



SmartSwitch 6500 User Guide

35 Industrial Way
Rochester, NH 03866
USA
(603) 332-9400

Part Number 04-0050-01 Rev. A
Order Number 9032706

NOTICE

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made. The hardware, firmware, and software described in this manual are subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Copyright 1998 - 99 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005
All Rights Reserved

Printed in the United States of America

SmartSwitch 6500 User Guide

Part Number 04-0050-01 Rev. A

Order Number: 9032706

SmartSwitch, SPECTRUM, LANVIEW, MicroMMAC, and BRIM are registered trademarks and Element Manager, EPIM, EPIMA, EPIM-F1, EPIM-F2, EPIM-F3, EPIM-T, EPIM-X, FOT-F, FOT-F3, HubSTACK, SEH, SEHI, and TMS-3 are trademarks of Cabletron Systems, Inc. All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

FCC CLASS A NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Note This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the SmartSwitch 6500 User Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.



Caution Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

DOC CLASS A NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

DECLARATION OF CONFORMITY ADDENDUM

Application of Council Directive(s): 89/336/EEC
73/23/EEC

Manufacturer's Name: Cabletron Systems, Inc.

Manufacturer's Address: 35 Industrial Way
P. O. Box 5005
Rochester, NH 03866

Product Name: SmartSwitch 6500

European Representative Name: Mr. J. Solari

European Representative Address: Cabletron Systems, Limited
Nexus House, Newbury Business Park
London Road, Newbury
Berkshire RG13 2PZ, England

Conformance to Directive(s)/Product Standards: EC Directive 89/336/EEC
EC Directive 73/23/EEC
EN 55022
EN 50082-1
EN 60950

Equipment Type/Environment: Networking Equipment, for use in a Commercial or Light Industrial Environment.

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer: Full Name: **Mr. Ronald Fotino**
Title: **Principal Compliance Engineer**
Location: **Rochester, NH. U.S.A.**

Legal Representative in Europe: Full Name: **Mr. J. Solari**
Title: **Managing Director - E.M.E.A.**
Location: **Newbury, Berkshire, England**

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

The IOM-29-4, IOM-29-4-IR, IOM-29-4-LR, IOM-39-1 and IOM-39-1-LR connectors use Class 1 Laser transceivers. Read the following safety information before installing or operating one of these modules.

The Class 1 Laser transceivers use an optical feedback loop to maintain Class 1 operation limits. This control loop eliminates the need for maintenance checks or adjustments. The output is factory set, and does not allow any user adjustment. Class 1 Laser transceivers comply with the following safety standards:

- 21 CFR 1040.10 and 1040.11 U. S. Department of Health and Human Services (FDA).
- IEC Publication 825 (International Electrotechnical Commission).
- CENELEC EN 60825 (European Committee for Electrotechnical Standardization).

When operating within their performance limitations, laser transceiver output meets the Class 1 accessible emission limit of all three standards. Class 1 levels of laser radiation are not considered hazardous.

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6dBm or 55×10^{-6} watts.

Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm^{-2} or $8 \times 10^3 \text{ W m}^{-2} \text{ sr}^{-1}$.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, you must remove power from the network adapter.

FIBER OPTIC PROTECTIVE CAPS



Warning READ BEFORE REMOVING FIBER OPTIC PROTECTIVE CAPS.

Cable assemblies and MMF/SMF ports are shipped with protective caps to prevent contamination. To avoid contamination, replace port caps on all fiber optic devices when not in use.

Cable assemblies and MMF/SMF ports that become contaminated may experience signal loss or difficulty inserting and removing cable assemblies from MMF/SMF ports.

Contamination can be removed from cable assemblies by:

1. Blowing surfaces with canned duster (Chemtronics p/n ES1270 or equivalent).
2. Using a fiber port cleaning swab (Alcoa Fujikura LTS p/n ACT-01 or equivalent) saturated with optical-grade isopropyl alcohol, gently wipe the end surface of ferrules first; then wipe down the sides of both ferrules.
3. Blow ferrule surfaces dry with canned duster.

Contamination can be removed from MMF/SMF ports by:

1. Using the extension tube supplied with canned duster, blow into the optical port, being careful not to allow the extension tube to touch the bottom of the optical port.
2. Reconnect cable and check for proper mating. If problems remain, gently wipe out optical port with a DRY fiber port cleaning swab and repeat step 1.



Warning To avoid contamination, replace port caps on all fiber optic devices when not in use.

REGULATORY COMPLIANCE SUMMARY

SAFETY

The SmartSwitch 6500 meets the safety requirements of UL 1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 73/23/EEC.

EMC

The SmartSwitch 6500 meets the EMC requirements of FCC Part 15, EN 55022, CSA C108.8, VCCI V-3/93.01, EN 50082-1, and 89/336/EEC.

REVISION HISTORY

Document Name: *SmartSwitch 6500 User Guide*

Document Part Number: 04-0050-01 Rev. A

Document Order Number: 9032706

Author: Bruce Jordan

Editor: Carre Gibson

Illustrator: Mike Fornalski

Date	Revision	Description
October 1998	A	Initial release

TABLE OF CONTENTS

1	Introducing the SmartSwitch 6500	1-1
1.1	SmartSwitch 6500 Modules	1-2
1.1.1	Cell Storage Module (CSM)	1-2
1.1.2	Translation and Scheduling Module (TSM)	1-2
1.1.3	CPU Module	1-2
1.1.4	Input/Output Modules (IOMs)	1-3
2	Switch Installation and Setup	2-1
2.1	Receiving the SmartSwitch 6500	2-1
2.1.1	Inspecting the Order	2-1
2.1.2	Unpacking	2-3
2.1.3	Check Accessory Carton Contents	2-4
2.2	Switch Installation and Assembly	2-5
2.2.1	Mounting the Chassis	2-5
2.2.2	Installing The Power Supplies	2-5
2.2.3	Installing the CSM	2-7
2.2.4	Installing the TSM with CPU Daughter Board	2-9
2.2.5	Installing Additional TSM Modules	2-11
2.2.6	Installing Other Modules in the SmartSwitch 6500 Chassis	2-11
2.3	Configuring the Switch	2-13
2.3.1	Initial Network Configuration	2-13
2.3.2	Backup/Redundancy Configuration	2-16
2.4	LED Descriptions	2-19
2.5	Using the Console	2-20
2.5.1	Port Numbering	2-20
2.5.2	Console Commands	2-21
2.5.3	Console Time-out	2-23
2.5.4	Creating an Alias	2-23
2.5.5	Ambiguous Commands	2-23
2.5.6	Console Help	2-24
2.6	SmartSwitch ATM Administrator	2-25
2.6.1	PC Installation	2-27
2.6.2	Solaris Workstation Installation	2-27
2.6.3	Starting SmartSwitch ATM Administrator	2-27
2.6.4	Initial SmartSwitch ATM Administrator Set Up	2-27
2.6.5	Default Community Strings	2-28
2.6.6	Accessing Online Help	2-28
3	IP Over ATM and LANE	3-1
3.1	Creating an IP over ATM VLAN	3-1
3.1.1	Default ATM Addressing for IP over ATM	3-3

3.2	Creating an Emulated LAN	3-3
3.2.1	ATM Addressing for LAN Emulation	3-6
3.2.2	ELANs Across Multiple Switches	3-7
3.2.3	Switch Clients	3-7
3.2.4	Distributed LANE Services	3-8
3.2.5	ELAN Join Policies	3-9
4	PNNI Routing	4-1
4.1	PNNI Node Addressing	4-1
4.2	Multi-level PNNI Topology	4-2
4.2.1	Connecting Multiple Peer Groups	4-2
4.2.2	Physical Connections Between Peer Groups	4-6
4.3	Managing Parallel PNNI Links	4-8
4.3.1	Aggregation Tokens	4-9
5	Routing	5-1
5.1	Additional Routing Protocols	5-1
5.2	IISP Routes	5-1
5.2.1	IISP Routing Considerations	5-2
5.3	UNI Routes	5-4
5.4	Route Metrics	5-5
5.5	IP Routing	5-6
6	Virtual Ports and Static Connections	6-1
6.1	PVC Connections	6-1
6.1.1	Point-to-Point PVCs	6-1
6.1.2	Point-to-Multipoint PVCs	6-2
6.1.3	Connecting to Local Switch Client Through a PVC	6-4
6.2	PVP Connections	6-4
6.2.1	Connecting PVPs	6-6
6.3	Virtual Ports	6-7
6.3.1	Creating Virtual Ports	6-7
7	Traffic Management	7-1
7.1	Traffic Management Capabilities	7-1
7.1.1	Traffic Descriptors	7-1
7.1.2	Call Admission Control Policy	7-3
7.1.3	Queue Buffers	7-5
7.1.4	EFCI, EPD, and RM Cell Marking	7-7
8	Upgrades and Firmware	8-1
8.1	Upgrading and Changing Firmware	8-1
8.1.1	Accessing the Boot Load Prompt	8-1
8.1.2	Boot Load Commands	8-2
8.1.3	Upgrading Boot Load firmware	8-4

8.1.4	Upgrading POST Diagnostic firmware	8-5
8.1.5	Upgrading Switch Operating firmware	8-6
8.1.6	Using the Update Firmware Command	8-7
9	Troubleshooting	9-1
9.1	Troubleshooting IP over ATM	9-1
9.2	Troubleshooting LAN Emulation	9-2
9.3	Troubleshooting PNNI Links	9-3
9.3.1	Switches in Same Peer Group	9-3
9.3.2	Switches in Different Peer Groups	9-3
9.4	Troubleshooting Congestion	9-4
9.4.1	Diagnosing Congestion	9-4
9.4.2	Global Congestion	9-4
9.4.3	Port Congestion	9-5
9.5	Events and Alarms	9-6
9.5.1	Event Categories	9-6
9.5.2	Viewing Events and Alarms	9-7
9.5.3	Deleting Events and Alarms	9-8
9.6	Saving Core Dumps	9-9
A	Specifications	A-1
B	Agent Support	B-1
B.1	MIB, SMI, MIB Files and Internet MIB Hierarchy	B-1
B.1.1	ZeitNet Cabletron Proprietary MIBs	B-2
B.1.2	Relation Between Object Identifier and the Represented Value	B-3
B.1.3	Supported protocols	B-4
B.1.4	Supported SMI Formats	B-4
B.1.5	Zeitnet Cabletron Proprietary MIB Groups	B-4
B.1.6	SmartSwitch 6500 MIB Support	B-6
B.1.7	MIB Exceptions	B-6
B.2	Managing the SmartSwitch 6500	B-7
B.2.1	Console Commands that Affect the Agent	B-7
B.2.2	Default Community Strings	B-8
C	Technical Support	C-1
C.1	Telephone Assistance	C-1
C.2	FAX Service	C-1
C.3	Electronic Services	C-1
C.4	Placing A Support Call	C-1
C.5	Hardware Warranty	C-2
C.6	Software Warranty	C-2
C.7	Repair Services	C-2
D	Acronyms	D-1

Index I-1

LIST OF FIGURES

Figure 2-1	SmartSwitch 6500 chassis	2-2
Figure 2-2	SmartSwitch CSM and TSM modules	2-3
Figure 2-3	Rack mounting the SmartSwitch 6500 chassis	2-5
Figure 2-4	Module placement in the SmartSwitch 6500 chassis	2-7
Figure 2-5	Installing CSM in slot 9	2-8
Figure 2-6	Difference between TSM module and TSM/CPU module	2-9
Figure 2-7	Installing a TSM/CPU module in slot 8	2-10
Figure 2-8	SmartSwitch 6500 chassis with Ethernet switch, TSMs, and CSMs	2-12
Figure 2-9	SmartSwitch 6500 connections for configuration	2-16
Figure 2-10	CSM and TSM LEDs	2-20
Figure 2-11	SmartSwitch ATM Administrator	2-26
Figure 4-1	Physical connectivity for multi-peer group example	4-3
Figure 4-2	Logical representation of connectivity between groups A and B	4-6
Figure 4-3	Adding a third PNNI node for next level connectivity	4-7
Figure 4-4	Aggregation token values and parallel links	4-10
Figure 5-1	IISP route across PNNI domain	5-3
Figure 5-2	Routes needed for a second IISP switch	5-3
Figure 5-3	IP routing through SW1 for connectivity to the Ethernet network	5-7
Figure 6-1	Terminating PVPs	6-7
Figure 8-1	Memory locations affected by the boot load commands	8-3
Figure B-1	Internet MIB hierarchy	B-2
Figure B-2	CSI ZeitNet Private MIBs	B-3
Figure B-3	Cabletron SmartSwitch 6500 object identifier example	B-4

LIST OF TABLES

Table 2-1	I/O module ID numbers	2-4
Table 2-2	Module combinations in 6500 chassis	2-12
Table 2-3	CSM LEDs	2-19
Table 2-4	TSM LEDs	2-19
Table 2-5	Default accounts and passwords	2-27
Table 3-1	ELAN Join Policies	3-10
Table 7-1	Traffic descriptor type number explanation	7-2
Table 8-1	Boot load commands	8-2
Table 9-1	Settings for Class of Service Queues	9-4
Table A-1	Hardware Specifications	A-1
Table A-2	Physical Specifications	A-1
Table A-3	ATM Port Specifications	A-2
Table A-4	Protocols Standards and Specifications	A-2
Table A-5	Management Standards and Specifications	A-3
Table A-6	RJ-45 to DB-9 Adapter (PC Serial Port Adapter)	A-3
Table B-1	Zeitnet proprietary MIB groupings	B-4

1 INTRODUCING THE SMARTSWITCH 6500

Welcome to the SmartSwitch 6500 User Guide. The SmartSwitch 6500 is a high-performance ATM switch that supports 10 Gbps non-blocking capacity, massive buffering capabilities, superior traffic management and shaping, a wide variety of port interfaces, and redundancy for fault tolerance in backbone environments.

The SmartSwitch 6500 fits into the SmartSwitch 6C110 chassis, and is based on a multi-module architecture consisting of the following three main modules

- Cell Storage module (CSM), contains the cell memory (512k cells)
- Translation and Scheduling module (TSM), supports the physical ports and hardware for traffic management and shaping
- CPU module (daughter card on TSM), contains the hardware for running the SmartSwitch 6500 system software
- Input/Output modules (IOM), provides the physical ATM ports (daughter cards on TSM)

Collectively, by communicating with each other over the chassis' high-speed backplane, these modules make up the SmartSwitch 6500, an integrated, high performance, ATM backbone switch. Furthermore, SmartSwitch 6500 modules can coexist within the SmartSwitch 6C110 chassis with other Cabletron networking devices. For example, the slots of the 6C110 chassis can be populated by a mix of SmartSwitch 6500 modules and SmartSwitch 6000 Ethernet switches.

Both the CSM and TSM are hot swappable. This means that you can install and remove TSMs and CSMs from the 6C110 chassis without turning of chassis power. However, removing either the active CSM or TSM/CPU does not trigger automatic switch-over to the redundant modules. For switch-over to occur the SmartSwitch 6500 must be rebooted.

By performing the steps described in the next two chapters of this manual, your switch will be physically assembled and installed, accessible on your Ethernet network, configured for redundancy, and running either an IP over ATM VLAN or an emulated Ethernet or Token Ring LAN.

Subsequent chapters provide instructions and information about switch use, maintenance, and problem solving. These topics include

- Creating multi-level PNNI network topologies
- Creating PVCs and PVP connections
- Creating and using virtual ports
- Adding routes
- Dealing with bandwidth and controlling congestion
- Upgrading software
- Troubleshooting



Note For detailed descriptions of SmartSwitch 6500 console commands and their use, see the SmartSwitch 6500 Reference Manual.

1.1 SMARTSWITCH 6500 MODULES

Before continuing, read the following section. This section is provided to quickly give you a better, more detailed understanding of the function and operation of each of the SmartSwitch 6500's modules.

1.1.1 Cell Storage Module (CSM)

CSMs provide the main switching fabric for the SmartSwitch 6500. The CSM also provides cell storage and output queuing, and dynamically shares memory among all active connections. The CSM monitors overall utilization of shared memory and communicates this information to the TSM modules, where it's used in making decisions about incoming cell-acceptance. The CSM controls TSM access to the backplane cell data busses at both ingress (TSM-to-CSM) and egress (CSM-to-TSM). The CSM can also provide clock and sync signal generation for network clocking.

For redundancy, the SmartSwitch 6500 supports up to two CSMs in a single 6C110 chassis. When one CSM is active, the other CSM is in standby mode. If the active CSM fails, the standby CSM can be made to assume the active role.



Note CSMs must reside in SmartSwitch 6C110 chassis slots nine (9) or ten (10).

1.1.2 Translation and Scheduling Module (TSM)

TSMs are responsible for SmartSwitch 6500 traffic management functions. For example, TSMs perform header translation for ingress and egress cell traffic, provide port queue management for ABR (including EPD and PPD during congestion), and EFCI marking for forward congestion. TSMs are responsible for per-port/per-class queue management, cell scheduling and both physical and logical multicast support. TSMs also provide system interfaces for the CPU modules, the SAR, and all I/O modules.

The SmartSwitch 6C110 chassis can contain up to eight TSMs, two of which can contain CPU modules. Also, each TSM can support up to two IOMs; depending on the interface type, this provides each TSM with up to eight ATM ports.

1.1.3 CPU Module

CPU modules are mounted on TSMs as daughter cards. The CPU module runs the system software, and provides both intra-switch and inter-switch communication for configuration and monitoring. The CPU module is also responsible for providing both a serial and Ethernet interface, through which the user interface and network management facilities are accessed.



Note While the CPU module provides the serial and Ethernet interfaces, the external connectors for these interfaces reside on the CSM module.

For redundancy, the SmartSwitch 6500 allows two CPU modules (each mounted on a separate TSM) to exist within the same SmartSwitch 6C100 chassis. When one CPU module is active, the other CPU is in standby mode. If the active CPU module fails, the standby CPU module can be made to assume the active role.



Note The TSMs that support the CPU modules must reside in SmartSwitch 6C110 chassis slots seven (7) or eight (8).

1.1.4 Input/Output Modules (IOMs)

IOMs provide the physical ATM ports for the SmartSwitch 6500 and are mounted as daughter cards on the TSMs. The TSMs of the SmartSwitch 6500 support a number of different I/O modules with a variety of interfaces and media types; I/O modules are described in detail in Appendix A, "Specifications." Each TSM can support up to two I/O modules, and each I/O module provides four physical ports (one physical port per OC-12 I/O module). This allows for a maximum of eight ports per TSM, and a total of 64 ports for a SmartSwitch 6C110 chassis populated by the maximum number of TSMs (eight TSMs).

2 SWITCH INSTALLATION AND SETUP

After reading this chapter, you will be able to perform the following tasks:

- Install the SmartSwitch 6500 switch modules into the SmartSwitch 6500 chassis
- Complete the initial configuration
- Use the console interface
- Install the SmartSwitch ATM Administrator graphical management software



Note For detailed information about setting up the SmartSwitch Chassis (6C110), see the 6C110 SmartSwitch 6500 Overview and Setup Guide.

2.1 RECEIVING THE SMARTSWITCH 6500

Your SmartSwitch 6500 is shipped to you in several cartons. The number of cartons and their contents depends on which components you order.

2.1.1 Inspecting the Order

The following is a general list of cartons and their contents that comprise a SmartSwitch 6500.

- SmartSwitch 6500 chassis with fan tray installed (see Figure 2-1)
- 6C205-3 power supply (or supplies); one per carton
- CSM module (or modules); one unit per carton (see Figure 2-2)
- TSM module (or modules) with CPU daughter board and I/O modules installed; one unit per carton (see Figure 2-2 and Figure 2-6)
 - Additional TSMs (without CPU daughter boards) with I/O modules installed; one unit per carton

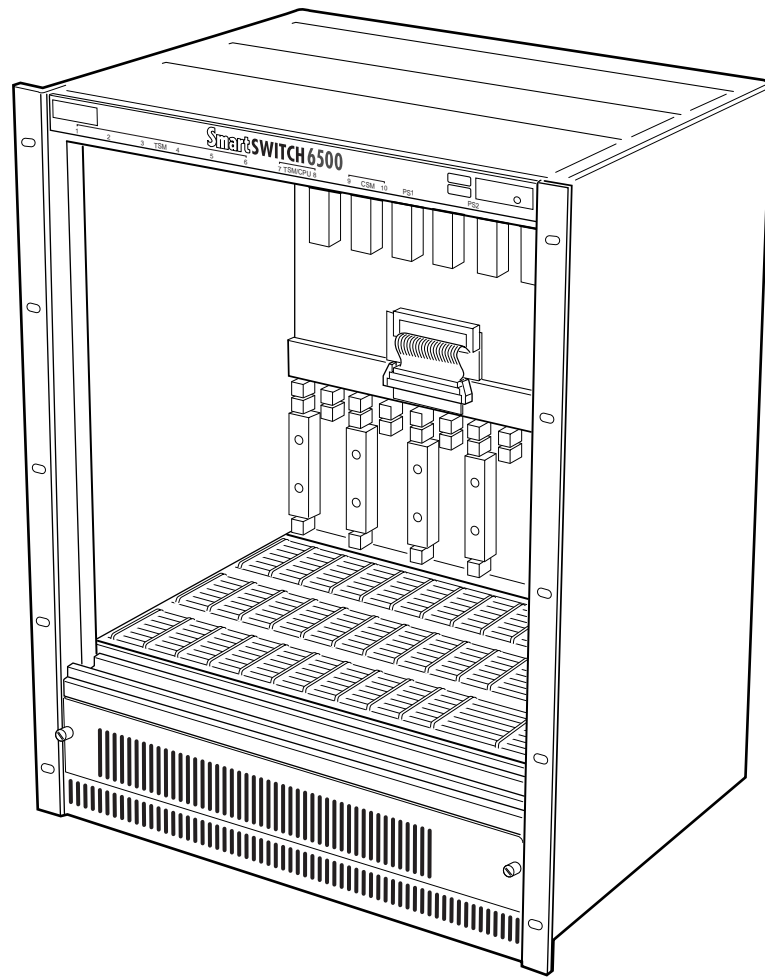


Figure 2-1 SmartSwitch 6500 chassis

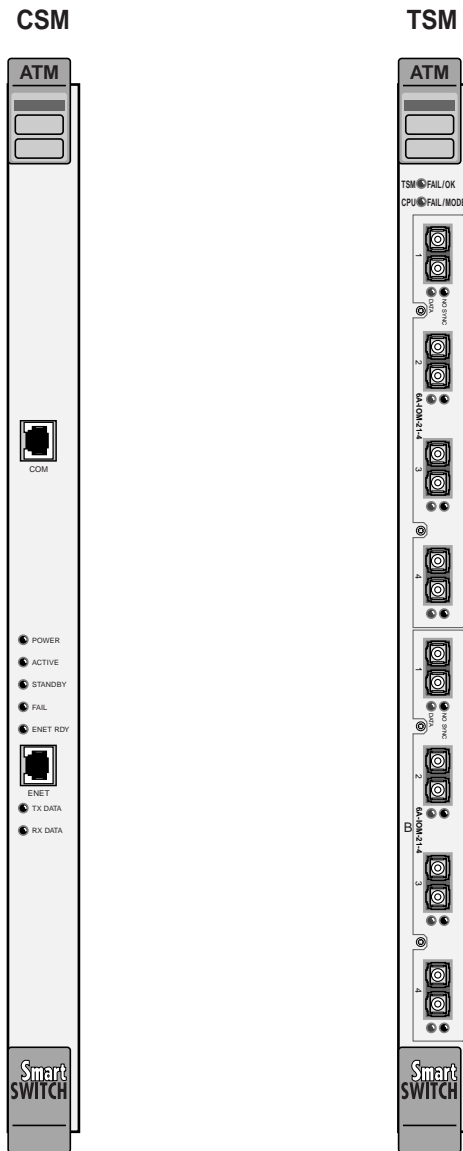


Figure 2-2 SmartSwitch CSM and TSM modules

2.1.2 Unpacking

1. Carefully unpack each component of the SmartSwitch 6500 (chassis, TSMs, CSM, and so on). Inspect each component for damage. Do not attempt to install damaged components. Contact the Cabletron Systems Global Contact Center immediately (see Appendix C, "Technical Support")
2. Inspect the TSMs. Make certain that the I/O modules installed are of the correct type and number (See Table 2-1).

Table 2-1 I/O module ID numbers

Face Plate Number	Physical Specification
IOM-21-4	155 Mbps OC-3/STM-1, MMF/SC (4 port)
IOM-22-4	155 Mbps STS-3c/STM-1, UTP-5/RJ-45 (4port)
IOM-29-4	155 Mbps OC-3/STM-1, SMF-IR/SC (1port) MMF/SC (3 port)
IOM-29-4-IR	155 Mbps OC-3/STM-1, SMF-IR/SC (4 port)
IOM-29-4-LR	155 Mbps OC-3/STS-1, SMF-LR/SC (4 port)
IOM-31-1	622 Mbps OC-12/STM-4, MMF/SC (1 port)
IOM-39-1	622 Mbps OC-12/STM-4, SMF-IR/SC (1 port)
IOM-39-1-LR	622 Mbps OC-12/STM-4, SMF-LR/SC (1 port)
IOM-67-4	45 Mbps DS-3, Coax/BNC (4 port)
IOM-77-4	34 Mbps E-3, Coax/BNC (4 port)

If the I/O module configuration is incorrect, contact the Cabletron Systems Global Contact Center immediately.

2.1.3 Check Accessory Carton Contents

Open the accessory carton and check that it contains the following items:

- 7-foot UTP cable terminated on both ends with RJ-45 connectors
- RJ-45 to 9-pin female adapter (labeled PC)
- Console cabling instruction sheet
- Diskettes containing switch software, MIB files, and release notes
- SmartSwitch 6500 Release Notes
- CD-ROM containing SmartSwitch ATM Administrator software for Windows 95/98, Windows NT, and Solaris 2.4/2.5
- CD-ROM containing the SmartSwitch 6500 User Guide, Reference Manual, related manuals, and Acrobat Reader

If any of these items is missing, contact the Cabletron Systems Global Contact Center immediately.

2.2 SWITCH INSTALLATION AND ASSEMBLY

The following is a list of steps for assembling your SmartSwitch 6500. Refer to Figure 2-4 for proper module placement.

2.2.1 Mounting the Chassis

1. Find someone to assist you. The SmartSwitch 6500 chassis is heavy enough to make this a two-person task.
2. Select a spot on a standard 19 inch equipment rack that provides at least two inches of air space above and below the chassis. This is necessary for proper ventilation and heat dissipation.
3. Secure the SmartSwitch 6500 to the equipment rack using the screws provided with the equipment rack. The chassis is secured by ten screws, five screws per side (see Figure 2-3).

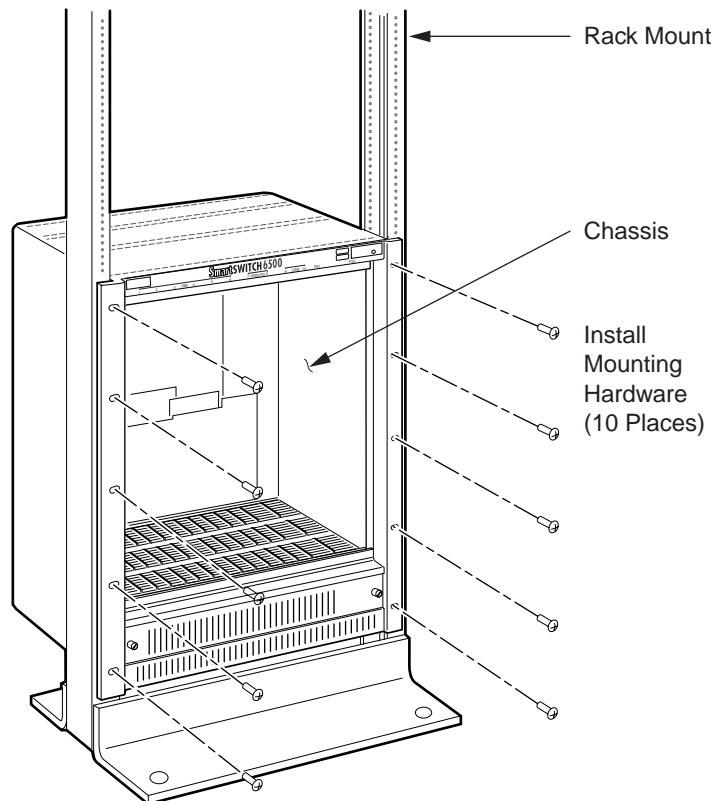


Figure 2-3 Rack mounting the SmartSwitch 6500 chassis

2.2.2 Installing The Power Supplies

1. Using a flat blade screwdriver, unscrew and remove the metal power supply blanks. The power supply blanks reside in the slots labeled PS1 and PS2.



Warning Never attempt to install a power supply while it is plugged in and operating.

2. With the power supply's power cord receptacle at the bottom, align the top and bottom of the power supply with the tracks in the slot. Slide the power supply into the chassis. If properly aligned, the power supply should slip in easily. Do not force the power supply; if it binds during insertion, remove the power supply and try inserting it again.



Note The power supply obscures the view of the tracks at the bottom of the chassis, so be sure to look at that area as you begin to slide the power supply into the chassis.

3. With the power supply in contact with the chassis backplane, press firmly until the power supply engages with the backplane's power connector.
4. Use a flat blade screwdriver to secure the power supply to the SmartSwitch chassis by tightening the two attached, slotted screws.
5. Insert the power cord into its receptacle on the front of the power supply. Plug the other end of the power cord into an appropriate power outlet.

If your SmartSwitch 6500 has a second power supply, repeat steps 1 through 5.

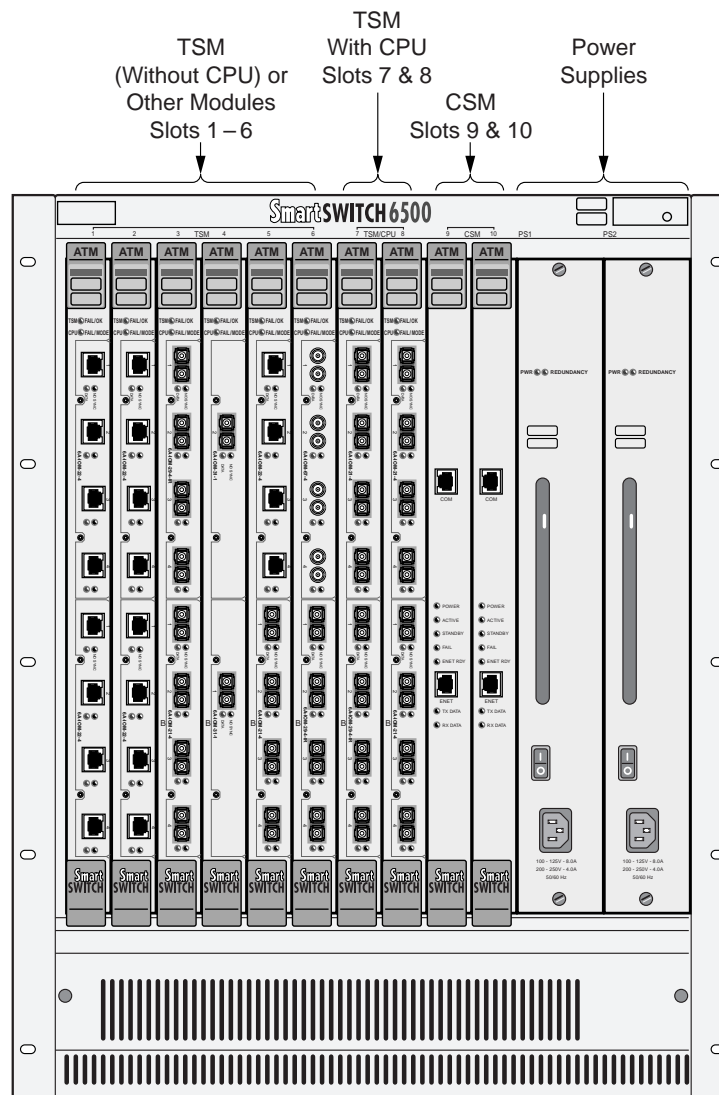


Figure 2-4 Module placement in the SmartSwitch 6500 chassis

2.2.3 Installing the CSM

Follow these instructions to install the CSM module into the chassis.

1. Remove the metal blank that covers either slot 9 or slot 10 of the chassis (CSMs can reside only in slots 9 and 10). See the legend on the top edge of the SmartSwitch 6500 chassis.
2. Open the ejectors at the top and bottom of the CSM module.
3. With the ejector labeled **6A-CSM512** at the top, align the top and bottom of the CSM module with the tracks in the slot (see Figure 2-5).
4. Slide the CSM module into the chassis. The CSM module obscures the view of the tracks at the bottom of the chassis, so be sure to look at that area as you begin to slide the module into the chassis.
5. Close the ejectors. The installation is complete.

If you have a second CSM module, repeat steps 1 through 5.

