Lucent Technologies
Bell Labs Innovations

TMX 880 Troubleshooting Guide

Release 8.0

300426574
February 2002

Notice. Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Limited Warranty. Lucent Technologies provides a limited warranty to this product.

Ordering Information. To order copies of this document, contact your Lucent Technologies account representative or visit the Lucent Product Documentation website at http://www.lucentdocs.com.

Technical Support. For technical support and other services, contact Lucent Customer Support.

Contents

About This Guide

Chapter 1 Overview

Chapter 2 Reviewing System Messages

Chapter 3 Reviewing System Alarms and Status Indicators

Chapter 4 Troubleshooting Power-Up and Boot Problems

Chapter 5 Getting Started Troubleshooting Interfaces and Protocols

Chapter 6 Troubleshooting Frame Relay

Chapter 7 Troubleshooting PPP

Chapter 8 Troubleshooting ATM

Chapter 17 Removing and Replacing Field Replaceable Units

Appendix A Power Requirements and Optical Specifications

Appendix B Adapter Card Connections

Appendix C Safety Instructions

Appendix D Acronyms

List of Figures

List of Tables

About This Guide

The *TMX 880 Troubleshooting Guide* describes how to isolate problems with the operation of a Lucent TMX 880^{TM} MPLS Core Switch, and suggests courses of action to remedy specified problems.

The book assumes that the reader is familiar with the system and with the product documentation listed under "Related Documents" in this section of the book. It also assumes that the reader is familiar with the network's topology and how the TMX 880 switch fits into this topology.

Intended Audience

This manual is intended for network administrators and system administrators who have experience working with network protocols, and command line configuration.

Documentation Conventions

This guide uses the following conventions:

Convention	Indicates	Example
`Courier regular`	Screen output or syntax.	`logging source-interface pos2/1`
Courier italic	Variable; generic text for which you supply a value.	`show ip interface [`*`interface-name`*`]`
`Courier bold`	User input.	`TMX 880#` **`show ip ospf database`**
Sans serif bold	Command names, options, and keywords in text.	By omitting the **no-summary** option...
Braces { }	Required argument; choose one.	`clock-source {line | internal}`

Brackets [ ]	Optional argument.	`set-overload-bit [on-startup seconds]`

Vertical bar |	Separates required or optional arguments to select from (“or”).	`show buffers swFab-buffers {iop | swfab}`
		`show ip bgp neighbors [ip-address | as-number] events [count]`

ver	Variable version number in filenames.	r*ver*.tar

This guide also uses the following conventions to call attention to important information.

► Notes provide additional information or helpful suggestions that may apply to the subject text.

⚠ Cautions notify the reader to proceed carefully to avoid possible equipment damage or data loss.

⚠ Warnings notify the reader to proceed carefully to avoid possible personal injury.

Related Documents

The following product documentation is also available:

- *TMX 880 Installation Guide*
- *TMX 880 Command Reference*
- *TMX 880 Command Quick Reference*
- *TMX 880 Configuration Guide*
- *Release Notes for the TMX 800 MPLS Core Switch - OS Software*
- *Navis TMX 880 Element Management System Installation Guide*
- *Navis TMX 880 Element Management System User’s Guide*
- *Release Notes for Navis TMX 880 Element Management System*

Overview

The Lucent TMX 880 ^{TM} MPLS Core Switch is a high-capacity system typically located within sophisticated networks. Responding to problem reports requires troubleshooting the problem within the context of the network and its configuration. Because problems you encounter may be caused by another system on the network, by connection media, or by the TMX 880 system, you need an understanding of the network topology and configuration. Troubleshooting problems on an TMX 880 system also requires a good understanding of the system, its configuration, and the system troubleshooting tools.

Successful operation of the TMX 880 MPLS Core Switch relies on the system configuration and the configuration on other systems to which it connects. Most system problems result from:

- System hardware
- Physical connections
- Configuration on the TMX 880 system
- Configuration on another system

The initial troubleshooting steps are the same for each of these problems. First you collect background information about the symptoms reported, then you view and analyze information about the interfaces. How you proceed depends on the result of this process.

System Troubleshooting Tools

The TMX 880 MPLS Core Switch provides the following troubleshooting tools:

- CLI commands
- Light emitting diodes (LEDs) and alarms
- SNMP messaging

The Navis TMX 880 Element Management System also provides monitoring and logging for the TMX 880 system. For information about the monitoring and logging tools available in the element management system, see the *Navis TMX 880 Element Management System User’s Guide*. Typically, you use the Navis TMX 880 EMS to configure and monitor ATM over MPLS.

CLI Commands

The CLI commands provide detailed information about specific modules on the system. These commands, that you run either at the console or through a Telnet session, provide the basis for your troubleshooting activities:

- **Show commands** — Display information about the configuration and operation of the system and system modules
- **Log commands** — Let you set the severity-level of messages saved, and lets you specify how log messages are stored
- **Debug commands** — Let you access debug-level messages for specified components
- **System management commands** — Provide SNMP commands, the **ping** command, and the **traceroute** command
- **File and directory management commands** — Let you manage system files, including copying both local and remote files

In some cases, show commands provide extensive output. If you access the CLI through a telnet session, you can save the output of the commands to a telnet log file, then review that file.

For detailed information about the CLI commands, see the *TMX 880 Command Reference.*

LEDs and System Alarms

The system has a comprehensive set of status indicators to monitor the system hardware and provide quick access to system status in a troubleshooting situation. The TMX 880 hardware provides status about the system in the form of numerous light emitting diodes (LEDs) and alarms. If you are at the same location as the system, or have someone from that location relaying information to you, you can obtain an overview of how the physical hardware is functioning. If you are troubleshooting a system remotely, you can run show commands to get some of the same information.

SNMP

The system should be configured to use SNMP to communicate with a network management station. The network management station then receives messages from the TMX 880 system and makes available performance and status information for the system.

Typically, network management stations are programmed to gather additional data on systems reporting error conditions. This data can provide a good staring point for your troubleshooting activities.

Other Troubleshooting Tools

The following types of troubleshooting tools can provide additional information about system operation:

- A light meter — Tests strength of signal for fiber optic cables.
- A Voltmeter — Tests system Voltage.
- Optical Time Domain Reflectometer (TDR) — Tests fiber optic cables.
- Protocol analyzer software — Analyzes packets transmitted on a network.

Troubleshooting Guidelines

Before you start troubleshooting, make sure that you have a good understanding of the problem and the condition of the system at the time of the reported problem. You should have the following information available:

- A description of the incident
- How often the incident occurred
- The events, including any system or network configuration changes, that immediately preceded the incident
- The amount of traffic on the system and the system interface(s) immediately before the incident occurred
- The scope of the incident, including the parts of the network impacted and the number of users affected

Use the following general guidelines for isolating and resolving system problems. Following these basic steps will help expedite problem isolation and resolution.

To troubleshoot a system problem:

1. If the system did not boot and display the CLI, troubleshoot boot problems.

   If the system does not boot for the initial system start-up, review the system LEDs and alarms before you start troubleshooting booting problems.

   On any subsequent start-up failures, ease of access to the system determines when in the process (if at all) you view system LEDs.

2. If the system boots but you do not see the CLI from a modem connection, it may indicate that flow control is not enabled. Enter Ctrl-Q to enable flow control. When flow control is enabled, the screen displays CLI output.

3. If the CLI did start:
   - Run the **show version** command to verify the version of the software running on the system.
   - Review recent activity on the system by running the **show logging** command.

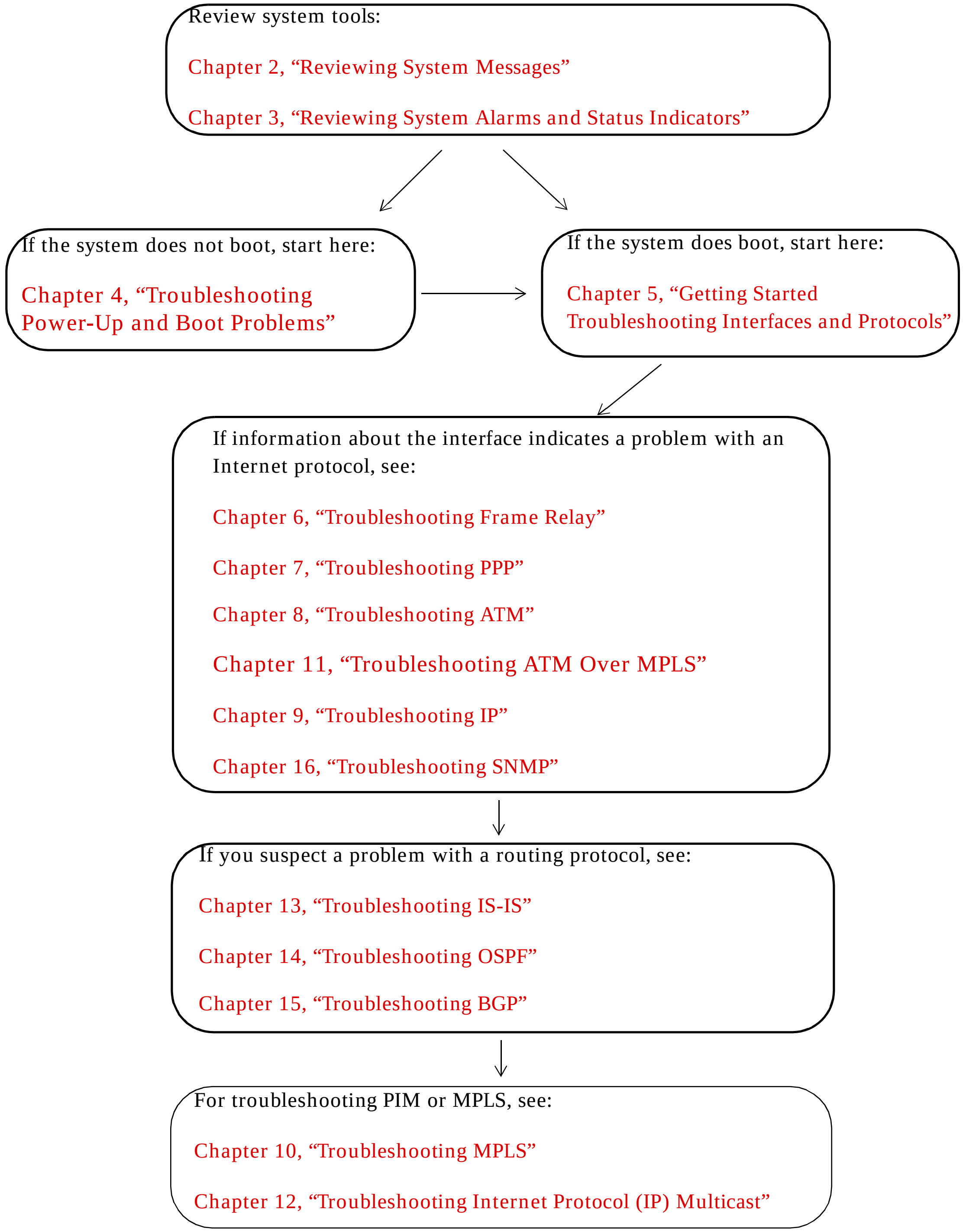
     For information about the logging utility, see Chapter 2, "Reviewing System Messages."
   - Run the **show all** command to make sure that system cards are operational.
   - Begin troubleshooting using the **show interfaces** command.

     The command provides summary information about the interfaces and protocols on the system.
   - Run other show commands and debug commands as needed.

     The troubleshooting procedures in Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols" describe how to proceed with troubleshooting for specified situations.
4. After you isolate the problem, correct the problem.
5. Test the change(s) to make sure that the problem is fixed.
6. If the problem still exists, go back to step 1, step 2 or step 3 as appropriate.

Using this Guide

The remainder of this book describes how to troubleshoot problems that may be encountered with the operation of the system. Figure 1-1 shows how to use this book to guide you through the troubleshooting process:



Review system tools:

Chapter 2, “Reviewing System Messages”

Chapter 3, “Reviewing System Alarms and Status Indicators”

If the system does not boot, start here:

Chapter 4, “Troubleshooting Power-Up and Boot Problems”

If the system does boot, start here:

Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols”

If information about the interface indicates a problem with an Internet protocol, see:

Chapter 6, “Troubleshooting Frame Relay”

Chapter 7, “Troubleshooting PPP”

Chapter 8, “Troubleshooting ATM”

Chapter 11, “Troubleshooting ATM Over MPLS”

Chapter 9, “Troubleshooting IP”

Chapter 16, “Troubleshooting SNMP”

If you suspect a problem with a routing protocol, see:

Chapter 13, “Troubleshooting IS-IS”

Chapter 14, “Troubleshooting OSPF”

Chapter 15, “Troubleshooting BGP”

For troubleshooting PIM or MPLS, see:

Chapter 10, “Troubleshooting MPLS”

Chapter 12, “Troubleshooting Internet Protocol (IP) Multicast”

Figure 1-1. Troubleshooting Road Map

2

Reviewing System Messages

The log utility on the TMX 880 MPLS Core Switch manages messages generated in response to system changes and error conditions. These messages can provide valuable information about problems you are troubleshooting. The log utility provides:

- **A circular log buffer** to receive and hold system messages

  The system replaces the oldest messages in the buffer with the newest ones when the buffer is at maximum capacity.

- **A log history buffer** to store a copy of the most critical messages

You can view messages currently in the log buffer, or the log history buffer, from the CLI.

Typically, users configure the system to send log messages to a Syslog server that parses the messages and provides alarms for specified error states. Consult the network administrator to determine how to effectively use network system configuration to view log messages.

The system also provides a debug utility that works in conjunction with the log utility. The debug utility enables the system to send various messages that have a severity level of debug to the log utility. You can view debug messages as you would other log messages.

Log Configuration

The system configuration for the log utility determines the severity, number, and type of messages stored in the buffer, in a file, or on a syslog server. By default, logging is enabled on the system and supports:

- Sending log messages only to the log buffer and sending the most critical log messages to the log history buffer
- Receiving log messages available through the route control processor (RCP), including those sent from the card control task to show card status

The default buffer sizes are:

- Log buffer — approximately 200 messages
- Log history buffer — 21 messages

The log utility supports standard logging levels. The log stores messages for a configured severity level and all numerically lower levels. Table 2-1 provides a description of the logging levels and lists the Syslog definition for the levels:

Table 2-1. Logging Severity Levels

Level	Severity	Description	Syslog Designations
0	emergencies	Condition makes the system unusable	LOG_EMERG
1	alerts	Requires immediate action	LOG_ALERT
2	critical	Requires attention	LOG_CRIT
3	errors	Indicates an error condition	LOG_ERR
4	warnings	Indicates a warning condition	LOG_WARNING
5	notifications	Notifies you of a significant condition	LOG_NOTICE
6	informational	Provides only informational messages	LOG_INFO
7	debugging	Indicates debugging condition	LOG_DEBUG

Verifying Log Configuration

Before you start using the log utility to get information about system performance, you should understand the logging configuration for the system you are troubleshooting.

