 6-15.

ATM cells are routed to the BXM from the BPX crosspoint switch, applied to the DRSIU, then to an egress queue per class of service, and then served out to the SUNI (OC-3/OC-12) or Demux/Mux (T3/E3). The SUNI or Demux/Mux, as applicable, processes the ATM cells into frames, processing the cells from the ATM layer to the physical and on out to the backcard trunk interface connecting to another node or network.

Figure 6-15 BXM Trunk Egress Operation

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



Detailed Description, Port (UNI) and Trunk Modes

The following provides a summary of the principal functions performed by the major functional circuits of the BXM.

DRSIU

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

SONET/SDH UNI (SUNI)

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

For ingress traffic, the BXM physical interface receives incoming SONET/SDH frames, extracts ATM cell payloads, and processes section, line, and path overhead. For egress traffic ATM cells are processed into SONET/SDH frames.

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

DeMux/Mux

The Demux/Mux and associated circuits implement the BXM physical layer processing for T3/E3 interfaces, providing header processing, framing, ATM layer mapping, and processing functions for T3 at a 44.736 Mbps rate or E3 at a 34.368 rate.

RCMP

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

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

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

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

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

SABRE

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

- ATM Forum Traffic Management 4.0 compliant ABR Virtual Source/Virtual Destination (VSVD).
- Terminates ABR flows for VSVD and Foresight control loops.
- Performs explicit rate (ER) and EFCI tagging if enabled.
- Supports Foresight congestion control and manages the designated service classes on a per VC basis with OAM processing.
- Supports OAM flows for internal loopback diagnostic self-tests and performance monitoring.
- Provides service queue decisions to the Ingress and Egress Queue Engines for per VC queues for ABR VCs.

Ingress and Egress Queue Engines

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

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

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

SIMBA

This serial interface and multicast buffer ASIC provides the following:

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

ACP Subsystem Processor

The ACP performs the following localized functions:

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

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

Fault Management and Statistics

Note This is a preliminary listing.

Fault Management and Statistics, Port (UNI) Mode

Compliant to Bellcore GR-253-CORE

Alarms:

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

Performance Monitoring:

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

Statistics:

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

    Basic: collection of 4 statistics per VC per direction

    Enhanced: collection of 12 statistics per VC per direction

OAM

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

Fault Management and Statistics, Trunk Mode

Compliant to Bellcore GR-253-CORE

Alarms:

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

Performance Monitoring:

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

Statistics:

Process Monitoring for ATM Header Cell Processing

- Cells discarded due to Header Errors (LCN mismatch)

Miscellaneous ATM Layer Statistics

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

Technical Specifications

Physical Layer

- Trunk or port (access) interface mode.
- Compliant to SONET standards.
  - *Bellcore GR-253-CORE, TR-TSY-000020
  - *ANSI T1.105, T1E1.2/93-020RA
- Compliant to SDH standards.
  - *ITU-T G.707, G.708 and G.709
  - *ITU-T G.957, G.958
- 1:1 BXM redundancy supported using 'Y' redundancy.
- Fiber optic interface characteristics are listed in Table 6-10 and Table 6-11.

Table 6-10 Fiber Optic Characteristics OC-12

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

Table 6-11 Fiber Optic Characteristics OC-3

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

General Information

- Card dimensions: 19"(H) x 1.1"(W) x 27"(D)
- Weight: 6 lb (2.7kg)
- Power -48 V DC at 85 W
- EMI/ESD: FCC Part 15, Bellcore GR1089-CORE

- IEC 801-2, EN55022
- Safety: EN 60950, UL 1950
- Bellcore NEBS:Level 3 compliant
- Optical Safety:
  - — Intermediate Reach IEC 825-1 (Class 1)
  - — Long Reach IEC 825-1 (Class 36)

General SONET Notes

SONET is defined across three elements, section, line, and path as shown in Figure 6-16 and described in Table 6-12. An advantage of this tiered approach is that management control can be exercised at each level, for example at the section level independent of the line or path level.

Figure 6-16 SONET Section, Line, and Path

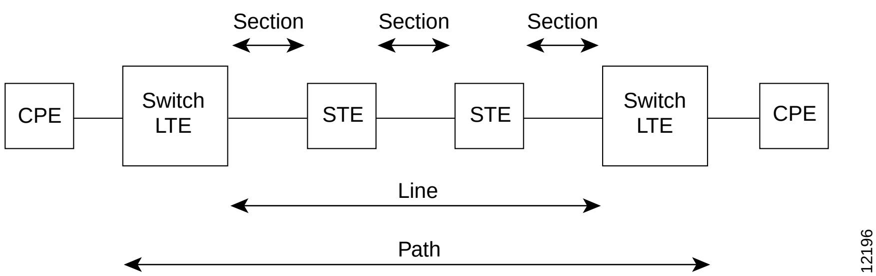


Table 6-12 SONET Section, Line, and Path Descriptions

Unit	Description
Section	A section is the fiber optic cable between two active elements such as simple repeaters. The active element terminating these sections is called Section Terminating Equipment (STE).
Line	A line is a physical element that contains multiple sections and repeaters and is terminated by line terminating equipment (LTE) at each end.
Path	A path includes sections and lines and terminates at the customer premises equipment (CPE).

Table 6-13 provides a cross-reference between OC-n optical carrier levels and the equivalent STS-n and SDH-n levels. It also includes the associated line rates.

Table 6-13 Digital Hierarchies

OC-n Optical Carrier	STS-n Synchronized Transport Signal	Line Rates (Mbps)	SDH-n Synchronized Digital Hierarchy	STM-n Synchronous Transport Module
OC-1	STS-1	51.84		
OC-3	STS-3	155.52	SDH-1	STM-1
OC-12	STS-12	622.08	SDH-4	STM-4
OC-48	STS-48	2488.32	SDH-16	STM-12

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 SuperUser 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 Superuser 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 Switching Command Reference* or the *Cisco WAN Switching Superuser Command Reference*. SuperUser 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

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.

MPLS

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 *Chapter 16, MPLS on BPX Switch*.

Dynamic Resource Partitioning for SPVCs

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 Switching 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 Switching 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.

PART 4

Functional Descriptions, General

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 9.2 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 7-1. 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 7-1).

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.

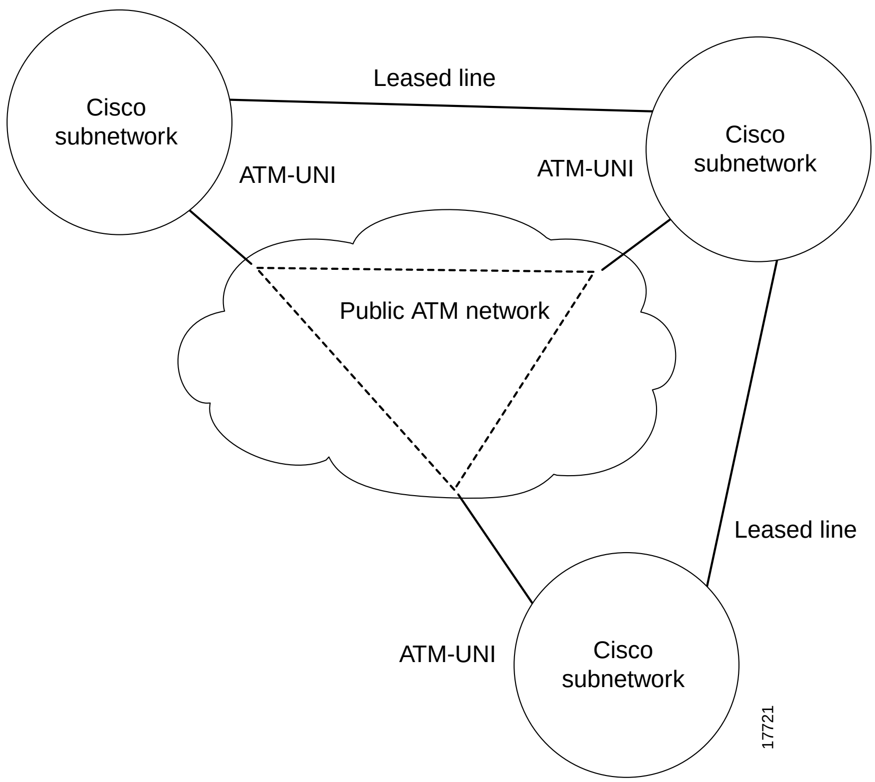
Typical ATM Hybrid Network with Virtual Trunks

Figure 7-1 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 7-1 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 7-1, depending on the specific BXM card.

Table 7-1 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.)

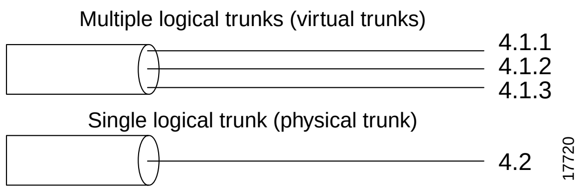
port = port number (1-16)

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 7-2, 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 7-2 Virtual and Physical Trunks on a BXM



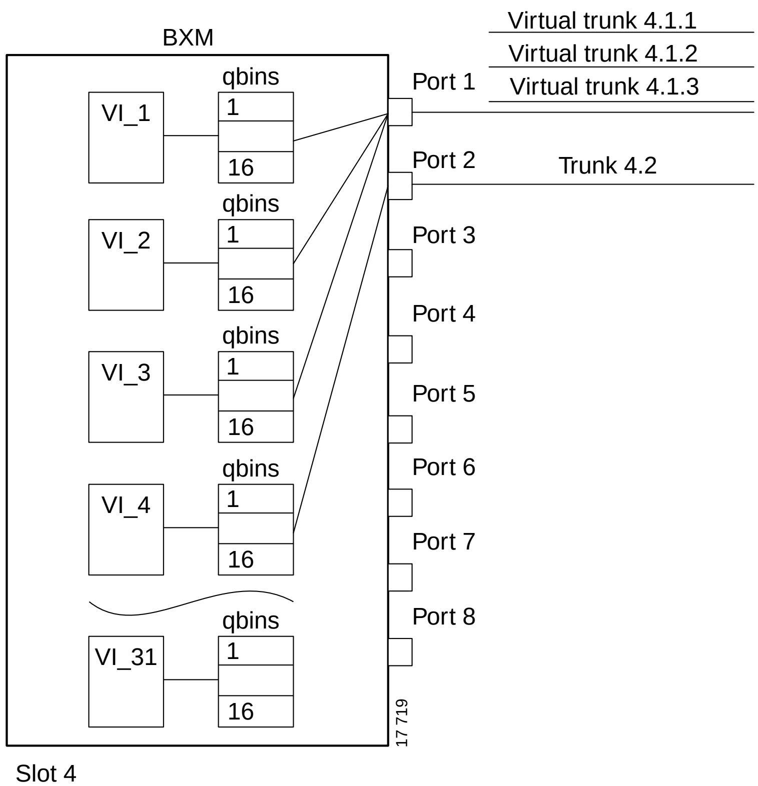
Virtual Interfaces

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 7-3, 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) that support master controllers use qbins 10-15, as applicable. MPLS and AutoRoute, or PNNI and AutoRoute can be supported simultaneously, and in this release, MPLS and PNNI at the same time on a given VSI.

Figure 7-3 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

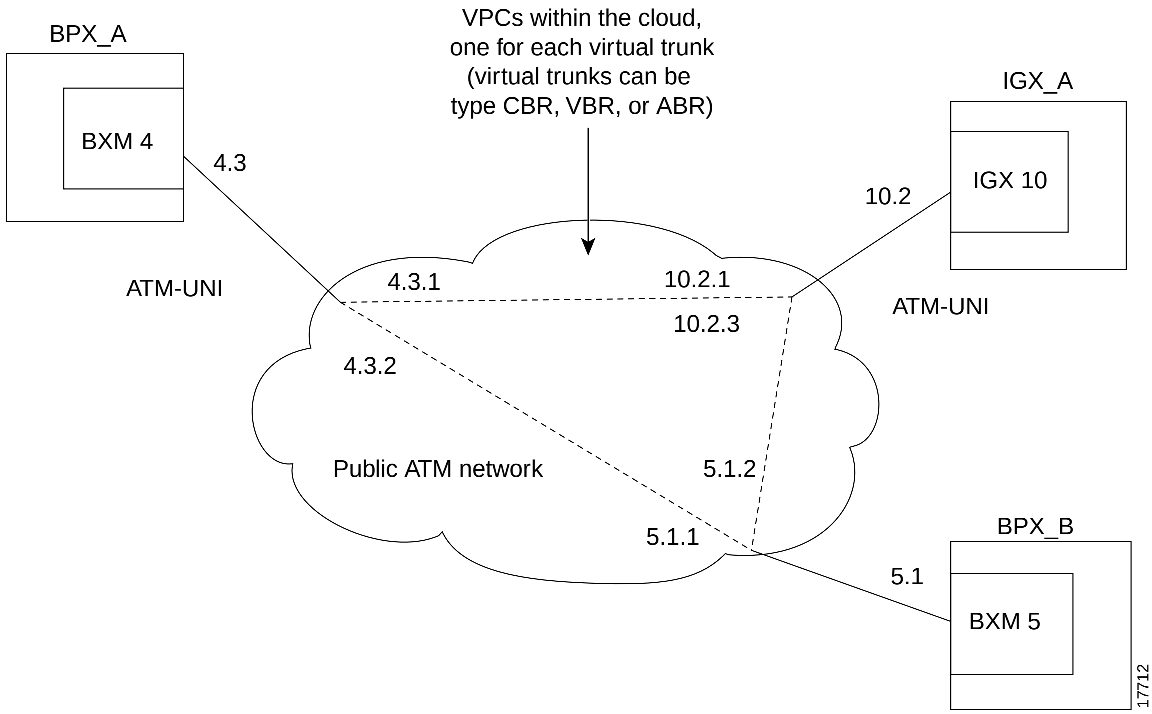
An example of a number of virtual trunks configured across a Public ATM Network is shown in Figure 7-4. There are three virtual trunks shown across the network, each with its own unique VPC.

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 7-2.

Figure 7-4 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 7-2 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 11, 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.

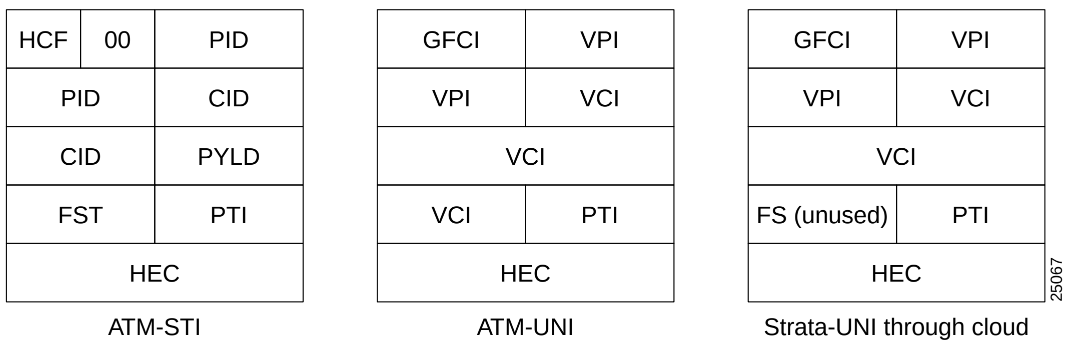
The VPI value across the virtual trunk is identical for all cells on a single virtual trunk. The VCI value in these cells determines the final destinations of the cells.On BNI cards, for virtual trunking a modified ATM UNI cell format (Strata-UNI) stores the ForeSight information, as applicable, in the 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 7-5 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 7-5 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 7-3. 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 7-3.

Table 7-3 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 7-4

Table 7-4 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 7-5 lists the number of connection ids for virtual trunks on various cards.

Table 7-5 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, and so on
- VBR Trunk: ATM VBR traffic, frame relay traffic, and so on
- ABR Trunk: ATM ABR traffic, ForeSight traffic, and so on

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

A VBR configured trunk is best suited to carrying frame relay and VBR traffic, and so on

An ABR configured trunk is best suited to carrying ForeSight and ABR traffic, and so on

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

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 7-6).

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, and so on
Step 5	At BPX_A	cnfrsrc 4.3.1 ... cnfrsrc 4.3.2 ...	Configure the number of conids, bandwidth, and so on, available for the virtual trunks.
Step 6	At BPX_B	uptrk 5.1.1 uptrk 5.1.2	Up virtual trunks 5.1.1 and 5.1.2 on BXM port 5.1.
Step 7	At BPX_B	cnftrk 5.1.1 ... cnftrk 5.1.2 ...	Configure the virtual trunks to match the cloud’s VPC configuration, including: VPI, header type (UNI or NNI), traffic classes, and VPC type, and so on
Step 8	At BPX_B	cnfrsrc 5.1.1 ... cnfrsrc 5.1.2 ...	Configure the number of conids, bandwidth, and so on, available for the virtual trunks.
Step 9	At IGX_A	uptrk 10.2.1 uptrk 10.2.3	Up virtual trunks 10.2.1 and 10.2.3 on IGX trunk port 10.2.

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

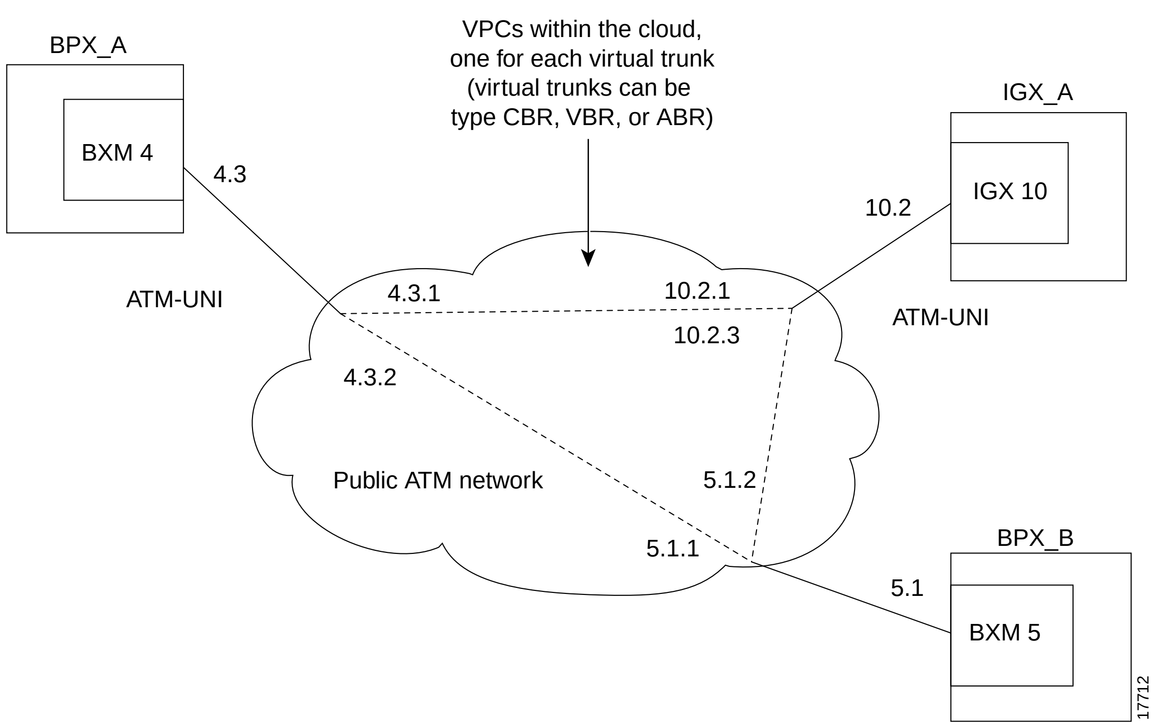
The VPI values chosen using **cnftrk** must match those used by the cloud VPC. In addition, both ends of the virtual trunk must match with respect to: Transmit Rate, VPC type, traffic classes supported, and the number of connection channels supported. The **addtrk** command checks for matching values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

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

BPX_A 4.3.1-10.2.1/IGX_A

BPX_A 4.3.2-5.1.1/BPX_B

Figure 7-6 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

In this release, 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 9, “SONET APS.”

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 7-6.

Table 7-6 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 7-6 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 7-7.

Table 7-7 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 7-7 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 7-8 and Table 7-8 and Table 7-9 show the log messaging for activating and adding a virtual trunk 1.2.1.

I

Table 7-8 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 7-9 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 7-10

Table 7-10 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 *Cisco WAN Switching Command Reference* and *Cisco WAN Switching 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 7-11 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 7-11 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 7-11 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 7-12 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 7-12 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 7-13 are BPX specific.

Table 7-13 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

Parameter-cnftrk	BXM		UXM	
	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

Descriptions	BXM Physical	BXM Virtual	UXM Physical	UXM 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
```

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:

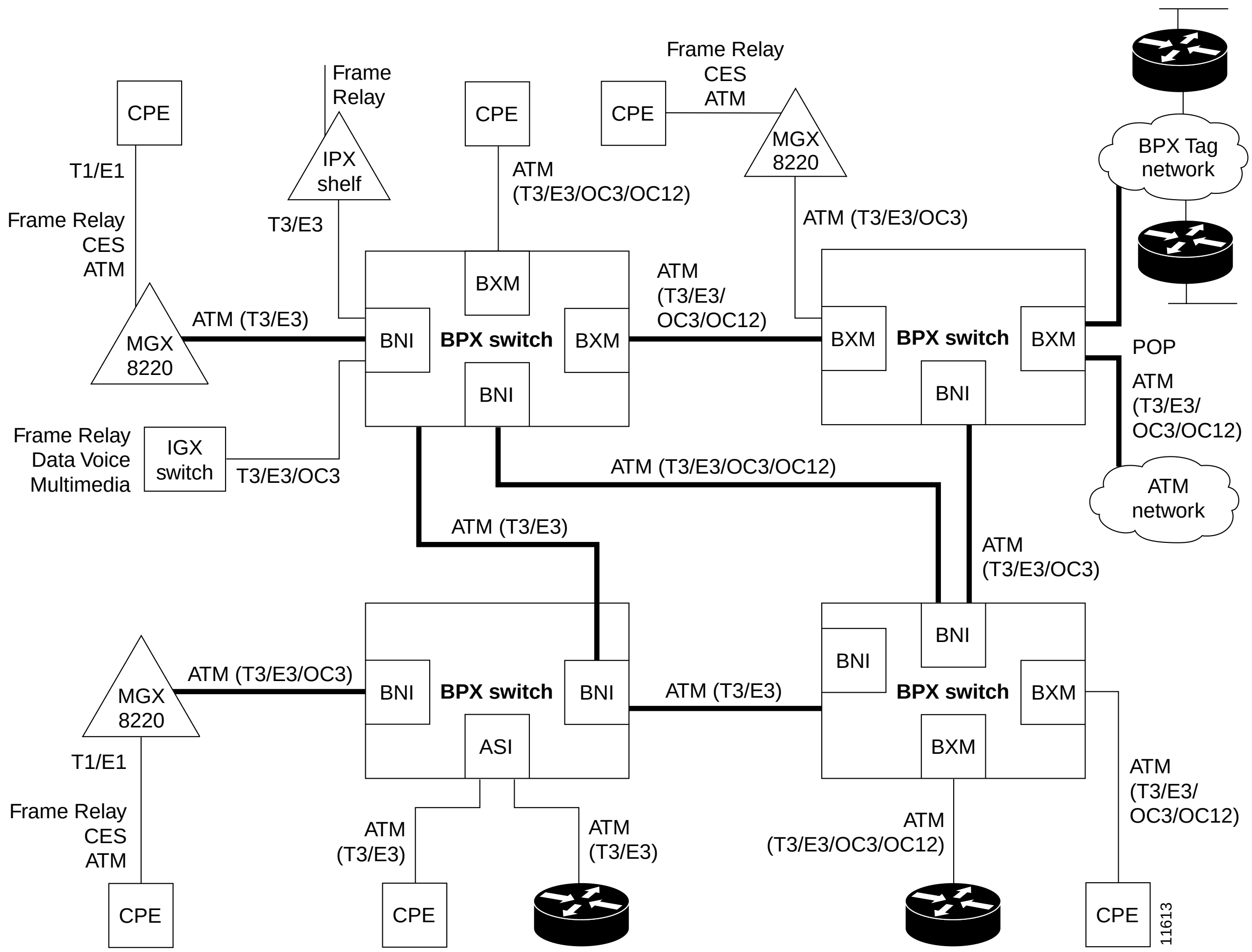
- ATM Connection Services
- SVCs
- Traffic Management Overview
- ATM Connection Requirements
- ATM Connection Flow
- rt-VBR and nrt-VBR Connections
- ATM Connection Configuration
- Traffic Policing Examples
- Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR
- LMI and ILMI Parameters

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 8-1 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 8-1 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 8-1 summarizes the major attributes of each of the traffic management classes:

Table 8-1 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 8-2 shows the data cell flow in the forward direction from a source to its destination along with its associated control loop. The control loop consists of two RM cell flows, one in the forward direction (from source to destination) and the other in the backward direction (from destination to source).

The data cell flow in the backward direction from destination to source is not shown, nor are the associated RM cell flows. However, these flows are just the opposite of that shown in the diagram for forward data cell flows.

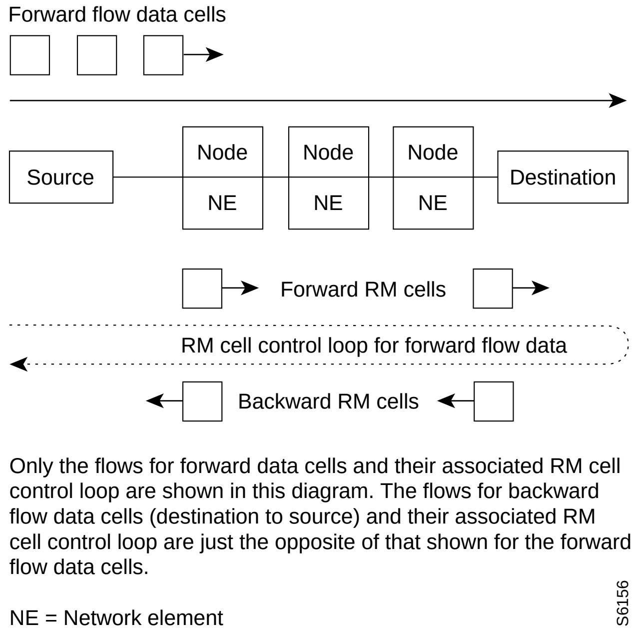
A source generates forward RM cells which are turned around by the destination and returned to the source as backward RM-cells. These backward RM-cells may carry feedback information from the network elements and/or the destination back to the source.

The parameter Nrm is defined as the maximum number of cells a source may send for each forward RM cell, that is, one RM cell must be sent for every Nrm-1 data cells. Also, in the absence of Nrm-1 data cells, as an upper bound on the time between forward RM cells for an active source, an RM cell must be sent at least once every Trm msecs.

BXM Connections

The BXM-T3/E3, BXM-155, and BXM-622 cards support ATM Traffic Management 4.0. The BXM cards are designed to support all the following service classes: Constant Bit Rate (CBR), real time Variable Bit Rate (rt-VBR), non-real time Variable Bit Rate (nrt-VBR), Available Bit Rate (ABR with VSVD, ABR without VSVD, and ABR using ForeSight), and Unspecified Bit Rate (UBR). ABR with VSVD supports explicit rate marking and Congestion Indication (CI) control.

Figure 8-2 ABR VSVD Flow Control Diagram



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 8-2 when prompted:

Table 8-2 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 8-3 when prompted:

Table 8-3 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 8-3 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 8-3, 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.

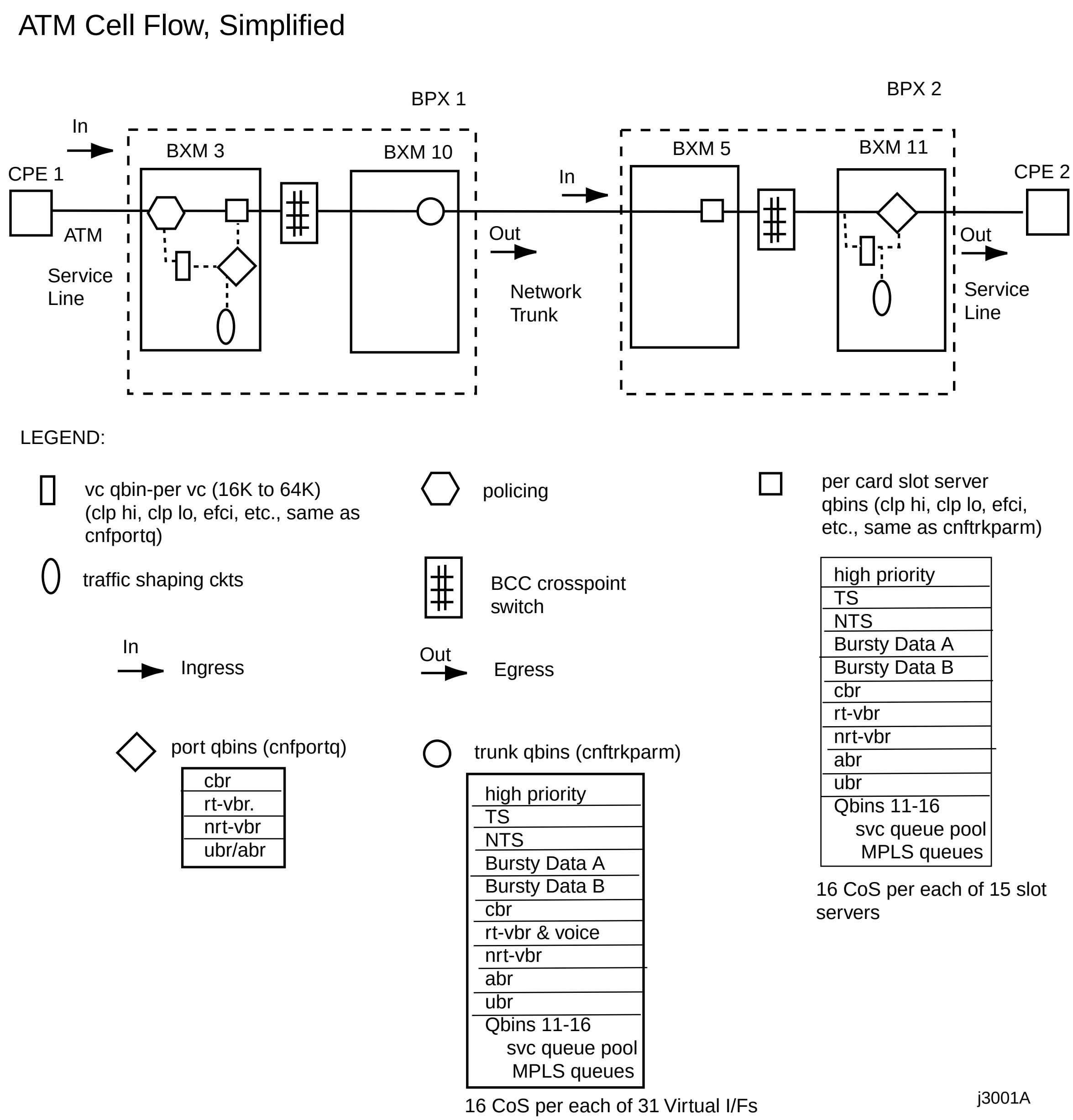
Cells are served out from the slot servers via the BPX backplane to the BCC crosspoint switch. The cells are served out on a fair basis with priority based on class of service, time in queue, bandwidth requirements, etc.

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 8-3 ATM Connection Flow via BPX Switches



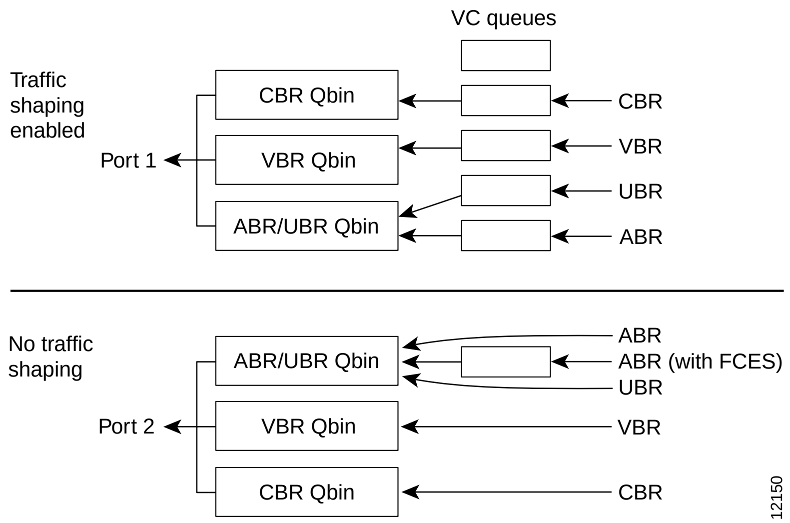
Traffic Shaping for CBR, rt-VBR, nrt-VBR, and UBR

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 8-4 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 8-4 Traffic Shaping Example



Traffic Shaping Rates

Traffic shaping rates are listed in Table 8-4.

Table 8-4 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    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

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    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 ]:
```

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 8-5, 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 8-6, 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 8-5 through Figure 8-10.
- Table 8-7, Connection Parameter Descriptions
  - This table defines the connection parameters listed in Table 8-6.

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

- Figure 8-5, CBR Connection Prompt Sequence
- Figure 8-6, rt-VBR and nrt-VBR Connection Prompt Sequence
- Figure 8-7, 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 8-8 is not available for ABR with ForeSight.

- Figure 8-8, 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 8-9, ABR ForeSight Connection Prompt Sequence
- Figure 8-10, UBR Connection Prompt Sequence
- Figure 8-13, ATFR Connection Prompt Sequence
- Figure 8-14, ATFST Connection Prompt Sequence
- Figure 8-15, ATFT Connection Prompt Sequence
- Figure 8-16, ATFTFST Connection Prompt Sequence
- Figure 8-17, ATFX Connection Prompt Sequence
- Figure 8-18, ATFXFST Connection Prompt Sequence

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

Table 8-5 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 8-6 Connection Parameters with Default Settings and Ranges

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC-3 & OC-12 RANGE	ASI T3/E3 RANGE	ASI-155 RANGE
PCR(0+1)[50/50]	50- T3/E3 cells/sec 50 - OC-3 50 - OC-12	T3: MCR – 96000 E3: MCR – 80000 Limited to MCR – 5333 cells/sec for ATFR connections.	OC-3 (STM1): 0 – 353200

Table 8-6 Connection Parameters with Default Settings and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC-3 & OC-12 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/E3OC-3/0C12	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.	OC-3/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/E3OC-3/OC-12	T3: MCR – 96000:T3 E3: MCR – 80000: E3 Limited to MCR – 5333 cells/sec for ATFR connections.	OC-3/STM1: 0 – 353200
MBS [1000/1000]	1 - 5,000,000cells	T3/E3: 10 – 24000 cells	OC-3 (STM1): 10 – 1000 cells
Policing[3] For CBR: [4]	1 - VBR.1 2 - VBR.2 3 - VBR.3 4 - PCR policing only 5 - off	1 - VBR.1 2 - VBR.2 3 - VBR.3 4 - PCR policing only 5 - off	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 8-6 Connection Parameters with Default Settings and Ranges (Continued)

PARAMETER WITH [DEFAULT SETTING]	BXM T3/E3, OC-3 & OC-12 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: For ForeSight: max[PCR/128, 10] For ABR STD[128]	If ForeSight, then in absolute (0 - PCR) If ABR then 2^n (1 - 32768)	If ForeSight, then in absolute (0 – PCR) If ABR, then 2^n (1 – 32768)	N/A
RDF: For ForeSight [93] For ABR STD [16]	If ForeSight, then % (0% - 100%) If ABR then 2^n (1 - 32768)	If ForeSight, then % (0% – 100%) If ABR, then 2^n (1 – 32768)	N/A
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 8-7 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 8-7 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 8-8)
FCES (Flow Control External Segments)	(see Meaning of VSVD and Flow Control External Segments, Figure 8-8)
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 8-5)
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

Table 8-7 Connection Parameter Descriptions (Continued)

Parameter	Description
FRTT (ATM Forum TM 4.0 term), BXM only.	Fixed Round Trip Time: the sum of the fixed and propagation delays from the source to a destination and back
TBE (ATM Forum TM 4.0 term), BXM only.	Transient Buffer Exposure: The negotiated number of cells that the network would like to limit the source to sending during start-up periods, before the first RM-cell returns.
IBS	Initial Burst Size
Trunk cell routing restriction (Y/N) [Y]	The default (Y) restricts ATM connection routes to include only ATM trunks. Selecting (N) allows the network to route these connections over non-ATM trunks (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 8-5 in the sequence in which they occur during the execution of the **addcon** command. The CBR policing definitions are summarized in Table 8-8.

Figure 8-5 CBR Connection Prompt Sequence

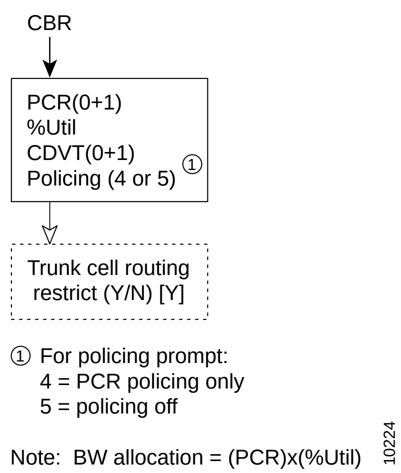


Table 8-8 CBR Policing Definitions

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 8-6 in the sequence in which they occur during the execution of the **addcon** command. The VBR policing definitions are summarized in Table 8-9.

Figure 8-6 rt-VBR and nrt-VBR Connection Prompt Sequence

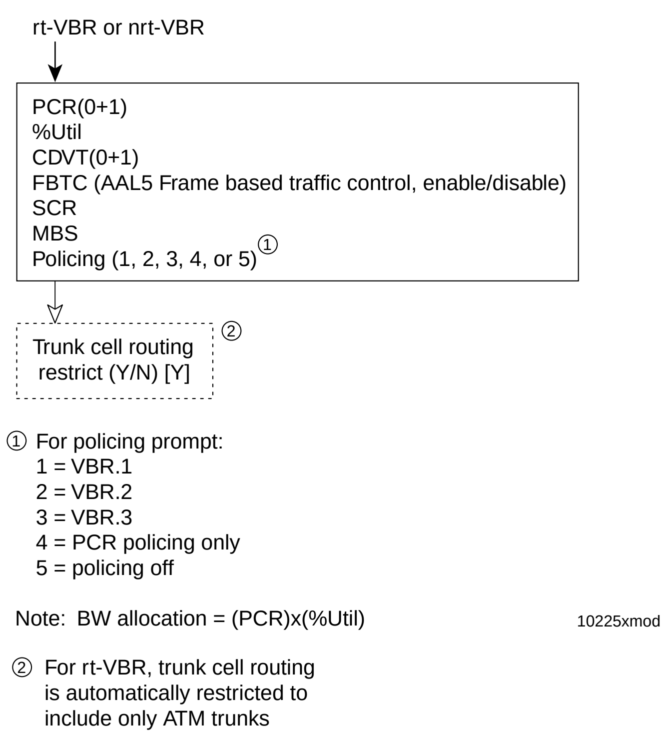


Table 8-9 VBR Policing Definitions

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 OC-3 cards.
- ABR standard with VSVD. (This is ABR standard with congestion flow control as specified by the ATM Traffic Management, Version 4.0)
  - Also, referred to as ABR.1.
  - Supported only by BXM cards.
  - Feature must be ordered.
- ABR with ForeSight congestion control
  - Also, referred to as ABR.FST.
  - Supported by BXM and ASI-T3 (& ASI-E3) cards.
  - Feature must be ordered.

ABR Connections

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

Policing for ABR connections is the same as for VBR connections which are summarized in Table 8-9.

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 8-7 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 8-8.

ABRSTD Connections

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

The parameters for an ABRSTD connection are shown in Figure 8-9 in the sequence in which they occur during the execution of the **addcon** command

Figure 8-7 ABR Standard Connection Prompt Sequence

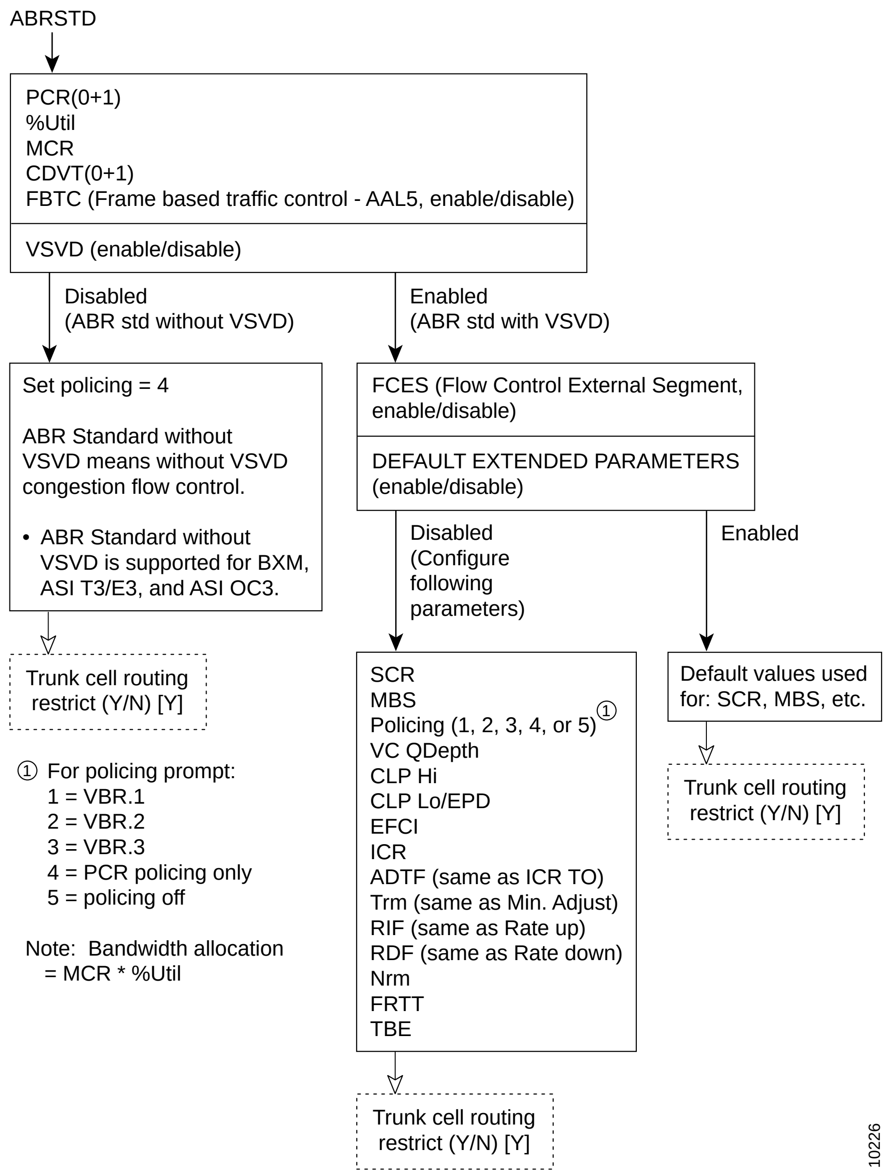
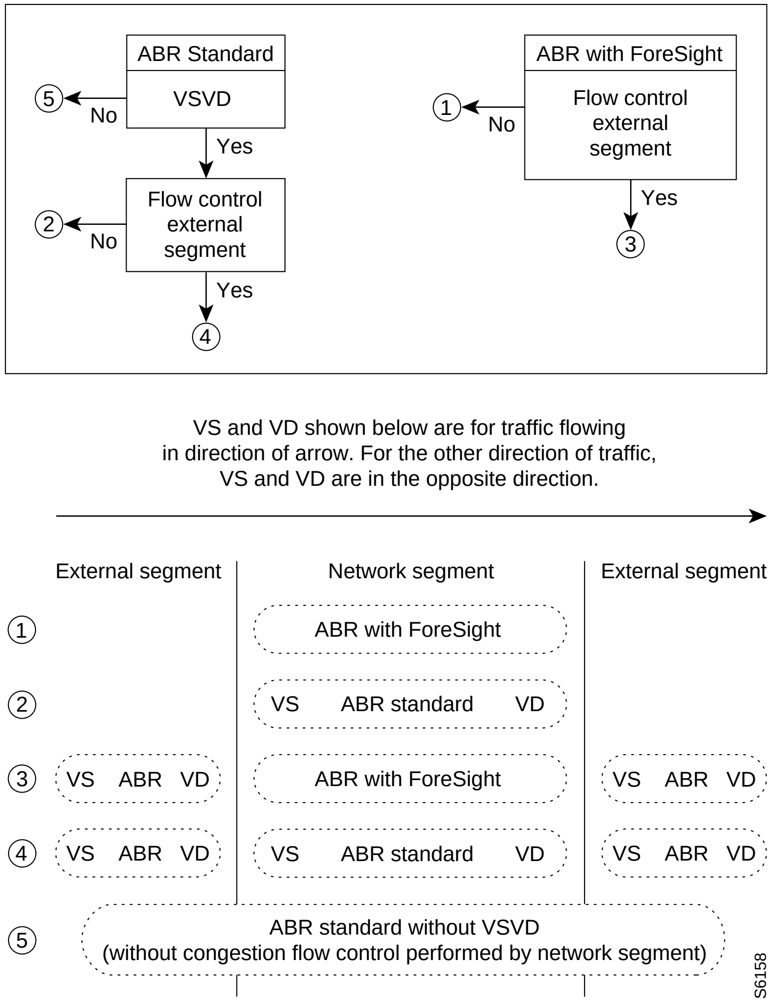


Figure 8-8 Meaning of VSVD and Flow Control External Segments

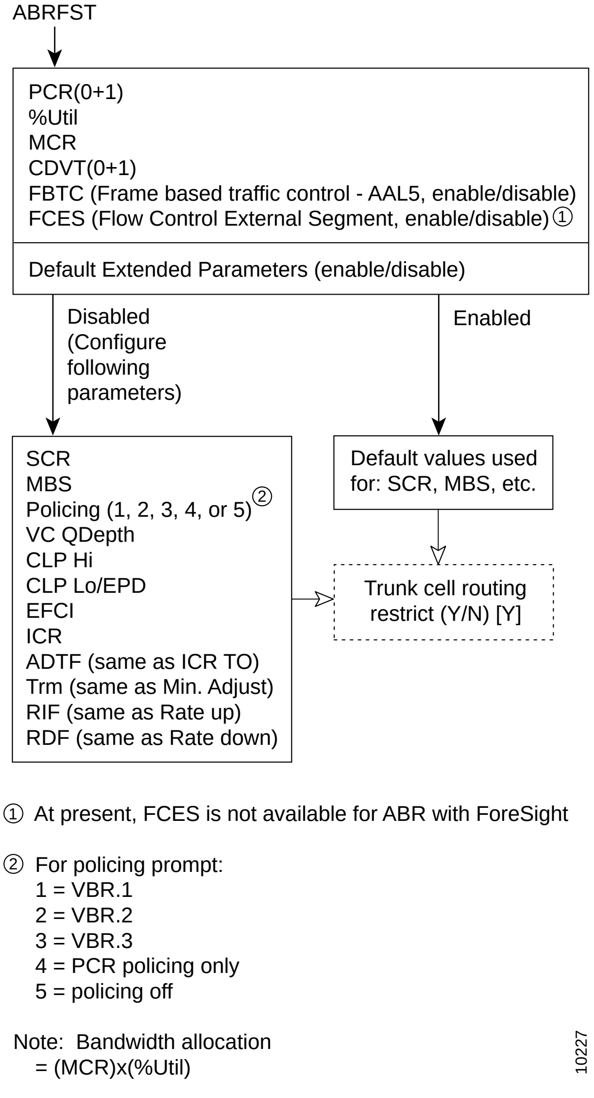


ABRFST Connections

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 8-9 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-9 ABR ForeSight Connection Prompt Sequence



UBR Connections

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

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

The parameters for a UBR connection are shown in Figure 8-10 in the sequence in which they occur during the execution of the **addcon** command.

The UBR policing definitions are summarized in Table 8-10.

Figure 8-10 UBR Connection Prompt Sequence

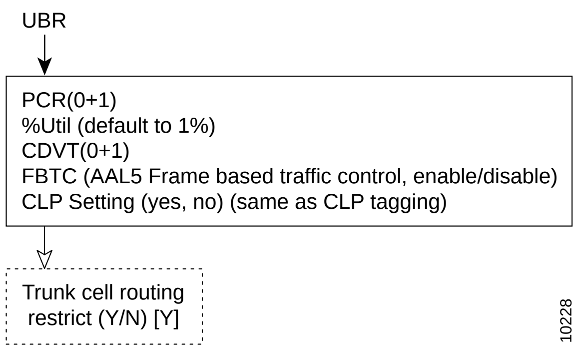


Table 8-10 UBR Policing Definitions

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**

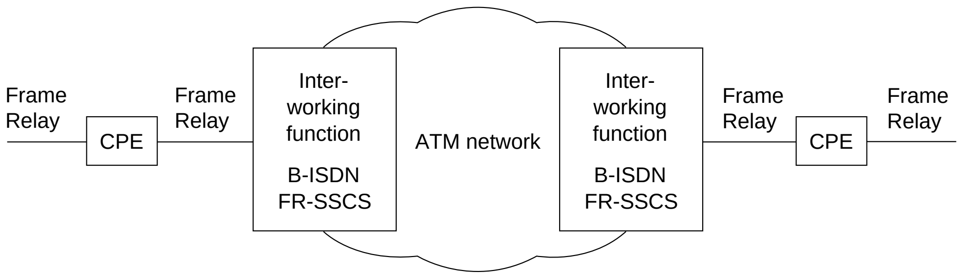
Network and Service Interworking Notes

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 8-11 and Figure 8-12).

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 8-11 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).