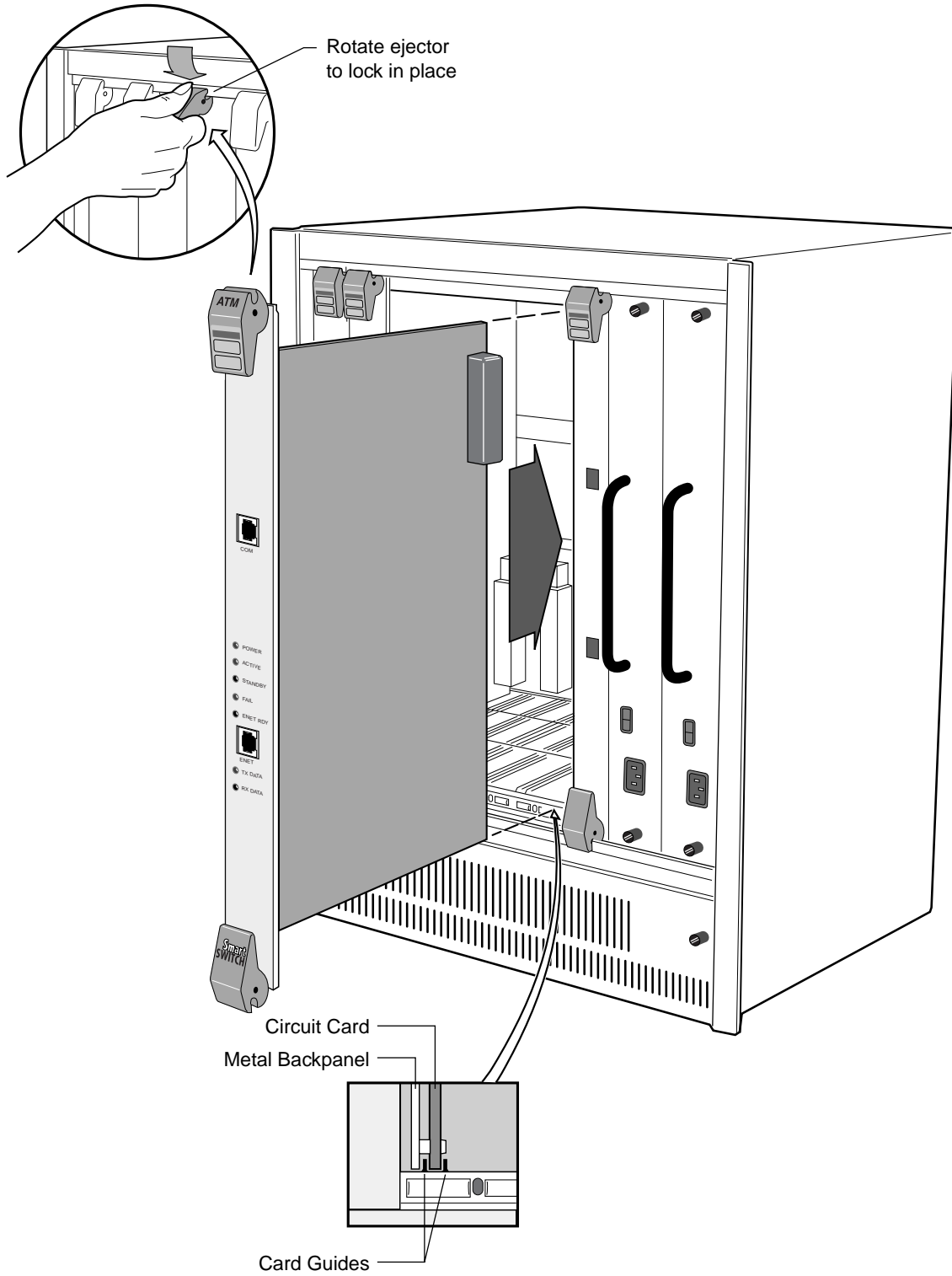


Figure 2-5 Installing CSM in slot 9

2.2.4 Installing the TSM with CPU Daughter Board

Follow these instructions to install the TSM/CPU module into the chassis.

1. Make sure that the TSM has a CPU daughter board installed (see Figure 2-6).
2. Remove the metal blank that covers either slot 7 or slot 8 of the chassis (TSMs with CPU daughter cards can reside only in slots 7 and 8). See the legend on the top edge of the SmartSwitch 6500 chassis.
3. Open the ejectors at the top and bottom of the TSM/CPU module.
4. With the ejector labeled **6A-TSM512** at the top, align the top and bottom of the TSM/CPU module with the tracks in the slot (see Figure 2-7).
5. Slide the TSM/CPU module into the chassis. The TSM module obscures the view of the tracks at the bottom of the chassis, so be sure to look at that area as you begin to slide the module into the chassis.
6. Close the ejectors. The installation is complete.

If you have a second TSM/CPU modules, repeat steps 1 through 6.

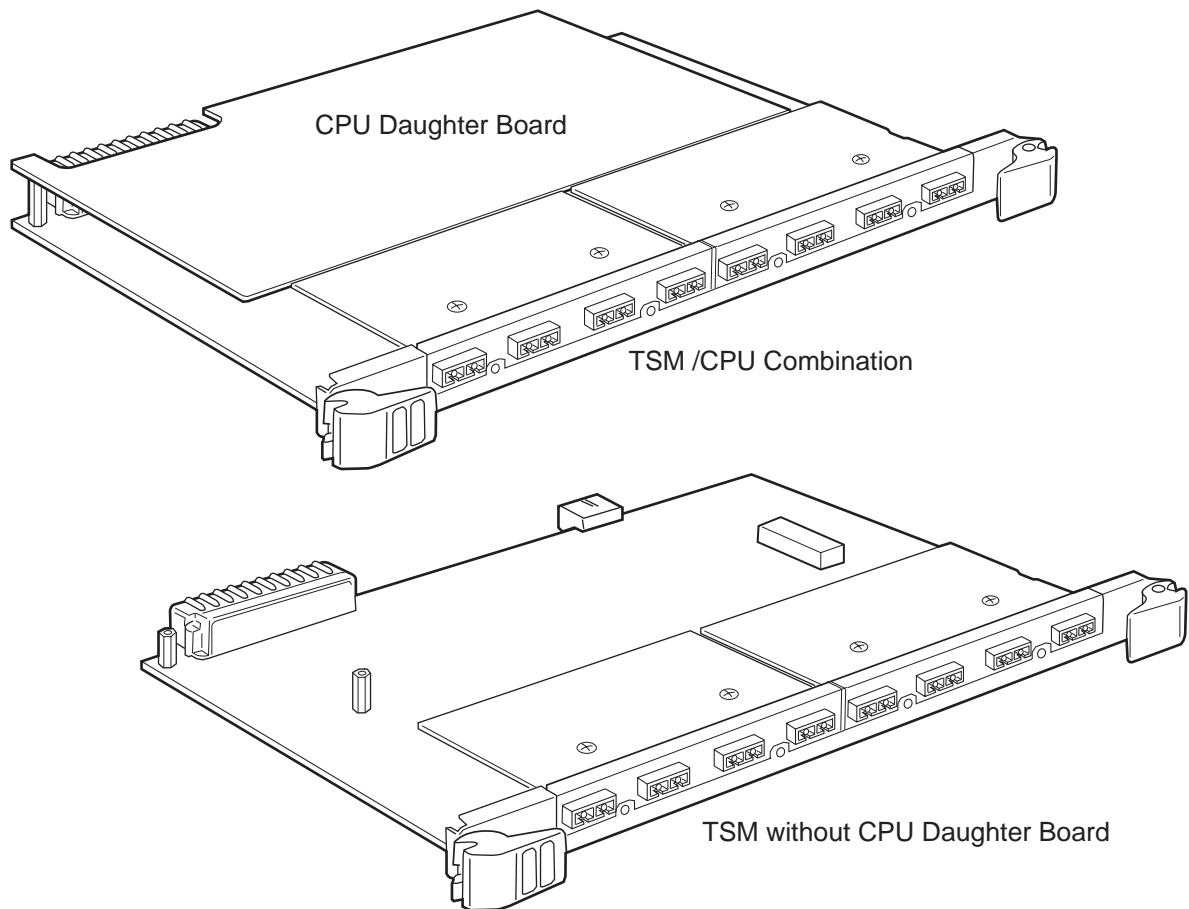


Figure 2-6 Difference between TSM module and TSM/CPU module

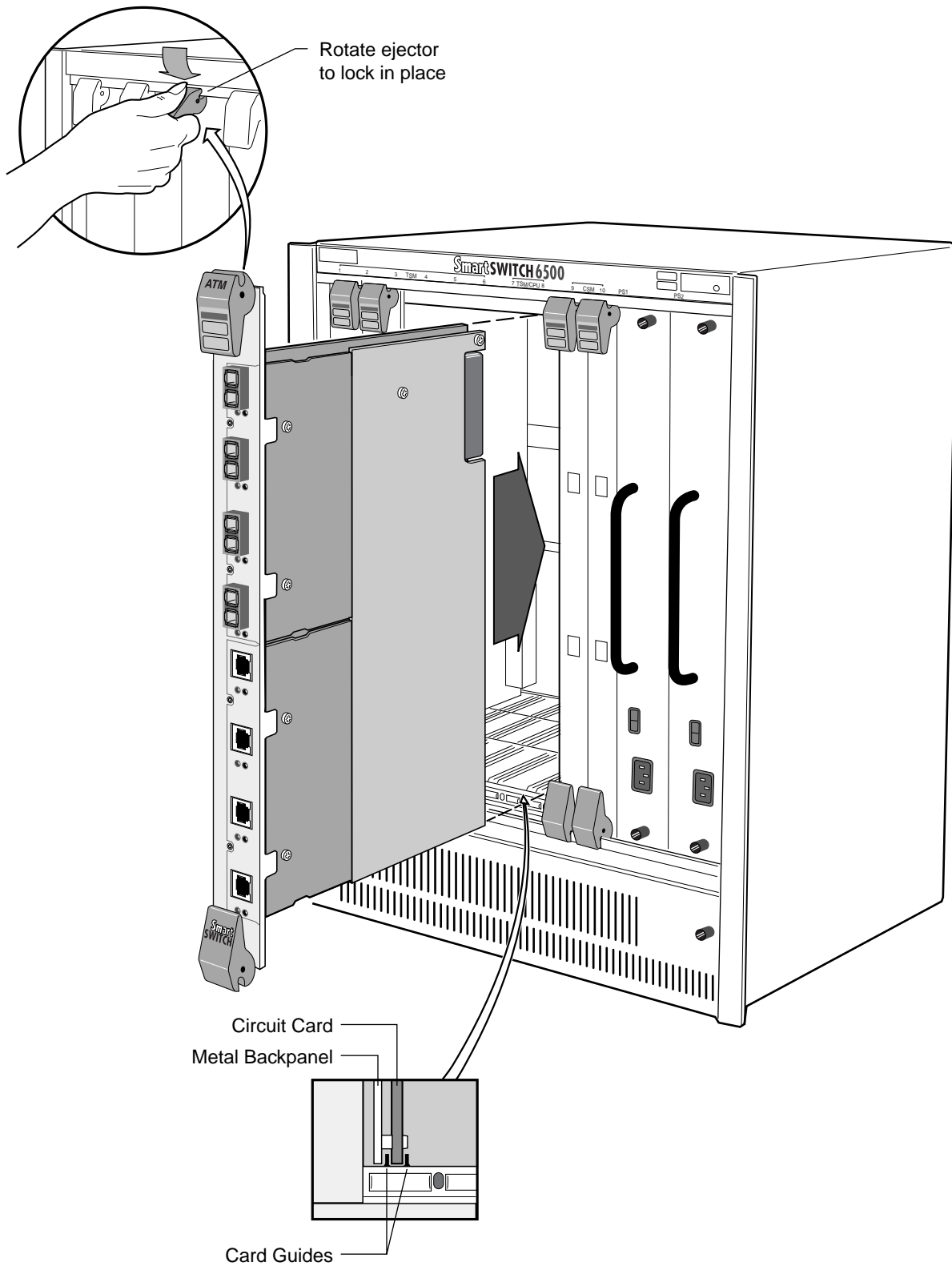


Figure 2-7 Installing a TSM/CPU module in slot 8

2.2.5 Installing Additional TSM Modules

TSM modules without CPU daughter boards can be installed in slots 1 through 6. See the legend on the top edge of the SmartSwitch 6500 chassis. Follow these instructions to install additional TSM modules.



Caution Do not attempt to insert a TSM module in either slot 9 or slot 10.

1. Remove the metal blank that covers one of the chassis' slots.
2. Open the ejectors at the top and bottom of the TSM module.
3. With the ejector labeled **6A-TSM512** at the top, align the top and bottom of the TSM module with the tracks in the slot.
4. Slide the TSM module into the chassis. The TSM module obscures the view of the tracks at the bottom of the chassis, so be sure to look at that area as you begin to slide the module into the chassis.
5. Close the ejectors. The installation is complete.

If you have additional TSM modules, repeat steps 1 through 5.

2.2.6 Installing Other Modules in the SmartSwitch 6500 Chassis

If all SmartSwitch 6500 chassis slots are not occupied by TSMs, other Cabletron SmartSwitch double-wide devices can reside within the chassis. For example, if slots are available, the chassis can also contain Ethernet switches, other ATM switches, and so on (see Figure 2-8 for an example).

Table 2-2 shows the maximum number of TSMs and Cabletron SmartSwitch double-wide modules that can be installed in the same SmartSwitch 6500 chassis.

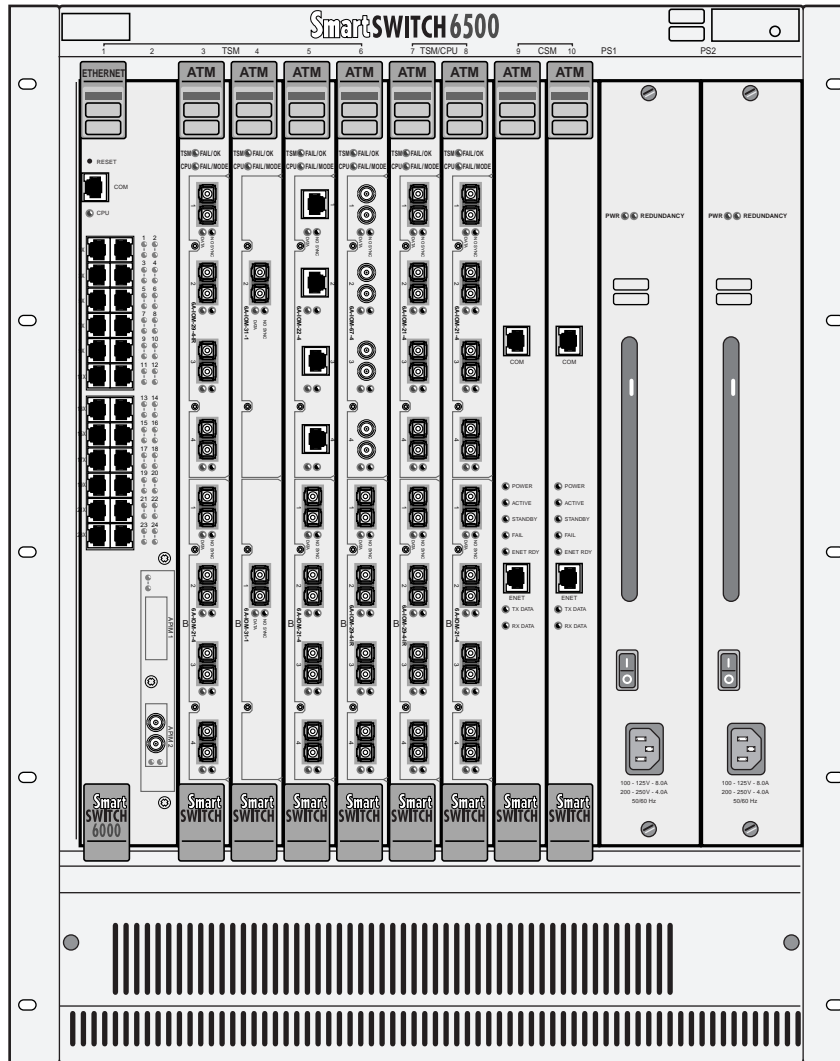


Figure 2-8 SmartSwitch 6500 chassis with Ethernet switch, TSMs, and CSMs

Table 2-2 Module combinations in 6500 chassis

Number of double-wide 6000 modules Installed	0	1	2	3
Number of TSM modules that can be installed	8	6	4	2

2.3 CONFIGURING THE SWITCH

This section describes the steps necessary to configure your SmartSwitch 6500 for operation. Configuration is divided into two operations: initial network configuration and backup/redundancy configuration. Initial network configuration makes the SmartSwitch 6500 accessible by the rest of your network. Backup/redundancy configuration allows you to save switch configurations and specify the files from which the slave TSM/CPU gets its configuration in the event the master TSM/CPU fails.

2.3.1 Initial Network Configuration

Initial network configuration of your SmartSwitch 6500 consists of making a terminal connection with the switch through the COM port to set the switch name, IP address, and subnet mask for the switch's Ethernet port. Once these tasks are complete, the switch can be reached over your Ethernet network for additional configuration and administration.

Perform the following steps to configure initial switch parameters.



Note If you have a redundant CSM, make the physical connections described below to the CSM in slot 9. By default, the CSM in slot 9 is the master CSM and is the only module with active **COM** and **ENET** ports.

1. Configure a dumb terminal or workstation running terminal emulation software with the following communication parameters:
 - Terminal emulation = VT100
 - Baud rate = 9600
 - Data bits = 8
 - Stop bits = 1
 - Flow control = none
2. Plug one end of the supplied RJ-45 UTP cable into the 9-pin RJ-45 adapter (see Figure 2-9).
3. Plug the other end of the UTP cable into the Master CSM's female RJ-45 jack labeled **COM** (see Figure 2-9).
4. Connect the master CSM module to your network by plugging a UTP cable into the CSM's female RJ-45 jack labeled **ENET** (see Figure 2-9).
5. Start the dumb terminal or workstation terminal emulation software.
6. As soon as power is applied to the SmartSwitch 6500, the module emits a series of diagnostic messages.
7. After the diagnostics are finished, the switch prompts for a password. Enter the default password, "admin."
8. Next, the switch prompts for the information necessary to make it accessible through your Ethernet network
 - Switch name
 - IP address
 - Subnet mask

- Default router — IP address of router (if any) that exists between the switch and its TFTP server.

The following is an example of the initial network configuration session.



Note For the sake of brevity, the start up messages have been abridged.

```
SmartSwitch 6500 Start-up Code
Cabletron Systems Inc.
```

```
Press any key to exit to Boot Load Prompt:
01
Bypassing POST
Verifying Checksum of Switch Software...
```

```
SmartSwitch Command Console
SmartSwitch Version 02.02.0 (c) Cabletron Systems Inc.
```

```
password:                : admin                < "admin" is the default password
The current user is      : Administrator
Could not find setup file
Running Setup Automatically
SwitchName(Smart6500)   : my_switch          < a switch name
IPAddress(10.0.0.1)     : 206.61.237.22       < an IP address
IPNetMask(255.255.255.0) : 255.255.255.0     < a subnet mask
Default Router()       : 206.61.237.5    < router through which the switch accesses its backup TFTP server
```

```
Confirm(y/n)?:y
Changing IP Address on System. Telnet session (if any) will be lost.
```

```
my_switch #
```



Note At this point, it's advisable to use the `passwd` command to change the default password.

9. Log off the local console connection. You can now perform additional configuration steps over your network using a telnet connection.



Note Only one console connection is allowed at any time. To reach the SmartSwitch 6500 through telnet, you must exit the local terminal connection by entering the `exit` command.

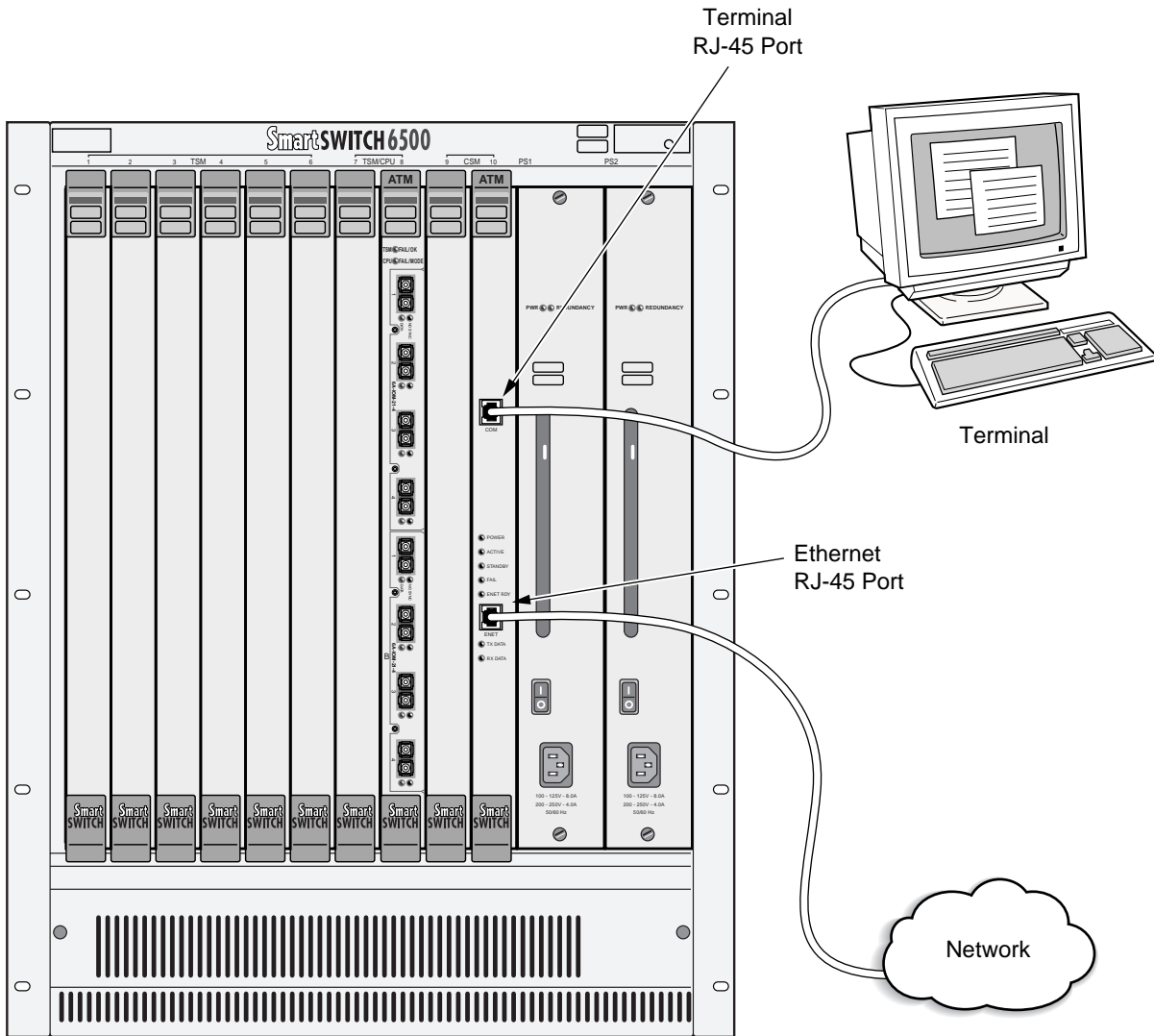


Figure 2-9 SmartSwitch 6500 connections for configuration

2.3.2 Backup/Redundancy Configuration

Backup/redundancy configuration consists of setting up the SmartSwitch 6500 to save configuration backup files used by the master TSM/CPU and slave TSM/CPU (if any). The backup configuration file contains all configuration changes made to the master TSM/CPU. For example, the backup file contains ELAN information, port configuration changes, PVCs, and so on.



Note The backup file does not contain an image of the switch operating firmware. For information on upgrading or replacing switch firmware, see Chapter 8, "Upgrades and Firmware."

Perform the following steps to configure backup capabilities.

1. On a workstation that can be reached by your SmartSwitch 6500 and is running TFTP server software, create a file under the /tftpboot directory. This file is used as the backup file by the master TSM/CPU and can initially be blank.
2. Make sure that the SmartSwitch 6500 has full read/write privileges to the file.
3. Enter the **backup switch** command on the SmartSwitch 6500. Specify the IP address of the TFTP server and the full path and file name to the backup file. For example:

```
Smart6500 # backup switch
ServerIP()                : 206.61.237.40           < IP address of the backup TFTP server
Path(public/Smart6500.ztr) : /tftpboot/backup.ztr    < full path and file name

Smart6500 #
```



Note Depending upon whether your TFTP server is running in secure or non-secure mode, you may not need to specify /tftpboot in the path to the backup file. If you experience *access violation* errors, try leaving off /tftpboot from the path.



Note It's a good idea to backup the SmartSwitch 6500 each time you make a permanent or significant change to the switch's configuration.

Once the SmartSwitch 6500 configuration is backed up, you can restore the master TSM/CPU configuration by entering the **restore switch** command. For example:

```
Smart6500 # restore switch
ServerIP(206.61.237.40)      : < Remembers last IP address entered
Path(tftpboot/backup/smart6500.ztr) : < Remembers last path and file name entered
```

Backup file is valid.

Restoring a backup file will completely replace any data stored in the flash, and requires a switch reboot

```
Are you sure this is what you want to do?
Confirm(y/n)?y                < Yes, restore the configuration
```

```
Restoration complete.
Rebooting is required to ensure correct operation,
Do you want to reboot now?
Confirm(y/n)?y                < Yes, reboot the switch
```

Redundancy Configuration for the Slave TSM/CPU

In the event the master TSM/CPU fails, the slave TSM/CPU module assumes the role of master. To do this, the slave TSM/CPU must know the location of a configuration file from which to obtain switch configuration information. When rebooted, the new master TSM/CPU automatically configures itself using the information contained within the configuration file. Use the **set redundancyinfo** command to tell the slave TSM/CPU the location and name of its configuration file.

The following example tells the slave TSM/CPU to use the master TSM/CPU's backup file as its configuration file. The master TSM/CPU's backup file is `backup.ztr`, and it's located in the `/tftpboot` directory:

```
Smart6500 # set redundancyinfo
HostIP()                : 206.61.237.40      < IP address of the TFTP server
PathFileName()          : /tftpboot/backup.ztr < full path and file name of master's backup file
Updating Slave redundancy config. Please wait...
```

```
Smart6500 #
```

Using the master TSM/CPU's backup file as the slave's configuration file assures that if the slave assumes the role of master, it will be configured identical to the previous master (ELANs, PVCs, PVPs, port settings, and so on). You can, however, instruct the slave TSM/CPU to use a file other than the master's backup file as its configuration file.



Note Remember that the slave TSM/CPU's configuration file must already exist and reside within the `/tftpboot` directory of the TFTP server.

Keep in mind that the `backup switch` command updates only the master's backup file. If the slave TSM/CPU is set to use a configuration file other than the master TSM/CPU's backup file, the `Backup Switch` command does not update the slave's configuration file with the master's current configuration.

If the slave's configuration file is not the master's backup file, use the `execute redundancyconfigbackup` command to sync the slave's configuration file with the master's current configuration. For example:

```
luxor2 # execute redundancyconfigbackup
Backup successful
```

```
luxor2 #
```

The slave TSM/CPU's configuration file now contains the current configuration of the master TSM/CPU.

Redundancy Configuration for CSMs

The SmartSwitch 6500 can use two CSM modules: one active (master), the other in standby (slave). By default, the CSM in slot 9 is recognized as the active (master) CSM by the active TSM/CPU module. To set the slave CSM as the master CSM perform the following steps:

1. Access the bootline prompt by rebooting the SmartSwitch 6500, then pressing a key during the start up countdown.
2. At the bootline prompt, enter the `sacsm` command. Mastership is transferred to the redundant CSM. Notice that the console becomes inactive.
3. Transfer both the COM port and Ethernet port cables to the new master CSM module, then press the space-bar to regain control of the console.
4. At the bootline prompt, enter the `go` command to allow the SmartSwitch 6500 to proceed with start up.



Note If the master CSM fails, move the COM port and Ethernet port cables to the slave CSM. Remove the failed CSM from the chassis and press the reset button. At start up, the master TSM/CPU will automatically discover the slave CSM and use it as the new master CSM.

2.4 LED DESCRIPTIONS

Both the CSM and TSM modules display several LED indicator lights. Table 2-3 and Table 2-4 explain the color, state, and meaning of the CSM and TSM indicator lights. Also, see Figure 2-10.

Table 2-3 CSM LEDs

LED	Green	Amber	Red	Unlit
POWER	Power on			No power
ACTIVE	CSM is active			CSM not active*
STANDBY	CSM is in standby mode			CSM is not in standby mode
FAIL			CSM is in fail	Normally off
ENET RDY	Ethernet interface is up and active			Ethernet interface not active*
TX DATA	Normally flashing, transmitting data on Ethernet port			
RX DATA	Normally flashing, receiving data on Ethernet port			

* Slave CSM

Table 2-4 TSM LEDs

LED	Green	Amber	Red	Unlit
TSM FAIL/OK	TSM is initialized			TSM not initialized
CPU FAIL/OK	CPU in active mode	CPU in standby mode*	CPU in fail	No CPU on TSM
DATA	Normally flashing when connected, data is passing through the port			No data is passing through port.
NO SYNC		Framer is not receiving sync		Normally off when connected, Framer is receiving sync

* Slave TSM/CPU

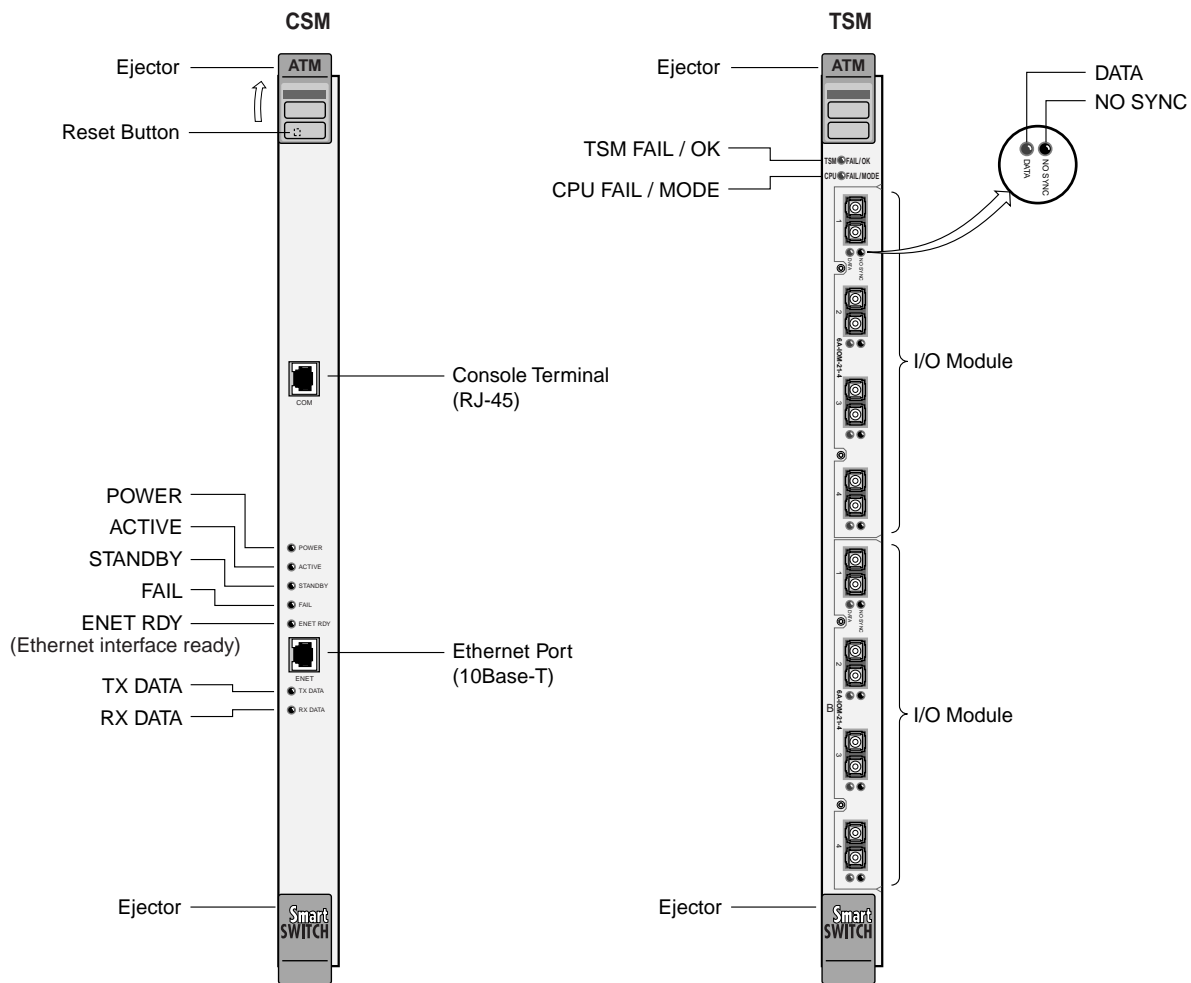


Figure 2-10 CSM and TSM LEDs

2.5 USING THE CONSOLE

Use the SmartSwitch 6500 console interface to configure and manage your switch. The following is a description of the console interface and its operation.

2.5.1 Port Numbering

The following convention is used for numbering physical ports on the SmartSwitch 6500:

slot number I/O module letter port number

For example, port 3 of I/O module A on the TSM in slot 5 is represented by: **5A3**

Virtual ports are designated by a period (.), and the virtual port number is appended to the physical port number. For example, virtual port 2 on physical port **7B1** is represented as: **7B1.2**

2.5.2 Console Commands



Note For detailed descriptions of all console commands, see the SmartSwitch 6500 Reference Manual.

All console commands use the syntax:

```
operator switch-attribute [<parameter 1> <parameter 2>... <parameter n>]
```

Where the **operator** is one of the following:

activate: Make a connection active.

add (create): Add a new instance of a switch-attribute.

backup: Backup the active TSM/CPU configuration.

clear: Clear a table, list, or configuration.

deactivate: Make a connection inactive.

delete (remove): Delete an instance of a switch-attribute.

execute: Perform the following action.

exit: Exit the switch console.

flush: Remove assigned values; for example, flush a route table.

modify (set): Change the values that currently define a switch-attribute.

show (display): Show the current values used by a switch-attribute.

start: Start a process on the switch; for example, start the LAN Emulation Configuration Server.

restart: Restart a process on the switch; for example, `restart client`.

restore: Restore the TSM/CPU configuration from its backup file.