To view the logging configuration for the system:

- Run the **show logging** command.

  The following sample output shows that the system sends messages only to the log buffer (not to a file or syslog server), and that it saves messages of the "informational" severity level (that is, the system stores messages for level 0-6).

  ```
  TMX 880# show logging
  Logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
      No Syslog Host configured
      Buffer logging: level INFO, 1288 messages logged
  Log Buffer (200 messages)
  .
  .
  .
  ```

The output from this command also shows the following if configured on the system:

- The filename of a file that stores system messages, and the message severity-level set
- The IP address of a syslog server that receives system messages, the facility type, and the message severity-level set
- Logging of messages for line cards, and the message severity-level set

Changing Log Configuration

Sending log messages to a file or to a Syslog server, changing buffer sizes, and logging messages from card local processors (LPs) requires configuration at the CLI.

Table 2-2. Log Configuration Commands

To configure this	Use this command
Access to system messages from all IOPs	**logging linecard**
Sending log messages to a file	**logging file**
Sending log messages to a syslog server	**logging** **logging facility** **logging trap**
The size of the log buffer	**logging buffered**
The severity level of messages stored size in the history buffer	**logging history**
Logging to a monitor for a Telnet session	**logging monitor**

► If you enable logging from the line cards, the content of the buffer on each IOP is sent to the buffer on the RCP. Because the log buffer on *each* line card stores approximately 200 messages, the buffer on the RCP can quickly fill.

The system sets a default severity level for each type of message logging if the level is not set by the user. Table 2-3 lists the default log level for the system logging activities:

Table 2-3. Default Severity Levels for Logging Information

Type of logging	Default log level
Log to the console	Informational
Log to a file	Debugging
Log to a syslog server	Informational
Line card log messages	Debugging
Log history buffer	Warning

Viewing Log Messages from a Telnet Session

You can view log messages from an active Telnet session, by configuring the monitor to display log messages.

To display log messages to the monitor during an active Telnet session:

1. Run the **terminal monitor** command to view messages:

   ```
   TMX 880# terminal monitor
   ```

2. Run the **logging monitor** command to enable logging to the monitor of an active Telnet session.

   This example, displays messages from the error severity level and higher:

   ```
   TMX 880# configure terminal
   TMX 880(config)# logging monitor errors
   ```

► The **terminal monitor** command and the **logging monitor** command can be entered in any order at the CLI.

Run the **terminal unmonitor** command to stop the display of log messages to an active Telnet session.

Message Types

If you want to see the types of messages available from the log utility, you can view the template used to create system messages for all modules, or for a specified one:

To view message templates for	Run this command
All modules	**show logging messages**
A specified module	**show logging messages** *module-type* where ***module-type*** is the name of the module listed by the **show logging messages ?** command.

The **show logging messages ?** command displays the modules for which you can display templates as shown in the following list:

all	All modules that provide log messages to the RCP
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol (routing protocol)
CCT	Card Control Task — Monitors the status of cards on the system
ENL	Event Notification Library

FPM	Forwarding Path Manager (Route Control Manager on the RCP)
FRL	Frame Relay
FRL_LMI	Frame Relay Local Management Interface
FRLSW	Frame Relay Switching
GBS	Global Buffer System
IPC	Inter-processor Communication
ISIS	Intermediate System to Intermediate System routing protocol
LOG	The log utility
LPF	LP forwarding task
MPLS	Multi-protocol Label Switching
MSDP	Multicast Source Discovery Protocol
MTRACE	Multicast traceroute
NML	Network Management Language — The component that configures SNMP
OSPF	Open Shortest Path First routing protocol
PIM	Protocol independent multicast — RCP protocol processing
PIMIOPBG	Protocol independent multicast — IOP background processing
PIMIOPDB	Protocol independent multicast — IOP database processing
PIMIOPFG	Protocol independent multicast — IOP foreground processing
PIMIOUPD	Protocol independent multicast — IOP database update receiver
PIMUPD	Protocol independent multicast — RCP database update sender
POLICY	Routing policies
POS	Packet over SONET
PPP	Point to Point Protocol
QOS	Quality of Service
RED	Redundancy

RSVP	Resource Reservation Protocol
SBM	Simple Buffer Management
SEC	Security
SNMP	Simple Network Management Protocol
System	Kernel system

▶ The log utility does not provide messages for IP on the system.

▶ SONET errors are not logged to the event log or displayed on the console. To display the current SONET state, you must use the **show sonet** command.

Getting System Information

The type of problem you are troubleshooting determines which features of the log utility will be most useful. Frequently, you use the system log utility in conjunction with the debug utility.

Naturally, you can view log messages only for those modules actually loaded on the system. The **show logging registered** command lists the loaded modules and shows the number of messages currently logged for a module.

Getting Information while Making System Changes

The **show logging** command displays all log messages that are in the log buffer. You can also display messages as the log buffer receives them by using the **logging console inline** command.

You use inline logging to:

- Ensure that all messages appear at the console.

  In a situation where the log utility receives many messages, you might miss seeing messages between subsequent **show logging** commands that you run.

- Run CLI commands and observe log messages to see whether your action initiated any system messages.

▶ Because logging messages inline is a high priority task, it can slow system performance. Turn inline logging off as soon as possible by using the **no logging console inline** command.

When troubleshooting a problem on the system you can clear the log buffer, make configuration or other system changes, then review the information in the log buffer. This way you deal with a smaller number of log messages.

To manage system messages during troubleshooting:

1. Review the messages currently stored by running the **show logging** command.
2. Run the **clear logging** command to erase the messages in the buffer.
3. Make configuration changes.
4. Run the **show logging** command to view system messages generated after the configuration change.

Getting Comprehensive Information for Cards

In many situations you want to view comprehensive information about the cards on the system. By default, the log utility provides basic information about the cards, but you can view additional information as needed.

To access messages for a line card:

- Run the **show logging *slot slot-number*** command to display status messages for a specified slot.

  or:

- To view all messages from all line cards, run the **logging linecard** command.

Collecting logging messages from the line cards sends a large number of messages to the log buffer. The content of the buffer will change quickly due to the influx of messages. You should send messages to a file (or view them from a syslog server) to make the messages accessible to you, otherwise messages will be lost as newer messages overwrite older ones in the log buffer.

Working with the Debug Utility

The debug utility on the system directs the types of messages specified (for example Frame Relay or OSPF) to the log utility. You enable logging of debug messages to the console or to the logging buffer. Messages sent to the log buffer can be viewed through the log utility at the CLI or from a file or syslog server if configured. For information about the logging utility, see "Log Configuration" on page 2-1 and "Getting System Information" on page 2-6.

You can enable debugging for:

- All modules
- A specified module
- A specified message, as identified by a message number
- All messages

The following modules provide debugging commands:

- ATM
- BGP (as IP BGP)
- Frame Relay
- IGP-TE
- IP
- IS-IS
- MPLS
- OSPF (as IP OSPF)
- PPP
- QoS

By using the debug command for a specified module, you can trace specific conditions. These messages are for use only in troubleshooting situations because they can generate a great deal of information. Turn off debugging as soon as you no longer need to see the debug messages, otherwise the numerous messages will clutter the log.

⚠ Use caution when turning on debugging. In some instances (for example with OSPF), the large number of messages generated places a heavy load on system resources and can slow system performance.

The following table provides general information about the debugging commands:

To do this	Use this command	Example
View which modules the debug utility supports.	**debug ?**	n/a
Turn on debugging for a specified module.	**debug *module-name***	To turn on debugging for OSPF: `TMX 880#` **`debug ip ospf`**
Turn off debugging for a specified module.	**undebug *module-name***	To turn off debugging for OSPF: `TMX 880#` **`undebug ip ospf`**
Send debug messages for a specified module to a log buffer.	**debug logging buffer *module-name***	To send OSPF debug messages to a log buffer: `TMX 880#` **`debug logging buffer ospf`**
Stop sending debug messages for a specified module to a log buffer.	**undebug logging buffer *module-name***	To stop sending OSPF debug messages to a log buffer: `TMX 880#` **`undebug logging buffer ospf`**
Turn off debugging for all modules.	**undebug all**	n/a
Enable logging of debug messages and send messages to the log buffer.	**debug logging buffer**	To send all debug messages to the log buffer: `TMX 880#` **`debug logging buffer all`**
Enable the logging of debug messages and display messages on the console.	**debug logging console**	To display all debug messages on the console screen: `TMX 880#` **`debug logging console all`**

Before beginning a debug session, consider enlarging the size of the buffer using the **logging buffered** command. If you make changes and want to see if the message-causing condition is corrected, empty the buffer with the **clear logging** command and then review messages in the buffer.

3

Reviewing System Alarms and Status Indicators

This chapter explains the panel Light Emitting Diodes (LEDs) on system cards. The LEDs provide status and alarm information. Some of these LEDs indicate optical fiber link problems. Troubleshooting optical fiber requires a good working knowledge of SONET technology.

This chapter also describes how to gather information about the alarm subsystem. The alarm subsystem monitors relay contacts on the STA to assert local visual and audible alarms when a problem occurs in the chassis.

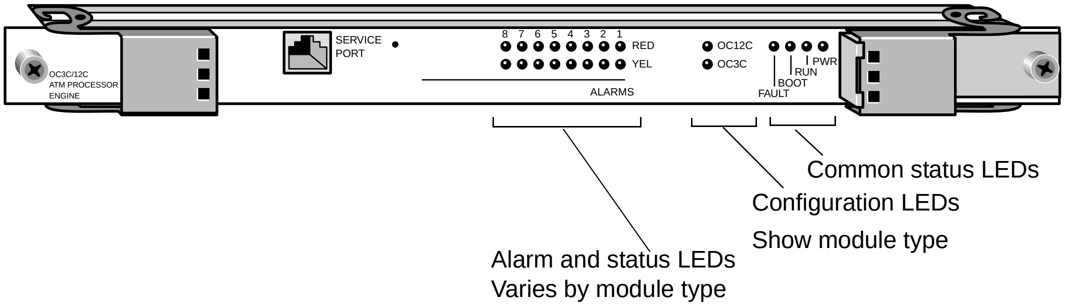
Equipment surveillance for a router site, also referred to as a Central Office (CO), is performed as:

- Remote surveillance which involves the use of network management software to provide Alarm, Status and Control (AS&C) information to a remote management center.
- Local surveillance which involves viewing system LEDs.

Failure indication is activated at the remote management system within 2 seconds of the failure while at the local site it is activated within 1 second of the failure.

Status Indicators

The module faceplates are designed to have a consistent look and feel for all module types. The faceplate of each IOP has LED sections as shown in Figure 3-1. This figure shows the faceplate for the ATM version of a OC-3c/OC-12c IOP:



Common status LEDs

Configuration LEDs

Show module type

Alarm and status LEDs
Varies by module type

Figure 3-1. IOP Module Faceplate Example

The following figure shows a similar faceplate for the Gigabit Ethernet IOP. This faceplate does not provide alarm and status LEDs:

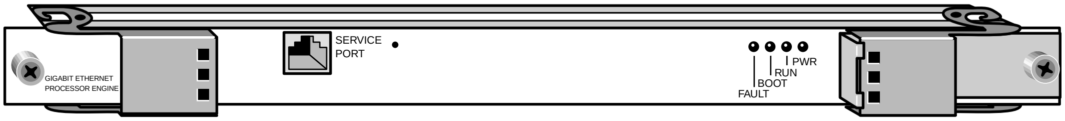
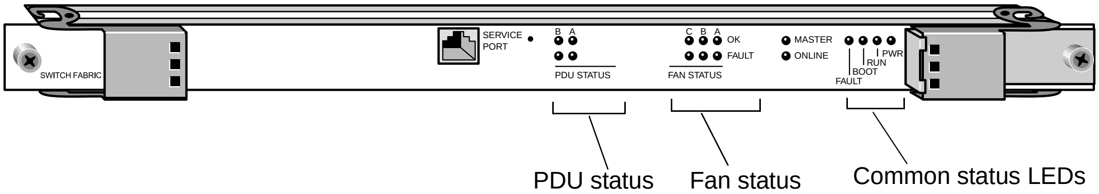


Figure 3-2. Gigabit Ethernet IOP Faceplate

- **Common status LEDs** — Provide information about the general status of the board
- **Configuration LEDs** — Contain configuration information to indicate whether, for example, an IOP is configured as an OC3c or OC12c
- **Alarm and status LEDs** — Reports interface conditions

Switch Fabric cards also have common status LEDs and configuration LEDs, but have status LEDs for the power distribution units (PDUs) and fan trays as shown in Figure 3-3:



PDU status

Fan status

Common status LEDs

Figure 3-3. Switch Fabric Faceplate

When a board is installed in the system, all LEDs turn on for a brief period (1-2 seconds) and then all turn off except the Power LED. From this point on the operation of the LEDs is described below.

Common Status LEDs

All IOP and Switch Fabric boards in the system have four LEDs, Power, Run, Boot, and Fault. The Power LED should illuminate whenever a card is inserted into the chassis. The following table describes the behavior of the other LEDs during different machine states. For additional information about problem conditions indicated by the LEDs, see Chapter 4, "Troubleshooting Power-Up and Boot Problems."

Machine State	Run	Boot	Fault	Comment
POST/Diagnostic	Off	1-second heart beat	On/Off	If a fault is encountered, diagnostics turn on the fault LED while continuing the 1-second heart beat to indicate a fault. It will turn off all LEDs before turning over control to the Load Op Code state.
Load Op Code	Off	5-second heart beat	On/Off	If a fault occurs while loading operational code the fault LED is illuminated and the Boot LED continues to beat at 5 second intervals. All LEDs are turned off prior to turning over control to the Operational State. Load time in excess of ten (10) minutes indicates a problem.
Operational State	On	Off	Off	This is the normal operational state.
Programming FLASH Image	On	On	On/Off	If the FLASH image is being updated both LEDs are on. The board *must not* be removed until this operation is complete as the image may get corrupted.

The *Power* LED is on continuously as long as all voltages are within tolerance. If any on board supply voltages move out of specification, the Power LED is extinguished. The voltage range for the PDU is -42 VDC to -60 VDC at 150 amps. The nominal value is -48 VDC.

Configuration LEDs

Two configuration LEDs indicate the mode in which the IOPs are operating.

Switch Fabric Configuration LEDs

Although you will see Master and Online LEDs on the switch fabric, neither of these are currently operational.