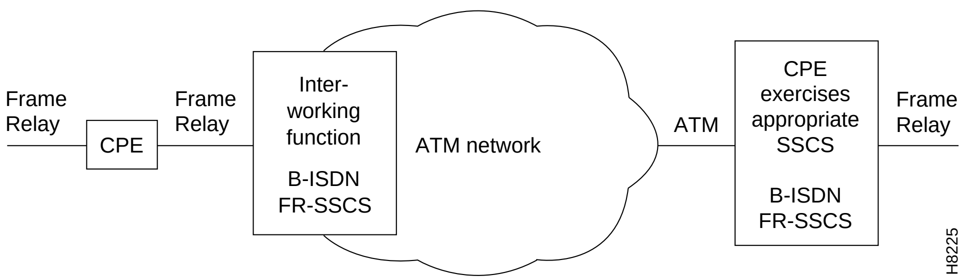
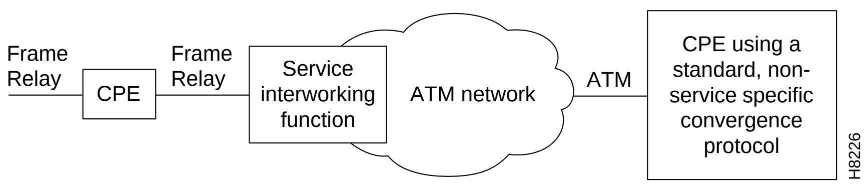


Figure 8-12 Frame Relay to ATM Service Interworking

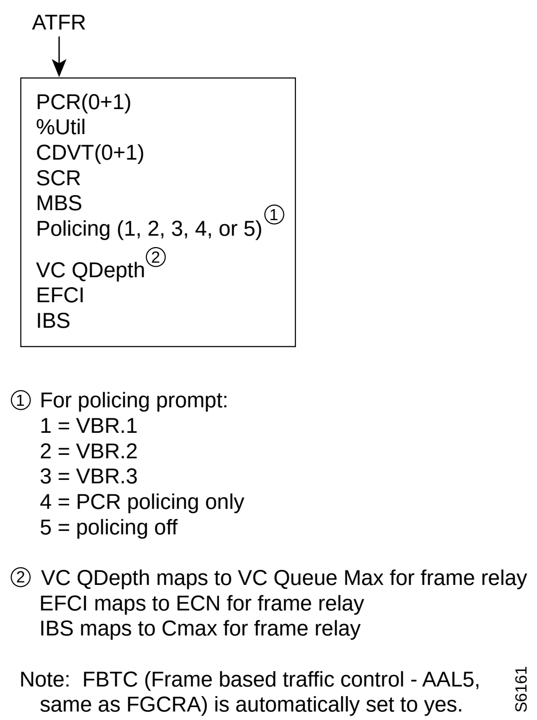


ATFR Network Interworking Connections

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 8-13 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-13 ATFR Connection Prompt Sequence

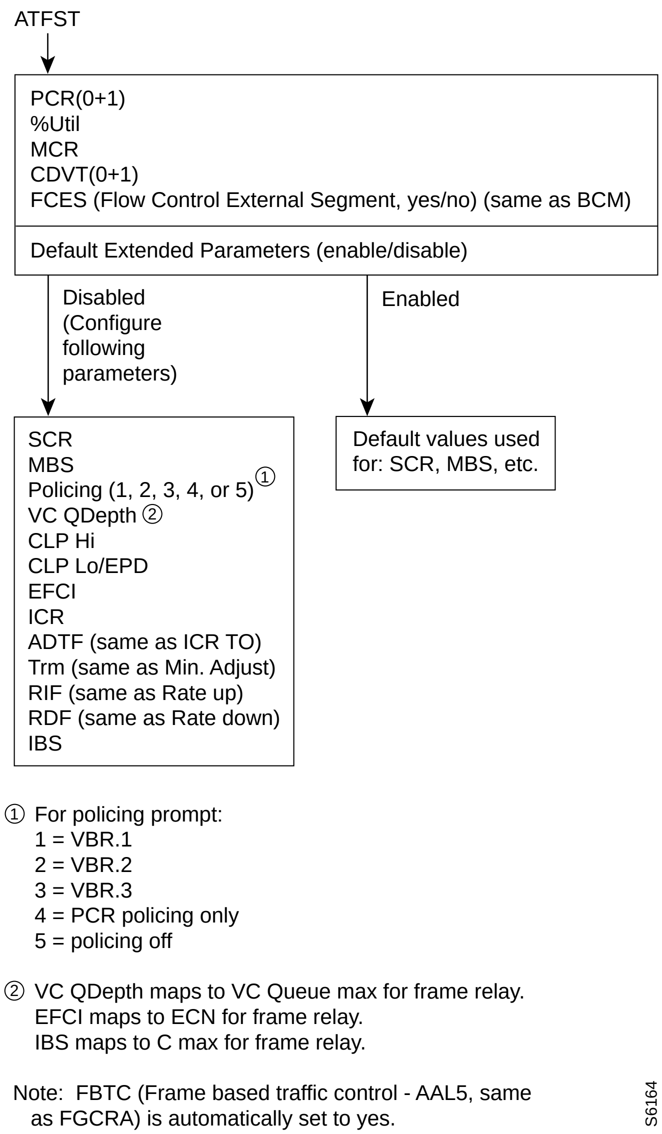


ATFST Network Interworking Connection

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 8-14 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-14 ATFST Connection Prompt Sequence

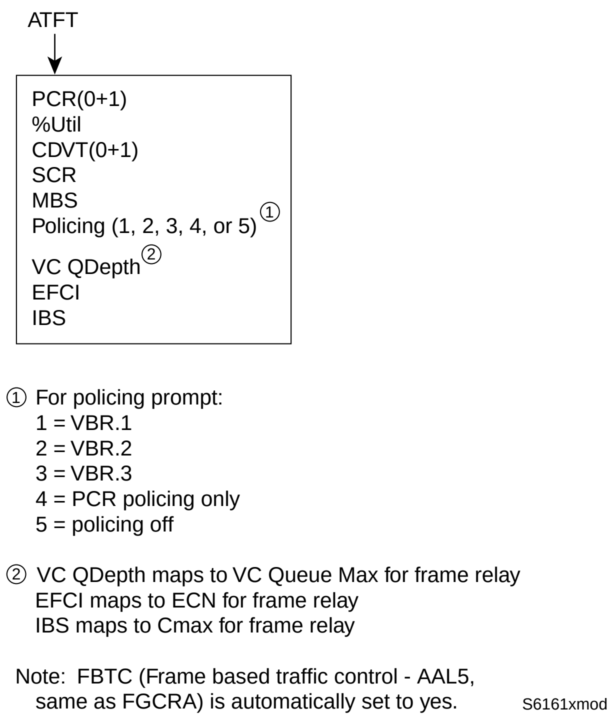


ATFT Transparent Service Interworking Connections

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 8-15 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-15 ATFT Connection Prompt Sequence

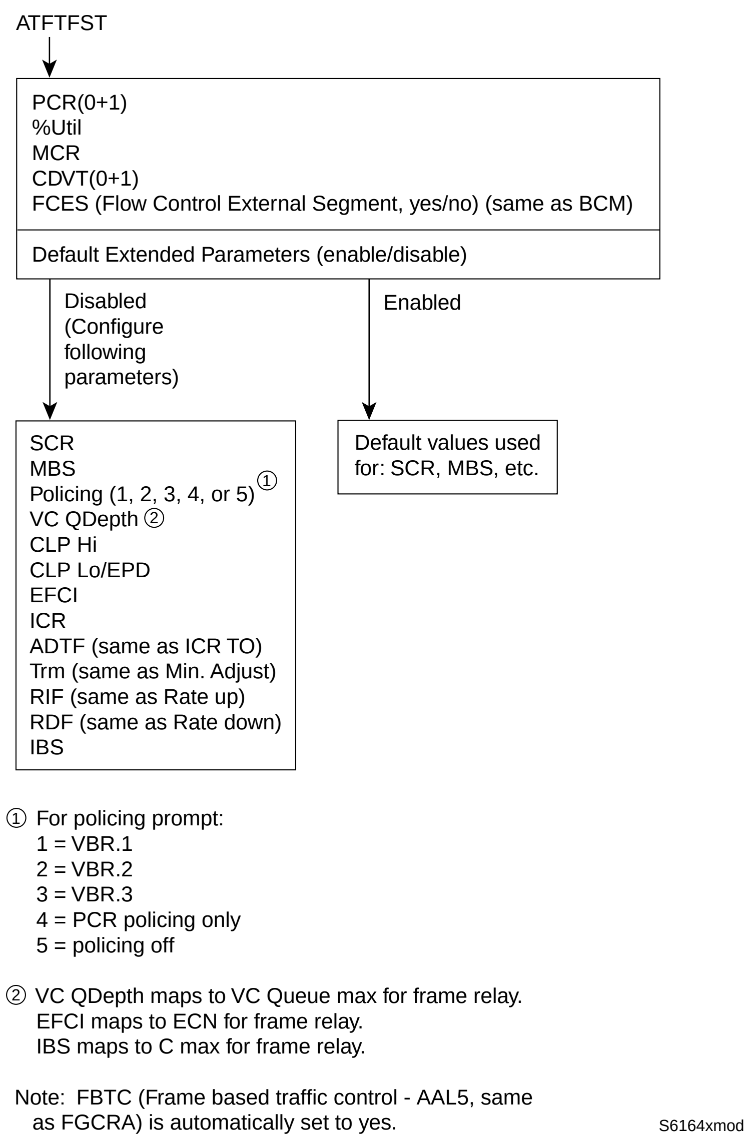


ATFTFST Transparent Service Interworking Connections

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

The parameters for an ATFTFST connection are shown in Figure 8-16 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-16 ATFTFST Connection Prompt Sequence

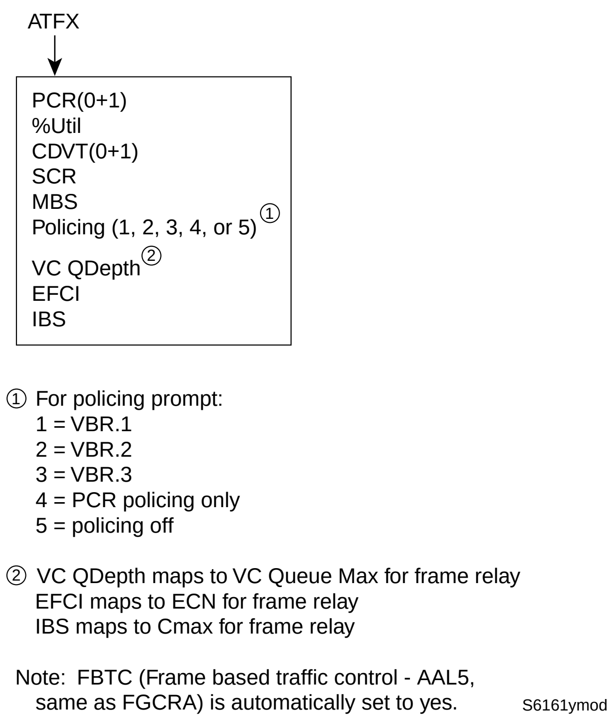


ATFX Translational Service Interworking Connections

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

The parameters for an ATFX connection are shown in Figure 8-17 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-17 ATFX Connection Prompt Sequence

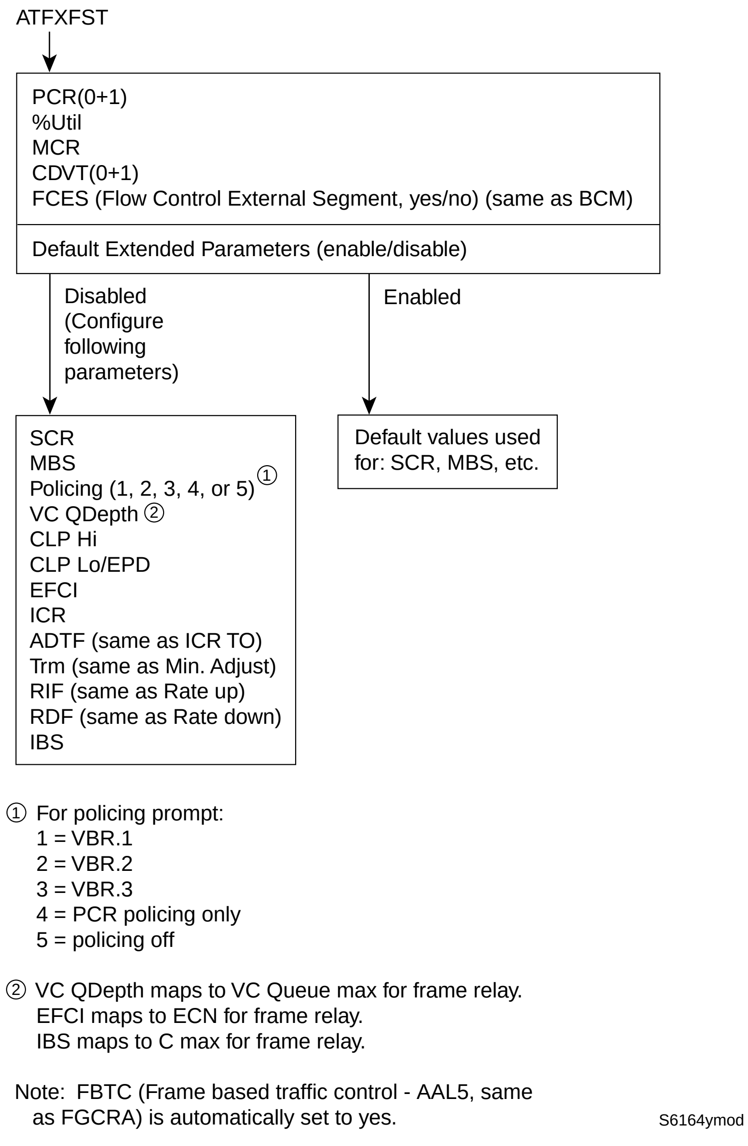


ATFXFST Translational Service Interworking Connections

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

The parameters for an ATFXFST connection are shown in Figure 8-18 in the sequence in which they occur during the execution of the **addcon** command.

Figure 8-18 ATFXFST Connection Prompt Sequence



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 8-19. 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 8-19 CBR Connection, UPC Overview

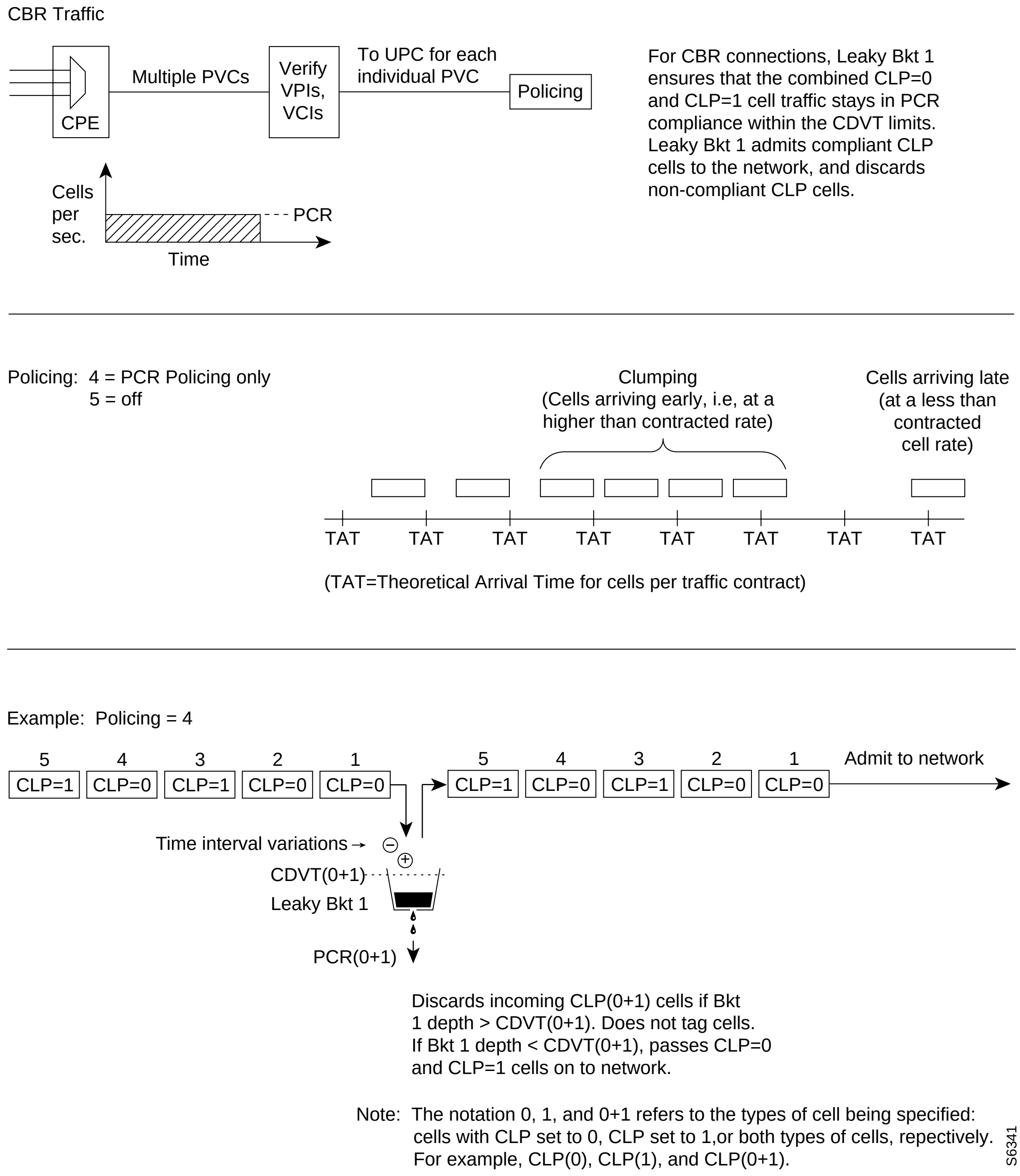


Figure 8-20 shows a CBR.1 connection policing example, with policing set to 4, where the CDVT depth of the single leaky bucket is not exceeded, and all cells, CLP(0) and CLP(1) are admitted to the network.

Figure 8-20 CBR.1 Connection with Bucket Compliant

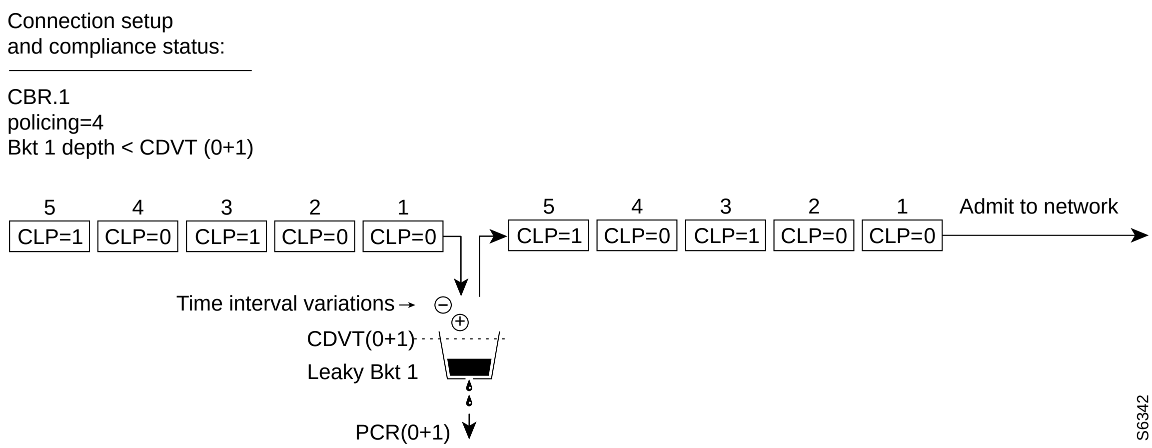
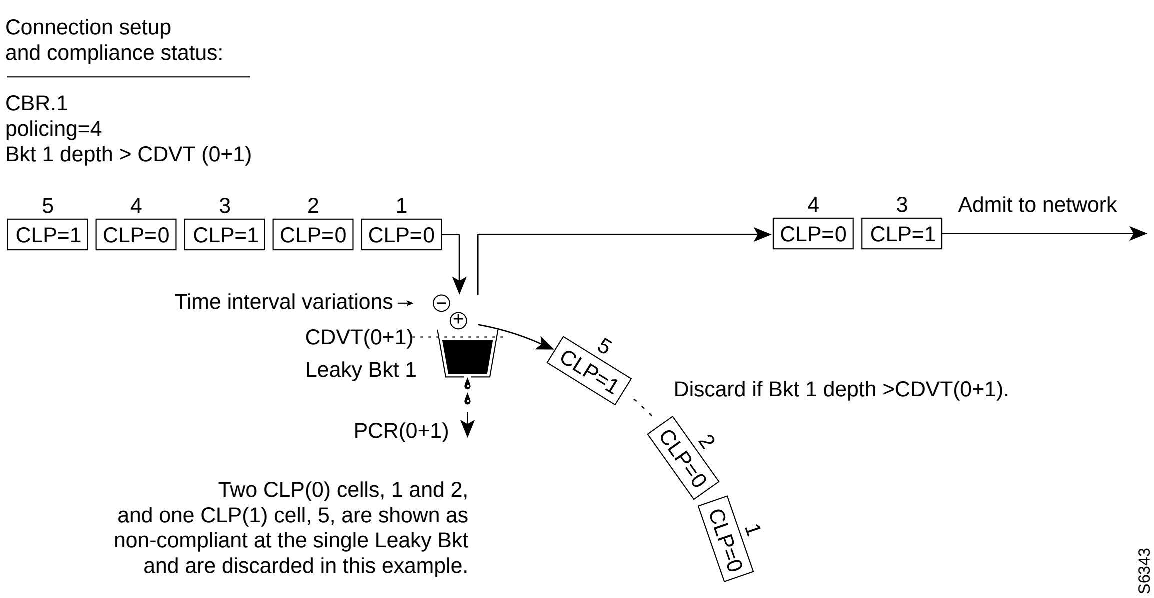


Figure 8-21 shows a CBR connection policing example, with policing =4, where the CDVT(0+1) of the single leaky bucket is exceeded and non-compliant cells are discarded. The leaky bucket only discards cells; it does not tag them

Figure 8-21 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 8-22.

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

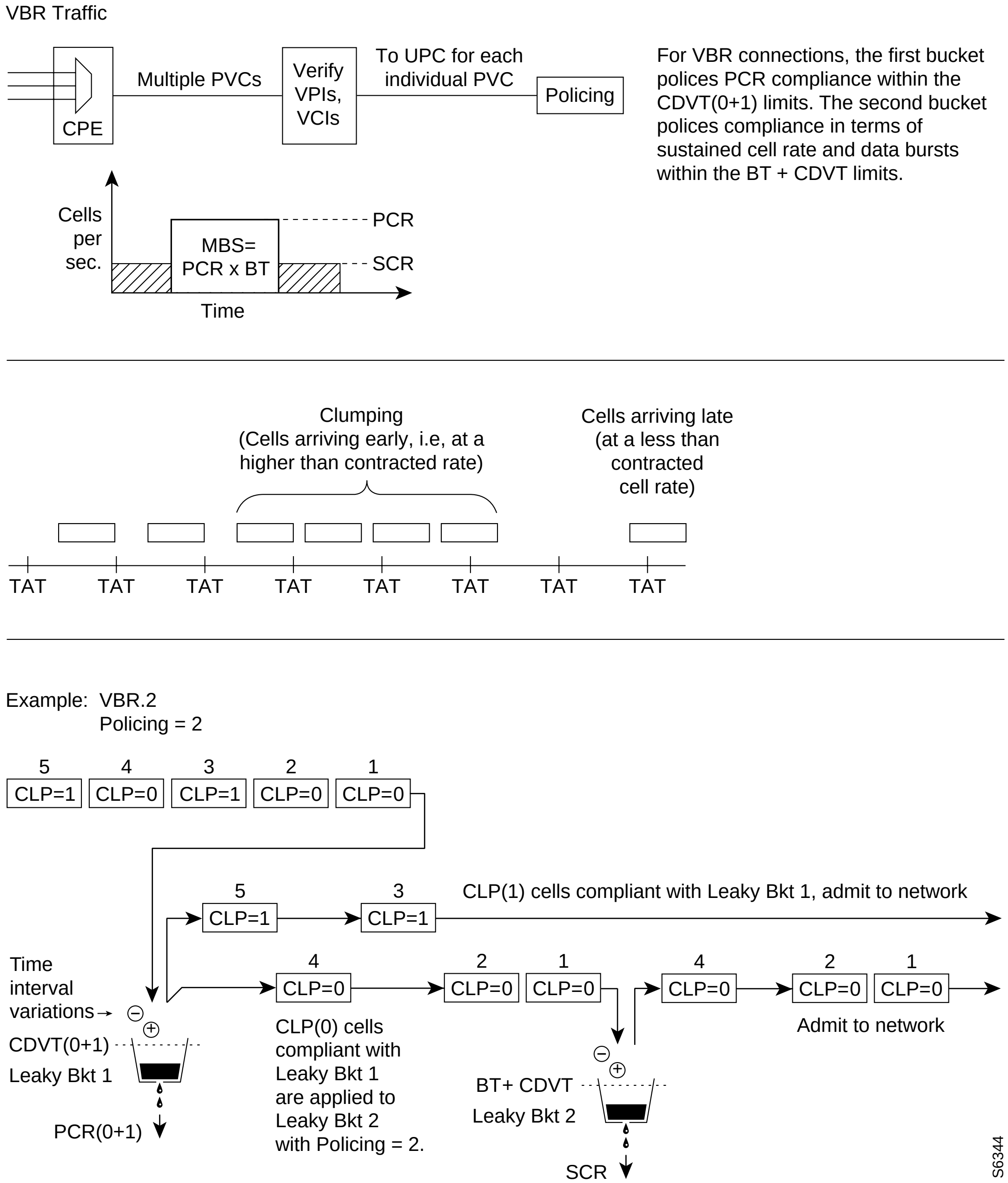
For VBR, traffic policing, depending on selected policing option, is based on:

- 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 8-22 VBR Connection, UPC Overview



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 8-23 shows a VBR connection policing example, with policing set to 4, leaky bucket 1 compliant, and all cells being admitted to the network.

Figure 8-23 VBR Connection, Policing = 4, Leaky Bucket 1 Compliant

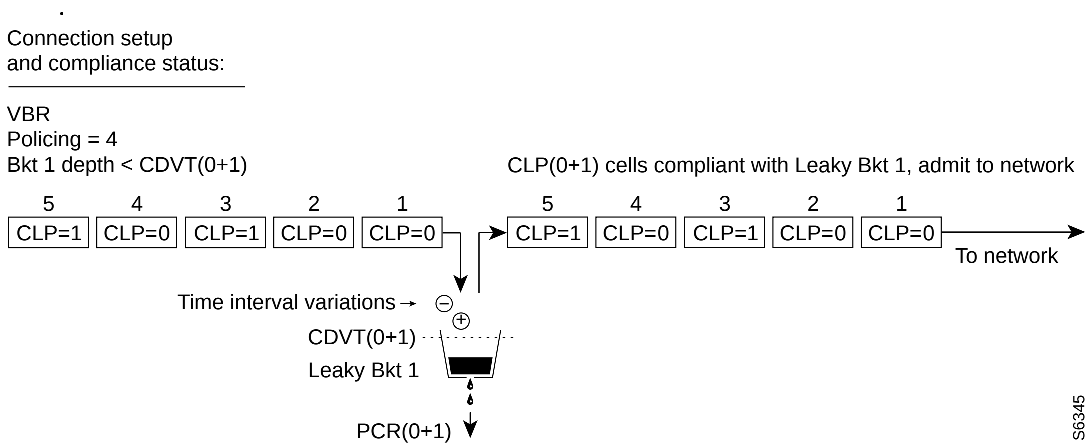


Figure 8-24 shows a VBR connection policing example, with the policing set to 4, and leaky bucket 1 non-compliant which indicates that the connection has exceeded the PCR for a long enough interval to exceed the CDVT (0+1) limit. Non-compliant cells with respect to leaky bucket 1 are discarded.

Figure 8-24 VBR Connection, Policing = 4, Leaky Bucket 1 Non-Compliant

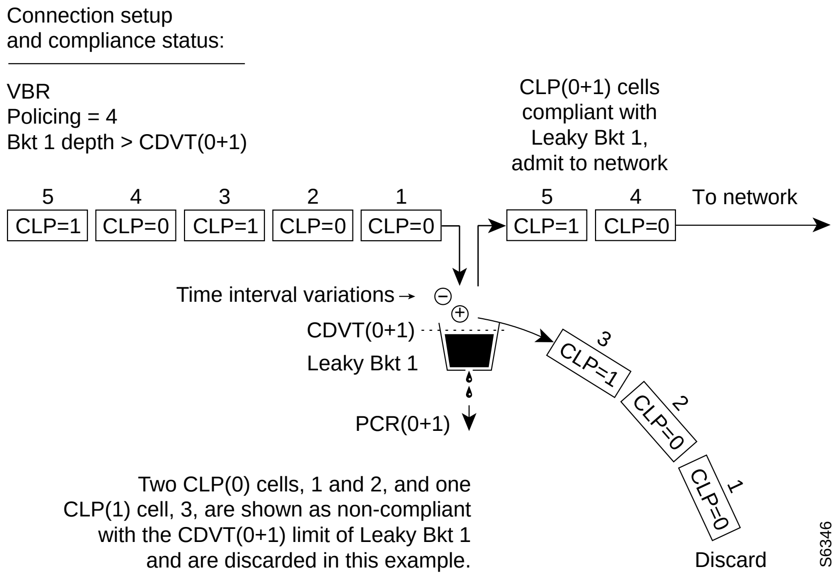


Figure 8-25 shows a VBR.2 connection policing example, with policing = 2, and both buckets compliant. Leaky bucket two is policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with the SCR sustained cell rate.

Figure 8-25 VBR.2 Connection, Policing = 2, with Buckets 1 and 2 Compliant

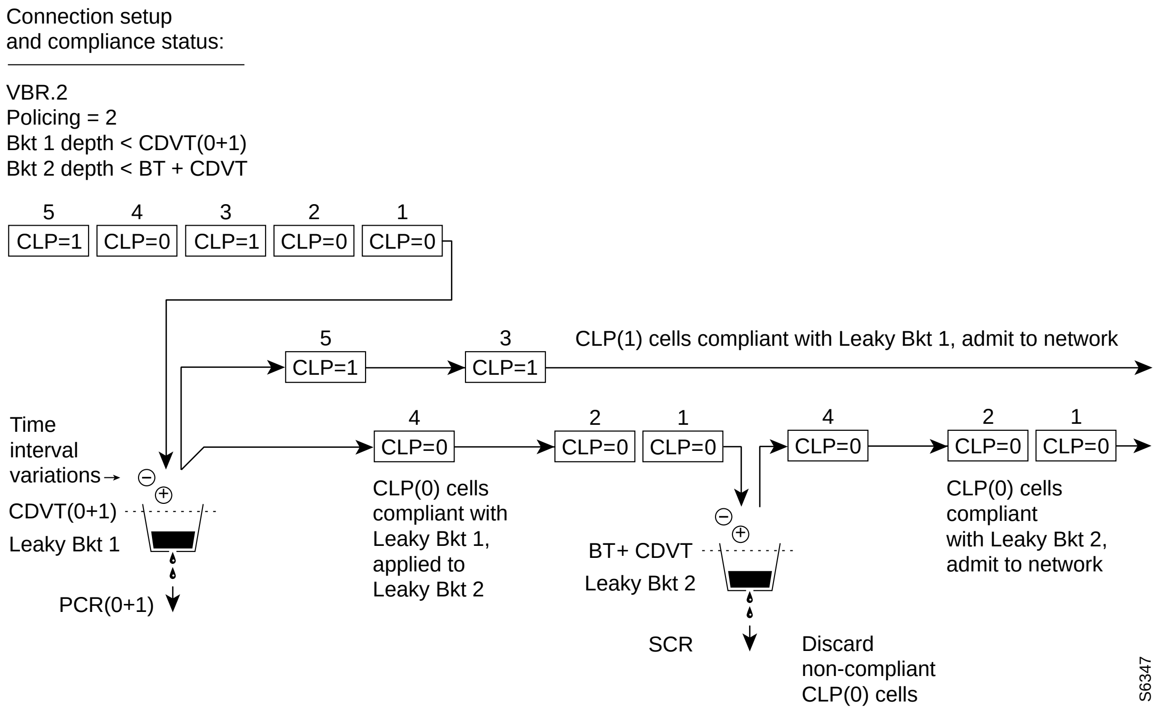


Figure 8-26 shows a VBR.2 connection policing example, with policing set to 2, and leaky bucket 2 non-compliant. Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR (sustained cell rate). In this example (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 8-26 VBR.2 Connection, Leaky Bucket 2 Discarding CLP (0) Cells

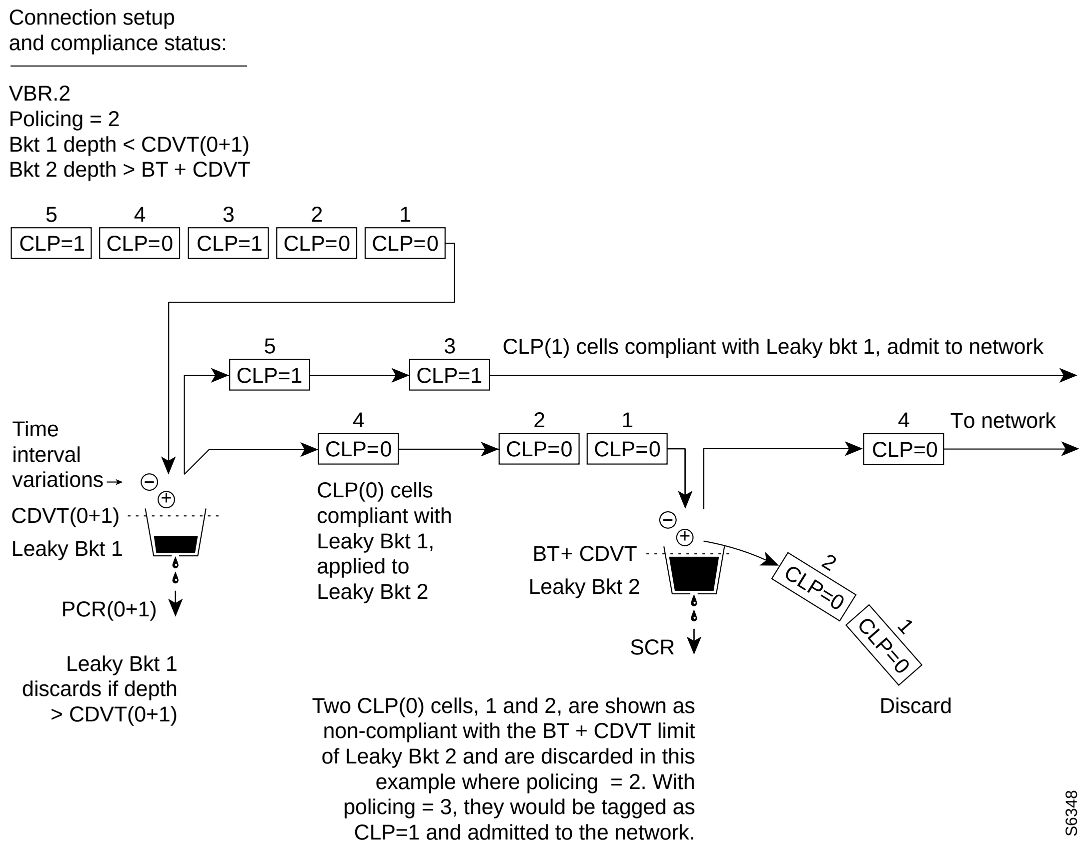


Figure 8-27 shows a VBR.1 connection policing example, with policing set to 1, and both buckets compliant. Leaky bucket 1 is policing the CLP (0+1) cell stream for conformance with the PCR limit. Leaky bucket 2 is policing the CLP (0+1) cell stream for conformance with CDVT plus maximum burst size MBS (as specified by BT), and for compliance with SCR sustained cell rate.

Figure 8-27 VBR.1 Connection, Policing = 1, with Buckets 1 and 2 Compliant

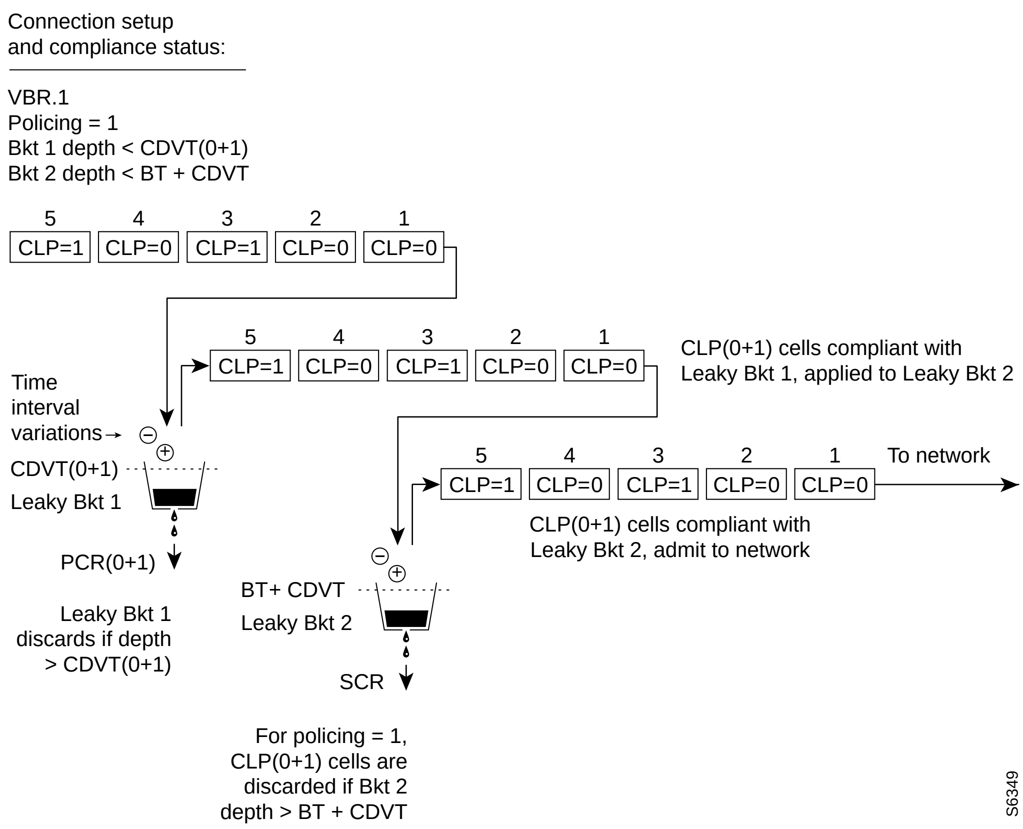
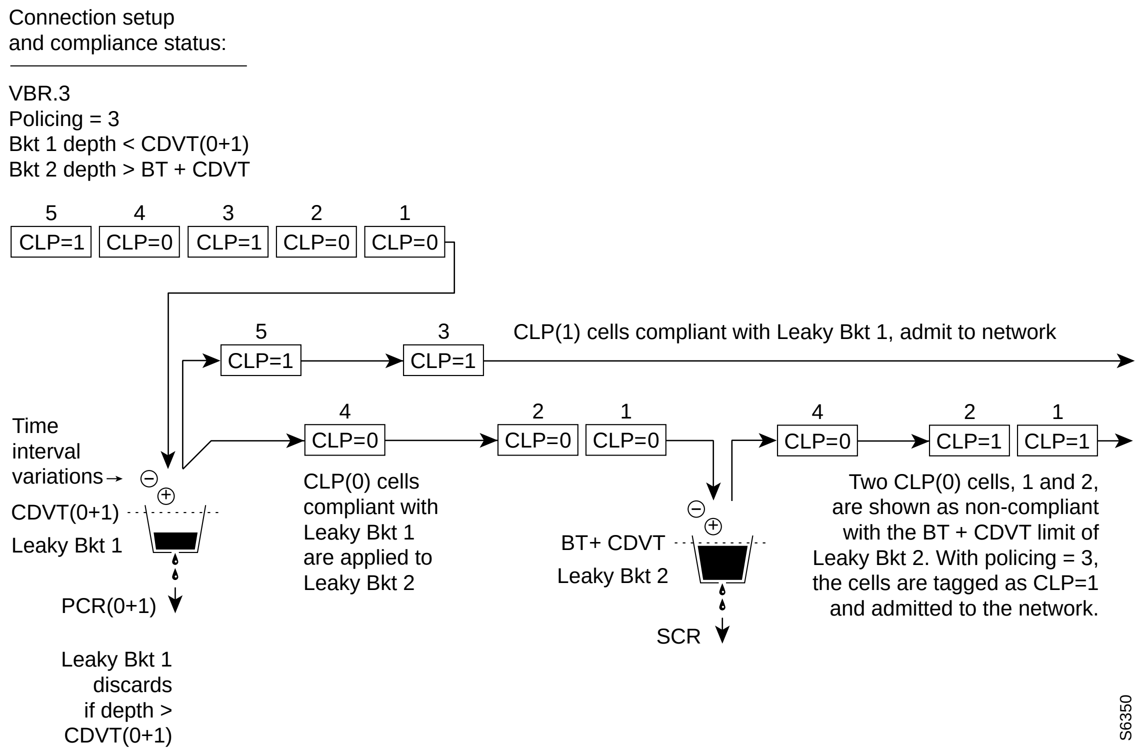


Figure 8-28 shows a VBR.3 connection policing example, with policing set to 3, and Leaky bucket 2 shown as non-compliant. Leaky bucket 2 is shown policing the CLP(0) cell stream for conformance with maximum burst size MBS (as specified by BT), and for compliance with SCR sustained cell rate. For the 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 8-28 VBR.3 Connection, Policing = 3, with Bucket 2 non-compliant



ABR Connection Policing

Available Bit Rate (ABR) connections are policed the same as the VBR connections, but in addition use either the ABR Standard with VSVD congestion flow control method or the ForeSight option to take advantage of unused bandwidth when it is available.

UBR Connection Policing

The contract for a unspecified bit rate connection is similar to the ABR connection service for bursty data. However, UBR traffic is delivered only when there is spare bandwidth in the network.

When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with the UPC parameters as shown in Figure 8-29.

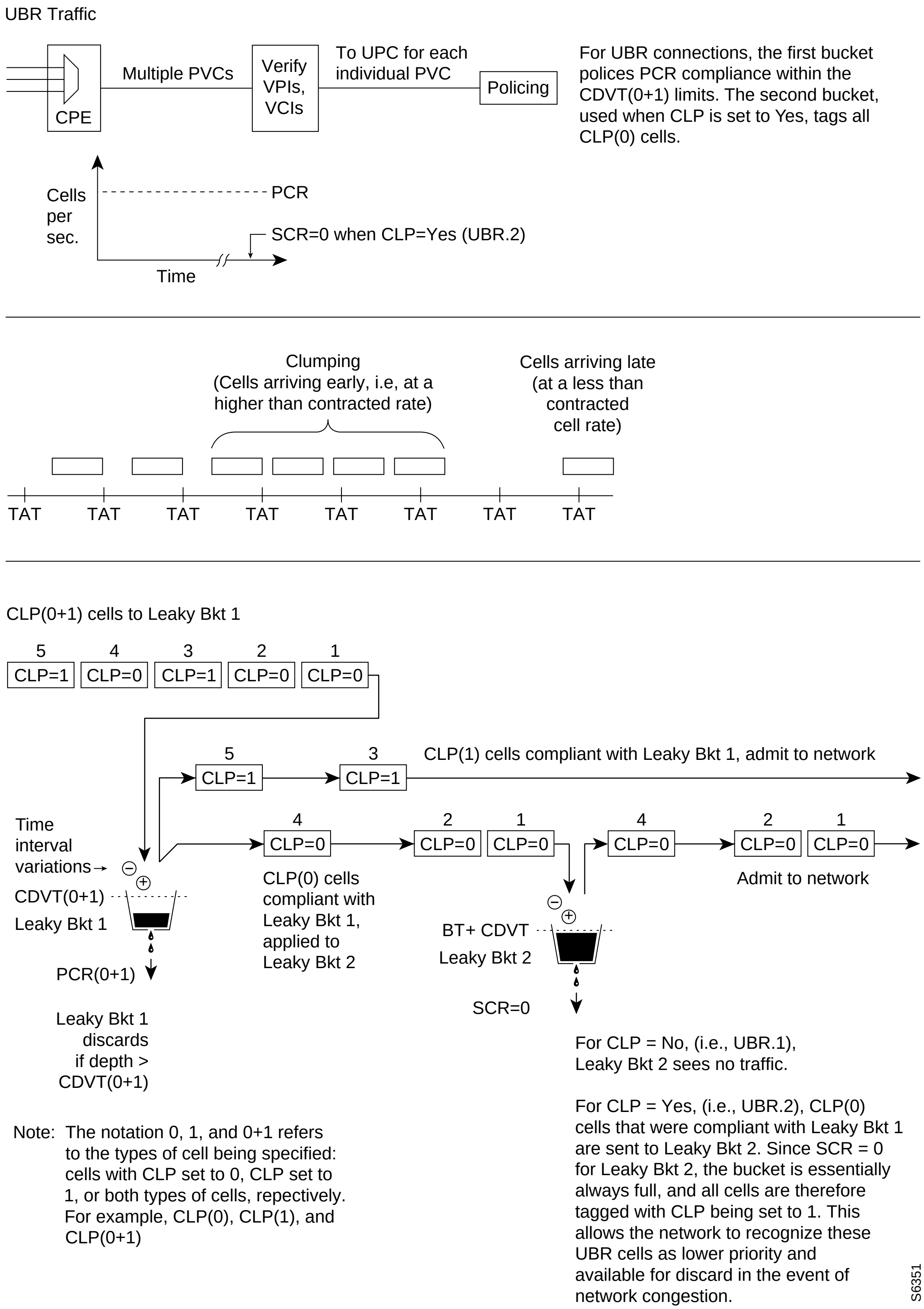
Leaky Bucket 1

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 8-29 UBR Connection, UPC Overview



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 8-11.

Table 8-11 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 8-11.

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 A-Bit 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 Cisco WAN Switching Command Reference*.

SONET APS

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 9-1 and shown in Figure 9-1 and Figure 9-2, respectively. APS 1+1 Annex B has the same general layout as shown in Figure 9-1, except that the active line is called the primary, and the standby line is referred to as the secondary.

Table 9-1 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 (i.e., LOS, LOF, Line AIS, or Bit Error Rate in excess of a configured limit) or a signal degradation condition (i.e., 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 9-1 APS 1+1 Redundancy

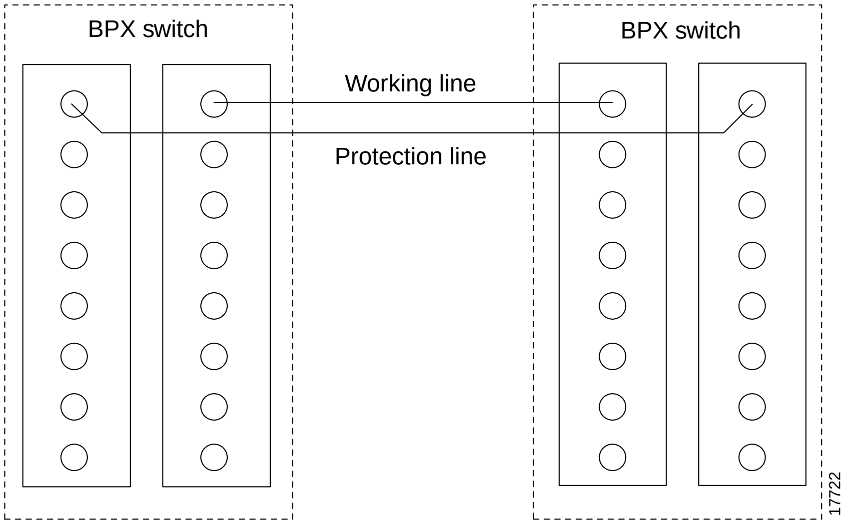
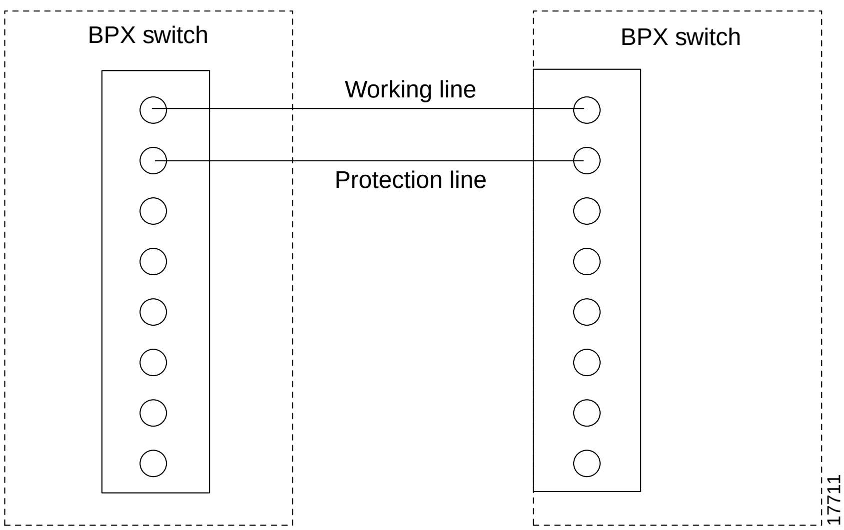


Figure 9-2 APS 1:1 Redundancy



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 9-2.

Table 9-2 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 9-3.

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 9-3 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 9-3. The types of available backcards are:

The types of redundant backcard and backplane sets required are:

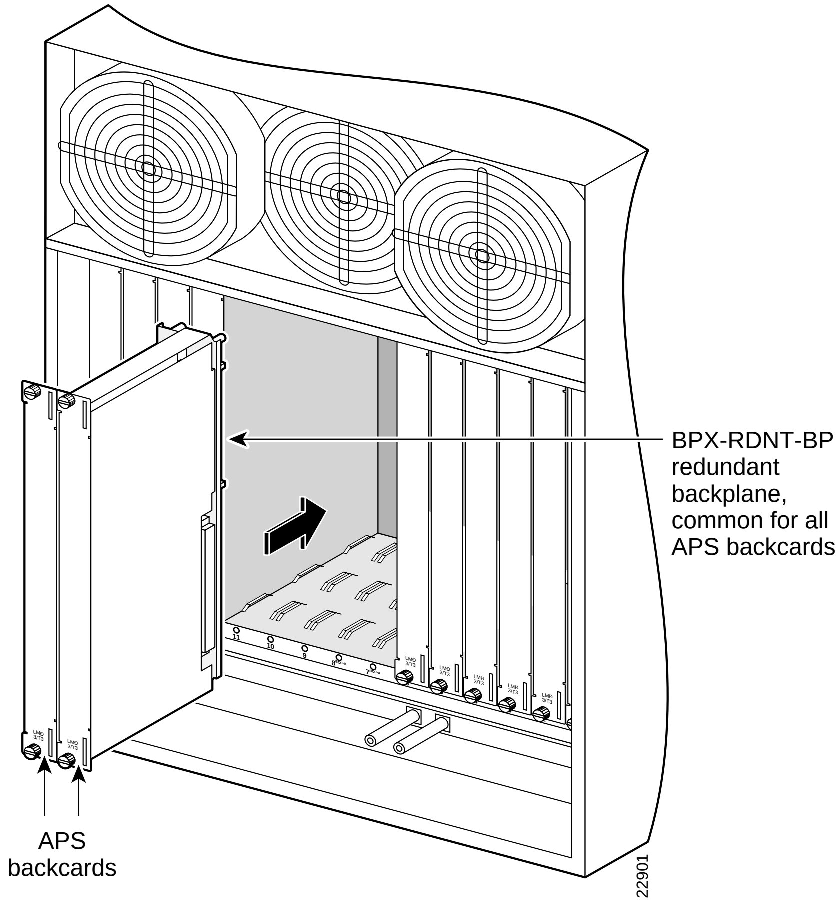
- BPX-RDNT-LR-155-8 (8 port, long reach, SMF, SC connector)
- BPX-RDNT-LR-622 (single port, long reach, SMF, FC connector)
- BPX-RDNT-SM-155-4 (4 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-155-8 (8 port, medium reach, SMF, SC connector)
- BPX-RDNT-SM-622 (single port, medium reach, SMF, FC connector)
- BPX-RDNT-SM-622-2 (2 port, medium reach, SMF, FC connector)

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

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

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

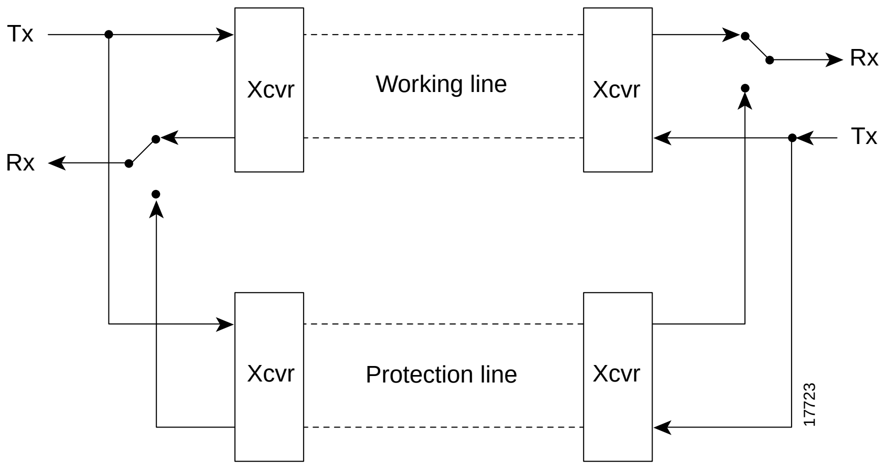
Figure 9-3 APS 1+1 Redundancy, Installing APS Backcards in APS Redundant Backplane



Traffic protected by APS 1+1 redundancy is carried via the working line and the protection line simultaneously (see Figure 9-4). 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 9-4 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 **(i.e., 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)

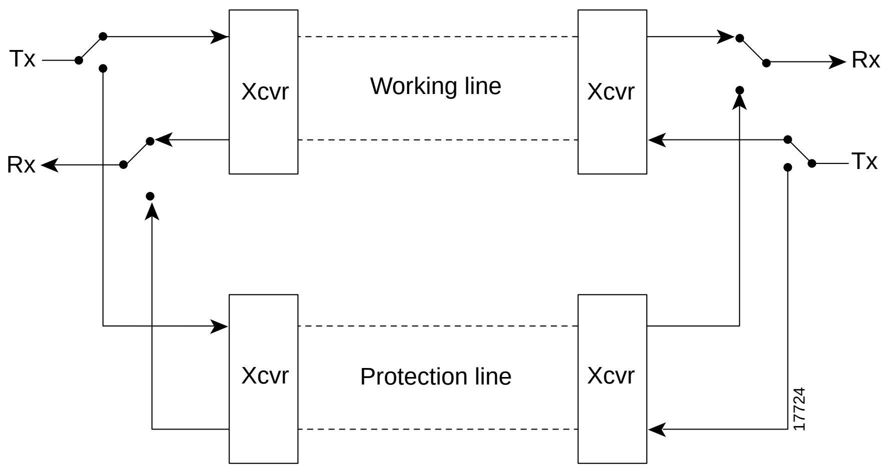
The APS 1:1 feature provides port and line redundancy for a single BXM front card and associated OC-3 or OC-12 redundant backcard.