If a command requires parameter values, it prompts you for them. For instance, in the example below, **show** is the operator, **portconfig** is the switch-attribute, and **7a1** is the parameter indicating that you want to show configuration information about port **7A1**.

```
Smart6500 # show portconfig 7a1
=====
Port: 7A1
-----
Parameter                Configured      Current
-----
Sig Type                  autoConfig     pnni10
Sig Role                  other          symmetric
Interface Type           private        private
Max vpi bits              0              0
Max vci bits              12             12
Max SVC vpci              0              0
Min SVC vci               32             32
Max Vccs                  4096           4096
-----
Other parameters
-----
Port Admin Status        UP
Ilmi Admin Status        Enabled AddressRegistration Connectivity
Oper State                UP
Trans Type                STS-3c
Media Type                MMF (S)
Bandwidth                 155 MB
Smart6500 #
```

If you don't specify parameters with the command, the console prompts you for an input value and provides a default value displayed in parenthesis. For example, if you enter **show portconfig** without specifying a port (as a parameter), the following appears.

```
Smart6500 # show portconfig
PortNumber(ALL)          :

Port   Intf   Sig   ILMI  Trans  Media  Max   Used  Oper
Name   Type   Type  State Type  Type   Bw(MBS) Bw(MBS) State
-----
CPU    private uni40  down  STS-3c MMF (S) 155.0 13.87 up
CPU.1  private pnni10 down  STS-3c MMF (S) 10.50 0.0  up
7A1    private autoConfig down  STS-3c MMF (S) 155.0 0.0  down
7A2    private pnni10 up    STS-3c MMF (S) 155.0 1.12 up
7A3    private autoConfig down  STS-3c MMF (S) 155.0 0.0  down
7A4    private autoConfig down  STS-3c MMF (S) 155.0 0.0  down
7B1    private uni30  up    STS-3c MMF (S) 155.0 0.75 up
7B2    private pnni10 up    STS-3c MMF (S) 155.0 0.75 up
7B3    private autoConfig down  STS-3c MMF (S) 155.0 0.0  down
Smart6500 #
```

In the example above, the default of “a11” ports is presented. You can either accept the default by pressing **Enter**, or you can enter a specific port number.



Note When you accept the (a11) default for **show**, the information displayed is often abridged.

2.5.3 Console Time-out

The console can be configured to exit if it does not sense a key stroke within a defined length of time. By default, the SmartSwitch 6500 is set to never time out (value = 0). To activate the time-out feature, use the `set consoleTimeout` command to adjust the time-out period:

```
Smart6500 # set consoletimeout
Timeout(0) : 30 <Will time-out in 30 minutes without input
Confirm (y/N)? : y
Smart6500 #
```

2.5.4 Creating an Alias

Use the `add alias` command to create shorter or easier-to-remember names for command lines. For example:

```
Smart6500 # add alias
AliasName() : traffic
AliasedString() : set switchtrafficcongestion
Smart6500 #
```

The above example creates an alias (`traffic`) that can be entered in place of the command `set switchTrafficCongestion`. For example:

```
Smart6500 # traffic
LowEPDWatermark(4096) :
HighEPDWatermark(4096) :
CLP1_DiscardWatermark(4096) :
RMCellMarkingEnable(enable) :
ExplicitRateMarkingEnable(enable) :
EFCIMarkingEnable(enable) :
```

```
Smart6500 #
```

Enter the `show alias` command to display a list of all defined aliases and the command lines to which they correspond.

```
:Smart6500 # show alias
AliasName(ALL) :
Alias List
=====
Index Alias Name : Aliased Command
1 PING : Start ping
2 port : show portconfig
3 traffic : set switchtrafficcongestion
Smart6500 #
```

2.5.5 Ambiguous Commands

If you enter part of a command, and that part is not unique, the console displays a numbered list of possible matching commands. For example, entering `show pnnin` is ambiguous because there are several commands that start with “pnnin.” In response, the SmartSwitch 6500 displays a list of the possible commands:

```
Smart6500 # show pnnin <“pnnin” is ambiguous
Objects beginning with pnnin for action show
0 : PnniNeighbor
1 : PnniNetworkLink
2 : PnniNetworkNode
3 : PnniNode
4 : PnniNodeTimer
(#)Command (Q)uit? : 3 <I meant PnniNode, so I enter number three (3) from the list
Smart6500 # show PnniNode
```

Selecting number three from the list automatically enters the corresponding command; pressing enter executes the command:

```
PNNI Node Information
=====
Level          : 80
Node Id        : 50:a0:39:00:00:00:00:00:00:00:28:c1:80:00:20:d4:28:c1:80:00
Lowest         : TRUE
Admin Status   : UP
Oper Status    : UP
Atm Address    : 39:00:00:00:00:00:00:00:28:c1:80:00:20:d4:28:c1:80:00
Peer Group Id  : 50:39:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Rst Transit    : FALSE
Rst Branching  : FALSE
DB Overload    : FALSE
Ptse           : 2
Smart6500 #
```

2.5.6 Console Help

The console provides several levels of help for console commands. For example, to list the switch attributes that can be used with a particular operator, enter the word **help** (or **?**) followed by the operator.

```
Smart6500 # help add
HELP ---- add
=====
add          [ AlarmConfig | Alias | ATMRoute | BUSELAN | Community | ELAN |
              Interface | IPATMClient | IPATMPVC | LANEClient | LECSELAN |
              LECSELANLEC | LECSTLVSET | LESELAN | NetPrefix | PnniMetrics |
              PnniSummaryAddress | PVC | Route | ServiceRegistry |
              TrafficDescriptor | TrapCommunity ]
Smart6500 #
```

To obtain an explanation of a command and its parameters, enter the word **help** (or **?**) before the command.

```
Smart6500 # ? add laneclient
Create LANE Client
=====
ClientNumber      Local Client Number (0-127)
LanName           Name of the ELAN to join
ServerType        Type of LANE Server [LECS, LES]
ServerAddress     ATM Address of the LANE Server
IPAddress         IP Address of the Client
NetMask           IP Netmask of the Client
MTU               MTU for the Client [1516, 9234, NONE]
Smart6500 #
```

While entering a command, you can obtain help about the current parameter by entering a question mark (?) at the prompt. For example:

```
Smart6500 # add atmroute
PortNumber(A1)      : a3
AtmAddress()        : 39:00:00:00:00:00:00:00:14:72:80
PrefixLength(104)  :
Index(0)            :
Type(Internal)      : ? < What does type mean?
The type of reachability. Use Internal, Exterior, or Reject.
Type(Internal)      : exterior
Scope(0)            :
MetricsTag(0)       :
Smart6500 #
```



Note Press the Esc key to back out of any command before you enter the last value.

2.6 SMARTSWITCH ATM ADMINISTRATOR

SmartSwitch ATM Administrator is a graphical user interface application that manages SmartSwitch ATM switches. It supports the following operations:

- Switch management
- Emulated Local Area Network (ELAN) management
- Connection management
- Alarm management
- Switch discovery
- Topology and chassis views
- PNNI group views

Additionally, the SmartSwitch ATM Administrator provides the following capabilities that are not available from the console interface:

- Use a graphical user interface
- Perform drag and drop operations
- Manage all switches from one console
- Perform transactions across multiple switches (for example, create an ELAN when the servers are not co-located)

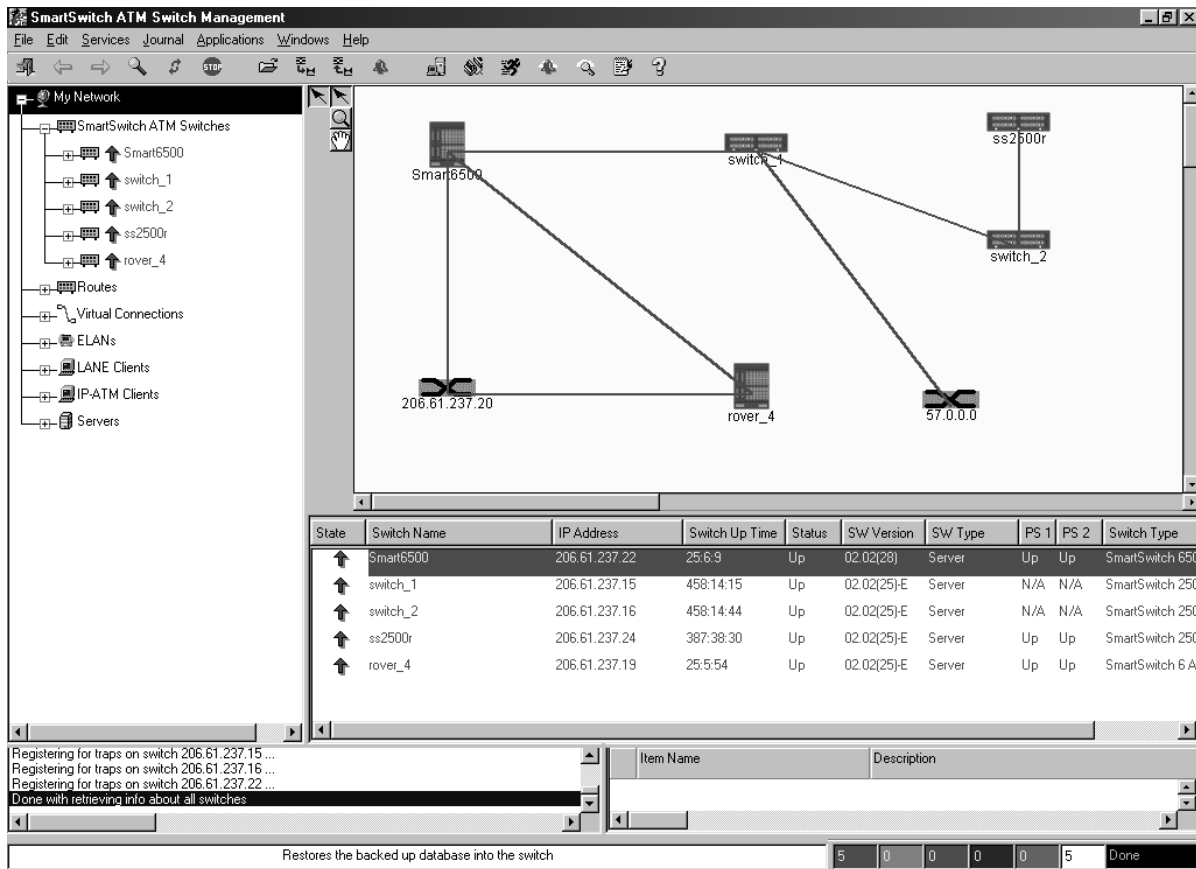


Figure 2-11 SmartSwitch ATM Administrator

SmartSwitch ATM Administrator can be installed on a workstation running Windows 95/98, Windows NT, or Solaris 2.4/2.5.

For Windows 95/98 or Windows NT, the following minimum hardware configuration is required:

- Pentium 133 Mhz or faster processor
- CD-ROM drive
- 20 MB free disk space
- 64 MB RAM
- Monitor with resolution of at least 800 x 600 pixels
- Ethernet or ATM network interface card

For Solaris 2.4/2.5, the following hardware configuration is required:

- Ultra-1 Sparc workstation or equivalent
- CD-ROM drive
- 100 MB free disk space
- 64 MB RAM
- 200 MB virtual memory (swap space)

- Color monitor
- Ethernet or ATM network interface card

2.6.1 PC Installation

The installation process for SmartSwitch ATM Administrator is essentially the same for all the supported operating systems. Follow these instructions for installation on Windows NT or Windows 95.

1. Insert the SmartSwitch ATM Administrator CD into your system's CD-ROM drive.
2. From the File Manager, double click on `setup.exe`.
3. Follow the instructions that appear on the screen.

2.6.2 Solaris Workstation Installation

1. Insert the SmartSwitch ATM Administrator CD into your system's CD-ROM drive. Typically, the CD-ROM drive is `cdrom0`.
2. With root privileges, type from the shell: `pkgadd -d /cdrom/<cd drive>`
3. Follow the instructions that appear on the screen.

2.6.3 Starting SmartSwitch ATM Administrator

Perform the following instructions to launch the SmartSwitch ATM Administrator.

- For the Windows version:
In the SmartSwitch ATM Network Management Tools (Common) program group, double click on the icon labeled SmartSwitch ATM Administrator. The SmartSwitch ATM Administrator Login dialog box appears.
- For the Solaris 2.4/2.5 version:
From a shell (using root privileges), type: `ssadmin`. The SmartSwitch ATM Administrator Login dialog box appears.

2.6.4 Initial SmartSwitch ATM Administrator Set Up

When you use SmartSwitch ATM Administrator for the first time, you should change the default passwords to prevent unauthorized access to the application. The application arrives with two user accounts set up as described in Table 2-5.

Table 2-5 Default accounts and passwords

User Name	Access Level	Default Password
admin	read/write	admin
guest	read only	guest

Perform the following steps to change the password.

1. Enter the default user name, **admin**. The user name is case sensitive.
2. Enter the default password, **admin**, and click the OK button or press Enter. The password is case sensitive.
3. The SmartSwitch ATM Administrator window appears. On the Applications menu, select User Management.

2.6.5 Default Community Strings

The following is a list of the default community strings used by the SmartSwitch 6500:

- **public** — Used for all standard SNMP communication
- **ILMI** — Used by ILMI channels between switches
- **zeitnet** — Used by the SmartSwitch ATM Administrator program



Caution If the community string *zeitnet* is changed on the SmartSwitch 6500 it must also be changed at the SmartSwitch ATM Administrator. Failure to do so, makes the SmartSwitch 6500 unreachable by the SmartSwitch ATM Administrator program.

2.6.6 Accessing Online Help

All SmartSwitch ATM Administrator operations (including changing passwords and adding users) are documented within the application's online help. Follow these instructions to access the online help facility.

1. From the Help menu, select SmartSwitch ATM Administrator Help Topics.
2. The Help Topics dialog box appears. You have three options for viewing online help:
 - Click the Contents tab to show the Table of Contents of the online help. Click on the topic you wish to read about.
 - Click the Index tab to select from an alphabetical list of help topics.
 - Click the Find tab to search for a particular topic.

3 IP OVER ATM AND LANE

This chapter describes working with the SmartSwitch 6500 IP over ATM VLAN and emulated LAN capabilities. At the end of this chapter you will be able to use your SmartSwitch 6500 switch to

- Create an IP over ATM VLAN
- Create an emulated Ethernet LAN (LANE)

3.1 CREATING AN IP OVER ATM VLAN

This section describes implementing IP over ATM on your SmartSwitch 6500 switch. The following assumptions are made:

- The SmartSwitch 6500 will have a client on the IP over ATM VLAN
- The ARP server will reside on the switch and correspond to the address of the switch client
- All end nodes (computers, edge devices, and so on) support Switched Virtual Circuits (SVCs)

1. Log into the switch, either through the terminal port or through the Ethernet interface by telnet.
2. Create a client on the switch and assign it as the ARP server for the VLAN.

```
SmartCell ZX # add ipatmclient
ClientNumber(0) : 1
ServerType(NONE) : local          < the ARP server is assigned to the switch client
ServerAddress()  :
IPAddress()      : 90.1.1.1       < IP address is for example only
NetMask(255.0.0.0) : 255.255.255.0 < subnet mask is for example only
MTU(9180)       :
SmartCell ZX #
```

The example above creates a client on the switch, designates the client as the ARP server for the VLAN (**serverType = local**), and assigns the client an IP address and subnet mask.



Note The command `add ipatmclient` always prompts you with a subnet mask that is appropriate for the IP address. However, if necessary, you can change the subnet mask to correspond to the strategy employed within your networks.



Caution Never create an IP over ATM VLAN (or an IP over ATM client) with the same subnet as the SmartSwitch 6500 Ethernet port.

- Enter the `show client` command to make sure the client is operational and to obtain the 20-byte ATM address of the ARP server. For instance, if you used the client number (client 1) from the example in step 2, enter the following command:

```
SmartCell ZX # show client 1
IP/ATM Client 1
=====
Client State      : Operational
Client Address    : 39:00:00:00:00:00:00:00:00:00:14:41:80:00:00:5A:01:01:01:00
Server            : is local
Server Connection : Established
MTU               : 9180
IP Address        : 90.1.1.1
IP NetMask        : 255.255.255.0
SmartCell ZX #
```

- Physically connect your end nodes and edge devices to the SmartSwitch 6500 ports.



Note Your end nodes do not need to be physically attached to the switch that contains the ARP server. For example, an end station is connected to a SmartSwitch 6500 that is connected through a route to the switch containing the ARP server. No special configuration is needed for this end station to participate in the VLAN because the end station automatically finds its path across the route to the ARP server and the other VLAN members.

- Configure the ATM interface or adapter for end nodes and edge devices. Typically, configuration consists of designating IP over ATM as the connection type, assigning the device an IP address, and specifying the 20-byte ATM address of the ARP server (the switch’s client address). For details on the SmartSwitch 6500 automatic addressing scheme for IP over ATM, see Section 3.1.1.
- As your end devices are configured and started, they register with the ARP server. You can test whether your IP over ATM VLAN is functional by pinging from one end device to another.

To make certain that all end devices are registered with the ARP server, you can inspect the switch’s ARP table using the `show ipatmarp` command. For example, if three end devices with IP addresses 90.1.1.2, 90.1.1.3, and 90.1.1.4 are added to the VLAN, the following ARP table entries should exist:

```
SmartCell ZX # show ipatmarp
ClientNumber(ALL) :
IP/ATM Server 2 ARP Table
IP Address          ATM Address
=====
90.1.1.2 39:00:00:00:00:00:00:00:00:00:14:41:80:00:00:5A:01:01:02:00
IP/ATM Server 3 ARP Table
IP Address          ATM Address
=====
90.1.1.3 39:00:00:00:00:00:00:00:00:00:14:41:80:00:00:5A:01:01:03:00
IP/ATM Server 4 ARP Table
IP Address          ATM Address
=====
90.1.1.4 39:00:00:00:00:00:00:00:00:00:14:41:80:00:00:5A:01:01:04:00
SmartCell ZX #
```



Note If configured devices fail to join the VLAN, see Chapter 5, "Routing." Section 5.3. Also, see Chapter 9, "Troubleshooting."

3.1.1 Default ATM Addressing for IP over ATM

The SmartSwitch 6500 provides a default format for ATM addresses used by IP over ATM.

Default Netprefix

The default netprefix is constructed from

39 + nine zero bytes + last three bytes of chassis MAC address

For example, if the chassis MAC address = 00:00:1D:A3:87:0B, then

Default netprefix = 39:00:00:00:00:00:00:00:00:00:A3:87:0B

Default IP Over ATM Client Address

The default client address is constructed from

netprefix + two zero bytes + client IP address (in hexadecimal) + trailing zero byte

For example

- netprefix = 39:00:00:00:00:00:00:00:00:00:A3:87:0B
- chassis MAC address = 00:00:1D:A3:87:0B
- client IP address = 90.1.1.1 (5A.01.01.01 in hexadecimal)

then,

IP over ATM client address = 39:00:00:00:00:00:00:00:00:00:A3:87:0B:00:00:5A:01:01:01:00

3.2 CREATING AN EMULATED LAN

This section describes the steps for implementing an Ethernet Emulated LAN (ELAN) on your SmartSwitch 6500. The following assumptions are made:

- The SmartSwitch 6500 switch will contain a client on the ELAN
- All end nodes (computers, edge devices, other switches, and so on) support the Well Known LECS Address or can obtain the address of the LECS using ILMI
- All end nodes support Switched Virtual Circuits (SVCs)



Note An ELAN comes pre-configured on SmartSwitch 6500 switches. The ELAN name is “ELAN000.” To use this ELAN, start the LECS, configure your end nodes and edge devices to use ELAN name ELAN000, and then plug them into the SmartSwitch 6500.

1. Enter the **start lecs** command to activate LANE server services on this SmartSwitch 6500.

```
SmartCell ZX # start lecs
NOTICE - 'LECS' ***** LECS started *****
SmartCell ZX #
```

2. Create an ELAN on your SmartSwitch 6500 switch by executing the **add elan** command. The following is an example.

```
SmartCell ZX # add elan
ELANNumber(0) : 1                < 1 is used instead of the default, (0)
ELANName(ELAN001) : Marketing    < ELAN is named Marketing instead of the default, (ELAN001)
ConnectMethod(SVC) :
ELANType(802.3) :                 <The default (Ethernet) is used
Multipoint(YES) :
MTU(1516) :
ErrorLogEnable(NO) :             < Take the default
MinimumTDEnable(NO) :           < Take the default
Distribute(PROXY) :
SmartCell ZX #
```

3. Use the **add laneclient** command to create a client for the switch on the ELAN:

```
SmartCell ZX # add laneclient
ClientNumber(0) : 1              < One is used instead of the default, (0)
LanName(ELAN001) : Marketing     < ELAN name is Marketing, not the default, (ELAN001)
ServerType(LECS) :
ServerAddress() :                < No LANE server address is specified; see note below
IPAddress() : 90.1.1.1           < IP address and subnet mask are specified only as examples
NetMask(255.0.0.0) : 255.255.255.0
MTU(1516) :
SmartCell ZX #
```



Note When you create a client, it automatically finds the LECS address using ILMI.



Note The command **add laneclient** always prompts you with a subnet mask that is appropriate for the IP address. However, if necessary, you can change the subnet mask to correspond to the strategy employed within your networks.

As the local client joins the ELAN, the following messages are sent to the Event Log (see Chapter 9, "Troubleshooting," Section 9.5):

```
NOTICE - 'ZLESSRV' LES Join 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:D4:
14:41:82:00
NOTICE - 'ZLESSRV' BUS Connect 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:D4:
14:41:82:00
```



Caution Never create an ELAN (or ELAN client) with the same subnet as the SmartSwitch 6500 Ethernet port.

4. Enter the `show client` command verify that the client is operational.

```
SmartCell ZX # show client 1
LANE Client 1
=====
Client State      : Operational
Client Address    : 39:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:81:00
LAN Name          : Marketing
LECS Addr Source  : ILMI
LECS Address      : 39:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:80:01
LES Address       : 39:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:82:02
LAN Type          : 802.3
MTU               : 1516
IP Address        : 90.1.1.1
IP NetMask        : 255.255.255.0
SmartCell ZX #
```



Note While creating an ELAN client for the switch is not absolutely necessary, it does provide management connectivity with the switch over its ATM ports (instead of the Ethernet port). See Chapter 5, "Routing." Section 5.5 for information about how to reach switches not directly connected to the Ethernet network.

5. Physically connect your end nodes and edge devices to the SmartSwitch 6500 ports.
6. Configure the ATM interface or adapter for all end nodes and edge devices. Typically, configuration consists of specifying LAN Emulation as the connection type, assigning the device an IP address that corresponds to the subnet of the switch's client, and indicating that you want the device to either acquire the LECS address through ILMI or use the Well Known Address as the address for the LECS. For details on the SmartSwitch 6500 automatic addressing scheme for LANE, see Section 3.2.1.
7. As each end device registers with the LES and BUS, messages are sent to the event log of the SmartSwitch 6500 containing the LECS. You can check connectivity by pinging between end nodes.



Note If configured devices fail to join the ELAN, see Chapter 5, "Routing." Section 5.3. Also, see Chapter 9, "Troubleshooting."

Your ELAN is now operational. Additional ELANs can be created in the same way.



Note While it is possible for a single ELAN on the SmartSwitch 6500 switch to support multiple subnets, in general, switch performance is best (and management easiest) when the "One-subnet-per-ELAN" rule is observed.

3.2.1 ATM Addressing for LAN Emulation

The SmartSwitch 6500 provides default formats for ATM addresses used by LAN emulation entities (local client, LECS, LES, and BUS). The default formats are constructed as follows.

Default Netprefix

The default netprefix is constructed from

39 + nine zero bytes + last three bytes of chassis MAC address

For example, the chassis MAC address = 00:00:1D:A3:87:0B,

then

default netprefix = 39:00:00:00:00:00:00:00:00:00:A3:87:0B

Default Client ATM Address

The default address for local clients is constructed from

netprefix + CPU MAC address with last byte summed with the client number + zero selector byte

For example

- netprefix = 39:00:00:00:00:00:00:00:00:00:A3:87:0B
- chassis MAC address = 00:00:1D:A3:87:0B,
- CPU MAC address = 00:20:D4:14:41:80,
- client number = 5

then,

client five's default ATM address = 39:00:00:00:00:00:00:00:00:00:A3:87:0B:00:20:D4:14:41:85:00

Default LECS ATM Address

The default LECS address is constructed from

netprefix + chassis MAC address + selector byte of 01

For example

- netprefix = 39:00:00:00:00:00:00:00:00:00:A3:87:0B
- chassis MAC address = 00:00:1D:A3:87:0B

then,

default LECS address = 39:00:00:00:00:00:00:00:00:00:A3:87:0B:00:00:1D:A3:87:0B:01

Default LES and BUS ATM Addresses

By default, the LES and BUS have the same ATM address. The default LES and BUS addresses are constructed from

netprefix + chassis MAC address + ELAN number summed with the numerical value two (2)

For example

- netprefix = 39:00:00:00:00:00:00:00:00:A3:87:0B
- chassis MAC address = 00:00:1D:A3:87:0B
- ELAN number = 3

then,

default LES and BUS addresses = 39:00:00:00:00:00:00:00:00:00:1D:A3:87:0B:05

3.2.2 ELANs Across Multiple Switches

ELANs can exist within a single switch, or they can span multiple switches. When an ELAN spans multiple switches, it's important that all switches within the group use the same LECS. The general rule is: "Within an administrative domain (a group of switches with related ELANs), there should be one and only one LECS." For this reason, never start the LECS on more than one switch within the administrative domain.



Note If an uplink, end node, or other ATM switch does not support PNNI, or if its version of ILMI is incompatible, it may be necessary to set up a static route between the device and the rest of the ELAN. See Chapter 5, "Routing."

3.2.3 Switch Clients

It is important to understand the concept of SmartSwitch 6500 client connections. A client connection is actually a connection between the VLAN and the SmartSwitch 6500 CPU; this CPU connection appears as if the switch is an end station on the VLAN. The SmartSwitch 6500 uses local clients to connect itself to the VLANs that it supports.

This is analogous to a phone company that supports a communication system. Even though the phone company maintains the circuits, a call to the phone company itself cannot be made unless the phone company has its own number and connection on its own phone system. Similarly, VLAN membership (and the reachability) of a SmartSwitch 6500 on any particular VLAN depends upon whether the SmartSwitch 6500 has a local client connection for that VLAN.

Clients are created using the command `add laneclient` for LAN emulation, and `add ipatmclient` for IP over ATM.

For example, the following command adds a switch client to the ELAN `elan1`:

```
SmartCell ZX# add laneclient
ClientNumber(0)           : 1
LanName(ELAN001)          : elan1
ServerType(LECS)          :
ServerAddress()           :
IPAddress()                : 128.213.77.95
NetMask(255.255.0.0)      :
MTU(1516)                 :
SmartCell ZX#
```

Prior to creating this local client connection, end devices could communicate with each other through `elan1`, but they could not communicate with the SmartSwitch 6500.

3.2.4 Distributed LANE Services

LANE services (LECS, LES, and BUS) can reside on different SmartSwitch 6500s. For example, the LECS can reside on one SmartSwitch 6500, while the LES and BUS reside on another. Use the `add lecselan`, `add leselan`, and `add buselan` to distribute LANE services among SmartSwitch 6500s.

The following steps create an ELAN with the LECS on switch SW1 and the LES and BUS on switch SW2.

1. Use the `add buselan` command to create the BUS on switch SW2:

```
SW2 # add buselan
ELANNumber(0)           : 1           < We'll use ELAN number = 1 throughout the example
ELANName(ELAN001)      : mis1        < We'll call the ELAN "mis1" throughout the example
ConnectMethod(SVC)     :
ELANType(802.3)        :
Multipoint(YES)        :
MTU(1516)              :
ErrorLogEnable(NO)     :
MinimumTDEnable(NO)   :
```

SW2 #

2. Use the `add leselan` command to create an LES on switch SW2:

```
SW2 # add leselan
ELANNumber(0)           : 1
ELANName(ELAN001)      : mis1
ConnectMethod(SVC)     :
ELANType(802.3)        :
Multipoint(YES)        :
MTU(1516)              :
ErrorLogEnable(NO)     :
MinimumTDEnable(NO)   :
ForwardPeakCellRate(0) :
BackwardPeakCellRate(0) :
Distribute(PROXY)      :
BUSATMAddress(39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:81:02) : < Created by add buselan
```

SW2 #

3. Use the `show leselan` command on SW2 to obtain the ATM address of the LES:

```
SW2 # show leselan 1

ELAN : mis1

ELAN Number       : 1
ELAN Name         : mis1
ATM Address       : 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:81 < ATM address of LES
:02
Max Frame Size    : 1516
Connection Method : SVC
Distribute VPI/VCI : 0/0
Distribute Method : PROXY
ELAN Type         : 802.3
Multipoint        : YES
Error Logging     : NO
Min TD Negotiation : NO
BUS Address       : 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:D4:14:41:81
:02
```

SW2 #

4. On switch SW1, use the command `add lecselan` to create the LECS:

```
SW1 # add lecselan
ELANNumber(0)                : 1
ELANName(ELAN001)           : mis1
LESAddress(39:00:00:00:00:00:00:00:A3:87:0B:00:00:1D:A3:87:0B:03): 39:00:00:00:00:00:00:00:00:14:41:80:00:20:d4:14:41:81:02 < Specify the LES address on SW2
ELANType(802.3)              :
MTU(1516)                    :
TLVSet()                      :
```

SW1 #

5. Use the `add laneclient` command on SW1 to add a client to the ELAN:

```
SW1 # add laneclient
ClientNumber(0)              : 1
LanName(ELAN001)            : mis1
ServerType(LECS)             :
ServerAddress()              :
IPAddress()                   : 90.1.1.22 < This IP address is for example only
NetMask(255.0.0.0)           : 255.255.255.0 < This subnet mask is for example only
MTU(1516)                    :
```

SW1 #

6. Use the `show client` command on SW1 to see that the client has reached all the distributed LANE services and has successfully joined ELAN `mis1`.

```
SW1 # show client
ClientNumber(ALL)            :
```

Client	Type	IP Address	Server Type	Server Conn	Status
1	LANE	90.1.1.22	LECS	Established	Operational

SW1 #

Notice in the example above that creating an ELAN with distributed services is a process of building from the bottom up: First, the BUS is created so that its address can be specified to the LES. Next, the LES is created so that its address can be specified to the LECS. Finally, the LECS is created.

If needed, all three ELAN services can exist on separate switches. For example, the BUS can exist on one switch (use the `add buselan` command), the LES can exist on another switch (use the `add leseelan` command), and the LECS can exist on another switch (use the `add lecselan` command).

3.2.5 ELAN Join Policies

The SmartSwitch 6500 provides control over the assigning of clients to ELANs. Control is accomplished by ELAN join policies. By default, the SmartSwitch 6500 has a single ELAN join policy defined — *Best Effort*. When a client attempts to join LANE services, the SmartSwitch 6500 uses information provided by the client to perform the *Best Effort* ELAN join test.

Best Effort Elan Join Test

The following describe the *Best Effort* test.

1. Does the client specify the name of the ELAN it wants to join?
 - If yes, check whether an ELAN exists by that name. If an ELAN exists by that name, assign the client to the ELAN. If no ELAN exists by that name, assign the client to the default ELAN (ELAN 0).
 - If no, check the client against the configuration information stored by the `add lecselanlec` command (see The LECSELANLEC Table, on page -11). If an entry exists that corresponds to the client, assign the client to the ELAN indicated. If the client does not correspond to an entry, assign it to the default ELAN (ELAN 0).



Note If the default ELAN (ELAN 0) has been deleted, the client is dropped.

By using ELAN join policies, clients attempting to join LANE services can be assigned to specific ELANs. Table 3-1 lists the ELAN join policies that can be configured on the SmartSwitch 6500.

Table 3-1 ELAN Join Policies

Policy No.	ELAN Join Policy	Information Source Checked
1	Best Effort	Default ELAN policy. Checks configuration information stored by the <code>add lecselanlec</code> command and during ELAN creation (<code>add elan</code> command).
2	By ATM Address	Checks configuration information stored by the <code>add lecselanlec</code> command.
3	By MAC Address	Checks configuration information stored by the <code>add lecselanlec</code> command.
4	By Route Descriptor	Checks configuration information stored by the <code>add lecselanlec</code> command.
5	By LAN Type	Checks configuration information stored during ELAN creation (<code>add elan</code> command).
6	By Packet Size	Checks configuration information from the <code>add lecspacketsize</code> command.
7	By ELAN Name	Checks configuration information stored by the <code>add lecselanname</code> command.



Note For detailed information on each of the commands that ELAN join policies interacts with, see the command descriptions in the SmartSwitch 6500 Reference Manual.

You can give each ELAN join policy a priority value to determine its hierarchy among other ELAN join policies. If you define several ELAN join policies, the policy with the greatest priority value is tried first. If that policy fails, the policy with the next greatest priority value is attempted, and so on. ELAN join policies with the same priority value

are ANDed together. For example, if three join policies are create, each with the same priority value, a client requesting LANE services must meet the criteria of all three policies to be assigned an ELAN. If the client fails to meet the requirements of all three policies, the policy with the next lowest priority value will attempt to assign the client to an ELAN.

Use the `add lecselanpolicy` command to create ELAN join policies. The following is an example of creating an ELAN join policy based on the *By Packet Size* policy.

```
Smart6500 # add lecselanpolicy
PolicyIndex()           : 2      < Can be any value other than one (1)
Type()                  : ?      < Use ? to see possible types
ELAN Policy Type (Values from 1 to 7 representing, in order, the policies BestEffort, byATMAddress,
byMacAddress, byRouteDescriptor, byLANType, byPacketSize and byELANName).
Type()                  : 6      < Specify type 6, assign ELAN by packet size requested by client
Priority()               : 1000   < Weight the policy at 1000

Smart6500 #
```



Note The lower the numerical value of a priority, the higher the priority. In the example above, a priority value of 1000 was specified. Subsequently, This policy will be tried before *Best Effort* (policy value = 65001).