IOP Configuration LEDs

IOPs that support more than one mode, for example a POS OC3/OC12 card, have two green configuration LEDs that indicate the mode for IOP is operation.

▶ The IOP mode is really determined by the I/O Adapter that is connected to the IOP.

Alarm and Status LEDs

The Alarm and Status LEDs provide information about interface status and about the status of the PDU(s) and fan trays in the system.

▶ All installed switch fabric boards will report the same status. The OK and Fault LEDs are mutually exclusive, only one illuminates at a time.

Fan Status LEDs

The Switch Fabric has two banks of 3 LEDs each that indicate fan tray status. Normal operation is indicated by the LEDs in the OK row being lit (green). LED's in the Fault row being lit (yellow) indicate fan tray failure.

The **show chassis** command also provides information about fan tray status. In the output from this command, numbers rather than letters identify the fan trays.

Status LED on the switch fabric module	Fault	Location of fan tray in chassis	Associated fan tray number in **show chassis** output
A	Yellow	top front	1
B	Yellow	bottom front	2
C	Yellow	rear	3

If a fan tray fails you should replace it. For instructions to replace a fan tray, see Chapter 17, "Removing and Replacing Field Replaceable Units."

PDU Status LEDs

The Switch Fabric also has two banks of 2 LEDs each that indicate PDU status. Normal operation is indicated by the LEDs in the OK row being lit (green). LED's in the Fault row being lit (yellow) indicate PDU failure.

The **show chassis** command also provides information about PDU status. In the output from this command, numbers rather than letters identify the PDU.

LED Label	Fault	Comments	Associated PDU number in **show chassis** output
A	Yellow	This LED indicates that the right (from the rear of the chassis) PDU faulted.	1
B	Yellow	This LED indicates that the left (from the rear of the chassis) PDU faulted.	2

IOP Alarm LEDs

Each row of LEDs on an IOP corresponds to a SONET port on the IOA. When lit, the YEL or RED indicators identify a SONET problem:

LED Label	Normal Operation	Error condition
RED	Off	When the RED LED is ON, one of the optical interfaces (port on the IOA) has a critical (local) SONET error.
YEL	Off	When the YEL LED is ON, one of the optical interfaces (port on the IOA) has a non-critical (far-end) SONET error.

For information about troubleshooting SONET problems, see "Evaluating SONET Problems" on page 5-11 in Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

IOP Single OC-192 POS Status LEDs

There are two Alarm LEDs on the OC-192 IOP module, a RED and a YEL SONET alarm.

IOP Single OC48c-POS Status LEDs

There are two Alarm LEDs on this module, a RED and a YEL SONET alarm.

IOP Quad OC48-POS Status LEDs

There are two banks of four LED alarms on this module, a RED and a YEL SONET alarm for each port.

IOP Dual OC12c/ Octal OC3c ATM/POS Status LEDs

This module has eight rows of red/yellow LEDs. If the module is configured in OC12c mode then only the first two rows are applicable.

Gigabit Ethernet IOP

The Gigabit Ethernet module has only the common status LEDs.

I/O Adapter Cards LEDs

All I/O Adapter (IOA) cards, also referred to as line cards, with the exception of the Gigabit Ethernet line card, have 3 LEDs as described in the following table.

LED Label	Normal Operation	Condition and Action
PWR (Green)	On	If PWR LED is off, refer to Table 4-3, "Power Up and Booting Problems," on page 4-7 in Chapter 4, "Troubleshooting Power-Up and Boot Problems."
RED	Off	When the RED LED is ON, one of the optical interfaces has a critical (local) SONET error. For information about troubleshooting SONET problems, see "Evaluating SONET Problems" on page 5-11 in Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
YEL	Off	When the YEL LED is ON, one of the optical interfaces has a non-critical (far-end) SONET error. For information about troubleshooting SONET problems, see "Evaluating SONET Problems" on page 5-11 in Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

The IOP associated with a specified IOA should show the same LED operational conditions.

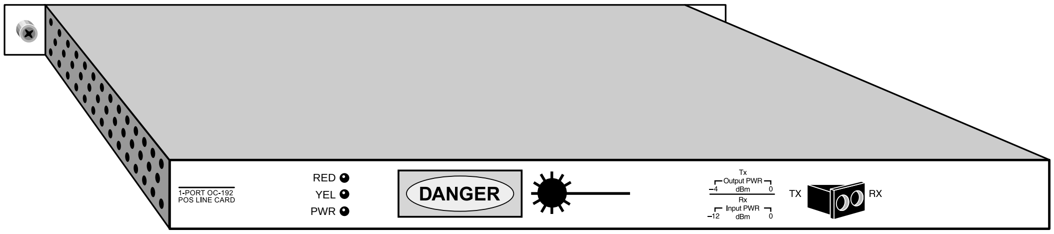


Figure 3-4. OC-192c IOA

Gigabit Ethernet Line Card

In addition to the power LED, the 2-port Gigabit Ethernet line card has two banks of LEDs, one bank for each port (that is one for port 0 and one for port 1). For the location of these additional LEDs, see Figure 3-5.

The 8-port Gigabit Ethernet line card has eight banks of LEDs, one bank for each port (port 0 through port 7).

LED Label	Normal Operation	Condition and Action
TX	On or Blinking	If the LED is ON, it indicates that data is being transmitted across the fiber. Off indicates traffic is not being transmitted. OFF may indicate a fault condition if an attempt is made to transmit traffic, but the LED remains off. Verify the network configuration.
RX	On or Blinking	If the LED is ON, it indicates that a port has data that has been received from the fiber. Off indicates traffic is not being received. OFF may indicate a fault condition if an attempt is made to receive traffic, but the LED remains off. Verify the network configuration.
Link	On	If the LED is ON, it indicates that the receive link is up and synchronized. Off indicates that the link is down. For a link to be operational, verify that the associated port is connected.

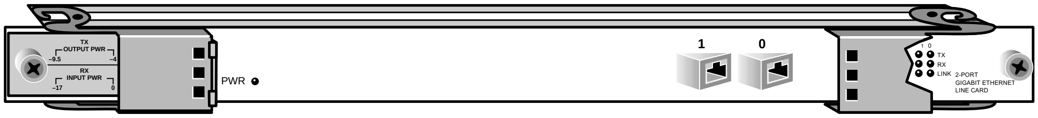


Figure 3-5. 2-port Gigabit Ethernet IOA

PDU LEDs

In addition to the PDU startup LEDs on the switch fabric, the PDU has two status indication LEDs clearly visible on the PDU front panel. The top LED is AMBER and the bottom LED is GREEN. These LED's indicate the status given in the following table.

PDU A LEDs		PDU B LEDs		PDU Condition
Amber	Green	Amber	Green	
Off	On	Off	On	Normal Operation
On	Off	Off	On	PDU A faulted
Off	On	On	Off	PDU B faulted
Off	Off	Off	Off	No Input power to either PDU
Off	Off	Off	On	No Input power to PDU A
Off	On	Off	Off	No Input power to PDU B

⚠ A PDU displaying a green LED must not be removed from an operating system unless the second PDU is also displaying a green LED.

A single green LED indicates that only a single PDU is operational. If this PDU is removed the system will crash.

SONET Timing and Alarm

The common status LEDs on the SONET/SDH Timing/Alarm Modules (STA) provide information about the general status of the board. Local surveillance involves the annunciation of audio and visual alarms when a problem occurs in the chassis, conditions that are due to external failures are not announced.

The TMX 880 system provides one set of visual and one set of audible alarm relay contacts on the rear of each STA module. When a problem occurs in the chassis or with the fiber, the MXOS software generates the alarm event and communicates the alarm condition to the STA card, which operates the alarm relay contacts for the system.

► When two STAs are present in the system, either set of alarm relay contacts may be used provided both STAs are operational.

Once asserted, any active alarm remains asserted, until the problem is eliminated. For example, Running commands to manually deactivate the chassis or modules results in an alarm condition. The physical removal of a card deactivates the associated card alarm.

Alarm Levels

The alarms initialize on a module-by-module basis; each alarm relay has three possible alarm states: Critical, Major and Minor.

- Minor Alarm: indicates a problem exists which is not currently interfering with necessary functionality.
- Major Alarm: indicates a problem exists which is interfering with necessary functionality.
- Critical Alarm: indicates a problem exists which either is or has the potential to interfere with total functionality.

Typical alarm levels for the modules are listed below:

- STA—Minor
- IOAs—Major
- PDUs—Major
- Switch Fabric—Major
- IOPS—Critical

The error conditions for the three alarm levels are based upon increasing severity. For example, a Major alarm caused by a switch fabric failure will escalate to a Critical alarm if the system is reduced to one switch fabric.

► Note that the associated alarm is cleared when a fan or PDU is pulled from the chassis. Otherwise, the alarm would be present through a module change which does not clearly indicate a fault condition.

Working with Alarms

The following table provides the alarm-related commands supported by the system.

Table 3-1. Alarm-related Commands

To do this	Use this command
Display information on current, potential or historical alarms	**show alarms all**
Show only currently asserted alarms	**show alarms active**
Display all alarms that have ever been asserted	**show alarms history**
Clear the historical counts	**clear alarm history**
Silence the audible alarm from the CLI (invokes the Alarm Cut Off [ACO])	**clear alarms relays**

Use the **show alarms** commands to analyze the alarm information. The alarm-related show commands display information about each card in the system. Watch the counts and replace problem modules to avoid potential problems.

To display only currently asserted alarms:

- Run the **show alarms active** command.
  - The `level` column in the command output displays the associated card alarm-level.
  - The `state` column, shows whether the module is in alarm ON or not in alarm OFF.
  - The ACO column displays the text pushed when you silence the alarm, either by pressing the ACO button or from running the **clear alarms relay** command at the CLI.
  - The `count` column displays the number of times the module has alarmed and whether or not the switch fabric has escalated from a Major to Critical alarm level.

  For example:

```
TMX 880# show alarms active
card alarms:
card      level  state  aco    count
SFC-00    MAJOR  ON            1 currently escalated to CRITICAL
SFC-01    MAJOR  ON            1 currently escalated to CRITICAL
SFC-02    MAJOR  ON            1 currently escalated to CRITICAL
PDU-01    MAJOR  ON     PUSHED 1
```

  The output shows four alarms are presently asserted on the system.

  - PDU-01 has caused a Major alarm; for which the operator pressed the ACO button.
  - The other three alarms occurred for three of the four switch fabric modules, the SFC units. Each of the SFCs failures caused a Major level alarm; however, when all but one of the total SFC units in the system alarmed, the alarm levels escalated from Major to Critical.

To display all of the active system alarms:

- Run the **show alarms all** command.

  This example of the **show alarms all** command output shows the same chassis (as above) after restoring the three failed SFCs to service.

```
TMX 880# show alarms all
card alarms:
  card    level     state  aco    count
  IOC-00  CRITICAL  OFF          0
  IOC-01  CRITICAL  OFF          0
  IOC-02  CRITICAL  OFF          0
  IOC-03  CRITICAL  OFF          0
  .
  .
  .
  SFC-00  MAJOR     OFF          1 can escalate to CRITICAL using index 0
  SFC-01  MAJOR     OFF          1 can escalate to CRITICAL using index 0
  SFC-02  MAJOR     OFF          2 can escalate to CRITICAL using index 0
  SFC-03  MAJOR     OFF          0 can escalate to CRITICAL using index 0
  RCP-00  MAJOR     OFF          0
  RCP-01  MAJOR     OFF          0
  STA-00  MINOR     OFF          0
  STA-01  MINOR     OFF          0
  FAN-00  MINOR     OFF          0
  FAN-01  MINOR     OFF          0
  FAN-02  MINOR     OFF          0
  FAN-03  MINOR     OFF          0
  PDU-00  MAJOR     OFF          0
  PDU-01  MAJOR     ON     PUSHED 1
interface  alarms:
  interfacelevel    state  aco    count
  IOC-00:00 MAJOR   OFF          5
  IOC-00:01 MAJOR   OFF          0
  IOC-00:02 MAJOR   OFF          0
  IOC-00:03 MAJOR   OFF          0
  IOC-00:04 MAJOR   OFF          0
  .
  .
  .
escalations:
  index   level     state aco    count
  0       CRITICAL  ON           2
```

Using the **all** argument displays each potential alarm in the system. Review the count column to establish the number of times each module has alarmed. The example above shows that:

- SFC 0 and SFC 1 have alarm counts of 1 while SFC 2 has an alarm count of 2 indicating it was non-operational two times.
- Interface 0 on IOC-00 has been nonoperational five times in the past.
- The escalation index entry has a count of 2, indicating that SFC2 may have alarmed 2 times while SFCs 0 and 1 were already alarming, resulting in 2 escalations.

To display all alarms that have asserted:

- Run the **show alarm history** command

  The following output displays all alarms that have asserted since the last clearing of alarm history.

```
TMX 880# show alarm history
card alarms:
card      level  state  aco      count
 SFC-01   MAJOR  ON     PUSHED   1 can escalate to CRITICAL using index 0
 SFC-02   MAJOR  ON     PUSHED   1 can escalate to CRITICAL using index 0
 SFC-03   MAJOR  OFF             2 can escalate to CRITICAL using index 0
 STA-01   MINOR  ON              4
 PDU-01   MAJOR  OFF             10
escalations:
 index    level     state  aco       count
  0       CRITICAL  OFF              1
```

The **show alarm history** command output shows:

- Two of the SFCs and STA-01 are in alarm.
- The ACO button was pushed to silence the SFC audio alarms.
- The STA alarm occurred after the ACO was pressed.
- Additionally, SFC-03, while not currently in alarm, had previously alarmed twice.

- The escalation index 0 alarm occurred once, indicating that at one point, three of the four SFC cards were simultaneously alarming.
- Finally, the PDU- 01, while currently functional, has faulted 10 times in the past and may need to be replaced.

Silencing the Alarm

You can silence any audio alarm by pressing the ACO button (located on the rear of the STA module, to the right of the visual alarm terminal block) or by running the **clear alarms relay** command.

► Silencing an audio alarm does not resolve the cause of the alarm or remove the alarm condition. The alarm will remain active until the problem is eliminated.

To determine the cause of the alarm condition run the show alarm active **command:**

```
TMX 880# show alarms active
card alarms:
  card    level     state  aco    count
  STA-01  MINOR     ON            1
```

To invoke the ACO run the clear alarms relays **command:**

```
TMX 880# clear alarms relays

ACO request queued!
```

To verify that the ACO has been pushed run the show alarm active **command:**

```
TMX 880# show alarms active
card alarms:
  card    level     state  aco    count
  STA-01  MINOR     ON     PUSHED 1
```

To clear the historical counts (optional) run the clear alarm history **command after the correcting the problem:**

```
TMX 880# clear alarms history
alarm counts cleared!
```

4

Troubleshooting Power-Up and Boot Problems

This chapter describes problems that can be encountered during system power-up and boot and outlines possible troubleshooting and corrective actions. The chapter also describes the different ways you can boot the system.