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 9-5). 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 9-5 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 bidirectional operation and nonrevertive 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:

```
sswye     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 9-4. 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 9-4 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 9-4 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 9-4 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 9-5. 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 9-5 K1 Switching Conditions

APS K1 Command Precedence
Lock out of Protection
Forced Switch

Table 9-5 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 9-6, 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 9-6 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 9-7 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 multi-port 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 9-14, 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 **(i.e., 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

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 9-8 Possible APS System Architectures

	APS 1:1		APS 1+1, 1+1 ignore K1		APS 1+1 Annex B	
Mode	**Revertive**	**Non-reverti ve**	**Revertive**	**Non-reverti ve**	**Revertive**	**Non-reverti ve**
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)
  -
  -

CHAPTER 10

ATM and Frame Relay SVCs, and SPVCs

This chapter provides a brief overview of switched virtual circuits and soft permanent virtual circuits with respect to the BPX switch and co-located Extended Services Processor. For additional information, refer to the *Cisco WAN Service Node Extended Services Processor Installation and Operation Release 2.2* document.

This chapter contains the following:

- ATM and Frame Relay SVCs and SPVCs
- BPX Switch and ESP Interfaces
- Signaling Plane
- Network Interworking Between Frame Relay and ATM
- Extended Services Processor
- Network Management
- Resource Partitioning

ATM and Frame Relay SVCs and SPVCs

With a co-located Extended Services Processor (ESP), the BPX switch adds the capability to support ATM and Frame Relay switched virtual circuits (SVCs) in addition to support for permanent virtual circuits (PVCs) as shown in Figure 10-1.

The Private Network to Network Interface (PNNI) protocol is used to route SVCs across the network. PNNI provides a dynamic routing protocol which is responsive to changes in network availability and will scale to large networks.

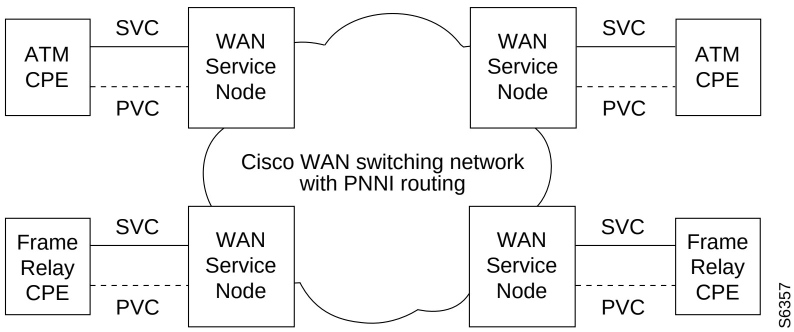
BPX switch resources, such as port VPI range and trunk bandwidth are partitioned between SVCs and PVCs. This provides a firewall between the two types of connections so that any SVCs that come on-line and off-line do not affect the availability of existing PVC services.

The following connections are supported with Release 9.1:

- Frame Relay SVC connections between Frame Relay end users over an ATM network (Network Interworking)
- ATM SVC connections between ATM end users
- SPVCs

The ESP provides the BPX switch with the ATM or Frame Relay signaling function. It interprets industry-standard signaling messages from ATM or Frame Relay CPE to provide the call setup and tear down for switched virtual circuits across the ATM network. In addition to SVC signaling, the ESP also performs PNNI routing, collects statistics, and processes alarms and billing records for SVC connections through the BPX switch.

Figure 10-1 Wide Area Network with BPX Switch and ESP



PVCs and SVCs

Both permanent virtual circuits and switched virtual circuits are defined by ATM and Frame Relay standards groups.

PVCs

After being added to a network, permanent virtual circuits (PVCs) remain relatively static. The PVC only allocates a physical circuit and consumes bandwidth when there is data to send. However, the permanent virtual circuit remains in place, always available for use, and is similar to a dedicated private line in this respect.

SPVCs

Soft permanent virtual circuits (SPVCs) are PVCs which are routed using the Private Network-Network Interface (PNNI) routing protocol. The “permanent” qualifier indicates that the virtual connection is established administratively, through an operator’s command, rather than on demand by signaling. A soft PVC is one where the establishment within the network is done by the ESP signaling (in this case, PNNI signaling), just as it is done for Frame Relay and ATM switched virtual circuits.

In the PNNI network, SPVC connections are established using the best available route. During a network failure, SPVC connections could be rerouted and the newly selected path many not be the optimal route. The ESP’s SPVC feature provides for auto-grooming of SPVCs. Auto-grooming is a background management process that evaluates SPVC connections; if a better path for the connection is found, the SPVC will be released and rerouted to the optimized path.

Refer to the *Cisco WAN Service Node Extended Services Processor Installation and Operation* for Release 2.2 document for detailed information about SPVCs.

SVCs

A switched virtual circuit (SVC) only exists when there is data to send and a calling process has been initiated. With a switched virtual circuit, there must be some signaling mechanism to build a connection each time the user (ATM or Frame Relay device in this case) needs it. In addition, when the call is disconnected, there must be a mechanism for the orderly disconnection of the call, and the network's resources must be relinquished. During a disconnect, the Cisco StrataCom network sweeps through its connection tables and removes the connection.

ATM SVCs are ATM connections setup and maintained by a standardized signaling mechanism between ATM CPE (ATM user end systems) across a Cisco StrataCom network. ATM SVCs are created on user demand and removed when the call is over, thus freeing up network resources.

Frame Relay SVCs are Frame Relay connections setup and maintained by a standardized signaling mechanism between Frame Relay CPE (Frame Relay user end systems) across a Cisco StrataCom network. Frame Relays SVCs are created on user demand and removed when the call is over, thus freeing up network resources.

BPX Switch and ESP Interfaces

The BPX switch supports the UNI and NNI interfaces for SVC operations as described in the following:

- UNI, that is the User Network Interface, is the interface for either ATM or Frame Relay customer premise equipment (CPE) to the BPX switch. The UNI is defined as any interface between a user device and an ATM network (that is, an ATM switch). The UNI defines the signaling method which the CPE must use to request and setup SVCs through the wide-area ATM network. In addition, the UNI is used to send messages from the network to the CPE (that is, user device) on the status of the circuit and rate control information to prevent network congestion.

  For ATM SVCs, the UNI supports either the ATM Forum 3.0 or 3.1 signaling standards as well as traditional ATM PVCs. (Remember the BPX switch also supports high-speed ATM UNI ports.)

  For Frame Relay, the UNI supports Frame Relay Forum Frame Relay User-to-Network SVC Implementation Agreement (FRF.4), which specifies the Frame Relay SVC signaling protocols. BPX switch Frame Relay UNIs (FRSMs) also support traditional Frame Relay PVCs.

- Network-to-Network Interface (NNI). The NNI is the interface to other BPX switch or foreign ATM Switches. The BPX switch supports Interim Inter-switch Protocol (IISP) 3.0 /3.1 or the Private Network to Network Interface (PNNI). These NNI interfaces provide the switching and routing functions between Cisco StrataCom wide-area networks and other networks. Information passing across a NNI is related to circuit routing and status of the circuit in the adjacent network. (Note that NNI could refer to both a connection between a BPX switch with ESP, and a connection between a BPX switch with ESP and a foreign switch.)

Interim Interswitch Protocol Routing

Interim Interswitch Protocol (IISP) is an interim static routing protocol defined by the ATM Forum to provide base level capability until the Private Network to Network Interface (PNNI) was specified. The IISP provides users with some level of multi-vendor switch interoperability based on the existing ATM Forum UNI 3.1 specifications. IISP assumes no exchange of routing information between switching systems. It uses a a fixed routing algorithm with static routes. Routing is done on a hop-by-hop basis by making a best match of the destination address in the call setup with address entries in the next hop routing table at a given switching system. Entries in the next hop routing table are configured by the user.

PNNI

The Private Network to Network Interface standards essentially define two protocols:

- Topology

  The Private Network to Network Interface (PNNI) defines a protocol for distributing topology information between switches and clusters of switches. This information is used to compute paths through the network. A key feature of the PNNI mechanism is its ability to automatically configure itself in networks in which the address structure reflects the topology. PNNI topology and routing are based on the well-known link-state routing technique.

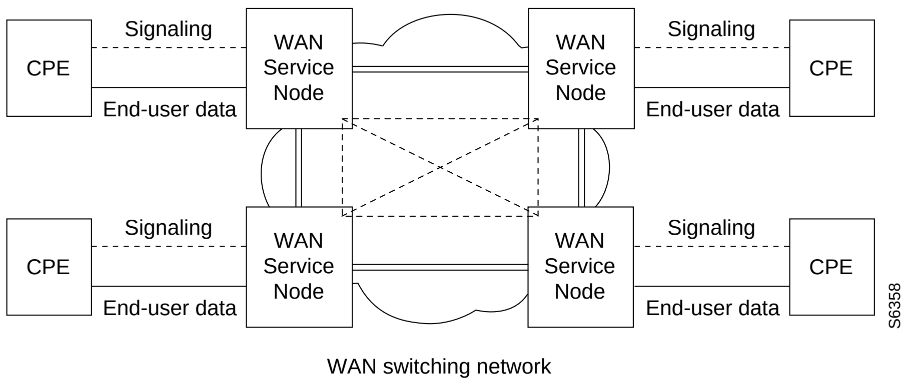
- Signaling

  PNNI also defines a second protocol for signaling, that is message flows used to establish point-to-point connections across the ATM network. This protocol is based on the ATM Forum UNI signaling, with mechanisms added to support source routing, crankback, and alternate routing of call setup requests in case of connection setup failure.

Signaling Plane

To support ATM and Frame Relay SVCs, the BPX switches essentially overlay a signaling network over a traditional (that is PVC-based) network. This signaling network, indicated by the dashed lines in Figure 10-2, connects all of the BPX switches with ESP and extends to the CPE. The signaling plane establishes and maintains SVCs between the CPE, that is, end users, across a Cisco StrataCom wide-area ATM network.

Figure 10-2 BPX Switch with ESP Network Signaling Plane



The signaling plane is created out of two basic types of signaling channels:

- User to Network Interface (UNI) signaling channels.
- Network to Network Interface (NNI) signaling channels.

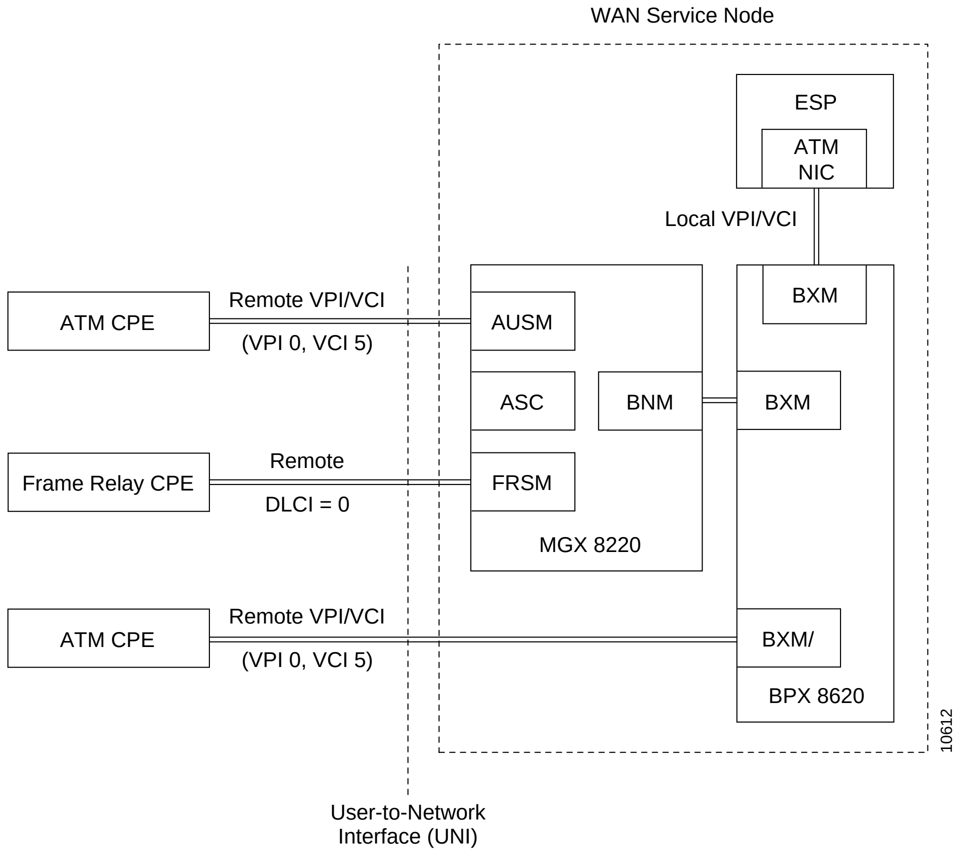
The signaling VCCs are normally configured during the provisioning of UNI ports and NNI trunks.

UNI Signaling Channel

There is an internal signaling VCC established between every UNI port on the BPX switch which will support ATM or Frame Relay SVCs and the ESP in the BPX switch.There are two types of UNI signaling channels supported by the BPX switch as shown in Figure 10-3.

- ATM UNI—For ATM CPE, these UNI VCCs extend from an ATM UNI port to the ESP. This is either a one segment cross-connect between the BXM (or ASI) attached to the ATM CPE and the BXM attached to the ESP within the BPX switch, or a two segment VCC from the MGX 8220 AUSM port connected to ATM CPE and the BXM attached to the ESP within the BPX switch. (Note that VPI 0 and VCI 5 are reserved on the ATM UNI port for ATM SVC signaling channels. The ILMI signaling channel will use VPI 0 and VCI 16, and the PNNI signaling channel will use VPI 0 and VCI 18.)
- Frame Relay UNI—For Frame Relay CPE, there will always be a two segment VCC between the MGX 8220 FRSM port connected to the ATM CPE and the BXM attached to the ESP within the BPX switch. (Note that DLCI 0 is reserved on the Frame Relay UNI port for Frame Relay SVC signaling channels.)

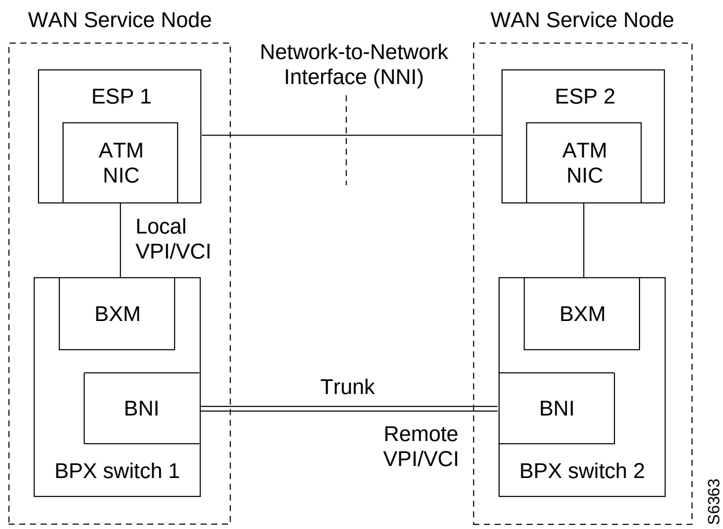
Figure 10-3 UNI Signaling Channels



NNI Signaling Channel

There is also a signaling channel established between each adjacent pair of BPX switches. This NNI signaling channel shown in Figure 10-4 is configured for either IISP or PNNI protocol. During IISP configuration, one side of the NNI signaling connection is configured as the user side and a weight is assigned. In the figure, the direct line between the ATN NICs indicates a logical connection; the physical connection is configured through BPX switch 1 and BPX switch 2.

Figure 10-4 ESP Signaling PVC



Network Interworking Between Frame Relay and ATM

Because the BPX switch is an ATM switch, Frame Relay SVCs that are setup and established across the Cisco StrataCom network must be translated into an ATM format to be carried across the network. At the far end, where typically the connection is terminated on another Frame Relay CPE, the ATM cells will have to be converted back to Frame Relay format. This is referred to as Network Interworking. Network Interworking can be performed between Frame Relay CPE and ATM CPE when the ATM CPE recognizes that it is connected to an interworking function (Frame Relay, in this case). The ATM CPE must then exercise the appropriate service specific convergence sublayer (SSCS). The SSCS will then convert the ATM cells to Frame Relay traffic.

In this release of the BPX switch with ESP, all Frame Relay SVC connections must be between Frame Relay CPE (that is, Frame Relay end users) or ATM CPE that is aware that it is performing Network Interworking, and all ATM SVC connections must be between ATM CPE (that is ATM end users). In other words, Service Interworking between ATM and Frame Relay SVCs is not supported in this release. (ATM and Frame Relay Service Interworking for PVCs is supported by the BPX switch.)

Extended Services Processor

The Extended Services Processor (ESP) is an adjunct processor shelf integrated into the BPX switch.

The basic ESP features include:

- 140 MIPS CPU, with a 143Mhz clock
- 128 Megabytes of memory
- 4 Gigabyte hard disk

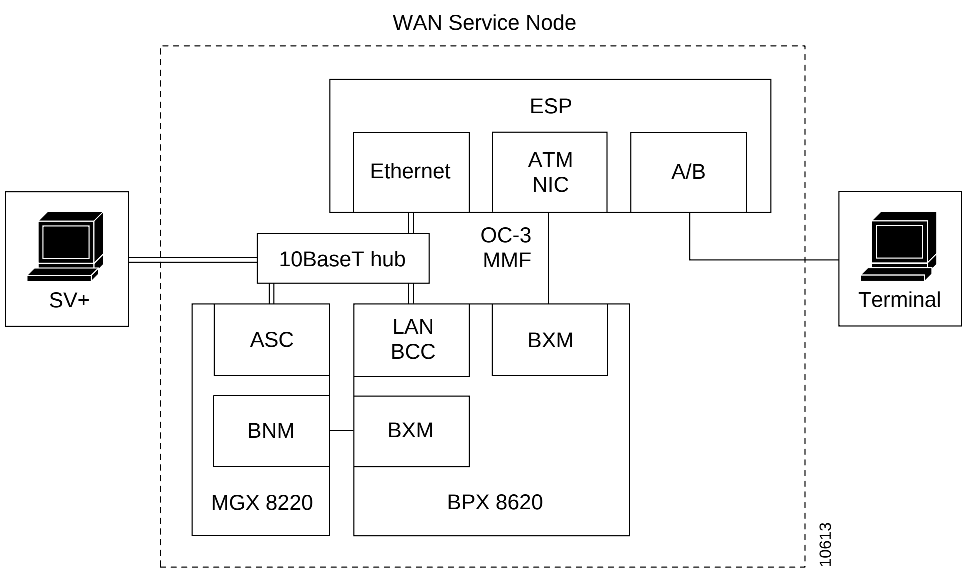
Available in either AC- or DC-powered models (ESP-AC or ESP-DC), the ESP is an orderable option for the BPX switch. The ESP can be configured in both non-redundant and redundant configurations. For the redundant configuration, two ESPs are installed in the BPX switch.

ESP Interfaces

The ESP uses three main physical interfaces, as shown in Figure 10-5:

- **Terminal port** for the direct connection of a terminal, such as a VT-100, to provide access for local configuration and to act as a console.
- **10Base-T Ethernet port** for connection to the Cisco WAN Manager Workstation and to the BPX switch. Telnet or XTERM sessions can be established through the Ethernet port, and perform the same functions as can be performed with a directly connected terminal.
- **ATM Network Interface Card (ATM NIC)** for connection to the BPX switch. The ATM NIC is typically connected to a BPX switch BXM card using OC-3 multimode fiber connection with SC connectors. There are optional cables with built-in optical attenuation that allow BXM single mode fiber (SMF) backcards to be connected to the ESP ATM NIC.

Figure 10-5 ESP Physical Interfaces



The ESP also provides the following application interfaces:

- **SNMP** to configure and monitor the ESP.
- **TFTP** (trivial file transfer protocol) for uploading statistics, Call Detail Records (CDRs), and downloading configuration files and new software releases and revisions.
- **Telnet** for accessing the ESP remotely, such as from the Cisco WAN Manager Workstation.

Stand-Alone ESP

A single ESP controlling a WAN Service Node, such as is shown in Figure 10-5, operates in the StandAlone mode. In the StandAlone mode there is no redundancy for a failed ESP. During the initial installation of a ESP, it can be configured as either Primary or Secondary but must be configured to operate in StandAlone mode.

When a second ESP is added to a single ESP operating in StandAlone mode, you must change the operating mode of a StandAlone ESP to Active or Standby mode.

Redundant ESPs

As shown in Figure 10-6, ESPs can be installed in redundant pairs in the WAN Service Node. In a redundant pair, one ESP is active, that is it controls the switched services in the WAN Service Node, and the other ESP is standby. The redundant ESPs are known as peers. The ESPs will switch roles from active to standby and vice versa under the following conditions:

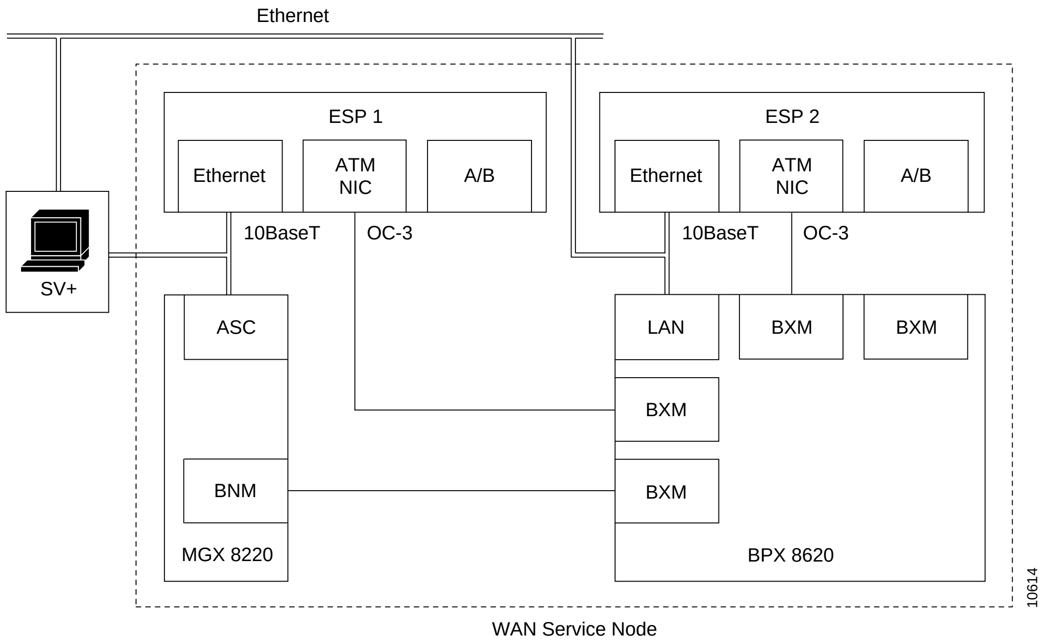
- Controlled switchover invoked from the active ESP Configuration Interface.
- The active ESP detects a major service affecting failure, such as a BPX switch polling failure or an ATM NIC card failure, and relinquishes the active role, by going Out of Service.
- The standby ESP detects that the inter-ESP paths have failed and assumes the active role.

Note During a switchover, all SVC connections will be torn down and the ATM or Frame Relay CPE will have to initiate another SVC call to reestablish them. During a switchover, all SPVC calls when be released, but when the standby ESP becomes active, it will reestablish the SPVCs.

Each ESP determines its role by means of Role Resolution protocol, which exchanges messages between the two units at startup. Both the active ESP and the standby ESP monitor its role and connectivity, and if appropriate, automatically switchover (that is, switch roles from active to Out of Service and from standby to active) with the peer ESP.

The redundant ESPs need to synchronize their database so that when the active ESP has gone out of service, the standby unit can take over and resume the service. There are two types of update mechanisms for synchronizing ESP databases. These are the bulk and real-time updates. The bulk update is used to synchronize a standby ESP with an active unit whenever it is restarted. The real-time updates are those messages that are exchanged after ESPs are synchronized and while both the active and standby ESPs are communicating.

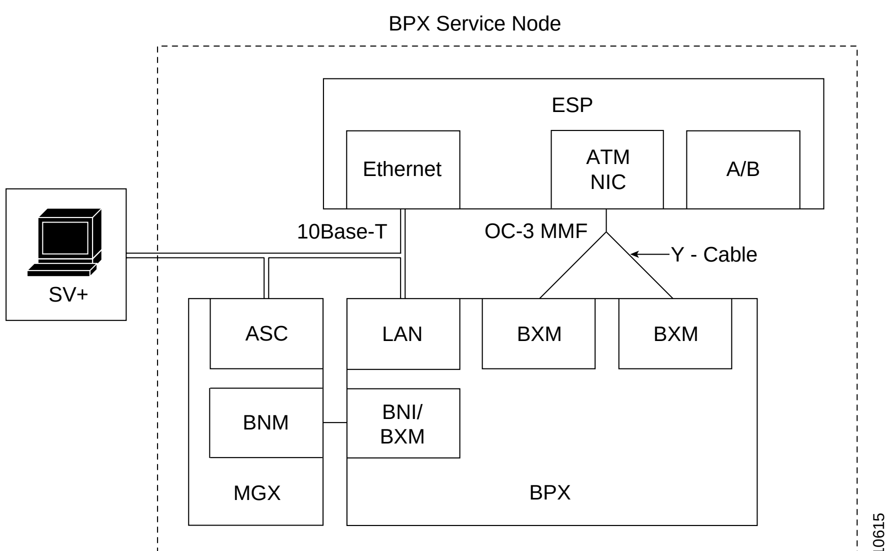
Figure 10-6 ESP Redundant Pair



Y-Cable Redundancy

The WAN Service Node provides another form of ESP redundancy protection through the use of Y-cables. With Y-cables, the ESP ATM NIC can be connected to two BXM cards or two BXM ports, as shown in Figure 10-7. This prevents the failure of a BXM card or port from disabling the ESP.

Figure 10-7 ESP Y-Cable Redundancy



Other Redundancy Options

Figure 10-7 illustrates only a single ESP-to-BXM redundancy option. There are four ESP-to-BXM redundancy options possible:

1. A single ESP with a Y-cable to redundant BXMs.
2. Two ESPs (a redundant pair), each attached to a single port on a single BXM.
3. Two ESPs (a redundant pair), each attached to a single port on two separate (redundant) BXMs.
4. Two ESPs (a redundant pair), each attached to different ports with Y-cables on two separate (redundant) BXMs.

Y-cables are for connecting the ESP's ATM Network Interface Card to redundant BXMs. They do not necessarily indicate that the ESP is connected in the redundant pair configuration (that is, an active and standby ESP). The Cisco WAN Service Node Extended Services Processor Installation and Operation document contains further information about ESP Y cables.

Network Management

As shown in Figure 10-5, the BPX switch can have an Ethernet LAN connection to a Cisco WAN Manager Workstation. Cisco WAN Manager discovers and monitors the ESP similarly to the way it does an MGX 8220 interface shelf. Cisco WAN Manager discovers the existence of the ESP when it is added to the BPX switch with the **addshelf** command. After discovery, the ESP will be displayed on the Cisco WAN Manager topology map as a shelf attached to the BPX switch.

Cisco WAN Manager manages the BPX switch by providing:

- Telnet access to the ESP Configuration Interface.
- Configuration backup and restore.
- Image download allows the user to select an ESP from the topology map and then select Image Download from a pull-down menu. A dialog screen displays the list of available image files and prompts the user to select a file. The selected file is sent to the ESP.

Resource Partitioning

During provisioning, resources on all UNI ports (both ATM and Frame Relay) are partitioned between SVCs and PVCs. Partitioning is performed using the BPX switch and MGX 8220 command line interfaces. This partitioning information is retrieved from the BPX switch by reading its port and trunk tables and from the MGX 8220 by reading the resource partitioning tables in the AUSM and FRSM MIBs.

The BPX switch line and routing or feeder trunk resources to be partitioned are:

- LCN range
- VPI range
- Port Queues
- Egress Queue pool size
- Bandwidth

MGX 8220 Feeder Trunk (BXM/BNI) resources to be partitioned are:

- LCN range
- Bandwidth

MGX 8220 AUSM port resources to be partitioned are:

- LCN range
- VPI range

MGX 8220 FRSM port resources to be partitioned are:

- LCN range
- DLCI range

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 Switching Command Reference* for further details. Refer to 9.2 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. In this release, two VSI controllers in different control planes can independently control the switch with no communication between controllers. The controllers are essentially unaware of the existence of other control planes sharing the switch. This is possible because different control planes used different partitions of the switch resources.

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 by 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

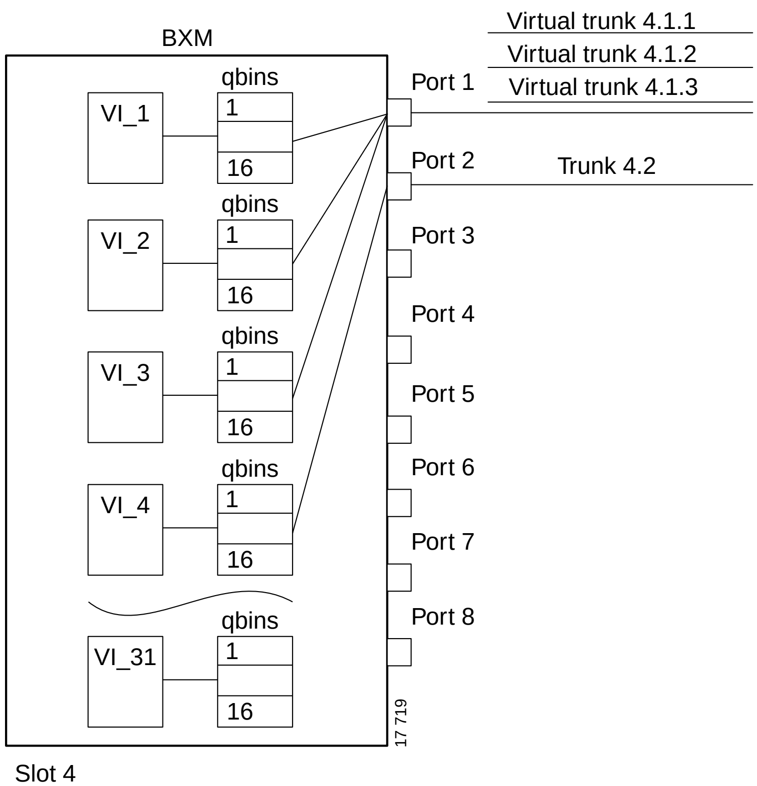
The BXM has 31 virtual interfaces that provide a number of resources including qbin buffering capability. One virtual interface is assigned to each logical trunk (physical or virtual) when the trunk is enabled. (See Figure 11-1.)

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 11-1).

Figure 11-1 BXM Virtual Interfaces and Qbins



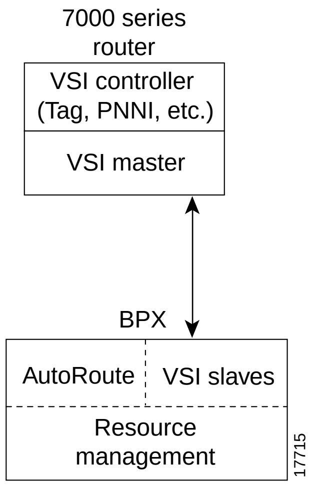
VSI Master and Slaves

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 11-2).

The controller sets up the following types of connections:

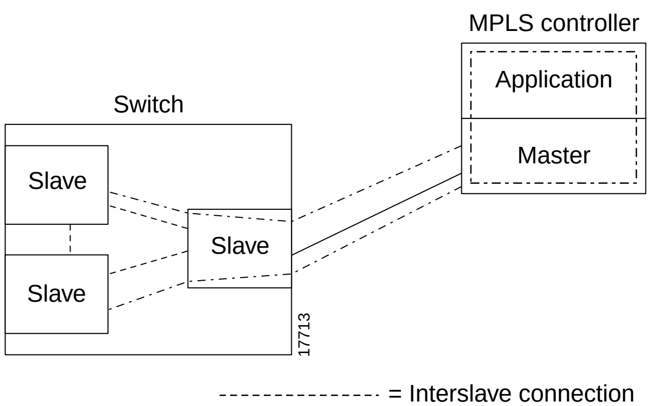
- Control virtual connections (VCs)
  - Master to Slave
  - Slave to Slave
- User Connection
  - User connection (that is, cross-connect)

Figure 11-2 VSI, Controller and Slave VSIs



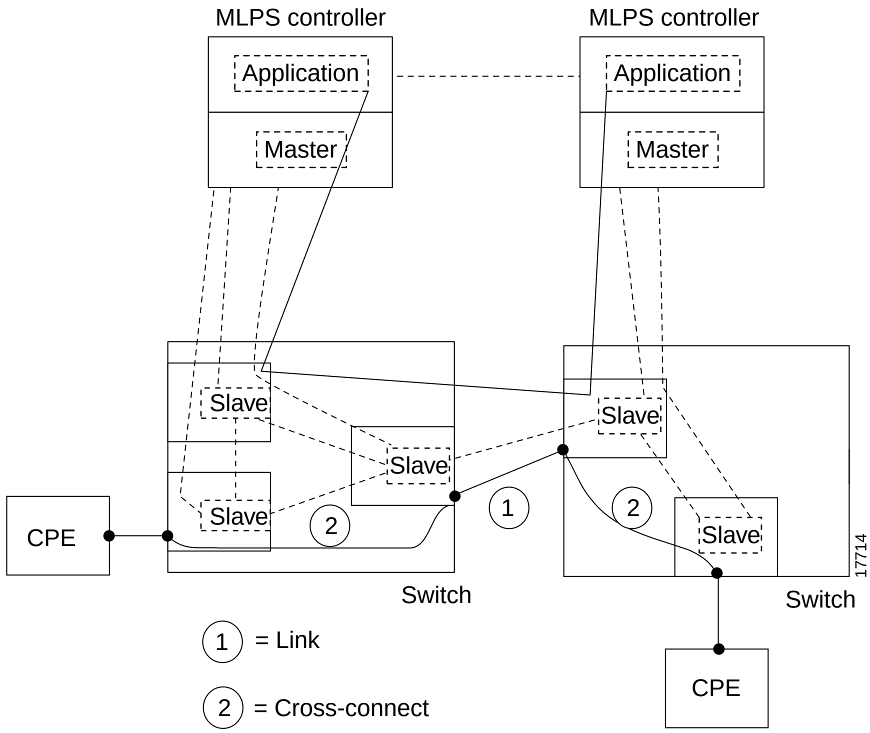
The controller establishes a link between the VSI master and every VSI slave on the associated switch. The slaves in turn establish links between each other (see Figure 11-3).

Figure 11-3 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 11-4.

Figure 11-4 Cross Connects and Links between Switches



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 In this release, you can configure partition resources between Automatic Routing Management PVCs and two VSI controllers (LSC or PNNI). See "Multiple Partitions" later in this section.

Prior to this release, just one controller (of a particular type) was supported, although you could have different types of controllers splitting up a partition's assets.

The resources that need to be configured for a partition are shown in Table 11-1 for a partition designated ifci, which stands for interface controller 1 in this instance. The three parameters that need to be distributed are the number of logical connections (lcns), bandwidth (bw), and virtual path ids (vpi).

Table 11-1 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, etc., information that is converted to a logical connection number (lcn).

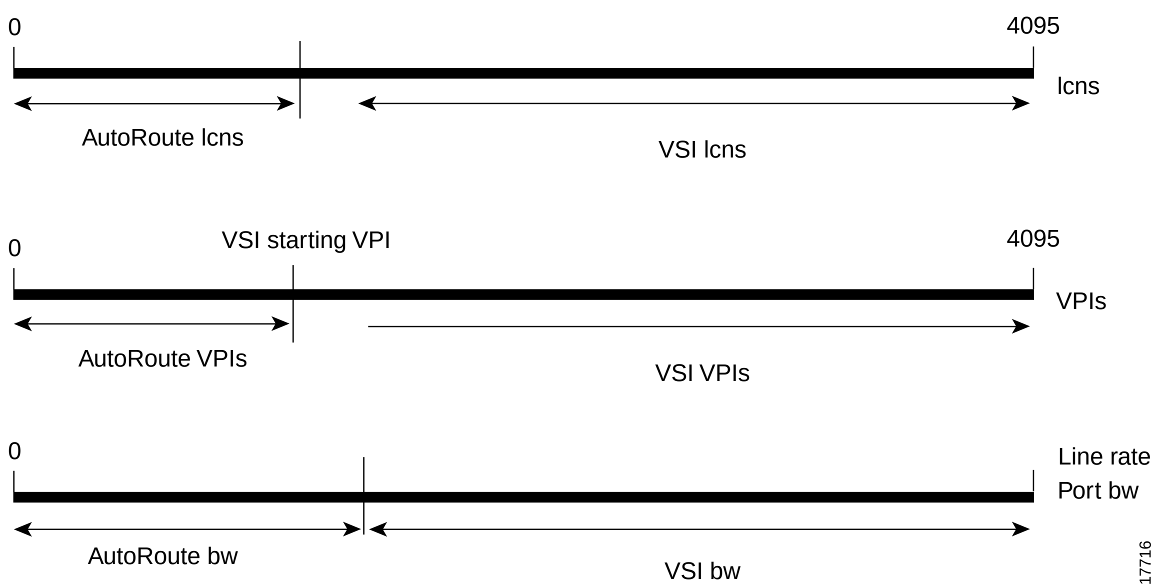
Some ranges of values available for a partition are listed in Table 11-2:

Table 11-2 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 11-5.

Figure 11-5 Graphical View of Resource Partitioning, Autoroute and VSI



Multiple Partitioning

In this release, you can configure partition resources between Automatic Routing Management PVCs and two VSI controllers (LSC or PNNI). Two VSI controllers in different control planes can independently control the switch with no communication between controllers. The controllers are essentially unaware of the existence of other control planes sharing the switch. This is possible because different control planes used different partitions of the switch resources.

You can add one or more redundant LSC controllers to one partition, and one or more redundant PNNI controllers to the other partition. In this release, two new templates have been added for interfaces with multiple partitions controlled simultaneously by a PNNI controller and an LSC.

The master redundancy feature allows multiple controllers to control the same partition. In a multiple partition environment, master redundancy is independently supported on each partition.

These limitations apply to multiple VSI partitioning:

- Only one or two partitions are supported.
- Resources cannot be redistributed amongst different VSI partitions.
- The resources that are allocated to a partition are: LCNS, Bandwidth and VPI range.
- Resources are also allocated to AutoRoute.The resources allocated to AutoRoute can be freed from AutoRoute and then allocated to VSI.
- No multiple partitions on Virtual Trunks. A Virtual Trunk is managed by either AutoRoute or by a single VSI partition.

Only one controller can be added to a BPX interface. Different controllers must be added to different switch interfaces.

For more information on multiple VSI partitioning, see the chapter on “VSI Commands” in the *Cisco WAN Switching Command Reference, Release 9.2.30*.

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 provides 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 (for example, BPX) and downloaded to the service modules (for example, 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 (for example PCR, MCR)
- Other ATM Forum Traffic Management 4.0 parameters

Each VC added by a VSI master is assigned to a specific service class by means of a 32-bit service type identifier. Current identifiers are for:

- ATM Forum service types
- Autoroute
- MPLS Switching

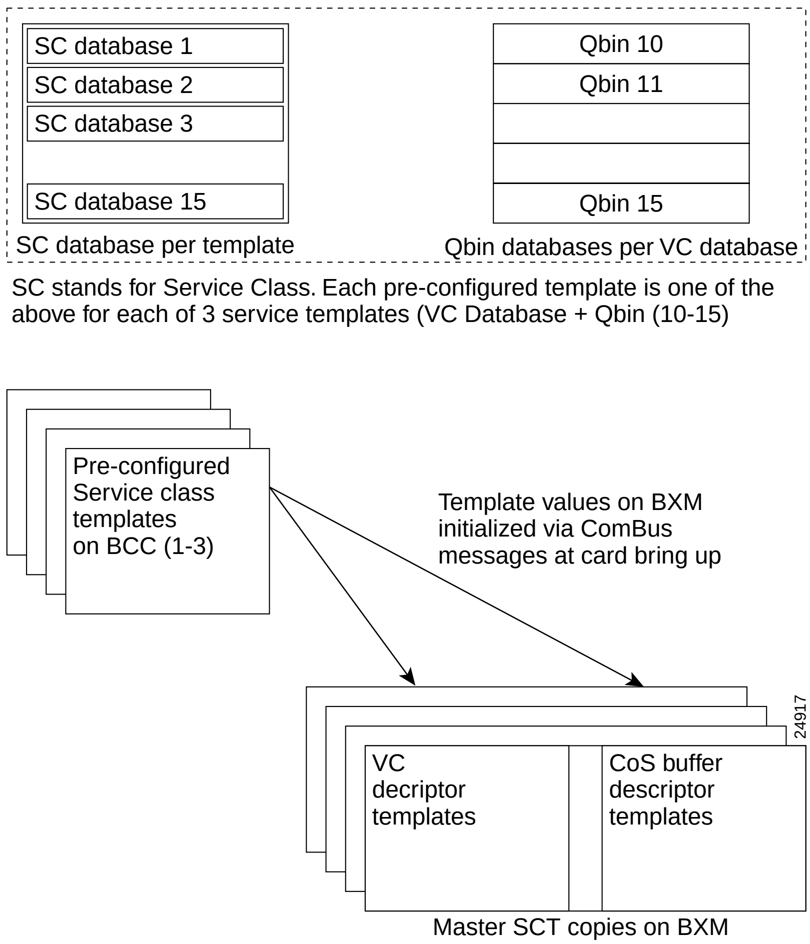
When a connection setup request is received from the VSI master in the Label Switch Controller, the VSI slave (in the BXM, for example) uses the service type identifier to index into a Service Class Template database containing extended parameter settings for connections matching that index. The slave 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 three service types of templates, and the user can assign any one of the templates to a virtual switch interface. (See Figure 11-6.)

Figure 11-6 Service Template Overview



Structure

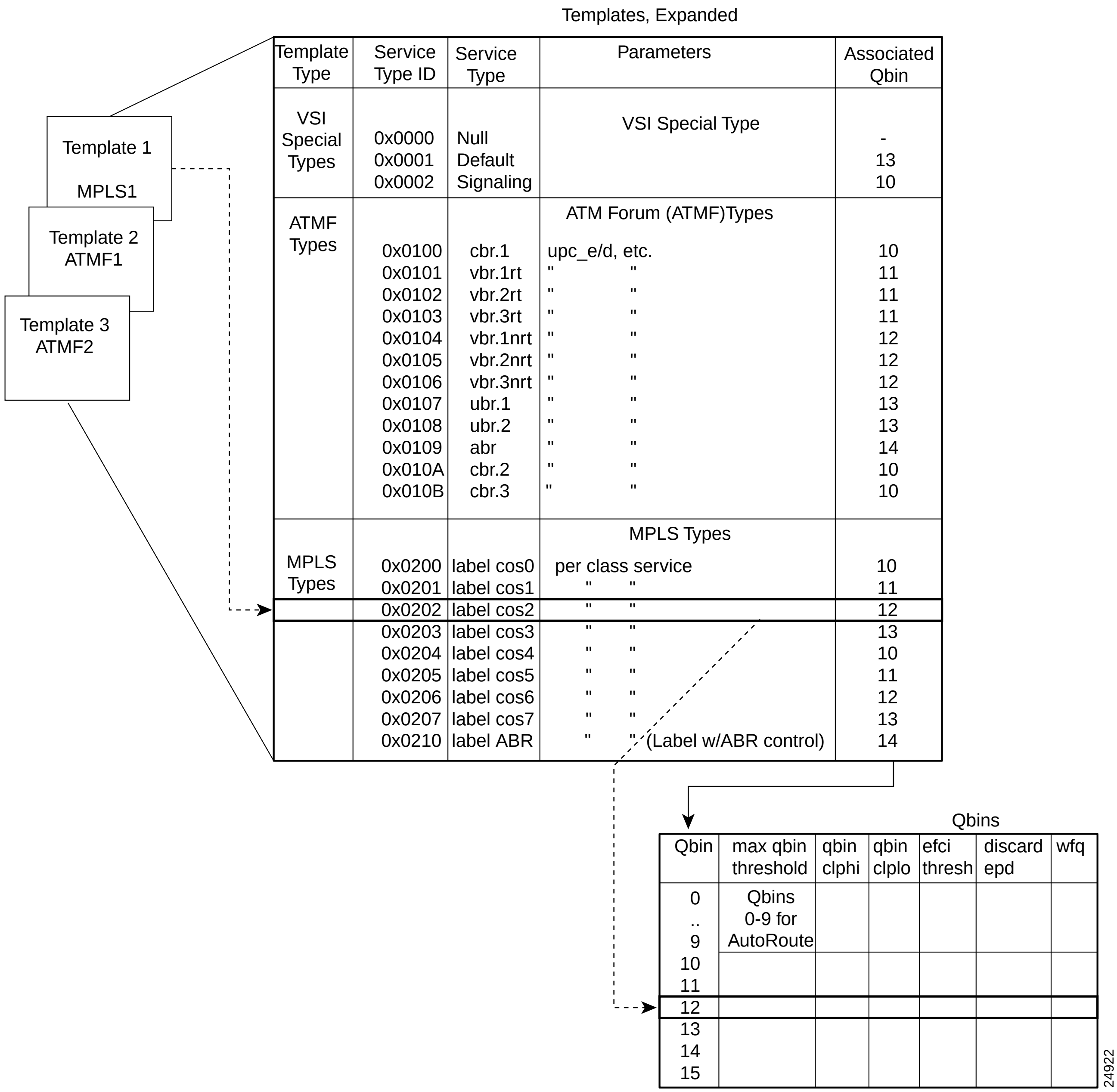
When the **upport** or **uptrk** command is used to activate an interface on the BXM card, the default service template, which is MPLS1, is assigned to the interface. This service template has an indentifier of "1". The service template assigned to an interface can be changed with the **cnfvsiif** command. 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 11-7). 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 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 11-7 Service Template and Associated Qbin Selection



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 11-3. 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 11-3 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

Additional 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

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 connection is granted 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 preassigned ingress service template containing CoS Buffer links is used.

Supported Service Types

The service type identifier is a 32-bit number. In this release, there are three service types: VSI Special Type, ATMF Types, and MPLS types, as shown in Table 11-4.

Table 11-4 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 11-5 through Table 11-8. Table 11-9 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 11-5 lists the parameters associated with Default (0x0001) and Signaling (0x0002) service template categories.

Table 11-5 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 11-6 and Table 11-7 lists the parameters associated with the PNNI service templates.

Table 11-6 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	-	-	-	-	-	167772 15
FRTT	-	-	-	-	-	*

Table 11-7 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 11-8 lists the connection parameters and their default values for label switching service templates.

Table 11-8 MPLS Service Types

Parameter	CoS 0/4	CoS 1/5	CoS 2/6	CoS 3/7	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 11-9 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 listed in Table 11-9 below. For example, a CBR service type have fewer parameters than an ABR service type.

Table 11-9 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
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

Table 11-9 Connection Parameter Descriptions and Ranges (Continued)

Object Name	Range/Values	Template Units
Reduced Format Rate Increase Factor (RRIF)	1 - 15	enumeration
Reduced Format Time Between Fwd RM cells (RTrm)	0 - 7	enumeration
Cut-Off Number of RM Cells (CRM)	1 - 4095	cells

Qbin Default Settings

The qbin default settings are shown in Table 11-10. The Service Class Template default settings for Label Switch Controllers and PNNI controllers are shown in Table 11-11

Note: Templates 2, 4, 6, and 8 add support for policing on PPD.

Table 11-10 Qbin Default Settings

QBIN	Max Qbin Threshold (usec)	CLP High	CLP Low/EPD	EFCI	Discard Selection
LABEL Template 1					
10 (Null, Default, Signalling, Tag0,4)	300,000	100%	95%	100%	EPD
11 (Tag1,5)	300,000	100%	95%	100%	EPD
12 (Tag2,6)	300,000	100%	95%	100%	EPD
13 (Tag3,7)	300,000	100%	95%	100%	EPD
14 (Tag Abr)	300,000	100%	95%	6%	EPD
15 (Tag unused)	300,000	100%	95%	100%	EPD
PNNI Templates 2 (with policing) and 3					
10 (Null, Default, CBR)	4200	80%	60%	100%	CLP
11 (VbrRt)	53000	80%	60%	100%	EPD
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Ubr)	105000	80%	60%	100%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Unused)	105000	80%	60%	100%	EPD
Full Support for ATMF and reduced support for Tag CoS without Tag-Abr Templates 4 (with policing) and 5					
10 (Tag 0,4,1,5, Default, UBR, Tag-Abr*)	300,000	100%	95%	100%	EPD
11 (VbrRt)	53000	80%	60%	100%	EPD
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Tag 2,6,3,7)	300,000	100%	95%	100%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Cbr)	4200	80%	60%	100%	CLP
Full Support for Tag ABR and ATMF without Tag CoS Templates 6 (with policing) and 7					
10 (Tag 0,4,1,5,2,6,3,7 Default, UBR)	300,000	100%	95%	100%	EPD
11 (VbrRt)	53000	80%	60%	100%	EPD

Table 11-10 Qbin Default Settings

QBIN	Max Qbin Threshold (usec)	CLP High	CLP Low/EPD	EFCI	Discard Selection
12 (VbrNrt)	53000	80%	60%	100%	EPD
13 (Tag-Abr)	300,000	100%	95%	6%	EPD
14 (Abr)	105000	80%	60%	20%	EPD
15 (Cbr)	4200	80%	60%	100%	CLP
Full Support for Tag CoS and reduced support for ATMF Templates 8 (with policing) and 9					
10 (Cbr, Vbr-rt)	4200	80%	60%	100%	CLP
11 (Vbr-nrt, Abr)	53000	80%	60%	20%	EPD
12 (Ubr, Tag 0,4)	300,000	100%	95%	100%	EPD
13 (Tag 1, 5, Tag-Abr)	300,000	100%	95%	6%	EPD
14 (Tag 2,6)	300,000	100%	95%	100%	EPD
15 (Tag 3, 7)	300,000	100%	95%	100%	EPD

Table 11-11 Service Class Template Default Settiings

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
MCR	Tag0-7: N/A TagAbr: 0% of PCR	Abr: 0%
AAL5 Frame Base Traffic Control (Discard Selection)	EPD	Hystersis
CDVT(0+1)	250,000	250,000
VSVD	Tag0-7: N/A TagAbr: None	Abr: None
SCR	Tag0-7: N/A TagAbr: 0	Vbr: 100% Abr: 0
MBS	Tag0-7: N/A TagAbr: 0	Vbr: 1000

Table 11-11 Service Class Template Default Settiings

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
Policing	Policing Disable	VbrRt1: GCRA_1_2, CLP01_CLP01, DISCARD on both policing action VbrRt2: GCRA_1_2, CLP01_CLP0, DISCARD on both policing action VbrRt3: GCRA_1_2, CLP01_CLP0, CLP DISCARD for 1st policier and CLP for 2nd policier VbrNRt1: same as VbrRt1 VbrNRt2: same as VbrRt2 VbrNRt3: same as VbrRt3 Ubr1: GCRA_1 CLP01, Discard Ubr2: GCRA_1_2 CLP01 DISCARD on policer 1. CLP01 TAG on policer 2 Abr: same as ubr1 Cbr1: same as ubr1 Cbr2: GCRA_1_2 CLP01_CLP0, Discard on both policing action Cbr3: GCRA_1_2 CLP01_CLP0, CLP UNTAG for policier 1 and CLP for policier 2
ICR	Tag0-7: N/A TagAbr: NCR	Abr: 0%
ADTF	Tag0-7: N/A TagAbr: 500 msec	Abr: 1000 msec (ATM forum it’s 500)
Trm	Tag0-7: N/A TagAbr: 0	Abr: 100

Table 11-11 Service Class Template Default Settiings

PARAMETER WITH DEFAULT SETTING	LABEL	PNNI
VC Qdepth	61440	10,000 160 - cbr 1280 - vbr
CLP Hi	100	80
CLP Lo / EPD	40	35
EFCI	TagABR: 20	20 (not valid for non-ABR)
RIF	Tag0-7: N/A TagAbr: 16	Abr: 16
RDF	Tag0-7: N/A TagAbr: 16	Abr: 16
Nrm	Tag0-7: N/A TagAbr: 32	Abr: 32
FRTT	Tag0-7: N/A TagAbr: 0	Abr: 0
TBE	Tag0-7: N/A TagAbr: 16,777,215	Abr: 16,777,215
IBS	N/A	N/A
CAC Treatment	LCN	vbr: CAC4 Ubr:LCN Abr: MIN BW Cbr: CAC4
Scaling Class	UBR - Scaled 1st	Vbr: VBR -Scaled 3rd Ubr: UBR - Scaled 1st Abr: ABR - Scaled 2nd Cbr: CBR - Scaled 4th
CDF	16	16

CHAPTER 12

BME Multicasting

This chapter contains an overview of multicasting and a description of the BME card used on the BPX switch for multicasting for PVCs.

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, such as, 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 port1 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 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

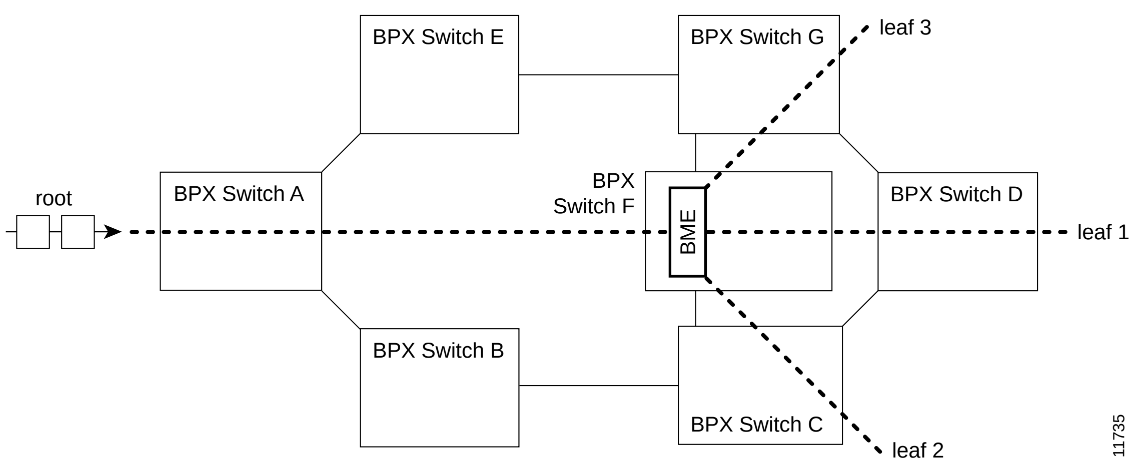
Cables are connected between port 1 and port 2 of the backcard, transmit to receive and receive to transmit.

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 12-1 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.

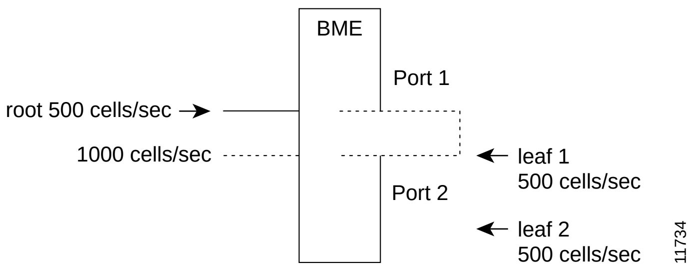
Figure 12-1 Replication of a Root Connection into Three Leaves



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 12-2.

Figure 12-2 Example of Traffic, OneRoot andTwo Leaves

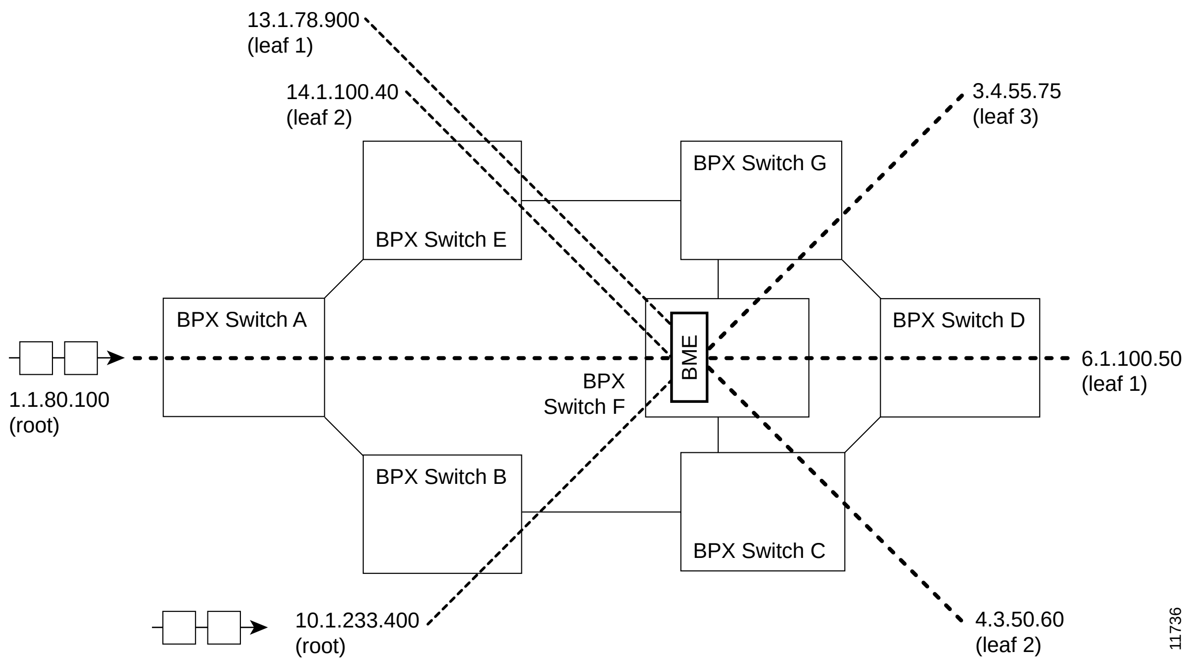


Adding Connections

Figure 12-3 shows two multicasting groups. 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 * * *

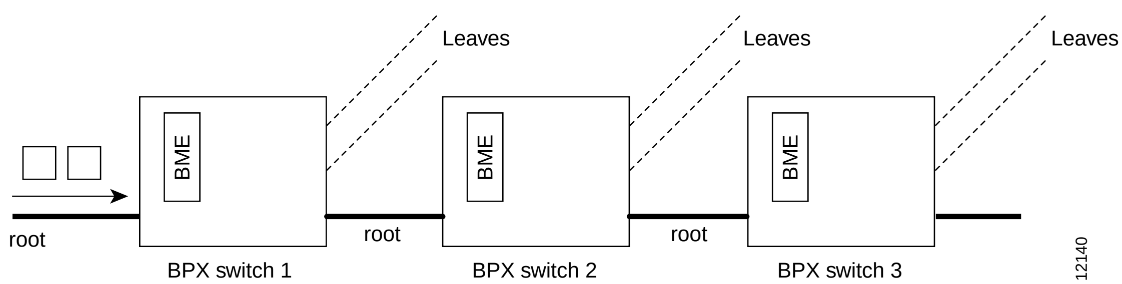
Figure 12-3 Adding Multicasting Connections



Multi-Segment Multicast Connections

Figure 12-4 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 12-4 Multi-Segment Multicast Connections



Multicast Statistics

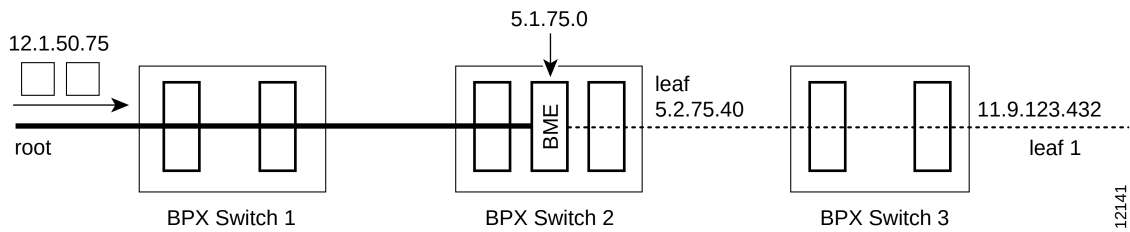
Channel statistics are available for leaf connections on the BME end. However, channel statistics are not available for the root connection on the BME end.

For the example in Figure 12-5:

- **dspchstats** 12.1.50.75 on BPX switch 1 (available)
- **dspchstats** 5.1.75.0 on BPX switch 2 (not available)

- **dspchstats** 5.2.75.40 on BPX switch 2 (available)
- **dspchstats** 11.9.123.432 on BPX switch 3 (available)

Figure 12-5 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.

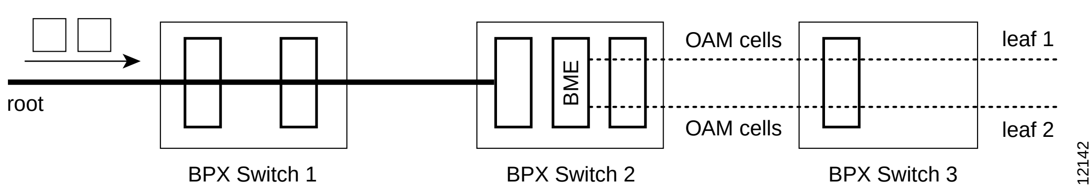
No policing functionality is available on the root connection on the BME end.

Alarms

OAM cells

OAM cells coming into the root are multicast into the leaves along with data, as shown in Figure 12-6.

Figure 12-6 OAM Cells

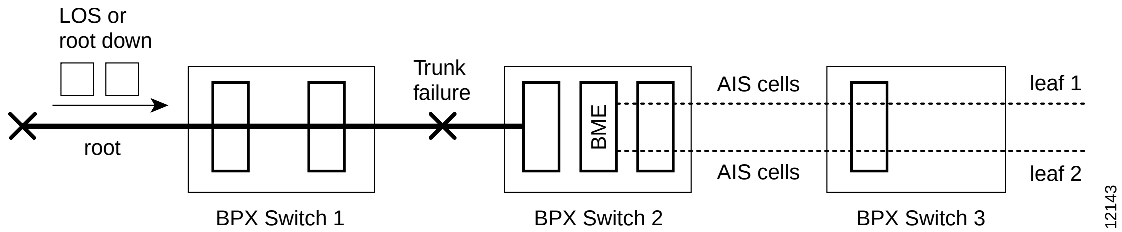


AIS cells

AIS cells are automatically generated on the leaves, as shown in Figure 12-7, 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 12-7 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.

Qbin example using **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 tsdelay 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 Manual*

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.

CHAPTER 13

Frame Relay to ATM Network and Service Interworking

This chapter describes Frame Relay to ATM interworking. Frame Relay to ATM Interworking allows users to retain their existing Frame Relay services, and as their needs expand, migrate to the higher bandwidth capabilities provided by BPX switch ATM networks.

This chapter contains the following:

- Service Interworking
- Networking Interworking
- ATM Protocol Stack
- AIT/BTM Interworking and the ATM Protocol Stack
- AIT/BTM Control Mapping, Frames and Cells
- Management, OAM Cells
- Functional Description
- Management

Frame Relay to ATM Interworking enables frame relay traffic to be connected across high-speed ATM trunks using ATM standard Network and Service Interworking (see Figure 13-1 and Figure 13-2).

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. See Figure 13-3 for some examples of ATM to Frame Relay Interworking.

Figure 13-1 Frame Relay to ATM Network Interworking

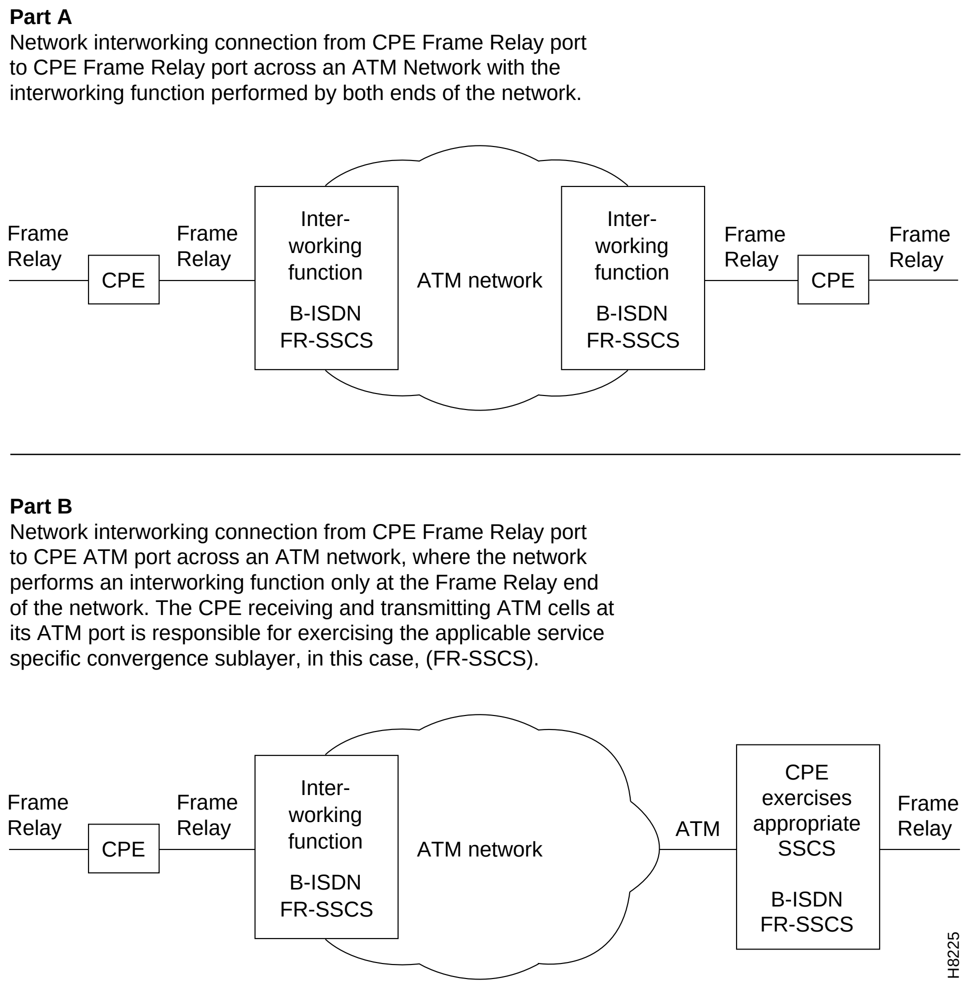


Figure 13-2 Frame Relay to ATM Service Interworking

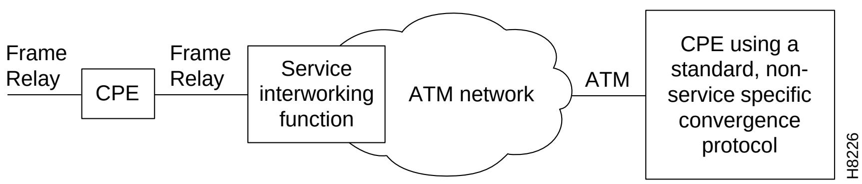
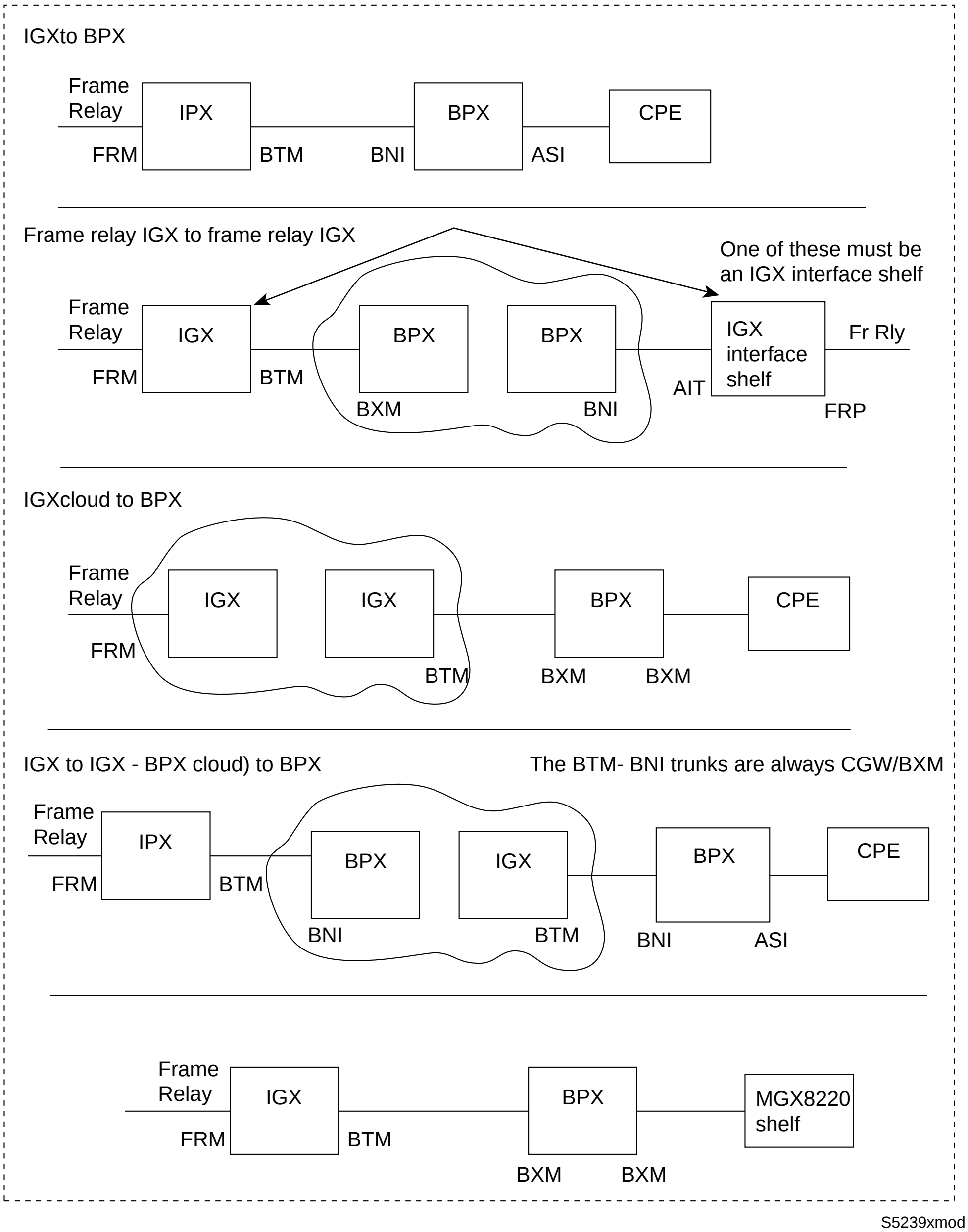


Figure 13-3 Frame Relay to ATM Interworking Examples with BTM Card on IGX Switch



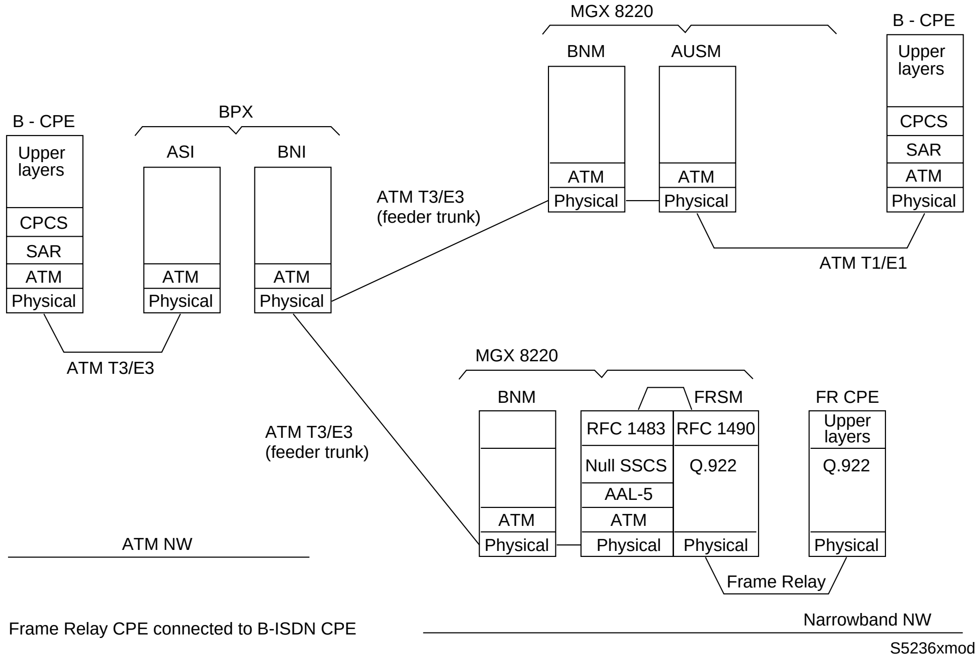
BTM Interworking Examples

Service Interworking

In Service Interworking, for example, for a connection between an ATM port and a frame relay port, unlike Network Interworking, the ATM device does not need to be aware that it is connected to an interworking function. The ATM device uses a standard service specific convergence sublayer, instead of using the Frame Relay FR-SSCS (see Figure 13-4).

The frame relay service user does not implement any ATM specific procedures, and the ATM service user does not need to provide any frame relay specific functions. All translational (mapping functions) are performed by the intermediate IWF. The ATM endpoints may be any ATM UNI/NNI interface supported by the MGX 8220, e.g., BXM, ASI, AUSM. Translation between the Frame Relay and ATM protocols is performed in accordance with RFC 1490 and RFC 1483.

Figure 13-4 Frame Relay to ATM Service Interworking Detail

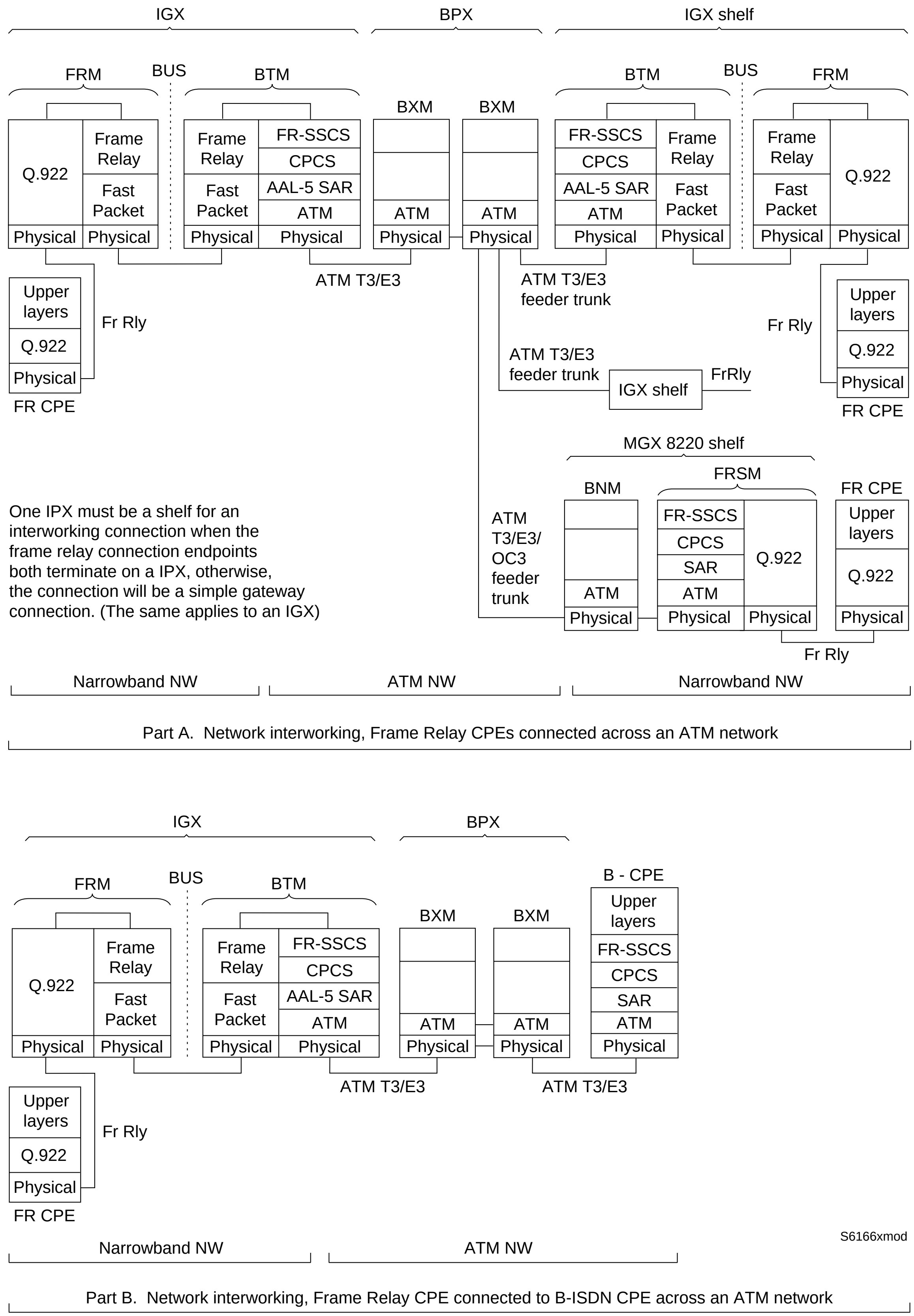


Networking Interworking

In Network Interworking, in most cases, the source and destination ports are frame relay ports, and the interworking function is performed at both ends of the connection as shown in Part A of Figure 13-5.

If a frame relay port is connected across an ATM network to an ATM device, network interworking requires that the ATM device recognize that it is connected to an interworking function (frame relay, in this case). The ATM device must then exercise the appropriate service specific convergence sublayer (SSCS), in this case the frame relay service specific convergence sublayer (FR-SSCS) as shown in Part B of Figure 13-5.

Figure 13-5 Frame Relay to ATM NW Interworking Detail

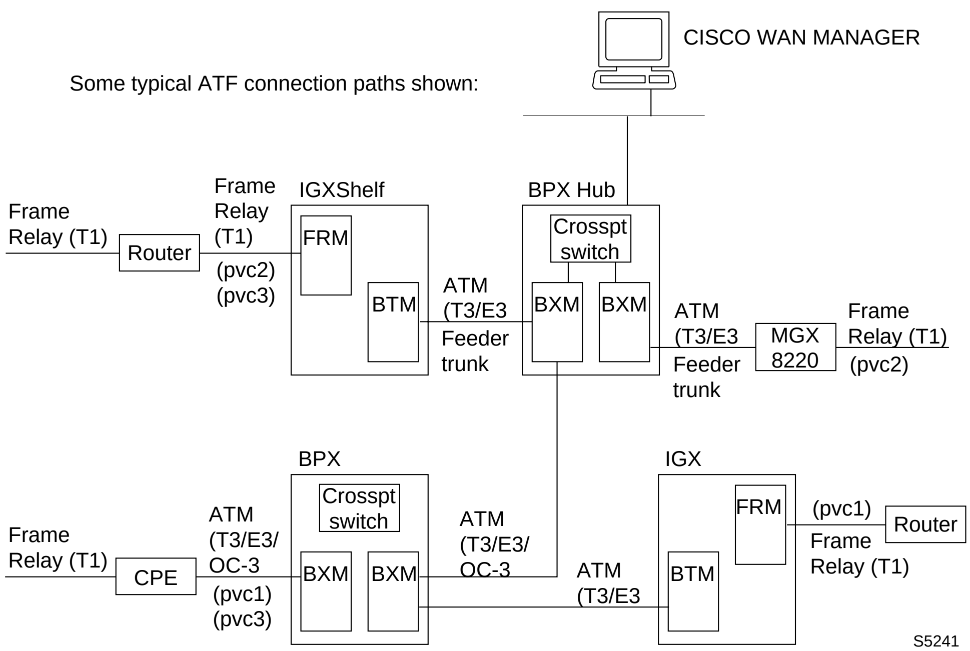


The frame relay to ATM networking interworking function is available as follows:

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

On the IGX switch, interworking is performed by the BTM card. A simplified example of the connection paths is shown in Figure 13-6. In interworking, the BTM card receives FastPackets from the FRM, rebuilds the frames, and converts between frames and ATM cells. Data is removed from one package and placed in the other. Congestion information from the header is mapped to the new package. This processing by the BTM trunk card is called Complex Gateway. BTM trunk cards are required on every BPX switch to IGX switch hop in a Frame Relay to ATM connection's path.

Figure 13-6 ATF Connections, Simplified Example



The cells within the frame are expected to possess the standard ATM Access Interface cell header. The traffic is assumed to have AAL-5 PDUs, and will not function properly otherwise (framing errors will result). Within the AAL-5 PDUs, the data must be packaged in standard frame relay frames, one frame per PDU (with respect to the AAL-5 layer).

The UPC and ForeSight algorithms are applied according to their configured values. The cell headers are converted into the proprietary Cisco WAN switching STI format before entering the network. The cells are delivered to their destination according to the configured route of the connection. Cells can be lost due to congestion.

Discard selection is based upon the standard CLP bit in the cells. When the routing path enters an IGX switch, a BTM card which supports Interworking traffic is required to convert the connection data from cells to frames (frames to fastpackets out onto MuxBus to FRP/cell bus to FRM), and visa versa. Additionally, the AAL-5 framing is removed upon conversion to frames, and added upon conversion to cells. At the destination (FRM), FastPackets are placed in the port queue and, when a complete frame has been assembled, the frame is played out the remote port in the original format (as provided in the frames delivered inside AAL-5 PDUs).

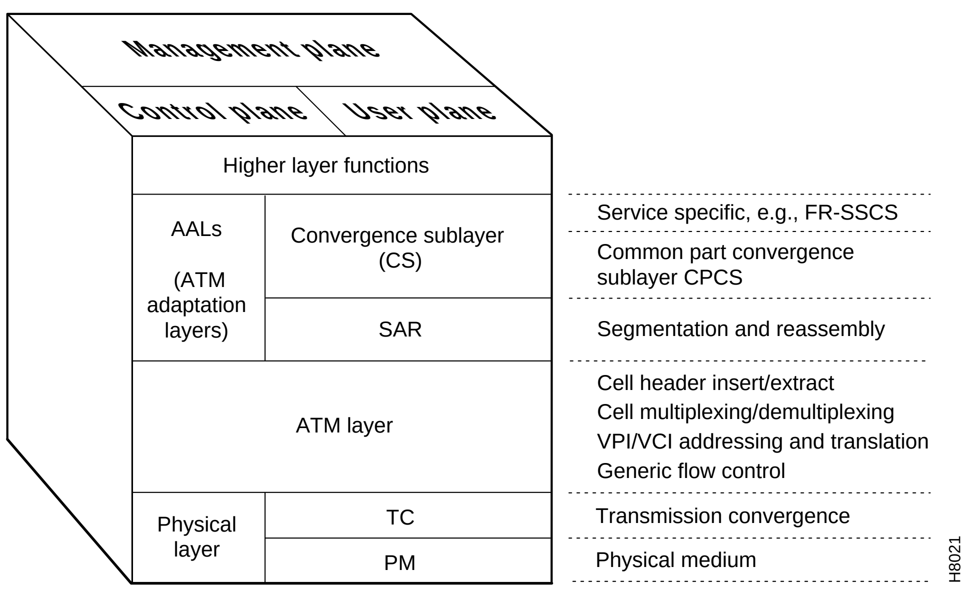
For each connection, only a single dlci can be played out for all traffic exiting the port, and is inserted into the frame headers. The standard LAPD framing format is played out the port on the FRM.

At the FRM card, several additional protocol mappings take place. First, the Interworking Unit acts as a pseudo endpoint for the purposes of ATM for all constructs which have no direct mapping into Frame Relay, such as loopbacks and FERF indications. Thus, end-to-end loopback OAM cells which ingress to FRM cards from the network are returned to the ATM network without allowing them to proceed into the Frame Relay network, which has no equivalent message construct. Further, AIS and supervisory cells and FastPackets (from the Frame Relay direction) are converted into their counterparts within the other network.

ATM Protocol Stack

A general view of the ATM protocol layers with respect to the Open Systems Interconnection model is shown in Figure 13-7. In this example, a large frame might be input into the top of the stacks. Each layer performs a specific function before passing it to the layer below. A protocol data unit (PDU) is the name of the data passed down from one layer to another and is the Service Data Unit (SDU) of the layer below it. For Frame Relay to ATM interworking, a specific convergent sublayer, Frame Relay Service Specific Convergent Sublayer, FR-SSCS is defined. This is also referred to as FR-CS, in shortened notation.

Figure 13-7 ATM Layers



BTM Interworking and the ATM Protocol Stack

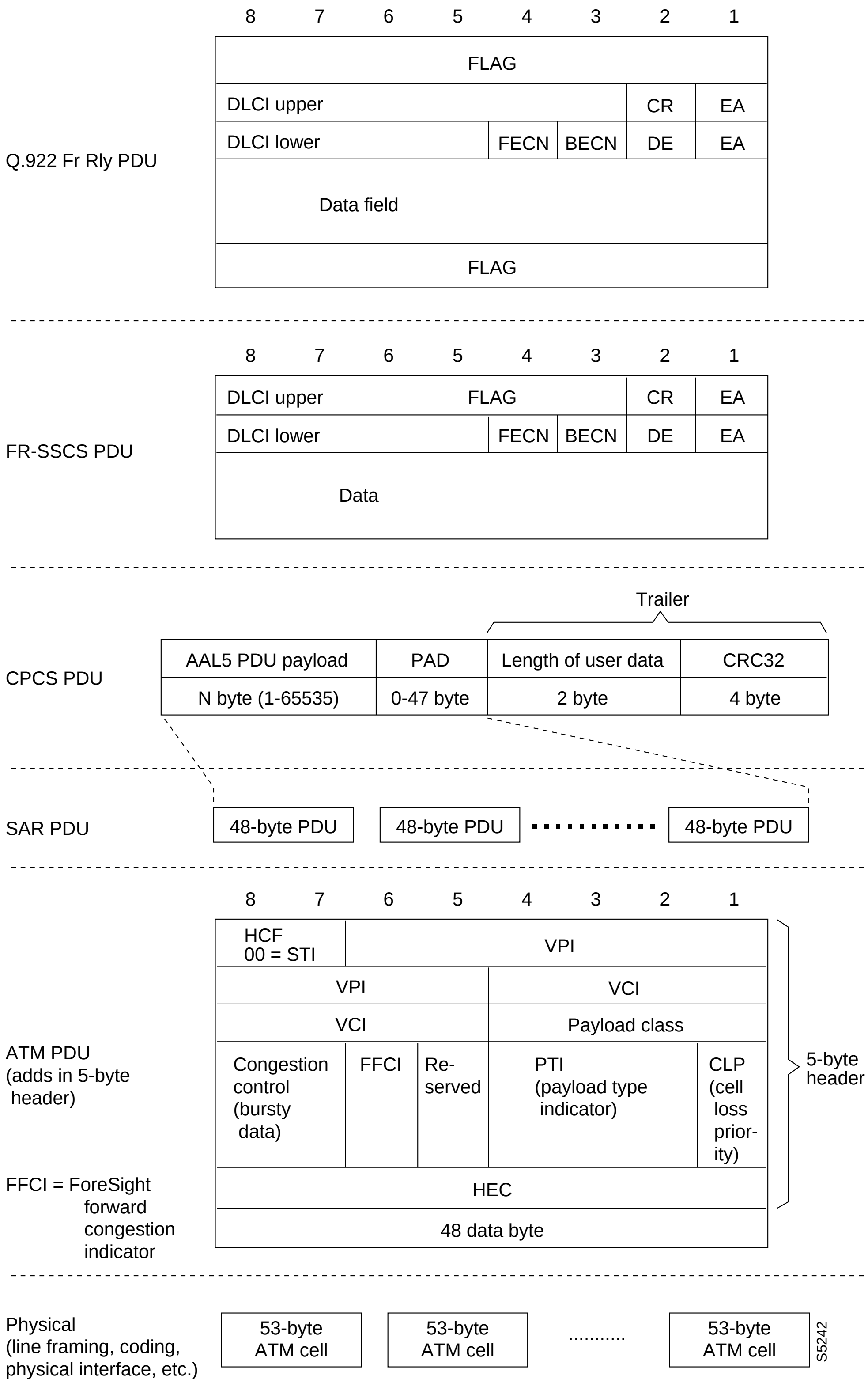
ATM to Frame Relay interworking (ATF) performs various tasks including the following:

- Conversion of PDUs between the frame relay and ATM virtual circuits of the frame relay and ATM user devices.
- Conversion between frame relay traffic service and ATM quality of service parameters.
- Mapping of management status, including connection, port, line, and trunk status and events.

Figure 13-8 depicts the function of the protocol stack layers in the interworking between ATM and Frame Relay PDUs. Interworking by the BTM card in the IGX switch includes the following functions:

- Translating the ATM pvc identifier (vpi.vci) to the frame relay pvc identifier (dlci) and vice versa.
- Mapping the Protocol Data Unit (PDU), which is essentially the data, between the Frame Relay Service Specific Convergence Sublayer (FR-SSCS) and the Frame Relay Q.922 core protocol, and vice versa.
- On the IGX switch, Incoming Frames are converted to FastPackets by the FRM card. The FastPackets are then routed to the FRM card via the IGX switch bus and converted back into Frame Relay Q.922 frames by the BTM card. The BTM card interworking function executes four layers to convert the Frame PDU to ATM cells:
    - FRCS layer (Frame Relay Service Specific Convergence Sublayer, FRSSCS, or FRCS for in shortened notation) which uses a PDU format identical to the Q.922 core (without CRC-16 or flags).
    - CPCS layer (Common Part Convergence Sublayer) which appends a CS-PDU trailer to the FR-PDU to create a CS-PDU.
    - Segmentation and Reassembly layer (SAR) which segments the CS-PDU (Protocol Data Unit) into SAR-PDUs (48 byte data entities).
    - ATM layer which attaches an ATM header to each SAR-PDU to create an ATM-SDU (Service Data Unit). The same process is performed in the reverse order by the AIT card when transforming cells to frames.

Figure 13-8 Protocol Stack Operation



BTM Control Mapping, Frames and Cells

In addition to performing DLCI to PVC/VCC conversion, the network interworking feature provided by the BTM in the IGX switch maps cell loss priority, congestion information, and management information between frame relay and ATM formats as follows:

CELL LOSS PRIORITY, Frame Relay to ATM Direction

Each frame relay to ATM network interworking connection can be configured as one of the following DE to CLP mapping choices:

- The DE bit in the frame relay frame is mapped to the CLP bit of every ATM cell generated by the segmentation process.

The following 2 choices are not available on IGX switch NIW (network interworking):

- CLP is always 0.
- CLP is always 1.

CELL LOSS PRIORITY, ATM to Frame Relay Direction

Each frame relay to ATM network interworking connection can be configured as one of the following CLP to DE mapping choices:

- If one or more ATM cells belonging to a frame has its CLP field set, the DE field of the frame relay frame will be set.

The following choice is not available:

- Choosing no mapping from CLP to DE.

CONGESTION INDICATION, Frame Relay to ATM direction

- EFCI is always set to 0.

CONGESTION INDICATION, ATM to Frame Relay Direction

- If the EFCI field in the last ATM cell of a segmented frame is set, then FECN of the frame relay frame will be set.

For PVC Status Management

The AIT/BTM does convert OAM cells to OAM fastpackets, and vice-versa, including the AIS OAM. Also, “Abit” status is now propagated via software messaging.

The ATM layer and frame relay PVC Status Management can operate independently. The PVC status from the ATM layer will be used when determining the status of the FR PVCs. However, no direct actions of mapping LMI Abit to OAM AIS will be performed.

Management, OAM Cells

OAM cell processing:

- F5 OAM loopback
- AIS
- FERF
- Cisco WAN switching Internal OAM

Functional Description

ATF Summary

Features

- Interworking: ATM to Frame Relay connections
- Connection Statistics
- Round Trip Delay measurements incorporated into the ForeSight algorithm
- Frame Based GCRA (FGCRA). This is an enhancement of the Generic Cell Rate Algorithm
- IBS (Initial Burst Size)
- cnfportq: 3 egress port queues are configurable CBR, VBR and VBR w/Foresight. (Queue Bin numbers and algorithm types are NOT user selectable.)
- BCM (Backward Congestion Messages)
- ILMI and associated configuration options and statistics
- Loopback functions: **tstdly**, **tstconseg**, **addrmtlp**, **addloclp**
- Selftest/ Background tests
- OAM flows: AIS, FERF, OAM loopback
- ASI/2 E3 support
- End-to-end status updates (per FR/ATM interworking)
- Annex G and associated configuration options and statistics
- ASI-1 as a clock source is supported.

Limitations

- Priority Bumping is not supported across the interface shelves, but is supported across the routing network.
- Statistical Line Alarms per Software Functional Specification (that is, Bellcore standards).
- Programmable Opti Class: although 4 connection classes are supported: CBR, VBR, VBR with Foresight, ATF, and ATF with ForeSight. Configuration of egress port queues and BNI trunk queues for these connection classes is available.
- Port loopback **tstport**

- Test **tstcon** not supported at BPX switch endpoints; it is supported at IPX switch endpoints
- Gateway terminated inter-domain connections
- Via connections through IPX switch

Some ATF Connection Criteria

ATF connections are allowed between any combination of ATM and Frame Relay UNI and NNI ports. Virtual circuit connections are allowed. Virtual path connections are not.

ATF connections can be mastered by the IGX switch or BPX switch end.

ATF bundled connections and ATF point-to-point connections are not supported.

ATF connections use the frame relay trunk queues: bursty data A for non-ForeSight, bursty data B for ForeSight.

Bandwidth related parameters are defined using cells per second (cps) on the BPX switch and bits per second (bps) on the IGX switch. On a given endpoint node, the bandwidth parms for both ends of the ATF connection are changed/displayed using this end's units. This saves the user from having to convert from cps to bps repeatedly.

ATF connections use the VBR egress queue on the ASI-1 card. ATF with ForeSight connections use the ABR egress queue.

Connection Management

The following user commands are used to provision and modify ATF connections:

- **addcon**
- **cnfcls**
- **cnfcon**
- **delcon**
- **dspcls**
- **dspcon**
- **dspcons**

Port Management

The following features are added to the ASI-1 at the port level:

- An ASI-1 card can be configured to use the network-network interface (NNI) addressing format. This feature is only available on a per-card level. Changing one port to or from NNI changes the other one with appropriate warnings to the user.
- ILMI activation/configuration/statistics
- LMI Annex G activation/configuration/statistics
- Port egress queue configuration
- Backward congestion management

Structure

- NNI

The NNI format supports a 12-bit VPI. Abit status changes are passed to the remote end of the connection.

- ILMI

The ILMI MIB and protocol was implemented in release 7.2. The additional support in consists of an activation and configuration interface, collection of statistics, and end-to-end status updates.

- LMI Annex G

The LMI Annex G protocol was implemented in release 7.2. The additional support consists of an activation and configuration interface, collection of statistics, and end-to-end status updates.

- Port egress queue configuration

Each of the pre-defined ASI-1 port egress queues can be configured by the user. These queues consist of CBR, VBR, and VBR with ForeSight (ABR). The configurable parameters are queue depth, EFCN threshold, and CLP thresholds.

- Backward congestion management

Backward congestion management cells indicate congestion across the UNI or NNI. Transmission of these cells is enabled on a per-port basis. Software allows BCM to be configured on a UNI or NNI port for maximum flexibility should BCM over UNI be standards-defined.

The following user commands are used to configure ASI-1 port features:

- **cnfport**
- **cnfportq**

Channel Statistics

Statistics are supported on a per-channel basis. A range of traffic and error statistics are available. ASI-1 channel statistics are enabled by StrataView+ or by the BPX switch control terminal using the existing statistics mechanism. The existing collection intervals apply.

Channel statistics of the following general types are supported:

- Cells received/transmitted, dropped, tagged as non-compliant or congested
- Cell errors
- AAL-5 frame counts, errors

The following user commands are used to configure and display channel statistics:

- **clrchstats**
- **cnfchstats**
- **dspchstats**
- **dspchstatcnf**
- **dspchstathist**

OAM Cell Support

OAM cells are detected and transmitted by the ASI-1 firmware. System software displays alarm indications detected by the firmware. Additionally, loopbacks between the ATM-UNI and the ATM-CPE can be established. ForeSight round-trip delay cells are generated by firmware upon software request.

System software deals with the following OAM cell flows:

- End-to-End AIS/FERF—software displays on a per-connection basis.
- External segment loopbacks—software initiates loopback of ATM-CPE via user command. The SAR creates the loopback OAM cell. External loopback cells received from the ATM-CPE are processed by the SAR.
- Internal ForeSight round trip delay—software commands the ASI-1 to measure the RTD excluding trunk queueing delay on each ForeSight connection. Software displays the result.
- Internal loopback round trip delay—software commands the ASI-1 to measure the RTD including trunk queueing delay on each ForeSight connection. Software displays the result.
- Internal Remote Endpoint Status—these cells are generated by one end of a connection due to remote network connection failure (Abit = 0). The other end ASI-1 detects these cells and reports the connection status to software, which displays it.

The following user commands are associated with OAM cell status changes:

- **dspalms**
- **dspcon**
- **dspport**
- **tstconseg**
- **tstdly**

Diagnostics

Loopbacks

- Local loopbacks loop data back to the local ATM-TE, via the local BPX switch. Remote loopbacks loop data back to the local ATM-TE, via the whole connection route up to and including the remote terminating card.
- Local and remote connection loopbacks, and local port loopbacks, are destructive.

Card Tests

- The generic card selftest mechanism on the BPX switch is modified to include the ASI-1 card.

Connection Tests

- The tstcon command is not supported. The tstdly command is used for connection continuity testing. ASI-1 tstdly is non-destructive, as compared with the IPX switch tstdly.

User Commands

The following user commands are associated with diagnostics changes:

- **addloclp**
- **addrmtlp**

- **cnftstparm**
- **dellp**
- **dspalms**
- **dspcd**
- **dspcds**
- **tstdly**

Virtual Circuit Features

The following virtual circuit features are supported by the ASI-1:

- Connection Groups

  Connection groups are supported for ASI-1 and BXM ATM Band interworking connection types, allowing termination of up to 5000 (grouped) virtual circuits per BPX switch. The connection grouping feature currently available on frame relay connections is expanded to include ASI-1 and BXM ATM and interworking connections.

- FGCRA

  Frame-Based Generic Cell Rate Algorithm is an ASI-1 firmware feature that controls admission of cells to the network. It is configurable on a per-connection basis. It is a Cisco WAN switching enhancement of the ATM-UNI standard Generic Cell Rate Algorithm. System software allows configuration of FGCRA on a per-connection basis.

- IBS

  Initial Burst Size is an ATM bandwidth parameter that is used by firmware to allow short initial bursts, similar to the Cmax mechanism on the IGX switch. It is configurable on a per-connection basis

- Full VPI/VCI addressing range

  The entire range of VPI and VCI on both UNI and NNI interfaces is supported. For ATM-UNI, 8 bits of VPI and 16 bits of VCI are supported. For ATM-NNI, 12 bits of VPI and 16 bits of VCI are supported. In either case, VPC connections only pass through the lower 12 bits of the VCI field.

- Connection Classes

  ATM and interworking connection classes are defined with appropriate bandwidth parameter defaults. These classes only apply at addcon time. They are templates to ease the user’s task of configuring the large number of bandwidth parameters that exist per connection.

User Commands

The following user commands are associated with virtual circuit feature changes:

- **addcon**
- **addcongrp**
- **cnfcon**
- **cnfatmcls**
- **delcon**
- **delcongrp**

- **dspatmcls**
- **dspcongrps**
- **grpcon**

AUser Commands

The following user commands are modified to support ASI-1 E3:

- **cnfln**
- **cnflnstats**
- **dspcd**
- **dspcds**
- **dsplncnf**
- **dsplns**
- **dsplnstatcnf**
- **dsplnstathist**
- **dspyred**
- **prtyred**

Management

Connection Management

Interworking connections may be added from either the BPX switch, the IGX switch, or the MGX 8220. Intra- and inter-domain interworking connections are supported.

Connection configuration parameters are endpoint-specific. Thus, the ATM-only parameters are only configurable on the BPX switch end. The IGX switch does not know about these parameters, so they cannot be configured or displayed at the IGX switch end. Parameter units are endpoint-specific also. Units on the BPX switch are cells per second, units on the IGX switch are bits per second.

Bundled interworking connections are not supported.

Virtual path interworking connections are not supported.

Routing

Interworking connections use the complex gateway feature of the AIT trunk card to repackage data from frames to ATM cells, and vice-versa. All BPX switch-IGX switch hops these connections route over must provide the complex gateway function. IGX switch-IGX switch hops (frame relay connections) can be any trunk card type. This requirement simplifies the routing mechanism when dealing with structured networks, as software does not know the type of trunks in remote domains.

Bandwidth Management

Bandwidth calculations for interworking connections assume a large frame size, which minimizes the loading inefficiency of packets vs. cells. In other words, the translation between packets and cells assumes 100 percent efficiency, so the conversion is simply based on 20 payload bytes per fastpacket vs. 48 payload bytes per ATM cell.

This mechanism keeps the fastpacket/cell conversion consistent with the bits per second/cells per second conversion. Thus, conversion of endpoint rates to trunk loading is straightforward.

User Interface

ATM connection classes are added for convenience. Classes can be configured as interworking or regular ATM. The **cnfcls** command is used to configure a class. The class is specified as part of the **addcon** command. ATM connection classes are maintained on all BPX switch. IPX switch nodes do not know about these classes.

A special ATM class is defined as the default interworking class. When an interworking connection is added from the frame relay end, the ATM-only parameters for this connection are taken from this default class.

Network-wide ForeSight parameters are supported for the frame relay end of interworking connections. The **cnffstparm** command is used to configure these parameters. Since the ATM end of interworking connections has per-virtual circuit ForeSight parameter configurability, the network-wide ForeSight parameters do not apply.

Note that the default ATM ForeSight parameters will match the default frame relay ForeSight parameters, with appropriate units conversion.

Port Management

The **cnfport** command supports the following new features:

- An ASI-1 card can be configured to be UNI or NNI.
- An ASI-1 UNI or NNI port can be configured to transmit Backwards Congestion Messages (BCM) to indicate congestion to the foreign ATM network.
- An ASI-1 UNI or NNI port can be configured for LMI, ILMI or no local management.

The **cnfportq** command supports configuration of queue depth, EFCN threshold, and CLP thresholds for all port egress queues (CBR, VBR, VBR w/ForeSight).

Connection Management

The NNI cell format has 12 bits for the VPI, so **addcon** allows specification of VPI 0-4095 on NNI ports.

Signaling

System software supports the following LMI/ILMI signaling actions:

- Internal network failure: software informs LMI/ILMI to set Abit = 0 for failed connections. Software informs ASI-1 to transmit AIS to port for failed connections.
- Port failure/LMI Comm Failure: software informs remote nodes terminating all affected connections. Remote node BCC informs LMI/ILMI to set Abit = 0, and ASI-1 to transmit AIS.
- LMI A = 0: software polls ILMI agent periodically for Abit status. Status changes are reflected in the 'dspcon' screen.

Alarms

LMI communication failure on an ASI-1 causes declaration of a minor alarm. The **dspport** screen shows the failure, as does the **dspalms** screen.

Abit = 0 on an NNI port causes declaration of a minor alarm. The d**spcon**, **dspcons**, and **dspalms** screens show this failure.

Tiered Networks

This chapter describes the tiered network architecture that supports interface shelves (non-routing nodes) connected to an IPX/IGX/BPX routing network.

The chapter contains the following:

- Routing Hubs and Interface Shelves
- BPX Routing Hubs in a Tiered Network
- IGX Routing Hubs in a Tiered Network
- User Interface Commands
- Cisco WAN Manager NMS

With Release 8.5, tiered networks now support voice and data connections as well as Frame Relay connections. With this addition, a tiered network can now provide a multi-service capability (Frame Relay, circuit data, voice, and ATM). By allowing CPE connections to connect to a non-routing node (interface shelf), a tiered network is able to grow in size beyond that which would be possible with only routing nodes comprising the network.

Routing Hubs and Interface Shelves

In a tiered network, interface shelves at the access layer (edge) of the network are connected to routing nodes via feeder trunks (Figure 14-1). Those routing nodes with attached interface shelves are referred to as routing hubs. The interface shelves, sometimes referred to as feeders, are non-routing nodes. The routing hubs route the interface shelf connections across the core layer of the network.

The interface shelves do not need to maintain network topology nor connection routing information. This task is left to their routing hubs. This architecture provides an expanded network consisting of a number of non-routing nodes (interface shelves) at the edge of the network that are connected to the network by their routing hubs.

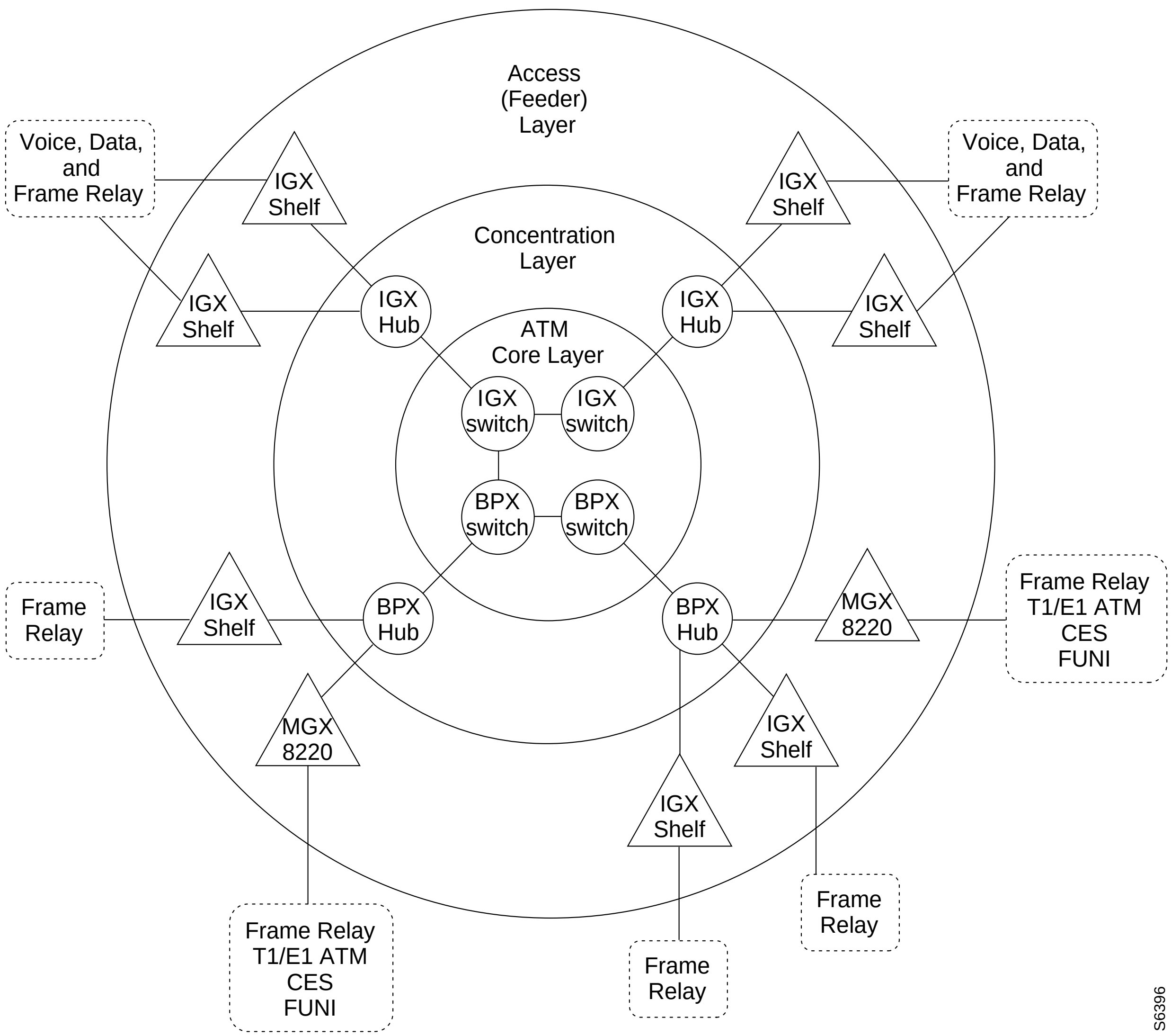
BPX and IGX Routing Hubs

Voice and data connections originating and terminating on IGX interface shelves (feeders) are routed across the routing network via their associated IGX routing hubs. Intermediate routing nodes must be IGX nodes.

Frame relay connections originating at IPX interface shelves and Frame Relay, ATM, CESM, and FUNI connections originating at MGX 8220 interface shelves are routed across the routing network via their associated BPX routing hubs.

Note The IGX switch may also be configured as an interface shelf feeding Frame Relay connections to a BPX routing hub.

Figure 14-1 Tiered Network with BPX and IGX Routing Hubs

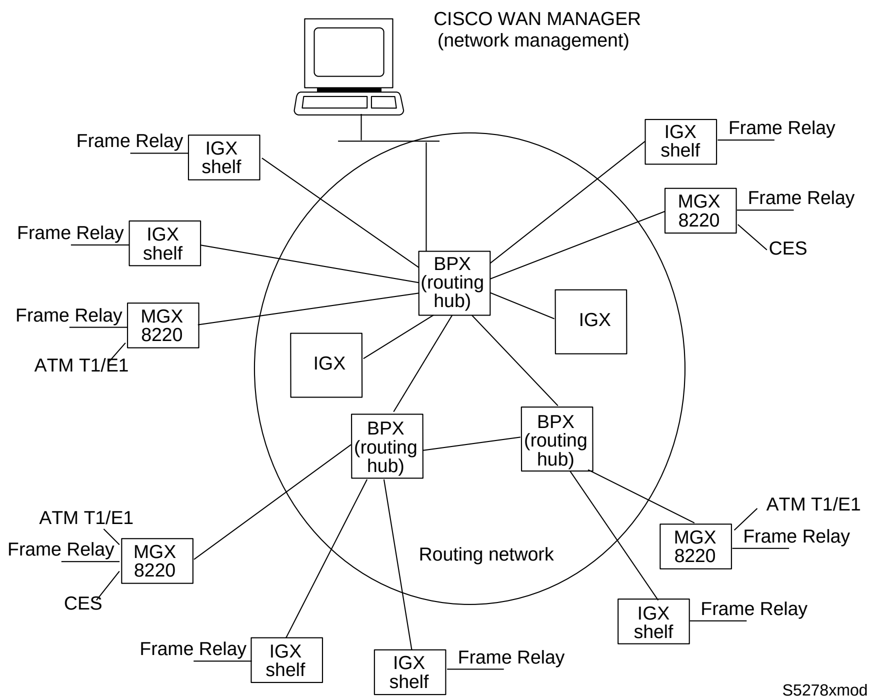


BPX Routing Hubs in a Tiered Network

Tiered networks with BPX routing hubs have the capability of adding interface shelves/feeders (non-routing nodes) to an IPX/IGX/BPX routing network (Figure 14-2). The MGX 8220 interface shelf, and IPX or IGX nodes configured as interface shelves are connected to BPX routing hubs. Interface shelves allow the network to support additional connections without adding additional routing nodes.

The MGX 8220 supports frame T1/E1, X.21 and HSSI Frame Relay, ATM T1/E1, and CES, and is designed to support additional interfaces in the future. The IPX interface shelf supports Frame Relay ports, as does the IGX switch (option is available to configure as an interface shelf).

Figure 14-2 Tiered Network with BPX Routing Hubs



Tiered Network Implementation

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

- MGX 8220 Release 4 level is required on all MGX 8220 interface shelves.
- Only one feeder trunk is supported between a routing hub and interface shelf.
- No direct trunking between interface shelves is supported.
- No routing trunk is supported between the routing network and interface shelves.
- The feeder trunks between BPX hubs and IPX or IGX interface shelves are either T3 or E3.
- The feeder trunks between BPX hubs and MGX 8220 interface shelves are T3, E3, or OC-3-c/STM-1.
- Frame Relay Connection management to an IPX interface shelf is provided by Cisco WAN Manager

- Frame Relay and ATM connection management to an MGX 8220 interface shelf is provide by Cisco WAN Manager
- Telnet is supported to an interface shelf; the vt command is not.
- Remote printing by the interface shelf via a print command from the routing network is not supported.

General

Annex G, a bi-directional protocol, defined in Recommendation Q.2931, is used for monitoring the status of connections across a UNI interface. Tiered Networks use the Annex G protocol to pass connection status information between a Hub Node and attached interface shelf.

Definitions

BPX Routing Hub	A BPX node in the routing network which has attached interface shelves. Also referred to as a hub node or BPX hub.
MGX 8220 Interface Shelf	A standards based service interface shelf that connects to a BPX routing hub, aggregrates and concentrates traffic, and performs ATM adapation for transport over broadband ATM networks.
IPX Interface Shelf	A special configuration of the IPX narrow band node designated as a interface shelf that supports Frame Relay connections.
IGX Interface Shelf	A special configuration of the IGX multiband node designated as a interface shelf that supports Frame Relay connections.
Feeder Trunk	Refers to a trunk which interconnects an interface shelf with the routing network via a BPX routing hub. A feeder trunk is sometimes referred to as an interface shelf trunk.
IPX/AF	Another name for the IPX interface shelf.
IGX/AF	Another name for the IGX interface shelf.
Routing Network	The portion of the tiered network which performs automatic routing between connection endpoints.
VPI	Virtual Path Identifier.
VCI	Virtual Connection Identifier.

Upgrades

Converting an IPX or IGX node to an interface shelf requires re-configuring connections on the node, as no upgrade path is provided in changing a routing node to an interface shelf.

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

Connections within tiered networks consist of distinct segments within each tier. A routing segment traverses the routing network, and an interface shelf segment provides connectivity to the interface shelf end-point. Each of these segments are added, configured and deleted independently of the other segments. The Cisco WAN Manager Connection manager provides management of these individual segments as a single end-to-end connection.

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

All Frame Relay connection types which can terminate on the BPX ASI card are supported on the BNI feeder trunk (currently VBR, CBR, ABR, and ATF types). No check is made by the routing network to validate whether the connection segment type being added to a BNI feeder trunk is actually supported by the attached interface shelf.

Co-locating Routing Hubs and Interface Shelves

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

Network Management

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

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

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

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

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

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

An interface shelf is displayed as a unique icon in the Cisco WAN Manager topology displays. The colors of the icon and connecting trunks indicate the alarm state of each. Channel statistics are supported by FRP, FRM, ASI, and MGX 8220 endpoints. BNIs, AITs, and BTMs do not support channel statistics. Trunk Statistics are supported for the feeder trunk and are identical to the existing BNI trunk statistics.

ForeSight

Foresight for an IPX interface shelf terminated Frame Relay connections is provided end-to-end between Frame Relay ports, regardless as to whether these ports reside on an IPX interface shelf or within the routing network.

Preferred Routing

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

Local and Remote Loopbacks

Connection local and remote loopbacks are managed at the user interface of the FRP endpoint routing node or interface shelf. The existing IPX Frame Relay port loopback feature is supported on the IPX interface shelf. Remote loopbacks are not supported for DAX connections. A new command **addlocrmtlp** is added to support remote loopbacks at FRP DAX endpoints.

Testcon and Testdly

Tstcon is supported at the FRP endpoints in a non-integrated fashion and is limited to a pass/fail loopback test. Fault isolation is not performed. This is the same limitation currently imposed on inter-domain connections. Intermediate endpoints at the AIT and BNI cards do not support the tstcon feature. Tstdelay is also supported for the FRP and ASI in a non-integrated fashion similar to that of the tstcon command.

IGX Routing Hubs in a Tiered Network

With tiered networks, IGX nodes on the edge of the network are configured as interface shelves and are connected to IGX nodes configured as router hubs. The interface shelves allow the network to support additional voice, data and Frame Relay connections without adding additional routing nodes. An example of 3-segment voice and data connections via an IGX interface shelf and IGX routing hubs is shown in (Figure 14-3). An example of a Frame Relay connection via an IGX interface shelf and routing hubs is shown in (Figure 14-4).

Figure 14-3 IGX Shelves and Routing Hubs, Voice and Data Connections

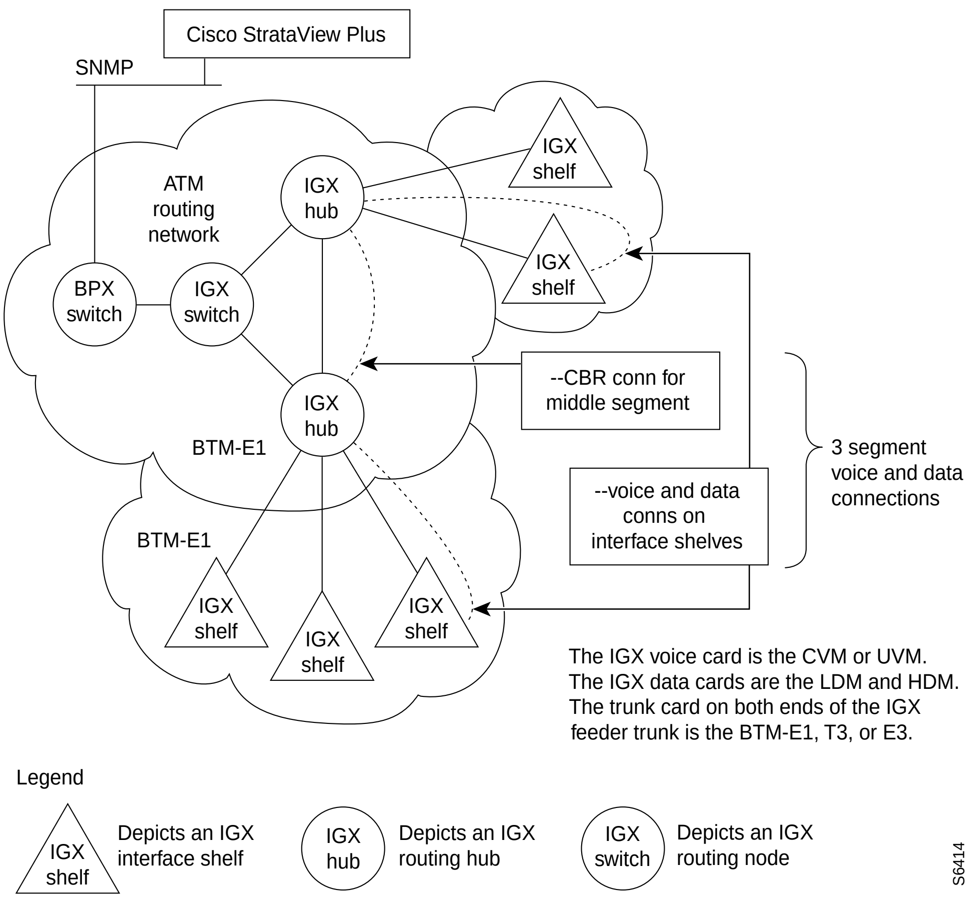
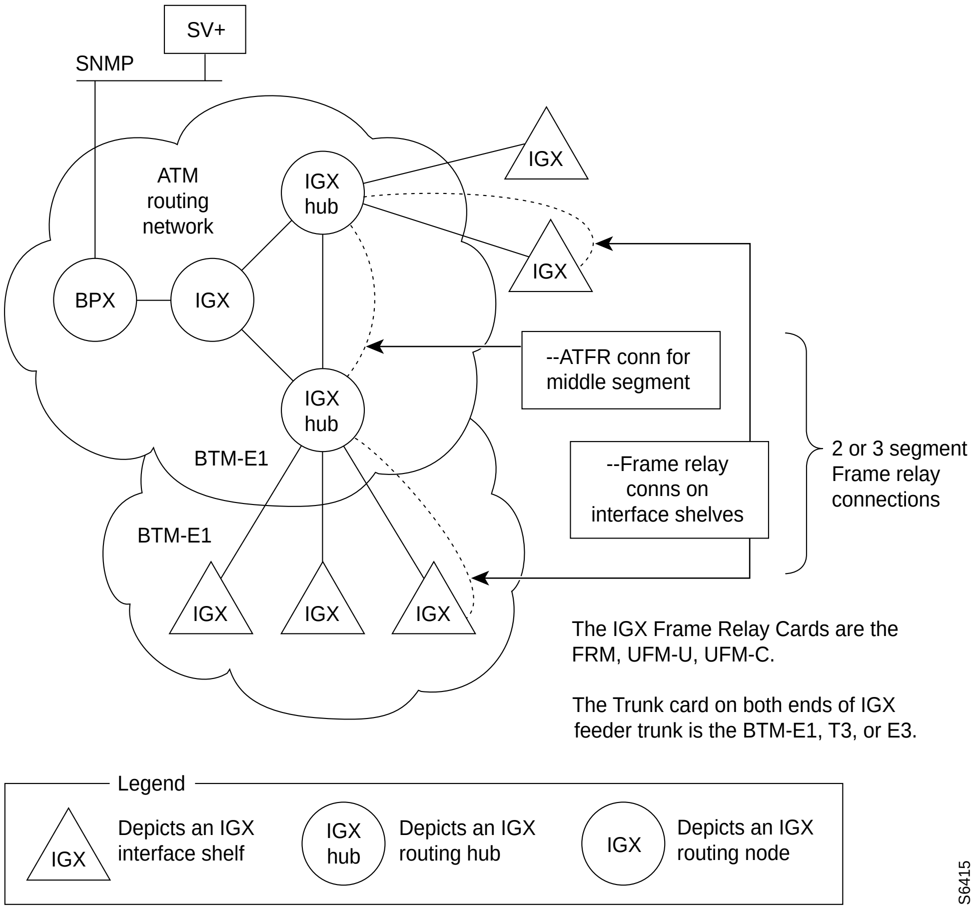


Figure 14-4 IGX Shelves and Routing Hubs, Frame Relay Connections



Tiered Network Implementation

The following applies to IGX routing hubs and interface shelves:

- An IGX routing hub supports up to 4 IGX interface shelves.
- An IGX interface shelf can have only one feeder trunk to the routing network.
- An IGX interface shelf is the only type of interface shelf that can connect to IGX routing hubs.
- No direct trunking between interface shelves is supported.
- No routing trunk is supported between the routing network and interface shelves.
- The feeder trunks between IGX hubs and IGX interface shelves are connected to a BTM-E1 backcard on each end of the trunk.
- Voice and data connection management to an IGX interface shelf is provided by Cisco WAN Manager
- Telnet is supported to an interface shelve; the vt command is not.

- Remote printing by the interface shelf via a print command from the routing network is not supported.

The following applies to voice and data connections over IGX interface shelves:

- 3-segment connections are supported, that is: originating IGX interface shelf data or voice card to IGX routing hub, across IGX intermediate nodes, as applicable, to IGX routing hub, to terminating IGX interface shelf data or voice card.
- 2-segment connections are not supported, (IGX interface shelf voice or data card to routing hub).
- Routing through the middle segment of the three segment connection is done via IGX routing nodes using CBR mode and simple gateway over the IGX trunks.
- Connection statistics are supported at user endpoints only.
- Adaptive voice is not supported.

The following applies to Frame Relay connections over IGX interface shelves via an IGX hub.

- 3-segment connections are supported, that is: originating IGX interface shelf Frame Relay card to IGX routing hub, across IGX intermediate nodes, as applicable, to IGX routing hub, to terminating IGX interface shelf data or voice card.
- 2-segment connections are supported, (IGX interface shelf Frame Relay card to routing hub).
- Routing through the middle segment of the three segment connection is done via IGX routing nodes using ATFR mode and simple gateway over the IGX trunks.
- Connection statistics are supported at user endpoints only.

General

Annex G, a bi-directional protocol, defined in Recommendation Q.2931, is used for monitoring the status of connections across a UNI interface. Tiered Networks use the Annex G protocol to pass connection status information between a Hub Node and attached Shelf.

Definitions

IGX Routing Hub	An IGX node in the routing network which has attached IGX interface shelves. Also referred to as a hub node or IGX hub.
IGX Interface Shelf	A special configuration of an IGX switch that is connected as a shelf to an IGX routing hub. An IGX interface shelf is sometimes referred to as IGX A/F or feeder. The IGX interface shelf does not perform routing functions nor keep track of network topology.
Feeder Trunk	Refers to a trunk which interconnects an IGX interface shelf with the routing network via an IGX routing hub. A feeder trunk is sometimes referred to as an interface shelf trunk.
IGX/AF	Another name for the IGX interface shelf.
Routing Network	The portion of the tiered network which performs automatic routing between connection endpoints.
VPI	Virtual Path Identifier.
VCI	Virtual Connection Identifier.

Upgrades

Converting an IGX node to an interface shelf requires re-configuring connections on the node, as no upgrade path is provided in changing a routing node to an interface shelf.

Only IGX nodes are able to act hub nodes for IGX interface shelves for voice and data transport over the IGX tiered network. An IGX node, acting as a hub node, is not restricted from providing any other feature which is normally available on IGX nodes. An IGX hub supports up to 4 IGX interface shelves.

Connections within tiered networks consist of three distinct segments within each tier. A routing segment traverses the routing network, with an interface shelf segment at each end providing connectivity to the interface shelf end-point. Each of these segments are added, configured and deleted independently of the other segments. The Cisco WAN Manager Connection Manager provides management of these individual segments as a single end-to-end connection.

Interface shelves are attached to the routing network via an IGX node using a BTM E1 trunk. The connection segments within the routing network are terminated on IGX feeder trunks.

Co-locating Routing Hubs and Shelves

The feeder trunk between an interface shelf and the routing network is a single point of failure, therefore, the interface shelves should be co-located with their associated hub node. Card level redundancy is supported by the Y-Cable redundancy for the CVM, LDM, and HDM.

Network Management

Communication between CPE devices and the routing network is provided in accordance with Annex G of Recommendation Q.2931. This is a bidirectional protocol for monitoring the status of connections across a UNI interface.

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

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

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

IGX routing hubs are the source of the network clock for its associated feeder nodes. Feeders synchronize their time and date to match their routing hub.

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

An interface shelf is displayed as a unique icon in the Cisco WAN Manager Network Management topology displays. The colors of the icon and connecting trunks indicate the alarm state of each. Channel statistics are supported by CVM, HDM, and LDM endpoints. Trunk Statistics are supported for the feeder trunk and are identical to the existing IGX trunk statistics.

Preferred Routing

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

Local and Remote Loopbacks

Connection local and remote loopbacks are managed at the user interface of the voice or data endpoint Routing Node or interface shelf. The existing IGX voice and data port loopback features are supported on the IGX interface shelf.

Testcon and Testdly

Tstcon is supported at the voice and data endpoints in a non-integrated fashion and is limited to a pass/fail loopback test. Fault isolation is not performed. Intermediate endpoints at the BTM cards do not support the tstcon feature. Tstdelay is also supported for the in a non-integrated fashion similar to that of the tstcon command.

IGX Interface Shelf Description

The IGX interface shelf supports the termination of voice and data connection segments to a BTM. The IGX interface shelf connects to the routing network via a BTM and associated BMT-E1 back card on both the interface shelf and the IGX routing hub.

IGX interface shelves support the following network management features:

- Interval Statistics enable/disable/collection

- IP Relay
- Robust Object Updates
- Robust Alarm Updates
- Real-time Counters
- Event Logging
- Software/Firmware Downloads
- Configuration Save/Restore
- SNMP

Configuration and Management

The interface shelves attached to each hub must have unique names. Each interface shelf must also be assigned a unique IP address.

An interface shelf communicates with a routing hub over a new type of NNI. It is similar to the existing Frame Relay NNI in purpose and function, and is based on the ATM LMI message set described by Recommendation 2931, Annex G. A routing hub and interface shelf use this NNI to maintain a control session with each other. Any change to the status of the feeder trunk affects this control session.

Feeder trunks are the communication path between the routing hub and the Feeder. These feeder trunks are supported by the BTM trunk card on both the IGX interface shelf and the IGX routing hub. Feeder trunks are upped using the "**uptrk**" command. Feeder trunks must be upped on both the routing hub and the interface shelf before it can be joined to the routing network.

An IGX node must be converted to an interface shelf by entering the appropriate command at the node. Once an IGX switch has been converted to an interface shelf, it can be joined to the IGX routing hub, by executing the **addshelf** command at the IGX routing hub. The **addshelf** command has the following syntax:

Shelf Management

addshelf <trunk> <shelf_type>

trunk	slot.port
shelf_type	I (IGX/AF)