Use the `show lecselanpolicy` command to show the newly created ELAN join policy.

```
Smart6500 # show lecselanpolicy

Index  Assignment Policy          Priority Value
-----
1      Best Effort (Proprietary)  65001
2      By Packet Size            1000 < The created policy, its index number, and its priority

Smart6500 #
```



Note In the example above, index 2 (or greater) was used because the *Best Effort* policy reserves index one.

The LECSELANLEC Table

Many of the ELAN join policies use the information supplied by the `add lecselanlec` command. Use the `add lecselanlec` command to create a list of clients and to assign the ELAN each client should join.



Note You can also assign a TLV set to be used by the client on the specified ELAN.

Clients are identified within the `lecselanlecs` list by one (or a combination of) the following attributes:

- ATM address
- MAC address
- Token Ring route descriptor (segment ID and bridge number)

- IP address

In the following example, a client is identified by its ATM address and IP address, and associates it with ELAN number 1.

```
Smart6500 # add lecselanlec
AtmAddress() : 39:00:00:00:00:00:00:00:00:00:44:55:66:11:22:33:44:55:66:00
MACAddress/RouteDesc() : < No MAC address is specified
Layer3Address[IP]() : 204.123.91.7
ELANNumber(0) : 1 < ELAN is specified by ELAN number
TLVSet() : < No TLV set is specified
```

Smart6500 #

If the currently defined ELAN policies use either *Best Effort* or *By ATM Address* and/or *By IP Address*, the client with the ATM address and IP address specified above will be assigned to ELAN 1.



Note To specify a TLV set with the `add lecselanlec` command, the TLV set must currently exist. Use the `add lecstlvset` command to create a TLV set. For detailed information on the `add lecstlvset` command, see the SmartSwitch 6500 Reference Manual.

4 PNNI ROUTING

The SmartSwitch 6500 default routing protocol is PNNI version 1.0. PNNI provides automatic and dynamic connectivity among all PNNI nodes within the same peer group. By configuring multi-level PNNI topologies and peer group leaders, full hierarchical PNNI routing can be established with connectivity between different peer groups.



Note For a complete explanation of all PNNI related commands, see the SmartSwitch 6500 Reference Manual.

4.1 PNNI NODE ADDRESSING

By default, all SmartSwitch 6500s come configured with a single PNNI node. All PNNI nodes are in the same peer group and at the same group level.

Default Peer Group ID = 50:39:00:00:00:00:00:00:00:00:00:00

Default Group Level = 80 (50 hexadecimal)

The SmartSwitch 6500 assigns default Node IDs based on the following format:

Default Node ID = level + child node's peer group level (see note) + 39 + nine zero (00) bytes + last three bytes of chassis MAC address + switch MAC address with 127 summed with the last byte + zero (00) byte



Note If the node does not have a child node, and the node is also at the lowest level, the second byte is assigned the constant value A0 (160 decimal).

For example, for a node at the lowest level (80), the *level* and *address length* bytes are 50 (80 in hexadecimal) and a0 (160 in hexadecimal), respectively.

The SmartSwitch 6500 assigns default Node ATM Addresses based on the following format:

Default Node ATM Address = 39 + nine zero (00) bytes + last three bytes of chassis MAC address + switch MAC address with 127 summed with the last byte + byte containing node index starting at zero (0) for the first node

Use the **show pnninode** command to view SmartSwitch 6500 PNNI node parameters. For example:

```
Smart6500 # show pnninode
NodeIndex(1)
:
=====
Node Index      : 1
Node Level     : 80
Node Id        : 50:a0:39:00:00:00:00:00:00:00:83:91:e5:00:20:d4:29:0e:ff:00
Lowest         : True
Admin Status   : Up
Oper Status    : Up
Node ATM Addr  : 39:00:00:00:00:00:00:00:00:00:83:91:e5:00:20:d4:29:0e:ff:00
Peer Group Id  : 50:39:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Rst Transit    : False
Complex Rep    : False
Rst Branching  : False
DB Overload    : False
Ptse          : 2

Smart6500 #
```



Note Keep in mind that the **Node ATM Address** is not the same as the ATM address of the switch client (if any). The **Node ATM Address** is used by PNNI to identify PNNI nodes and does not correspond to LANE entities.

4.2 MULTI-LEVEL PNNI TOPOLOGY

Having all ATM switches on your network in the same peer group is a simple way of assuring connectivity between all nodes. However, depending on the size and complexity of your network, there are advantages to dividing your PNNI network into different peer groups and levels. The basic steps for creating multiple peer groups and multiple levels are as follows:

- Set the peer group IDs of SmartSwitch 6500s to differentiate their peer group membership.
- Select one (or more) SmartSwitch 6500 within each peer group as the Peer Group Leader (PGL).
- Add a higher-level PNNI node to each PGL switch. This higher-level node represents its peer group as a Logical Group Node (LGN) within the next highest (parent) peer group. Connectivity between the peer groups is established within the parent peer group.
- Communicate the PGL's existence to the rest of the peer group by setting its leadership priority.
- Physically connect the two peer groups.

4.2.1 Connecting Multiple Peer Groups

This section presents a practical, step-by-step example of creating a multi-level, multiple peer group topology. The example is based on the following components and organization (see Figure 4-1).

- Six SmartSwitch 6500s divided into two peer groups:
 - Three SmartSwitch 6500s in peer group A (switches SWA1, SWA2, and SWA3)
 - Three SmartSwitch 6500s in peer group B (switches SWB1, SWB2, and SWB3)

1. Physically connect switches SWA1, SWA2, and SWA3. Similarly, physically connect switches SWB1, SWB2, and SWB3 (see Figure 4-1).

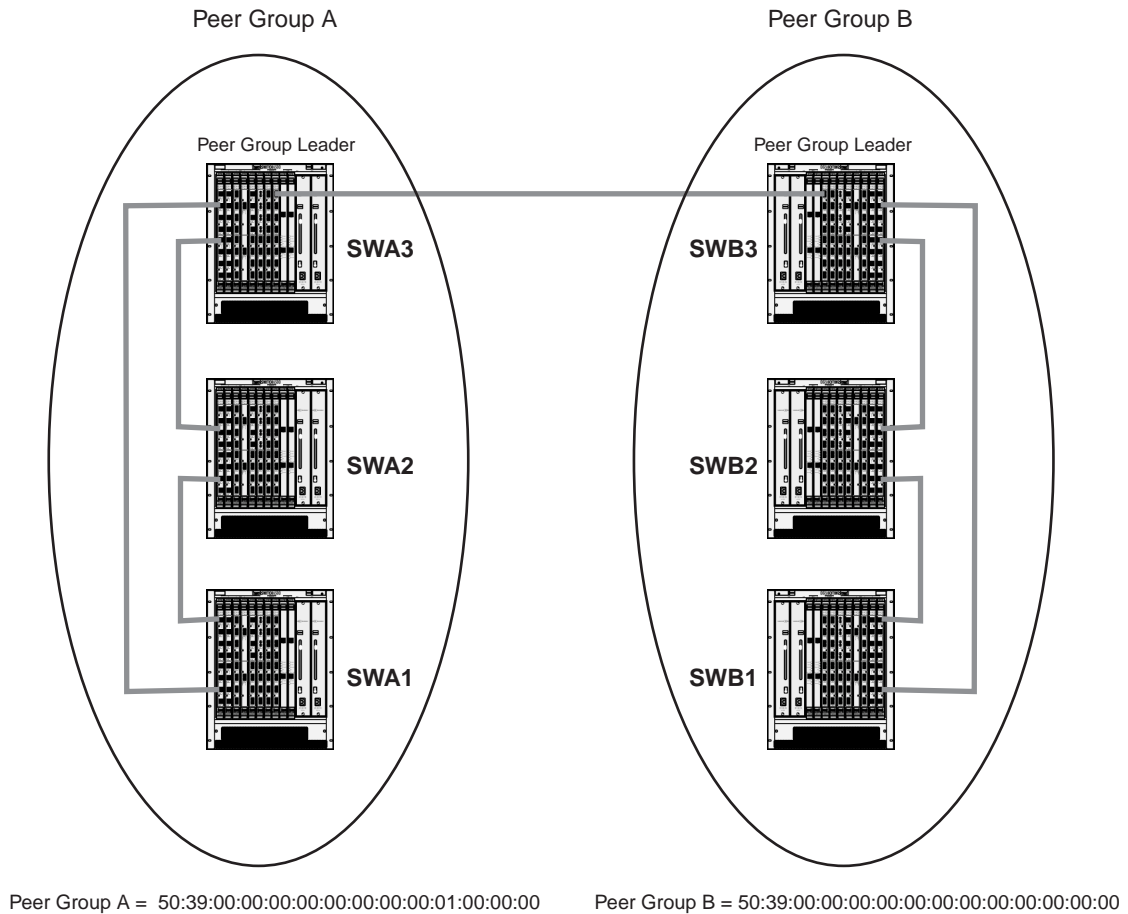


Figure 4-1 Physical connectivity for multi-peer group example

2. Use the `set pnnipeergroupid` command to change the peer group ID of the switches in group A to 50:39:00:00:00:00:00:00:00:00:01:00:00:00. The three remaining switches with the default peer group ID will comprise group B:

```
A1 # set pnnipeergroupid
NodeIndex(1) :
PeerGroupId(50:39:00:00:00:00:00:00:00:00:00:00:00) : 50:39:00:00:00:00:00:00:
00:00:01:00:00:00 < Change the tenth byte to 01
```

Console: You have changed the node configuration. If this node has a parent node, make sure its parent node configuration is compatible with the new configuration.

Console: You will have to reboot for the new node configuration to take effect.

```
A1 #
```

Reboot the switch, and repeat the process for switches SWA2 and SWA3.



Note The first byte of the peer group ID indicates the peer group's level. It also indicates the number of significant bits used in the peer group ID. For example, if the level indicator is 50 (80 decimal), then 80 bits / 8 = 10 bytes; and only 10 of the 13 bytes are significant (39:00:00:00:00:00:00:00:00). If you create a new peer group ID, make sure that the bytes you change are within the range of significant bytes for the peer group's level.

3. Use the `show pnnilink` command to check the PNNI connectivity within each peer group. For example, switch SWA3 sees links to the other two members of its peer group:

```
A3 # show pnnilink
Num(ALL) :
```

Num	Port Number	Node Index	Remote Node IP Addr	Hello State	Link Type
1	7A2	1	206.61.237.20	2WayInside	Lowest Level Horizontal Link
2	7A3	1	206.61.237.19	2WayInside	Lowest Level Horizontal Link

A3 #

4. Select switch SWA3 to be the PGL of group A and switch SWB3 to be the PGL of group B.

5. Use the `add pnninode` command to add a second, higher-level, node to switch SWA3:

```
A3 # add pnninode
NodeIndex(2) : < Specifies node number 2
NodeLevel(72) : < 72 is above the group A's level of 80
ComplexRepresentation(N) :
```

A3 #

Do the same for switch SWB3:

```
B3 # add pnninode
NodeIndex(2) : < Specifies node number 2
NodeLevel(72) : < 72 is above the group B's level of 80
ComplexRepresentation(N) :
```

B3 #

6. Use the `set pnnipglelection` command to set SWA3 and SWB3's leadership priority so that they are elected as PGLs within their respective peer groups:

```
A3 # set pnnipglelection
NodeIndex(1) :
LeadershipPriority(0) : 205 < Highest priority in election process
ParentNodeIndex(0) : 2 < Node 2 will represent the peer group A in the parent group
InitTime(15) :
OverrideDelay(30) :
ReElectTime(15) :
```

A3 #

Do the same on switch SWB3:

```
B3 # set pnnipglelection
NodeIndex(1) :
LeadershipPriority(0) : 205 < Highest priority in election process
ParentNodeIndex(0) : 2 < Node 2 will represent the peer group B in the parent group
InitTime(15) :
OverrideDelay(30) :
ReElectTime(15) :
```

B3 #

7. Use the `show pnnipglelection` command to verify that switches SWA3 and SWB3 have become the PGLs of their respective peer groups. For example, on switch SWA3, enter the following:

```
A3 # show pnnipglelection
NodeIndex(1) :
```

```
PGL Election Information
=====
Node Index      : 1
Leadership Priority : 100
Parent Node Index : 2
Init Time       : 15 secs
Override Delay  : 30 secs
Reelect Time    : 15 secs
Time Stamp      : 228588
Election State   : Operating as PGL < Switch SWA3 has become PGL of group A
Preferred PGL    : 50:a0:39:00:00:00:00:00:00:00:00:00:00:a3:87:0b:00:20:d4:28
:c1:ff:00
Peer Group Leader : 50:a0:39:00:00:00:00:00:00:00:00:00:00:a3:87:0b:00:20:d4:28
:c1:ff:00
Active Parent Node Id : 48:50:39:00:00:00:00:00:00:00:00:00:00:00:01:00:20:d4:28
:c1:ff:00
```

A3 #

8. Physically connect switch SWA3 to SWB3 to establish connectivity between peer groups A and B.

9. Use the `show pnnilink` command to check the connectivity between the peer groups. In the following example, `show pnnilink` is entered on switch SWA3 and shows a link to switch SWB3 (SWB3's IP address is 206.61.237.23):

```
A3 # show pnnilink
Num(ALL) :
```

Num	Port Number	Node Index	Remote Node IP Addr	Hello State	Link Type
1	7A1	1	206.61.237.20	2WayInside	Lowest Level Horizontal Link
2	7A3	1	206.61.237.19	2WayInside	Lowest Level Horizontal Link
3	7B1	1	206.61.237.23	CommonOut	Outside and Uplink < Physical link to switch SWB3
4	--	2	N/A	2WayInside	Horizontal Link to/from LGN < Logical link between the switches

A3 #



Note Notice that the IP address entry for the logical link between the LGNs is N/A (Not Applicable). Logical entities do not have IP addresses.

Connectivity is now established between the two peer groups. For example, if LANE services are running on a switch within peer group A, LANE clients can exist in group B. The clients in group B will traverse the link between the two groups, find the LANE server in group A, and join the ELAN. Figure 4-2 shows a logical representation of the topology created in the example.

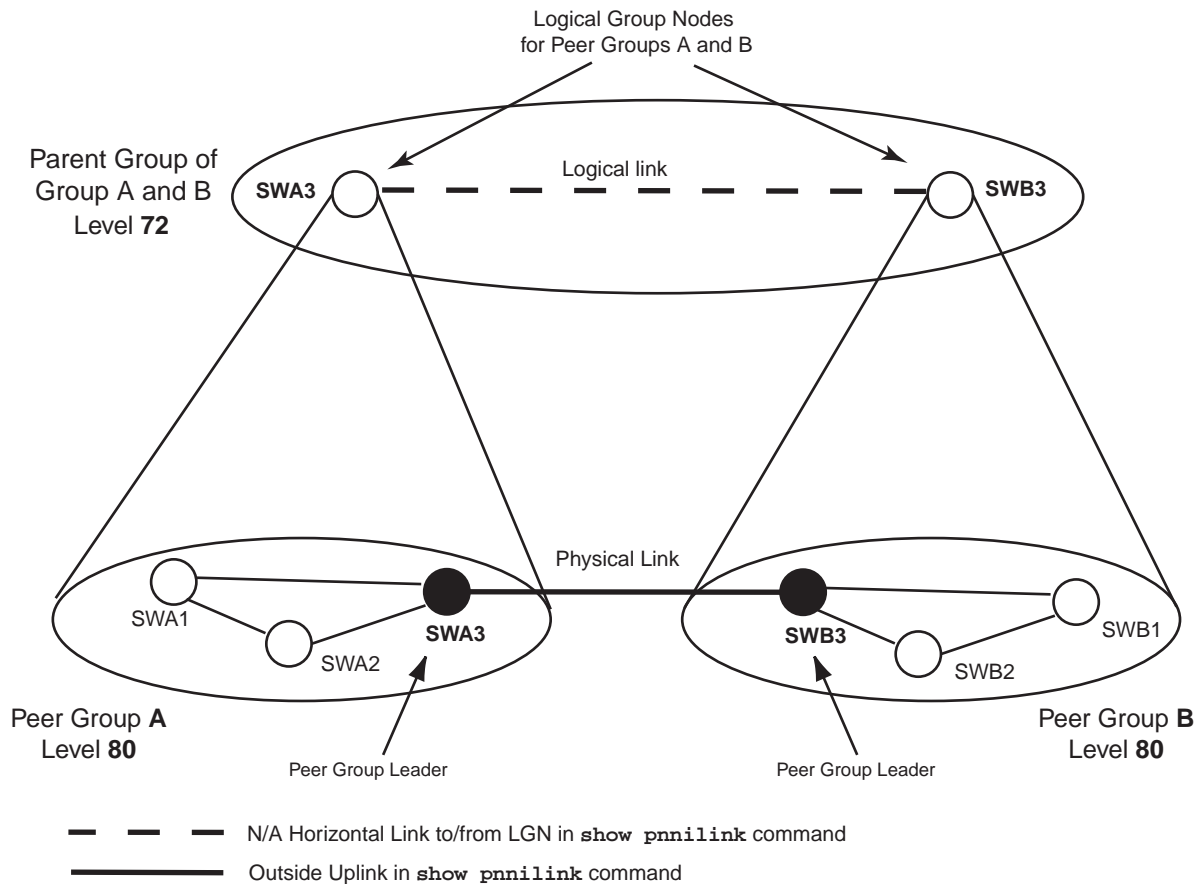


Figure 4-2 Logical representation of connectivity between groups A and B

4.2.2 Physical Connections Between Peer Groups

Keep in mind that the two PGL switches (switches SWA3 and SWB3) do not have to be directly connected to each other for the two peer groups to maintain connectivity. PGLs can find each other through any physical link that connects the two groups. For example, if a second physical link is made between two other switches in groups A and B (for instance, between SWA1 and SWB2), and if the physical link between the PGLs is removed, the PGLs will reestablish their connectivity across the second physical link.

Adding Higher-level Peer Groups

Adapting the process in the example above, more sophisticated PNNI topologies can be created. For example, to establish connectivity with other parent groups at level 72, do the following:

1. Make a physical connection between any two switches represented in the separate parent groups.

2. Add a third node (at level 64) to either switch SWA3 or SWB3.
3. Use the `set pnnipglelection` command to designate the switch's second node (not third) as the PGL for the parent peer group, and specify the third node as the parent node of the second.
4. Perform steps 2 and 3 for switches with the same role in the other level 72 parent groups.

These steps create a grandparent group at level 64, and establishes a virtual link between the LGNs that represent the LGNs at level 72 (see Figure 4-3).

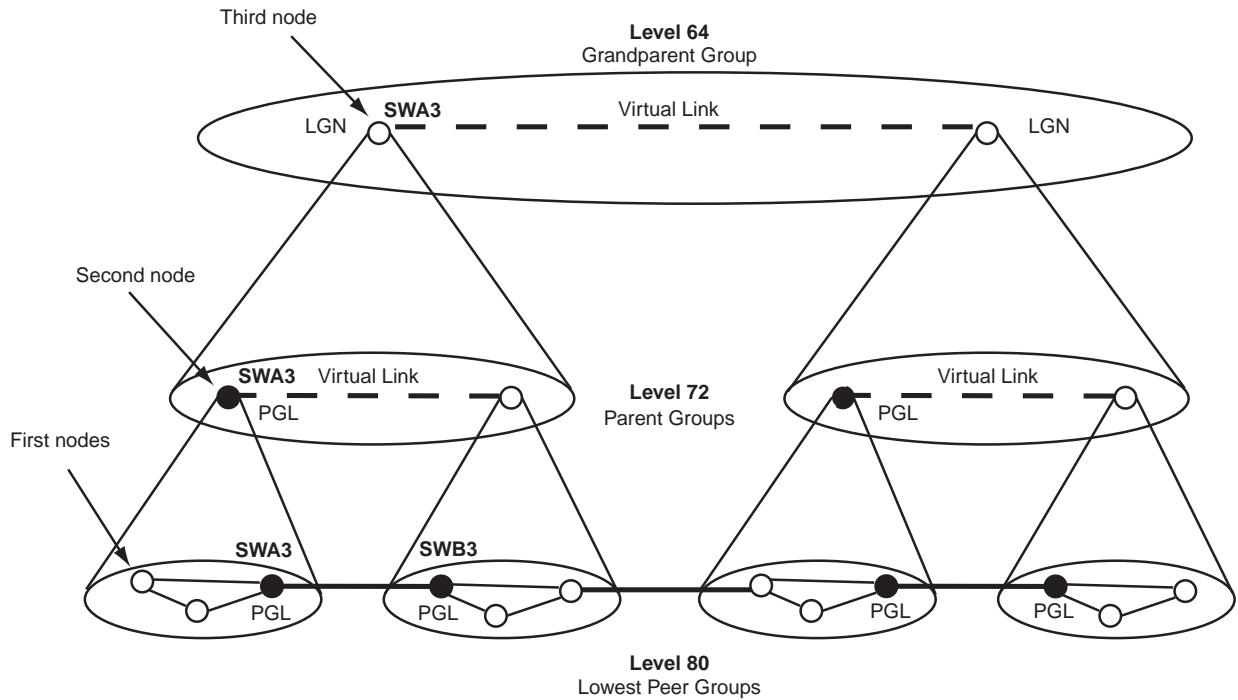


Figure 4-3 Adding a third PNNI node for next level connectivity

4.3 MANAGING PARALLEL PNNI LINKS

SmartSwitch 6500s can be connected by more than one physical link. PNNI treats these connections as parallel physical links. By default, parallel links are considered to have equal capabilities with regard to call set ups.

For example, if a second link is added between switch A3 and switch B3 (from the example above), this parallel link can be seen using the `show pnnilink` command.

```
A3 # show pnnilink
Num(ALL) :
```

Num	Port Number	Node Index	Remote Node IP Addr	Hello State	Link Type
1	7A1	1	206.61.237.20	2WayInside	Lowest Level Horizontal Link
2	7A3	1	206.61.237.19	2WayInside	Lowest Level Horizontal Link
3	7B1	1	206.61.237.23	CommonOut	Outside and Uplink
4	7B2	1	206.61.237.23	CommonOut	Outside and Uplink < Second physical link to B3
5	--	2	N/A	2WayInside	Horizontal Link to/from LGN
6	--	2	N/A	2WayInside	Horizontal Link to/from LGN < Second logical link to B3

A3 #

You can adjust the advertised capabilities of each link (on a per-port, per-service class basis) by changing the link's administrative weights. Use the `show pnniinterface` command to view the current administrative weights. For example:

```
Smart6500_1 # show pnniinterface
PortNumber(ALL) :
```

Port Number	Admin Wt CBR	Admin Wt RTVBR	Admin Wt NRTVBR	Admin Wt ABR	Admin Wt UBR	Aggregation Token
CPU	5040	5040	5040	5040	5040	0
CPU.1	5040	5040	5040	5040	5040	0
7A1	5040	5040	5040	5040	5040	0
7A2	5040	5040	5040	5040	5040	0
7A3	5040	5040	5040	5040	5040	0
7A4	5040	5040	5040	5040	5040	0
7B1	5040	5040	5040	5040	5040	1
7B2	5040	5040	5040	5040	5040	0
7B3	5040	5040	5040	5040	5040	0

Smart6500_1 #

A link's administrative weight defines its desirability to the PNNI routing service when setting up a call of a particular class of service. The lower the numerical value of the administrative weight, the more desirable the route. For example, a route with administrative weight 200 for a particular class of service is considered a better route than one with the default weight of 5040 for that service. As a result, the administrative weight provides a quantitative way to control which routes are favored for call set up with regard to service class.

The ability to control the PNNI routing service in this fashion allows for parallel routes to be weighted such that one link is designated as the favored for a particular service class, while a parallel link can be designated as the favored route for a different service class.

Use the `set pnniinterface` command to set the administrative weight of a physical link originating from a particular port. The following is an example of increasing the administrative weight for CBR call setups through the physical link on port 7a1:

```
Smart6500_1 # set pnniinterface
PortNumber( ) : 7a1 < Link on port 7a1
AdminWtCBR(5040) : 100 < Set the desirability for CBR connections higher on this link
AdminWtRTVBR(5040) :
AdminWtNRTVBR(5040) :
AdminWtABR(5040) :
AdminWtUBR(5040) :
AggregationToken(0) :
RccServCategory(NRTVBR) :
RccServCategory(NRTVBR) :

Smart6500_1 #
```

4.3.1 Aggregation Tokens

An aggregation token is associated with each physical PNNI link. The value of the token determines how a physical link is advertised to the rest of the network. By default, all physical links (even parallel links) use an aggregation token of zero (0). When physical PNNI links have the same token value, the links are represented as a single logical link within the parent peer group. For example, no matter how many physical links connect peer groups A and B, they are represented within the parent group as a single logical link. Using different token values for physical links causes the links to be represented (and advertised) as separate logical links within the parent group.

Continuing with the earlier example of multi-level topologies, add a second physical PNNI link between peer groups A and B by physically connecting switch SWA2 to switch SWB2. By setting the aggregation token of this physical link to a value different from the physical link connecting switches SWA3 and SWB3, a second logical link appears within the parent group.

For example, the physical link between SWA3 and SWB3 has an aggregation token value of zero (0). Use the `set pnniinterface` command to change the value of the aggregation token for the physical link between SWA2 and SWB2 to one (1):

```
A2 # set pnniinterface
PortNumber( ) : 7b2 < Link on switch SWA2 comes from this port
AdminWtCBR(5040) :
AdminWtRTVBR(5040) :
AdminWtNRTVBR(5040) :
AdminWtABR(5040) :
AdminWtUBR(5040) :
AggregationToken(0) : 1 < Change the value of the aggregation token from the default
RccServCategory(NRTVBR) :

A2 #
```

Perform the same operation on switch SWB2 in group B:

```
B2 # set pnniinterface
PortNumber( ) : 4a3 < Link on switch B2 comes from this port
AdminWtCBR(5040) :
AdminWtRTVBR(5040) :
AdminWtNRTVBR(5040) :
AdminWtABR(5040) :
AdminWtUBR(5040) :
AggregationToken(0) : 1 < Change the value of the aggregation token from the default
RccServCategory(NRTVBR) :

B2 #
```

The physical connection from switch SWA2 to switch SWB2 is now advertised as a second logical link within the parent peer group (see Figure 4-4).

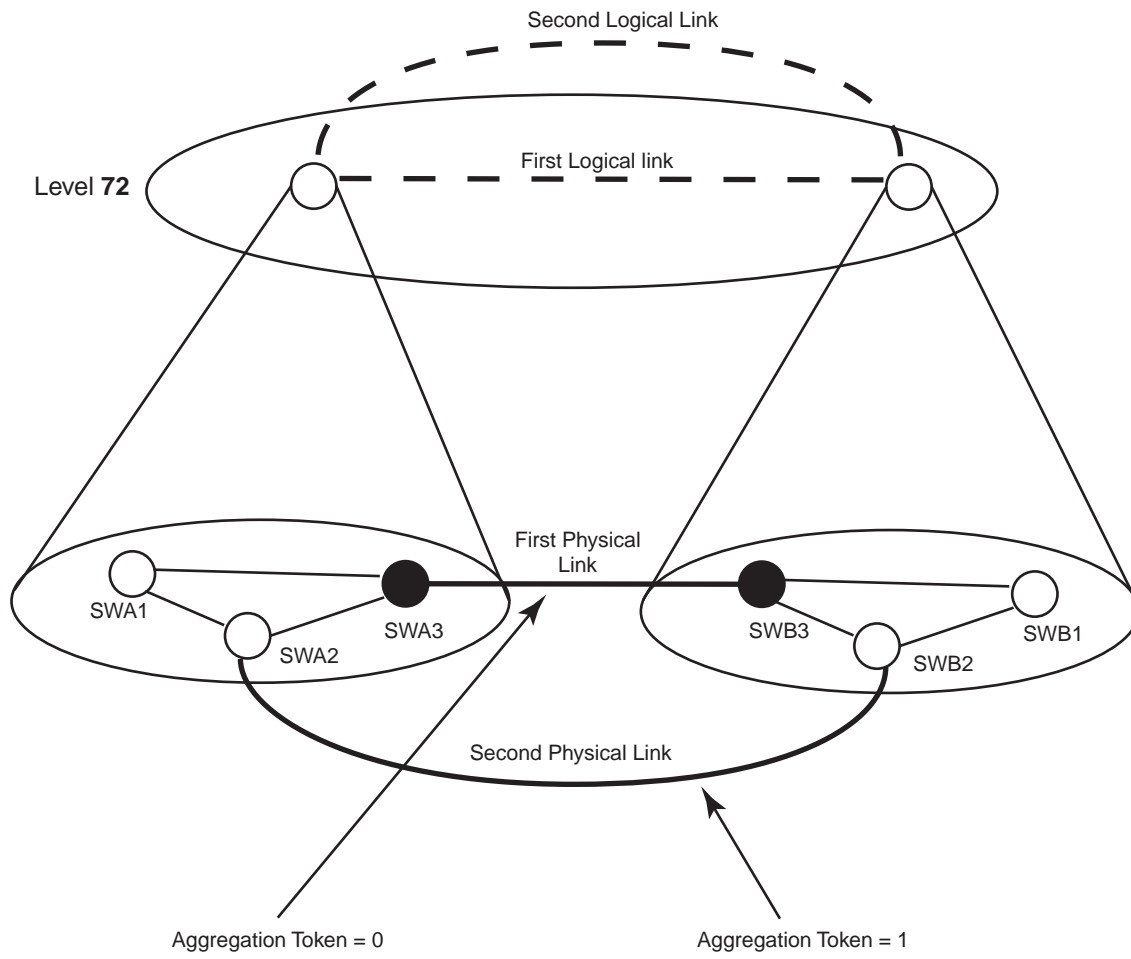


Figure 4-4 Aggregation token values and parallel links

5 ROUTING

5.1 ADDITIONAL ROUTING PROTOCOLS

Along with PNNI, the SmartSwitch 6500 supports additional ATM routing protocols:

- IISP — Use to connect with devices that do not support PNNI
- UNI — Use to connect end stations (also to connect devices whose implementation of ILMI is incompatible with the SmartSwitch 6500)



Note Both IISP and UNI routes are created and modified using the `ATMRoute` command. The proper route type is determined by the SmartSwitch 6500 through interface signaling information.

5.2 IISP ROUTES

Use the `add atmroute` command to create an IISP route that links the SmartSwitch 6500 to a device that supports only IISP routing. For example,

1. Physically connect port `5b2` of the SmartSwitch 6500 to the IISP device.
2. Enter `show netprefix` to determine the netprefix of port `5b2` on the SmartSwitch 6500:

```
Smart6500 # show netprefix 5b2
Port      NetPrefix
-----
5B2      39:00:00:00:00:00:00:00:00:14:41:80
Smart6500 #
```

3. Determine the address of the IISP device. (For this example, this could be a port address, we use `52:00:00:00:00:00:00:00:00:14:51:80`)
4. Enter the `add atmroute` command to create a static route to the IISP device:

```
Smart6500 # add atmroute
PortNumber() : 5b2
AtmAddress() : 52:00:00:00:00:00:00:00:00:14:51:80
PrefixLength(104) :
Index(0) :
Type(Internal) : exterior < This is an exterior route
Scope(0) :
MetricsTag(0) :
Smart6500 #
```



Note The `add atmroute` command allows you to specify a set of metrics to be used with the route. For more information on metrics and metric tags, see Section 5.4, Route Metrics.

5. Enter the `show atmroute` command to determine whether the route was created:

```
Smart6500 # show atmroute
AddressNumber(ALL)          :
No. Port Route Address                                     Type Protocol
=====
1  7B4 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:d4:14:41:80  I  MGMT
2  7B4 39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:d4:14:41:81  I  MGMT
3  -- 39:00:00:00:00:00:00:00:00:00:14:59:00                    I  PNNI
4  -- 39:00:00:00:00:00:00:00:00:00:28:e9:80                    I  PNNI
5  -- 39:00:00:00:00:00:00:00:00:00:28:f5:00                    I  PNNI
6  7B4 47:00:79:00:00:00:00:00:00:00:00:00:00:00:a0:3e:00:00:01  I  MGMT
7  5B2 52:00:00:00:00:00:00:00:00:00:14:51:80                    I  MGMT < This is our route
Smart6500 #
```

The route to the IISP device appears as **route 7**, and with Protocol Type of **MGMT** (management).

6. Create a route on the IISP device that refers to the netprefix
(39:00:00:00:00:00:00:00:00:00:14:41:80) of port **5b2** on the SmartSwitch 6500.



Note For IISP routes to work with certain devices, ILMI may also need to be disabled on the SmartSwitch 6500. Use the `set portconfig` command to disable ILMI on the SmartSwitch 6500 on a per-port basis.

5.2.1 IISP Routing Considerations

When creating routes between the SmartSwitch 6500 (running PNNI) and IISP devices, the criteria that characterize IISP connectivity still apply. To reach a SmartSwitch 6500 within the PNNI domain, the IISP device must have a configured route that points directly to a port on the target SmartSwitch 6500. Conversely, there must be a SmartSwitch 6500 that has a direct physical link (and a route over that link) to the IISP device. The following two examples illustrate this point.

IISP Routing Example One

In Figure 5-1 Switch A is an IISP device connected to the PNNI domain through Switch B. Switch A contains an LEC, which is a member of an ELAN whose LECS is on Switch C (within the PNNI domain). If the LEC on Switch A is to make contact with the LECS on Switch C, Switch A must contain an IISP route directly to switch C. Furthermore, Switch B must contain a route to switch A over the physical link that connects the two switches.



Note Dotted lines in the diagrams below represent one-way IISP routes to the devices pointed to by the arrowheads. Each route is defined on the device from which the dotted line originates.