Refer to the *TMX 880 Installation Guide* for instructions on booting and configuring the system after installation.

Successful System Start-up

The following indicate successful power-up and system boot:

- After power up:
  - All power indicators/LEDs for PDU(s) and cards are green.
  - PDU status can be verified by the PDU LEDs on the Switch Fabric.
- After a successful boot:
  - All Power and Run LEDs are green.
  - The CLI prompt appears on the console screen.

Installation Directory and File Structure

The TMX 880 MPLS Core Switch uses single image management and a startup file to start the system. The following table lists the system files.

Table 4-1. System Files

File	Description
`/pcmcia0/releases/startup.dat`	Stores the location of the system image file used at system start-up, and the location of a backup directory that contains a backup image file. The system creates the startup.dat file.

Table 4-1. System Files

File	Description
`/pcmcia0/startup.cfg`	The default name of the configuration file used at system start-up. A different configuration file may be specified from the **boot config** command.
`/pcmcia0/releases/current/`*`rver`*`.tar` where *`rver`*`.tar` is the version-specific name of the file, for example r800.tar would be the tar file for version 8.0.0 of the MXOS software.	The single image file that contains system software files. The system boots from the image file in the current directory, unless otherwise specified by the **boot system** command.
`/pcmcia0/releases/backup/`*`rver`*`.tar` where *`rver`*`.tar` is the version-specific name of the file.	The single image file that contains system software files. The system boots from the image file in the backup directory (unless otherwise specified by the **boot backup** command), if boot from the image file in the current directory fails.

Monitoring Boot Activity

You can monitor system booting activity as follows:

- **Console** — View boot messages. At completion of the boot process, the CLI prompt displays.

  ▶ From the console you can interrupt the boot process to change boot parameters. For information about how to change boot parameters, see "Booting Using a PCMCIA Card."

- **Cards** — View card LEDs. When cards have booted correctly, the Run LED on each card is a solid/steady green. For information about the system LEDs, see Chapter 3, "Reviewing System Alarms and Status Indicators."

It can take 5 to 10 minutes for all the cards in the system to boot.

Boot Methods

For standard system operation, the system boots from a PCMCIA (Personal Computer Memory Card, International Association) card. For information about initial booting and configuration, see the *TMX 880 Installation Guide*.

For troubleshooting boot problems, you can boot the RCP over the network and copy files to the PCMCIA card. To start the system, you then boot from the new image on the PCMCIA. For information about this process, see "Booting over the Network."

Booting Using a PCMCIA Card

Booting the system requires the PCMCIA card have a valid boot image.

To boot the system using a PCMCIA card:

1. Plug the laptop, PC, or terminal server into the console port of the RCP.
2. Place the PCMCIA card into its slot in the RCP.
3. Power up the system.

For more information about setting up connections to the system, see the *TMX 880 Configuration Guide*.

The boot process starts automatically and ends when the boot task's program counter reaches 0. You can stop the boot process *before the count reaches zero* to change or confirm parameters:

- Press any key to stop boot process.

  The VxWorks boot prompt, `[VxWorks Boot]:` appears.
- Press **`p`** to view boot parameters.
- Press **`c`** to change boot parameters, or to retain the default value, press Enter.
- Type **`help`** at the prompt to view other options.

For example, to change the boot device you would press a key to stop the boot process, enter **`c`** and the press Enter, and then at the prompt enter the boot device to use:

```
boot device : pcmcia
```

The following table describes the boot parameters.

Table 4-2. Boot Parameters

Output	Description
`boot device : pcmcia`	The device used to boot the system: **`pcmcia`** — boot from a PCMCIA card (for standard system start-up) **`dc`** — boot the RCP from the network (for troubleshooting only) **`fm`** — flash card
`processor number : 0`	The number is always zero. Press the Enter key after this line.
`host name :nm1`	Host name assigned to host inet address. A network boot uses this entry.

Table 4-2. Boot Parameters

`file name:`
`/pcmcia0/releases/current/NxRcp.st`
	The RCP VxWorks image file.
	Note: The filename is case-sensitive.
	Press the Enter key after this line.

`inet on ethernet (e) :`
`     10.0.100.74:ffffc000`
	A value must be set on this line.

`host inet (h) : 192.0.1.4`	The IP address of the server to use for network boot.
`gateway inet (g) :192.0.0.1`	A gateway system used to connect to the server used for a network boot.
`user (u) : target`	User name to log into the FTP server for a network boot.
`ftp password (pw) : password`	Password to log into the FTP server for a network boot.
`flags (f) : 0x0`	The system supplies this value, *do not* change it.
`target name (tn) : rcp-frontier`	The name of a target. The entry must start with **`rcp`** or **`mtx`**.
`startup script (s) :`	During normal operation this line should be blank. A script file may be written to halt booting at this stage, and the name of that script file specified here. If you stop the boot process here, a view of VxWorks is loaded, but the RCP is not operational.
`other (o) : CF=/pcmcia0/startup.cfg;`	**`CF`** specifies the configuration file `startup.cfg`. The directory path may be different from the one displayed here.
`[VxWorks Boot]:`	Press **`p`** to verify your changes.

► After the system boots, you can set the configuration file used at boot-time from the CLI by using the **boot config** command.

Booting over the Network

If the system fails to boot because of a problem with the PCMCIA card, you can boot the RCP from a network server. To boot over the network you need:

- An FTP server
- An NxRcp.st file on the FTP server
- An FTP client

  The FTP client may be on the same system as the FTP server.
- IP connectivity from the FTP server and client to the TMX 880 system

To boot from the network:

1. Configure an FTP server with a user name of **`target`** and password of **`password`**.
2. On the TMX 880 system, interrupt the boot process to change the boot parameters.

   Press the Enter key to interrupt the boot process or press Ctrl x to extend the boot countdown time and then press Enter.
3. Change the boot parameters as indicated in the following list. Bold face type in the output column indicates changes required:

Output	Description of parameter changes
`Press any key to stop auto-boot...`	
`1`	
`[VxWorks Boot]:` **`c`**	
`'.' = clear field;  '-' = go to previous field;  ^D = quit`	
`boot device:` **`dc`**	Change to **`dc`** to boot the RCP from the network.
`processor number: 0`	
`host name:` **`Temp`**	Change the host name, in this example, **`Temp`**.
`file name: /pcmcia0/releases/current/NxRcp.st /NxRcp.st`	Change to specify the name of the file (in the default FTP server directory) that the system uses to boot.
`inet on ethernet (e): 10.0.100.145:ffffc000`	
`inet on backplane(b):`	
`host inet(h):` **`192.10.10.10`**	Set the IP address of the of FTP Server, in this example **`192.10.10.10`**.

Output	**Description of parameter changes**
`gateway inet(g):` **`10.0.0.1`** `>`	Set the default gateway for the TMX 880 system.
`user (u):` **`target`**	Set the username to log into the FTP server. This setting should be **`target.`**
`ftp password (pw) (blank = use rsh):` **`password`**	Set the password to log into the FTP server. This setting should be **`password.`**
`flags (f): 0x0`	
`target name (tn): mtx1`	
`startup script(s):` **`tbd`**	If needed, set to an entry required to display an RCP prompt
`other (o)`	

4. Enter **@** to restart boot process.

   The TMX 880 system should boot and display a -> prompt

5. On the TMX 880 system, use the **cd** command to move to the directory that will hold the files to be transferred to the system. For example,

   ```
   cd /pcmcia0/releases/current
   ```

6. If needed on the system running an FTP client, move to the directory that contains the files to be transferred to the TMX 880 system. For example:

   ```
   C:\> cd temp
   ```

7. Open an FTP session from the FTP client to the IP address for inet on Ethernet on the TMX 880 MPLS Core Switch.

   The following example opens an FTP session to an TMX 880 system that has the Ethernet address set to 10.0.100.145:

   ```
   C:\TEMP> ftp 10.0.100.145
   Connected to 10.0.100.145.
   220 VxWorks (5.3.1) FTP server ready
   User (10.0.100.145:(none)): target
   331 Password required
   Password: password
   230 User logged in
   ftp> bin
   200 Type set to I, binary mode
   ftp> hash
   Hash mark printing On (2048 bytes/hash mark).
   ```

8. Use the FTP **put** command to transfer files from the network server to the TMX 880 system.

9. After the file transfer completes, compare the size of the files on the server with the size of the files on the TMX 880 system.

   The size of a file on the server should be the same as the size of the file with the same name of the TMX 880 system.

10. Reboot the TMX 880.
11. Interrupt the boot process, change the boot parameters to their original settings, and reboot.

Power Up and Booting Problems

The following table lists power-up and booting problems and possible troubleshooting methods and solutions to these problems.

Table 4-3. Power Up and Booting Problems

For this symptom	Do this
PDU Status LED • Green LED not lit or: • Yellow lit	**1.** Make sure that the PDU is properly seated in its bay and that the power connector is securely connected to the PDU. **2.** Check that the connector is wired correctly. For information about wiring the PDU, see *TMX 880 Installation Guide*. **3.** With a voltmeter, check that there is -48 VDC, nominal, at the connector by inserting the voltmeter probes in the holes at the top of the connector. **4.** If the PDU appears to be failing, as a final check install the PDU in the other PDU bay. If the problem persists, it indicates that the PDU is bad. For more information on PDU LEDs, see Chapter 3, “Reviewing System Alarms and Status Indicators.”
Card(s) Power on LED does not come on at power up	If power is present at other boards: **1.** Reseat the card and make sure the thumb screws are tight. **2.** Remove the card from its present slot and insert it in another slot. If the LED still does not come on, replace the card. **3.** If another card is available, swap cards in the slots to ensure that it is a card failure rather than a problem in the chassis power circuit.

Table 4-3. Power Up and Booting Problems

For this symptom	Do this
Booting does not run to completion You may see error messages such as: • `Unable to locate a file` • `Unable to open a file` This may indicate an incomplete or corrupt image on the PCMCIA card.	**1.** If another system is available, verify the image on the PCMCIA card by plugging the card into the RCP of that system and executing the **show flash** command. **2.** If the image is intact and correct: – Replace the RCP and reboot. – If that also fails insert the RCP into the other RCP slot and reboot. **3.** If the PCMCIA card image is incomplete or corrupted: – Obtain a new PCMCIA card or: – Boot off the network (see the section "Booting over the Network").
`Wrong system` `software` message is displayed when router is booting	Determine whether the system has: • Incompatible hardware and software versions. • Wrong image on the PCMCIA card. – Obtain a new PCMCIA card or: – Boot off the network (see the section "Booting over the Network").
`Can't attach to device error` message	Check that: • The PCMCIA card is installed correctly in its slot. • The cable is connected to the network. • The boot parameter is **pcmcia**. For a network boot, the boot parameter is **dc** and an IP address must be configured on the management ethernet port.
CLI prompt not available after boot at RCP	Ensure that: • You are using the correct cable to connect the management console (using a DB-9 to RJ-45 adapter). • The RS232 link between the console and the RCP is intact. • The terminal is configured correctly. • For a modem connection, this may indicate that flow control is not enabled. Enter Ctrl-Q to enable flow control. When flow control is enabled, the screen displays CLI output

Table 4-3. Power Up and Booting Problems

For this symptom	Do this
Card Run LED does not come on	**1.** Make sure that the card finished booting. It takes 5 to 10 minutes for all the cards to boot. **2.** Run the **show chassis** command to see if the system recognizes the card. **3.** Run the **show all** command at the CLI `(cards)#` prompt to view card status. **4.** To obtain more detailed information about the status of the card: – Connect the console directly to the card. – Reboot the card by depressing the reset button located just above the connector. – Monitor the output to the console for failure indications. **Note:** If you press the reset button on a board three times (or the number of times set by the **threshold** command), the board will lock on the third (or otherwise specified) reset. This is by design to prevent the card from creating flapping routes. To unlock the board, issue a (cards)# **reload** command to reload the specified board.
Switch Fabric (SF) Run LED is on but card is not operational or: if you are working remotely, the system response is quite long	If the system has been successively rebooted, without allowing time for the RCP to recognize the switch fabric modules, power cycle the chassis, that is, turn the PDU circuit breaker OFF and ON again. For more information about rebooting the system, see "Rebooting the System" on page 4-9.

Status of Fans and PDUs

System fans must be operational after system boot. The TMX 880 fans and PDU(s) appear to be in a false or fault state shortly after the system boots. This is a temporary status condition that shows up only during the boot cycle.

Rebooting the System

The switch fabric modules and the RCP must be synchronized for the system to work correctly. When the router boots, make sure that RCP recognizes the switch fabric modules before booting the system again. Run the **show chassis** command to determine the status of the switch fabric modules. The command output should show the status as active.

The following segment of the output from the **show chassis** command shows that the switch fabric modules are active:

```
TMX 880# show chassis
.
.
.
Chassis Card Slots:
RCP-0    RCP-1    SF-0     SF-1     SF-2     SF-3     STA-0    STA-1
primary |        |        |active  |active  |        |active  |active  |
        |        |        |up      |up      |        |up      |up      |
.
.
.
```

If you reboot the system, before the RCP recognizes the switch fabric modules, the cards may not be synchronized. In this case, you must shutdown, then restart, the chassis for the system to operate correctly.

5

Getting Started Troubleshooting Interfaces and Protocols

This chapter describes how to start troubleshooting system interfaces and protocols that are not functioning correctly. In these cases, you verify that the system hardware is operational, then gather information about interfaces that are not operating properly. Your findings determine how you proceed.

The chapter also describes how to reset an interface, a common procedure that can remedy some interface problems.

Before You Start

Before continuing, make sure the CLI is running on the system. If you cannot access the CLI, see Chapter 4, “Troubleshooting Power-Up and Boot Problems.”

► If you are working at the router site, to proceed make sure that the Console serial port is connected into a terminal console using a DB-9 cable. This will give you direct access to the Route Control Processor (RCP).