```
delshelf <trunk> | <shelf_name>   deletes interface shelf
```

dspnode: Displays feeder trunk status. IGX routing hubs display the status of all attached IGX interface shelves. IGX interface shelves display a single status item, that of the attached IGX hub node.

Alarm Management of Interface Shelf on the IGX Hub Node

dspalms The field, interface shelf alarms, shows a count of the number of interface shelves which are Unreachable, in Minor Alarm, or in Major Alarm. The nnn-A bit status failures for interface shelf connections are also shown.

Alarm Management on the IGX Interface Shelf

dspalms The field, routing network Alarms, shows a count of major and minor alarms in the routing network. Feeder Abit connection status reported by feeder NNI is shown in the "Connection Abit Alarms" field.

dspnode: Shows if the routing network is reachable and the attached IGX hub node.

Port Management

Uses existing commands.

Connection Management

Parameters entered at Cisco WAN Manager when adding connections.

Bandwidth Management

Parameters entered at Cisco WAN Manager when adding connection. Bandwidth performance monitored by viewing selected statistics at Cisco WAN Manager NMS.

Bandwidth Efficiency

Since voice traffic is time sensitive, and low-speed voice connections can result in SGW cells being sent with only a single packet placed in the cell in order to avoid excessive delay between cells. It may be necessary to use the **cnfcmb** command on the interface shelves in order to configure the packet combining timeout rate for a particular application.

Statistics

Enabled and monitored via Cisco WAN Manager.

User Interface Commands

Refer to the Command Reference manual for additional information on commands associated with tiered networks. The following is a list of most often used commands with IGX routing hubs and IGX interface shelves supporting voice and data connections.

Shelf

addshelf

delshelf

dspnode

dspalms

dsptrks

Data Connection Commands

addcon

dspcon

dspcons

Data Channel Commands

cnfchdfm

cnfcheia

cnfcldir

cnfdchtp

cnfdclk

cnfict

Voice Connection Commands

addcon

Voice Channel Commands

cnfchadv

cnfchutil

cnfchkdl

cnfcos

cnfechec

cnfchgn

cnfcond

cnfrcvsig

cnfvchtp

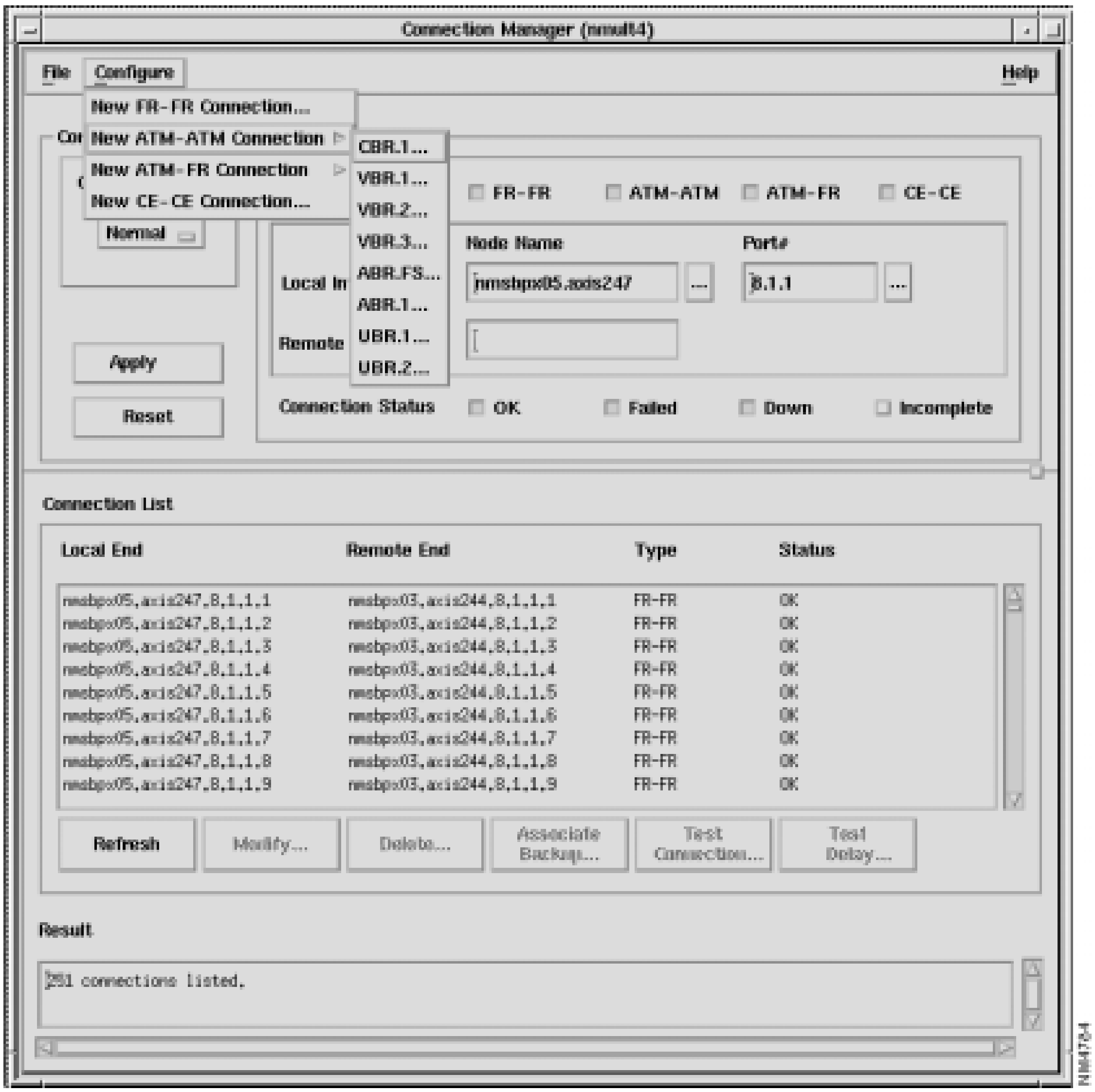
cnfxmtisig

cnfcmb

Cisco WAN Manager NMS

Interface shelf and feeder trunk information is reported to Cisco WAN Manager by the routing hub and interface shelf. Cisco WAN Manager can virtually connect to any node in the network via a TCP/IP connection. The Cisco WAN Manager Connection Manager is used to add, delete, and monitor voice and data connections for tiered networks with IGX hubs. It is also used to add, delete and monitor Frame Relay connections for tiered networks with BPX hubs. A sample of the Connection Manager GUI is shown in Figure 14-5.

Figure 14-5 Cisco WAN Manager Connection Manager



BPX SNMP Agent

This chapter introduces the functions of the Simple Network Management Protocol (SNMP) agent that is embedded in each BPX node. To benefit from this chapter, readers should have a general knowledge of SNMP, IP protocols, and MIBs.

The chapter contains the following:

- Introduction
- SNMP Overview
- SNMP Functions
- MIB II Support
- Cisco WAN Switching Proprietary MIB Structure

Introduction

An SNMP agent is embedded in each BPX node. (This feature is an addition to and functionally different from the SNMP Proxy Agent that can be used by a non-Cisco WAN Manager workstation to provide access to a MIB on the Cisco WAN Manager workstation which contains data extracted from the Cisco WAN Manager Informix database.) The SNMP agent permits an SNMP manager to view and set certain network objects in Management Information Bases (MIBs) that are maintained in each BPX node within a managed network. The embedded SNMP agent supports the standard Internet MIB II, the ATM 3.1 UNI MIB, and a Cisco WAN Switching proprietary MIB. The Cisco WAN Switching proprietary MIB contains information necessary to control ports and connections on the switches in the network. The standard Internet MIB II contains MIB modules defined by the Internet Engineering Steering Group (IESG). SNMP support is available on both IPX and BPX switches.

The proprietary MIB is supplied on a tape for compilation into the user's SNMP manager.

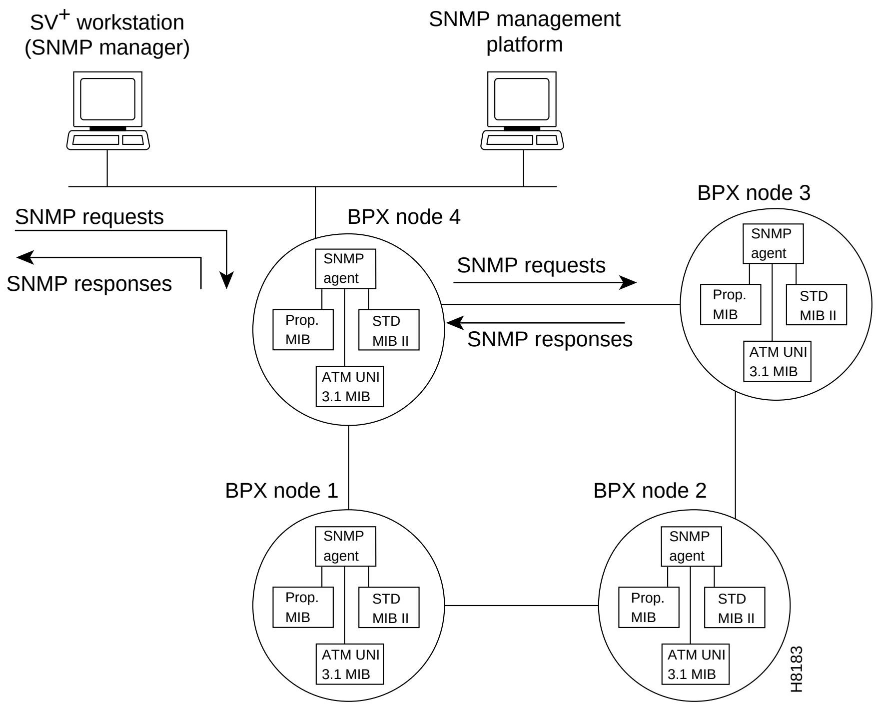
SNMP Overview

An SNMP manager manages the SNMP agents in each BPX node in a single domain. To gain access to network nodes, the SNMP manager is connected to one of the BPX nodes through its Ethernet port, which acts as a gateway for the SNMP manager to communicate with all the other BPX nodes in the domain.

In multiple networks, a separate SNMP manager must exist for each network that is being managed. Furthermore, nodes within a multi-network can be managed by multiple SNMP managers. Also, ATM connections that span multiple networks are supported in the SNMP MIB.

Figure 15-1 shows an SNMP manager and the nodes within a domain.

Figure 15-1 SNMP Manager and Agents in a BPX Domain



Communication between the agents and the SNMP manager uses the standard UDP protocol encapsulated within IP protocol. The communication link between the SNMP manager and the directly attached BPX node uses the Ethernet interface of an BCC processor card. The SNMP manager can be either local or remote to the BPX node.

Figure 15-1 illustrates the SNMP manager's communication with the agents in the network. Each node in the domain must have a network IP address assigned by the **cnfnwip** command (see the *Cisco WAN Switching Command Reference* publication for details). The manager uses the network IP address to address an agent in the domain. The directly attached node (Node 4 in Figure 15-1) directs the SNMP message to the addressed BPX node. Responses from the agent go to the directly attached node then pass over the Ethernet link to the SNMP manager.

Note The LAN IP address of the directly attached node must be configured with the **cnflan** command.

SNMP Functions

The SNMP protocol provides a basic query-response model for network management. The network manager has access to Get (Get-Next) and Set functions.

A Get request lets the manager read variables in the BPX switch. The request consists of a single variable or a list of variables. The BPX database subsequently returns the requested values.

The Get-Next request lets the manager obtain the successor to the given variable's object identifier. The returned object identifier can serve as input to another Get-Next request so the manager can lexicographically walk through the MIB.

A Set request lets the manager modify variables in the BPX switch. The request consists of either a single variable or a list of variables. The values supplied in the request modify the BPX database. The variables and their associated values in the request message are put into a response message and returned to the requesting management workstation. The format of the Set response message is the same as that of the Get response message.

SNMP requests from the manager have the same access level as non-privileged users. Non-privileged access can be read-only, read-write, or no access. To maintain access control, each Get and Set request is checked for the correct community string. The community string determines the access privileges that a management workstation has. A separate community string exists for Get requests and Set requests.

The node initializes the community strings to no access, so the user must set the strings to the appropriate values. The community strings can be set and displayed by the **cnfsnmp** and **dspsnmp** super-user commands, respectively (see the *Cisco WAN Switching Super-User Command Reference* publication for details).

Responses to Get, Get-Next, and Set requests are returned in a response packet along with a status field. The status field can be one of the following:

- noError (0) — Successful operation.
- tooBig (1) — The agent could not fit the results of an operation into a single SNMP message.
- noSuchName (2) — The requested operation identified an unknown variable when attempting to modify a variable.
- badValue (3) — Requested operation specified an incorrect syntax or value when attempting to modify a variable.
- readOnly (4) — Requested operation attempted to modify a variable that, according to the community profile, may not be written. (No longer supported by Standards.)
- genErr (5) — All other failure responses.

If an error occurs, the appropriate error code is encoded in ASN.1 format and inserted into the response packet.

Note In the sections that follow, user-specified command names are in lower case.

Responses to Get (Get-Next) Requests

When an SNMP manager workstation sends an SNMP Get request packet to a BPX agent, it utilizes the IP protocol for addressing. The request packet can use either a LAN interface for a locally attached management workstation or a network interface for remote access. Each packet is in ASN.1 format, which is suitable for transmission via the UDP protocol. Once it arrives, the packet is decoded to a Protocol Data Unit (PDU). This PDU is the SNMP internal packet structure.

A PDU consists of one or more variables requested by the manager. The PDU's community string is validated for correct access permissions, then the requested variables are collected within an SNMP varbind list for processing.

For each variable in the request message, the agent calls a user-defined test function that makes sure the requested variable exists. If the test confirms the existence of the variable, the agent calls a user-defined get function to gain access to the BPX database for the specified variable. The get function is appropriate for the type of request (Get or Get-Next).

A get function can read either a single scalar value or a single column entry from the database row. The user-defined get-next function provides a way to read a table of unknown elements. The get-next function returns the lexicographically next variable in the table with respect to the next variable. This mechanism lets the manager sequentially retrieve the entire table.

The test and get functions result in a Get response packet. If an error occurs, the appropriate error code is encoded in ASN.1 format and placed in the packet. If no errors occur, the returned values are encoded and placed in the response packet. The response packet goes to the workstation that originated the Get request.

ATM Set Requests

SNMP Set requests support the ATM functions in the following list. Refer to the *Cisco WAN Switching Command Reference* for command descriptions.

- Add ATM connection (**addcon**)
- Delete ATM connection (**delcon**)
- Up ATM connection (**upcon**)
- Down ATM connection (**dncon**)
- Modify ATM connection (**cnfrcon**, **cnfcos**, **cnfpref**, **cnfrcon**)
- Test ATM connections (**tstcon**, **tstdelay**)

SNMP Set requests can implement the following BPX commands on ATM ports:

- Up ATM port (**upfrport**)
- Down ATM port (**dnfrport**)
- Modify ATM port (**cnffrport**)

Responses to Set Requests

When an SNMP manager workstation sends an SNMP Set request packet to a BPX agent, it utilizes the IP protocol for addressing. The request packet can use either a LAN interface for a locally attached management workstation or a network interface for remote access. Each packet has the ASN.1 format, which is suitable for transmission via the UDP protocol. Once it arrives, the packet is decoded to a Protocol Data Unit (PDU). This PDU is the SNMP internal packet structure.

Each variable in the varbind list is located, checked for visibility in the current MIB view, checked for write-access, and type-matched against the set request. A user-defined function is then called to validate the Set PDU. This validation mainly determines if the Set request packet follows the guidelines defined for the BPX switch. This function returns either good status or an error. The error indicates the PDU is bad and should be rejected. Processing continues with tests for accessibility and acceptability.

Each variable in the varbind list is tested for accessibility and acceptability. User-defined test functions associated with each variable are called to implement the tests. A failed test returns a specifier for the variable and a reason code. Any failed test results in a failed Set request. Upon successfully passing the test functions, the set request can proceed to set the requested variables on the specified switch. The SNMP agent calls a user-specified set function to implement the modifications.

Upon either a successful completion or an error, the Set request PDU is modified to become the response PDU. The response PDU also contains the values of the variables in the original Set request. This PDU is encoded into ASN.1 format and inserted into the response packet. The Set response packet goes to the workstation that generated the request.

MIB II Support

The BPX SNMP agent supports the following groups in the Internet SNMP MIB II:

- ARP
- ICMP
- Interfaces
- IP
- SNMP
- System
- TCP
- UDP

Cisco WAN Switching Proprietary MIB Structure

This section is an overview of the Cisco WAN Switching proprietary MIB. The proprietary MIB resides under the enterprises branch of the SNMP tree structure (1.3.6.1.4.1.StrataCom (351)). For detailed information on the structure and contents of the MIB, refer to the actual MIB that is included on the release tape. The MIB is in ASN.1 format.

The MIB provides network managers with BPX information on a per switch basis. This information in the MIB relates to ATM service. The SNMP agent MIB has two major branches of information. These are the Switch Service Objects and Switch Connections.

Each variable in the MIB also includes the following:

- An access level (read-only, read-write, or no access)
- A defined MIB view, which allows appropriate agents to have access to platform-specific information

Switch Service Objects

The higher level Switch Services branch shows the available ATM services. This service information exists in a configuration table and a statistics table for each logical port on the switch. The configuration parameters for a logical port allow the manager to view and modify a specified available port. The statistics table gives the manager access to real-time counter statistics associated with a specified available port.

Switch Connections

The Switch Connections branch supports per switch management of ATM connections. In this branch, the MIB defines the following:

- Connections—a general view of all available ATM connections on a switch
- Endpoints
- Bandwidth class
- Endpoint Statistics
- Endpoint mapping

The following is a list of the categories of connection information:

- Local description (such as, domain.node.slot.port.vpi.vci, group id) (read-only)
- Remote description (such as, domain.node.slot.port.vpi.vci) (read-only)
- Status of the connection (read-only)
- Failure reasons (read-only)
- Current route information (read-only)
- Preferred route information (read-write)
- Access to open space information (read-only)
- Pointer to endpoint-specific information (read-only)

The ATM endpoint-specific information (last item in the previous list) provides the mechanism for the manager to provision and configure ATM connections. The available endpoint-specific information is:

- Local description (such as, domain.node.slot.port.vpi.vci) (read-write)
- Remote description (such as, domain.node.slot.port.vpi.vci) (read-write)
- ATM applicable bandwidth parameters (read-write)
- Foresight enable status (read-write)
- Trunk avoid types (read-write)
- Connection priority (read-only)
- Foresight round-trip delay (read-only)

Bandwidth Class

The bandwidth class information gives the manager a view of the available bandwidth classes that are configured on the switch. The manager can use a selected class as a template to create a ATM endpoint.

Endpoint Statistics

The endpoint statistics are real-time counter statistics about a specific endpoint.

Endpoint Mapping

The endpoint mapping information lets the manager have access to connection and endpoint-specific indices. The indices are associated with physical attributes of a connection (for example, *slot.port.vpi.vci*). The manager can use the indices returned to it to gain access to connection and/or endpoint-specific information.

PART 5

MPLS

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. Refer to Release Notes for new 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 multiservice 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, Cisco 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.

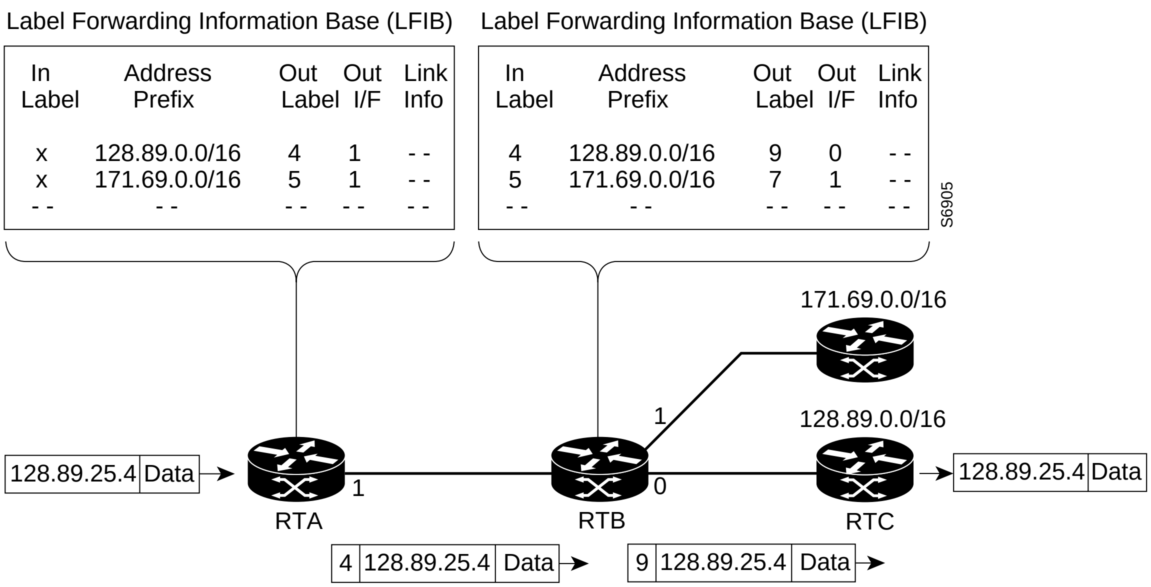
Figure 16-1 shows an example of label switching. It shows an unlabeled IP packet with destination 128.89.25.4 arriving at Router A (RTA). RTA checks its LFIB and matches the destination with prefix 128.89.0.0/16. (The /16 denotes 16 network masking bits per the Classless Interdomain Routing (CIDR) standard.) 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 16-1 Label Forwarding Information Base (LFIB) in an IP Packet Environment



Label Switching in an ATM WAN

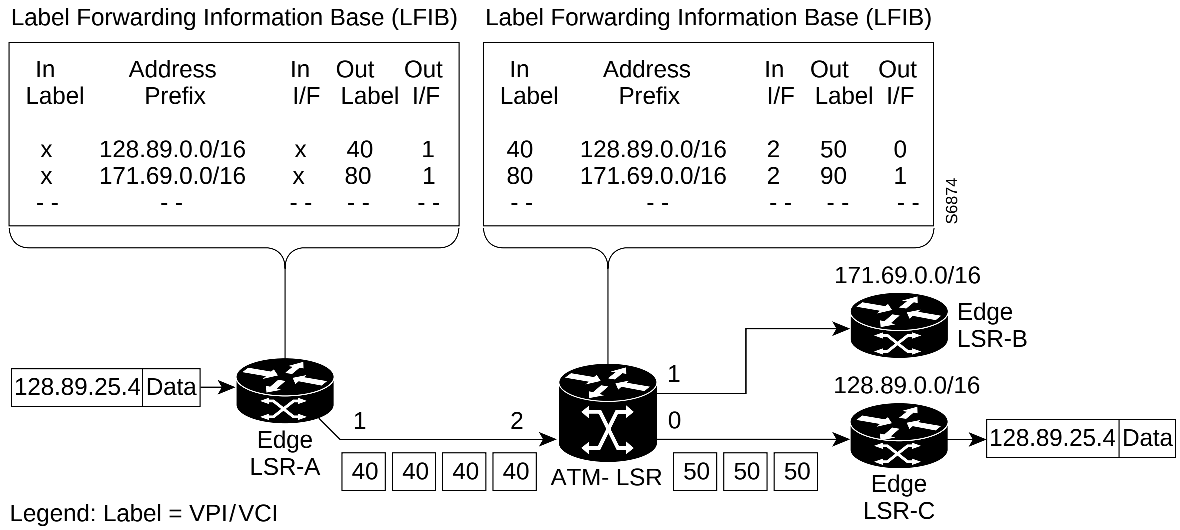
With label switching over an ATM network, the forwarding and control components can be described as follows:

- 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 16-2 shows the forwarding operation of an ATM switch in which the labels are designated VCIs. In Figure 16-2, 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 16-2 Label Forwarding Information Base (LFIB) in an ATM Environment



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 16-3 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.

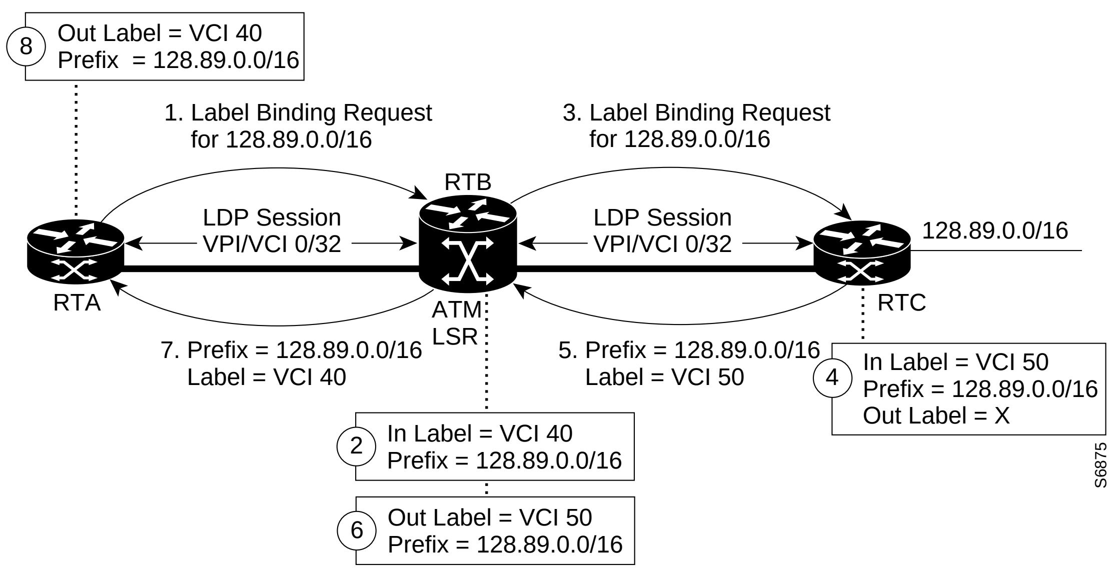
6 RTB sets the outgoing label to VCI 50.

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 16-3, except that the events labeled 7 and 8 in the figure may occur concurrently with event 3.

Figure 16-3 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 16-3. 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.

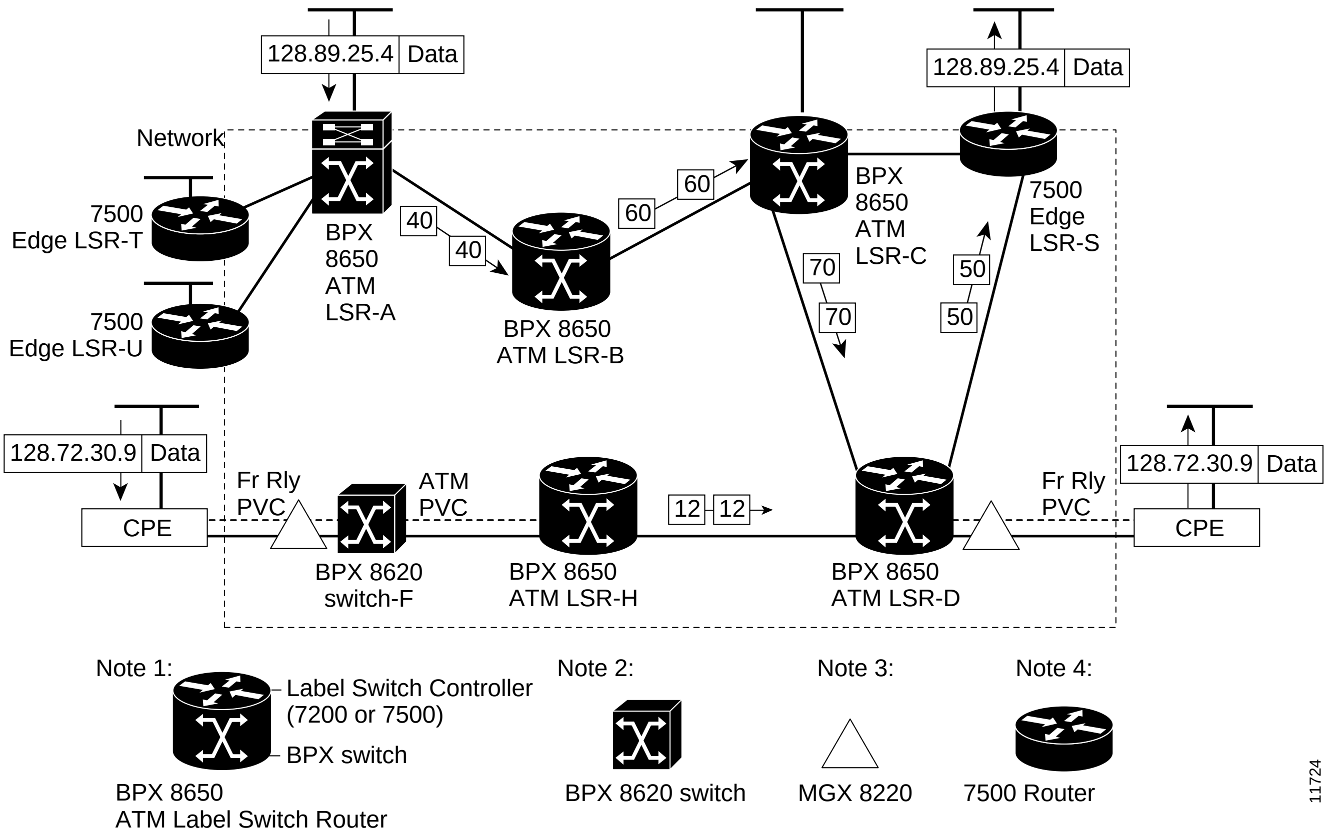
The router component of the label switches that are located at the boundaries of the network (BPX 8650 ATM-LSR-A, BPX 8650 ATM-LSR-C, BPX 8650 ATM-LSR-H), perform edge-routing network layer services including the application of labels to incoming packets. The edge label switch routers, 7500 edge LSR-S, 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 16-4 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 16-4, 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 16-4 BPX Label Switching



Virtual Switch Interfaces

When a virtual switch interface (VSI) is activated on a port, trunk, or virtual trunk so that it can be used by a master controller, such as a PNNI SVC or an MPLS controller, the resources of the virtual interface associated with the port, trunk, or virtual trunk are made available to the VSI.

VSI was implemented first on the BPX 8650 in Release 9.1, which uses VSI to perform Multiprotocol Label Switching. Release 9.1 allowed support for VSI on BXM cards and for partitioning BXM resources between Automatic Routing Management (formerly called AutoRoute) and a VSI-MPLS controller. In the current release, you can configure partition resources to be shared between Automatic Routing Management PVCs and one VSI control plane, but not both.

The second implementation of VSI on the BPX provides the following extensioned functionality:

- class of service templates
- virtual trunks support for VSI
- support for VSI master redundancy, and
- SV+ support for VSI

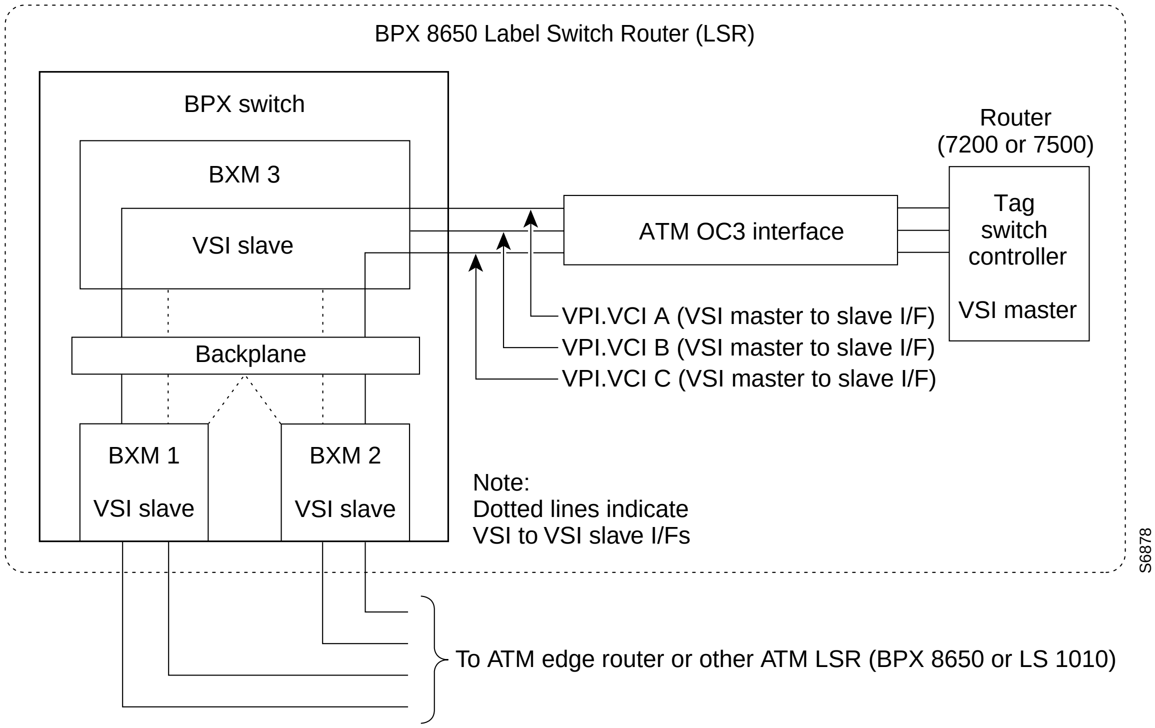
In this release, you can configure partition resources between Automatic Routing Management PVCs and two VSI controllers (LSC or PNNI). Two VSI controllers in different control planes can independently control the switch with no communication between controllers. The controllers are essentially unaware of the existence of other control planes sharing the switch. This is possible because different control planes used different partitions of the switch resources.

For more information on multiple VSI partitioning, see "VSI Commands" in the *Cisco WAN Switching Command Reference, Release 9.2.30.*

Figure 16-5 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 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 16-5 BPX Switch VSI Interfaces



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 16-6 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 16-7.

Figure 16-6 Connection Setup, End Points on same VSI Slave

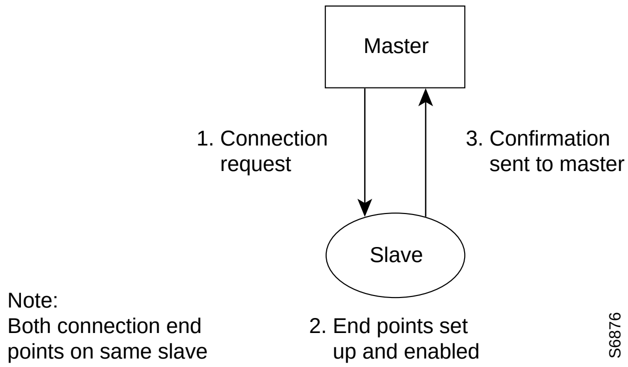
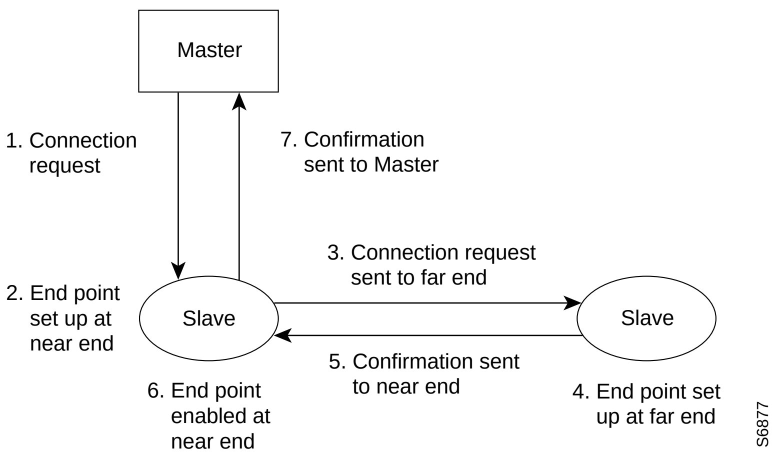


Figure 16-7 Connection Setup, End Points on Different VSI Slaves



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 by 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 16-1.

Table 16-1 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 this release, up to two VSI partitions may be used. VSI partitions may be used to support the Cisco 6400 as well as the 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 16-2. 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 16-2 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 16-3. If these values are not applicable, then other values may be configured using the **cnfrsrc** command.

Table 16-3 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 that 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:

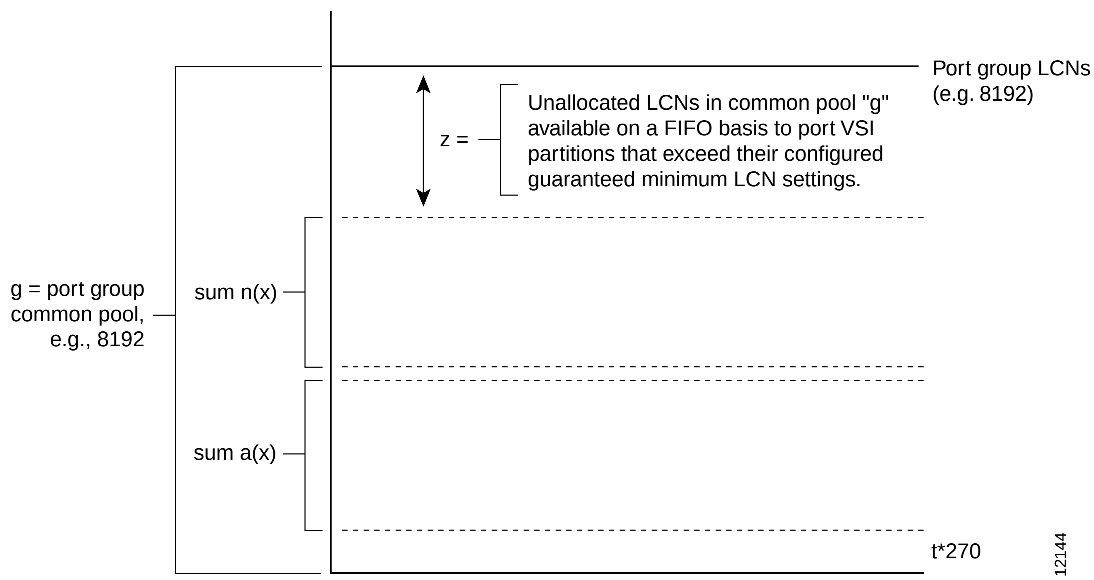
$$\text{sum}\ (\ a\ (x)\ ) + \text{sum}\ (\ n_1\ (x)\ ) + t * 270 <= g$$

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 16-8 shows the relationship of these elements.

The “270” value reflects the number of LCNs that 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 16-8 Port VSI Partition LCN Allocation Elements



Note Label switching can operate on a BXM card configured for either trunk (network) or port (service) mode. Ports on the card can be configured either as ports 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 (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 Switching 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 (the Cisco 6400, the 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:
```