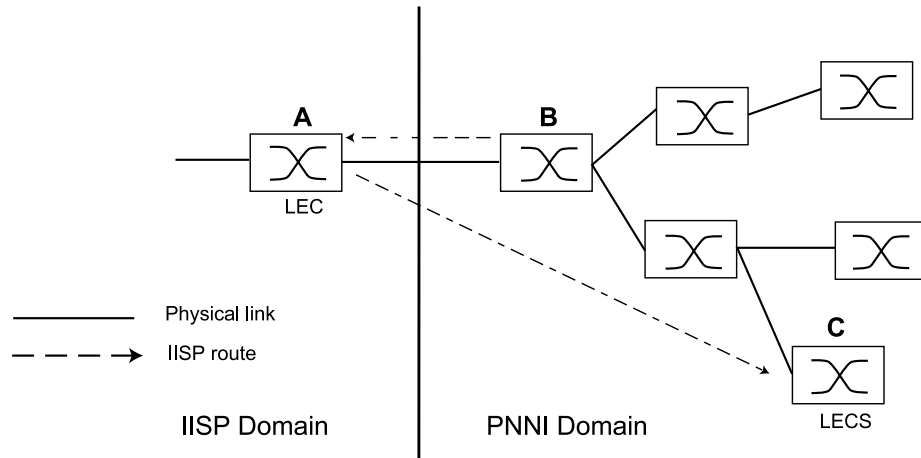


Figure 5-1 IISP route across PNNI domain

IISP Routing Example Two

A second IISP device (Switch D) is added behind Switch A. If Switch D also needs to reach Switch C for LANE support, additional IISP routes must be defined between Switches D and C, B and D, and A and D. Figure 5-2 shows the typical “route to every point reached” IISP topology.

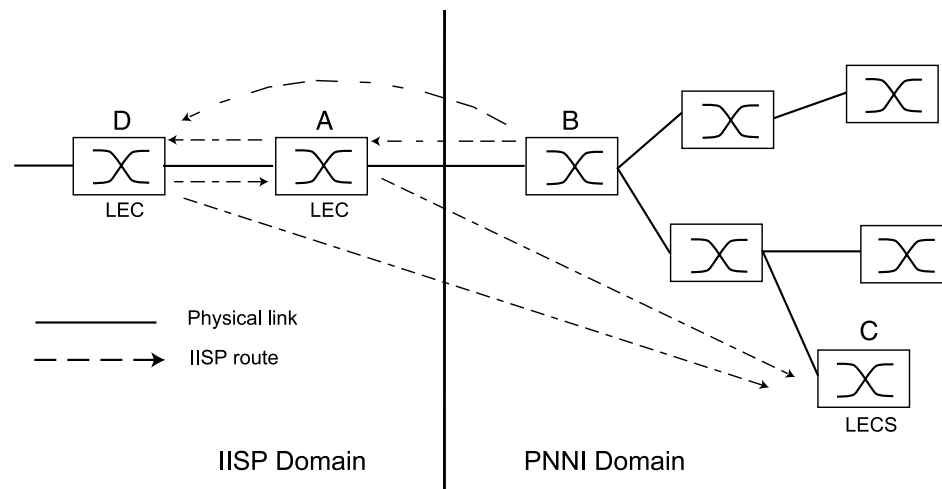


Figure 5-2 Routes needed for a second IISP switch

5.3 UNI ROUTES

Use the `add atmroute` command to create UNI routes. For example, connect an end station adapter (with MAC address 00:11:22:33:44:55) to port 7A2 of the SmartSwitch 6500. If the adapter does not support ILMI or its ILMI is incompatible with the SmartSwitch 6500, you must create a static UNI route between the adapter and port 7A2 of the SmartSwitch 6500. The following is an example:

1. Enter the `show netprefix` command to obtain the netprefix of port 7A2:

```
Smart6500 # show netprefix
PortNumber(ALL)                : 7a2
Port#    NetPrefix
=====
7A2      39:00:00:00:00:00:00:00:00:00:14:59:00
Smart6500 #
```

2. Reconfigure the adapter with an ATM address made from the netprefix of port 7A2 and the adapter's MAC address: 39:00:00:00:00:00:00:00:00:14:59:00:00:11:22:33:44:55:00.
3. Use the `add atmroute` command to create a static UNI route that specifies port 7A2 and the adapter's new ATM address.

```
Smart6500 # add atmroute
PortNumber()                    : 7a2
AtmAddress()                    : 39:00:00:00:00:00:00:00:00:14:59:00:00:11:22:33:44:55:00
PrefixLength(152)              :
Index(0)                        :
Type(Internal)                 :
Scope(0)                        :
MetricsTag(0)                  :
Smart6500 #
```

4. Enter the `show atmroute` command to check that the UNI route was added.

```
Smart6500 # show atmroute
AddressNumber(ALL)              :
No.  Port  Route Address                                     Type Protocol
=====
1    7B4    39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:d4:14:41:80  I    MGMT
2    7B4    39:00:00:00:00:00:00:00:00:00:14:41:80:00:20:d4:14:41:81  I    MGMT
3    --     39:00:00:00:00:00:00:00:00:00:14:59:00                    I    PNNI
4    7A2    39:00:00:00:00:00:00:00:00:00:14:59:00:00:11:22:33:44:55  I    MGMT < Our added UNI route
5    --     39:00:00:00:00:00:00:00:00:00:28:e9:80                    I    PNNI
6    --     39:00:00:00:00:00:00:00:00:00:28:f5:00                    I    PNNI
7    7B4    47:00:79:00:00:00:00:00:00:00:00:00:00:00:00:00:a0:3e:00:00:01  I    MGMT
8    5B2    52:00:00:00:00:00:00:00:00:00:14:51:80                    I    MGMT
Smart6500 #
```

The UNI route appears in the table as **Route 4**, with Protocol Type of **MGMT** (management).



Note For UNI routes to work with certain devices, ILMI may also need to be disabled on the SmartSwitch 6500. Use the `set portconfig` command to disable ILMI on the SmartSwitch 6500 on a per-port basis.

5.4 ROUTE METRICS

Route metrics are assigned to routes using a metric tag (one of the input parameters for `add atmroute`). The metric tag specifies a particular pair of incoming and outgoing metrics contained within a list of metrics. Metrics are created using the `add pnnimetric` command. Each metric pair specifies a set of values that describe a route's Service Category, cell rates, bandwidth, and administrative weight. Locally, metric values determine the behavior of the link, while network-wide, PNNI's Generic Call Admission Control (GCAC) assesses metrics when establishing calls.

In the following example, a metric pair is created (with metric tag of 9) that specifies CBR as the Service Category, administrative weight of 200, Max Cell Rate of 1000 cells per second, and an Available Cell Rate of 750 cells per second.

First, we create the outgoing member of the metric pair:

```
Smart6500 # add pnnimetrics
MetricsTag(1)                : 9
TrafficDirection(Outgoing)   :      < 1st pair member, we accept the default (Outgoing)
ServiceCategory(UBR)         : cbr
GCAC_CLP(2)                  :
AdminWeight(5040)            : 200
MaxCellRate(-1)              : 1000
AvailableCellRate(-1)        : 750
MaximumCellTransferDelay(-1) :
CellDelayVariation(-1)       :
CellLossRatioForCLP=0(-1)    :
CellLossRatioForCLP=0+1(-1)  :
CellRateMargin(-1)           :
VarianceFactor(-1)           :
```

Next, we create the incoming member of the metric pair:

```
Smart6500 # add pnnimetrics
MetricsTag(1)                : 9
TrafficDirection(Outgoing)   : incoming < 2nd pair member, we set as incoming
ServiceCategory(UBR)         : cbr
GCAC_CLP(2)                  :
AdminWeight(5040)            : 200
MaxCellRate(-1)              : 1000
AvailableCellRate(-1)        : 750
MaximumCellTransferDelay(-1) :
CellDelayVariation(-1)       :
CellLossRatioForCLP=0(-1)    :
CellLossRatioForCLP=0+1(-1)  :
CellRateMargin(-1)           :
VarianceFactor(-1)           :
Smart6500 #
```

Enter `show pnnimetric` to view the newly created metric pair:

```
Smart6500 # show pnnimetrics
Metrics(ALL) :
```

Metrics	Metrics Tag	Direction	Index	GCAC CLP	Admin Wt	Service Categories
1	0x9	Incoming	0x10	CLP0+1	200	CBR < Incoming pair member
2	0x9	Outgoing	0x10	CLP0+1	200	CBR < Outgoing pair member
3	0x111113	Outgoing	0x1	CLP0+1	5040	UBR
4	0x111113	Outgoing	0x2	CLP0+1	5040	ABR
5	0x111113	Outgoing	0x4	CLP0	5040	NRTVBR
6	0x111113	Outgoing	0x18	CLP0	5040	CBR RTVBR
7	0x111114	Outgoing	0x1	CLP0+1	5040	UBR
8	0x111114	Outgoing	0x2	CLP0+1	5040	ABR
9	0x111114	Outgoing	0x4	CLP0	5040	NRTVBR
10	0x111114	Outgoing	0x18	CLP0	5040	CBR RTVBR

```
Smart6500 #
```

The newly created metric pair appears at the top of the list as metrics 1 and 2.

Once the metric is created, we can specify its metric tag number within the definition of a route:

```
Smart6500 # add atmroute
PortNumber() : 6b2
AtmAddress() : 39:00:00:00:00:00:00:00:00:55:77:88
PrefixLength(104) :
Index(0) :
Type(Internal) :
Scope(0) :
MetricsTag(0) : 9 < The index tag of our metric pair
Smart6500 #
```

5.5 IP ROUTING

The SmartSwitch 6500 switch provides limited IP routing. IP routing allows switches that are not connected directly to Ethernet to communicate with an Ethernet-based network management system (NMS). The connection is made by adding IP routes on the non-connected switches that specify a client on a connected switch as their gateway to the Ethernet.



Note SmartSwitch 6500 IP routing performance is inadequate for routing between VLANs. If you need to create routes between VLANs on your SmartSwitch 6500, use a router equipped with an ATM interface. Consult Cabletron Customer Support for recommended routers.

For example,

- Switch SW1 and the NMS are on an Ethernet network with address 128.205.99.0.
- The IP address of SW1's Ethernet port is 128.205.99.254.
- The IP address of SW1's LANE client is 90.1.1.254.
- The IP address of SW2's LANE client is 90.1.1.33.
- SW2 is not physically connected to the Ethernet network.

- SW2 is connected to SW1 through PNNI, and both switches are part of the same emulated LAN.

To reach SW2 with the Ethernet-based NMS, create an IP route that assigns SW1's switch client as SW2's default gateway to the network 128.205.99.0. Enter the following on SW2 (see Figure 5-3):

```
Smart6500 # add route
DestNetIP() : 128.205.99.0 < address of the Ethernet network to reach
GatewayIP() : 90.1.1.254 < IP address of SW1's LANE client
Smart6500 #
```

Switch SW2 can now communicate with the NMS on the Ethernet network.

To see the route, enter the `show route` command on SW2

```
Smart6500 # show route
ROUTE NET TABLE
destination      gateway          flags  Refcnt  Use      Interface
-----
0.0.0.0          0.0.0.0         1      0        0        zn0
90.1.1.0         90.1.1.33       1      0        1688     zn1
128.205.99.0    90.1.1.254      1      3        5660     ei0
-----
ROUTE HOST TABLE
destination      gateway          flags  Refcnt  Use      Interface
-----
127.0.0.1       127.0.0.1       5      0        0        lo0
-----
Smart6500 #
```

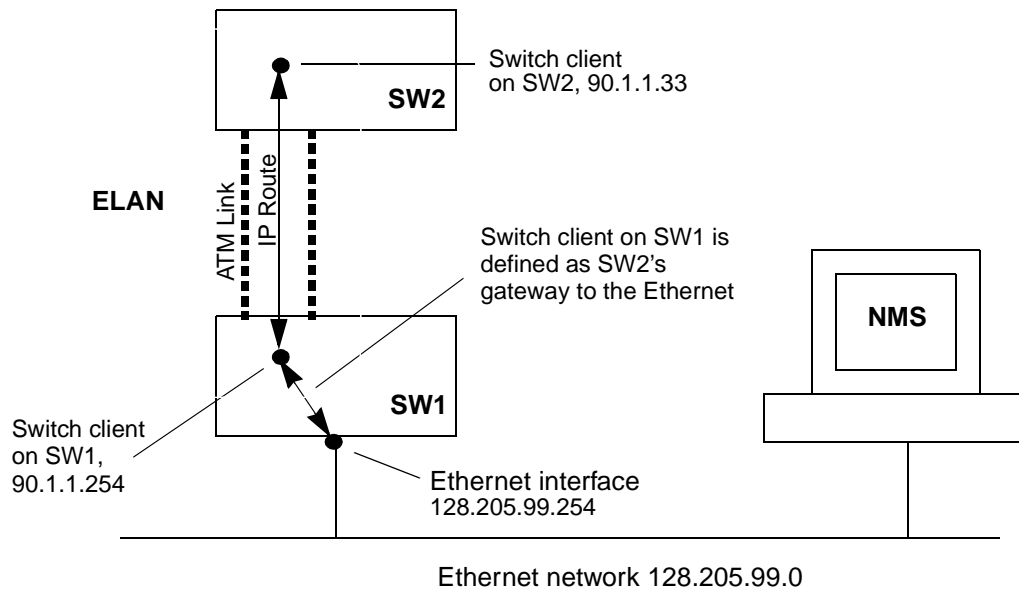


Figure 5-3 IP routing through SW1 for connectivity to the Ethernet network



Note The NMS must also contain a route that specifies the Ethernet interface of the Ethernet connected switch as the gateway to the ELAN subnet.

6 VIRTUAL PORTS AND STATIC CONNECTIONS

6.1 PVC CONNECTIONS

The SmartSwitch 6500 supports Permanent Virtual Circuits (PVCs), both point-to-point and point-to-multipoint. Use PVCs to connect devices (that do not support SVCs) to a switch's local client. Also, use PVCs to make connections through the SmartSwitch 6500 between devices that support only PVCs.

Use point-to-point PVCs to connect one end node to another for two-way communication. Use point-to-multipoint PVCs to connect a broadcast end node to a group of receiving end nodes; traffic is one way.



Note PVCs use traffic descriptors to define their traffic characteristics. See Chapter 7, "Traffic Management," Section 7.1.1 for further information on traffic descriptors.

6.1.1 Point-to-Point PVCs

The procedure for setting up a PVC connection between two end nodes through the SmartSwitch 6500 consists of specifying the ports and the Virtual Path Connection Identifier and Virtual Channel Identifiers (VPCI and VCI).

1. Use **add trafficdescriptor** to define a traffic descriptor to use with the PVC:

```
Smart6500 # add trafficdescriptor
Executing this command : add TrafficDescriptor
TrafficType(UBR)                : cbr
TrafficDescriptorType(2)        :
PCRCLP01(100)                   :
QOSCLASS(1)                      :
AalType(5)                       :
```

Smart6500 #

For this example, we specify CBR as the traffic type, then take the remaining defaults. Enter the **show trafficdescriptor** command to obtain the index number of the new traffic descriptor. In this example, the index number is two (2).

```
Smart6500 # show trafficdescriptor
```

```
=====
```

TD#	Traff Type	Desc Type	QoS	Peak Cell Rate		Sust Cell Rate		Max Burst Size		Min Cell Aal Type	
				(Kb/s)		(Kb/s)		(Kb/s)			
				CLP_0	CLP_0+1	CLP_0	CLP_0+1	CLP_0	CLP_0+1		Rate (Kb/s)
1	NRTVBR	7	0	0	10872	5436	0	2052	0	0	5
2	CBR	2	1	0	100	0	0	0	0	0	5
176	NRTVBR	2	1	0	1585	0	0	0	0	0	5

```
=====
```

```
Smart6500 #
```

- Use **add pvc** to create the PVC; specify the ports through which the connection is established, the VPI/VCI pair to use with each port, and the traffic descriptor to use.

```
Smart6500 # add pvc
ConnType(PTP) :
Port-1-Number() : 7a1 < Specify first port
Port-1-VPCI() : 0 < Specify its VPCI
Port-1-VCI() : 100 < Specify its VCI
Port-2-Number() : 7b2 < Specify second port
Port-2-VPCI() : 0 < Specify its VPCI
Port-2-VCI() : 100 < Specify its VCI
Port1-to-Port2TrafficDescriptorIndex() : 2 < We use our traffic descriptor
Port2-to-Port1TrafficDescriptorIndex() : 2
```

```
Smart6500 #
```

The example above creates a PVC between ports 7a1 and 7b2 with VPCI/VCI = 0/100.

- Plug the end nodes into the specified SmartSwitch 6500 ports (7a1 and 7b2).
- Configure each end node with the proper IP address, subnet mask, and VPCI/VCI pair = 0/100.

The end nodes can communicate with each other through the point-to-point PVC connection.

6.1.2 Point-to-Multipoint PVCs

Instructions in this section describe how to set up a point-to-multipoint connection through your SmartSwitch 6500.

Example: Create a point-to-multipoint connection between a broadcasting workstation on port 7a1 and three other workstations connected to ports 7a2, 7a3, and 7a4.

- Use **add trafficdescriptor** to create two new traffic descriptors, one for the forward direction, the other for the backward direction. For this example, for the forward traffic descriptor, we select UBR and accept the defaults.

```
Smart6500 # add trafficdescriptor < This is the forward descriptor
TrafficType(UBR) : < We use UBR for this example
TrafficDescriptorType(11) :
PCRCLP01(100) : < Take the default values
QOSCLASS(0) :
AalType(5) :
```

```
Smart6500 #
```


However, on a point-to-multipoint connection there should be no traffic in the backward direction, so we define the backward traffic descriptor with its Cell Loss Priorities set to zero (0)

```
Smart6500 # add trafficdescriptor
TrafficType(UBR)                : < This is the backward traffic descriptor
TrafficDescriptorType(11)       :
PCRCLP01(100)                   : 0 < Set PCRCLP01 to zero
QOSCLASS(0)                     :
AalType(5)                      :
```

```
Smart6500 #
```

2. Use **show trafficdescriptor** to obtain the new traffic descriptors' index numbers.

```
Smart6500 # show trafficdescriptor
```

```
=====
```

TD#	Traff Type	Desc Type	QoS	Peak Cell Rate (Kb/s)		Sust Cell Rate (Kb/s)		Max Burst Size (Kb/s)		Min Cell Rate (Kb/s)	Aal Type
				CLP_0	CLP_0+1	CLP_0	CLP_0+1	CLP_0	CLP_0+1		
1	NRTVBR	7	0	0	10872	5436	0	2052	0	0	5
2	CBR	2	1	0	100	0	0	0	0	0	5
3	UBR	11	0	0	100	0	0	0	0	0	5
4	UBR	11	0	0	0	0	0	0	0	0	5
176	NRTVBR	2	1	0	1585	0	0	0	0	0	5

```
=====
```

```
Smart6500 #
```

In the example above, traffic descriptor three (3) will be used in the forward direction, and traffic descriptor four (4) will be used in the backward direction.

3. Use **add pvc** to successively create point-to-multipoint PVCs for ports B2, B3, and C1.

```
Smart6500 # add pvc
ConnType(PTP)                   : pmp
Port-1-Number()                 : 7a1
Port-1-VPCI()                   : 0
Port-1-VCI()                    : 101
Port-2-Number()                 : 7a2
Port-2-VPCI()                   : 0
Port-2-VCI()                    : 101
Port1-to-Port2TrafficDescriptorIndex() : 3
Port2-to-Port1TrafficDescriptorIndex() : 4
```

```
Smart6500 #
```

4. Perform step 3 for ports 7a3 and 7a4.

5. Connect the workstations to their respective ports.

6. Configure the workstations for the same subnet and VPCI/VCI pair = 0/101.

The broadcasting workstation on port 7a1 can send traffic to the receiving workstations on ports 7a2, 7a3, and 7a4.

6.1.3 Connecting to Local Switch Client Through a PVC

All PVC connections to the SmartSwitch 6500 local clients use the CPU port. This port is either 7b4 or 8b4 depending on the slot in which the master TSM/CPU module resides.

Follow these instructions to connect an end node to a SmartSwitch 6500 local client through a point-to-point PVC.

1. Use `add pvc` to create the PVC.

```
Smart6500 # add pvc
ConnType(PTP)                :
Port-1-Number()              : 7a1
Port-1-VPCI()                : 0
Port-1-VCI()                 : 100
Port-2-Number()              : 7b4 < The CPU port
Port-2-VPCI()                : 0
Port-2-VCI()                 : 100
Port1-to-Port2TrafficDescriptorIndex() : 2
Port2-to-Port1TrafficDescriptorIndex() : 2
```

Smart6500 #

2. Use `add ipatmclient` to create the IP over ATM local client.

```
Smart6500 # add ipatmclient
ClientNumber(0)              : 2 < Set client number 2
ServerType(None)             : local < ARP server is on the switch
ServerAddress()              :
IPAddress()                  : 100.1.1.0
NetMask(255.0.0.0)          :
MTU(9180)                   :
```

Smart6500 #

3. Use `add ipatmpvc` to associate the end node's IP address with the PVC.

```
Smart6500 # add ipatmpvc
ClientNumber(0)              : 2 < Specify local client number
DestinationIP()              : 100.1.1.22 < End node's IP address
DestinationVPI(0)            :
DestinationVCI(33)           : 100 <VCI was specified as 100
```

Smart6500 #

4. Connect the end node to port 7a1 of the SmartSwitch 6500.
5. Configure the end node with IP address 10.1.1.22, subnet mask 255.0.0.0, and VPI/VCI pair = 0/100.

6.2 PVP CONNECTIONS

The SmartSwitch 6500 supports the creation of Permanent Virtual Path (PVP) connections. The basic process for creating a PVP is as follows:

- Create a traffic descriptor for the PVP that meets its bandwidth and service category requirements.
- Use the `set portconfig` command to turn off signaling and ILMI on both ports to be connected by the PVP.



Note Dedicated PVP switches do not signal on their physical ports. However, you can leave signaling active on physical ports on the SmartSwitch 6500 if desired.

- Use the `set portconfig` command to specify a number of bits to be used for VPIs (`MaxVpiBits` parameter). Note that a PVP cannot use VPI zero. Consequently, the number of VPI bits must be greater than zero (0) on both ports. Determine the number of Available VPIs from the `MaxVpiBits` setting by using the following equation:

$$\text{Available VPIs} = 2^{\text{MaxVpiBits}-1}$$

For example if `MaxVpiBits` is set to 3, then Available VPIs is:

$$\text{Available VPIs} = 2^3 - 1 = 8 - 1 = 7 \text{ VPIs (VPIs 1 through 7)}$$

We have seven Available VPIs (and not eight) because the zero (0) VPI cannot be used for PVPs.

- Use the `add pvp` command to create the PVP connection.

The following is a practical example of creating a PVP connection between ports `7a4` and `7b1`.

1. Use the `set portconfig` command to turn off signaling and ILMI and to specify bits for VPIs on port `7a4`:

```
Smart6500 # set portconfig
PortNumber( )           : 7a4      < Specify first port for PVP
PortAdminStatus(up)    :
IlmiAdminStatus(up)   : down   < Turn off ILMI
SigType( )             : nnipvc < Turn off signaling
SigRole(network)      :
InterfaceType(private) :
MaxVpiBits(0)          : 1      < 1 bit for VPIs: 21-1 = 1 VPI
MaxVciBits(12)         :
MaxSvcVpci(1)          :
MinSvcVci(32)          :
MaxVccs(8192)          :
MaxSvpVpci(1)          :
MaxVpcs(1)             :
```

Smart6500 #

2. Use the `set portconfig` command to turn off signaling and ILMI and to specify bits for VPIs on port `7b1`:

```
Smart6500 # set portconfig
PortNumber( )           : 7b1      < Specify the second port
PortAdminStatus(up)    :
IlmiAdminStatus(up)   : down
SigType( )             : nnipvc
SigRole(network)      :
InterfaceType(private) :
MaxVpiBits(0)          : 1      < 1 bit for VPIs: 21-1 = 1 VPI
MaxVciBits(12)         :
MaxSvcVpci(1)          :
MinSvcVci(32)          :
MaxVccs(8192)          :
MaxSvpVpci(1)          :
MaxVpcs(1)             :
```

Smart6500 #

3. Use the `add pvp` command to create the pvp connection:

```
Smart6500 # add pvp
ConnType(PTP)                :      < See note below
Port-1-Number()              : 7a4  < Specify the first port
Port-1-VPI()                 : 1    < Specify its VPI
Port-2-Number()              : 7b1  < Specify the second port
Port-2-VPI()                 : 1    < Specify its VPI
Port1-to-Port2TrafficDescriptorIndex() : 2  < Set the traffic descriptors
Port2-to-Port1TrafficDescriptorIndex() : 2

Smart6500 #
```



Note Point-to-multipoint PVPs are currently not supported on the SmartSwitch 6500.

4. Use the `show pvp` command to display the PVP connection:

```
Smart6500 # show pvp
PortNumber(ALL)              :
CrossConnectId(ALL)          :
CrossConnectSubId(ALL)       :

=====
Conn Conn |          Low          |          High          | Admin
Id  SubId | Port  VPI  Type | Port  VPI  Type | Status
=====
3   1     7A4   1   PTP  7B1   1   PTP  UP
=====

Total number of PVPs = 1

Smart6500 #
```

In the example above, we stopped ILMI and signaling on the ports used for the PVP. Stopping ILMI and signaling is characteristic of a “true” PVP connection. However, if necessary, a PVP can be created between ports running ILMI and signaling. In this case, the PVP coexists with the rest of the connections (if any) established across the connection.

6.2.1 Connecting PVPs

PVPs are physically connected to other devices in the following two ways:

- Physically connecting the PVP port to another PVP switch

When connecting to another PVP switch, the VPI numbers assigned to the ports carrying the PVP on each switch must match. For example if a PVP exits switch 1 on port 7a1 and enters switch 2 on port 3b4, the VPI number assigned to port 7a1 on switch 1 and port 3b4 on switch 2 must be the same (see Figure 6-1).

- Terminating the PVP port to a virtual port

PVPs can be terminated on virtual ports (see Section 6.3). To terminate a PVP on a virtual port, the *virtual port number* must be the same as the VPI number for the PVP (see Figure 6-1). For example, to terminate a PVP with VPI number of 3, physically connect it to a port that contains a virtual port with virtual port number equal to three (7a1.3, 5b2.3, 6b4.3 and so on).

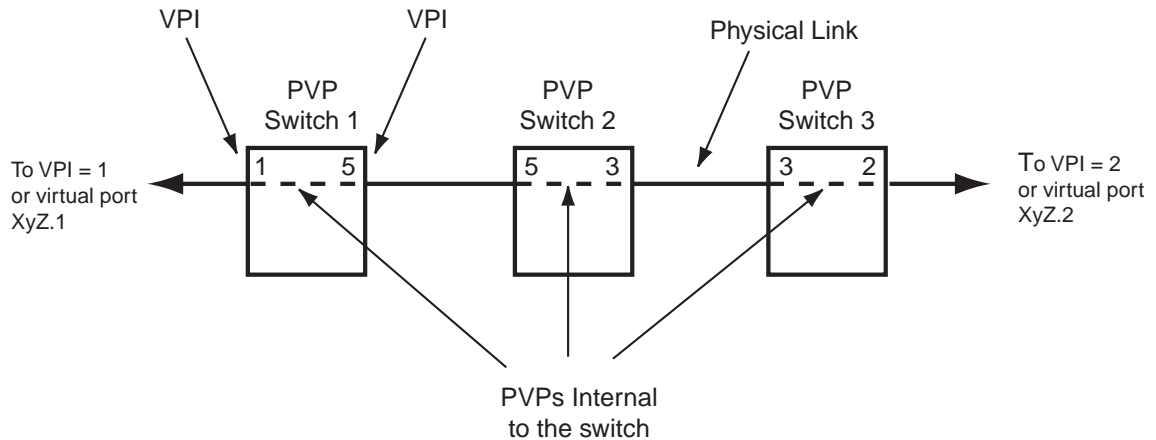


Figure 6-1 Terminating PVPs

6.3 VIRTUAL PORTS

The SmartSwitch 6500 supports the ability to create virtual ports. Typically, virtual ports are used for terminating Permanent Virtual Path (PVP) connections. Virtual ports are designated by the following convention:

number of the physical port + a period + virtual port number

For example, **7a1.3**, **3a4.7**, **5b2.1**, and so on.



Note Zero (0) cannot be used as a virtual port value. Virtual port zero (0) is reserved, and represents the physical port. For example, **7a1.0** and **5b2.0** represent the physical ports **7a1** and **5b2**, and are not available for designating virtual ports.

6.3.1 Creating Virtual Ports

Virtual ports are created on physical ports by first allocating a range of Virtual Path Identifiers (VPIs), and then distributing the VPIs among the virtual ports. The number of VPIs used depends on the number of virtual ports needed and the range of VPIs controlled by each virtual port.

When creating virtual ports, it's important to remember that the virtual port number represents the *Base VPI* used by the virtual port. For example, the virtual port **5b1.3** uses *Base VPI* = 3.

Creating virtual ports on the SmartSwitch 6500 consists of the following basic process

- Create a traffic descriptor for the virtual port that meets its bandwidth and service category requirements.



Note To assure that virtual ports receives the exact bandwidth required, you may want to assign them traffic descriptors that specify CBR as the service class.

- Use the `set portconfig` command to turn off signaling on the physical port on which you are creating the virtual ports.



Note Signaling is usually not used on physical ports on which virtual ports are created. However, you can leave signaling active on the physical ports if necessary.

- Use the `MaxVpiBits` parameters of the `set portconfig` command to set the number of bits to use for VPIs for virtual ports on this physical port:

$$\text{Available VPIs} = 2^{\text{MaxVpiBits}} - 1$$

For example, if `MaxVpiBits` is set to 3, then the number of VPIs available for virtual ports is:

$$\text{Available VPIs} = 2^3 - 1 = 8 - 1 = 7$$



Note The value for Available VPIs is also the *highest* number that can be used to specify a virtual port on the physical port. For instance, in the example above, `7a1.7` is the highest virtual port that can be created using `MaxVpiBits = 3`.

- Use the `add port` command to create the virtual port and to specify the number of VPIs used by the virtual port. Note that the `add port` command also uses the `MaxVpiBits` parameter, however, here it's used to define the number of VPIs the virtual port uses, based on the equation:

$$\text{VPIs Used by Virtual Port} = \text{Base VPI} + (2^{\text{MaxVpiBits}-1})$$

For example, if the virtual port number is `5b2.1` (Base VPI = 1), and `MaxVpiBits = 1`, then the total number of VPIs used by this virtual port is:

$$\text{Base VPI} + (2^1-1) = 1 + (2-1) = 1 + 1 = 2 \text{ VPIs}$$

So port `5b2.1` controls VPI 1 (the Base VPI) and VPI 2.



Note For PNNI, the number of VPIs used by each virtual port should be one (1). For virtual UNI, the number of VPIs used by each virtual port should correspond to the number of VPIs on the user side of the UNI connection (For information on virtual UNI, refer to the ATM Forum specification for ILMI 4.0.).

The following is a practical, step-by-step example of creating a virtual port on physical port `7a1` that controls a single VPI.

1. Use the `set portconfig` command to turn signaling off on physical port `7a1`:

```
Smart6500 # set portconfig
PortNumber()                : 7a1
PortAdminStatus(up)         :
IlmiAdminStatus(up)         :
SigType(autoConfig)         : nnipvc < Turn off signaling by setting SigType to nnipvc
SigRole(network)            :
InterfaceType(private)      :
MaxVpiBits(0)                : < Default MaxVpiBits = 0
MaxVciBits(13)               : < Default MaxVciBits = 13
MaxSvcVpci(0)                :
MinSvcVci(32)                :
MaxVccs(8192)                :
MaxSvpVpci(0)                :
MaxVpcs(0)                   :
```

Smart6500 #

2. Use the `set portconfig` command to assign two bits to `MaxVpiBits`:

```
Smart6500 # set portconfig
PortNumber()                : 7a1
PortAdminStatus(up)         :
IlmiAdminStatus(up)         :
SigType(nniPvc)             :
SigRole(network)            :
InterfaceType(private)      :
MaxVpiBits(0)                : 1 < Set to 1 — this translates to VPIs = 21-1 = 1
MaxVciBits(12)               : < Notice that MaxVciBits has reduced itself by 1 bit
MaxSvcVpci(7)                :
MinSvcVci(32)                :
MaxVccs(8192)                :
MaxSvpVpci(7)                :
MaxVpcs(7)                   :
```

Smart6500 #



Note The command `set portconfig` is used here twice for the purposes of clarity only. Normally, you would turn off signaling and set the `MaxVpiBits` within the same instance of `set portconfig`.

3. Use the `PortNumber` and `MaxVpiBits` parameters of the `add port` command to create the virtual ports.

```
Smart6500 # add port
PortNumber( )                : 7a1.1 < The .1 means our Base VPI is one (1)
PortAdminStatus(up)         :
IlmiAdminStatus(up)         :
SigType(autoConfig)         :
SigRole(other)              :
InterfaceType(private)      :
MaxVpiBits(0)               : 0 < VPIs used = Base VPI + (20 - 1) = 1 + 0 = 1
MaxVciBits(10)              :
MaxSvcVpci(1)               : < Confirms that we have only one VPCI for this virtual port
MinSvcVci(32)               :
MaxVccs(2048)               :
TrafficDescriptorIndex( )   : 1 < Specify traffic descriptor to be used with virtual port

Smart6500 #
```

Our virtual port is now created, and uses just one VPI: the Base VPI (.1).

The following is an example creates virtual port **7b2.4**, which uses seven VPIs, starting at Base VPI = 4.