Viewing and Assessing System Overview Information

You begin troubleshooting by obtaining an overview of the system and the status of interfaces. The interfaces must be operational and running the configured line protocols before you begin evaluating other problems such as routing errors.To view overview information:

1. Run the **show all** command at the `(cards)#` prompt to view the status of system cards.

   The command output shows the type of card in each slot, the status of a card — booting, quiescent, operational, reset, or failed — the number of interfaces on an IOP, the number of times the card failed since the it last loaded, and how many times a card can fail before a manual reset is required:

The number of times a card can fail before the system holds it in a Reset state

The number of times the card failed since it last booted

```
TMX 880# cards
TMX 880(cards)# show all
------+------------------------+---------------+----+------+------+
Slot  |Type                    |State          | No.|Failed|Failed|
      |                        |               | Ifs| Count|Thresh|
------+------------------------+---------------+----+------+------+
IOC: 1|OC3c-8 ATM              |    Operational|   8|     0|     2|
IOC: 2|OC48c-1 POS             |    Operational|   1|     0|     2|
IOC: 4|OC48c-1 POS             |    Operational|   1|     0|     2|
IOC: 5|OC12c-2 ATM             |    Operational|   2|     0|     2|
IOC: 6|OC12c-4 POS             |    Operational|   4|     0|     2|
IOC: 7|OC48c-1 POS             |    Operational|   1|     0|     2|
IOC:11|OC48c-1 POS             |    Operational|   1|     0|     2|
IOC:13|OC12c-4 POS             |    Operational|   4|     0|     2|
SFC: 1|Switch Fabric           |    Operational|   0|     0|     2|
STA: 1|Clock Timing Adapter    |    Operational|   0|     0|     2|
```

```
TMX 880(cards)# exit
```

2. Run the **show interfaces** command.

   The output from the command displays general information about interface behavior, interface settings (such as the encapsulation type for an interface), and packet activity. The following example output shows that interface pos2/0 is up, the line protocol is up, and that packets are being transmitted:

Interface type

Interface status

Protocol status

```
TMX 880# show interfaces
pos7/0 is up, line protocol is up (ifindex is 36)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is pos7/0, Packet over SONET OC-48c
       IP Address is 148.14.14.1, subnet mask is 255.255.255.0
(IP Cid 3)
  MTU 4470 bytes, BW 2405376 Kbit
  Encapsulation PPP, crc 32
  Scramble on
  Interface up time 04:14:33
  Last input 00:00:09, output 00:00:09
  Last clearing of "show interface" counters never
  5 minute input rate 8 bits/sec, 0 packets/sec
  5 minute output rate 8 bits/sec, 0 packets/sec
  Input: 0:1688 packets, 0:143940 bytes, 1 errors, 1 drops
    Local input: 0:1687 packets, 0:141396 bytes, 288 drops
    Local 5 minute input rate 8 bits/sec, 0 packets/sec
  Output: 0:1099 packets, 0:13320 bytes, 0 errors, 0 drops
    Local output: 0:1100 packets, 0:13338 bytes
    Local 5 minute output rate 8 bits/sec, 0 packets/sec
```

Packet status

Figure 5-1 shows the troubleshooting steps you take based on the output from these commands. On operational cards, you first make sure the interface is up; then make sure the line protocol is up. In the case of ATM interfaces, if the interface is up the line protocol is also up. For other interface types, you may need to resolve a configuration problem with the line protocol to make an interface operational. After the interface and the line protocol are up, you observe the packet activity on the interface to see whether the interface is passing packets without error.

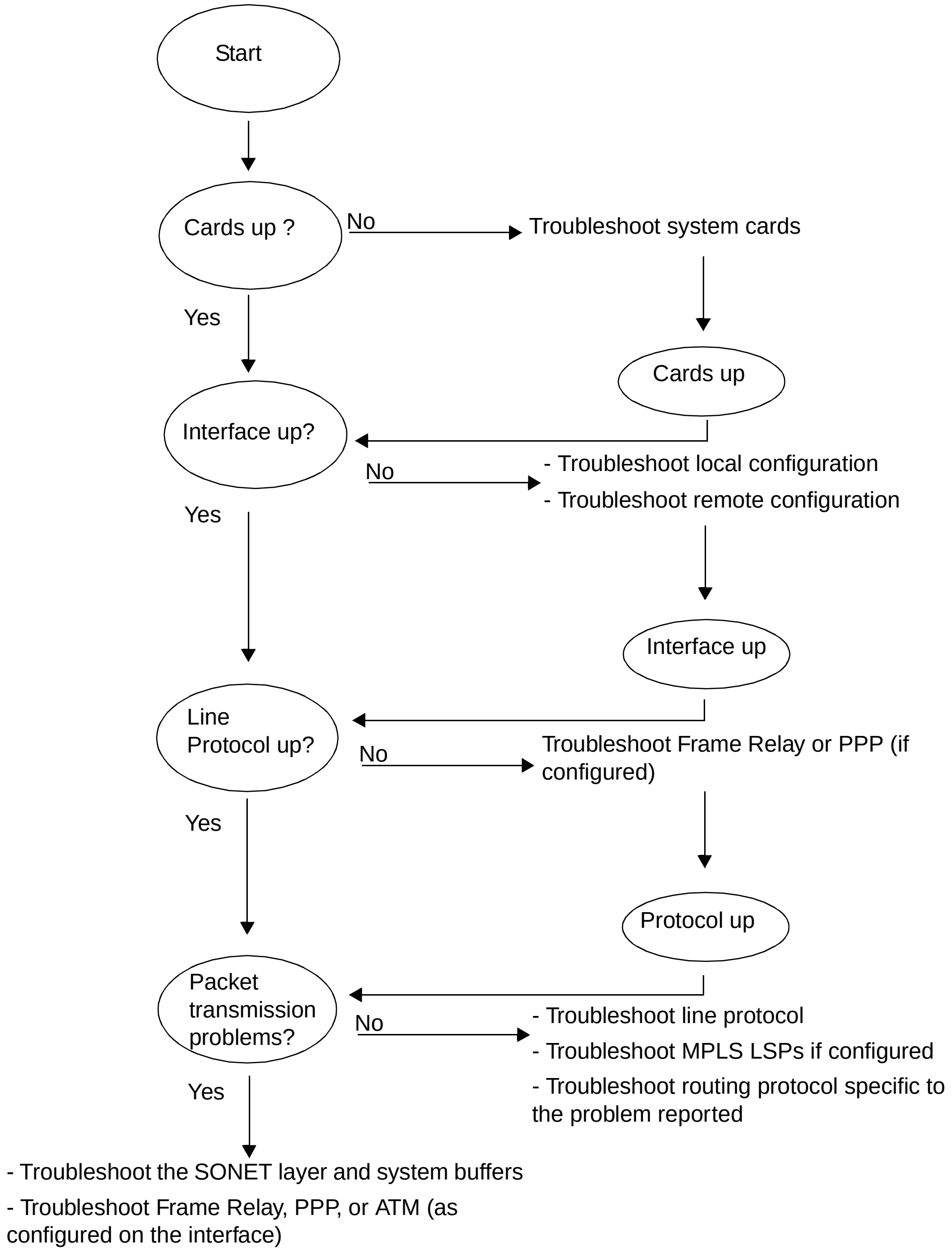

Start
Cards up ?
No
Troubleshoot system cards
Yes
Cards up
Interface up?
No
- Troubleshoot local configuration
- Troubleshoot remote configuration
Yes
Interface up
Line Protocol up?
No
Troubleshoot Frame Relay or PPP (if configured)
Yes
Protocol up
Packet transmission problems?
No
- Troubleshoot line protocol
- Troubleshoot MPLS LSPs if configured
- Troubleshoot routing protocol specific to the problem reported
Yes
- Troubleshoot the SONET layer and system buffers
- Troubleshoot Frame Relay, PPP, or ATM (as configured on the interface)

Figure 5-1. Initial Troubleshooting Steps

Basic Troubleshooting Commands

The following table lists the primary commands you use to troubleshoot system cards and interfaces:

Table 5-1. Commands to Evaluate Cards and Interfaces

To do this	Use this command
Reset the value for the number of card failures recorded by the system.	**failurecount**
View the operational status of cards on the system.	`TMX 880(cards)#` **show**
View information about events that affected system cards.	**show event-trace**
View the status of and summary information about an interface. View detailed interface statistics.	**show interfaces**
View logging information for an interface.	**show logging *slot-number***
View SONET statistics for an interface.	**show sonet**
Reset the number of card failures after which the system holds a card in the Reset state.	**threshold**

Verifying the Operational Status of System Cards

Before you start troubleshooting interfaces, make sure that the system cards are operational. You can evaluate status by running commands at the CLI. If you cannot bring the card to an operational state from the CLI, the remainder of card troubleshooting is done at the router site.

To verify card operation:

1. Run the **show** command to review the status of the cards.

   Look for cards in a `Reset` or `Failed` state. If no cards are in these states, go to "Troubleshooting Interfaces" on page 5-6.

   ```
   TMX 880# cards
   TMX 880(cards)# show all
   ------+-------------------------+----------------+----+------+------+
   Slot  |Type                     |State           | No.|Failed|Failed|
         |                         |                | Ifs| Count|Thresh|
   ------+-------------------------+----------------+----+------+------+
   IOC: 1|OC3c-8 ATM               |     Operational|   8|     0|     2|
   IOC: 2|OC48c-1 POS              |     Operational|   1|     0|     2|
   IOC: 4|OC48c-1 POS              |     Operational|   1|     0|     2|
   IOC: 5|OC12c-2 ATM              |     Operational|   2|     0|     2|
   IOC: 6|OC12c-4 POS              |     Operational|   4|     0|     2|
   IOC: 7|OC48c-1 POS              |     Operational|   1|     0|     2|
   ```

```
IOC:11|OC48c-1 POS              |     Operational|   1|     0|     2|
IOC:13|OC12c-4 POS              |     Operational|   4|     0|     2|
SFC: 1|Switch Fabric            |     Operational|   0|     0|     2|
STA: 1|Clock Timing Adapter     |     Operational|   0|     0|     2|
TMX 880(cards)# exit
```

► When troubleshooting an IOP, you can prevent the card from reaching the `Failed Threshold` by using the **failurecount** command to reset the Failed Count threshold, or by using the **threshold** command to increase the Failed Threshold.

2. If a card is not operational, run the **show event-trace** command to view information about events that affected system cards. You can view information about all cards, or about a specified one:

```
TMX 880# show event-trace ioc 2
SLOT STATE TRACE TABLE -- IOC 2
+------------------+----------------+----------------+----------
State Entered      |Duration        |State Name      |Event Name
+------------------+----------------+----------------+----------
2000-10-08 11:44:35|         01m 00s|           Empty|iocInserted
2000-10-08 11:45:35|         03m 01s|           Reset|iocHello
2000-10-08 11:48:36|             01s|           Reset|iocDiagComplete
2000-10-08 11:48:37|             10s|         Booting|iocBootComplete
2000-10-08 11:48:47|             00s|       Quiescent|adminUp
2000-10-08 11:48:47|             01s|BufferManagement|bmAvailableGood
2000-10-08 11:48:48|             50s|         GoingUp|iocGoneUp
2000-10-08 11:49:38|         58m 57s|     Operational|
```

3. If the card is not operational, and it is not clear why it is not functioning correctly, you can try unloading, then reloading the card:

```
TMX 880# cards
TMX 880 (cards)# unload ioc 2
.
.
.
TMX 880(cards)# reload ioc 2
```

4. If the card does not become operational, troubleshoot the card at the router site.

To troubleshoot system cards at a router site:

1. Review the status indicators on the card that presents an operational problem. For information about status indicators, see Chapter 3, "Reviewing System Alarms and Status Indicators."

2. Shutdown an inoperative card in preparation to removing the card from the system:

```
TMX 880# cards
TMX 880 (cards)# shutdown ioc 2
```

3. Remove the card from its slot.

   For an IOC, remove the IOA, then the IOP.

4. Inspect the card for any bent pins.

   If the card has pins that are bent, replace the card. If the pins appear to be intact, go to the next step.

5. Reseat the card(s) in the associated slot(s), ensuring that the card is properly engaged.
6. Activate the card by running the **no shutdown** command:

   ```
   TMX 880# cards
   TMX 880 (cards)# no shutdown ioc 2
   ```

7. If the card remains inoperative, replace the card with another one to see whether this resolves the problem.
8. If the card does not become operational, contact Lucent Customer Support.

Troubleshooting Interfaces

The most common causes of an interface being down on an operational card are:

- The system is not correctly configured.
- The system at the other end of the link is not up, or is not properly configured.
- A problem at the physical layer (the system hardware or the optical fiber).

When you troubleshoot an interface that is down, you take steps to remedy problems (as discussed in the following sections) then run the **show interfaces** command to see whether the change you made brought the interface up.

To troubleshoot system interfaces:

1. View messages saved in the log file by running the **show logging** command for a specified slot.

   Examine all Error and Critical messages.

   Messages that indicate excessive bit errors point to a problem at the SONET layer. For information about investigating SONET errors, see "Evaluating SONET Problems" on page 5-11.

2. Run the **show interfaces** command to view interface statistics.

   ▶ You can run the **show ip interface** command to quickly scan the status of *IP interfaces*.

   The following example shows the output for a single POS interface:

   ```
   TMX 880# show interfaces pos11/0

   pos11/0 is up, line protocol is up (ifindex is 54)
     Framing SONET, Clock-source Chassis, Laser is On
           Loopback not set
     Hardware is pos11/0, Packet over SONET OC-48c
           IP Address is 11.11.11.1, subnet mask is 255.255.255.0 (IP Cid 4)
     MTU 4470 bytes, BW 2405376 Kbit
     Encapsulation PPP, crc 32
     Scramble on
     Interface up time 00:39:27
     Last input 00:00:03, output 00:00:03
     Last clearing of "show interface" counters never
     5 minute input rate 16 bits/sec, 0 packets/sec
   ```

```
    5 minute output rate 32 bits/sec, 0 packets/sec
    Input: 0:493 packets, 0:16112 bytes, 21 errors, 1 drops
      Local input: 0:472 packets, 0:5794 bytes, 0 drops
      Local 5 minute input rate 16 bits/sec, 0 packets/sec
    Output: 0:493 packets, 0:6342 bytes, 0 errors, 2 drops
      Local output: 0:494 packets, 0:6360 bytes
      Local 5 minute output rate 32 bits/sec, 0 packets/sec
  TMX 880#
```

For this type of command output	Do this
line protocol is down	On an interface that is up, make sure that the following match on both sides of a link: • SONET framing • CRC on POS interfaces — the **show interfaces details** command displays values for `Bad CRC` if there is a mismatched CRC For more information about troubleshooting line protocols that are down, see the associated chapter: • Chapter 6, “Troubleshooting Frame Relay” • Chapter 7, “Troubleshooting PPP” Operational ATM interfaces have an active line protocol.
line protocol is admin down	Determine why the interface was shutdown (using the **shutdown** command). Restart the interface when appropriate by using the **no shutdown** command.
Laser is Off	Turn the laser on for the interface by running the **laser** command.
Scramble on	Make sure that the system at the other side of the link also has scramble enabled.
Iput and/or output rates at zero	If the interface should transmit traffic, go to step 3.
Input and/or Output showing errors and/or drops	• Determine if the system is dropping packets as designed. The system typically drops packets if: – An interface is congested. When a quality of service congestion mechanism is configured on the interface, it drops packets as configured. – Routes or MPLS LSPs have not been set up – The line has insufficient buffers • If you see input packet drops on an interface with PPP encapsulation, see Chapter 7, “Troubleshooting PPP.” This behavior might indicate a PPP connection or timeout issue. • Otherwise, go to step 3.