For this release, two controllers are supported. The user interface will block the activation of partitions with ID higher than 1 if the card does not support multiple partitions.

When enabling a partition, If [start_VPI, end_VPI] of the partition contains any “reserved” VPI, an error message is displayed and you are prompted for different values for start_VPI, end_VPI. Thus, if VPI 10 is used for control VCs on an interface, then you cannot include VPI 10 in any VSI partition by using the **cnfrsrc** command. An error message would be displayed.

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 16-4.

Table 16-4 cnfrsrc Parameter Summary

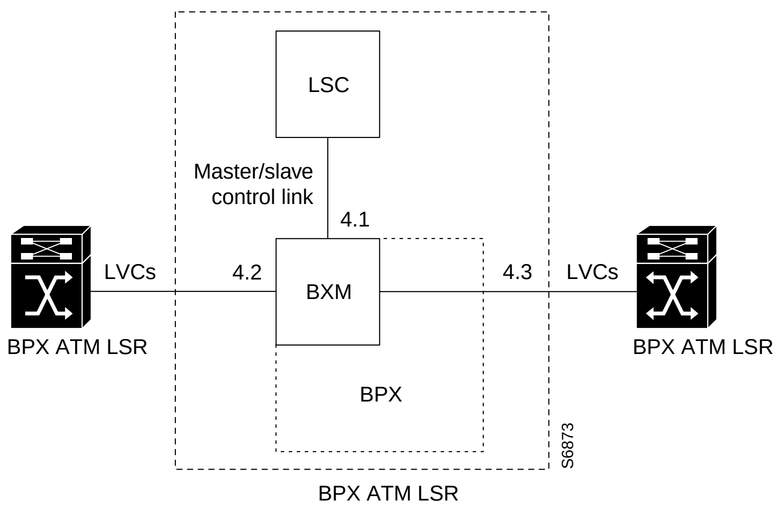
Parameter (cnfrsrc)	Example Value	Description
slot.port	4.1	Specifies the slot and port number for the BXM.
maxpvclcns	256	The maximum number of LCNs allocated for AutoRoute PVCs for this port.
maxpvcbw	26000	The maximum bandwidth of the port allocated for AutoRoute use.
partition	1... 2	Partition number.
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 (Cisco 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 16-9.

Note For label switching, the BXM may operate in either trunk or port mode. 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 16-9 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 16-3. 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 14*.

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.

- **addctrlr**
- **addshelf**
- **cnfqbin**
- **cnfrsrc**
- **delctrlr**
- **dspcd**
- **dspcds**
- **dspctrlrs**
- **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.

addctrlr

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

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

The first step is to run the command **addshelf** with shelf type set to "X" to add a AAL5 feeder. This ensures that Annex G protocol runs between the BPX and the SES.