1. Use the `set portconfig` command to turn off signaling and set the `MaxVpiBits` to 4:

```
Smart6500 # set portconfig
PortNumber( )                : 7b2 < Specify physical port to contain the virtual port
PortAdminStatus(up)         :
IlmiAdminStatus(up)         :
SigType(autoConfig)         : nnipvc < Turn off signaling
SigRole(network)            :
InterfaceType(private)      :
MaxVpiBits(0)               : 4 < Available VPIs are set to 24 - 1 = 16 - 1 = 15 VPIs
MaxVciBits(9)               : < MaxVciBits decrements by 4
MaxSvcVpci(15)              :
MinSvcVci(32)               :
MaxVccs(8192)               :
MaxSvpVpci(15)              :
MaxVpcs(15)                 :

Smart6500 #
```

2. Use the `add port` command to create the port and to specify the number of VPIs:

```
Smart6500 # add port
PortNumber( )                : 7b2.4 < Specify virtual port number (and Base VPI)
PortAdminStatus(up)         :
IlmiAdminStatus(up)         :
SigType(autoConfig)         :
SigRole(other)              :
InterfaceType(private)      :
MaxVpiBits(0)               : 3 < VPIs used = Base VPI + (23 - 1) = 4 + 7 = 11
MaxVciBits(9)               :
MaxSvcVpci(7)               : < Confirms that there are seven VPCI for this virtual port
MinSvcVci(32)               :
MaxVccs(4096)               :
TrafficDescriptorIndex( )   : 1

Smart6500 #
```

In the example above, the virtual port controls eight VPIs. Counting from the Base VPI, these are 4, 5, 6, 7, 8, 9, 10, and 11. Notice that other virtual ports can be created on this physical port because we haven't used all of the available VPI specified by the `set portconfig` command. For example, the next (higher) virtual port that's possible to create is **7b2.12** because the Base VPI is beyond the eight VPIs used by **7b2.4**.

Things To Watch Out For When Creating Virtual Ports

- Make certain that the virtual port number (Base VPI) plus the VPIs designated by `MaxVpiBits` does not exceed the Available VPIs as specified by `MaxVpiBits` in the `set portconfig` command.
- If you create more than one virtual port on a particular physical port, make certain that you do not run out of Available VPIs as specified by `MaxVpiBits` in the `set portconfig` command.
- If you create more than one virtual port on a particular physical port, make certain that no overlap occurs among the VPIs used by the virtual ports.
- Make sure the CAC policy is set correctly for the number of virtual ports.
- Make certain that the traffic descriptors used by the virtual ports were created with the appropriate bandwidth and category of service.

7 TRAFFIC MANAGEMENT

7.1 TRAFFIC MANAGEMENT CAPABILITIES

This section describes how the SmartSwitch 6500 manages bandwidth and congestion. It briefly describes console commands that affect how the SmartSwitch 6500 manages traffic. This section also provides guidelines for setting some traffic control parameters.

The SmartSwitch 6500 has extensive abilities for managing the flow of traffic. Traffic management includes all operations performed by the SmartSwitch 6500 that ensure optimum switch throughput, where throughput is based on rate of packet loss, available bandwidth, and traffic processing overhead. Under most conditions, the SmartSwitch 6500 can efficiently and automatically manage switch traffic. However, if necessary, you can adjust the switch traffic management parameters. For example, it might be necessary to adjust parameters for a port that carries a large amount of CBR traffic or a very large number of simultaneous connections.

The SmartSwitch 6500 provides console commands that affect traffic flow on a global, port, or category of service level. These console commands affect switch traffic flow by controlling

- Bandwidth allocation
- Call Admission Control (CAC) policies
- The service category for a connection
- Buffer memory allocation
- Threshold settings for anti-congestion routines



Caution Do not change traffic control settings unless you have expert-level experience with ATM switching. Back up the switch configuration before making changes. Also, make notes of the changes you make to the traffic control parameters.

7.1.1 Traffic Descriptors

Traffic characteristics of an ATM source are signaled through a set of traffic descriptors during connection establishment. The SmartSwitch 6500 uses traffic descriptors for resource allocation during call set up and guarantees the Quality of Service (QoS) across the connection. The source traffic descriptor is a set of parameters that describes the expected bandwidth utilization of a connection. You can set these parameters,

- Peak Cell Rate (PCR)
- Sustainable Cell Rate (SCR) and Maximum Burst Size (MBS)
- Minimum Cell Rate (MCR) — signaled through UNI4.0 signaling only

Traffic descriptors vary for each QoS. If a connection is bi-directional, a traffic descriptor has to be assigned to each direction and need not be the same in both directions.

SmartSwitch 6500 user data cells are classified according to the state of a cell loss priority (CLP) bit in the header of each cell. A CLP 1 cell has a lower priority than a CLP 0 cell and is discarded first. Source traffic descriptors can specify CLP 0 cell traffic, CLP 1 cell traffic, or the aggregate CLP 0+1 traffic.

Use the `trafficdescriptor` commands to view, create, and delete traffic descriptors.

For example, enter the `show trafficdescriptor` command to view all currently defined traffic descriptors.

```
Smart6500 # show trafficdescriptor
=====
TD#  Traff  Desc  QoS  Peak Cell Rate  Sust Cell Rate  Max Burst Size  Min Cell Aal Type
     Type   Type                (Kb/s)          (Kb/s)          (Kb/s)          Rate
                   CLP_0  CLP_0+1  CLP_0  CLP_0+1  CLP_0  CLP_0+1  (Kb/s)
=====
1    NRTVBR  7     0     0     10872   5436   0     2052   0     0     5
2    CBR     2     1     0     100     0       0     0     0     0     5
176 NRTVBR  2     1     0     1585   0       0     0     0     0     5

Smart6500 #
```



Note You cannot use the default traffic descriptors for user-defined PVCs. All traffic descriptors used to define PVCs must be created by the user.

The Descriptor Type parameter in the example above corresponds to the traffic descriptor types defined in the UNI3.0/UNI3.1 specification. Descriptor types are specified numerically and correspond to the descriptions in Table 7-1.

Table 7-1 Traffic descriptor type number explanation

Type	Valid Service Category	Descriptor Characteristics
1		No Traffic Descriptor
2	CBR	PeakCellRate CLP0+1
3	CBR	PeakCellRate CLP0+1, PeakCellRate CLP0
4	CBR	PeakCellRate CLP0+1, PeakCellRate CLP0, Tag CLP = 1
5	VBR	PeakCellRate CLP0+1, SustCellRate CLP0+1, MaxBurstSize CLP0+1
6	VBR	PeakCellRate CLP0+1, SustCellRate CLP0, MaxBurstSize CLP0
7	VBR	PeakCellRate CLP0+1, SustCellRate CLP0, MaxBurstSize CLP0, Tag CLP = 1
8	ABR	PeakCellRate CLP0+1, Minimum Cell Rate
11	UBR	BestEffort

A user-defined PVC must have user-defined traffic descriptors. For instance, if a video link over a PVC requires a peak cell rate of 8000 kb/s, create a traffic descriptor for CBR traffic that specifies 8000 as the peak cell rate.

```
Smart6500 # add trafficdescriptor
TrafficType(UBR)           : cbr
TrafficDescriptorType(2)   : 3
PCRCLP01(100)             : 8000
QOSCLASS(1)                :
AalType(5)                 :
```

Smart6500 #

Each traffic descriptor is identified by a unique index number. Use the index number to specify which traffic descriptor to use when setting up a PVC. For example, the `add pvc` command prompts you for the traffic descriptor index.

```
Smart6500 # add pvc
ConnType(PTP)              :
Port-1-Number()            : 7a1
Port-1-VPCI()              : 0
Port-1-VCI()               : 100
Port-2-Number()            : 7b2
Port-2-VPCI()              : 0
Port-2-VCI()               : 100
Port1-to-Port2TrafficDescriptorIndex() : 3 < Forward traffic descriptor
Port2-to-Port1TrafficDescriptorIndex() : 2 < Backward traffic descriptor
```

Smart6500 #

Notice in the example above that you can use different traffic descriptors for forward and backward traffic provided that both traffic descriptors used belong to the same service category.

7.1.2 Call Admission Control Policy

Call Admission Control (CAC) policy defines the bandwidth allocation scheme used by the CAC when setting up connections. The SmartSwitch 6500 offers three schemes that can be set on a per-port, per-service class basis,

- Conservative
- Moderate
- Liberal

Under conservative policy, the CAC allocates bandwidth closest to the requested bandwidth and QoS parameters. Conversely, liberal policy causes the CAC to allocate the least amount of bandwidth. And the CAC under moderate policy allocates intermediate amounts of bandwidth.

Depending on the type of traffic on your network, each of these CAC policies has its advantages. For instance, liberal policy allows a larger number of connections over that of the conservative or moderate policy. Liberal policy assumes that the traffic pattern of individual VCs does not overlap most of the time. For example, if VC1 and VC2 are created under the liberal CAC policy, it's assumed that the probability of both VCs sending large bursts of cells at the same time is relatively low. On the other hand, conservative policy assumes that there might be a larger overlap of traffic from different VCs, and provides each VC with bandwidth closer to the requested bandwidth. This higher bandwidth provides a guarantee of quality for each VC.

Use the command `show caceqbwallocscheme` to view the current CAC policies used by each port for each class of service.

```
Smart6500 # show caceqbwallocscheme
PortNumber(ALL) :
```

Port#	Alloc Scheme for				
	CBR	RTVBR	NRTVBR	UBR	ABR
7A1	CON	CON	CON	LIB	CON
7A2	CON	CON	CON	LIB	CON
7A3	CON	CON	CON	LIB	CON
7A4	CON	CON	CON	LIB	CON
7B1	CON	CON	CON	LIB	CON
7B1.3	CON	CON	CON	LIB	CON
7B2	CON	CON	CON	LIB	CON
7B3	CON	CON	CON	LIB	CON
CPU	CON	CON	CON	LIB	CON
CPU.1	CON	CON	CON	LIB	CON

```
Smart6500 #
```



Note The CAC affects both physical and virtual ports as indicated in the example above (7b1.3 is a virtual port).

If there are a large number of connections of a particular class of service on a particular port, and these connections begin to slow down and show signs of congestion, use the `set caceqbwallocscheme` command to change the CAC policy to moderate or conservative.

```
Smart6500 # set caceqbwallocscheme
PortNumber() : 7a1
ServiceCategory(CBR) : ubr
AllocScheme(LIBERAL) : moderate

Smart6500 #
```

Use the `set cacservicelassbw` command to change the amount of bandwidth on a per-port basis that the CAC recognizes as available for each class of service. Available bandwidth for a class of service is specified as a percent of total port bandwidth. For example, to increase the bandwidth for CBR calls on port 7a1 to 20 percent of total port bandwidth, enter the following

```
Smart6500 # set cacservicelassbw
PortNumber() : 7a1
MaxBandwidth_In_Percentage-CBR(1) : 20 < Increase to 20%
MaxBandwidth_In_Percentage-RT_VBR(1) :
MaxBandwidth_In_Percentage-NRT_VBR(7) :
MaxBandwidth_In_Percentage-UBR(89) : 70 < Decrease by 20%
MaxBandwidth_In_Percentage-ABR(1) :
```

```
Smart6500 #
```

Notice in the example above that the total percentage for all service classes on the port must not exceed 100 percent. Furthermore, if the `set cacservicelassbw` command is used to alter a physical port, the change also affects any virtual ports on that physical port.

7.1.3 Queue Buffers

The SmartSwitch 6500 performs buffering using a shared-memory architecture. Buffer space is divided into queues for each class of service. In turn, ports are allocated some portion of each of the service class queues. This allocation is controlled on a per-port basis by the `porttrafficcongestion` commands.

QoS is defined on an end-to-end basis in terms of cell loss ratio, cell transfer delay, and cell delay variation.

For example, enter the `show porttrafficcongestion` command to view current buffer utilization.

```
Smart6500 # show porttrafficcongestion
PortNumber(ALL) :
```

PortID	QueueId	ServiceClass	MinIndex	MinValue	MaxIndex	MaxValue
=====						
CPU	1	CBR	10	64	15	1024
CPU	2	RTVBR	8	256	13	4096
CPU	3	NRTVBR	8	256	13	4096
CPU	4	ABR	8	256	12	8192
CPU	5	UBR	8	256	12	8192
=====						
7A1	1	CBR	10	64	15	1024
7A1	2	RTVBR	8	256	13	4096
7A1	3	NRTVBR	8	256	13	4096
7A1	4	ABR	8	256	12	8192
7A1	5	UBR	8	256	12	8192
=====						
7A2	1	CBR	10	64	15	1024
7A2	2	RTVBR	8	256	13	4096
7A2	3	NRTVBR	8	256	13	4096
7A2	4	ABR	8	256	12	8192
7A2	5	UBR	8	256	12	8192
=====						
7A3	1	CBR	10	64	15	1024
7A3	2	RTVBR	8	256	13	4096
7A3	3	NRTVBR	8	256	13	4096
7A3	4	ABR	8	256	12	8192
7A3	5	UBR	8	256	12	8192
=====						

More (<space>/q)? :

MinValue and **MaxValue** are thresholds set on a per-queue, per-port basis and are measured in cells (53 bytes). The **MinValue** threshold is the amount of buffer space guaranteed to a call of a particular service class on the corresponding port. The **MaxValue** threshold is the maximum amount of buffer space that a call of a particular service class is allowed on the corresponding port.

QoS corresponds to the queues as follows:

- Queue 1 — Constant Bit Rate (CBR)
- Queue 2 — Real Time Variable Bit Rate (rt-VBR)
- Queue 3 — Non-real time Variable Bit Rate (Nrt-VBR)
- Queue 4 — Available Bit Rate (ABR)

- Queue 5 — Unspecified Bit Rate (UBR)

If calls of a particular service class are being dropped on a particular port, use the `set porttrafficcongestion` command to raise the port's queue Min threshold.

For example, to change both the Min and Max amounts of buffer space used for CBR calls on port `7a3`, first enter the `show porttrafficcongestion` command to determine the current minimum threshold level:

```
Smart6500 # show porttrafficcongestion
PortNumber(ALL)                : 7a3

PortID QueueId ServiceClass MinIndex MinValue MaxIndex MaxValue
=====
7A3    1      CBR           10      64      15      1024
7A3    2      RTVBR          8      256     13      4096
7A3    3      NRTVBR         8      256     13      4096
7A3    4      ABR            8      256     12      8192
7A3    5      UBR            8      256     12      8192

Smart6500 #
```

CBR on port `7a3` is currently using 64 (`MinIndex 10`) as its minimum threshold. Use the `show minmax` command to determine a new minimum threshold for CBR:

```
Smart6500 # show minmax
-----
MinIndex  MinValue  MaxIndex  MaxValue
-----
0         65536     0         1048576
1         32768     1         786432
2         16384     2         524288
3         8192      3         393216
4         4096      4         262144
5         2048      5         196608
6         1024      6         131072
7         512       7         98304
8         256       8         65536
9         128       9         49152
10        64        10        32768
11        32        11        16384
12        16        12        8192
13        8         13        4096
14        4         14        2048
15        0         15        1024

Smart6500 #
```

From the table, we'll select 128 (`MinIndex 9`). Use the `set porttrafficcongestion` command to assign this value to CBR for port `7a3`.

```
Smart6500 # set porttrafficcongestion
Port(ALL)                : 7a3
QueueNumber( )           : 1    < Corresponds to CBR
MinIndexNumber( )        : 9    < MinIndex for 128
MaxIndexNumber( )        : 15   < Specify the current MaxIndex
```


7.1.4 EFCI, EPD, and RM Cell Marking

To control switch congestion, the SmartSwitch 6500 implements standard resource management cell (RM-cell) marking, explicit forward congestion indicator cell marking (with backward RM cell marking), and early packet discard (EPD). These congestion control schemes are triggered when the number of cells within shared memory reaches user-definable thresholds. Use the `switchtrafficcongestion` commands to view and set these thresholds.

For example, enter the `show switchtrafficcongestion` command.

```
Smart6500 # show switchtrafficcongestion
```

```
Switch Traffic Congestion Parameters
=====
Low EPD Threshold           : 209715 cells
High EPD Threshold         : 104857 cells
CLP1 Discard Threshold     : 131072 cells
RM Cell Marking Enable     : OFF
EFCI Cell Marking Enable   : OFF
Explicit Rate Marking Enable : OFF
```

```
Smart6500 #
```

For most types of traffic, EPD triggering is tied to the low EPD threshold. Signaling traffic, however, is tied to the high EPD threshold; this assures that signaling packets are discarded only when congestion is most severe.

Use the `set switchtrafficcongestion` command to change thresholds for EPD and to enable or disable RM and EFCI cell marking. For example:

```
Smart6500 # set switchtrafficcongestion
LowEPDWatermark(4096)      :
HighEPDWatermark(4096)    :
CLP1_DiscardWatermark(4096) :
RMCellMarkingEnable(enable) :
ExplicitRateMarkingEnable(enable) :
EFCIMarkingEnable(enable)  :
```

```
Smart6500 #
```


8 UPGRADES AND FIRMWARE

8.1 UPGRADING AND CHANGING FIRMWARE

This section describes the low-level boot load commands. Boot load commands are used for setting switch start-up behavior and for performing firmware downloads. Use the boot load commands to:

- Set which copy of the boot load firmware is the default copy
- Clear all configurations stored within the flash file system
- Check boot load firmware version numbers
- Load switch firmware upgrades
- Set whether power-on system tests (POST) are automatically run at start-up
- Manipulate the master/slave relationship for TSM/CPU's and CSM's

8.1.1 Accessing the Boot Load Prompt

Boot load commands are executed from the boot load prompt. The boot load prompt is not part of the switch console, and is accessible only after a reboot and before the switch firmware is loaded. Consequently, the boot load commands can be used only through a terminal connection.

Perform the following steps to gain access to the boot load prompt:

1. Connect a dumb terminal (or workstation running terminal emulation software) to the RJ-45 terminal port on the front of the SmartSwitch 6500.
2. Enter the `reboot` command from the terminal.
3. Wait for the following message to appear:
"Press any key to exit to boot load prompt."
4. Before the countdown reaches zero, press a key to access the boot load prompt. Notice that the boot load prompt (`=>`) differs from the prompt used by the switch console.

8.1.2 Boot Load Commands

The following table describes the commands available from the boot load prompt, their use, and their associated parameters.

Table 8-1 Boot load commands

Command	Action	Parameters
<code>chpi</code>	<p>Change default boot load image:</p> <p>Sets one of two images of the boot load firmware as the default. Default boot load image is executed at start-up.</p>	<p><code>chpi 0</code> = set boot load image 0 as default</p> <p><code>chpi 1</code> = set boot load image 1 as default</p>
<code>clfs</code>	<p>Clear flash file system:</p> <p>Clear flash file system of all switch configuration information.</p>	none
<code>dcfg</code>	<p>Display boot load configuration:</p> <p>Displays revision numbers of both boot load images, the switch MAC address, and the file space (in hexadecimal) available for additional MAC addresses.</p> <p>Shows whether POST is set to run at switch start-up.</p>	none
<code>df</code>	<p>Download Firmware:</p> <p>Downloads firmware images from a TFTP/Bootp server.</p> <p>Different components of the switch firmware are downloaded, depending on the parameter used with this command.</p>	<p><code>df B</code> = download boot load firmware</p> <p><code>df S</code> = download switch operating firmware</p> <p><code>df P</code> = download diagnostics (POST)</p> <p><code>df (none)</code> = download switch operating firmware</p>
<code>go</code>	<p>Run switch firmware:</p> <p>Exit the boot load prompt, and run switch operating firmware.</p>	<p><code>go V</code> = run switch firmware, do not run POST</p> <p><code>go P</code> = run POST before running switch firmware</p> <p><code>go (none)</code> = run switch firmware, do not run POST</p>
<code>he</code>	<p>Show help:</p> <p>Displays help for a boot load command or displays list of all boot load commands.</p>	<p><code>he [<command>]</code> = display help for command specified</p> <p><code>he</code> = display list of all boot load commands</p>
<code>ponf</code>	<p>POST on or off:</p> <p>Changes start-up action: either run POST before running switch firmware or skip POST and go directly to switch firmware.</p>	<p><code>ponf V</code> = run switch firmware after start-up timeout</p> <p><code>ponf P</code> = run POST before running switch firmware</p>

Table 8-1 Boot load commands (Continued)

Command	Action	Parameters
<code>scsm</code>	Switch to the redundant CSM: Tells the SmartSwitch 6500 to transfer CSM mastership to the slave CSM.	none
<code>swms</code>	Switches CPU mastership to other TSM/CPU: Changes the slave TSM/CPU to the master.	none

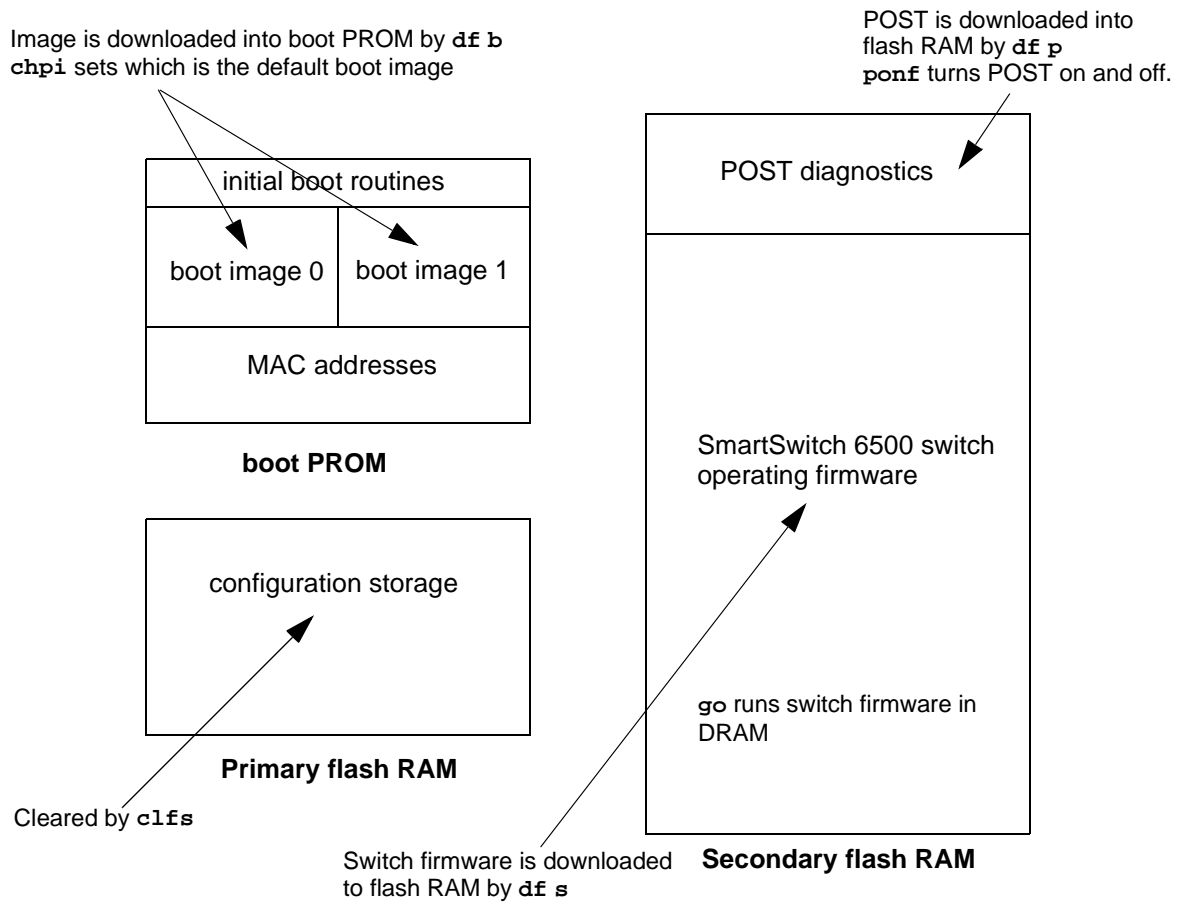


Figure 8-1 Memory locations affected by the boot load commands

8.1.3 Upgrading Boot Load firmware

Two images of the boot load firmware reside in flash RAM. The two images are identified as boot load image 0 and boot load image 1. Both boot load images can be upgraded by using a TFTP/Bootp server. However, an upgrade is always written over the boot load image that is not currently running. This insures that if a boot load upgrade fails, there is still one good boot load image to fall back on.

Follow the steps below to upgrade the switch boot load firmware.

1. Set up the TFTP/Bootp server software on a workstation.
2. Connect both the TFTP/Bootp server and the SmartSwitch 6500 to your Ethernet network. Make sure that the TFTP/Bootp server can be reached by the SmartSwitch 6500 Ethernet interface.
3. Connect a dumb terminal (or PC running terminal emulation software) to the SmartSwitch 6500 Terminal port.
4. Copy the SmartSwitch 6500 boot load firmware image into the appropriate location on the TFTP/Bootp server. (In this example, the firmware is copied to c:\tftpboot\images\boot.ima.)
5. Set up the TFTP/Bootp server tables (or equivalent file) with:
 - SmartSwitch 6500 MAC address
 - IP address of the SmartSwitch 6500 Ethernet interface
 - path to the boot image file on the TFTP/Bootp server
6. From the terminal connection, enter the `reboot` command.
7. When the following message appears,

```
"Press any key to exit to boot load prompt."
```

stop the countdown by pressing any key. The boot load prompt (`=>`) appears on the terminal screen.

8. Enter the `df b` command. The SmartSwitch 6500 contacts the TFTP/Bootp server and downloads the file into the boot load image location that corresponds to the boot load image not currently running. For example, if boot load image 0 is running, `df b` downloads the file into boot load image 1, leaving boot load image 0 untouched.

```
=>df b
You've requested a Boot Load Software download
Are you sure?(Y/N)y
Initializing ethernet...
Starting Bootp...
  Boot file: c:\tftpboot\images\boot.ima
Using TFTP to get bootfile "c:\tftpboot\boot\boot.ima" .
.....
.....
Validity checks of the Boot Load Software Downloaded file...
All Validity checks OK
Programming downloaded image into Boot Load Software1 area, please wait...
New Boot Load Software programmed successfully.
Modifying Control/Stat field to reflect new image change, please wait...
Control/Stat field programmed successfully.
Please reboot to execute new Boot Load Software
=>
```

9. If the new boot load firmware passes the validity checks, it is marked as the new default image. In the example above, boot load image 1 becomes the new default image.
10. Reboot the SmartSwitch 6500 to run the new boot load firmware. Notice that the boot load message at start-up indicates that the SmartSwitch 6500 is now loading and running boot load image 1.

Changing the Default Boot Load Image

Continuing with the example above, perform the following steps to set boot load image 0 back to being the default.

1. Reboot the SmartSwitch 6500.
2. When the following message appears

```
"Preparing to run Default Primary Image: 1
Enter 0 or 1 to override and force one of these primary image sectors to run:"
```

press the zero (0) key. The SmartSwitch 6500 loads boot load image 0.

3. Use the `chpi` command to make boot load image 0 the default.

```
=>chpi 0
Old Default Primary Image Number: 1
Erasing Sector in Primary Flash sector4
Programming control/stat info into Primary Flash sector4
New Default Primary Image Number: 0
=>
```

4. Reboot the SmartSwitch 6500. Boot load image 0 is now used as the default image.

```
Preparing to run Default Primary Image: 0
Enter 0 or 1 to override and force one of these primary image sectors to run:
```

8.1.4 Upgrading POST Diagnostic firmware

1. Set up the TFTP/Bootp server software on a workstation.
2. Connect both the TFTP/Bootp server and the SmartSwitch 6500 to your Ethernet network. Make sure that the TFTP/Bootp server can be reached by the SmartSwitch 6500 Ethernet interface.
3. Connect a dumb terminal (or workstation running terminal emulation software) to the SmartSwitch 6500 Terminal port.
4. Copy the SmartSwitch 6500 diagnostic firmware image into the appropriate location on the TFTP/Bootp server. (In this example, the firmware is located at `c:\tftpboot\images\post.ima`.)
5. Set up the TFTP/Bootp server tables (or equivalent file) with:
 - SmartSwitch 6500 MAC address
 - IP address of the SmartSwitch 6500 Ethernet interface
 - path to the POST file on the TFTP/Bootp server
6. From the terminal connection, enter the `reboot` command.
7. When the following message appears,

```
"Press any key to exit to boot load prompt."
```

stop the countdown by pressing any key. The boot load prompt (`=>`) appears on the terminal screen.

8. Enter the `df p` command. The SmartSwitch 6500 contacts the TFTP/Bootp server and downloads the diagnostic firmware into flash RAM.

```
=>df p
You've requested a POST Software download
Are you sure?(Y/N)y
Initializing ethernet...
Starting Bootp...
  Boot file: c:\tftpboot\images\post.ima
Using TFTP to get bootfile "c:\tftpboot\images\post.ima" .
.....
```

```

.....
.....
.....
.....
Validity checks of POST software Downloaded file...
All Validity checks OK
Programming downloaded image into POST Software section, please wait...
New POST Software programmed successfully
=>
    
```

9. Check whether the diagnostic download is successful by entering the `go p` command. This forces the SmartSwitch 6500 to run POST before starting the switch firmware.

8.1.5 Upgrading Switch Operating firmware



Note SmartSwitch 6500 operating firmware can also be updated using the switch console `update firmware` command (see Section 8.1.6).

1. Set up the TFTP/Bootp server software on a workstation.
2. Connect both the TFTP/Bootp server and the SmartSwitch 6500 to your Ethernet network. Make sure that the TFTP/Bootp server can be reached by the SmartSwitch 6500 Ethernet interface.
3. Connect a dumb terminal (or workstation running terminal emulation software) to the SmartSwitch 6500 Terminal port.
4. Copy the SmartSwitch 6500 switch operating firmware image into the appropriate location on the TFTP/Bootp server. (In this example, the firmware is located at `c:\tftpboot\images\server.ima`.)
5. Set up the TFTP/Bootp server tables (or equivalent file) with:
 - SmartSwitch 6500 MAC address
 - IP address of the SmartSwitch 6500 Ethernet interface
 - path to the operating firmware file on the TFTP/Bootp server
6. From the terminal connection, enter the `reboot` command.
7. When the following message appears,

"Press any key to exit to boot load prompt."

 stop the countdown by pressing any key. The boot load prompt (`=>`) appears on the terminal screen.
8. Enter the `df s` command. The SmartSwitch 6500 contacts the TFTP/Bootp server and downloads the switch operating firmware into flash RAM.

```

=>df s
You've requested a Switch Software download
Are you sure?(Y/N)y
Initializing ethernet...
Starting Bootp...
  Boot file: c:\tftpboot\images\server.ima
Using TFTP to get bootfile "c:\tftpboot\images\server.ima" .
.....
.....
.....
.....
    
```



```

.....
Validity checks of the Switch Software Downloaded file...
All Validity checks OK
Programming downloaded image into Switch Software section, please wait...
New Switch Software programmed successfully
=>

```

9. Check whether the switch download is successful by entering the `go` command.

8.1.6 Using the Update Firmware Command

You can upgrade the operating firmware of the SmartSwitch 6500 while the switch is running its current firmware. This procedure is known as a hot upgrade and is accomplished by the `update firmware` command.

When the SmartSwitch 6500 is started (or rebooted), it copies its operating firmware from flash RAM to the CPU's program memory. When a hot upgrade is performed, the image in flash RAM is erased and replaced with the new firmware image. While the upgrade is occurring, the switch continues to run its copy in program memory. When the switch is rebooted, the new firmware image residing in flash RAM is copied into system memory and then run.

To use the hot upgrade feature, the SmartSwitch 6500 must have network access to an end station running TFTP server software. The SmartSwitch 6500 operating firmware file must reside within the directory specified by the TFTP server software. Often, this directory is `/tftpboot`. However, it may be different with your TFTP server software.

The following is an example of a hot upgrade:

```

Smart6500 # update firmware
ServerIP()                : 206.61.237.127          < IP address of TFTP server
Path(public/Smart6500.ima) : builds/luxor2/server.ima < Path and name of file to download

```

You are updating the code image in the flash.

```

Are you sure this is what you want to do?
Confirm(y/n)?y           < Specify Yes to start download process

```

```

Verifying bootfile builds/luxor2/server.ima on 206.61.237.127
...passed.

```

Erasing Flash.

```

Using TFTP to get and program bootfile builds/luxor2/server.ima from 206.61.237.127.
4904K (5021760 bytes) received.

```

Flash update succeeded.

You will have to reboot for the new image to take effect.

```

Smart6500 #

```

Notice that the `update firmware` command does not use `Bootp` to find the TFTP server. Instead, the `update firmware` command requires that you specify the IP address of the TFTP server, the path to the image file, and the file name.

Unsuccessful Update

If the `update firmware` command fails, DO NOT turn off or attempt to reboot your SmartSwitch 6500 switch. In its current state, the operating firmware normally stored in flash RAM is erased. The switch is functioning only because it is running the image of the operating firmware that resides in volatile system memory.

If possible, determine why the `update firmware` command failed. Possible causes are:

- The SmartSwitch 6500 lost network connectivity before it finished its download
- The wrong file or a corrupt file was downloaded into memory

If you can correct the problem, enter the `update firmware` command to continue with the upgrade process. However, if you are unable to correct the problem, use the `df` (download flash) command and a TFTP/Bootp server to replace the operating firmware on your SmartSwitch 6500. Follow the procedure outlined below:

1. Set up TFTP/Bootp server software on a workstation.
2. Connect both the TFTP/Bootp server and the SmartSwitch 6500 to your Ethernet network. Make sure that the TFTP/Bootp server can be reached by the SmartSwitch 6500 Ethernet interface.
3. Connect a dumb terminal (or workstation running terminal emulation software) to the SmartSwitch 6500 Terminal port.
4. Copy the SmartSwitch 6500 operating firmware image into the appropriate location on the TFTP/Bootp server.
5. Set up the TFTP/Bootp server tables (or equivalent file) with the SmartSwitch 6500 MAC address and IP address. You may also need to specify the path to the image file to be downloaded.
6. From the terminal connection, enter the `reboot` command.
7. When the following message appears,

```
"Press any key to exit to boot load prompt. "
```

stop the countdown by pressing any key. The boot load prompt (`=>`) appears on the terminal screen.