3. Run the **show interfaces detail** command to view input and output statistics for a specified interface, or all interfaces.

The initial lines in the command output are the same as the lines for the **show interfaces** command. The `Input` and `Output` sections display additional statistics.

```
TMX 880# show interfaces pos11/0 details

pos11/0 is up, line protocol is up (ifindex is 54)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is pos11/0, Packet over SONET OC-48c
       IP Address is 11.11.11.1, subnet mask is 255.255.255.0
(IP Cid 4)
  MTU 4470 bytes, BW 2405376 Kbit
  Encapsulation PPP, crc 32
  Scramble on
  Interface up time 00:47:30
  Last input 00:00:06, output 00:00:06
  Last clearing of "show interface" counters never
  5 minute input rate 16 bits/sec, 0 packets/sec
  5 minute output rate 16 bits/sec, 0 packets/sec
  Input: 0:589 packets, 0:17264 bytes, 21 errors, 1 drops
    Input Drops:
      No Buf Space         1          FE Drop              0
      VC Inactive          0          Non Pref Drop        0
      Hard Watermark       0
    Input Errors:
      Bad CRC              21         HDLC Abort           0 Values should
      Invalid Pkt          0          Bad L2 Hdr           0 be zero
      Fifo Overflow        0          MTU Exceeded         0
      Pkt Too Small        0          Pkt Too Large        0
      TTL Error            0          Tunnel TTL Error     0
      Bad Version          0
    Local input: 0:568 packets, 0:6946 bytes, 0 drops
    Local 5 minute input rate 16 bits/sec, 0 packets/sec
      Queue 0:
        Packets    568        Bytes      6946
        Drops      0          Drop Bytes 0
      Queue 1:
        Packets    0          Bytes      0
        Drops      0          Drop Bytes 0
      Queue 2:
        Packets    0          Bytes      0
        Drops      0          Drop Bytes 0
  Output: 0:589 packets, 0:7494 bytes, 0 errors, 2 drops
    Output Drops:
      Invalid L2Id         2
    Output Errors:                                             Values should
      Packet Parity        0          Insuff Byte Cnt      0 be zero
      Queue Flush          0          Switch Fabric Err    0
      Buf Addr Mismatch    0          Bad Buf Desc         0
    Local output: 0:590 packets, 0:7512 bytes
```

Local 5 minute output rate 16 bits/sec, 0 packets/sec

For this type of command output	Do this
Input	
No Buf Space	Look for output buffer or switch fabric problem indicators, and see “Evaluating System Buffers” on page 5-13.
Bad CRC	Make sure that the CRC setting on both sides of the link are the same. Mismatched CRC values make the line protocol for the link inoperative. For information about setting the CRC, see “Working with CRC Values” on page 5-10.
MTU Exceeded	Investigate the MTU settings on the local and remote systems. Make configuration changes as needed. Use the **ip mtu** command to change the setting on a TMX 880 system.
Queue statistics	Look at the number of packets and bytes dropped in relation to the queue configuration. Review the quality of service configuration for the interface.
FE Drop Invalid Pkt Pkt Too Small HDLC Abort Bad L2 Hdr Pkt Too Large	Investigate the configuration of the system at the other side of the link. All of these conditions indicate a problem at the far end.
Output	
Buf Addr Mismatch Switch Fabric Err Bad Buf Desc	If cards have recently been added to the system, make sure that the system was populated correctly. Verify that buffers on the switch fabric are functioning correctly. See “Evaluating System Buffers” on page 5-13.
Increase in output counters Any errors reported in the output	**1.** If cards have recently been added to the system, make sure that the system was populated correctly. **2.** Verify that buffers on the switch fabric are functioning correctly. See “Evaluating System Buffers” on page 5-13. **3.** Verify that all cards are operational by running the **show** command for cards again.

For this type of command output	Do this
Packet (input and output) drop counters greater than zero	Keep in mind that input error conditions on an input card can be a symptom of a problem on the output card. Congestion on an output card can cause congestion on an input card that has a system path to the congested output card. Link-layer configuration problems (such as misconfigured DLCIs) and routing problems can also be responsible for error conditions when passing packets. **1.** Verify that buffers on the switch fabric are functioning correctly. See “Evaluating System Buffers” on page 5-13. **2.** Make sure that the SONET layer is functioning properly, see “Evaluating SONET Problems” on page 5-11.

3. Verify that the system at the other side of the link is running and is correctly configured.

Working with CRC Values

The CRC settings on both sides of a link must be the same. You change the CRC value from 32 to 16, or from 16 to 32.

The default CRC settings are:

- Releases 1.5.2 and later: 32
- Releases prior to 1.5.2 (Release 3 of the FPGA): 16

To change the CRC value:

1. Run the **fcs** command to change the CRC value on an TMX 880 system. The following example input changes the CRC from 32 to 16:

```
TMX 880# configure terminal
TMX 880(config)# interface pos2/0
TMX 880(config-if)# fcs 16
```

2. For an *OC-48c card*, reboot the card for the change to take effect. The following example reboots the IOP in slot 2:

```
TMX 880# cards
TMX 880(cards)# reload ioc 2
```

The command form **fcs 32** changes the CRC from 16 to 32.

Evaluating SONET Problems

Interfaces that show packet transmission problems may be experiencing a problem at the SONET layer. You can get preliminary information about SONET problems at the CLI, but additional SONET troubleshooting must continue at the router site. Often a problem with the cabling causes a SONET transmission problem.

► SONET errors are not logged to the event log or displayed on the console. To display the current SONET state, use the **show sonet** command.

To troubleshoot SONET from the CLI:

- Run the **show sonet** command to displays statistics for a specified interface:

```
TMX 880# show sonet pos11/0

Medium Type:                                                  sonet
Medium Line Coding:                                             NRZ
Medium Line Type:                                   ShortSingleMode
Medium Circuit Identifier:

Current Section Status:                                  No Defect.
Current Section Errored Seconds:                                  0
Current Section Severely Errored Seconds:                       207
Current Section Severely Errored Framing Seconds:               207
Current Section Coding Violations:                            65535

Current Line Status:                                     No Defect.
Current Line Errored Seconds:                                     0
Current Line Severely Errored Seconds:                            0
Current Coding Violations:                                      382
Current Line Unavailable Seconds:                                 0

Path Label byte (C2 flag):                               0xcf (POS)
Current Path Width:                                     sts48cSTM16
Current Path Status:                                     No Defect.
Current Path Errored Seconds:                                     0
Current Path Severely Errored Seconds:                            0
Current Path Coding Violations:                                   0
Current Path Unavailable Seconds:                               207
```

For this type of command output	Do this
Path Label byte (C2 flag)	Make sure that the value set is compatible with other POS devices. See the **pos flags c2** command reference page in the *TMX 880 Command Reference*.

For this type of command output	Do this
Medium Circuit Identifier	If an OC-12 POS interface connects to another system that uses a multi-mode cable, make sure that the TMX 880 system uses a multi-mode cable for that connection (rather than a single mode cable) otherwise signal attenuation may be necessary.
Current Section Severely Errored Framing Seconds	A framing error can indicate a bad cable, or a signal to noise ratio that is too high. Continue troubleshooting SONET layer problems at the router site.

To troubleshoot SONET at the router site:

⚠ Observe safety precautions whenever working directly with the system. See Appendix C, “Safety Instructions.”

1. Verify with a light meter that the receive signal levels are set to the correct values for the optical carrier (OC) associated with the interface.

If the receive signal level is higher than the specified value, use inline attenuation to reduce the level of the receive signal. To review the values for receive signal levels, see Appendix A, “Power Requirements and Optical Specifications.”

2. Inspect the cable to look for and then fix:

- A kinked cable or one that has a bend radius that is too narrow
- A frayed cable

▶ If you disconnect then reconnect a cable, make sure the cable is correctly attached.

3. Clean a suspected dirty cable with a cable cleaner.

If this action does not resolve the problem, change the cable.

4. If the optical link has been up and operating correctly for any amount of time, it is important to investigate possible problems in equipment in the fiber path between the local system and the system at the other end of the link. Look for a history of:

- Changes to the remote system and its cabling
- Changes to cabling, repeaters, and so forth
- Reported equipment problems

Evaluating System Buffers

The dynamic buffer management system on the TMX 880 MPLS Core Switch reserves buffers for each IOP to insure that an IOP has buffer space available. The buffer management system also shares additional buffers from a buffer pool to meet system demand. The system reclaims buffers as they become available and returns them to the buffer pool. It also reclaims buffers if a buffer is not returned to the buffer pool when the system is finished with it.

To troubleshoot system buffers:

1. Review the allocated and reclaimed buffers reported by each IOP by running the **show buffers swfab-buffers** command.

   The output for the command shows a summary of the buffers for each IOP:

   ```
   TMX 880# show buffers sw iop
        IOP         SF0         SF1         SF2         SF3         RECL

          2       13312        1000        1000        1000            0
          4       13312        1000        1000        1000            0
          6       13312        1000        1000        1000            0
          8       13312        1000        1000        1000            0
   ```

   If you do not see any buffers listed for a switch fabric, make sure that the card is operational, see "Verifying the Operational Status of System Cards" on page 5-4.

2. If the switch fabric is operational, but does not show buffers, contact Lucent Customer Support.

Resetting an Interface

In some instances, you may need to reset an interface for an interface to become operational. On PPP links, resetting an interface can open the link control protocol (LCP), and a network control protocol such as IPCP.

To reset an interface:

1. Run the **shutdown** command to shut down the interface.

   The following example input shuts down interface pos2/0:

   ```
   TMX 880# configure terminal
   TMX 880(config)# interface pos2/0
   TMX 880(config-if)# shutdown
   ```

2. Use the **no shutdown** command to start the interface running again.

   The following example input restarts interface pos2/0:

   ```
   TMX 880# configure terminal
   TMX 880(config)# interface pos2/0
   TMX 880(config-if)# no shutdown
   ```

If other instances, such as a card that is down, you need to reload the card:

- Run the **reload** command for a card.

  The following example input reboots the IOP in slot 2:

  ```
  TMX 880# cards
  TMX 880(card)# reload ioc 2
  ```

6

Troubleshooting Frame Relay

This chapter describes the basic behavior for Frame Relay running on the TMX 880 MPLS Core Switch, the configuration required to enable Frame Relay on the system, and how to troubleshoot problems with Frame Relay operation.

Before You Start

Before reading this chapter you should be sure that the POS and serial interfaces configured to use Frame Relay are up. For information about system interfaces, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

Basic Frame Relay Behavior

A system with POS and serial interfaces correctly running Frame Relay has:

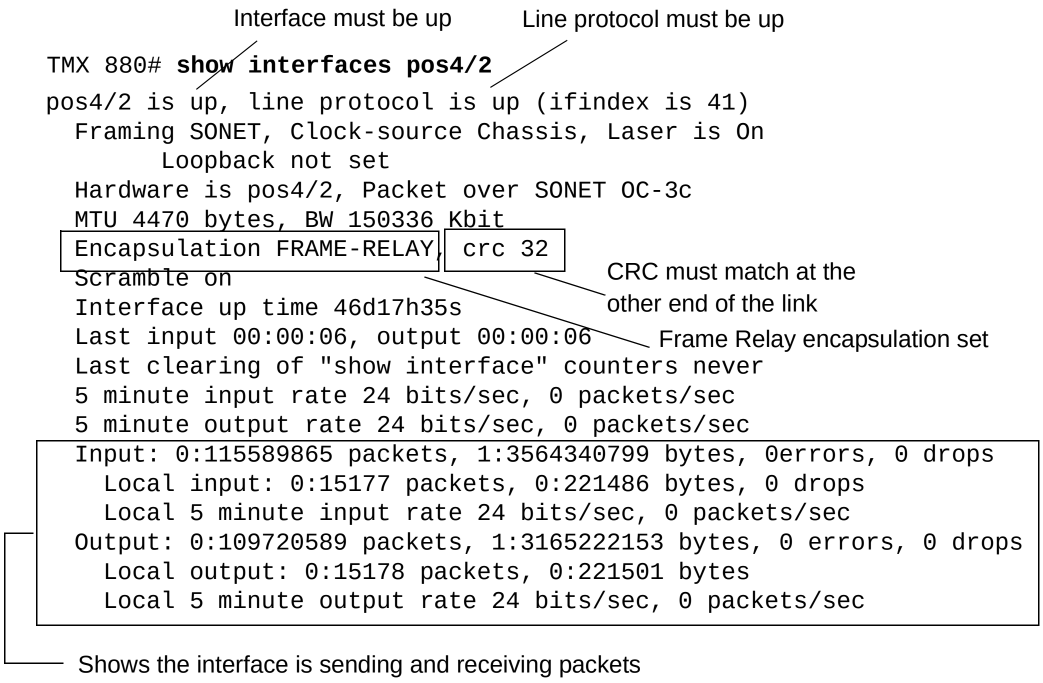
- The line protocol up on the interfaces configured to use Frame Relay encapsulation
- Interfaces configured to use Frame Relay encapsulation communicating with remote routers as configured

► Typically, for Frame Relay routing, Frame Relay encapsulation is set on subinterfaces. Subinterfaces are logical interfaces on a physical port.

In this chapter, the use of the term interface refers to both interfaces and subinterfaces in the context of Frame Relay routing.

Output from the **show interfaces**, **show frame-relay pvc summary**, and the **show frame-relay lmi** commands show the operational status of Frame Relay on the configured interfaces.

The **show interfaces** command verifies that Frame Relay encapsulation is enabled on the appropriate interfaces, and that each Frame Relay interface is sending and receiving packets:



```
TMX 880# show interfaces pos4/2
pos4/2 is up, line protocol is up (ifindex is 41)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is pos4/2, Packet over SONET OC-3c
  MTU 4470 bytes, BW 150336 Kbit
  Encapsulation FRAME-RELAY, crc 32
  Scramble on
  Interface up time 46d17h35s
  Last input 00:00:06, output 00:00:06
  Last clearing of "show interface" counters never
  5 minute input rate 24 bits/sec, 0 packets/sec
  5 minute output rate 24 bits/sec, 0 packets/sec
  Input: 0:115589865 packets, 1:3564340799 bytes, 0errors, 0 drops
    Local input: 0:15177 packets, 0:221486 bytes, 0 drops
    Local 5 minute input rate 24 bits/sec, 0 packets/sec
  Output: 0:109720589 packets, 1:3165222153 bytes, 0 errors, 0 drops
    Local output: 0:15178 packets, 0:221501 bytes
    Local 5 minute output rate 24 bits/sec, 0 packets/sec
```

Interface must be up
Line protocol must be up
CRC must match at the other end of the link
Frame Relay encapsulation set
Shows the interface is sending and receiving packets

The **show frame-relay pvc summary** command lets you view the status of the data link connection identifiers (DLCIs) configured.