Then run the **addctrlr** command to set up the VSI control channels from the PNNI SES controller to the VSI slave processes running on the BXM cards to ensure full VSI functionality for the PNNI controller. You execute the **addctrlr** command on an existing AAL/5 interface shelf.

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

When you add VSI controller capabilities onto an AAL/5 interface shelf (or feeder), the switch software prompts you for the specifics of the VSI controller:

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

There could be 12 BXM cards on the BPX node and the PNNI controller would control VSI partitions on those BXM cards that support VSI capability. Hence a separate VSI control channel must be set up from the PNNI control to each BXM card that supports VSI.

Suppose you specify a VPI value of 0 and start VCI value of 40 for the VSI control channels. Then the control channel corresponding to any BXM card on slot 1 would use VPI, VCI values <0, 40>. The VSI control channels to other slots would use the VPI, VCI values of <0, 40+slot-1>, where "slot" corresponds to the slot number of the BXM card.

Note ESP 2.x interface shelves can still be configured; however, an ESP 2.x shelf cannot coexist with an AAL/5 interface shelf with VSI configured on the same node. The Annex G capabilities of the AAL/5 interface shelf are the same as in Release 9.1.

Caution For feeder trunk interfaces, the **addctrlr** command will fail if the AutoRoute connections terminating on the feeder interface use the same VPI VCI as those specified for theVSI control channels.You must delete the connections before proceeding if connections with VPI and VCI in the range exist in the range you specified.

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

Full Name

Add VSI capabilities to a AAL5 feeder interface.

Syntax

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

Parameters—addctrlr

Parameter	Description
<slot.port>	Slot and Port numbers corresponding to the feeder trunk
<controller-id>	Controller ID corresponding to the PNNI controller. Values: 1 - 32
<partition-id>	Partition ID of the VSI partition controlled by the PNNI controller
<control_vpi>	Starting VPI of the VSI control channels used for communication between the VSI master residing on the SES and VSI slaves residing on the BXM cards. There can be a total of 12 such channels one for each slave residing on each BXM card. For a trunk interface with NNI header type: Valid values for this parameter are: 0–4095 For a trunk interface with UNI header type Valid values for this parameter are: 0–255. Default value: 0
<start_vci>	Starting VCI of the VSI control channels. This vci value is assigned to the first VSI control channel (between the VSI master and the VSI slave residing on the BXM card in slot 1). The last VSI control channel corresponding to communication with the VSI slave on slot 14 will use the vci value of (<start_vci>+14-1). The valid values are: 33 – 65521. Default value: 40

Related Commands

addshelf, delctrlr, dspctrlrs

Attributes

Privilege	Jobs	Log	Node	Lock
1	No	Yes	BPX	Yes

Example 1

```
addctrlr 10.4 3 2 0 40
```

Description

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

System Response

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

                    BPX Controllers Information

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


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

Last Command: addctrlr 10.4 3 2 0 40


Next Command:
```

Description

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

System Response

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

                    BPX Controllers Information

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


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

Last Command: addctrlr 10.3 3 1 0 40


Next Command:
```

addshelf

Adds an ATM link between a BXM card on a BPX node and a label switch controller such as Cisco 6400 or 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 16-5 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 (LSR) 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 (LSC).

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 16-6 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.
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.
control_vpi	Choose the value for <control_VPI> such that: if <control_VPI> = 0, <control_VCI_start> can be set to a value > 40. If any VSI partition exists on the interface, then control_VPI < start_VPI or control_VPI > end_VPI for all partitions on that interface. An error message appears if the control VPI falls into the VPI range belonging to a VSI partition. No AutoRoute connection exists on (VPI.start_VCI to VPI.start_VCI+14). If any AutoRoute connection exists on these VPI/VCI values, you are not allowed to use these VPI/VCI values. This VPI is reserved for control VCs. Default = 0
control_vci_start	Default = 40

The (VPI.VCI) of the 15 control VCs is:
(control_VPI.control_VCI_start) to (control_VPI.control_VCI_start+14).

The control VC used for slot n (1<= n<=15) is:
(control_VPI.control_VCI_start + n -1).

Example for Interface Shelves

Add an MGX 8220 at trunk 11.1. After you add the shelf, the screen displays a confirmation message and the name of the shelf. Add the MGX 8220 (may be referred to 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 to the VSI chapter for additional information on configuring resources. See the *Cisco WAN Switching Command Reference* for more detail.

Syntax

cnfrsrc <slot.port.vtrk>

or

cnfrsrc <slot>.<port>.<vtrk> <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
1-6	No	No	BPX	No

Related Commands

`dsprsrc`

Parameters—cnfrsrc

Parameter	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	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 16-7. If these values are not applicable, then other values may be configured using the **cnfrsrc** command.

Table 16-7 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

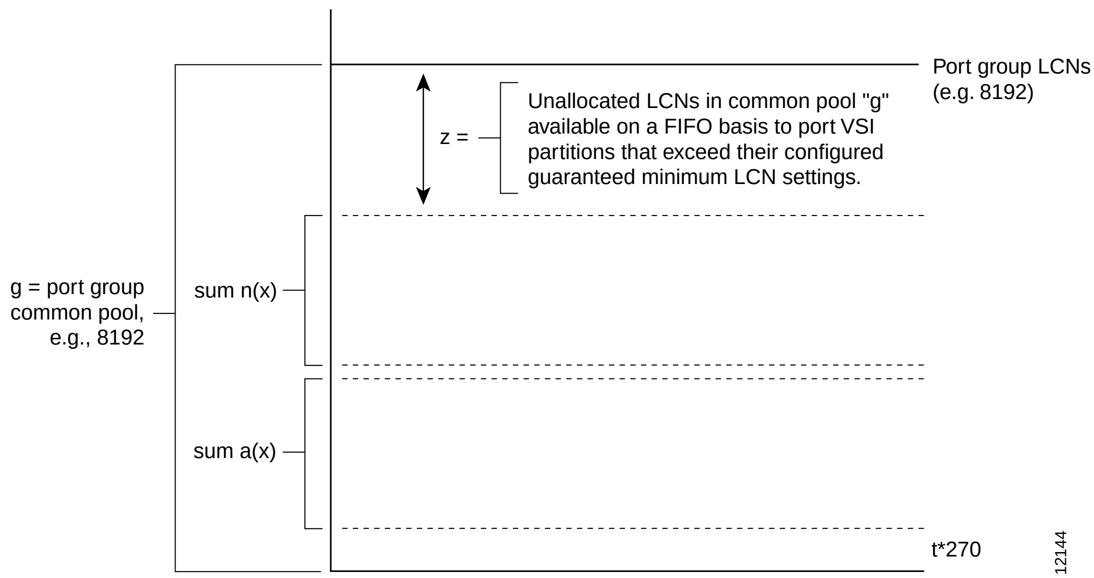
More rigorous allocations are possible when default values are not applicable. For example, the LCN allocations for a port group must satisfy the following limit:

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 16-10 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 16-10 Port VSI Partition LCN Allocation Elements



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 16-9 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 16-11. The allocations for ports 5-8 are similar to that shown in Figure 16-11, but with correspondingly different values.

As shown in Figure 16-12, "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 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 16-8 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 16-8 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 16-8 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.

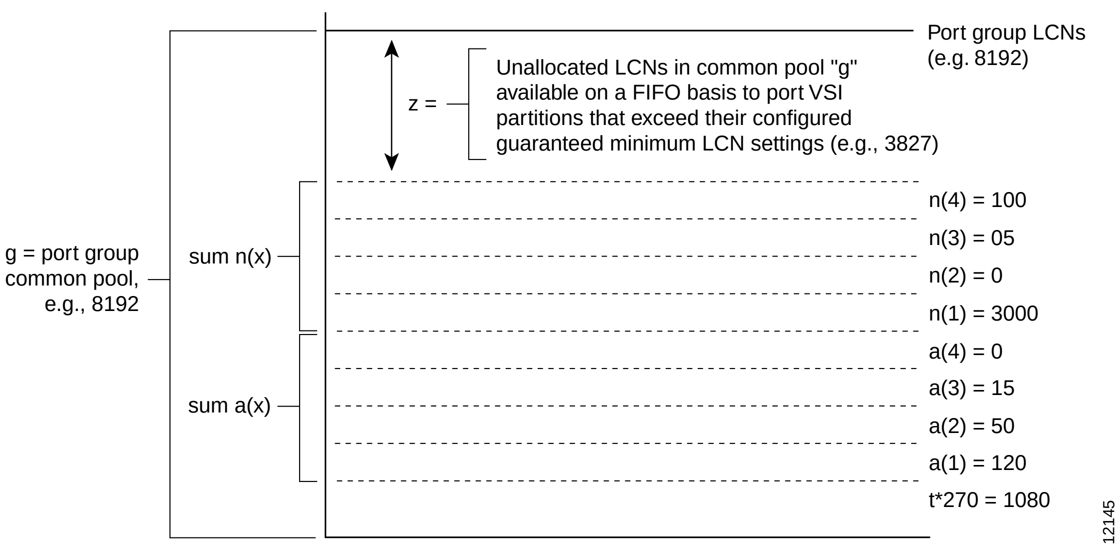
— Port 7 is guaranteed to be able to support 100 PVCs and 200 LVCs. It will not support any more.

— 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 16-8 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 16-11 LCN Allocations for Ports 1-4, Ports Configured in Trunk Mode Example



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 16-9 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 16-12. The allocations for ports 5-8 are similar to that shown in Figure 16-12, but with correspondingly different values.

As shown in Figure 16-12, “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 16-9 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 16-9 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 16-9 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.

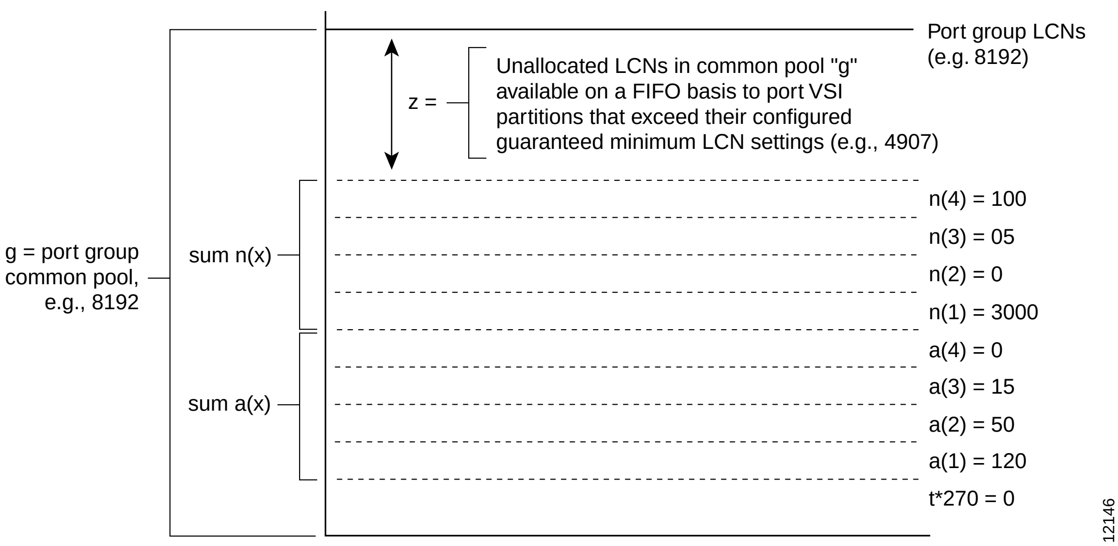
— Port 7 is guaranteed to be able to support 100 PVCs and 200 LVCs. It will not support any more.

— 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 16-9 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 16-12 LCN Allocations for Ports 1-4, Ports Configured in Port Mode Example



delctrlr

Deletes VSI capabilities on a trunk interface to which a Feeder of type AAL5 is attached. Use this command to delete a controller, such as a SES PNNI controller, from a BPX node. It deletes the VSI control channels used to communicate between the VSI master on the PNNI controller and the VSI slaves on the BXM cards.

You run this command as the first step in deleting a PNNI controller from a BPX node. The second step is to run the command **delshelf** to delete the AAL5 feeder.

(Do not use **delctrlr** to delete a VSI Label Switching controller from a BPX node; you must use **delshelf** to delete a VSI Label Switching controller from a BPX node.)

PNNI runs on the Service Expansion Shelf (SES) hardware.

To add SES PNNI controller capabilities onto the newly-created AAL/5 interface you use the **addctrlr** command. You are prompted to enter the controller ID and partition ID. This creates an interface through which a PNNI controller can use the VSI protocol to control the node resources that were previously specified by using the **cnfrsrc** command.

You remove a PNNI controller from a BPX node by using the **delctrlr** command. For example, this might be a VSI controller such as an PNNI controller configured with VSI capabilities as an AAL/5 interface shelf to a BPX. When you delete one of the controllers by using the **delctrlr** command, the master-slave connections associated with this controller are deleted. The control VCs associated with other controllers managing the same partition will not be affected.

Note To add a VSI Label Switch Controller, you use **addshelf** and **delshelf** commands, as in releases previous to Release 9.2.

Full Name

Delete VSI capabilities from an AAL5 feeder interface.

Syntax

delctrlr <slot.port> <controller id>

Parameters

Parameter	Description
slot.port	Slot and port numbers corresponding to the feeder trunk.
controller id	Controller ID number corresponding to the PNNI controller you are deleting. ID numbers should correspond to an active PNNI controller. Valid controller values are: 1 – 32

Related Commands

addctrlr, dspctrlrs, dspnode

Attributes

Privilege	Jobs	Log	Node	Lock
1	Yes	Yes	BPX	Yes

Example 1

`delctrlr 10.3`

Description

Delete VSI controller with interface shelf (feeder) type of AAL/5 connected on trunk 10.3 from the list of controllers connected to BPX node named “night”.

System Response

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

                        BPX Controllers Information

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



Last Command: delctrlr 10.3
```

System Response

```
night          TN    StrataCom       BPX 8600    9.2.   Apr. 11 1998 14:31 GMT

                        BPX Controllers Information

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



Last Command: delctrlr 10.3
```

Example 2

`delctrlr <slot.port><controller_id>`

Description

Deletes controller from port 3 on slot 10, with controller name "E", and controller ID of 1.

System Response

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

                        BPX Controllers Information

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




Last Command: delctrlr 10.3
```

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.

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

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:
```

dspchuse

The **dspchuse** command displays the a summary of the channel distribution in a given slot. It shows the distribution of channels between AutoRoute pvcs, networking channels, VSI management channels, and channels allocated to the VSI slave.

This command applies only to BXM cards. Previously a debug command, **dspchuse** is available to multiple users at all privilege levels in this release.

Full Name

Display channel distribution

Syntax

dspchuse <slot >

Related Commands

dspvsiif, dspvsipartinfo

Attributes

Privilege	Jobs	Log	Node	Lock
1-6	No	No	BPX	No

Parameters—dspchuse

Parameter	Description
max	Maximum number of channels supported on the card or port group.
used	Number of channels currently used; this includes all types of channels: networking channels, pvcs, svcs, vsi master-slave vcs, and channels allocated to vsi partitions.
avail	Number or channels still available for use.
netw	Number of network channels used. For each trunk interface (feeder trunk, physical trunk, or virtual trunk) that is upped some channels are reserved for networking. For a feeder or a physical trunk 271 channels are reserved. For a virtual trunk, the first one upped on the port will reserve 271, any subsequent virtual trunk on the same port will reserve 1 more channel.
pvc cnfg	Number of pvcs configured.
svc cnfg	Number of svcs configured.
vsi mgmt	Number of channels used for VSI master-slave vcs. Note: the sum of port group VSI management vcs may be less than the number of VSI management vcs at the card level. This is because the backplane management connection (the leg of the connection from the backplane to the slave) requires resources at the card level but not at the port group level.
vsi cnfg	VSI channels reserved for use by the slave to set up connections requested via the VSI interface. Although the configuration of the partitions is done on a per-interface basis, the pool of LCNs is managed at the card level and at the port group level..
pvc used	Channels currently used by AutoRoute connections.
vsi min	VSI min channels configured for a partition via the **cnfrsrc** command.
vsi max	VSI max channels configured for a partition via the **cnfrsrc** command.

Example 1

dspchuse 13

Description

Display channel management summary for slot 13.

System Response

```
sw53 TN StrataCom BPX 8600  9.2.10  Jan. 10 1999 14:31 GMT

            Channel Management Summary for Slot 13

          max    used   avail   netwpvc  cnfgvsi  mgmt vsi cnf

card 13:  16320  8675   7645    1358    2304     13    5000
port grp 1:8160  5849   2311    813     1024     12    4000
port grp 2:8160  2825   5335    545     1280      0    1000

          pvc cnfg pvc used nw used vsi mgmt vsi min vsi max

port 1:   256              0    271       0
part 1:                                      1000   4000
part 2:                                      2000   4000
port 2:   256              0    271       0
port 3:   256              0    271      12

This Command: dspchuse 13

Continue?
```

dspctrlrs

Use the **dspctrlrs** command to display all VSI controllers, such as an SES PNNI controller, on a BPX or IGX node. This command lists:

- the controller ID,
- the partition the controller uses,
- the trunk/interface to which a controller is attached,
- the controller type (always a VSI controller),
- the interface type (AAL/5, VSI (Label Switching), or
- MGX 8220 (formerly called AXIS) interface shelf, and
- the name of the controller/entity on which the controller exists (that is, node name, equipment name).

(Note that you use **addshelf** and **delshelf** to add and delete a VSI controller such as a Label Switching Controller to a BPX node.)

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

Full Name

Displays all VSI controllers. For example, all PNNI controllers on a BPX or IGX node.

Syntax

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

Related Commands

addctrlr, addshelf, cnfctrlr, delctrlr, dspnode

Attributes

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

Example 1

```
dspctrlrs
```

Description

Display VSI controllers on BPX node sw174.

System Response

```
sw174          TRM    StrataCom       BPX 8620    9.2.xS  Sep 20 1998 14:31 GMT


                        BPX 8620 VSI controller information

Ctrl Id   Part Id    Trunk   Ctrlr Type    Intfc Type    Name
1        1           2.1     VSI           AAL/5         SIMFDR0



Last Command: dspctrlrs
```

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.

You can use the **dspnode** command to display the VSI controllers on a BPX node. In this release, you can display the control_VPI and control_VCI_start of the particular controller, as shown in Example 2.

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 1

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:
```