8. Enter the `df s` command. The SmartSwitch 6500 contacts the TFTP/Bootp server and downloads the operating firmware into its flash RAM.

```
=>df s
You've requested a Switch Software download
Are you sure?(Y/N)y
Initializing ethernet...
Starting Bootp...
  Boot file: c:\tftpboot\images\server.ima
Using TFTP to get bootfile "c:\tftpboot\images\server.ima" .
.....
.....
.....
.....
.....
Validity checks of the Switch Software Downloaded file...
All Validity checks OK
Programming downloaded image into Switch Software section, please wait...
New Switch Software programmed successfully
=>
```

9. Enter the `go` command to start the SmartSwitch 6500.

9 TROUBLESHOOTING

This chapter provides basic troubleshooting for diagnosing and fixing problems with VLAN, emulated LANs, and ATM traffic congestion.

9.1 TROUBLESHOOTING IP OVER ATM

You have configured an IP over ATM VLAN, but your network applications are not working. Use these questions and tests to help determine the cause of the problem.

1. Check for connectivity: Try pinging between end nodes and from the SmartSwitch 6500 (using `ping`) to its end nodes. If you cannot ping, check physical connectivity (disconnected cable and so on).
2. Check IP routes and addresses.
 - Use the `show route` command to check the SmartSwitch 6500 route table.
 - Are the destination addresses correct for the specified gateways?
 - Are there any routing loops?
 - Are one or more of the destination addresses mapped to the wrong subnet?
 - Use `show client` (ARP server is on SmartSwitch 6500) to check the local client.
 - Does the client have the correct IP address?
 - Is the subnet correct? Is the ATM address correct?
 - Is the server type correct?
 - Check end node configurations.
 - Are end nodes configured correctly?
3. Check ARP statistics.
 - Use `show ipatmarp` (if the ARP server is on the SmartSwitch 6500).
 - Are there entries in the table?
 - Are the ATM addresses correct?
 - Use `show clientarp` (ARP server is not on SmartSwitch 6500) to check local client's ARP Table.
 - Are there entries in the table? If not, recheck client and end node configuration.
 - Are the ATM addresses correct?
4. Check ILMI, UNI routes, and PVCs (if applicable).
 - If using SVCs, use `show ATMRoute` to check whether static UNI routes are correct and whether dynamic UNI routes are established and correct. If dynamic routes are incorrect or missing, try creating static routes instead.
 - If using PVCs, use `show pvc` to check if PVCs connect the correct resources through the correct ports.
 - If using PVCs, use `show ipatmpvc` to check if local switch clients are mapped to the correct end node IP addresses.

5. If working through these questions does not solve the problem, contact Cabletron Systems Customer Service. (See Appendix C, "Technical Support").

9.2 TROUBLESHOOTING LAN EMULATION

You have configured an Emulated LAN and your network applications are not working. Use these questions and tests to help determine the cause of the problem.

1. Check for connectivity. Try pinging between end nodes. Ping from the SmartSwitch 6500 (using `ping`) to its end nodes. If you cannot ping, check physical connectivity (disconnected cable and so on).
2. Execute the `show lecs` command on the switch that contains the LECS. If the LECS is down, start it by executing the `start lecs` command.
 - If running distributed LANE services (LECS on one switch and LES and BUS on another switch) execute the `show les` command on the switch running the LES and BUS. If the LES and BUS are down, start the LES and BUS by executing the `start les` command.
3. Check IP routes and addresses.
 - Use `show route` command to check the SmartSwitch 6500 route table.
 - Are the destination addresses correct for the specified gateways?
 - Are there any routing loops?
 - Are one or more of the destination addresses mapped to the wrong subnet?
 - Use `show client` to check the SmartSwitch 6500 local ELAN client.
 - Does the client have the correct IP address?
 - Is the subnet correct?
 - Is the ATM address correct?
 - Is the server type correct?
 - Check end nodes configurations.
 - Are end nodes configured correctly?
4. If the ELAN spans multiple switches, check the following:
 - Is the LECS address correct on all switches?
 - Can all switches reach the switch providing LECS support?
 - If using the Well Known LECS Address, are all switches correctly mapped?
5. Check the LECS database.
 - Use `show lecselan` to check the names and numbers of ELANs.
 - Are ELAN names correct?
 - Is the ATM address of the LES correct?
6. Check whether LES is connected.
 - Use `show lescient` to check whether devices are registered with the LES. If clients are registered, check end node configuration. If not registered, check multi-point signaling.
 - Use `set leselan` to turn off multi-point signaling on a per-ELAN basis.

- Do devices begin to register with the LES and BUS once multi-point signaling is turned off?
7. Check whether BUS is connected.
 - Use `show busclient` to check whether devices are registered with the BUS. If clients are registered, check end node configuration. If not registered, check multi-point signaling.
 - Use `set leselan` to turn off multi-point signaling on a per-ELAN basis.
 - Do devices begin to register with the LES and BUS once multi-point signaling is turned off?
 - Check IISP routes to the switch containing the LES and BUS.
 - Are all IISP routes correct?
 - Does a new IISP route need to be added so devices can reach the LES and BUS?
 8. If working through these questions does not solve the problem, contact Cabletron Systems Customer Service. (see Appendix C, "Technical Support").

9.3 TROUBLESHOOTING PNNI LINKS

You have physically connected another company's ATM switch with your SmartSwitch 6500. Each switch supports PNNI, but there is no connectivity between the two devices. When dealing with PNNI connectivity, two possible configurations must be considered:

- The SmartSwitch 6500 and the other switch are in the same peer group
- The SmartSwitch 6500 and the other switch are in different peer groups

Use the following procedures to diagnose and resolve PNNI connectivity problems.

9.3.1 Switches in Same Peer Group

1. Check the physical connection. Make sure that the switches are connected correctly.
2. Check that both switches are in the same peer group. On the SmartSwitch 6500, enter the `show pnninode` command to view the peer group ID. If not the same peer group, perform the following:
 - Set the peer group ID on either switch to match the other. On the SmartSwitch 6500, use the `set pnnipeergroup` command to change the peer group ID.
3. Check the signalling type of each switch. If either switch does not show PNNI as the signaling type on the connecting port. Perform the following:
 - Turn off ILMI and manually set the signaling type to PNNI. On the SmartSwitch 6500, enter the `show portconfig` command to view signaling type for all ports. If necessary, use the `set portconfig` command to turn off ILMI and manually set signaling to `pnni10`.
4. If none of the above actions have corrected the problem, contact Cabletron Systems Customer Service (see Appendix C, "Technical Support").

9.3.2 Switches in Different Peer Groups

1. Check the physical connection between the peer groups. Make sure that the switches are connected correctly.

2. Make certain that the switches in the other peer group support multi-level PGLs and border nodes. If not, the other switches must be placed in the same peer group as the SmartSwitch 6500 if you want them to connect.
3. Are the switches within the peer groups communicating with each other? If not, fix the connectivity problem within the peer group (see Section 9.3.1).
4. Has the Peer Group Leader (PGL) been elected in both groups? If not, start the election process. On the SmartSwitch 6500 use the `set pnniplgelection` command to start the PGL election process.
5. Do both peer groups have a parent node (grandparent node, great grandparent, etc.) in a common peer group?
 - If not, create a parent node within a higher-level peer group that's common to both peer groups. On the SmartSwitch 6500, use the `add pnninode` command to create the parent node.
 - If they do, contact Cabletron Systems Customer Service (see Appendix C, "Technical Support")

9.4 TROUBLESHOOTING CONGESTION

If the bandwidth of your SmartSwitch 6500 begins to decrease, and if connections are being lost or packets are being dropped at a high rate, it's possible that your switch is becoming congested. Congestion can occur on the port level, the global switch level, or both levels.

If you suspect that your SmartSwitch 6500 is experiencing congestion, follow the steps outlined below to diagnose and resolve the cause of congestion.

9.4.1 Diagnosing Congestion

1. Enter the `show portstats` command, and take the default of (a11).
2. If cells are being dropped only on specific ports, proceed to the "Port Congestion" section.
3. If cells are being dropped on all ports, the indication is global congestion. Proceed to the "Global Congestion" section.

9.4.2 Global Congestion

1. Is the total cell drop rate equal to the Unknown VC cell drop rate?
 - If yes, the switch is improperly set up. Check the switch configuration.
 - If no, this indicates global congestion. Continue.
2. Set the `porttrafficcongestion` values to those recommended in the table below.

Table 9-1 Settings for Class of Service Queues

Service Class	Recommended Settings
CBR	Fewer than 100 connections on a port: Min = 64, Max = 1024
CBR	More than 100 connections on a port: Min = 128, Max = 1024

Table 9-1 Settings for Class of Service Queues (Continued)

Service Class	Recommended Settings
rt-VBR	Bandwidth* utilization less than 20%: Min = 16, Max = 1024
rt-VBR	Bandwidth* utilization greater than 20%: Min = 128, Max = 4096
Nrt-VBR	Min = 256, Max = 4096
UBR	Min = 256, Max = 8192
ABR	Min = 256, Max = 8192

*Use the `show portconfig` command to view bandwidth utilization

3. Has the congestion subsided?
 - If yes, you are done.
 - If no, continue.
4. Have you changed the EPD threshold (`set switchtrafficcongestion` command)?
 - If yes, replace it to the default setting. If congestion subsides, you are done.
 - If no, continue.
5. Enter the `show cacinfo` and `show portconfig` commands for each port. Is the allocated bandwidth small and is the traffic mostly UBR?
 - If no, go back to step 4 and check next port.
 - If yes, continue.
6. Enter the `show porttrafficcongestion` command. Is the UBR queue `MaxValue` large?
 - If no, go back to step 4.
 - If yes, continue.
7. Reduce the UBR queue `MaxValue` by a small amount, then wait a few minutes.
8. Enter the `show portstats` command, and take the default of `all`. Is the number of cells dropped increasing for this port, and quickly decreasing for all other ports?
 - If yes, proceed to the “Port Congestion” section.
 - If no, continue.
9. Is the number of cells being dropped by all other ports decreasing somewhat?
 - If no, go back to step 6.
 - If yes, continue.
10. Enter the `set caceqbwallocscheme` command and set call admission control for this port to a more conservative policy (`moderate` or `conservative`).
11. Go back to step 4 until all ports have been checked.

9.4.3 Port Congestion

1. Enter the `show portstats` command a few times, noting the value for cells dropped and unknown VCs dropped. Is the number of cells dropped equal to the number of VCs dropped?

- If yes, the switch is improperly set up. Check the switch configuration.
 - If no, this indicates port congestion. Continue.
2. Enter the `show cacinfo` command for this port. Note the bandwidth allocated for each Quality of Service on this port.
 3. For each class of service, enter the `set porttrafficcongestion` command. Set the `MaxValue` to the value recommended in Table 9-1, “Setting for Class of Service Queues.”
 4. Have you performed step 3 for every class of service for this port?
 - If no, go to step 3.
 - If yes, continue.
 5. Enter the `set caceqbwallocscheme` command for this port. Set call admission control for this port to a more conservative policy (`moderate` or `conservative`).
 6. Check VC statistics for this port using either the `show pvc /d` or `show svc /d` command, whichever is appropriate. If the port belongs to the high virtual channel link (VCL), read the forward statistics. If the port belongs to the low VCL, read the backward statistics. If the port belongs to both high and low VCLs, read both statistics.
 7. Is the number of cells received increasing?
 - If no, go through step 6 a few more times. If cells received still do not increase and congestion persists, contact Cabletron Customer support.
 - If yes, continue.
 - Enter the `show cacinfo` command for this port. Is the Allocated Bandwidth less than the Cell Reception Rate obtained from `show pvc /d` or `show svc /d` in step 6?
 - If no, go through step 6 a few more times. If cells received still do not increase and congestion persists, contact Cabletron Customer support.
 - If yes, this VC is misbehaving. Take appropriate action, for example, terminate the VC.

9.5 EVENTS AND ALARMS

The SmartSwitch 6500 switch records and reports its operation in real-time through the use of events and alarms. An event is an occurrence of a significant activity. For instance, a port going down or a client joining an ELAN are examples of events. Alarms are a specific class of events defined as “events that the user needs to know about or attend to immediately.” Alarms do not always indicate switch faults. Alarms may also be informational events. For instance, “LECS Operational” is an example of an alarm that is not a switch fault, but is an activity that the user should know about immediately.

9.5.1 Event Categories

Events are grouped into the following categories:

- Critical — Impacts the entire switch, leaving the system unavailable or in a degraded state
- Major — Impacts a feature of the switch, leaving the feature unavailable or in a degraded state
- Minor — Impacts the system or feature, leaving it in a sub-optimal state
- Informational — An occurrence of an activity that the user should know about

Both events and alarms are stored within circular memory buffers. When the buffers become full, older events and alarms are overwritten by newer entries. Both events and alarms are stored in shared RAM. However, the 40 most recent alarms are also stored in flash RAM. Storing these 40 alarms in flash RAM makes them persistent between reboots of the SmartSwitch 6500, and provides information about the state of the switch prior to reboot.



Note Alarms are collected and stored in flash RAM in groups of four. As a result, some of the most recent alarms may not be persistent. For example, there are 24 (6 times 4) alarms stored in flash RAM. If a 25th alarm occurs, and the switch is rebooted, only the 24 alarms are persistent. The 25th alarm is dropped because the number of alarms (after 24) did not reach the next multiple of four (28).

9.5.2 Viewing Events and Alarms

Use the `show events` command to view a list of the currently logged events. For example,

```
Smart6500 # show events
Index(ALL)                                     :
0  33554474  MAJOR EVENT           000:00:04:311
-----
LES ReadServerConfig: Unable to open config file les.db

1  33554653  INFO EVENT             000:00:04:320
-----
LECS Database non existing - creating default ELAN

2  117571585  MINOR EVENT            000:00:07:341
-----
SAAL connection has become active, initiated locally
Port ID 0x01c41000
Protocol 0x02

3  117571585  MINOR EVENT            000:00:07:585
-----
SAAL connection has become active, initiated locally

More(<space>/q)?:
```

Events are displayed in the following format:

- Event number — The index number of the event in the circular buffer
- Event ID — A unique ID assigned to the event
- Category — Whether this event is critical, major, minor, or informational
- Time — Time of event, in switch up-time in hours, minutes, seconds, and milliseconds
- Object — The object affected by the event (port, LEC, and so on)
- Description — Brief message describing the event

Event messages can be automatically displayed on the SmartSwitch 6500 console. Use the `set eventdisplay` command to display events on the console as they occur:

```
Smart6500 # set eventdisplay
EventDisplay(OFF)                               : on
Smart6500 #
```



Note Depending on the activity of your SmartSwitch 6500, the appearance of events on the SmartSwitch 6500 may be too frequent to use the SmartSwitch 6500 console comfortably. It is recommended that you turn on the automatic display of events only when troubleshooting.

Use the **show alarms** command to view a list of the currently logged alarms. For example,

```
Smart6500 # show alarms
Index(ALL)                                     :
0  33554702  000:07:05:300
-----
pvcm_cac_admit: failed  501037

1  33554652  023:56:23:317
-----
LECS Operational

2  117506049  024:01:54:083
-----
Failed to re-establish SAAL connection
Port ID 0x01c81000
T309    10000

3  117506049  024:01:54:430
-----

More(<space>/q)?:
```

Alarms are displayed in the following format:

- Alarm number — The index number of the alarm in the circular buffer
- Alarm ID — A unique ID assigned to the alarm
- Time — Time of alarm, in switch up-time in hours, minutes, seconds, and milliseconds
- Object — The object affected by the alarm (port, LEC, and so on)

Alarm messages can be automatically displayed on the SmartSwitch 6500 console. Use the **set alarmdisplay** command to display alarms on the console as they occur:

```
Smart6500 # set alarmdisplay
alarmDisplay(OFF)                               : on
Smart6500 #
```

9.5.3 Deleting Events and Alarms

To delete events or alarms currently logged within your SmartSwitch 6500, use the **delete events** and **delete alarms** commands, respectively.

9.6 SAVING CORE DUMPS

The SmartSwitch 6500 core dump feature allows you to specify a local Ethernet host where, in the event of a system failure, the SmartSwitch 6500 sends a copy of its memory. SmartSwitch 6500 system memory is saved to two files, one containing CPU memory (`core_cpu`), the other common memory (`core_cmn`). These files can then be sent to Cabletron customer support for analysis.



Note To use the core dump feature, the local Ethernet host must be running TFTP server software, and you must have write access to the TFTP directory.

Enter the `set coredump` command to enable the core dump feature. For example,

```
Smart6500 # set coredump
EnableCoreDump(n)           : y                < "y" to enable core dump feature
ServerIP()                   : 204.95.77.240   < IP address of my TFTP server
CoreDumpFile()               : /tftpboot/bobr/core < full path name for core dump files
userName()                   : bobr            < login name on the server
UserPassword()               :                 < password
Smart6500 #
```



Note The `set coredump` command uses FTP to create the `core_cpu` and `core_cmn` files. If your server does not run FTP, create these files manually. Then execute the `set coredump` command.



Note On UNIX systems, make sure that the permissions are set correctly so that data can be written.



Note For security, the `set coredump` command retains your password only long enough to create the core dump files. Your password is then dropped from system memory.

To see the current core dump configuration, enter the `show coredump` command.

```
Smart6500 # show coredump

Core Dump Enabled   : Yes
Core Dump Server IP : 204.95.77.240
Core Dump File      : /tftpboot/bobr/core

Smart6500 #
```

If a system failure occurs while the core dump feature is enabled, the SmartSwitch 6500 console appears similar to the example below. The SmartSwitch 6500 then begins sending images of its memory to the core dump files on the TFTP server.

```

Illegal access. Bus Error.
IP: e0103288   PFP: e04be080
r0(pfp): e04be040      r1(sp): e04be0c0      r2(rip): e00dd7dc
r3      : 00000000      r4      : e00f8f0c      r5      : e0409f10
r6      : 00000003      r7      : e00f8f0c      r8      : e0409f40
r9      : 00000003      r10     : 00000030      r11     : e00f8f0f
r12     : 00000008      r13     : 00000001      r14     : e00d22f0
r15     : 00000008
d2000000: Core Dump
Common DRAM dumped to /tftpboot/bobr/core_cmn
CPU DRAM dumped to /tftpboot/bobr/core_cpu
ffffffff ffffffff ffffffff ffffffff *.....*
d2000010: ffffffff ffffffff ffffffff ffffffff *.....*
d2000020: ffffffff ffffffff ffffffff ffffffff *.....*
d2000030: ffffffff ffffffff ffffffff ffffffff *.....*
d2000040: ffffffff ffffffff ffffffff ffffffff *.....*
d2000050: ffffffff ffffffff ffffffff ffffffff *.....*
d2000060: ffffffff ffffffff ffffffff ffffffff *.....*
d2000070: ffffffff ffffffff ffffffff ffffffff *.....*
d2000080: ffffffff ffffffff ffffffff ffffffff *.....*
d2000090: ffff
SmartSwitch 6500 Start-up Code
Cabletron Systems Inc.

```

Copy the information displayed on the console and send it to your Cabletron customer support representative along with the core dump files. (See Appendix C, "Technical Support")

APPENDIX A SPECIFICATIONS

This appendix lists the technical specifications for the SmartSwitch 6500 switch.

Table A-1 Hardware Specifications

Specification	Value
Processor	i960HD, 66 MHz
Switching engine	10 Gbps, non-blocking
Max I/O ports*	Up to 63 OC-3, DS-3, or E3 — Up to 15 OC-12
Port-to-port latency	11 microseconds
CPU DRAM memory	128 MB
Buffer memory (cells)	512 K
Flash memory	16 MB
Serial port	RS-232c compliant; RJ-45 connector
Ethernet port	IEEE 802.3 compliant; RJ-45 connector

*On TSM/CPU modules, ports 7b4 and 8b4 are reserved for the CPU, and can not support connections

Table A-2 Physical Specifications

Specification	Value
Dimensions chassis	62.2 cm H x 43.3 cm W x 35.6 cm D 24.5" H x 17.3" W x 14" D
Dimension (CSM, TSM)	41.9 cm H x 3.1 cm W x 28.6 cm D 16.5" H x 1.2" W x 11.25" D
Weight (empty chassis)	13.6 kg (30 lbs)
Weight (CSM, TSM)	2.3 kg (5 lbs)
Approx. power requirements (5V)	TSM + two OC3 I/O modules = 12 Amps CPU module = 2 Amps CSM = 8 Amps

Table A-2 Physical Specifications (Continued)

Specification	Value
Operating temperature	5 to +40 C (41 to 104 F)
Operating humidity	5% to 90% RH, non-condensing

Table A-3 ATM Port Specifications

Media	Port Speed	Framing	Connector	Max. Tx Power	Min. Tx power	Max. Rx power	Min. Rx power	Range
SMF-IR	155 Mbps	STS-3c or STM-1	SC	-8 dBm	-15 dBm	-8 dBm	-31 dBm	15 Km
SMF-IR	622 Mbps	STS-12c or STM-4	SC	-8 dBm	-15 dBm	-7 dBm	-28 dBm	15 Km
SMF-LR	155 Mbps	STS-3c or STM-1	SC	0 dBm	-5 dBm	-8 dBm	-34 dBm	50 Km
SMF-LR	622 Mbps	STS-12c or STM-4	SC	+2 dBm	-3 dBm	-7 dBm	-28 dBm	45 Km
MMF	155 Mbps	STS-3 or STM-1	SC	-14 dBm	-19 dBm	-14 dBm	-31 dBm	2 Km
MMF	622 Mbps	STS-12c or STM-4	SC	-14 dBm	-20 dBm	-14 dBm	-26 dBm	500 m
Cat. 5 UTP	155 Mbps	STS-3c or STM-1	RJ-45	--	--	--	--	100 m
75 ohm coax	44.7 Mbps	DS-3 nonchannelized	BNC, female	n/a	n/a	n/a	n/a	150 m to DSX
75 ohm coax	34.3 Mbps	E-3 nonchannelized	BNC, female	n/a	n/a	n/a	n/a	150 m to DSX

Table A-4 Protocols Standards and Specifications

Protocol	Standard
Signaling	ATM Forum UNI 3.0 ATM Forum UNI 3.1 ATM Forum UNI 4.0 ATM Forum ILMI 4.0

Table A-4 Protocols Standards and Specifications (Continued)

Protocol	Standard
ATM routing protocols	IISP PNNI 1.0 (including PGL and border node support) UNI
LAN protocols	ATM Forum LANE 1.0 (Ethernet and Token Ring) IETF RFC 1577 Classical IP over ATM LUNI 2.0

Table A-5 Management Standards and Specifications

Management Protocol	Supported MIBs
SNMPv2c See Appendix B, "Agent Support."	MIB II (RFC 1213) Interface Table MIB (RFC 1573) AToM MIB (RFC 1695) AToM2 MIB (pre-standard) LANE MIB (ATM Forum) ILMI 4.0 MIB (ATM Forum) IP over ATM MIB (pre-standard) PNNI MIB SmartSwitch 6500 MIBs (proprietary)

Table A-6 RJ-45 to DB-9 Adapter (PC Serial Port Adapter)

RJ-45 Pin	RJ-45 Color	DB-9 Pin	DB-9 Description
1	Blue	2	Receive
4	Red	3	Transmit
5	Green	5	Ground

APPENDIX B AGENT SUPPORT

This appendix briefly describes the support provided for managing the SmartSwitch 6500 using Simple Network Management Protocol (SNMP).

B.1 MIB, SMI, MIB FILES AND INTERNET MIB HIERARCHY

A MIB (Management Information Base) is the term used to represent a virtual store of management data on a device. Given the structure of management data, it can be operated upon (retrieved, created or modified) using the SNMP protocol. The structure of that data is defined using a subset of a notation called Abstract Syntax Notation (ASN.1). This subset is called SMI (Structure of Management Information). A file containing the definition of that structure is called a MIB file. To provide for a uniform naming convention for all MIBs, from all vendors, for all kinds of data, a standard format is used. This format is a hierarchy and is termed the Internet MIB Hierarchy.

The MIB structure is logically represented by a tree hierarchy (see Figure B-1). The root of the tree is unnamed and splits into three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.

These branches and those that fall below each category have short text strings and integers to identify them. Text strings describe object names, while integers allow computer software to create compact, encoded representations of the names. For example, the ZeitNet MIB variable znIpAtmClient is an object name and is also represented by the number one.

An object identifier in the Internet MIB hierarchy is the sequence of numeric labels on the nodes along a path from the root to the object. The object for the Internet Standard for MIB II is represented by the object identifier 1.3.6.1.2.1. It also can be expressed as iso.org.dod.internet.mgmt.mib (see Figure B-1).



Note For the authoritative reference on the concepts described in this section, refer to RFCs 1901 through 1908.

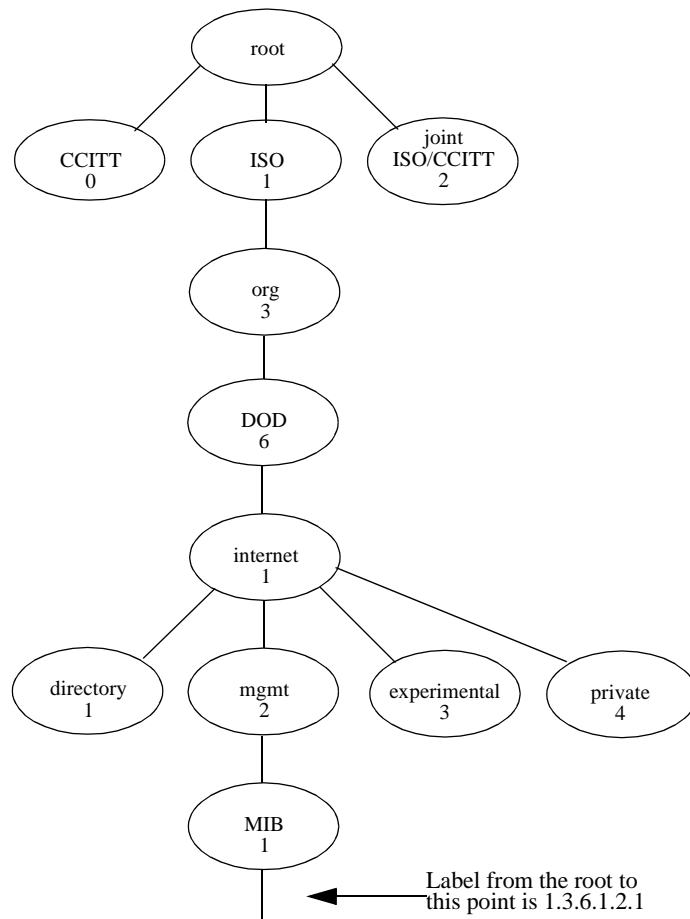


Figure B-1 Internet MIB hierarchy

B.1.1 ZeitNet Cabletron Proprietary MIBs

The location of some of ZeitNet proprietary MIBs in the Internet hierarchy is shown in Figure B-2. All nodes starting with “zn” represent Zeitnet objects.

The private ZeitNet MIB is represented by the object identifier 1.3.6.1.4.1.1295, or iso.org.dod.internet.private.enterprise.zeitnet. The ZeitNet proprietary MIBs include the subtrees shown in Figure B-2.

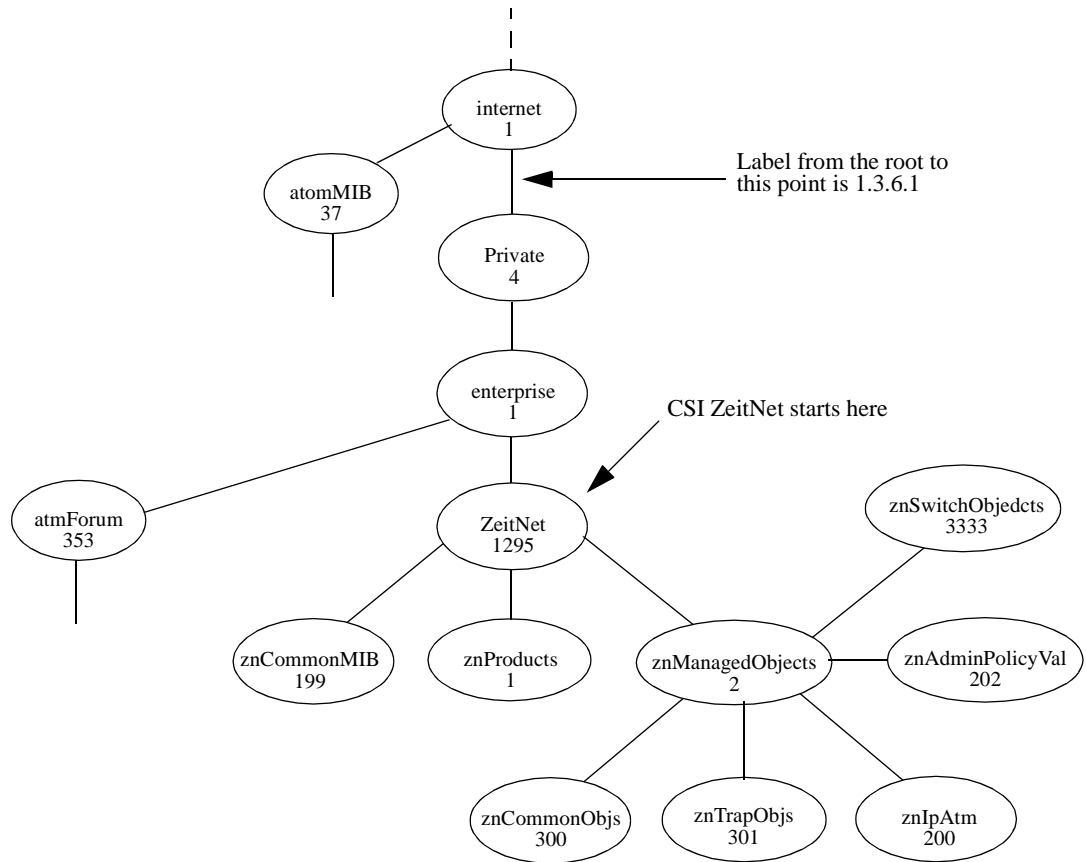


Figure B-2 CSI ZeitNet Private MIBs

In Figure B-2, the ZeitNet proprietary group is identified by 1.3.6.1.4.1.1295; its subgroup, called znProducts, is identified by 1; and the first variable is znManagedObjects with a value of 2. Therefore, the object znManagedObjects has an object identifier of 1.3.6.1.4.1.1295.2.

B.1.2 Relation Between Object Identifier and the Represented Value

In Figure B-3, the znLec object (representing LAN Emulation Client information) has an Object Identifier of 1.3.6.1.4.1.1295.2.3333.9.1.1. The znLecDDCount object representing the number of Data direct connections maintained by one LEC (Lan Emulation Client) has an object identifier of 1.3.6.1.4.1.1295.2.3333.9.1.1.1. Querying for the value represented by this object identifier (using the SNMP protocol), returns the actual number of data direct connections for the identified LEC.

:

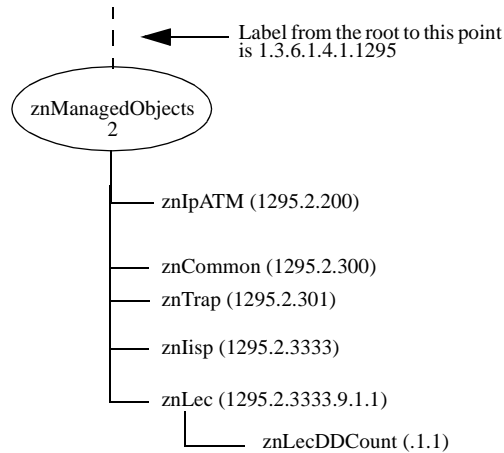


Figure B-3 Cabletron SmartSwitch 6500 object identifier example

B.1.3 Supported protocols

The SmartSwitch 6500 supports Simple Network Management Protocol (SNMP). Both the SNMPv1 and SNMPv2c formats of the protocol are supported.

B.1.4 Supported SMI Formats

Zeitnet proprietary MIBs are defined using SNMPv2c format of the SMI.

B.1.5 Zeitnet Cabletron Proprietary MIB Groups

The following table of Zeitnet proprietary MIB groups lists group name, object identifier, and group function.