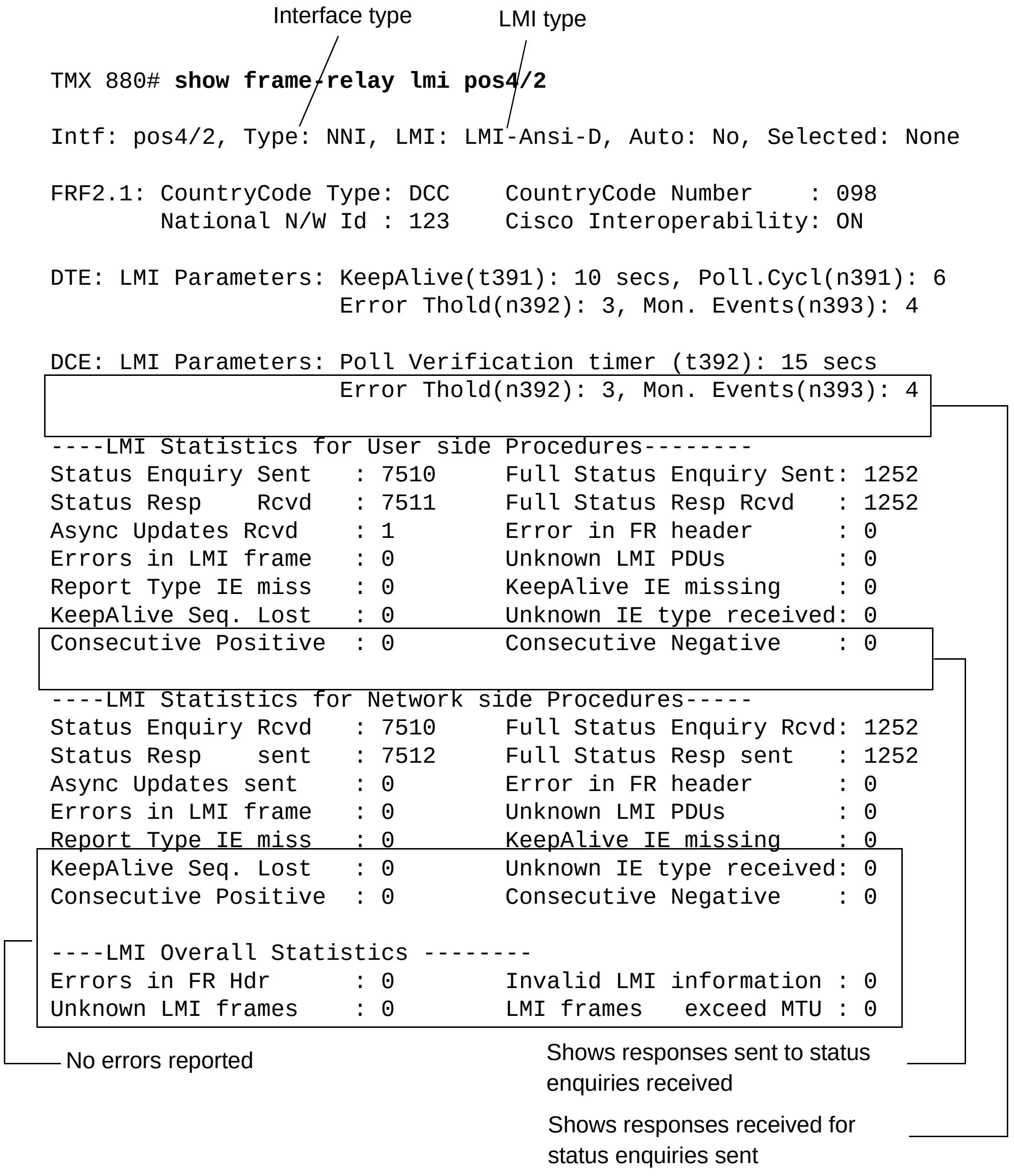
The command output on the system shows summary information for each interface configured to use Frame Relay. For example:

```
TMX 880# show frame-relay pvc summary
========= DLCI Summary For Interface pos4/2 =========

DLCI       State             opState    Type         Sub-Intf     Map-Class

----       -----             -------    ----         --------     ---------

0         Active            Up         LOCAL        none         default-control
1023      Active            Up         LOCAL        none         default-control
16        Active            Up         PPROUTED     pos4/2.16    default
```

► It is common to see DLCIs in various states. Although individual DLCIs may be down, the local management interface (LMI — the line protocol for Frame Relay) remains up.

The **show frame-relay lmi** command lets you view information about the status of the LMI.

The following example output is for an NNI interface. For a DTE interface the command displays only user side procedures; for a DCE interface only network side procedures. The example also shows that FRF2.1 is enabled. Cisco Interoperability ON indicates that the Link Access Procedure for Frame Relay (LAPF) packets are padded with zeros (NULLs), making the minimum packet size 10. This enables the switch/router to interoperate with non-Lucent systems which may require frames of a minimum 10 bytes in length.



```
TMX 880# show frame-relay lmi pos4/2

Intf: pos4/2, Type: NNI, LMI: LMI-Ansi-D, Auto: No, Selected: None

FRF2.1: CountryCode Type: DCC    CountryCode Number    : 098
        National N/W Id : 123    Cisco Interoperability: ON

DTE: LMI Parameters: KeepAlive(t391): 10 secs, Poll.Cycl(n391): 6
                     Error Thold(n392): 3, Mon. Events(n393): 4

DCE: LMI Parameters: Poll Verification timer (t392): 15 secs
                     Error Thold(n392): 3, Mon. Events(n393): 4

----LMI Statistics for User side Procedures--------
Status Enquiry Sent   : 7510     Full Status Enquiry Sent: 1252
Status Resp    Rcvd   : 7511     Full Status Resp Rcvd   : 1252
Async Updates Rcvd    : 1        Error in FR header      : 0
Errors in LMI frame   : 0        Unknown LMI PDUs        : 0
Report Type IE miss   : 0        KeepAlive IE missing    : 0
KeepAlive Seq. Lost   : 0        Unknown IE type received: 0
Consecutive Positive  : 0        Consecutive Negative    : 0

----LMI Statistics for Network side Procedures-----
Status Enquiry Rcvd   : 7510     Full Status Enquiry Rcvd: 1252
Status Resp    sent   : 7512     Full Status Resp sent   : 1252
Async Updates sent    : 0        Error in FR header      : 0
Errors in LMI frame   : 0        Unknown LMI PDUs        : 0
Report Type IE miss   : 0        KeepAlive IE missing    : 0
KeepAlive Seq. Lost   : 0        Unknown IE type received: 0
Consecutive Positive  : 0        Consecutive Negative    : 0

----LMI Overall Statistics --------
Errors in FR Hdr      : 0        Invalid LMI information : 0
Unknown LMI frames    : 0        LMI frames   exceed MTU : 0
```

Interface type
LMI type
No errors reported
Shows responses sent to status enquiries received
Shows responses received for status enquiries sent

Frame Relay Configuration

This section summarizes how Frame Relay can be configured on the system, and provides background information for troubleshooting Frame Relay.

Basic Frame Relay configuration requires:

- Setting Frame Relay encapsulation on specified interfaces

  By default, the system sets the interface type to NNI and the LMI type to ANSI. You can change these values if needed.
- If you want to enable routing on an interface, configuring an IP address and network mask on the interface
- Defining the DLCIs for specified interfaces

Depending on the network configuration, the following may be enabled:

- Frame Relay routes
- Static ARP entries
- Frame Relay maps

► A Frame Relay DLCI supports either Frame Relay switching *or* Frame Relay routing. Frame Relay sub-interfaces support *only* routing. To allow routing and switching on a POS or serial interface, the subinterfaces are used exclusively for the routing and the main interface for switching. Lucent Technologies recommends that you configure an IP address for subinterfaces (for example pos2/0.1) but *not* for the main interface (for example pos2/0).

Basic Frame Relay Interface Configuration

The following example enables Frame Relay encapsulation on interface pos4/2 and sets the LMI type. It also sets the IP address and the map value for a sub-interface, and creates a DLCI:

```
TMX 880# configure terminal
TMX 880(config)# interface pos4/2
TMX 880(config-if)# encapsulation frame-relay
TMX 880(config-if)# frame-relay intf-type dce
TMX 880(config-if)# exit
TMX 880(config)# interface pos4/2.1 point-to-point
TMX 880(config-subif)# ip address 192.0.2.1 255.255.255.252
TMX 880(config-subif)# frame-relay map ip 192.0.24.2 17
TMX 880(config-subif)# exit
```

► If an interface type is configured to DTE or DCE, one end of a link must be configured to DTE and the other to DCE.

PVC Switching Example

The following example sets a static route for PVC switching:

```
TMX 880# configure terminal
TMX 880(config)# frame-relay switching
TMX 880(config)# interface pos5/6
TMX 880(config-if)# encapsulation frame-relay
TMX 880(config-if)# exit
TMX 880(config)# interface pos5/7
TMX 880(config-if)# encapsulation frame-relay
TMX 880(config-if)# exit
TMX 880(config)# frame-relay route pos5/6 16 pos5/7 16
```

Frame Relay Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with Frame Relay running on a system:

Table 6-1. Commands to Troubleshoot Frame Relay

To do this	Use this command
Set the country code (area code) and type of country code (cc or dcc) for an interface based on E164. The country code is passed to the end user when a DLCI goes inactive to locate exactly the position of the problem.	**frame-relay countrycode**
Set the network-id on the interface. The network ID is passed to the end user when a DLCI goes inactive to exactly locate the problem.	**frame-relay network-id**
Turn on or off debugging messages for the LMI protocol to view through the log utility. The debugging information provides a complete breakdown of the LMI protocol packets from the RCP.	**debug frame-relay lmi** **undebug frame-relay lmi**
Turn on or off debugging messages for permanent virtual circuits (PVCs).	**debug frame-relay pvc** **undebug frame-relay pvc**
View LMI statistics. When FRF2.1 is enabled, also view: • Enabled LAPF statistics • Set LAPF parameters • Set country code and network ID	**show frame-relay lmi**
View current map entries and related information.	**show frame-relay map**
View PVC statistics for Frame Relay interfaces.	**show frame-relay pvc**

Table 6-1. Commands to Troubleshoot Frame Relay

To do this	Use this command
When FRF2.1 is enabled on the interface, if the DLCI is inactive and if the inactive information is received for the DLCI, view: • The reason why the DLCI is inactive • The country code where the inactive information was generated • The ID of the network that generated the inactive information.	**show frame-relay pvc int interface-name dlci number**
View a summary of PVC information.	**show frame-relay pvc summary**
View all configured Frame Relay routes and their status.	**show frame-relay route**
View status of Frame Relay encapsulation on configured interfaces.	**show interfaces**

Troubleshooting Frame Relay

The most common causes of Frame Relay problems are:

- The line protocol is down on an interface that uses Frame Relay encapsulation.
- A Frame Relay interface cannot connect to a remote system.

Anytime you suspect a problem with Frame Relay encapsulation, you should view log messages using the **show logging** command. You should also enable debugging by using the **debug frame-relay lmi** or the **debug frame-relay pvc** command to make debugging messages available to you through the log utility. For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

If a Frame Relay link is down:

1. Check for configuration problems.

   Configuration problems can bring a line protocol down on an interface that uses Frame Relay encapsulation.

2. Evaluate connections to the remote system.

The following sections discuss the specific steps you take to isolate and remedy problems running Frame Relay on the system.

Configuration

A configuration problem, either on the local system, the remote router, or both can bring a line protocol down on an active interface using Frame Relay encapsulation.

The local and remote systems must have compatible settings for:

- CRC
- The interface type, NNI, DTE, or DCE — For NNI both sides of the link must use the same type. For DTE and DCE one side of the link must use DTE and the other DCE.
- LMI — The LMI type must be the same on the systems in a communication path to a remote router. ANSI is the default type on the TMX 880 MPLS Core Switch.

You begin troubleshooting the line protocol by evaluating interfaces and interface LMIs. If these two are not the source of the problem, you troubleshoot PVCs configured on the interface.

To troubleshoot a line protocol that is down:

1. Run the **show interfaces** command to verify that the protocol is down on an active interface that has Frame Relay encapsulation configured.

   The following example output shows that the line protocol (that is the LMI on interface pos4/2) is down:

```
pos4/2 is up, line protocol is down (ifindex is 41)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is pos4/2, Packet over SONET OC-3c
  MTU 4470 bytes, BW 150336 Kbit
  Encapsulation FRAME-RELAY, crc 16
```

2. Run the **show interfaces detail** command. If the output shows `Bad CRC,` check the values for the CRC set on the local and remote systems.

   For information about resetting the CRC, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

3. Run the **show frame-relay lmi** ***interface-name*** command to view statistics about the LMI for a system interface.

The command output provides general configuration information about a specified interface and displays Frame Relay statistics for that interface:

Interface type LMI type Auto detection of LMI type enabled

```
TMX 880# show frame-relay lmi pos4/2
Intf: pos4/2, Type: NNI, LMI: LMI-Ansi-D, Auto: Yes, Selected: None

FRF2.1: CountryCode Type: DCC    CountryCode Number    : 098
        National N/W Id : 123    Cisco Interoperability: ON

DTE: LMI Parameters: KeepAlive(t391): 10 secs, Poll.Cycl(n391): 6
                     Error Thold(n392): 3, Mon. Events(n393): 4

DCE: LMI Parameters: Poll Verification timer (t392): 15 secs
                     Error Thold(n392): 3, Mon. Events(n393): 4

----LMI Statistics for User side Procedures--------
Status Enquiry Sent   : 7510     Full Status Enquiry Sent: 1252
Status Resp    Rcvd   : 7511     Full Status Resp Rcvd   : 1252
Async Updates Rcvd    : 1        Error in FR header      : 0
Errors in LMI frame   : 0        Unknown LMI PDUs        : 0
Report Type IE miss   : 0        KeepAlive IE missing    : 0
KeepAlive Seq. Lost   : 0        Unknown IE type received: 0
Consecutive Positive  : 0        Consecutive Negative    : 0

----LMI Statistics for Network side Procedures-----
Status Enquiry Rcvd   : 7510     Full Status Enquiry Rcvd: 1252
Status Resp    sent   : 7512     Full Status Resp sent   : 1252
Async Updates sent    : 0        Error in FR header      : 0
Errors in LMI frame   : 0        Unknown LMI PDUs        : 0
Report Type IE miss   : 0        KeepAlive IE missing    : 0
KeepAlive Seq. Lost   : 0        Unknown IE type received: 0
Consecutive Positive  : 0        Consecutive Negative    : 0

----LMI Overall Statistics --------
Errors in FR Hdr      : 0        Invalid LMI information : 0
Unknown LMI frames    : 0        LMI frames   exceed MTU : 0
Status Enq Poll Excd  : 0        Enq. Poll rate insuffici: 0
Status for uncfg PVC  : 0        Unexpected PVC status IE: 0
```

For this type of command output	Do this
`LMI:` *type*	Determine the LMI type for system at the other end of the link, and make sure that the type is the same as the LMI type on the local system. **Note:** If the link is down, the LMI is down.