Example 2

dspnode

Description

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

System Response

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

                   BPX 8620 Interface Shelf Information

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




Last Command: dspnode
```

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 VSI configuration of the specified partition on a BXM card.

Note To display a specific partition, you can enter the optional partition_id parameter for the **dsprsrc** command. In this release, the valid partitions are 1 and 2.

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, IGX, BPX	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, IGX, BPX	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

resetcd 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	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, IGX, BPX	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

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 further information regarding the Cisco 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 a 7200 or 7500 router and a BPX switch shelf, where a 7200 or 7500 router provides the controlling function to the BPX switch shelf.

When MPLS is running in the network, the routing protocol, e.g., 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, e.g., 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

— 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 17-1 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 17-1, (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 17-1 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 17-1 High-Level View of Configuration of an MPLS Network

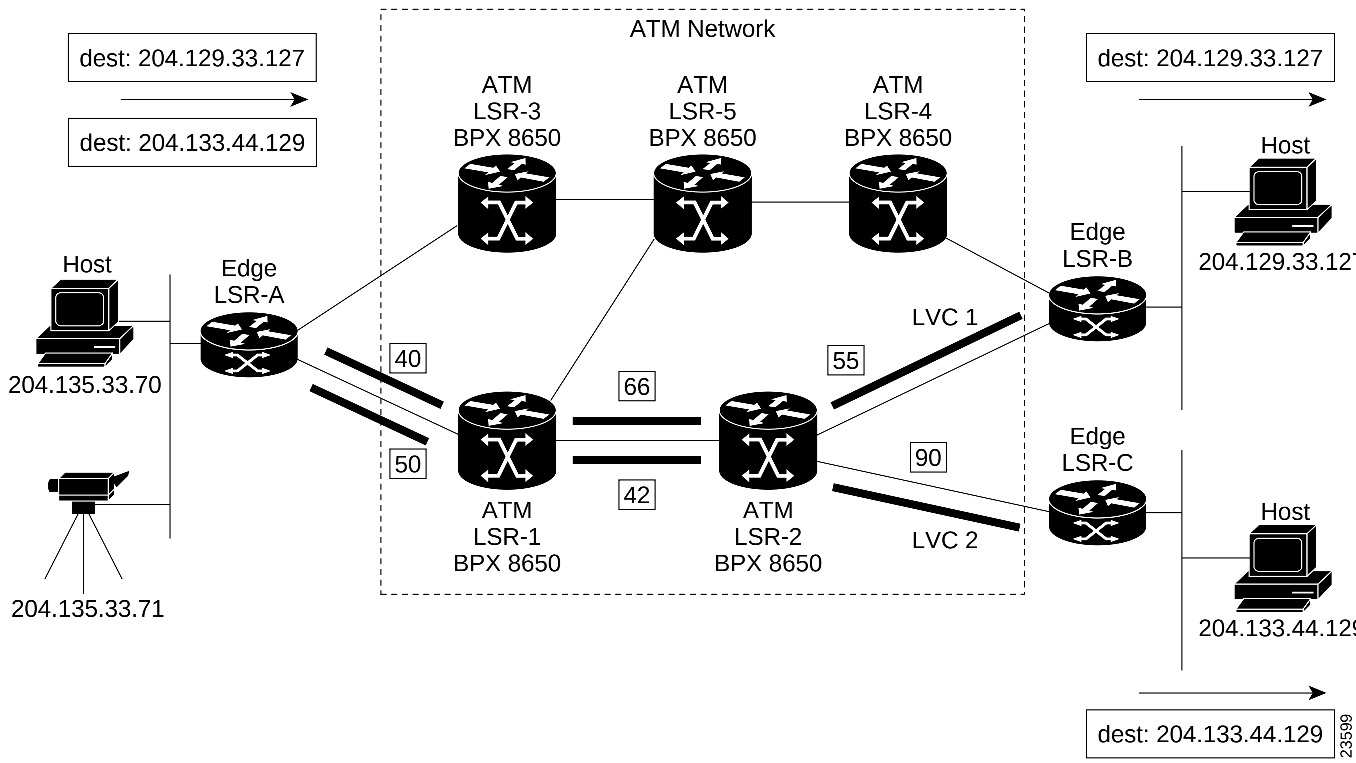
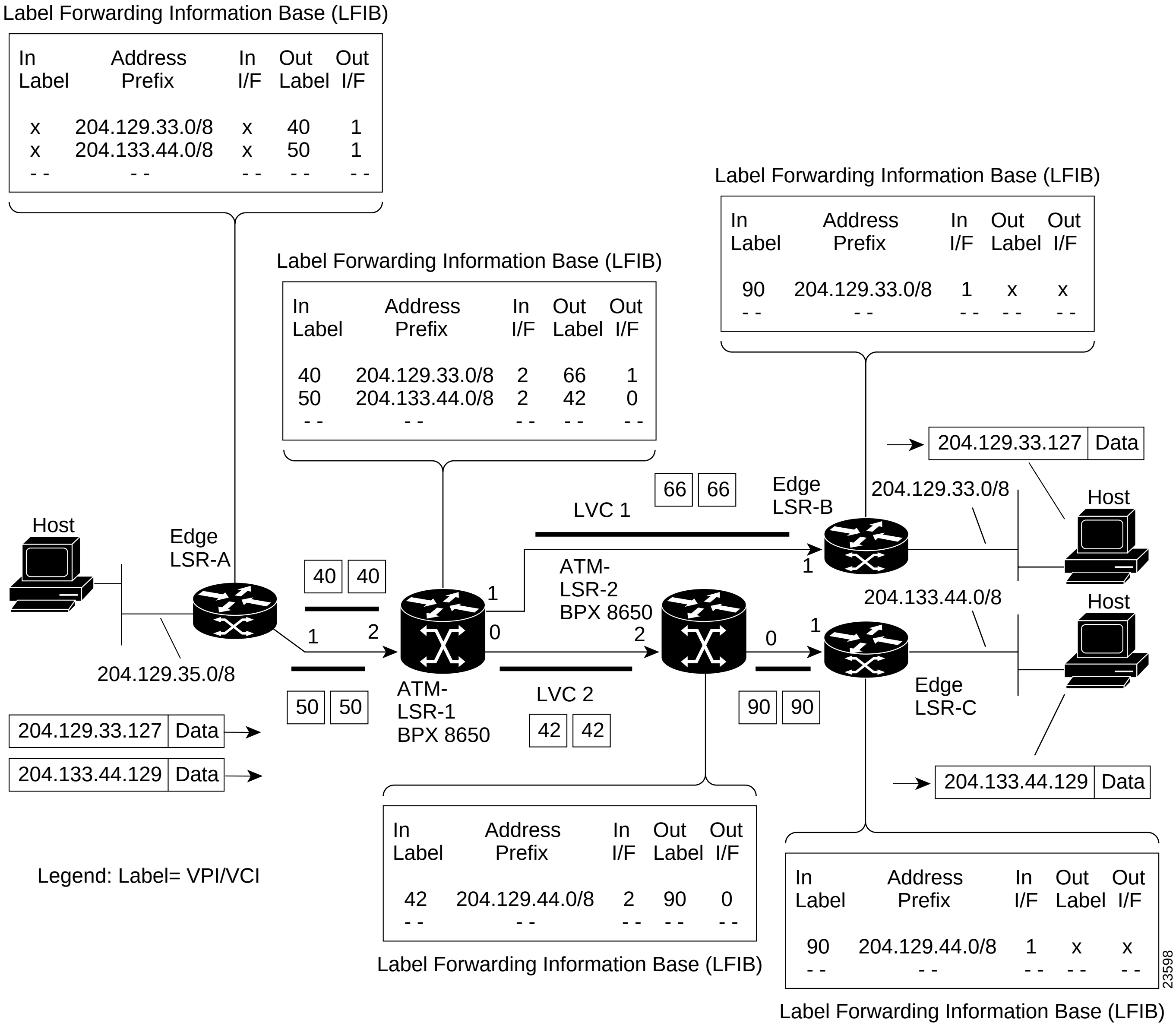


Figure 17-2 is a simplified diagram showing the MPLS label swapping that might take place in the transportation of the IP packets in the form of ATM cells across the network on the LVC1 and LVC2 virtual circuits.

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 17-2 Label Swapping Detail



Initial Setup of MPLS Switching

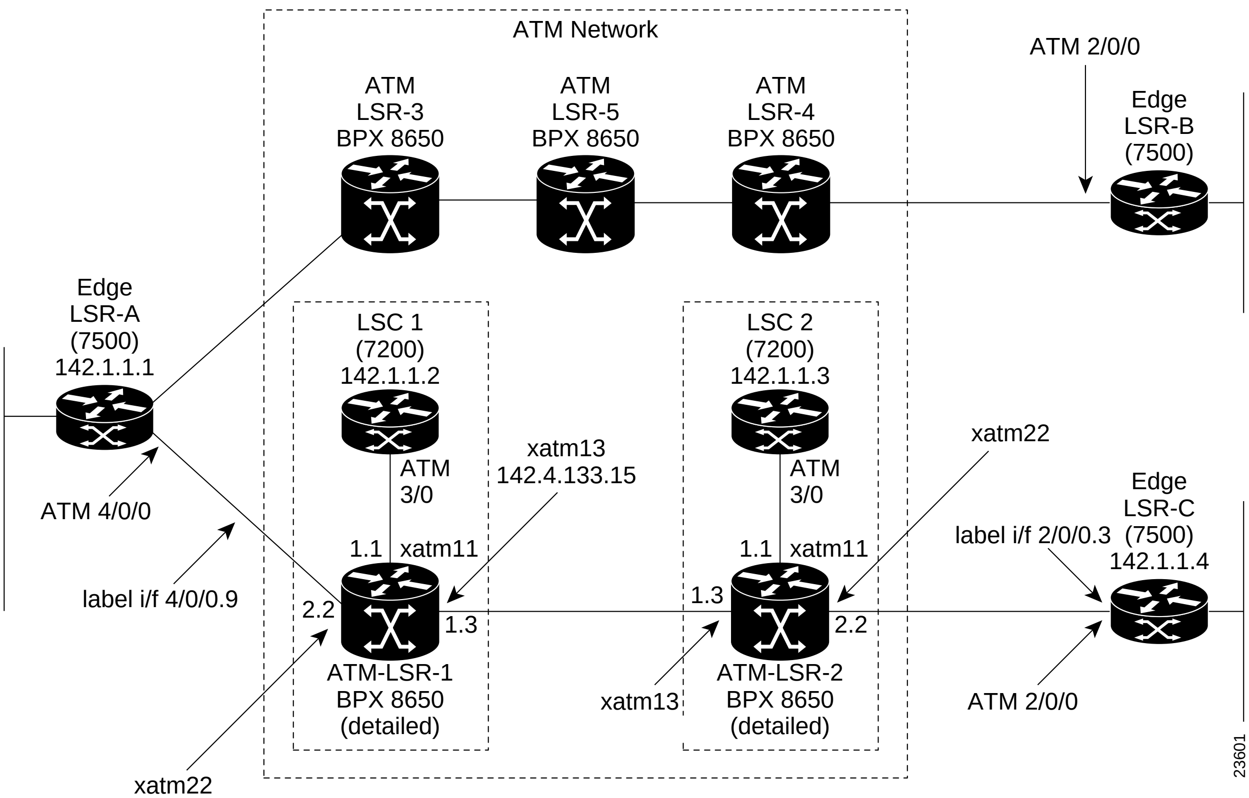
The following provides an example of configuring BPX 8650 MPLS label switches (ATM-LSRs) for MPLS switching of IP packets through an ATM network, along with configuration for 7200/7500 routers for use as Label edge routers (Edge LSRs) at the edges of the network.

See Figure 17-3 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 17-3. 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 (7200 or 7500 router).

Figure 17-3 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.

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.

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, e.g., 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.

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 17-28.

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 17-28.

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	

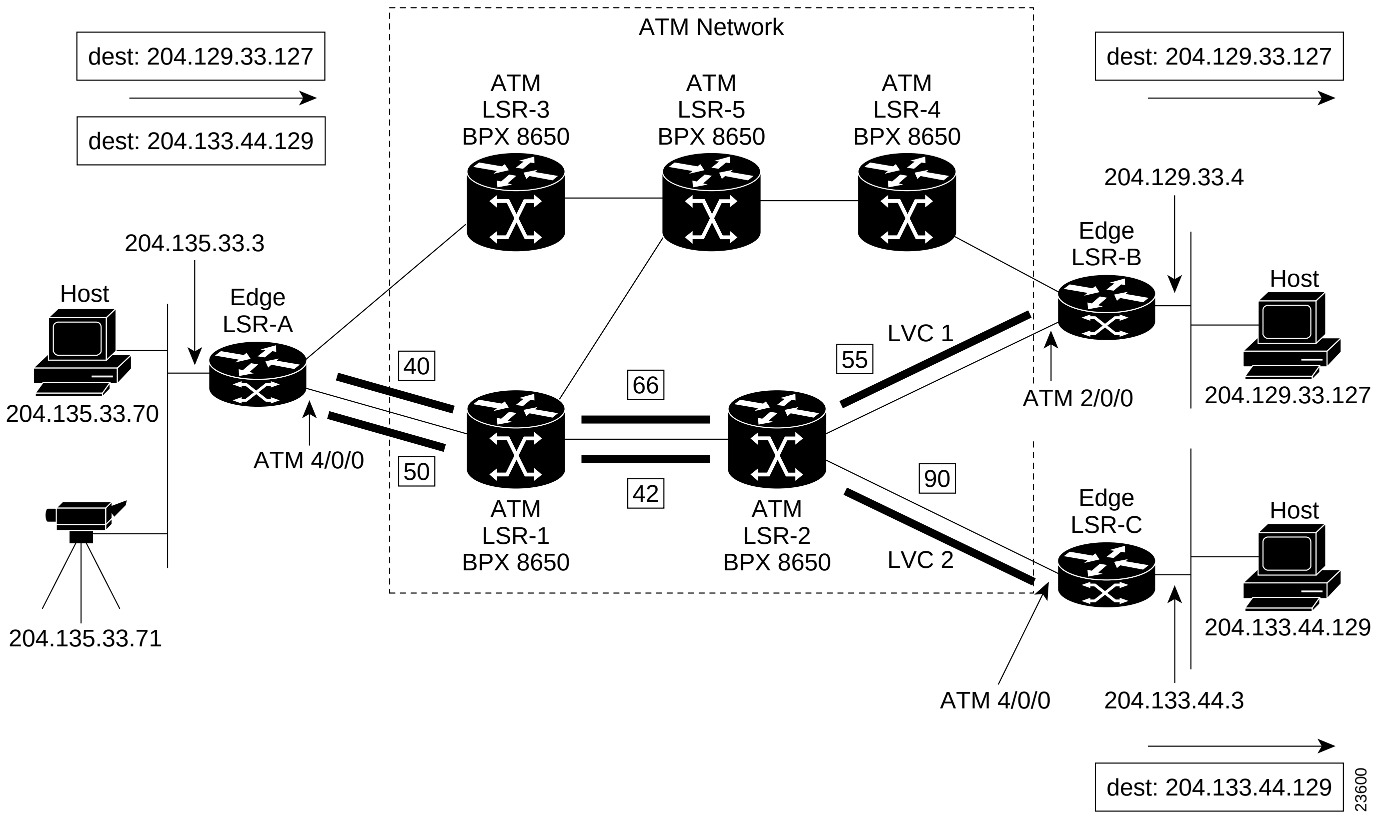
Configuration of Cisco 7500 as an Edge Router, Edge LSR-C

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, e.g., OSPF, sets up the LVCs via MPLS as shown in Figure 17-4.

Figure 17-4 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 tag switch connections. If the ping doesn't work, but all the tag 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 tag (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 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 17-32 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 17-1 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 17-1 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#
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)#

Table 17-1 Cisco IOS Operating Modes (Continued)

Mode of Operation	Usage	How to Enter the Mode	Prompt
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

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 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 18-1 lists these functions and the means by which they are delivered.

Table 18-1 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 Switching 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.

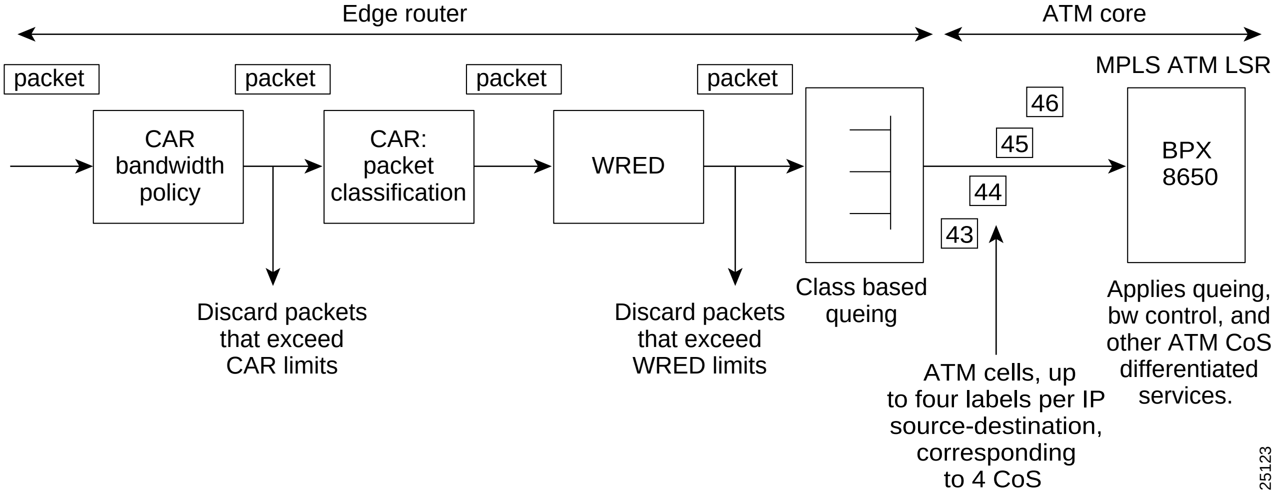
The key to an effective, network-wide IP QoS plan is scalability. Applying QoS on a flow-by-flow basis is not practical because of the huge numbers of IP traffic flows in carrier-sized networks. A scalable way to provide higher levels of service quality with minimal loss in granularity is to implement 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 18-1). 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 18-1 Multiple LVCs for IP QoS Services



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.

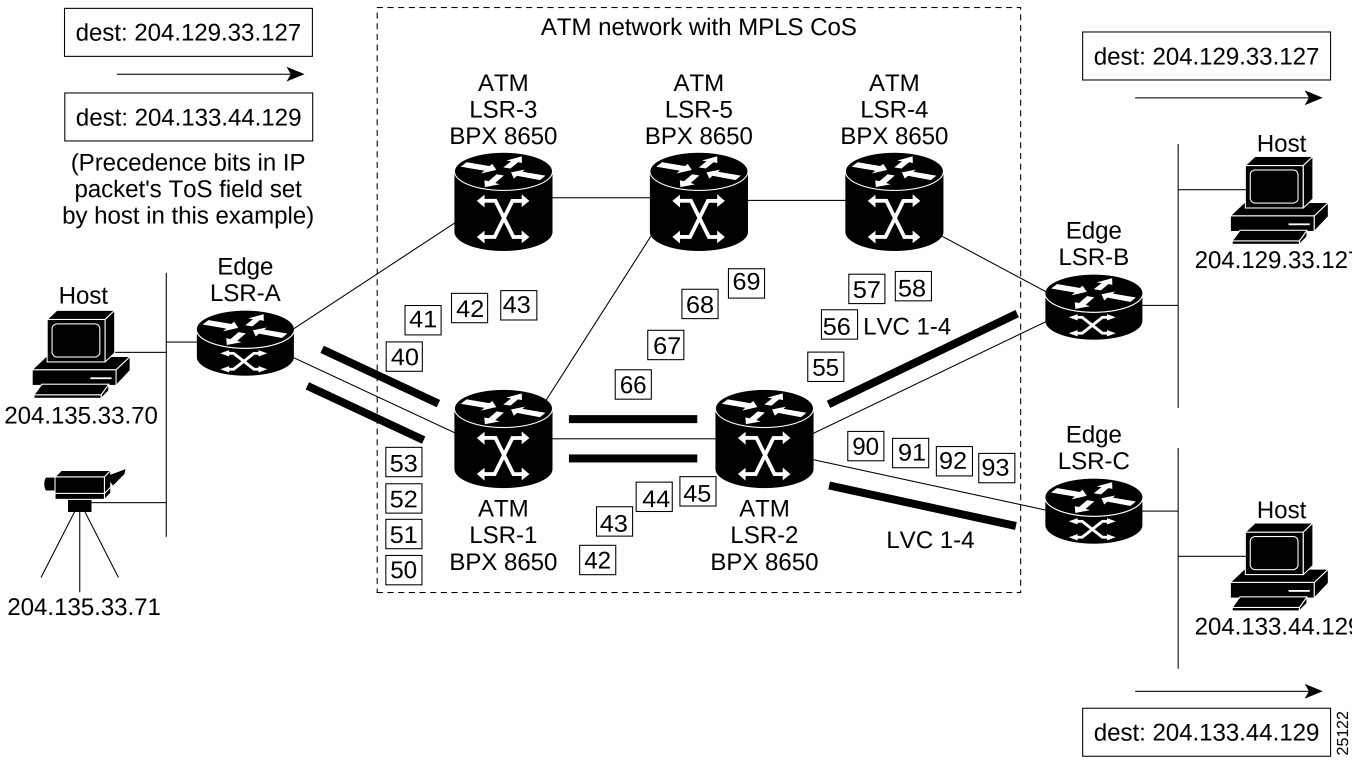
Then the ATM LSR performs a MPLS data table lookup and assigns the appropriate template class of service template and qbin characteristics. The default mapping for CoS is listed in Table 18-2.

Table 18-2 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 18-2 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 18-2 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 (such as, 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 18-3). 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.

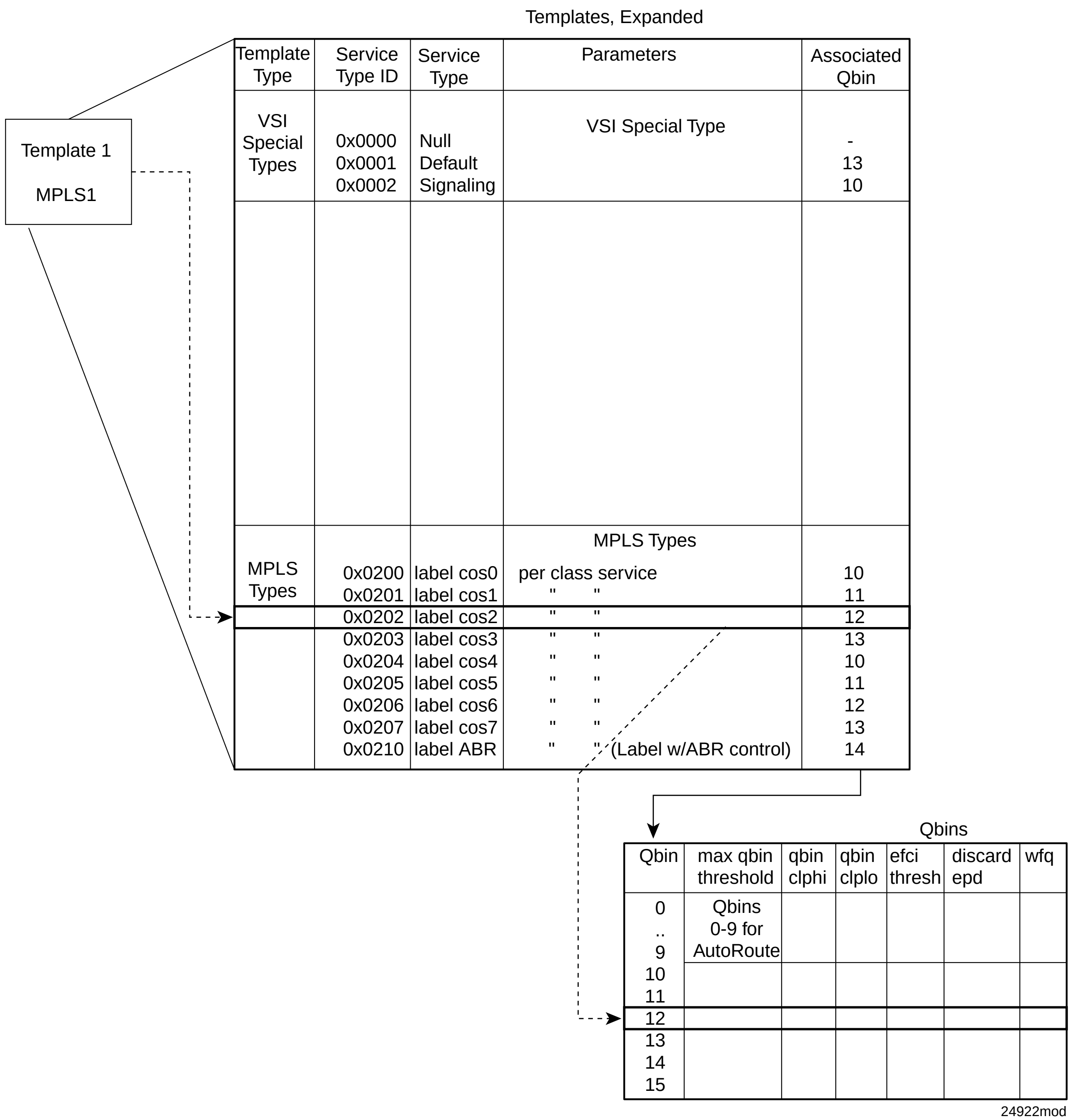
When a connection setup request is received from the VSI master in the Label Switch Controller, the VSI slave (in the BXM, for example) uses the service type identifier to index into a Service Class Template database (Figure 18-3) containing extended parameter settings for connections matching that index. 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 18-3). 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 18-3 Service Template and Associated Qbin Selection



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 18-4), 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 18-4 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.

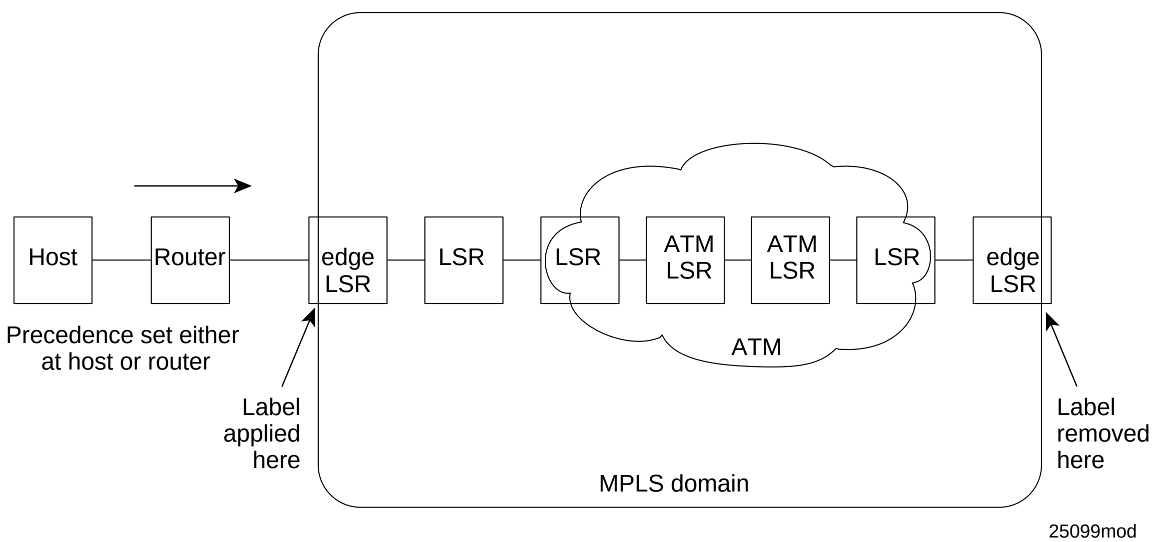
Step 4 Map the MPLS and MPLS CoS bits to an ATM Label-VC in (LSR at edge of ATM cloud).

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 18-4 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 18-3. 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 18-3 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 18-4.

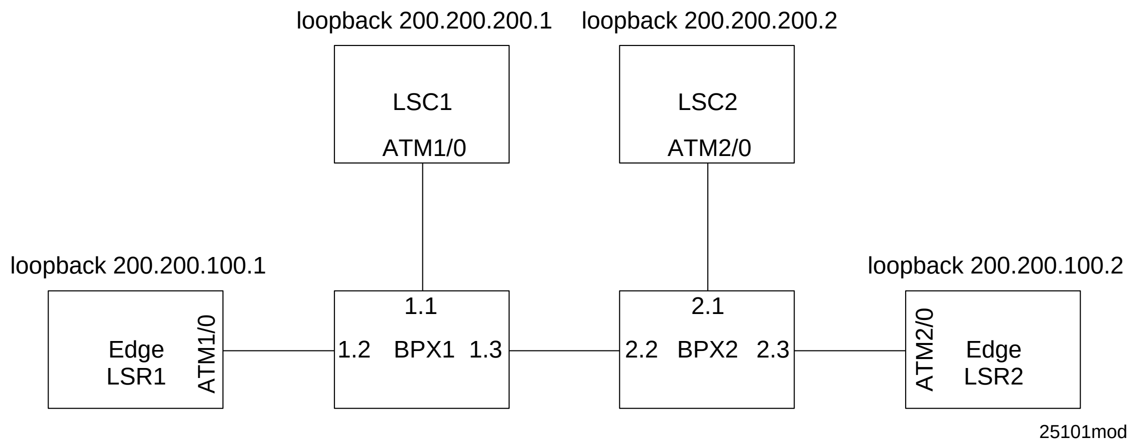
Table 18-4 Class of Service and Relative Bandwidth Weighting Setup

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 18-5.

Figure 18-5 MPLS CoS with BPX 8650 LSRs, Configuration Example



Configuration

Configure the following resources according to the example setup shown in Figure 18-5:

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.

d*sptrks//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
d*sptrks//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

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 Release notes for supported features.

The chapter contains the following:

- Introduction
- MPLS VPN Benefit Summary
- MPLS VPN Features
- MPLS VPN Description
- List of Terms
- Related Features and Technologies
- Related Documents
- Prerequisites
- MPLS Labeling Criteria
- MPLS VPNs over IP+ATM Backbones Description
- MPLS VPN Operation
- Configuration, Example, and Commands
- Configuring the BPX 8650 ATM LSR
- Configuring VRFs
- Configuring BGPs
- Configuring Import and Export Routes
- Verifying VPN Operation

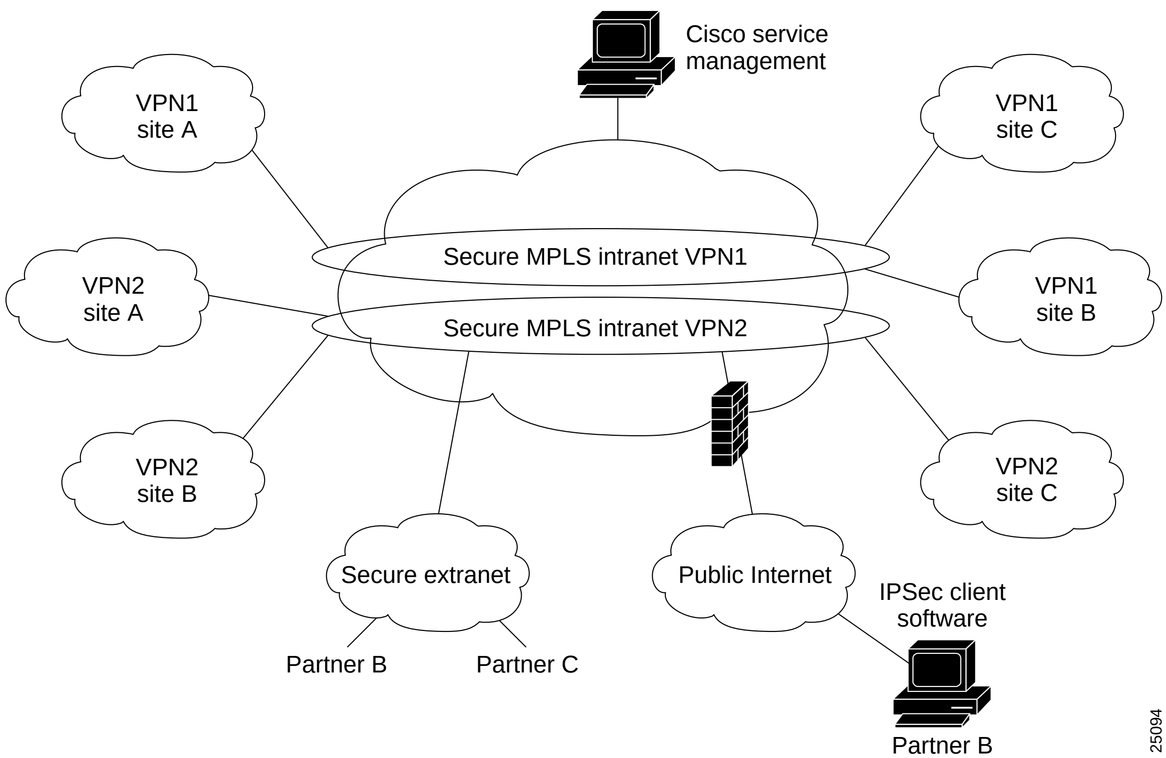
Introduction

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 19-1). 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 19-1 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, and so on., 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

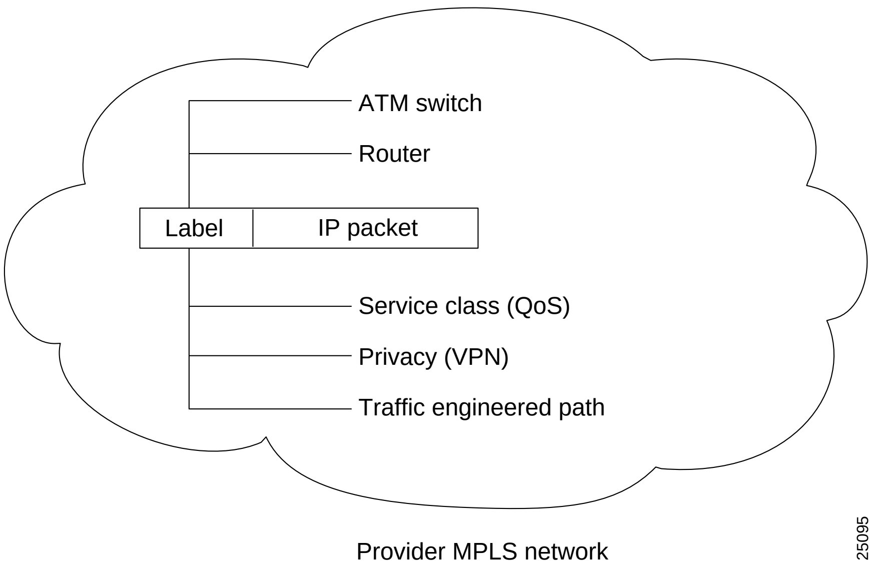
GRE

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 19-2).

Figure 19-2 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.

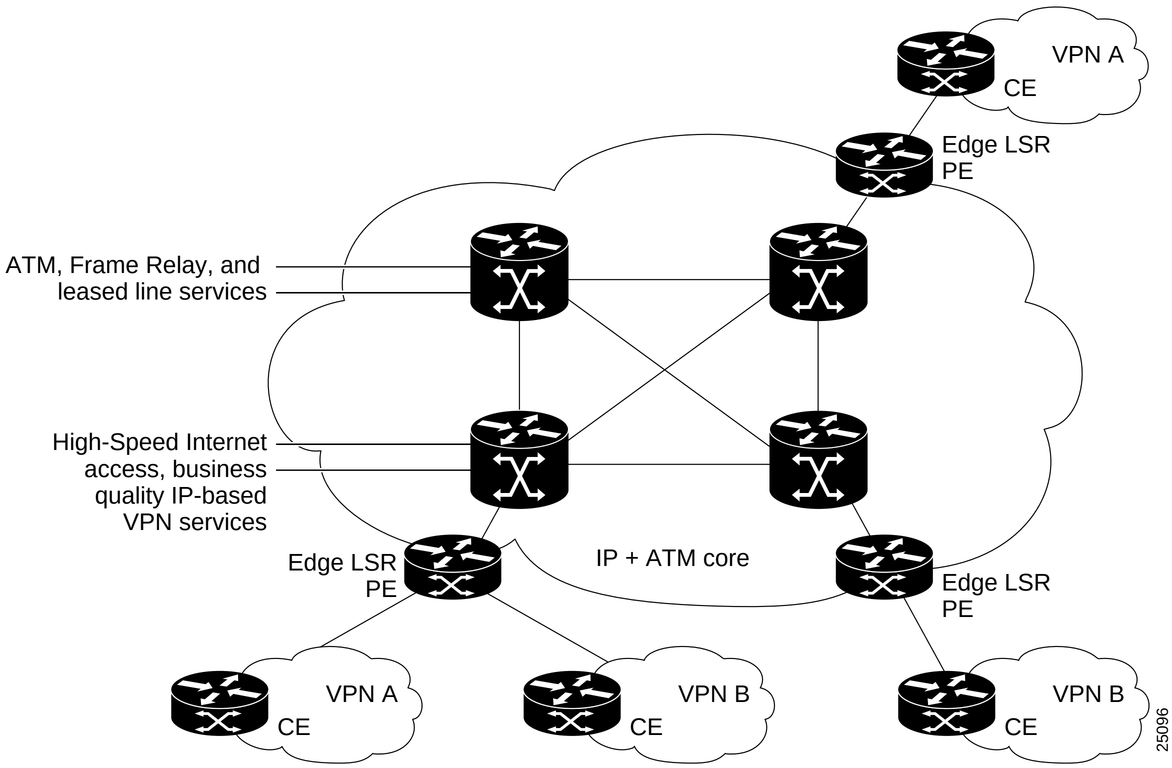
Because MPLS uses different policy mechanisms to assign labels to packets, it decouples packet forwarding from the content of IP headers. Labels have local significance, and they are used many times in large networks; therefore, it's nearly impossible to run out of labels. This characteristic is essential 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 19-3).

Figure 19-3 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 19-4), 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 19-4 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, e.g., 10.x.x.x)

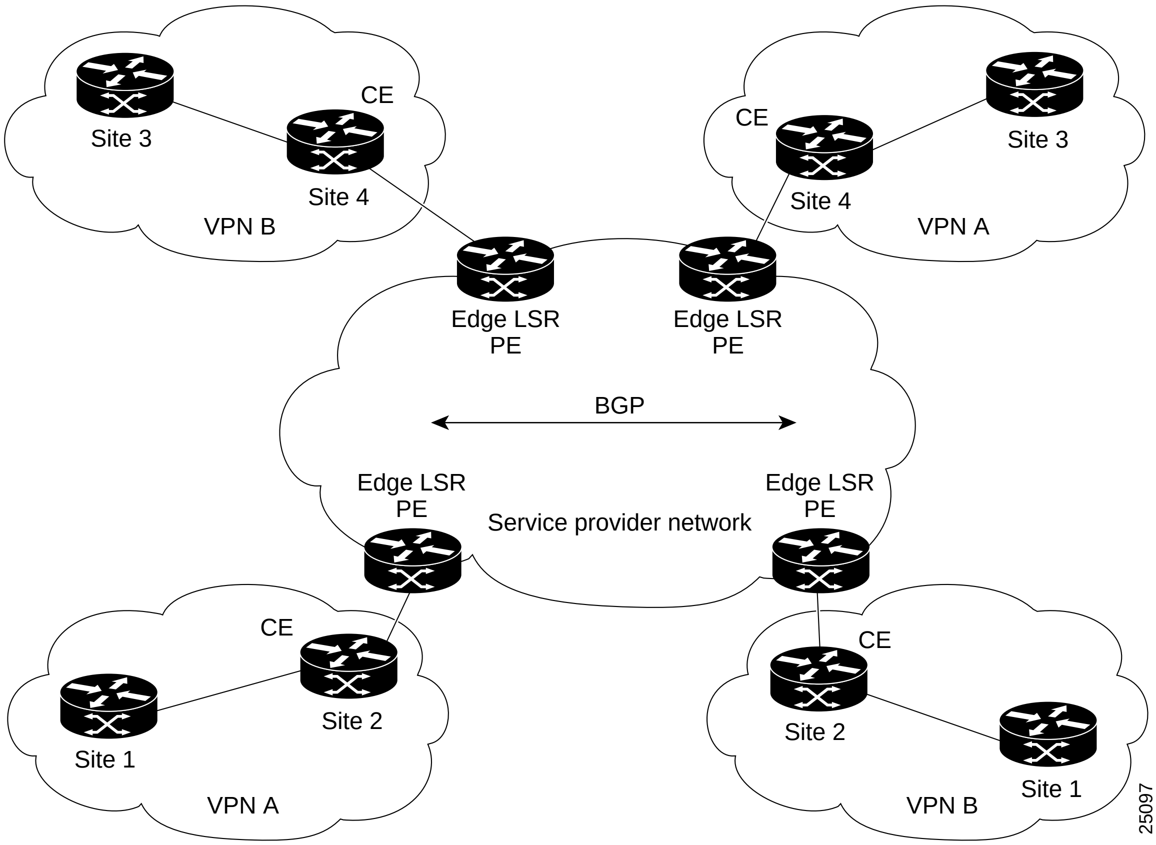
25100mod

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 19-5 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.

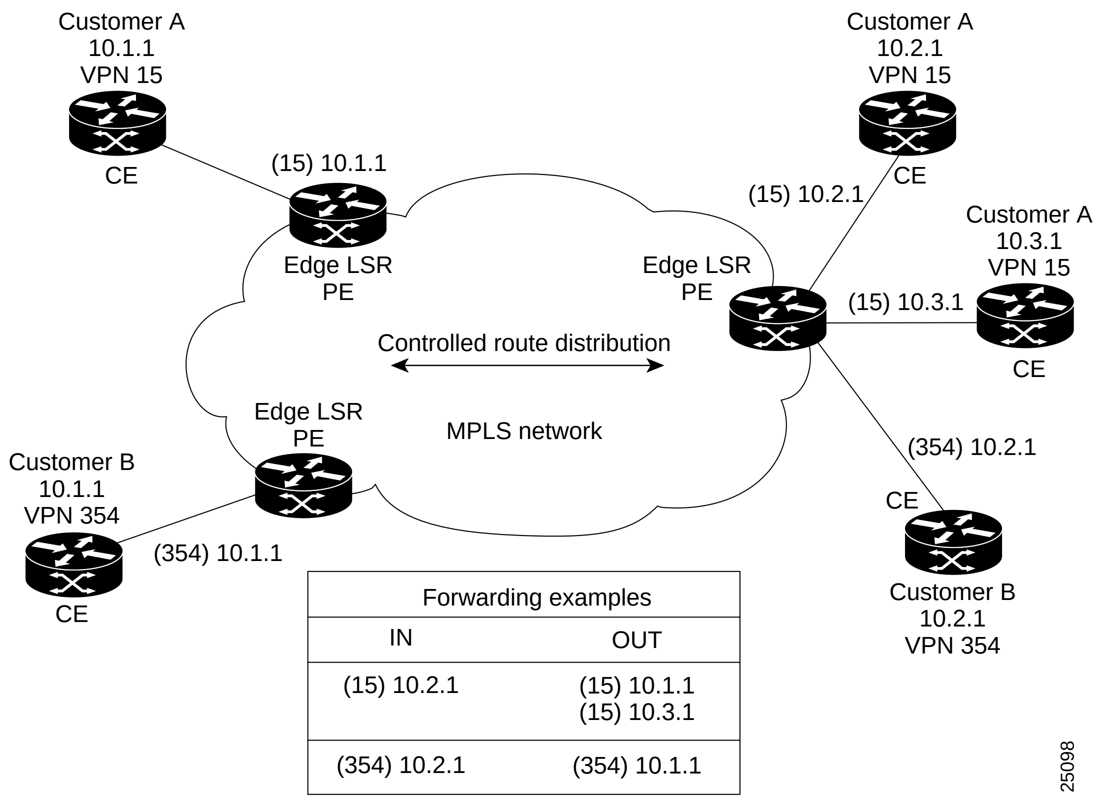
Figure 19-5 VPN with Service Provider Backbone



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 19-6). 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 19-6 Using MPLS to Build VPNs



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 Switching 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

Repair and Replacement

CHAPTER 20

Repair and Replacement

This chapter describes periodic maintenance procedures, troubleshooting procedures, and the replacement of major BPX switch components.

The chapter contains the following:

- Preventive Maintenance
- Troubleshooting the BPX switch
- Replacing Parts

Preventive Maintenance

Most monitoring and maintenance of the BPX switch is done via the BPX switch operating system software. Preventive maintenance of the BPX switch hardware is minimal and requires only the following:

1. Periodically check the node supply voltage and internal cabinet temperature with the **dspasm** command. It should not exceed 50 C.
2. Periodically check the event log with the **dsplog** command.
3. Periodically check the network alarm status with the **dspalms** command.

Troubleshooting the BPX Switch

This section describes basic troubleshooting steps to be taken for some of the more obvious node failures (refer to Table 20-1). This is not an exhaustive set of procedures, and does not take into account any of the diagnostic or network tools available to troubleshoot the BPX switch. Refer to the *Cisco WAN Switching Command Reference* for information on commands and command usage.

Caution Do not perform any disruptive tests or repairs to the BPX switch on your own. Before proceeding with troubleshooting, call Customer Service so they can provide you with assistance in locating the fault and provide repair information.

General Troubleshooting Procedures

The BPX switch runs self tests continuously to ensure proper function. When the node finds an error condition that affects its operation, it downs the card or trunk affected. It then selects a standby card or alternate trunk if one is available.

The FAIL indicators on the cards indicate that the system has found these cards defective in some mode, and now considers them as failed cards. Use Table 20-1 to find the cause and obtain the information on replacing the failed component.

Caution When using Table 20-1 for troubleshooting, call Customer Service before performing any disruptive testing or attempting to repair the BPX switch. This ensures that you have isolated the correct problem area. It also enables Customer Service to provide assistance in performing the necessary procedures.

Warning CContact Customer Service before attempting to replace fuses on backplane and refer to instructions in Replacing Card Slot and Fan Fuses on the System Backplane.

Table 20-1 Troubleshooting the BPX Switch

Symptom	Probable Cause	Remedy
Front panel LED on individual card not lighted.	Card Fuse.	Check card fuse. Replace if defective. Try another card of the same type. If still no LED lighted, backplane card slot fuse may be defective. Refer to Replacing Card Slot and Fan Fuses on the System Backplane.
No front panel LEDs are lighted.	AC Systems: Circuit Breakers on AC Power Supply Tray. DC Systems: Circuit breakers on Power Entry Module(s) switched off.	Switch on circuit breakers. If problem persists, pull all cards and power supplies out to see if a shorted card or supply exists.
	BPX switch power cord plug dislodged from AC receptacle.	Check that no one is working on the system, shut off source breaker, then reconnect power cord.
Power supply **ac** LED lit but **dc** LED not lit.	Power supply defective.	Check DC ok LEDs on ASM. If out, remove and replace power supply. If on, PS LED probably defective.
Card front panel **fail** LED lit.	Card failed self-test.	Check status of card at NMS terminal using **dspcds** screen. If alarm confirmed, try card reset (**resetcd** command). Finally, remove and replace the card.
Card **stby** LED on.	Card is off-line.	Not a problem as long as primary card is active.
ASM **major** or **minor** LED on.	Service-affecting (major) or non-service affecting (minor) system fault.	Check NMS event log to identify problem reported.
	Failed card in local node.	See remedy for card **fail** LED indication.
	Network trunk failed.	Observe **Port** LEDs on each BNI or BXM (ports configured in trunk mode). Use NMS **dsptrk to** locate failure.
	Failure in remote node. May be another BPX switch or an IPX switch.	Use NMS **dspnw** screen to locate node in alarm. Refer to *Cisco WAN Switching Command Reference* for additional information.
	Internal temperature is higher than normal resulting from blocked air flow or defective fan.	Check front and back of node cabinet for freedom of air flow. Replace any fan that may have failed or slowed. Use NMS dsppwr screen to check node temperature.
ASM **hist** LED lit.	If no other alarm indications, a fault occurred in the past but has been cleared.	Press ASM **history clear** button. Check NMS event log to determine cause.

Table 20-1 Troubleshooting the BPX Switch (Continued)

Symptom	Probable Cause	Remedy
BXM **Port** LED is red or orange (BXM configured for trunk mode).	Trunk is in local or remote alarm.	Use NMS **dsptrk** screen to confirm trouble.
BNI **Port** LED is red or orange.	Trunk is in local or remote alarm.	Use NMS **dsptrk** screen to confirm trouble. Use short BNC loopback cable at LM-BNI connectors for local test of trunk. Loop trunk at DSX-3 crossconnect to check cable.
No BXM **card** or **port** LED on.	No trunks or lines, as applicable on card are upped. Card has not necessarily failed.	Up at least one of the trunks or lines, as applicable, associated with the card (Trunks if BXM configured for trunk mode, lines if BXM configured for port mode).
No BME **card** or **port** LED on.	No lines are upped. Card has not necessarily failed.	Up at least one of lines, as applicable, associated with the card.
No BNI **card** or **port** LED on.	No trunks on card are upped. Card not necessarily failed.	Up at least one of the trunks associated with the card.
BXM **Port** LED is red or orange (BXM configured for port mode)	Line is in local or remote alarm.	Use NMS **dsplns** screen to confirm trouble.
BME **Port** LED is red or orange	Line is in local or remote alarm.	Use NMS **dsplns** screen to confirm trouble.
ASI **Port** LED is red or orange.	Line is in local or remote alarm.	Use NMS **dsplns** screen to confirm trouble.
No ASI **card** or **port** LED on.	No lines on card are upped. Card not necessarily failed.	Up at least one of the two lines associated with the card.
BCC **fail** LED flashing	Downloading system software or configuration data.	Wait for download to complete.
BCC **LAN** LED flashing	Normal for node connected to NMS terminal over Ethernet. If it does **not** flash, there may be problems with node to NMS data path.	Check that the cabling to the NMS is firmly connected to the LAN port on the LM-BCC back card. An alternate connection is to the control port.
No BCC card LED on.	Preparing to download new software (momentary condition).	Wait for download to begin.
	Command issued to run a software rev. that was not available in the network.	Check that proper s/w rev. is available on another node or on NMS.

Displaying the Status of Cards in the Node

When a card indicates a failed condition on the alarm summary screen, use the Display Cards (**dspcds**) command to display the status of the circuit cards on a node. The information displayed for each card type includes the card slot number, software revision level, and the status of the card. The possible status description for each card type are listed in Table 20-2. Refer to the *Cisco WAN Switching Command Reference* for more information on the Display Cards command.

Table 20-2 Card Status for the BPX Switch

Card Type	Status[1]	Description
All card types	Active	Active card.
	Active - F	Active card with no terminal failure.
	Standby	Standby card.
	Standby - F	Standby card with no terminal failure.
	Standby - T	Standby card performing diagnostics.
	Standby - F -T	Standby card with no terminal failure performing diagnostics.
	Failed	Card with terminal failure.
	Unavailable	Card is present but it may be in one of the following states: a. The node does not recognize the card. b. The card is running diagnostics.
	Down	Downed card.
	Empty	No card in that slot.
BCC	Same status as for all card types, plus:	
	Updating	Standby BCC downloading the network configuration from an active BCC. Note: Red FAIL LED flashes during updating.
	Cleared	BCC is preparing to become active.
	Downloading Software	There are downloader commands that appear when the system is down- loading software to the BCC.
	Minor	BCC Redundancy alarm indicates node is configured for redundancy but no standby BCC is equipped.

1. Cards with an F status (no terminal failure) are activated only when necessary. Cards with a failed status are never activated.

Replacing Parts

After an alarm occurs, use the BPX switch software to isolate the problem. If an BPX switch part has failed, then it must be replaced.

Caution Only authorized personnel should remove and replace parts on the BPX switch system.

Parts should be replaced only by qualified personnel who have taken the Cisco training courses or been trained by a qualified system manager. For assistance in diagnosing or replacing a failed part, call Customer Service.

When replacing a part, save the electrostatic bag, foam, and carton that the new part comes in. These packaging materials are needed for returning the failed part to Cisco. Contact Customer Service for information on returning parts.

Replacing a Front Card

The BPX switch front cards are as follows:

- Broadband Controller Card (BCC)
- BXM-T3/E3, BXM-155, BXM-622
- Broadband Network Interface Card (BNI)
- Alarm and Status Monitor (ASM)
- Access Service Interface (ASI-1)

Caution Ground yourself before handling BPX switch cards by placing a wrist strap on your wrist and clipping the wrist strap lead to the cabinet.

When a card has failed, the red FAIL indicator for that card turns on. Before replacing it, check to see if the card only needs to be reseated. After reseating the card, wait for it to run its self-tests to see if the ACTIVE light comes on. If the card is seated correctly, but the FAIL light is still on, replace the card.

To remove a front card, perform the following steps:

Step 1 If the front panel **fail** lamp is on, remove the card and go to Step 3. Otherwise, go to Step 2.

Step 2 Check the status of the card using the **dspcd** or **dspcds** commands. It should be failed or standby if the node is actively carrying traffic.

Step 3 If an active card (ASI, BNI) needs to be replaced, "down" it first with the **dncd** command. Removing an active card affects operation only slightly if there is a standby card.

Step 4 If a BCC has failed, the other BCC will switch from standby mode to active. Use the **dspcd** command to verify that the standby BCC has entered the active mode. Then you can remove the failed BCC.

Caution Never remove the active BCC until the standby BCC has entered the "active" mode. Using the **dspc**d command is the only reliable way to determine that the standby BCC has finished updating and has entered the "active" mode.

Step 5 Unlatch the Air Intake Grille. Locate the small access hole in the top, center of the Air Intake Grille.

Step 6 Fully insert a medium, flat-bladed screwdriver in the access hole.

Step 7 Rotate the screwdriver to release the spring latch holding the grille. (Figure 20-1). The top of the grille should pop out.

Step 8 Tilt the grille forward to approximately a 45 angle.

Step 9 Put on a wrist strap to discharge any static.

Step 10 Rotate the top and bottom card extractors on the front of the card.

Step 11 Hold the card at the top and bottom and gently slide it out of the slot.

To install a front card in the BPX switch, perform the following steps:

Step 1 Unlatch the Air Intake Grille as described in Step 5 through Step 8 of the previous procedure for removing the front card.

Step 2 Remove the replacement card from the antistatic shipping container.

Step 3 Hold the replacement card at top and bottom and gently insert it over the guides, and slide it all the way to the rear of the cabinet.

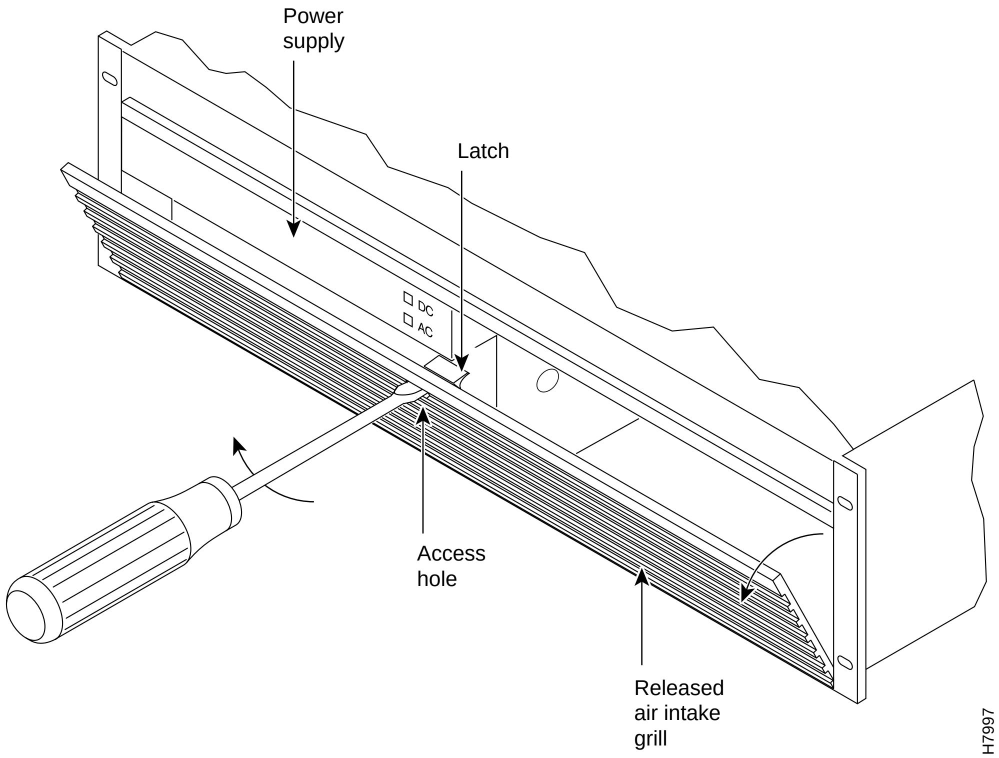
Note The card should slide in easily with a light sliding friction from the EMI gaskets on adjacent cards. If it does not, check to see if there is anything restricting it—do not use excessive force.

Step 4 Rotate the top and bottom latches on the card and push the card into the rear connector. You will feel the card seat itself as you push it in.

Step 5 Press firmly on the top and bottom extractors to complete the card seating process. The extractor should snap back to a vertical position after the card is properly seated.

Step 6 Replace the air intake grille by swinging it up and pressing in at the top until the latch snaps into place.

Figure 20-1 Unlatching the Air Intake Grille



Replacing a Line Module

The configuration of the back card may be slightly different depending on whether it is a single card or redundant card configuration. A standby card in a redundant card configuration may be removed without disrupting system operation even if it is a BCC. Removing a single card, however, will cause a system outage.

Caution Removing an active, single back card disrupts service on the node.

To remove a line module, perform the following steps:

Step 1 Check the status of the card using the **dspcd** or **dspcds** command. It should be failed or standby or replacement will affect operation of the node.

Step 2 If an active card needs to be replaced, "down" it first with the **dncd** command. Removing an active card affects operation only slightly if there is a standby card.

Step 3 Before removing a LM-BCC, make sure the standby BCC **stby** indicator is on steady. A flashing **stby** indicator indicates it is in the process of downloading either configuration data or software and is not ready to accept a transfer.

Step 4 For a single card configuration, disconnect the cables from the back card face plate. Make a note of the location of each cable so that it can be replaced correctly.

Step 5 For a redundant card configuration, disconnect the appropriate leg of the Y-cable connecting to the back card to be replaced. DO NOT REMOVE THE OTHER LEG GOING TO THE BACKUP CARD.

Step 6 Loosen the two captive screws on the back card faceplate and, pulling on the top and bottom card extractors, slide the card straight out of the shelf slot. (See Figure 20-2.)

To install a line module, perform the following steps:

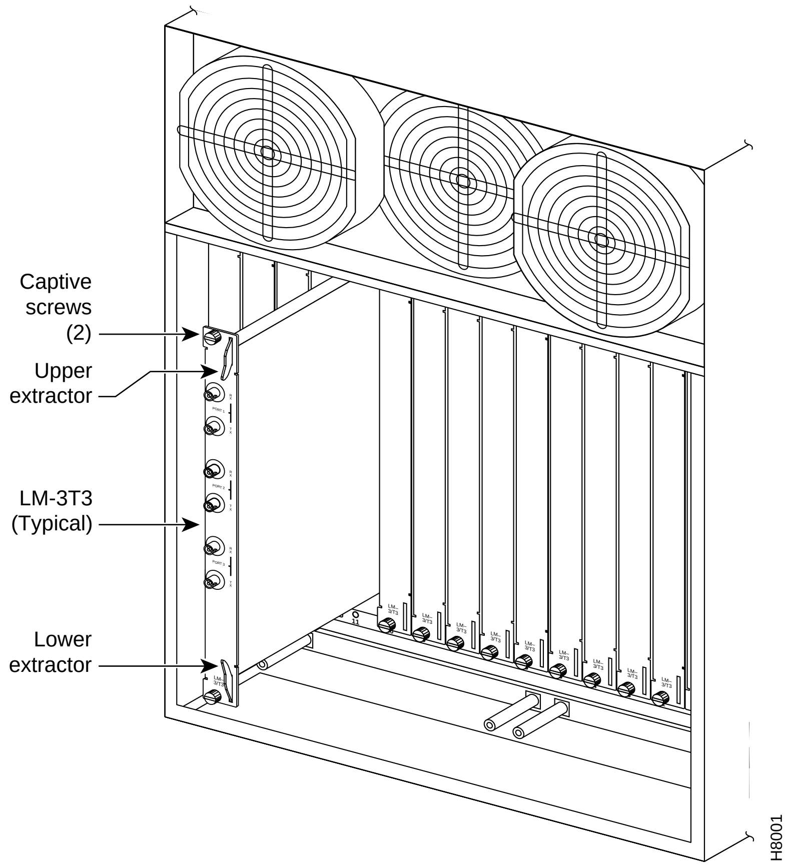
Step 1 Insert the line module (such as, LM-3T3) into the slot from which the defective card was removed (see Figure 20-2).

Step 2 Tighten the two captive screws. (Tighten securely, but do not overtighten.)

Step 3 Reconnect the T3 trunk cables to the LM-3T3 connectors from which they were disconnected.

Step 4 Perform the appropriate steps to bring the lines that were disconnected back on line.

Figure 20-2 Removing a Line Module



Replacing a DC Power Entry Module

DC Power Entry Modules (PEMs) contain few active components so they should rarely need replacement. Access is from the back of the node. To remove a PEM, proceed as follows:

Step 1 Check the node system voltage by using the Display Power (**dsppwr)** command. Note which input has failed, A or B. Power Supply A is the unit on the right side facing the rear of the node.

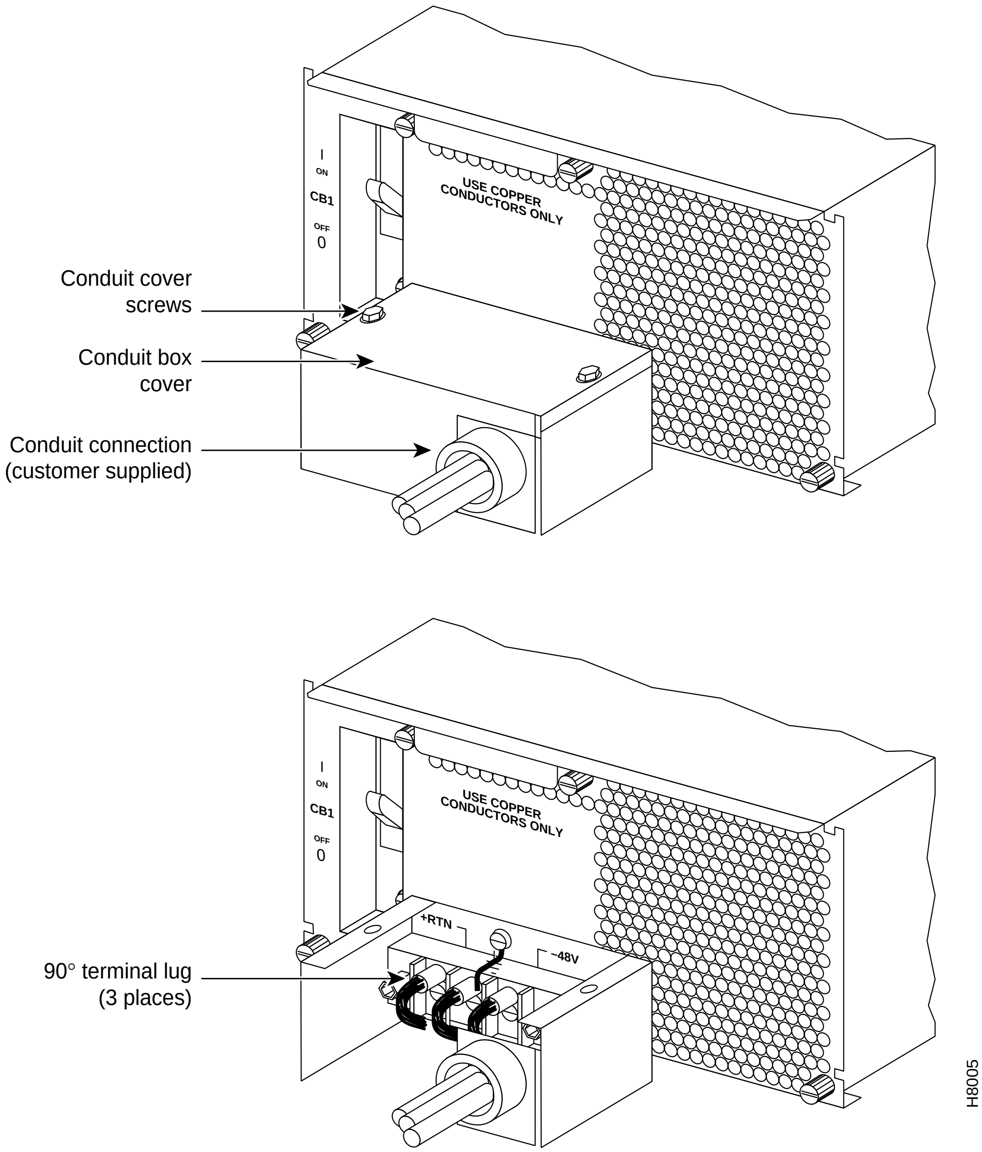
Step 2 Turn off the primary source of power to the PEM to be replaced.

Step 3 Turn off the circuit breaker on the PEM to be replaced.

Step 4 Remove the two screws holding the conduit box cover (see Figure 20-3). Or, remove the plastic cover plate over the input terminal block.

Step 5 Remove the power input wiring at the PEM terminal block.

Figure 20-3 DC Power Entry Module with Conduit Box



Step 6 If a conduit box is used, remove it. Remove the ground screw above the middle terminal block connector (see Figure 20-3).

Step 7 Remove the two standoffs on each side of the terminal block and pull the conduit box straight back. Set it aside. Do not try to remove the terminal block.

Step 8 Loosen the two captive screws (at the bottom corners) holding the PEM. Loosen the two connector jackscrews adjacent to the finger pull.

Step 9 Grasp the finger pull lip at the top of the PEM and pull the unit straight out.

Step 10 Replacement is the reverse of removal.

Replacing an AC Power Supply

BPX switches are powered by redundant power supplies; either power supply can supply the current requirements of the node. The AC Power Supply is part of an assembly which is replaced as a single unit. Access to the AC Power Supply assembly is from the front, but first, the Air Intake Grille must be removed.

To remove a power supply, proceed as follows:

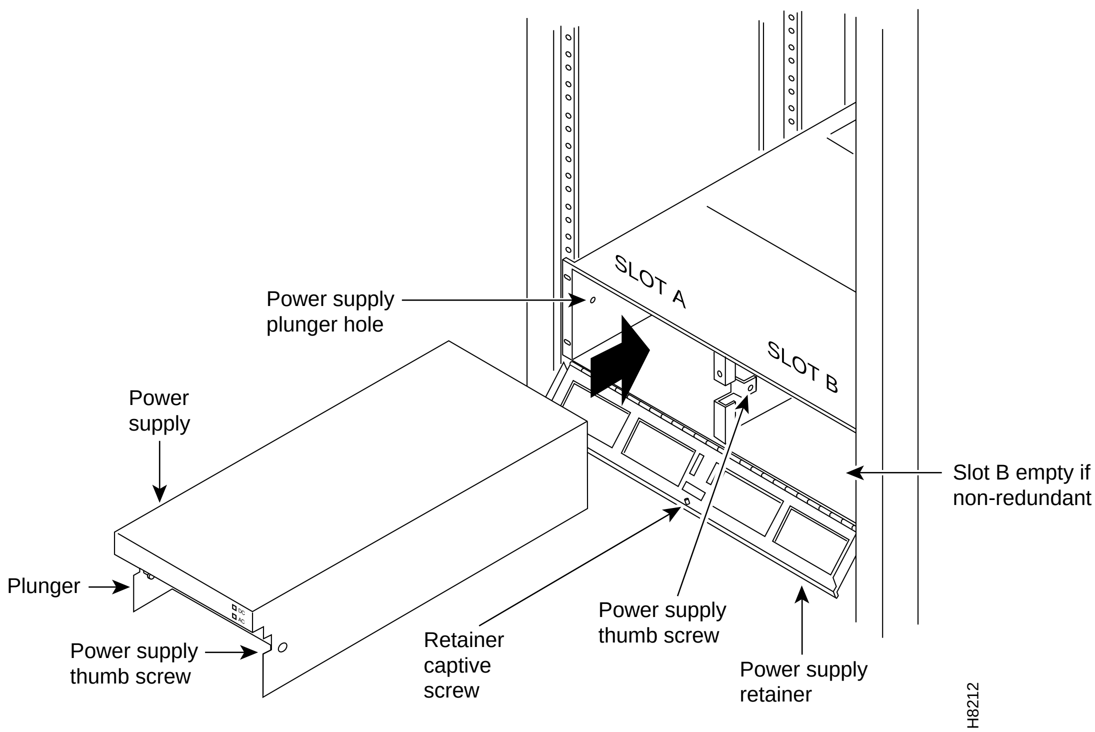
Step 1 If you haven't already done so, check the status and output voltage of the power supplies at the node using the **dspasm** command. Note which power supply is failed, A or B. Power supply A is on the right side facing the rear of the node.

Step 2 Remove the Air Intake Grille. Locate the small access hole in the top, center of the Air Intake Grille.

Step 3 Fully insert a flat-bladed screwdriver (with a 1/4 in. blade) in the access hole.

Step 4 Rotate the screwdriver to release the spring latch holding the Air Intake Grille (see Figure 20-4). The grille should pop out.

Figure 20-4 AC Power Supply Assembly



Step 5 Tilt the grille forward approximately a 45 angle, then lift if out and set it aside. This exposes the power supply retainer bracket.

Step 6 With a flat-bladed screwdriver, loosen the retainer bracket hold-down screw in the center of the bracket and tilt the bracket.

Step 7 Identify which power supply needs replacement. Power supply A is the unit on the left, B is on the right. In most cases, the failed unit will be identified by a front panel lamp indication.

Step 8 There are two power supply securing fasteners, one on each side of the power supply assembly (Figure 20-4). The one on the left of each supply is a spring-loaded pin, the one on the right of each supply is a normal thumb-screw. Loosen the thumb-screw on the right.

Step 9 With the right hand, grip the power supply under the front panel. With the left hand, pull out the spring-loaded pin on the left side of the supply and hold it out as you pull out the power supply assembly.

Step 10 The power supply assembly weighs approximately 15 pounds (33 Kgs.). Support the bottom of the power supply as you pull it straight out, until it is free of the shelf.

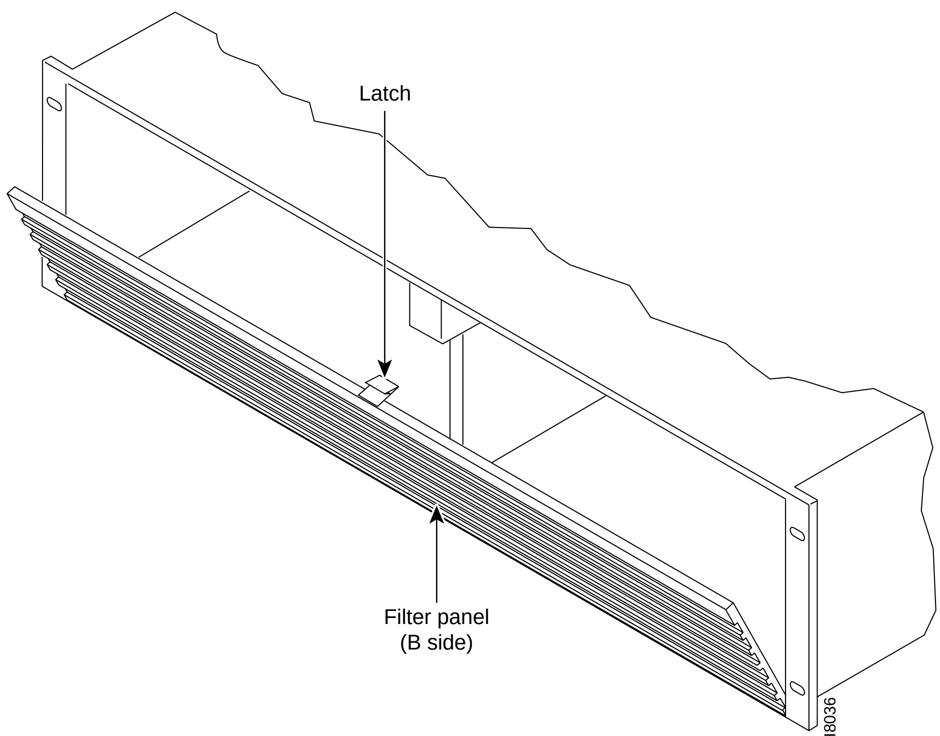
Field-Installing a Second AC Power Supply

To field-install a redundant power supply, perform the following steps:

Step 1 If the front Air Intake Grille has already been removed, go to the next step. If not, remove it using Step 2 through Step 6 of the previous procedure.

Step 2 If converting a node from single to redundant powering, first remove the blank filler panel over position B (right side). With Air Intake Grille open, remove three screws attaching the filler panel to the retainer bracket (see Figure 20-5).

Figure 20-5 Removing Blank Filler Panel (B side shown)



Step 3 Slide a replacement power supply assembly into the tracks of the power supply shelf.

Step 4 When the power supply is completely seated, the spring-loaded pin will snap into place to assure that the power supply has mated with its connector.

Step 5 Screw in the thumb-screw on the right side of the power supply assembly until it is finger tight.

Step 6 Flip the retaining bracket up and tighten its thumbscrew.

Step 7 Reinstall the Air Intake Grille and press firmly on the top, center of the Air Intake Grille until the latch snaps into place.

Step 8 Check the status and output voltage of the replacement power supply using the **dspasm** command. Make sure the status is OK and the output voltage is 48V.

Replacing the Fan Assembly

The Fan Assembly provides the primary cooling for the BPX switch and is located at the top, rear of the BPX switch cabinet. There are three fans in the Fan Assembly. The fan on the right (number 1) and the one on the left (number 3) can be changed out individually with very little effort or interruption in the operation of the node. The fan in the middle (number 2) requires powering down the node and removing the Fan Assembly to replace.

Caution You must work quickly but carefully to prevent heat buildup in the node which could damage the cards.

To replace fan number 1 or number 3 in the Fan Assembly, perform the following steps:

Step 1 Use the **dspasm** command to check the status of the three fans.

Step 2 From the rear of the BPX switch, visually check that the fan(s) is indeed not turning or turning slowly.

Step 3 From the back of the cabinet, unplug the small fan power cord from its appropriate receptacle on the Fan Assembly.

Step 4 Remove the two screws holding the fan and the fan shield to the-fan housing. Be careful not to drop the hardware into the rear of the cabinet.

Step 5 Remove the fan. Replace the fan in reverse order. Use the existing fan grille.

To replace fan number 2 requires powering down the node and replacing the whole Fan Assembly. Under normal ambient room temperatures, this can be scheduled for the next available quiet time. Perform the following steps:

Step 1 Use the **dspasm** command to check the status of the three fans.

Step 2 From the rear of the BPX switch, visually check that fan number 2 is not turning or turning slowly.

Step 3 At the rear of the BPX switch, turn the circuit breaker(s) OFF to power down the node.

Step 4 Loosen the eight captive screws holding the Fan Assembly in place.

Step 5 With one hand, pull the Fan Assembly back just far enough to gain access to the Fan Assembly power cord. This cord connects to the Fan Assembly to the backplane.

Step 6 Unplug the power cord and remove the Fan Assembly.

Step 7 Plug the power cord in the replacement Fan Assembly into the backplane connector.

Step 8 Install the replacement Fan Assembly.

Step 9 Tighten the eight screws holding the Fan Assembly in place.

Replacing the Temperature Sensing Unit

The temperature sensing unit is located on the ASM card. If the temperature indication using the **dspasm** command does not appear to be correct, try a replacement ASM card.

Replacing Card Slot and Fan Fuses on the System Backplane

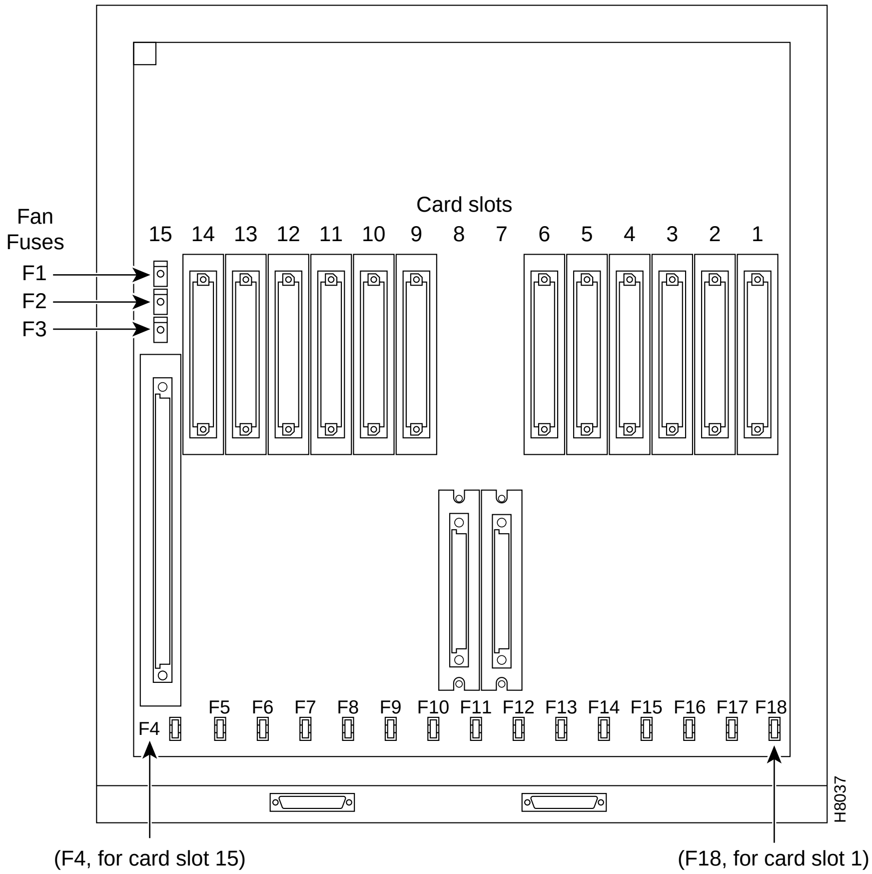
There is a separate fuse provided on the System Backplane for each card slot. These fuses are numbered F4 through F18, corresponding to card slots F15 down through F1 (see Figure 20-6). There are three separate fan fuses provided on the System Backplane. These fuses are numbered F1 through F3, corresponding to Fans 1 through 3 (see Figure 20-6).

Warning For both personnel safety and to prevent equipment damage, power down the BPX switch before replacing fan fuses F1 through F3, or card slot fuses F4 through F18 on the System Backplane. For continued protection against risk of fire, replace only with same type and rating of fuse.

Backplane fuses rarely need replacement. Backplane fuses are intended to prevent catastrophic damage to the backplane in the event of accidental shorting of -48VDC on the backplane to chassis ground. This type of event could be caused by bent backplane pins, inadvertent contact of conductive elements (EMI Cans, EMI Gaskets, etc.) to power pins, or (in the case of a fan fuse) a pinched wire harness.

These fuses are located in sockets on the backplane and are therefore not readily accessible. A special tool and a special set of instructions are required for fuse replacement. It is recommended that only factory-trained personnel perform the procedure. Contact Customer Service for further information.

Figure 20-6 Card Slot and Fan Fuse Locations on System Backplane



PART 7

Reference

BPX Node Specifications

This appendix lists information for the BPX system specifications. (Refer to on-line documents for latest information).

General

System Capacity:	1 shelf with 15 card slots. Requires 1 or 2 dedicated slot(s) for BCC card. Requires 1 dedicated slot for ASM card.
Network Interface:	T3, E3, OC3, and OC12.
Network Trunks:	32 per node max.
Network Interface Protocol:	ATM layer using 53-byte cell.
Cell Switching:	Crosspoint switch matrix, non-blocking.
Switch Capacity:	9.6 Gbps or 19.2 Gbps (with BCC-4).
Slot Rate:	800 Mbps each, including overhead.
Connection Rate:	20 million cell connections/sec. between slots.
Classes of Service:	32 queues per port, assignable.
Clock Sources:	Internal, free-running oscillator, Stratum 3. Phase-locked to any appropriate network interface. External input at T1 or E1 rate.
Clock Output:	Single clock output at T1 or E1 rate for synchronizing co-located IPX node(s) or CPE.
Cabinet Size:	22.75 inches (57.8 cm) high. 19.0 inches (48.25 cm) wide. 27.0 inches (68.6 cm) deep.

Weight, approx:	73 lb. (33.2 kg.) empty BPX shelf, w/fans but no PS. 6 lb. (2.7 kg.) each card. 18 lb. (8.2 kg.) empty AC Power Supply Tray. 16 lb. (7.3 kg.) each AC Power Supply. 2 lb. (0.9 kg.) each DC Power Entry module.
Clearance Requirement:	At least 30 inches front and rear clearance; nominal 12 inch side clearance.
Power Source:	AC system: 180 – 264 VAC, 47 to 63 Hz. DC system: –42 to –56 VDC.
Power Requirements:	AC BPX-15: 13 A at 180 VAC (2300 VA). DC BPX-15: 40 A at –42 VDC (1680W).
Input Power Connector:	AC: 3-conductor IEC receptacle. 8 feet (2.4 m.) power cord supplied. DC: 3 Ring lug screw terminal connectors.
Circuit Breakers:	AC: 15 A on AC power supply assembly. DC: 40A on power entry module.
Fuses:	Individual Backplane Card slot fuses, F1 through F3 for Fans 1 through 3, and F4 through F18 for card slots 1 through 15, 5A-120VAC rating.
Operating Environment:	Operating Conditions are listed in Table A-1.
Shock:	Withstands 10G, 10 ms. at 1/2 sine wave.
Vibration:	Withstands 1/4 G, 20–500 Hz.
Heat Transfer to Room:	**U**p to 7200 BTUs depending on node configuration.

Table A-1 Ambient Temperature and Humidity Limits

	Limits	
Conditions	**Fahrenheit**	**Centigrade**
Operating Temperature	+40 to +100 degrees	+4.5 to +38 degrees
Recommended	+68 to + 86 degrees	+20 to +30 degrees
Short-Term Temperature[1]	+35 to +120 degrees	+1.7 to + 49 degrees
Operating Relative Humidity	20% to 55% (non-condensing)	
Short-Term Relative Humidity	10% to 80% non-condensing	

1.Room temperature refers to conditions at a location 5 feet above the floor and 15 inches in front of the equipment.

ATM Trunk Interface (BXM-T3/E3 Cards)

Characteristic	T3 (DS3)	E3
Line Rate:	44.736 Mbps +/- 20 ppm	34.368 Mbps +/- 20 ppm
Line Code:	B3ZS	HDB3
Cell Transfer Rate:	96,000 cells per second (PLCP mode) 104268 cells per second (HEC/Direct mode)	80,000 cells per second
Framing:	ANSI T1.107, T1.107a	ITU T G804, G.832
Signal Level:	TA-TSY-000773 (PLCP)	ITU-T G.703
Transmission Convergence Sublayer:	DS3 PLCP frame format DS3 HEC mapped format	G.832 E3 frame format
	T3 (DS3) and E3	
Port Interface, trunk mode,		
-framing:	Framing for T3, C bit parity per ANSI T1.107/107A	
-port alarm processing	RDI (yellow alarm) and AIS	
Port Interface, port (UNI) mode:		
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF	
Connector:	SMB	

ATM Trunk Interface (BXM-155 Cards)

Line Rate:	155.52 Mbps	
Line Code:	NRZ	
Signal Level:	Min dBm	Max dBM
MMF LED TX	-22	-15
MMF LED RX	-31	-10
SMF IR TX	-15	-8
SMF IR RX	-34	-10
SMF LR TX	-5	0
SMF LR RX	-34	-10
Framing Format:	STS-3c, STM-1	
Port Interface:	LMI, ILMI	

ATM Cell Rate:	353,208 cells/sec.
Jitter:	ATM Forum UNI 3.1
ATM Layer Protocol:	LMI, ILMI
Port Alarm Processing:	LOS, LOF, LOP, Path AIS, Path Yellow
Line Errors Counted:	
Connector:	SC for MMF, SMF (IR) and SMF (LR)
Max. Cable Lengths:	MMF ~2 KM
	SMF IR ~20 KM
	SMF LR ~40 KM
Indicators:	Card status Port status

ATM Trunk Interface (BXM-622 Cards)

Line Rate:	622.08 Mbps	
Line Code:	NRZ	
Signal Level:	Min dBm	Max dBM
SMF IR TX	-15	-8
SMF IR RX	-28	-8
SMF LR TX	-2	+2
SMF LR RX	-28	-8
Framing Format:	STS-12c, STM-4	
Port Interface:	LMI, ILMI	
ATM Cell Rate:	1,412,830 cells/sec.	
Jitter:	ATM Forum UNI 3.1	
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF, LOP, Path AIS, Path Yellow	
Line Errors Counted:		
Connector:	SMF-FC	
Max. Cable Lengths:	SMF IR ~20 KM	
	SMF LR ~40 KM	
Indicators:	Card status Port status	

ATM T3 Trunk Interface (BNI-T3, LM-3T3)

Line Rate:	44.736 Mbps 20 ppm, asynchronous.
Line Code:	B3ZS.
Signal Level:	DSX-3.
Framing Format:	C-bit parity is monitored. No other framing or control bits in the DS3 frame are either altered or monitored.
Protocol:	Physical Layer Convergence Protocol per AT&T Publication TA-TSY-000772 and 000773.
ATM Cell Rate:	96,000 cells/sec. Limited to 80,000 cells/sec. when interfacing with the IPX.
Alarms Sent:	Remote.
Alarms Received:	AIS. Loss of Signal. Remote. Loss of Framing.
Line Errors Counted:	BPV. Parity Bit Errors.
Jitter:	Meets ACCUNET T45 specification (Pub 54014).
Connector:	75 ohm BNC.
Recommended Cable Lengths:	450 feet (150 m.) to a DS3 crossconnect.
Indicators:	Card status. Port status.

ATM E3 Trunk Interface (BNI-E3, LM-3E3)

Line Rate:	34.368 Mbps 20 ppm, asynchronous
Line Code:	HDB3
Signal Level:	CCITT G.703
Framing Format:	CCITT G.804, G.832
Port Interface:	75 ohm unbalanced
Barrier:	Fully barriered per EN 41003
ATM Cell Rate:	80,000 cells/sec
Jitter:	per CCITT G.823
ATM Layer Protocol:	per CCITT I.361 with HEC
Port Alarm Processing:	AIS Loss of Signal Remote Alarm Indication Loss of Framing
Line Errors Counted:	BPV Parity Bit Errors
Connector:	75 ohm BNC
Max. E3 Cable Lengths:	100 meters. Cabling must not exceed -6 dB/1000 feet at E3 rates. Cisco supplies cable with a maximum attenuation of 7 dB/1000 feet, but the maximum cable length must not exceed 100 meters.
Indicators:	Card status Port status

ATM OC3 Trunk Interface (BNI-OC3, LM-OC3)

Line Rate:	155.52 Mbps	
Line Code:	NRZ	
Signal Level:	Max	Min
MMF TX	–8 dBm	–15 dBm
MMF RX	–8 dBm	–28 dBm
SMF LR TX	0 dBm	–5 dBM
SMF LR RX	–10 dBm	–34 dBm
Framing Format:	STS-3c, STM1	
Port Interface:	LMI, ILMI	
ATM Cell Rate:	353,208 cells/sec.	
Jitter:	< 0.1 UI p-p, < 0.01 UI rms	
ATM Layer Protocol:	LMI, ILMI	
Port Alarm Processing:	LOS, LOF, LOP, Path AIS, Path Yellow	
Line Errors Counted:	Section BIP8, Line BIP24, Line FEBE, Path BIP8, Path FEBE	
Connector:	MMF SC SMF FC/PC	
Max. Cable Lengths:	MMF ~ 2 KM KM SMF IR ~20 KM SMF LR ~40 KM	
Indicators:	Card status Port status	

ATM Service Interface (BXM-T3/E3 Cards)

Capacity:	8 or 12 ports per card
Interface:	DS3/T3/E3
Line Rate:	DS3 44.736 Mbs, E3 34.368 Mbps
No. of channels per card:	16,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (BXM-155 Cards)

Capacity:	4 or 8 ports per card
Interface:	OC-3c/STM-1
Line Rate:	155.52.08 Mbps
No. of channels per card:	16,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (BXM-622 Cards)

Capacity:	2 ports per card
Interface:	OC-12c/STM-4
Line Rate:	622.08 Mbps
No. of channels per card:	16,000/32,000
No. of channels per node:	
VPI Addressing Range:	ATM UNI 3.1 compliant
VCI Addressing Range:	ATM UNI 3.1 compliant
Queues:	16 COS with 32 Virtual Interface (VI) queues

ATM Service Interface (ASI-1, LM-2T3)

Capacity:	2 ports per card
Interface:	T3
Line Rate:	96,000 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	32, 16 per line (port) includes CBR, VBR, and ABR queues

ATM Service Interface (ASI-1, LM-2E3)

Capacity:	2 ports per card
Interface:	E3
Line Rate:	80,000 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	32, 16 per line (port) includes CBR, VBR, and ABR queues

ATM Service Interface (ASI-2, LM-OC3)

Capacity:	2 ports per card
Interface:	OC3
Line Rate:	353,208 cells/sec.
No. of channels per card:	1000
No. of channels per node:	1000 or 5000 (grouped)
VPI Addressing Range:	0–255 (UNI), 0-1023 (NNI)
VCI Addressing Range:	1–4095
Queues:	

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. (next page) 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) or 13 A 250 Vac BS1363, 3-prong fused plug (UK, Ireland) CEE 7/7 (Continental Europe) AS3112 (Australia/New Zealand) CEI23-16/VII (Italy)

DC Powered Nodes

DC wiring (Table 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 StrataView Plus NMS computers, control terminals, and modems. It is also used for external clock inputs from a clock source. See *Appendix C, BPX Switch Peripherals*, for more details on peripherals that can be attached to these ports.

Auxiliary and Control Port Cabling

The auxiliary and control ports are used to connect one of the nodes in the network to a control terminal, StrataView NMS workstation, or modem connections for remote alarm reporting or system monitoring. Refer to Table 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 StrataView Plus 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.
Suggested Cable:	TBS
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 (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	75 coax/BNC-BNC, 10'	T3 or E3 trunk interface
T3-E3-25	75 coax/BNC-BNC, 25'	
T3-E3-50	75 coax/BNC-BNC, 50'	
T3-E3-75	75 coax/BNC-BNC, 75'	
T3-E3-xx	length to be specified	
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	Cisco P/N
T3 trunk	LM-3T3	TBS
E3 trunk	LM-3E3	TBS
Aux./Cont. ports	LM-BCC	TBS
Ext. Clk. In	LM-BCC	TBS
Ext. Clk. Out	LM-BCC	TBS

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

Cisco StrataView Plus Terminal

A Cisco StrataView Plus workstation is recommended for managing a network containing IPX, IGX, and BPX switch. Refer to the *Cisco StrataView Plus Operation Manual* and *Cisco StrataView Plus Installation Manual* for setup instructions and specifications for the Cisco StrataView Plus NMS, which is required to provide network alarm, control, and statistics monitoring.

Note For network management, a Cisco 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 Cisco 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 Cisco 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.
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. Refer to 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.

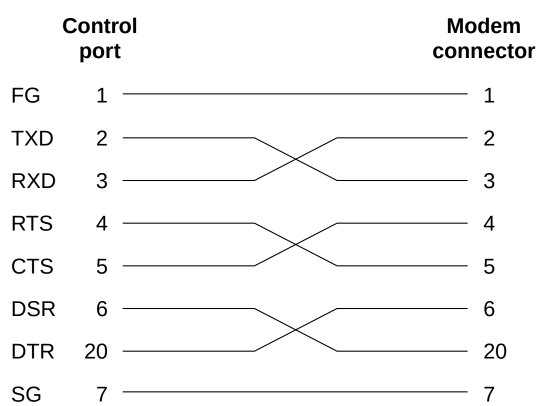
Step 6 Connect the modem to the BPX CONTROL port using a null-modem cables Figure C-1. A null modem cable is used, as the connection is essentially a DCE to DCE rather than a DTE to DCE connection.

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)



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

12138

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 Figure C-2.

Step 7 Ask customer service to assist in testing the operation of the modem setup.

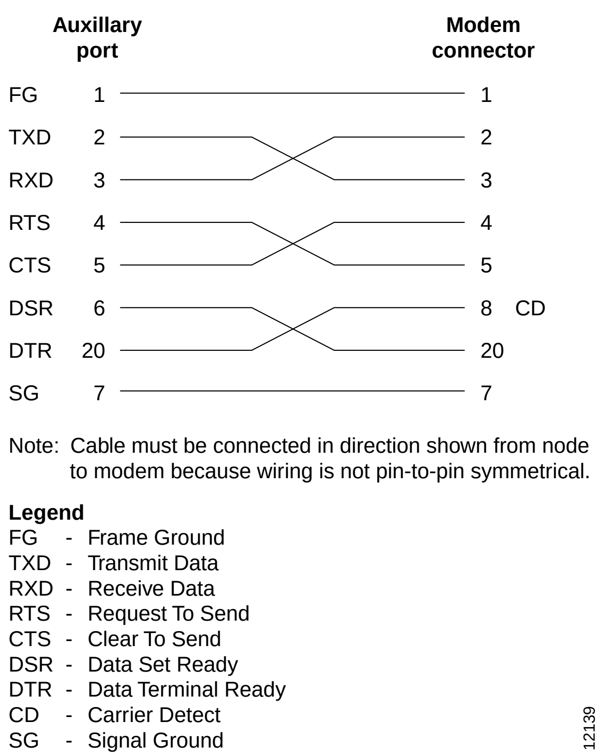
Table C-8 V.34R Auto-Dial Configuration (dial-out to customer service)*

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)



AT3-6ME Interface Adapter

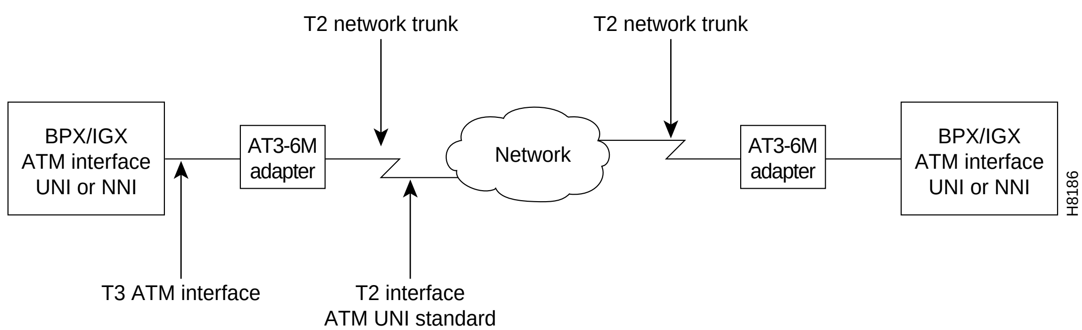
This appendix describes the AT3-6ME Interface Adapter, sometimes referred to as the T3-T2 Interface Adapter, that is used with the BPX switch to provide a 6 Mbps ATM network interface to T2 transmission facilities.

Application

The AT3-6ME Interface Adapter is used with the BPX Broadband ATM Switch or the IPX Narrowband Switch in applications where it is required to interface a 6 Mbps T2 digital network facility to the 45 Mbps T3 ATM port on the BPX, IGX, or IPX node.

Applications include networks where T2 transmission facilities are available. Users with ATM networks who require somewhat more bandwidth than is provided by the T1 or E1 ATM network connections but do not need the full T3 bandwidth provided by the BPX ATM network ports can also benefit from using the AT3-6ME Interface Adapter. See Figure D-1 for a typical application.

Figure D-1 Network Application



General Description

The AT3-6ME Interface Adapter is a bi-directional device which provides a conversion between transmission systems of different transmission rates, the North American T3 (44.736 Mbps) and the Japanese 6M (T2). It is used only in ATM networks. The adapter is transparent to both users and the network.

The T3 interface operates at 44.736 Mbps with the B-ISDN Physical Layer Convergence Protocol (PLCP) and meets the ATM Forum standards. The T2 interface operates at 6 Mbps according to the Japanese Nippon Telephone & Telegraph (NTT) User-Network Interface (UNI) specifications.

ATM cells from one interface are mapped to the other interface enabling users with ATM node equipment with North American T3 ATM ports to operate in a T2 network. The ATM cell throughput on a T2 digital trunk using this adapter is limited to 14,490 cells per second.

The cell transfer rate for T2 is greatly reduced from the T3 cell rate out of a T3 port on an IPX using the ATMT card or from a BPX port. It is very important to restrict the cell rate from the node when using a T2 trunk. Cell rate adaptation is done via software trunk configuration at the T3 ATM interface, where the non null cell throughput is limited to the T2 capacity. In the T2 to the T3 direction, the T3 ATM interface has more than enough capacity to accommodate the T2 cell rate.

The Interface Adapter can buffer a 70-cell burst at the T3 rate before the T2 interface will begin to drop cells. Cells will continue to be dropped until the T3 interface returns to a rate that complies with the bandwidth of the T2 interface.

All alarms and line errors are passed through the Interface Adapter unchanged. Any existing network management system has an instant view of the actual network transmission system. Errors at the ATM layer propagate through from one interface to the other, thus the end user has the complete knowledge and statistical information regarding the network status at all times. Therefore a special network management interface is not required.

Since the T3 interface is asynchronous and the T2 is synchronous, the AT3-6ME can be configured to carry the synchronization information through from one interface to the other. The synchronization is carried through the T3 interface using the PLCP-embedded 8 KHz. The T2 interface clock may be generated locally or it may be slaved to the public network.

Equipment Description

The AT3-6ME is fully contained in a metallic housing designed to be mounted in a 19" equipment rack. It occupies only one rack mounting space and is powered from normal AC line powering. The power supply accommodates an input voltage over the range 90 to 240 VAC, 50 or 60 Hz.

Interface Connectors

The interface connectors are located on the rear panel (see Table D-1 and Figure D-2). These connectors include:

- Two T3 BNC connectors, XMT and RCV.
- Two 6M BNC connectors, XMT and RCV.
- A single RS-232 male, subminiature 9-pin control terminal interface.
- AC input connector with integral fuse.

The control terminal is a standard RS-232 interface DTE interface. No hardware handshake is required for the interface. The diagnostic display comes up immediately. It operates at 9.6 Kbps with any ASCII terminal.

Table D-1 Rear Panel Connectors

Connector	Type	Description
T3 RX	BNC	Receive T3 input from BPX, IGX, or IPX ATM port.
T3 TX	BNC	Transmit T3 output to BPX, IGX, or IPX ATM port.
T2 RX	BNC	Receive 6 MB input from T2 facility.
T2 TX	BNC	Transmit 6 MB input to T2 facility.
RS-232	DB9	Control terminal connection.
Primary Power	IEC	AC power input with fuse.

Front Panel Indicators

The front panel of the system provides LED indicators for the alarm status of the transmit and the receive T3 and the T2 interfaces (refer to Table D-2 and Figure D-2). Also on the front panel are indications for power and for operating status (Fail/Active).

The Overflow LED indicates that the cell rate coming from the T3 interface exceeds the bandwidth of the T2 facility and that the Interface Adapter buffer has overflowed.

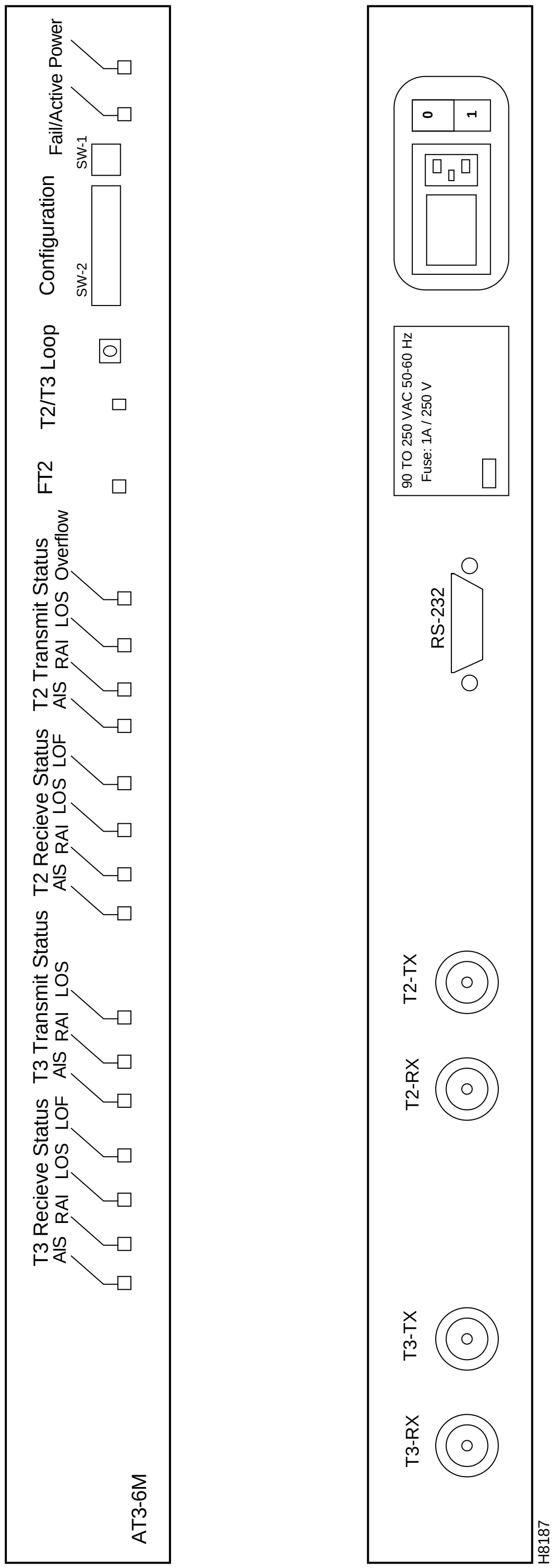
Table D-2 Front Panel Indicators

Indicator	Color	Description
T3 Receive Status—AIS	Green	Alarm Indication signal detected on the RCV T3 line.
T3 Receive Status—RAI	Yellow	Remote Alarm Indication signal detected on the receive T3 line.
T3 Receive Status—LOS	Red	Loss of receive T3 signal.
T3 Receive—LOF	Red	Loss of frame on receive T3 signal.
T3 Transmit Status—AIS	Green	Alarm Indication signal detected on the transmit T3 line.
T3 Transmit Status—RAI	Yellow	Remote Alarm Indication signal detected on the transmit T3 line.
T3 Transmit Status—LOS	Red	Loss of transmit T3 signal.
T2 Receive Status—AIS	Green	Alarm Indication signal detected on the RCV T2 line.
T2 Receive Status—RAI	Yellow	Remote Alarm Indication signal detected on the receive T2 line.
T2 Receive Status—LOS	Red	Loss of receive T2 signal.