Table B-1 Zeitnet proprietary MIB groupings

Name	Object Identifier	Function
zeitnet	1.3.6.1.4.1.1295	All Zeitnet Proprietary Objects
znProducts	1.3.6.1.4.1.1295.1	ZeitNet product specific
znManagedObjects	1.3.6.1.4.1.1295.2	Various classes of Managed entities
znIpAtm	1.3.6.1.4.1.1295.2.200	IP ATM services
znIpAtmClient	1.3.6.1.4.1.1295.2.200.1	IP ATM Client Services

Table B-1 Zeitnet proprietary MIB groupings (Continued)

Name	Object Identifier	Function
znIpAtmServer	1.3.6.1.4.1.1295.2.200.2	IP ATM Server Services
znCommonObjs	1.3.6.1.4.1.1295.2.300	Zeitnet Specific Information
znTrapObjs	1.3.6.1.4.1.1295.2.301	ZeitNet Traps
znSwitchObjects	1.3.6.1.4.1.1295.2.3333	Switch/hardware specific information
znSystem	1.3.6.1.4.1.1295.2.3333.1	Hardware and software system level information
znSwitchDiscoveryTable	1.3.6.1.4.1.1295.2.3333.1.34	Neighbor switch configuration
znConfig	1.3.6.1.4.1.1295.2.3333.2	Switch software configuration management.
znModule	1.3.6.1.4.1.1295.2.3333.3	Switch Module information.
znPort	1.3.6.1.4.1.1295.2.3333.4	Switch Port Information.
znPortTrafficCongTable	1.3.6.1.4.1.1295.2.3333.4.3	Traffic management
znSignalling	1.3.6.1.4.1.1295.2.3333.5	Signalling timer information
znSar	1.3.6.1.4.1.1295.2.3333.8	SAR specific information.
znVlan	1.3.6.1.4.1.1295.2.3333.9	Zeitnet Lane Services Group
znLanEmulation	1.3.6.1.4.1.1295.2.3333.9.1	Zeitnet LAN Emulation Group
znLec	1.3.6.1.4.1.1295.2.3333.9.1.1	LAN Emulation Client Specific
znLes	1.3.6.1.4.1.1295.2.3333.9.1.2	Lan Emulation Server Specific
znBus	1.3.6.1.4.1.1295.2.3333.9.1.3	Broadcast and Unknown Server information.
znLecs	1.3.6.1.4.1.1295.2.3333.9.1.4	Lan Emulation Configuration Server Info
znSSCOP	1.3.6.1.4.1.1295.2.3333.12	SSCOP Configuration
znEventTable	1.3.6.1.4.1.1295.2.3333.13.2	Event table
znEventAlarmTable	1.3.6.1.4.1.1295.2.3333.13.5	Alarm table
znTrafficDescrExtTable	1.3.6.1.4.1.1295.2.300.13	Proprietary extensions to atmTrafficDescrParamTable
znCacStats	1.3.6.1.4.1.1295.2.3333.4.5	CAC Statistics Group
znSwitchHW	1.3.6.1.4.1.1295.2.3333.14	Hardware Characteristics of the Switch Group
znSlotTable	1.3.6.1.4.1.1295.2.3333.14.4	Table of I/O Slots
znCpuPortTable	1.3.6.1.4.1.1295.2.3333.14.13	Table of CPU Ports
znIOModuleTable	1.3.6.1.4.1.1295.2.3333.14.15	Table of I/O Modules
znPortExtTable	1.3.6.1.4.1.1295.2.3333.14.10	Extensions to znPortTable

B.1.6 SmartSwitch 6500 MIB Support

The SmartSwitch 6500 is shipped with the following MIBs:

- MIB II (RFC 1213)
- Interface Table MIB (RFC 1573)
- AToM MIB (RFC 1695)
- AToM2 MIB (pre-standard)
- LANE MIB (ATM Forum)
- ILMI 4.0 MIB (ATM Forum)
- PNNI MIB (ATM Forum)
- IP over ATM MIB (pre-standard)
- SmartSwitch 6500 Switch MIBs (proprietary)



Note Along with the MIBs, the CD-ROM also contains a README file and the release note.

B.1.7 MIB Exceptions

With the current implementation of MIB files, conformance to ATM standards for the SmartSwitch 6500 ATM switch includes the following exceptions.

Non-Conformance

- atmInterfaceIlmiVpi — Read-only
- atmInterfaceIlmiVci — Read-only
- aal5VccTable — Not supported
- atmSvcVcCrossConnectRowStatus Set — Not supported
- atmConfigSigType — The values given below are not supported:
 - ituDss2
 - atmfBici2Dot0
- znIpAtmClientDDVcType — Accepts only pvc(2) in sets
- lecMulticastSendType — Accepts only best effort (1)
- lecMulticastSendAvgRate — Accepts values only up to 370370
- lecMulticastSendPeakRate — Accepts values only up to 370370
- leArpEntryType — Accepts only staticVolatile (4) and staticNonVolatile (5)
- lesControlTimeout — Read-only
- atmTrafficDescrParamIndexNext — Not supported
- atmVplCastType — The values given below are not supported:
 - p2mpRoot

- p2mpLeaf
- atmVplReceiveTrafficDescrIndex — Doesn't accept ABR traffic descriptor
- atmVplTransmitTrafficDescrIndex — Doesn't accept ABR traffic descriptor

Not Supported

The following MIB objects are not supported. If used, these objects return either the value zero or the message, "Not supported."

- atmInterfaceDs3PlcpTable
- atmInterfaceTCTable
- atmSvcVpCrossConnectTable
- atmSigSupportTable
- atmSigDescrParamTable
- atmIfAdminAddrTable
- atmVclAddrBindTable
- atmAddrVclTable
- atmVclGenTable
- atmfMyOsiNmNsapAddress
- lecRouteDescrTable
- leRDArpTable

B.2 MANAGING THE SMARTSWITCH 6500

Your SmartSwitch 6500 must be IP reachable by the NMS before it can be managed. The default connection between the SmartSwitch 6500 and the NMS is the SmartSwitch 6500 Ethernet interface. Use the `show switchconfig` command to find the IP address of the SmartSwitch 6500. An NMS can use this IP address to reach the SmartSwitch 6500 through Ethernet. An NMS can also manage the SmartSwitch 6500 through one of its ATM ports if the SmartSwitch 6500 has a client connection into a VLAN or emulated LAN.

Note that the SmartSwitch 6500 itself, is not reachable through ATM until a client for the switch is created and participates as a member of a VLAN or ELAN. Your NMS uses that switch client's address to access and manage the switch.

To create a client for the switch, use the `add ipatmclient` command for VLANs and `add laneclient` for emulated LANs.

Use the `set mynmaddr` command to tell the SmartSwitch 6500 which interface to use when communicating with your NMS. For detailed information about these commands, see the SmartSwitch 6500 Reference Manual.

B.2.1 Console Commands that Affect the Agent

The following is a list of the console commands that affect the operation of the SmartSwitch 6500 SNMP agent. For detailed descriptions of these commands, see the SmartSwitch 6500 Reference Manual.

- Community: Sets the community strings for the SmartSwitch 6500

- `TrapCommunity`: Specifies the NMS to which traps are sent
- `MyNMAddr`: Specifies the IP address through which the switch is managed
- `TrustedNMS`: Specifies the IP address of the NMS allowed to perform the following commands:
 - `update firmware`
 - `backup`
 - `restore`
 - `reboot`

B.2.2 Default Community Strings

The following is a list of the default community strings used by the SmartSwitch 6500:

- `public` — Used for all standard SNMP communication
- `ILMI` — Used by ILMI channels between switches
- `zeitnet` — Used by the SmartSwitch ATM Administrator program



Caution If the community string *zeitnet* is changed on the SmartSwitch 6500 it must also be changed at the SmartSwitch ATM Administrator. Failure to do so, makes the SmartSwitch 6500 unreachable by the SmartSwitch ATM Administrator program.

APPENDIX C TECHNICAL SUPPORT

This appendix tells you what to do if you need technical support for your SmartSwitch 6500.

Cabletron offers several support and service programs that provide high-quality support to our customers. For technical support, first contact your place of purchase. If you need additional assistance, contact Cabletron Systems, Inc. There are several easy ways to reach Cabletron Customer Support and Service.

C.1 TELEPHONE ASSISTANCE

Our Technical Support Center is available Monday through Friday, 8am to 8pm Eastern Time, by calling 603-332-9400.

C.2 FAX SERVICE

You can fax support questions to us any time at 603-337-3075.

C.3 ELECTRONIC SERVICES

You can contact Cabletron's Bulletin Board Service by dialing 603-335-3358.

Our internet account can be reached at support@ctron.com.

You can also check our home pages on the World Wide Web.

- <http://www.Cabletron.com>
- <http://www.ctron.com>

C.4 PLACING A SUPPORT CALL

To expedite your inquiry, please provide the following information:

- Your Name
- Your Company Name
- Address
- Email Address
- Phone Number
- FAX Number
- Detailed description of the issue (including history, what you've tried, and conditions under which you see this occur)

- Hardware model number, software version, and switch configuration (that is, what part types are in what slots)

C.5 HARDWARE WARRANTY

Cabletron warrants its products against defects in the physical product for one year from the date of receipt by the end user (as shown by Proof of Purchase). A product that is determined to be defective should be returned to the place of purchase. For more detailed warranty information, please consult the Product Warranty Statement received with your product.

C.6 SOFTWARE WARRANTY

Cabletron software products carry a 90-day software warranty. During this period, customers may receive updates and patches for verified, reported software issues.

C.7 REPAIR SERVICES

Cabletron offers an out-of-warranty repair service for all our products at our Santa Clara Repair Facility. Products returned for repair will be repaired and returned within 5 working days. A product sent directly to Cabletron Systems, Inc. for repair must first be assigned a Return Material Authorization (RMA) number. A product sent to Cabletron Systems, Inc., without an RMA number displayed outside the box will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, contact the Cabletron Technical Support. When you call for an RMA number, your support representative will spend a few minutes with you, making sure the board is defective. Once they confirm the board is defective, they will assign an RMA number. Payment, shipping instructions, and turnaround time will be confirmed when the RMA number is assigned.

APPENDIX D ACRONYMS

A

AAL	ATM Adaptation Layer
AAL1	ATM Adaptation Layer Type 1
AAL2	ATM Adapter Layer Type 2
AAL3/4	ATM Adapter Layer Type 3/4
AAL5	ATM Adapter Layer Type 5
AALM	ATM Adaptation Layer Mux
ABR	Available Bit Rate
AFI	Authority and Format Identifier
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
AvCR	Available Cell Rate

B

BE	Bridged Ethernet
BER	Bit Error Ratio (Rate)
B-ICI	Broadband Inter-Carrier Interface
B-ISDN	Broadband Integrated Services Digital Network

BOOTP	Boot Protocol
BUS	Broadcast and Unknown Server

C

CAC	Call Admission Control
CAN	Campus Area Network
CAT-3	Category 3 unshielded twisted pair cable
CAT-5	Category 5 unshielded twisted pair cable
CBR	Constant Bit Rate
CCITT	Comite Consultatif Internationale de Telegraphique et Telephonique (Consultative Committee on International Telegraphy and Telephony)
CCR	Current Cell Rate
CDV	Cell Delay Variation
CER	Cell Error Ratio
CES	Circuit Emulation Service
CI	Congestion Indicator
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CMIP	Common Management Information Protocol
COM	Communication
COS	Class of Service
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRS	Cell Relay Service
CS	Convergence Sublayer
CTD	Cell Transfer Delay

D

DCC	Digital Cross Connect, generic DACS or Direct Connect Card, data interface module
DF	Download Flash
DS-0	Digital Signaling 0
DS-1	Digital Signaling 1
DS-3	Digital Signaling 3
DTE	Data Terminal Equipment
DTL	Designated Transit List
DVT	Delay Variation Tolerance

E

E-1	European standard for digital transmission service at 2 Mb/s.
E-3	European standard for digital transmission service at 34.4 Mb/s (transports 16 E1 circuits)
E-NET	Ethernet
EFCI	Explicit Forward Congestion Indicator
EISA	Extended Industry Standard Architecture
ELAN	Emulated Local Area Network
EMI	Electro-Magnetic Interference
ENR	Enterprise Network Roundtable
EOF	End of Frame
EPD	Early Packet Discard
EPROM	Erasable Programmable Read-Only Memory
ESD	Electro-Static Device
ESI	End System Identifier
ESM	Expansion Switch Module

F

FCS	Frame Check Sequence
FIFO	First In First Out
FTP	File Transfer Protocol

G

GB/S	Gigabits per second
GCAC	Generic Call Admission Control
GCRA	Generic Cell Rate Algorithm
GFC	Generic Flow Control

H

HEC	Header Error Check
------------	--------------------

I

IEEE	Institute of Electrical and Electronic Engineers
ICMP	Internet Control Message Protocol
ID	Identification Number
IE	Information Element
IETF	Internet Engineering Task Force
IISP	Interim Inter-Switch Signaling Protocol

Acronyms

ILMI	Integrated Local Management Interface
I/O	Input/Output
IOM	Input/Output Module
IP	Internet Protocol
IP/ATM	Internet Protocol over ATM
IPX	Internetwork Packet Exchange protocol
ITU-TSS	International Telecommunications Union-Telecommunications Standards Sector
ISDN	Integrated Service Digital Network

K

KB/S	Kilobits per second
-------------	---------------------

L

LAN	Local Area Network
LANE	LAN Emulation
LE	LAN Emulation
LE-ARP	LAN Emulation-Address Resolution Protocol
LEC	LANE Client
LECS	LAN Emulation Configuration Server
LECSELAN	LAN Emulation Configuration Server Emulated LAN
LES	LANE Server
LESELAN	LANE Server Emulated LAN
LIS	Logical IP Subnetwork
LLC	Logical Link Control

LMI Local Management Interface

M

MAC Media Access Control

MAN Metropolitan Area Network

Mb/S Megabits per second

MBS Maximum Burst Size

MCR Minimum Cell Rate

MIB Management Information Base

MMF Multi-Mode Fiber

MP Multi-Point

MSM Main Switch Module

MTU Maximum Transfer Unit

N

NAKS Negative Acknowledges

NDIS Network Driver Interface Specification

NETBEUI NetBIOS Extension User Interface

NFS Network File System

NIC Network Interface Controller/Card

NLS Natural Language Syntax

NMS Network Management System

NNI	Network Node Interface or Network-to-Network Interface
NRT-VBR	Non Real Time - Variable Bit Rate
NRZ	Non-Return to Zero
NSAP	Network Services Access Point

O

OAM	Operations and Maintenance
OAM&P	Operations, Administration, Maintenance and Provisioning
OC-1	Optical Carrier 1
OC-N	Optical Carrier n (where "n" is an integer)
ODI	Open Data-link Interface
OOB	Out of Band
OSI	Open Systems Interconnection

P

PC	Personal Computer
PC	Priority Control
PCI	Peripheral Component Interconnect
PCR	Peak Cell Rate
PDU	Protocol Data Unit
PGL	Peer Group Leader
PMD	Physical Media Dependent Sub-layer
PMP	Point-to-Multipoint
PNNI	Private Network Node Interface or Private Network-to-Network Interface

PPD	Partial Packet Discard
PROM	Programmable Read-Only Memory
PTI	Payload Type Indicator
PTP	Point-to-Point
PTSE	PNNI Topology State Element
PTSE	PNNI Topology State Packet
PVC	Permanent or Provisioned Virtual Circuit

Q

QOS	Quality of Service
QSAAL	Q-Signaling ATM Adaptation Layer. (Q represents the Q-series of the ITU-T (International Telecommunications Union)).

R

R	Read-Only Access
RAM	Random Access Memory
RCC	Routing Control Channel
RCR	Raw Cell Received
RD	Receive Deactivated
RFC	Request for Comment
RM	Resource Management
RMA	Return Merchandise Authorization
RQU	Receive Queue Underrun
RS-#	Recommended Standard defined by Electronic Industries Association
RT-VBR	Real Time - Variable Bit Rate

RW Read-Write Access

S

SAAL Signaling ATM Adaptation Layer

SAR Segmentation And Reassembly

SAR-PDU SAR Protocol Data Unit

SBE System Bus Error

SCR Sustainable Cell Rate

SDH Synchronous Digital Hierarchy

SEAL Simple Efficient Adaptation Layer

SMF Single Mode Fiber

SMDS Switched Multimegabit Data Service

SNMP Simple Network Management Protocol

SONET Synchronous Optical Network

STM-1 Synchronous Transport Module 1

STM-N Synchronous Transport Module n (where 'n' is an integer)

STM-NC Synchronous Transport Module n - concatenated (where 'n' is an integer)

STP Shielded Twisted Pair

STS-1 Synchronous Transport Signal 1

STS-N Synchronous Transport Signal n (where 'n' is an integer)

STS-NC Synchronous Transport Signal n - concatenated (where 'n' is an integer)

SVC Switched Virtual Circuit

SVCC Switched Virtual Channel Connection

T

T-1	Transmission System 1
T-3	Transmission System 3
TAXI	Transparent Asynchronous Transmitter/Receiver Interface
TCP	Transmission Control Protocol
TD	Traffic Descriptor
TDM	Time-Division Multiplexing
TFTP	Trivial File Transfer Protocol
TLV	Type, Length and Value

U

UBR	Unspecified Bit Rate
UME	UNI Management Entity
UNI	User-Network Interface
UP	Unnumbered Poll
UPC	Usage Parameter Control
UTOPIA	Universal Test and Operations Physical Interface for ATM
UTP	Unshielded Twisted Pair

V

VBR/RT	Variable Bit Rate/Real Time
VBR/NRT	Variable Bit Rate/Non-real Time
VC	Virtual Circuit

Acronyms

VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VLAN	Virtual LAN
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VT	Virtual Tributary

W

WAN	Wide Area Network
------------	-------------------

INDEX

Symbols

? 2-24

Numerics

6A-CSM512 2-7

6A-TSM512 2-9, 2-11

6C110 chassis 1-1

A

accessing the boot load prompt 8-1

accessory carton 2-4

administrative weight 4-8

agent support B-1

aggregation tokens 4-9

alarm categories 9-7

alarms 9-6

 deleting 9-8

alias 2-23

allocating queue buffers 7-5

ambiguous commands 2-23

ARP server 3-2

ATM ports A-2

atmroute command 5-1

Available VPIs 6-8

B

backing up switch configuration 2-17

backup configuration 2-16

 TFTP server 2-17

Backup/Redundancy Configuration 2-16

bandwidth on class of service 7-4

Base VPI 6-7

Best Effort 3-10

Boot Load Commands 8-2

 chpi 8-2

 clfs 8-2

 dcfg 8-2

 df 8-2

 go 8-2

 he 8-2

 memory affected by 8-3

 ponf 8-2

 scsm 8-3

 swms 8-3

boot load firmware 8-4

boot load prompt 8-1

BUS 3-4

C

Cabletron technical support C-1

CAC 7-3

 allocating bandwidth 7-4

 conservative 7-3

 liberal 7-3

 moderate 7-3

CAC policies

 defined 7-3

CAC policy by class of service 7-4

call admission control policies

 defined 7-3

Call Admission Control policy 7-3

CCITT B-1

cell marking 7-7

Cell Storage Module 1-2

changing default boot load image 8-5

changing the password 2-15

chassis dimensions A-1

chassis module placement 2-7

chpi 8-2

class of service CAC policy 7-4

class of service queue buffers 7-5

clfs 8-2

COM port 2-13

COM port configuration 2-13

commands

 activate 2-21

 add 2-21

 add alias 2-23

 add atmroute 5-1, 5-4

 add elan 3-4, 3-10

 add ipatmclient 3-1, 6-4

 add ipatmpvc 6-4

 add laneclient 3-4

 add lecselanlec 3-10, 3-12

- add lecselannametable 3-10
- add lecselanpolicy..... 3-11
- add lecspacketsize..... 3-10
- add lecstlvset..... 3-12
- add pnnimetrics..... 5-5
- add pnninode..... 4-4
- add port 6-10
- add pvc..... 6-2, 7-3
- add route 5-7
- add trafficdescriptor..... 7-3
- backup switch 2-17
- clear..... 2-21
- create..... 2-21
- deactivate 2-21
- delete..... 2-21
- display 2-21
- execute 2-21
- execute redundancyconfigbackup... 2-18
- exit 2-15, 2-21
- flush 2-21
- help 2-24
- modify 2-21
- passwd..... 2-15
- reboot 8-8
- remove 2-21
- restart 2-21
- restore 2-21
- restore switch 2-17
- set..... 2-21
- set caceqbwallocscheme 7-4
- set cacservicelclassbw..... 7-4
- set ConsoleTimeOut 2-23
- set coredump..... 9-9
- set eventdisplay..... 9-7
- set pnniinterface..... 4-9
- set pnnipeergroupid 4-3
- set pnnipglelection 4-4
- set portconfig 5-2, 5-4, 6-5, 6-9
- set porttrafficcongestion 7-6
- set redundancyinfo..... 2-17
- show 2-21
- show alarms 9-8
- show atmroute..... 5-2, 5-4
- show caceqbwallocscheme 7-4
- show client 3-2, 3-5
- show events..... 9-7
- show ipatmarp..... 3-2
- show lecselanpolicy 3-11
- show minmax 7-6
- show netprefix..... 5-1
- show pnniinterface 4-8
- show pnnilink..... 4-4
- show pnnimetric..... 5-6
- show pnninode 4-2
- show pnnipglelection 4-5
- show porttrafficcongestion 7-5
- show pvp 6-6
- show route..... 5-7
- show switchtrafficcongestion 7-7
- show trafficdescriptor 6-2, 7-2
- start..... 2-21
- start lecs 3-4
- that affect the agent..... B-7
- update firmware 8-6, 8-7
- community B-7
- community strings 2-28
- configuration
 - initial 2-13
- configuration back up 2-17
- configuration restoration 2-17
- Configuring the Switch 2-13
- congestion management
 - diagnosing congestion..... 9-4
 - global congestion 9-4
 - port congestion..... 9-5
 - troubleshooting 9-4
- connecting PVPs..... 6-6
- console commands 2-21
 - format..... 2-21
- console help..... 2-24
- console time-out 2-23
- core dump files 9-9
- core dump security 9-9
- core dumps 9-9
- CPU 1-2
- CPU Module..... 1-2
- creating a VLAN 3-1
- creating an alias 2-23
- CSM..... 1-2, 2-18
 - installation..... 2-7
 - redundancy..... 2-18
 - reset button..... 2-20
- CSM placement 2-7

D

dcfg.....	8-2
default client address.....	3-3
default community strings.....	2-28
default ELAN.....	3-4
default IP over ATM client.....	3-3
default netprefix.....	3-3, 3-6
default router.....	2-13
deleting events and alarms.....	9-8
df.....	8-2
diagnosing congestion.....	9-4
dimensions.....	A-1
distributed LANE services.....	3-8

E

EFCI.....	7-7
ELAN.....	3-3
default.....	3-4
ELAN join policies.....	3-9
ELAN policy	
adding a policy.....	3-11
Best Effort.....	3-10
By ATM Address.....	3-10
By ELAN Name.....	3-10
By LAN Type.....	3-10
By MAC Address.....	3-10
By Packet Size.....	3-10
By Route Descriptor.....	3-10
identifying clients.....	3-12
index number.....	3-11
priority value.....	3-11
ELANs across multiple switches.....	3-7
Emulated LAN.....	3-3
enabling EFCI marking.....	7-7
enabling RM cell marking.....	7-7
ENET port.....	2-13
EPD.....	7-7
EPD threshold.....	7-7
Ethernet port.....	2-13
event categories.....	9-6
event persistence.....	9-6
event queue.....	9-6
events.....	9-6
deleting.....	9-8
events and alarms.....	9-6
viewing.....	9-7

F

firmware.....	8-1
---------------	-----

G

go.....	8-2
---------	-----

H

hardware reset.....	2-20
hardware warranty.....	C-2
he.....	8-2

I

I/O module ID numbers.....	2-4
I/O module letter.....	2-20
I/O modules	
physical specification.....	2-4
IISP routes.....	5-1
IISP routing considerations.....	5-2
IISP routing example.....	5-2, 5-3
ILMI.....	5-4
ILMI 4.0.....	6-8
initial configuration.....	2-13
Input/Output Modules.....	1-3
Installing Additional TSM Modules.....	2-11
Installing Other Modules in Chassis.....	2-11
installing power supplies.....	2-5
Installing the CSM.....	2-7
Installing TSM with CPU Board.....	2-9
internet MIB hierarchy.....	B-1
IOM-21-4.....	2-4
IOM-22-4.....	2-4
IOM-29-4.....	2-4
IOM-29-4-IR.....	2-4
IOM-29-4-LR.....	2-4
IOM-31-1.....	2-4
IOM-39-1.....	2-4
IOM-39-1-LR.....	2-4
IOM-67-4.....	2-4
IOM-77-4.....	2-4
IOMs.....	1-3
IP over ATM.....	3-1, 9-1
ARP server.....	3-1, 3-2
ARP table.....	3-2
ATM addressing.....	3-3
client.....	3-2

creating VLAN	3-1
viewing ARP table.....	3-2
IP over ATM client	3-3
IP Routing	5-6
ISO/CCITT.....	B-1

L

LAN emulation	
across multiple switches	3-7
add an ELAN	3-4
adding a client.....	3-4
ATM addressing	3-6
BUS.....	3-4
creating an ELAN	3-4
default client ATM address	3-6
default ELAN.....	3-4
default LECS ATM address.....	3-6
default LES and BUS ATM address..	3-6
distributed LANE services.....	3-8
ELAN join policies	3-9
LES	3-4
netprefix.....	3-6
starting the LECS.....	3-4
switch clients	3-7
LANE	3-1, 9-2
LANE service.....	3-3
distributed	3-8
LECS	3-4
LECSELANLEC table	3-11
LED	
active.....	2-19
CPU fail/ok	2-19
data.....	2-19
enet rdy	2-19
fail.....	2-19
no sync	2-19
power	2-19
rx data	2-19
standby.....	2-19
TSM fail/ok.....	2-19
tx data.....	2-19
LED descriptions.....	2-19
LEDs.....	2-19
LES.....	3-4
LGN.....	4-2
logical group node.....	4-2
logical link.....	4-5

M

Management Standards	A-3
master TSM/CPU	2-17
MaxIndex.....	7-6
MaxVpiBits	6-5, 6-8
metrics	5-5
MIB	
exceptions	B-6
object identifier	B-3
zeitnet.....	B-1
ZeitNet Cabletron proprietary.....	B-2
MIB exceptions	B-6
MIB groupings	
zeitnet.....	B-4
znBus	B-5
znCacStats.....	B-5
znCommonObjs	B-5
znConfig.....	B-5
znCpuPortTable	B-5
znEventAlarmTable	B-5
znEventTable	B-5
znIOModuleTable	B-5
znIpAtm	B-4
znIpAtmClient	B-4
znIpAtmServer.....	B-5
znLanEmulation.....	B-5
znLec.....	B-5
znLeCS	B-5
znLes	B-5
znManagedObjects.....	B-4
znModule	B-5
znPort	B-5
znPortExtTable	B-5
znPortTrafficCongTable	B-5
znProducts.....	B-4
znSar	B-5
znSignalling	B-5
znSlotTable	B-5
znSSCOP	B-5
znSwitchDiscoveryTable	B-5
znSwitchHW	B-5
znSwitchObjects	B-5
znSystem	B-5
znTrafficDescrExtTable.....	B-5
znTrapObjs.....	B-5
znVlan	B-5
MIBs	A-3
non-conformance	B-6

not supported	B-7
objects not supported	B-7
supported	B-6
MinIndex	7-6
module combinations in chassis	2-12
module placement	2-7
multi-level PNNI topology	4-2

N

netprefix	3-3, 3-6
Network Configuration	2-13
node ATM address	4-1

O

object identifier	B-3
operating humidity	A-2
operating temperature	A-2

P

parallel links	4-8, 4-9
password	2-15
PC adapter pin-out	A-3
PC serial port adapter	A-3
permanent virtual circuits	6-1
PGL	4-2
physical ports	
75 ohm coax	A-2
Cat. 5 UTP	A-2
MMF	A-2
SMF-IR	A-2
SMF-LR	A-2

PNN

managing parallel links	4-8
-------------------------------	-----

PNNI

adding higher-level peer groups	4-6
adding nodes	4-4
administrative weight	4-8
aggregation tokens	4-9
class of service	4-8
connecting multiple peer groups	4-2
default node ATM address	4-1
example	4-2
logical link	4-5
multi-level topology	4-2
node address	4-1
parallel links	4-8, 4-9

physical connections and peer groups	4-6
setting peer group ID	4-3
starting PGL election	4-4
troubleshooting	9-3
viewing links	4-4
viewing PGL	4-5

PNNI node addressing	4-1
PNNI routing	4-1
point-to-multipoint PVCs	6-2
point-to-point PVCs	6-1
ponf	8-2
port congestion	9-5
port number	2-20
port numbering	2-20
power requirements	A-1
PVCs	6-1
backward traffic descriptor	6-3
connecting to local switch client	6-4
creating	6-1, 6-2
point-to-multipoint	6-2
point-to-point	6-1
traffic descriptor	6-1
PVPs	6-4
add pvp	6-6
connecting	6-6
creating	6-6
disabling signaling	6-5
MaxVpiBits	6-5
set portconfig	6-5
viewing	6-6

Q

queue buffer allocation	7-5
queue buffers	7-5

R

redundancy	
CPU	2-17
CSM	2-18
TSM	2-17
redundancy configuration	2-16
scsm	8-3
swms	8-3
redundancy for CSM	8-3
redundancy for TSM/CPU	2-17
reset	2-20

- reset button 2-20
- restoring switch configuration..... 2-17
- RFCs..... B-1
- RJ-45 to DB-9 adapter..... A-3
- RM cell marking..... 7-7
- route metrics 5-5
- Routing
 - IISP 5-1
- routing 5-1
 - class of service 5-5
 - IISP considerations 5-2
 - IISP example..... 5-2, 5-3
 - ILMI..... 5-2, 5-4
 - incoming metric 5-5
 - IP 5-6
 - metrics..... 5-5
 - outgoing metric 5-5
 - reaching an NMS 5-7
 - reaching the Ethernet interface 5-7
 - UNI 5-4

- S**
- scsm..... 8-3
- security 2-15, 2-27, 9-9
- signaling A-2
- slave TSM/CPU..... 2-17
- slave TSM/CPU redundancy 2-17
- slot number 2-20
- SmartSwitch 6500 1-1
 - accessory carton..... 2-4
 - changing the password..... 2-15
 - compatibility 2-11
 - configuration..... 2-13
 - console 2-20
 - inspecting the order..... 2-1
 - installation and setup 2-1
 - installing power supplies 2-5
 - LEDs 2-19
 - module combinations..... 2-12
 - mounting the chassis..... 2-5
 - network configuration..... 2-13
 - redundancy..... 2-16
 - SNMP agent..... B-1
 - supported MIBs B-6
 - traffic management 7-1
 - unpacking..... 2-1
- SmartSwitch 6500 Modules 1-2
- SmartSwitch 6C110 chassis 1-1
- SmartSwitch ATM Administrator 2-25
 - default community strings 2-28, B-8
 - initial set up..... 2-27
 - online help..... 2-28
 - passwords..... 2-27
 - PC installation..... 2-27
 - requirements..... 2-26
 - Solaris installation..... 2-27
 - starting 2-27
- SMI Formats supported B-4
- SNMP B-1
 - community B-7
 - console commands that affect the agentB-7
 - default community strings B-8
 - managing the SmartSwitch 6500 B-7
- SNMP agent support B-1
- SNMPv1 B-4
- SNMPv2c A-3, B-4
- software warranty C-2
- specifications
 - ATM ports..... A-2
 - ATM routing protocols A-3
 - buffer memory A-1
 - chassis dimensions A-1
 - chassis weight A-1
 - CPU DRAM memory A-1
 - CSM dimensions..... A-1
 - Ethernet port A-1
 - flash memory A-1
 - LAN protocols A-3
 - management standards..... A-3
 - max I/O ports A-1
 - MIBs A-3
 - module weights..... A-1
 - operating humidity A-2
 - operating temperature A-2
 - PC adapter pin-out A-3
 - PC serial port adapter..... A-3
 - physical ports A-2
 - port-to-port latency A-1
 - power requirements..... A-1
 - protocols..... A-2
 - RJ-45 to DB-9 adapter A-3
 - serial port A-1
 - signaling..... A-2
 - standards A-2
 - switching engine A-1

TSM dimensions.....	A-1
weight	A-1
supported MIBs.....	A-3
switch configuration.....	2-13
Switch Installation and Assembly.....	2-5
Switch Installation and Setup.....	2-1
switch name.....	2-13
swms.....	8-3

T

technical specifications	A-1
technical support	C-1
electronic services.....	C-1
fax service.....	C-1
hardware warranty	C-2
placing a support call.....	C-1
repair services	C-2
software warranty	C-2
TFTP server.....	2-17
TLV set.....	3-11
Traffic Descriptors	7-1
traffic descriptors	
characteristics	7-2
creating	7-1
type number	7-2
Traffic Management.....	7-1
traffic management	
cell marking	7-7
changing EPD thresholds.....	7-7
EFCI.....	7-7
enabling EFCI marking	7-7
enabling RM cell marking	7-7
EPD.....	7-7
EPD threshold.....	7-7
MaxIndex.....	7-6
MinIndex	7-6
queue buffers	7-5
RM cell marking.....	7-7
Translation and Scheduling Module	1-2
Troubleshooting	9-1
troubleshooting	
congestion.....	9-4
core dumps.....	9-9
diagnosing congestion	9-4
event categories	9-6
events and alarms.....	9-6
global congestion.....	9-4

IP over ATM.....	9-1
LAN emulation	9-2
PNNI links	9-3
port congestion.....	9-5
switches in different peer groups.....	9-3
switches in same peer group	9-3
TSM.....	1-2
installation.....	2-11
TSM LEDs	2-19
TSM placement	2-7
TSM/CPU	
installation.....	2-9
TSM/CPU module.....	2-9

U

UNI routes	5-4
update firmware.....	8-6
upgrades	8-1
upgrading	
boot load firmware.....	8-4
changing default boot load image.....	8-5
POST diagnostics.....	8-5
switch operating firmware	8-6
unsuccessful update	8-7
update firmware	8-7
Upgrading and Changing Firmware.....	8-1
Using the Console	2-20

V

VCI.....	6-2
viewing alarms	9-7
viewing events.....	9-7
virtual port.....	6-6
root port	6-7
virtual port numbering.....	2-20
virtual ports	6-7
assigning	6-6
assigning VPIs	6-8
Available VPIs.....	6-8
Base VPI.....	6-7
creating	6-7
ILMI 4.0.....	6-8
MaxVpiBits.....	6-8
numbering convention	6-7
things to watch out for	6-11
virtual UNI.....	6-8

VPIs used	6-8
virtual UNI	6-8
VLAN	
creating	3-1
IP over ATM.....	3-1
VPI	6-2
VPI/VCI pair	6-2

W

warranty	
hardware	C-2
software.....	C-2

Z

ZeitNet Cabletron proprietary MIBs	B-2
ZeitNet MIB	B-1