T2 Receive—LOF	Red	Loss of frame on receive T2 signal.
T2 Transmit Status—AIS	Green	Remote Alarm Indication signal detected on the transmit T2 line.
T2 Transmit Status—RAI	Yellow	Loss of transmit T2 signal.
T2 Transmit Status—LOS	Red	Loss of frame on transmit signal.
Overflow	Red	T3 receive cell rate exceeds the T2 line capacity.
FT2	Red	Fractional T2 indication for future use.
T3/T2 loop	Red	Indicates the unit is in loop back mode, external toward the T3 and T2 line interfaces.
Active/Fail	Green/Red	Upon power up the system will go through extensive self tests. If self-test passes, the Active/Fail LED will be green; if self-test fails the LED will be RED.
Power	Green	Power ON indication.

DIP Switches

The adapter has two front panel DIP switches, a two-position (SW-1), and a 12-position (SW-2) switch. SW-1 controls the configurations that may interrupt operation and should be done through a two-step operation. SW-2 enables all other configuration parameters.

Figure D-2 Front and Rear Panel Features



Installation

Install the AT3-6ME in a rack adjacent to the BPX enclosure (allowing room for any AC Power Supply Assembly that may also need to be mounted) or in the IPX enclosure wherever there is space for the AT3-6ME adapter.

System Connections

Two short BNC-BNC cables are required to connect the AT3-6ME to the BPX or IPX node.

Step 1 For use with BPX switch, connect one cable between one of the three TX connectors on a selected BPX LM-3T3 card and the T3-RX connector on the AT3-6ME back panel. For IPX applications, connect to the TX connector on the ATMT back card.

Step 2 Connect the other cable between the associated RX connector on the BPX LM-3T3 or ATMT card and the T3-TX connector on the AT3-6ME back panel.

Step 3 Connect the cable coming from the 6 Mbps facility to the T2-RX connector on the AT3-6ME.

Step 4 Connect the cable going to the 6 Mbps facility to the T2-TX connector on the AT3-6ME.

Step 5 Connect the AC power cord to the IEC connector on the rear of the AT3-6ME.

AT3-6ME Configuration

The adapter configuration is done via a set of DIP switches located on the front panel. There are two sets of switches, a 12-position switch and a two position switch. The two position switch enables the configuration change via the terminal and enable/disable the loop push button located in the front panel (to secure against accidental operation). Review both Table D-3 and Table D-4. Set the appropriate DIP switches with the power off.

Table D-3 DIP Switch SW-1 Selection Guide

Switch	Position	Function
1	Down	Enable configuration via the TTY.
1	Up	Disable configuration via the TTY (default).
2	Down	Enable front panel loop push button.
2	Up	Disable front panel loop push button (default).

Table D-4 DIP Switch SW-2 Selection Guide

Switches	Position	Function
1 2	Up Up	Internal synchronization source for the T2 transmitter
1 2	Up Down	Slave T2 transmitter to T3 line
1 2	Down Down	Slave T2 transmitter to T2 receiver
3 4	Up Up	Long length T3 cable
3 4	Up Down	Medium length T3 cable
3 4	Down Down	Short length T3 cable; system is co located to IPX/IGX/BPX[1] (default)
5, 6	don't care	Unused
7	Up	ATM converter mode
7	Down	Test Mode
8	Up	Enable BPV relay from T2 to T3
8	Down	Disable PV relay from T2 to T3
9	Up	Long length T2 cable
9	Down	Short length T2 cable (default)[1]
10, 11, 12	Don't care	Unused

1.T2 and T3 cable length should be set to "short" upon power-up for self-test.
Upon LOS, defaults to "internal synchronization."

BPX, IGX, or IPX Port Configuration

The trunk on the BPX, IGX, or IPX node must be reconfigured from Cisco StrataView Plus or a local control terminal.

Step 1 Telnet to the first node equipped with an AT3-6ME.

Step 2 Use the Configure Trunk (**cnftrk**) command to select T2 for the Tx Trunk Rate.

Step 3 Set the RCV Trunk Rate to 28980 cps.

Step 4 Repeat steps 1 through 3 for all other nodes using the AT3-6ME.

Operation

The following paragraphs describe the various operating modes for the AT3-6ME. The unit is basically designed for unattended operation. Any failures in the unit or any line alarms or errors will be propagated.

Power-Up Sequence

During the system power-up, the unit goes through a self test procedure. The Power LED turns green. The Active/ Fail LED stays off until the self test sequence is completed. At the end of the self test the loop LED comes on for about 5 seconds.

Through the self test, all LEDs light up. When the test is completed successfully the Active/Fail LED turns green. If the system fails self test, it will repeat the self-test twice more. If it continues to fail, the Active/Fail LED turns red.

Normal Operation

In standard operation the AT3-6ME system relays ATM cells from the T2 6M to the T3 interface. To accommodate for the difference in the transmission rate, the AT3-6ME removes all null cells from the T3 interface. The T3 sources connected to the AT3-6ME must regulate their ATM Cell rate not to exceed the T2 6M cell rate. The AT3-6ME can absorb up to 70 cells in a single burst.

The AT3-6ME Interface Adapter can interface to any ATM UNI or NNI line at the T2 or T3 rate. The AT3-6ME Relays alarms and errors from one interface to the other. It relays the alarm and error conditions as indicated in Table D-5.

Table D-5 Alarm Handling

Alarms Passed Thru (both directions)	Errors Relayed Thru (both directions)
AIS	HEC Error—both directions.
RAI	BPV (up to 10^{-5} rate)—6M to T3 only.
LOS	
LOF	

Remote Loop Operation

The AT3-6ME has the capability of creating a remote loop on both the T3 and the T2 sides for test purposes. The loop can be activated by manually pressing a front-panel switch or through the control terminal. The loopbacks are through looping relays at the two interfaces and they operate simultaneously.

To activate the loop from the front panel, one must first enable the proper DIP switch on SW-1. Then press and hold the front panel push button for one second. This is to prevent accidental operation of the loop. Once the loop is set it can be removed by operating the loop switch a second time or it will automatically remove itself after one hour.

Terminal Operation

The system is designed to operate without a terminal. There is a terminal interface designed for diagnostics and maintenance purpose only. The terminal interface is always active and continuously displays the user prompt. The terminal interface operating parameters are as follows:

Electrical Interface:	RS232
DTE/DCE:	DCE
Speed:	9.6 Kbps
Handshake:	NON
Connector:	Male DB9

Upon power up, the system goes through power up diagnostics. The terminal displays the diagnostics sequence. Upon successful self test the unit is available for operation. The terminal will display the actual set up of the system represented by the DIP switches (see Table D-6). If the configuration was overwritten through the TTY, the terminal will display the actual set up that could be different then the dip switch setting.

Table D-6 DIP Switch Settings

1	2	3	4	5	6	7	8	9	10	11	12	1	2
0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

Commands

Commands are entered after the user prompt. Commands are available to display the various error counters and alarms associated with the T2 line and the T3 port interface, select the source of timing for the DSU, and to enable and remove the remote loop. Table D-7 lists available commands for use with the AT3-6ME terminal interface while Table D-8 indicates the display format.

Table D-7 Command Summary

Command	Parameters	Meaning
?		Help Menu.
dspstat		Display status.
dspstat clear		Clears the status display.
Override dipsw	0 1	Disable TTY configuration entry. Enable TTY configuration entry. Operates only when DIP switch 1-1 is down.
Sync source	0 1 2	System is slaved to the 6M line. System is slaved to the T3 line. System runs of its internal clock.
Remote loop	No of seconds stop	Enable remote loop back operation. Cancel the loop back operation.

Table D-8 Status Display

Status	T3[1]	T2[1]
BPV	NNN	NNN
Parity Errors	NNN	X
Framing Errors	NNN	NNN
PLCP Framing Errors	NNN	X
HEC Errors	NNN	NNN
RX Cells	NNN	NNN
TX Cells	NNN	NNN
AIS	1/0	1/0
1/0	1/0	1/0
LOF	1/0	1/0
Overflow	X	1/0

1.X = not available

Specifications

The following are the specifications for the AT3-6ME Interface Adapter:

T3 interface

Line rate:	44.736 Mbps 20 ppm
Framing format:	C-bit parity
Line code:	B3ZS
Physical layer:	PLCP format
ATM layer:	UNI per the ATM Forum UNI 3.0 specification
Cell Rate:	Up to 96,000 cells/sec.
Connector:	75 ohm BNC

T2 Interface

Line rate:	6.312 Mbps
Line code:	B8ZS
Synchronization:	Internal 6.312 Mbps 30 ppm or Slave to the incoming 6 Mbps line or Slave to the T3 PLCP frame
Framing format:	ITU-T G.703
ATM Layer:	Per NTT UNI specification dated 1993
Queue:	75 cell FIFO
Cell Rate:	Up to 14,490 cells/sec.
Connector:	75 ohm BNC

Power

Input Power:	90 VAC to 250 VAC, 50/60 Hz
Power consumption:	30 watts
Input Power Connector:	Universal power entry module with fuse
Fuse size:	1/2A 250 VAC

Mechanical

Rack Mounting Space:	1 rack mount space, 19" rack
Size:	19" x 1.75" x 8.5"

Terminal Interface

Speed:	9.6 Kbps
Type:	DTE
Handshake:	NONE
Connector:	DB9

Glossary

A

A-bit (active bit)
The bit in the frame relay frame header that indicates the status of the far end user device and the status of the PVC segment in the foreign network.

A-law
An analog to digital encoding scheme used to convert voice samples to an 8-bit data word used in CEPT E1 multiplex equipment. (See also -law.)

ABR (Available Bit Rate)
ATM connection type for bursty traffic, such as data. Provides closed loop control of service rate that allows connections to use additional bandwidth when available. ABR may be used with ATM Traffic Management 4.0 standards VSVD flow congestion control, or with the proprietary ForeSight flow congestion control. (See also CBR and VBR.)

ACO (Alarm Cut Off)
A switch to turn off the audible alarm outputs from a node while leaving the visual alarm outputs unchanged.

adaptive voice
An optional feature of the IPX switch that disables VAD from connections using it whenever there is excess bandwidth available to allow the normal encoded voice to be carried on the packet line. (See also VAD.)

ADPCM (Adaptive Differential Pulse Code Modulation)
A compression method that samples voice 8,000 times per second, and uses the changes between samples as the basis for compression. Increases the capacity of a T1 line from 24 to 48 channels.

ADTF (Allowed Cell Rate Decrease Factor)
Time permitted between sending RM cells before the rate is decreased to ICR.

AIT (ATM Interworking Trunk Card)
The AIT front card provides an ATM trunk interface for the IPX switch. The AIT operates in conjunction with a backcard, AIT-T3 or AIT-E3.

AIT-E3 (ATM Interworking Trunk E3 Interface Card)
The AIT-E3 backcard provides an E3 interface for the AIT (IPX switch) or BTM (IGX switch) ATM trunk cards.

AIT-T3 (ATM Interworking Trunk T3 Interface Card)
The AIT-T3 backcard provides a T3 interface for the AIT (IPX switch) or BTM (IGX switch) ATM.

alternate routing
An automatic rerouting of a failed connection by a node to a new route through the network to maintain service.

AMI (Alternate Mark Inversion)
The line code used for T1 and E1 lines where the "1s" or "marks" on the line alternate between positive polarity and negative polarity.

arbiter
A BPX administration processor that polls each network port to control the data flow in and out of the crosspoint switch matrix.

ARC (Alarm Relay Card)
An alarm front card for the IPX switch.

ARI (Alarm Relay Interface Card)
An alarm interface back card for the IPX and IGX switches.

ARM (Alarm Relay Module)
An alarm front card for the IGX switch.

ASM (Alarm/Status Monitor Cards)
An alarm front card and back card set for the BPX switch.

ATM (Asynchronous Transfer Mode)
Data transmission that uses a very flexible method of carrying information, including voice, data, multimedia, and video between devices on a local or wide area network using 53-byte cells on virtual circuits. The 53 byte cell consists of data and a small header. (See also cell relay.)

ATM Switched Virtual Circuits (SVCs)
A member of the INS product family that uses ATM SVC Server Shelves and software to enhance a Cisco WAN switching network with ATM switched virtual circuits.

ATM SVC Server Shelf
An adjunct processor used in the INS ATM SVC application to enhance traditional Cisco WAN switching networks with ATM switched virtual circuits. The ATM SVC Server Shelf is co-located with and connected to a BPX switch.

auxiliary port
An RS-232 port on the front panel of the SCC card used for connecting a printer or an out-dial modem. This port is a one-way, outgoing port.

B

B3ZS (Bipolar with Three Zero Suppression)
A protocol for T3 lines that converts a channel word with three consecutive zeros into a code which at the far end is converted back to three zeros.

B8ZS (Bipolar with Eight Zero Suppression)
A T1 line protocol that converts a channel word with eight consecutive zeros into a code which, at the far end, is converted back to eight zeros. Allows 64 Kbps clear channel operation while assuring the ones density required on the T1 line.

bandwidth reservation
An IPX software feature that allows circuits to automatically become active (or “upped”) at a specified time and date and downed at some later time and date. For circuits that do not need to be available 100% of the time.

B channel
In ISDN, a full-duplex, 64-kbps channel used to send user data. Also known as the bearer channel. Compare with D channel.

BCC
The control card for the BPX switch.

BC-E1 (Backcard E1)
E1 interface card used on IPX and IGX switches.

BC-E3 (Backcard E3)
E3 interface card used on IPX and IGX switches.

BC-J1 (Backcard J1)
J1 interface card used on IPX and IGX switches.

BC-SR (Backcard Subrate)
Subrate interface card used on IPX and IGX switches.

BC-T1 (Backcard T1)
T1 interface card used on IPX and IGX switches.

BC-T3 (Backcard T3)
T3 interface card used on IPX and IGX switches.

BC-Y1 (Backcard Y1)
Y1 interface card used on IPX and IGX switches.

BDA (Bframe Destination Address)
The address of the slot.port.channel for which the Bframe is destined. This address is part of the Bframe header and is only used across the switch fabric locally in the node.

Bframe
The BPX frame is the 64-byte format for messages used to encapsulate ATM cells which are sent across the switch fabric.

bipolar violations
Presence or absence of extra “1” bits on a T1 transmission facility caused by interference or a failing line repeater. These extra or missing bits interrupts one of the rules for bipolar pairs of a digital transmission line.

BISDN (broadband ISDN)
ITU-T communication standards designed to handle high-bandwidth applications. Compare with ISDN.

BNI (BPX Network Interface Card)
The front card used to network BPX switches together and to connect to AXIS shelves, and IPX and IGX nodes configured as shelves. Supports T-3, E-3, and OC3 trunks carrying ATM cells.

BPX Switch
A high-speed broadband, high-capacity ATM cell relay network switch from for private and public networks.

BRI (Basic Rate Interface)
ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data. Compare with PRI.

bundled connections
Frame relay connections grouping a number of ports into one permanent virtual circuit.

BTM (Broadband Trunk Module)
The BTM provides an ATM trunk interface for the IGX switch. The BTM operates in conjunction with a backcard, AIT-T3, or AIT-E3.

BXM
A series of BPX cards, BXM-T3/E3, BXM-155, or BXM-622 which can be configured for either trunk or line (service access) modes. These cards support ATM Traffic Management 4.0, including VSVD congestion flow control.

C

CAS (Channel Associated Signalling)
A signalling mode in E1 transmission where the signalling bits for all 30 E1 channels are carried in timeslot 16. Timeslots 1 to 15 and 17 to 31 carry encoded voice bits only.

CBR (Constant Bit Rate)
ATM Connection type for constant bit rate traffic such as voice or synchronized data requiring a low variation in delay. (See also, VBR and ABR.)

CCDV (Compliant Cell Delay Variation)
A parameter utilized in defining ATM Constant Bit Rate service. The amount of delay that is acceptable between ATM cells for them to be accepted as compliant (usable).

CCITT (Consultive Committee for International Telephone and Telegraph)
An international telecommunications advisory committee established under the United Nations to recommend worldwide standards for data and voice communications.

CCS (Common Channel Signalling)
A carrier signalling mode in E1 transmission where signalling bits are not used. CCS typically separates user data from signalling information. A signalling channel is used to provide signalling for all other user data channels in the system.

CDP (Channelized Data PAD)
An IPX dual-purpose front card that can carry voice traffic, a combination of voice and data, or just data. The CVM card is used in conjunction with a BC-T1, BC-E1, or BC-J1 backcard.

CDVT (Cell Delay Variation Tolerance)
Controls time scale over which the PCR is policed.

Cell
A unit of data with a fixed number of bytes. For ATM the cell size is 53 bytes.

cell relay
A form of digital communications using fixed length cells consisting of data and a small header IPX FastPacket was an early implementation of cell relay. The 53 byte ATM cell consists of data and a small header.

CEPT
CEPT is the European Conference of Posts and Telecommunications Administrations. This association is comprised of European Telecommunications service providers that participate in relevant areas of the work of CEN/CENELEC.

CGA (Carrier Group Alarm)
A major alarm condition for a T1 multiplexer or PABX that results in all channels being taken out of service.

channel
The logical end point for a connection.

circuit line
A T1 or E1 line that connects a user device, such as a PABX or channel bank to the IPX switch. Carries customer DS0 voice and data circuits. (See also line.)

Cisco StrataView Plus
A Unix-based workstation and software used as a network management system (NMS) for Cisco WAN switching networks. It is part of the StrataSphere group. Provides a graphical user interface for configuration, maintenance, administration of the network. Collects and displays network statistics.

clear channel capability
When all eight bits of a channel word in the T1 line signal are available for transmitting customer data with no restrictions on content. Also referred to as 64 Kbps clear channel.

Cmax
A frame relay connection parameter that specifies the number of packets allowed in the initial burst of data after which the data bandwidth is reduced to the connection's minimum specified bandwidth.

CLLM
Consolidated Link Layer Management. A protocol used to transmit ForeSight messages across the frame relay NNI port.

CLP (Cell loss priority)
Cell loss Priority. CLP Hi and CLP Lo thresholds are configurable.

Complex Gateway
Refers to interworking of a connection with respect to the IPX and IGX nodes. For example, in a Frame Relay to ATM interworking, the Frame Relay data is extracted from FastPackets and transformed to ATM cells with redundant overhead bits discarded.

composite data rate
The sum of the data rates for all circuits transmitting on the same synchronous or frame relay data card.

control port

An RS-232 port on the face plate of a back card for a controller card (BCC, NPC, NPM.) that may used for connecting a control terminal. This port is bi-directional.

COS (Class of Service)

The priority assigned each user connection. Defines which circuits get rerouted first during a network failure.

courtesy downing

A software feature that is used to conserve network bandwidth by automatically “downing” a voice connection when the signalling status indicates an inactive (on-hook) circuit. The circuit is automatically “upped” when the circuit becomes active.

CRC (Cyclical Redundancy Check)

A method of error checking that detects errors in a block of data. Unlike parity checks, the CRC can detect multiple data errors within the block and thus equipment using a CRC error check can derive a error rate.

crosspoint switch

A two-dimensional data switch type that is arranged in a matrix of all input connections along one axis and all output connections along the other axis. Each input and output line has a switch point where the two axis intersect that can be enabled (switch closed) or disabled (switch open). The central matrix switch providing the switching matrix for traffic routing by the BPX switch.

CSU (Channel Service Unit)

A network protection unit that terminates any T1 span line connected to the carrier's central office, providing receive direction regeneration and maintenance loopback for the 1.544 Mbps signal.

D

D4-format

A digital signal format with 24 eight-bit channels plus one synchronizing bit per T1 line. Channels are assigned in a straight, numeric sequence.

DACS (Digital Access and Control System)

Equipment, usually found in the telephone company central office, that is used to groom and retime the 24 channels in a DS1 signal. Individual DS0 channels can be cross-connected from one DS1 source and inserted in another DS1 source either with the same or with a different channel number.

DAS Server Shelf

The adjunct processor used in INS Dial-Up Frame Relay applications to provide frame relay dial-up and dial-backup circuits. The DAS Server Shelf is co-located with and connected to an IPX or IGX switch.

DCE (Data Communications Equipment)

As defined by the RS-232 standard, any device that transmits or receives information. Usually used with data terminal equipment (DTE, like a computer or network node).

D channel

A message-oriented ISDN signalling channel, typically carried in DS24 of a PRI on T1 facilities or TS16 of a PRI on E1 facilities. Compare to B channel.

DDS (Digital Data Service)

An AT&T dial-up data service offering for 2.4 to 56 Kbps over subscriber loop cable. Requires a Data Service Unit, DSU, at customer premise for interface to the DDS trunk.

Device Code

The first 8 bits of a FastPacket Address.

DFM (Data Frame Multiplexing)

An optional feature that saves data channel bandwidth by analyzing data channel content and suppressing repetitive data patterns.

Dial Access Switching

Another name for the INS Dial-Up Frame Relay application.

Dial-Up Frame Relay

An INS application that uses a DAS Server Shelf and software to enhance Cisco WAN switching networks with frame relay soft permanent virtual circuits (SPVCs) for dial-up dial-backup connections.

DLCI (Data Link Connection Identifier)

A field in a frame relay data packet that identifies the destination for the data.

domain

A grouping of nodes sharing common interests or attributes.

domain name

A unique name consisting of the letter "D" immediately followed by a number (1–8) delineated by a "." (period) from the node name (1–8 characters maximum). Example: D1.alpha.

domain number

A number from 1–8 assigned with the cnfdmn command. The number assigned is part of the domain name.

DPNSS

Digital Private Network Signalling System. A common-channel message-oriented signalling protocol commonly used by private branch exchanges (PBXes). The INS Voice Network Switching application supports DPNSS signalling.

DS0 (Digital Signal 0)

A 64 Kbps channel used to transmit encoded voice and/or data. There are 24 DS0 channels in a circuit T1 (DS1) line. DS0 data is transmitted using one or more DS0 circuits in a T1 or E1 circuit line.

DS0A

An extension of DS0 that defines the format for assembling various low-speed data circuits (1.2 to 19.6 Kbps) into a single 64 Kbps DS0 channel.

DS1 (Digital Signal 1)

A digital transmission standard that carries 24 individual channels in a bipolar, high-speed line signal at 1.544 Mbps. DS1 signal level is 3V.

DSI (Digital Speech Interpolation)

An algorithm that analyzes DS0 voice bits for non-speech codes. Suppresses these bits to conserve packet line bandwidth and inserts a code to indicate to the far end that these bits have been removed. Similar to DFM for data channels. Also, referred to as VAD (Voice Activity Detection).

DTE (Data Terminal Equipment)

As defined by the RS-232 standard, any device that generates or utilizes information. (See also, DCE.)

E

E1

European transmission service at the rate of 2.048 Mbps.

E3

Transmission service at a rate of 34.368 Mbps.

ECN (Explicit Congestion Notification)

A frame relay feature to signal the onset of network congestion to external devices. Sets FECN and BECN bits in frame relay header to indicate forward and backward congestion.

F

Fast EIA

Same as interleaved EIA. Seven data circuit control leads in each direction are transmitted in alternating bytes with data. For fast control lead response to data being turned on and off but with a sacrifice in packet line bandwidth.

FBTC (Frame Based Traffic Control)

An AAL5 frame based traffic control that provides the possibility of discarding the whole frame, not just one compliant cell. This avoids wasting bandwidth by continuing to send the cells in a frame once a cell has been found to be non-compliant.

FGCRA (Frame Based Generic Cell Rate Algorithm)

An enhancement option to GCRA that allows an entire frame to be discarded if any of its cells are non-compliant, rather than transmitting a partial frame over the network.

flat network

A non-structured network, a network in which there are no junction nodes or domains.

foreign network

An adjacent network that is owned and managed by a different party than the one that owns the local network.

ForeSight

A proprietary optional feature that uses feedback techniques to dynamically allocate extra bandwidth to frame relay and ATM connections when the network bandwidth is available and not used by other connections. (See also VSVD.)

frame forwarding

A software feature allowing point-to-point frame relay type connection for various data applications that do not conform to the Frame Relay Interface Specification.

FPC (FastPAD Back Card)

The FPC is used with an FTC (IPX switch) or FTM (IGX switch) card. The FPC provides either a T1, E1, V.35, or X.21 interface.

frame relay connection class

A tag for a frame relay circuit which indicates the class of service to be provided for this connection. Parameters associated with a connection class include minimum information rate guaranteed, peak information rate expected, maximum network delay, etc.

FRI (Frame Relay Interface Card)

The backcard for an FRP (IPX switch) or FRM (IGX switch) card. The FRI provides V.35, X.21, T1, or E1 interfaces.

FRP (Frame Relay PAD)

An IPX frame relay front card that supports 1-4 data ports, and in single-port mode, operates up to 2.048 Mbps. The card is used in conjunction with FRI-V.35, X.21, T1, or E1 backcards.

FRM (Frame Relay Module)

An IGX frame relay front card that supports 1-4 data ports, and in single-port mode, operates up to 2.048 Mbps. The card is used in conjunction with FRI-V.35, X.21, T1, or E1 backcards.

FRM-2 (Frame Relay Module)

An IGX frame relay front card that provides an interface to the frame relay Port Concentrator Shelf (PCS). The card is used with the FRI-2-X.21 backcard which connects to the PCS.

FRP-2 (Frame Relay Module)

An IPX frame relay front card that provides an interface to the frame relay Port Concentrator Shelf (PCS). The card is used with the FRI-2-X.21 backcard which connects to the PCS.

FRP-2 (Frame Relay Module)

An IPX frame relay front card that provides an interface to the frame relay Port Concentrator Shelf (PCS). The card is used with the FRI-2-X.21 backcard which connects to the PCS.

Frame Relay Service

A packet interface data transmission protocol used for connecting widely-separated LANs. Characterized by long intervals of no data to be sent interspersed with bursts of large volumes of data; sometimes referred to as “bursty data”.

frame slip

A T1 error condition caused by a timing problem between the network and the IPX switch. When this happens, the IPX switch inserts a blank DS1 frame or drops an idle DS1 frame so there is no loss of customer data.

FRTT (Fixed Round Trip Time)

The sum of the fixed and propagation delays from the source to a destination and back.

Full Status Report

A message sent across the NNI indicating the A-bit status of all connections routed across this NNI frame relay port.

FTC (FastPAD Trunk Card)
An IPX frame relay front card that provides an interface to a FastPAD. The FTC is used with an FPC backcard. that provides either a T1, E1, V.35, or X.21 interface.

FTM (FastPAD Trunk Module)
An IPX frame relay front card that provides an interface to a FastPAD.

G

gateway
A node that is configured to handle both T1 and E1 packet and circuit lines for direct interface international circuits. (See also Seamless International IPX Network.)

GCRA (Generic Cell Rate Algorithm)
GCRA is a "continuous leaky-bucket" process that monitors the cell depth in the input queue for each PVC to determine whether to admit a new cell to the network without setting the Cell Loss Priority bit.

global addressing
A frame relay addressing convention that uses the DLCI to identify a specific end device somewhere else in the frame relay network. In a global addressing scheme, the DLCI is a unique number for each port in the network.

grouped connections
Frame relay connections grouping a number of ports onto one permanent virtual circuit. Similar to bundled connections except the grouped connections do not have to be contiguous, nor do they all have to be added simultaneously.

H

HDB3 (High Density Bipolar Three)
A new line interface for E1, similar to B8ZS for T1, which eliminates patterns with eight or more consecutive zeros. Allows for 64 Kbps clear channel operation and still assure the ones density required on the E1 line.

HDP (High Speed Data PAD)
An IGX front card that supports one to four medium speed, synchronous data channels.

I

IGX Switch
A multi-service, multi-band ATM cell relay network switch for private and public networks.

Intelligent Network Server (INS)
INS is the broad name for a range of products that enhance traditional Cisco WAN switching networks. These products include Dial-Up Frame Relay, Voice Network Switching, and ATM Switched Virtual Circuits.

interleaved EIA
Same as "Fast EIA".

IPX Switch
A narrowband cell relay network switch from for private and public networks.

ISDN (Integrated Services Digital Network)
A service provided by the telephone company or OCC that supports combined customer voice and data connections over the twisted pair subscriber loop. Requires special equipment at the customer premise and a connecting central office switch that is capable of providing ISDN.

J

J1
A. multiplexed 24-channel circuit line to a PBX conforming to the Japanese TTC-JJ-20 circuit standard. Similar to E1, it operates at 2.048 Mbps.

junction node
A node handling inter-networking of domains.

junction trunk
A packet line connecting junction nodes.

L

LCON
The logical connection used to represent an individual routing entity.

LDM (Low Speed Data Module)
An IGX data front card that supports up to 8 synchronous or asynchronous data ports. When used with an LDI4/DDS, an LDP can provide 56-Kbps Digital Data Service (DDS) interfaces to the IGX switch.

LDP (Low Speed Data PAD)
An IPX data front card that supports up to 8 synchronous or asynchronous data ports. When used with an LDI4/DDS, an LDP can provide 56-Kbps Digital Data Service (DDS) interfaces to the IPX switch.

LEC (Lower Expansion Card)
An expansion back card for the IPX 32 that connects upper shelf bus to lower shelf bus and the active NPC to standby NPC.

line
Connects a user device to a service interface, for example, a router to an ASI or AUSM card, a data line to a data card, a frame relay line to an FRP or a port concentrator, or a T1 or E1 line to a CDP card.

link
The network connection between two nodes.

LMI (Local Management Interface)
The protocol and procedures for control of IPX frame relay connections. Used for configuration, flow control, and maintenance of these connections.

local addressing

A frame relay addressing convention that uses the DLCI to identify the IPX frame relay port at the interface between the user device and the frame relay network. In local addressing, a particular DLCI is used only at the local FR connection. The DLCI may be reused at any other IPX node in the network.

local alarm

An IPX alarm indicating that the associated T1 line is down due to a local failure of its receive path.

local bus

An IPX utility bus (LB/0 or LB/1**)** located on the midplane, which provides the electrical connections between various front and back cards. For example, the front and back cards of the Low Speed Data PAD group (LDP and LDI) plug into this utility bus.

logical port

A frame relay circuit consisting of either 1, 6, 24 (T1,) or 31 (E1) contiguous DSO's on a T1 or E1 physical port.

M

major alarm

A local or remote failure that is affecting operation of the network.

MBS (Maximum Burst Size)

Maximum number of cells which may burst at the PCR but still be compliant.

MCR (Minimum Cell Rate)

The minimum cell rate that is supported by an ATM connection for an ABR connection.

MIR (Minimum Information Rate)

The minimum information rate that is supported by a frame relay connection.

minor alarm

A local or remote failure that is not affecting operation of the network, but nonetheless should be investigated.

MUXBUS

A high-speed IPX backplane bus that carries data and timing between card slots for both circuit line and packet line data. Consists of the TDM bus carrying the data and the system clock bus that is used to synchronize all data flowing on and off the TDM bus.

N

n+1 redundancy

A redundancy method in which a group of cards share the same standby redundant card.

Network-to-Network Interface (NNI)

The protocol at a frame relay port that serves as a bidirectional interface between a local Cisco WAN switching network and a separate and independent “other” network.

node

An IPX/IGX/BPX switch serving as a connection point to the network. At a node, connections from service lines are routed to trunks for transmission to other nodes in the network.

NPC (Network Processor Card)

Micro-processor based system controller front card that contains the software used to operate the IPX switch.

NPM (Network Processor Module)

Micro-processor based system controller front card that contains the software used to operate the IGX switch.

Nrm

Maximum number of cells a source may send for each forward RM cell, i.e., an RM cell must be sent for every Nrm-1 data cells.

NTC (Network Trunk Card)

IPX front card that coordinates fastpacket trunk traffic to another node via a number of backcards: T1, E1, Y1, and subrate (RS449, X.21, and V.35).

NTM (Network Trunk Module)

IGX front card that coordinates fastpacket trunk traffic to another node via a number of backcards: T1, E1, Y1, and subrate (RS449, X.21, and V.35).

O

OC-3

Standard optical transmission facility rate of 155.20 Mbps.

OCC (Other Common Carrier)

In the United States, reference to all the other telecommunications companies providing various transmission services other than AT&T.

P

packet line

Packet line referred to a line used to carry FastPackets between IPX nodes in a network. The term in these documents is replaced by the more general “trunk” which is defined as a physical link from node to node, node to shelf, or node to network. The trunk may be one that supports 24-byte FastPackets (packet trunk), or one that supports 53 byte ATM cells (cell trunk).

packet switching

A system that breaks data strings into small units (packets), then individually addresses and routes them through the network.

PAD (Packet Assembler/Disassembler)

A device that converts a serial data stream into discrete packets in the transmit direction and converts the received packets back into a serial data stream. Adds header information in the transmit packet to allow it to be routed to the proper destination.

partially-interleaved EIA

One control lead in each direction, generally RTS-CTS, is transmitted in same byte as seven data bits. For fast control lead response to data being turned on and off.

PBX (private branch exchange)

Digital or analog telephone switchboard, classified as customer premise equipment (CPE), used to connect private and public telephone networks.

PCM (Pulse Code Modulation)

The system for transmitting telephone signals digitally. Voice is sampled 8000 times per second and converted to an 8-bit digital word.

PCR (Peak Cell Rate)

The maximum rate for an ATM connection at which cells are allowed into the network.

PCS (Port Concentrator Shelf)

The PCS is an external shelf that expands the capacity of the FRP card. The PCS is sued with the FRP-2 (IPX switch) or FRM-2 (IGX switch) card to 44 frame relay connections. The PCS connects to the FRI-2.X.21 backcard.

PIR (Peak Information Rate)

The peak level in bits per second allowed for a frame relay connection.

PLCP (Physical Layer Convergence Protocol)

A protocol defined for use with Switched Megabit Data Service. Used on DS3 ATM trunks in the BPX switch.

PLPP (Physical Layer Protocol Processor)

A custom VLSI processor used in the T3 ATM port interface of the BPX BNI card to handle the coding and decoding of the PLCP bit structure. Functions handled by the PLPP include header check sequence generation and checking, DS3 framing, and optional payload scrambling/descrambling.

plesiochronous network

A network where there is more than one source of network timing. The multiples sources must be operating at the same frequency but are not phase locked (synchronous) with each other.

port

Refers to a signal connection on a data back card that interfaces to a customer circuit or data device. The number of ports on a card ranges from 1 to 8 depending on the particular card type.

PRI (Primary Rate Interface)

An ISDN interface to primary rate access. Primary rate access consists of a single D channel for signalling and 23 (T1) or 30 (E1) B (bearer) channels for user data. A PRI is typically carried on T1 or E1 facilities.

privilege level

A level between 1 and 6 that is assigned to each IPX command. Each operator is assigned a privilege level by the system administrator. The operator may only access and execute commands equal to or lower than his or her own privilege level. Level 1 is the highest and level 6 is the lowest.

PVCs

Permanent Virtual Connections (circuits). Connections that are assigned but not connected until data is sent, thereby not using bandwidth when idle.

Q

Q.921/Q.931

ITU-T specifications for the ISDN use network interface (UNI) data link layer.

QSIG

A common-channel message-oriented signalling protocol, defined by the European Telecommunications Standard Institute (ETSI), commonly used by private branch exchanges (PBXes). The INS Dynamic Network Switching application supports QSIG signalling to the Cisco WAN switching network.

queue

A buffer that is used to temporarily hold data while it waits to be transmitted to the network or to the user.

R

RIF (Rate increase factor)

Controls the amount by which the cell transmission rate may increase upon receipt of an RM cell.

RDF (Rate decrease factor)

Controls the amount by which the cell transmission rate may decrease upon receipt of an RM cell.

red alarm

Another name for local alarm as the local alarm lamp on most digital transmission equipment is red in color.

remote alarm

An IPX alarm indicating that the associated T1 line is down due to a receive line failure on another node. (See also yellow alarm.)

RPS (repetitive pattern suppression)

Also called data frame multiplexing (DFM). An option for data circuits where repeating strings of data are replaced on the packet line by a single occurrence of the data string and a code that indicates to the far end how may repetitions of the string was being transmitted. Used to conserve network bandwidth.

robbed bit signaling

A type of signaling used on T1 lines where the signaling bits for each channel are substituted for the least significant voice bit in each channel word during frames 6 and 12.

RS-232

A physical and electrical interface standard for a low-speed, unbalanced, serial, data interface adopted by the EIA committee on data communications. Generally used for data circuits operating at data rates below 56 Kbps.

RS-422/423

Another EIA standard electrical interface for serial data circuits operating at higher data rates than RS232. RS422 is a balanced interface; RS423 is unbalanced. Uses RS-449 for the physical interface (connector).

RS-449

The physical interface for the RS422 and R423 electrical interfaces. Contains the Processor Controller Card and the PCC utility bus, and provides system timing and control via the system bus.

S

SAR (Segmentation and Reassembly)

The process of breaking a dataframe containing data from a number of virtual paths or circuits apart so that the individual paths/circuits can be switched by reassembling the data into a new frame with a different sequence.

SCC (System Clock Card)

An IPX backcard that works in conjunction with the NPC. The SCC provides a centralized clock generation function and provides serial and LAN port interfaces.

SCM (System Clock Module)

An IGX backcard that works in conjunction with the NPM. The SCM provides a centralized clock generation function and provides serial and LAN port interfaces.

SCR (Sustainable Cell Rate)

Rate above which incoming cells are either tagged or discarded.

SDP (Synchronous Data PAD)

An IPX front card that supports one to four medium speed, synchronous data channels.

SDI (Synchronous Data Interface)

The back card for the SDP (IPX switch) or HDM (IGX switch) cards. The SDI is available with V.24, X.21, and V.35 interfaces.

seamless international network

An IPX network that is configured to carry traffic over international borders (E1-T1 or T1-E1)—see also gateway.

Simple Gateway

Refers to FastPacket to ATM interworking with respect to the IPX and IGX nodes. In the simple gateway mode, FastPackets are encapsulated in their entirety into cells. Compare with complex gateway.

SIU (Serial Interface Unit)

A set of circuits common to all BPX cards used for transmitting and receiving via the crosspoint switch.

Soft PVC

A PVC in the INS Dial-Up Frame Relay application that is dormant in the networks database until it is activated by a call into the network by a user.

spanning tree

An IPX network topology in which there is only one path available between any two sources in a frame relay multicast group. Spanning trees are required to prevent frames broadcast from a single source to multiple receptors from circulating endlessly around the network a result of frame relay circuits not having properly closed loops.

speech detection
Determining the presence or absence of speech for Digital Speech Interpolation. Performed in either the CDP card or VDP card in an IPX node.

split clock
A data clocking configuration where the timing for the transmit data is obtained from one source (e.g. user device) and the timing for the receive data is obtained from another source (e.g. IPX switch).

Status Enquiry
A message transmitted by a FR NNI port requesting an updated status from the attached foreign network. This message is used as a heartbeat to detect when a port has failed.

StrataBus
On the BPX switch, contains crosspoint wiring used to carry ATM trunk data between both the network interface and service interface modules and the crosspoint switch as well as providing control, clock, and communications.

subrate data
Multiple low-speed data circuits carried in a single DS0 timeslot.

superrate data
Single high-speed data circuit carried in multiple DS0 timeslots.

SCR (Sustained Cell Rate)
Long term limit on the rate a connection can sustain.

SVC (switched virtual circuit)
A virtual circuit that is dynamically established on demand and torn down when transmission is complete. SVS do not need to reserve any network resources when they are not in use. Called a switched virtual connection in ATM terminology. Compare with PVC.

system bus
A two-part IPX data bus. One part carries system commands between the PCC all other IPX cards; the other carries time division multiplexed data.

T

T1
The standard US. multiplexed 24-channel voice/data digital span line. Operates at a data rate of 1.544 Mbps.

T3
Transmission service at DS3 rate of 44.736 Mbps.

TBE (Transient Buffer Exposure)
The negotiated number of cells that the network would prefer to limit the source to send during the start-up period.

TDM (time division multiplexing)
The process of combining several communication channels by dividing a channel into time increments and assigning each channel to a timeslot.

timestamp
A field in certain FastPacket formats that indicates the amount of time the packet has spent waiting in queues during the transmission between its source and destination nodes. Used to control the delay experienced by the packet.

Trm
An upper bound on the time between RM cells for an active source, i.e., RM cell must be sent at least once every Trm msec.

trunk
A physical link between two nodes. The trunk may be one that supports 24-byte FastPackets (packet trunk), or one that supports 53 byte ATM cells (cell trunk.)

trunk conditioning
A set of signalling and information bits that indicate a DS1 line failure.

trunk queues
The buffers in packet line cards (NTC, TXR) where the various FastPackets are queued up for transmission over the packet line(s). The buffers attempt to prioritize each packet so it experiences minimum delay.

U

-law
An analog to digital encoding scheme used to convert voice samples to an 8-bit data word used in D3/D4 T1 multiplex equipment.

UBR
Unspecified Bit Rate.

UNI (User to Network Interface)
The user to network interface, used for ATM connection to CPE. Compare with NNI.

UPC (Usage Parameter Control)
A general procedure for controlling the rate of user data applied to an ATM network. There are a number of different algorithms for performing UPC. See also GCRA.

USART (Universal Synchronous/Asynchronous Receiver Transmitter)
A single-chip device used in certain applications that allows microprocessors to communicate with input/output (I/O) devices.

User to Network Interface (UNI)
The protocol at a frame relay port that passes information between the network and the user device attached to the port.

V

V.21
A CCITT interface standard often used for data transmission over modems.

V.35

A data communications interface standard adopted by the CCITT. Often used for data circuits operating at 56 Kbps and above.

VAD (Voice Activity Detection)

Used to statistically compress voice by not sending packets in the absence of speech.

VBR (Variable Bit Rate)

Connection type for variable bit rate traffic such as bursty data. Compare with CBR and ABR.

VC_Q

Frame relay buffer allocation parameter that specifies the maximum queue size reserved in the FRP card for the FR connection.

virtual circuit

A circuit that acts like it is an individual transmission path but is actually shared with other circuits over a single transmission path. Compare with PVCs.

VNS

The adjunct processor used in the INS Voice Network Switching application. The VNS is co-located with and connected to an IGX or IPX switch.

Voice Network Switching

An INS application used to provide voice or data switched virtual circuits over a Cisco WAN switching network for PBXes using either QSIG or DPNSS signalling.

VS/VD (Virtual Source/Virtual Destination)

ATM Forum Traffic Management 4.0 method of providing congestion flow control for ABR connection types. Resource Management (RM) cells are used to convey management information between sources and destinations.

vt (virtual terminal)

An IPX control terminal that is the active control terminal at one node but is physically attached to another node.

W

WAN (Wide Area Network)

A network of transmission circuits generally spanning a large region or territory for transmission of voice and data between widespread end users. An IGX/BPX network is an example of a WAN.

X

X.21

A CCITT standard for data interfaces transmitting at rates up to approximately 2 Mbps.

X.25

A commonly-used standard that defines the protocol for low-speed data packet networks.

XON/XOFF

A simple communications protocol for controlling the flow of data from one device to another. An XON sent from a receiving device indicates it is ready to accept data and the transmitting device may begin to output data. An XOFF from the receiving device indicates that it can no longer store any more data and the transmitting device should temporarily cease transmitting.

Y

Y-cable(s)

A short adapter cable forming an electrical branch (thus the term Y) for connecting a single customer data or trunk connection to two identical back cards to provide hardware redundancy on the IGX switch.

Y-cable redundancy

A redundancy type used in the IPX switch when a 1:1 card redundancy is implemented using a split or Y-cable for the data connection between the user device and the primary and standby IGX interface card.

Y1

A digital trunk conforming to the Japanese “Y” circuit standard, for use as a packet line. Similar to T1, it operates at 1.544 Mbps.

yellow alarm

Another name for remote alarm as the remote alarm lamp on digital transmission equipment is always yellow in color.

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V