For this type of command output	Do this
`Type: type`	• For DCE or DTE, verify that one end of the interface runs DCE and the other end runs DTE. • For NNI, verify that both ends run NNI. Use the **frame-relay intf-type** command to set or change the setting for the TMX 880 MPLS Core Switch.

For a DTE or NNI interface, the system is not sending status enquiry messages:
`Status Enquiry Sent: 0`
or:
For a DTE or NNI interface, the system is not receiving status response messages:
`Status Resp Rcvd: 0`
or:
Keepalive messages are being lost:
`KeepAlive Seq. Lost: 0`
	1. Verify whether the interface is sending and receiving packets by running the **show interfaces *interface-name*** command.
	2. Run the **debug frame-relay lmi** command to enable LMI debugging, then review these messages for problem indicators.

Counters that display a value for any of the following output fields:
`Keepalive IE missing`
`Error in FR header`
`Unknown LMI frames`
`Invalid LMI information`
Values in these fields indicate Frame Relay corruption or a mismatched LMI type between the local and the remote system.
	Run the **debug frame-relay lmi** command to enable LMI debugging, then review these messages for problem indicators.

3. Run the **show frame-relay pvc summary** command to determine whether the DLCIs on the Frame Relay interfaces are active:

   - Review the list of DLCIs for each interface to make sure the settings are correct.
   - Review the list of DLCIs for each interface *on the remote system*, and verify if these settings are correct.

► Use the **frame-relay interface-dlci** command to configure or create a DLCI for a specified interface.

```
TMX 880# show frame-relay pvc summary
========= DLCI Summary For Interface pos4/2 =========

DLCI       State                opState    Type         Sub-Intf     Map-Class

----       -----                -------    ----         --------     ---------

0         Active               Up         LOCAL        none         default-control
1023      Active               Up         LOCAL        none         default-control
16        Active               Up         PPROUTED      pos4/2.16    default
```

These DLCIs are control DLCIs and therefore will always be active

For this type of command output	Do this
`State — Inactive` An inactive state indicates a communication problem between the TMX 880 system and another system or media in the PVC path.	Troubleshoot the systems from the local system to the next hop, then to the next hop and so forth: • Make sure the cabling and physical media is intact to the next system. • Make sure the router at the end of the hop is up and is correctly configured to run Frame Relay.
`opState — Down` The opState shows the status of the service adaptation (SA) task.	Verify that the path configuration for a PVC is correct.

`Type`
`Sub-Intf`
`Map-Class`
	Review these settings for each DLCI, and verify whether the settings are correct.
	If you need to change any of these values:
	• To assign a DLCI to a sub-interface, use the **frame-relay interface-dlci** command.
	• To change the map class, use the **frame-relay map** command.

Connections

Before you begin troubleshooting connections from a Frame Relay interface to another system, make sure that the line protocol for the interface is up and that Frame Relay is correctly configured, see “Configuration” on page 6-6.

Troubleshooting connections requires an understanding of how Frame Relay connections are configured among systems. Make sure that you are familiar with the network configuration.

The connection should be operational if the following conditions are met:

- The routers at either end of a link are up and correctly configured.

- The path between the two routers is correctly configured at each intervening switch.
- The links configured through the path are operational.

To troubleshoot Frame Relay connections:

1. Use the **ping** command to verify that the system can connect to the other router. If any connection problems exist, troubleshoot the network connection between the two systems. For information about troubleshooting IP, see Chapter 9, "Troubleshooting IP."

   Typically, the system sends packets to a specified address from a single interface. You can run the **show ip route** command to verify which interface sends packets to a destination IP address.

   If the interface cannot connect to the remote router, run the **show interfaces *interface-name*** command to make sure the interface is up and is sending and receiving packets. If the command output indicates a problem with the interface, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

2. Run the **show frame-relay pvc summary** command to evaluate the state of the DLCIs:

State should be Active and opState Up

```
TMX 880# show frame-relay pvc summary

========= DLCI Summary For Interface serial14/7 =========

DLCI       State                  opState    Type         Sub-Intf     Map-Class

----       -----                  -------    ----         --------     ---------


0         Active                Up        LOCAL       none         default-control
1023      Active                Up        LOCAL       none         default-control
900       Active                Up        LOCAL       none           default
200       Active                Up        PPROUTED    serial14/7.10 default
201       Active                Up         PPROUTED   serial14/7.11 default
========= DLCI Summary For Interface pos4/2 =========

DLCI       State                  opState    Type         Sub-Intf     Map-Class

----       -----                  -------    ----         --------     ---------


0         Active                Up        LOCAL       none         default-control
1023      Active                Up        LOCAL       none         default-control
16        Active                Up        PPROUTED    pos4/2.16     default
```

   For information about working with the command output, see step 3 on page 6-9.

3. Run the **show frame-relay pvc** command to make sure the interface is sending and receiving packets. If there is a problem with packet transmission, see "Frame Relay Configuration" on page 6-4.

4. If Frame Relay cross-connects are configured on the system, run the **show frame-relay route** command to verify configuration, and fix any errors that might exist.

The following example output shows bidirectional cross-connects:

```
TMX 880#  show frame-relay route

Input Intf      Input Dlci      Output Intf     Output Dlci  Status(->/<-)
----------      ----------      -----------     -----------  -------------

pos5/6          16               pos5/7          16           active(A/A)
pos5/7          16               pos5/6          16           active(A/A)
```

5. If the interface is using Frame Relay switching, verify routing information by running the **show frame-relay map** command, and fix any configuration errors that exist.

   The following example output shows entries in a Frame Relay map:

```
TMX 880# show frame-relay map
Host            Interface       DLCI     DLCI State      ARP Type
192.0.2.4       pos13/1.20      0160     ACTIVE          Static
192.0.2.8       pos13/1.19      0159     ACTIVE          Static
172.0.24.4      pos13/1.18      0158     ACTIVE          Static
192.0.24.8      pos13/1.17      0157     ACTIVE          Static
```

7

Troubleshooting PPP

This chapter describes the basic behavior for the Point to Point Protocol running on an interface, the configuration required to enable PPP on the system, and how to troubleshoot problems with PPP operation.

Before You Start

Before reading this chapter you should be sure that the POS and serial interfaces configured to use PPP are up. For information about system interfaces, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

Basic PPP Behavior

A system with POS and serial interfaces correctly running PPP has:

- The line protocol up on an interface that has PPP encapsulation enabled
- A link to another system from an interface configured to use PPP
- IP or IS-IS up on connections configured to use these protocols

Output from the **show interfaces** command verifies that PPP encapsulation is enabled on the appropriate interfaces, and that the interface is sending and receiving packets. If the line protocol is up and the interface is transmitting packets without error, PPP is functioning correctly on the interface.

Link Control Protocol is up

```
TMX 880# show interfaces
pos3/0 is up, line protocol is up (ifindex is 12)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is pos3/0, Packet over SONET OC-12c
       IP Address is 10.10.10.10, subnet mask is 255.255.255.0 (IP Cid
2)
  MTU 4470 bytes, BW 601334 Kbit
  Encapsulation PPP, crc 32
  Scramble on
  Interface up time 00:00:00
  Last input 10:50:57, output 00:00:21
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 8 bits/sec, 0 packets/sec
  Input: 0:99563 packets, 0:4974706 bytes, 0 errors, 0 drops
    Local input: 0:99549 packets, 0:4825778 bytes, 0 drops
    Local 5 minute input rate 0 bits/sec, 0 packets/sec
  Output: 0:93409 packets, 0:3859896 bytes, 0 errors, 0 drops
    Local output: 0:93409 packets, 0:3859924 bytes
    Local 5 minute output rate 8 bits/sec, 0 packets/sec
```

Packets being transmitted without error

PPP encapsulation

If the link also uses a network protocol, the associated network control protocol must be up for the link to pass data or to route data.

If the interface has this configured	This PPP sub-protocol runs
An IP address or IP unnumbered	IPCP — Internet Protocol (version 4) Control Protocol
IS-IS	OSICP — OSI Control Protocol
MPLS	MPLSCP — MPLS Control Protocol

The output for the **show ppp** command shows output in the following form, where *protocol* is the network protocol — such as IPCP, for each network protocols that is up:

```
protocol FSM state=9(Opened), seenAck=1
```

PPP Link Establishment

Before you begin troubleshooting PPP, you should have an understanding of how PPP establishes a link. This information will help you interpret the output from the **show ppp** command — the primary command to troubleshoot PPP connectivity problems.

When PPP establishes a point-to-point link the Link Control Protocol (LCP) negotiates configuration options for the link with the remote system. When LCP successfully negotiates the set of options, the LCP layer is open as demonstrated by the line protocol for the interface being up. The LCP manages a link, including closing it.

Each network control protocol then negotiates the configuration options for the associated protocol. The network control protocol then manages the protocol on the link, for example and IPCP manages IP on the link.

The phases and states PPP transitions through when forming a link are consistent with those outlined in RFC 1661. Refer to this RFC for detailed information about PPP.

Link Phases

When PPP sets up a link, it progresses through specified phases. The following list summarizes the PPP link phases. Notice that phase 3 establishes the LCP link, and phase 6 the network control protocol link.

0 — Dead	Shows no link activity. This phase starts after disconnection and ends with link initialization.
1 — Initialize	Starts the connection process.
2 — Dormant	Waits for an indication that the physical layer is ready.
3 — Establish	Sets up configuration for the link through the LCP.
4 — Authenticate (optional)	Sets up link authentication if required.
5 — Callback (not supported)	
6 — Network	Sets up network configuration through IPCP, OSICP, and MPLSCP (if the associated protocols are configured on the interface).
7 — Terminate	LCP closes the link due to events such as an idle timeout, loss of carrier, or authentication failure.
8 — Holdoff	Waits for the peer to disconnect before proceeding to the Dead phase.

Connections States

As the link progresses through the various link phases described in the preceding section, each control protocol transitions through a series of connection states. The following list summarizes these states.

When reviewing this list, keep in mind that the connection states the system progresses through depends on which side sent the configuration request, and whether the link is opening or closing.

00 — Initial The protocol is not configured.

As such, this state does not appear in the output for the **show ppp** command.

01 — Starting The protocol is configured on the interface, and has started. The protocol is administratively open and is waiting for the physical layer to come up.

02 — Closed The physical link is up, but the protocol is not configured.

03 — Stopped The protocol encountered a failure situation, such as a the protocol not being configured on the other end of the link.

04 — Closing The protocol starts closing the link.

This is a transitory state. In most cases, you will not see this state in the output from the **show ppp** command.

05 — Stopping The protocol is waiting for confirmation from the remote system to terminate the link.

This is a transitory state. In most cases, you will not see this state in the output from the **show ppp** command.

06 — Request sent The protocol sent a configuration request and is waiting for a reply from the other side of the link.

07 — ACK received The protocol received a positive acknowledgment from the other end of the link indicating that the other side received a protocol configuration request.

08 — ACK sent The protocol acknowledged the receipt of a configuration request from the other end of the link.

09 — Opened The protocol is up and available for use.

PPP Configuration

This section summarizes basic PPP configuration on the system, and provides background information for troubleshooting PPP.

Basic PPP configuration requires:

- Setting PPP encapsulation on specified interfaces.
- Configuring an IP address and network mask on the interface, or setting the interface to IP unnumbered to transmit data on the route.

Basic PPP Interface Configuration Example

The following example enables PPP encapsulation on interface pos2/0 and specifies an IP address and netmask:

```
TMX 880# configure terminal
TMX 880(config)# interface pos2/0
TMX 880(config-if)# encapsulation ppp
TMX 880(config-if)# ip address 192.0.2.0 255.255.255.252
TMX 880(config-if)# exit
```

PPP with IS-IS Configuration Example

The following example enables PPP encapsulation on interface pos2/2, specifies an IP address and netmask, and enables IS-IS on the interface:

```
TMX 880# configure terminal
TMX 880(config)# interface pos2/2
TMX 880(config-if)# encapsulation ppp
TMX 880(config-if)# ip address 192.0.2.4 255.255.255.252
TMX 880(if-config)# ip router isis
TMX 880(config-if)# exit
```

PPP Troubleshooting Commands

The following table lists the commands you use to troubleshoot PPP on an operational interface:

Table 7-1. Commands to Troubleshoot PPP

To do this	Use this command
Turn on debugging messages for PPP. You can enable debug messages for LCP, network control protocols (IPCP, MPLSCP, OSICP, machine state, link layer management, and system information).	**debug ppp** **undebug ppp**
View configuration and status information for IP interfaces.	**show interfaces**
View PPP-related state information for interfaces configured to use PPP encapsulation.	**show ppp** ***interface-name***

Troubleshooting PPP

The most common PPP problems are:

- The line protocol is down on an interface that uses PPP encapsulation.
- A PPP link shows packet transmission errors.
- A PPP link alternating between an operational and non-operational state.

These problems can be caused by:

- Unsuccessful PPP option negotiation.
- PPP not configured or not configured correctly at the other end of the link.
- The CRC may not match on each end.
- An echo interval (keepalive) that is too short.

Anytime you suspect a problem with PPP, you should view log messages using the **show logging** command. You should also enable debugging by using one of the **debug ppp** commands to make debugging messages available to you through the log utility. You can enable debug messages for each of the different control protocols. For information about working with the log and debug utilities, see Chapter 2, “Reviewing System Messages.”

You troubleshoot PPP problems in the following order:

1. Identify LCP problems, and fix them to bring the line protocol (LCP) up.
2. After LCP is up, troubleshoot connectivity problems with IPCP.
3. After IPCP is up, troubleshoot problems with other network control protocols.

To troubleshoot PPP:

1. Run the **show interfaces** command to verify that the line protocol is down.

   If the line protocol is up and there are no input packet transmission problems, you should verify that IPCP and other network control protocols are open if the associated protocols are configured on the interface.

   Input packet errors or drops in the command output may indicate that the link is going up and down.

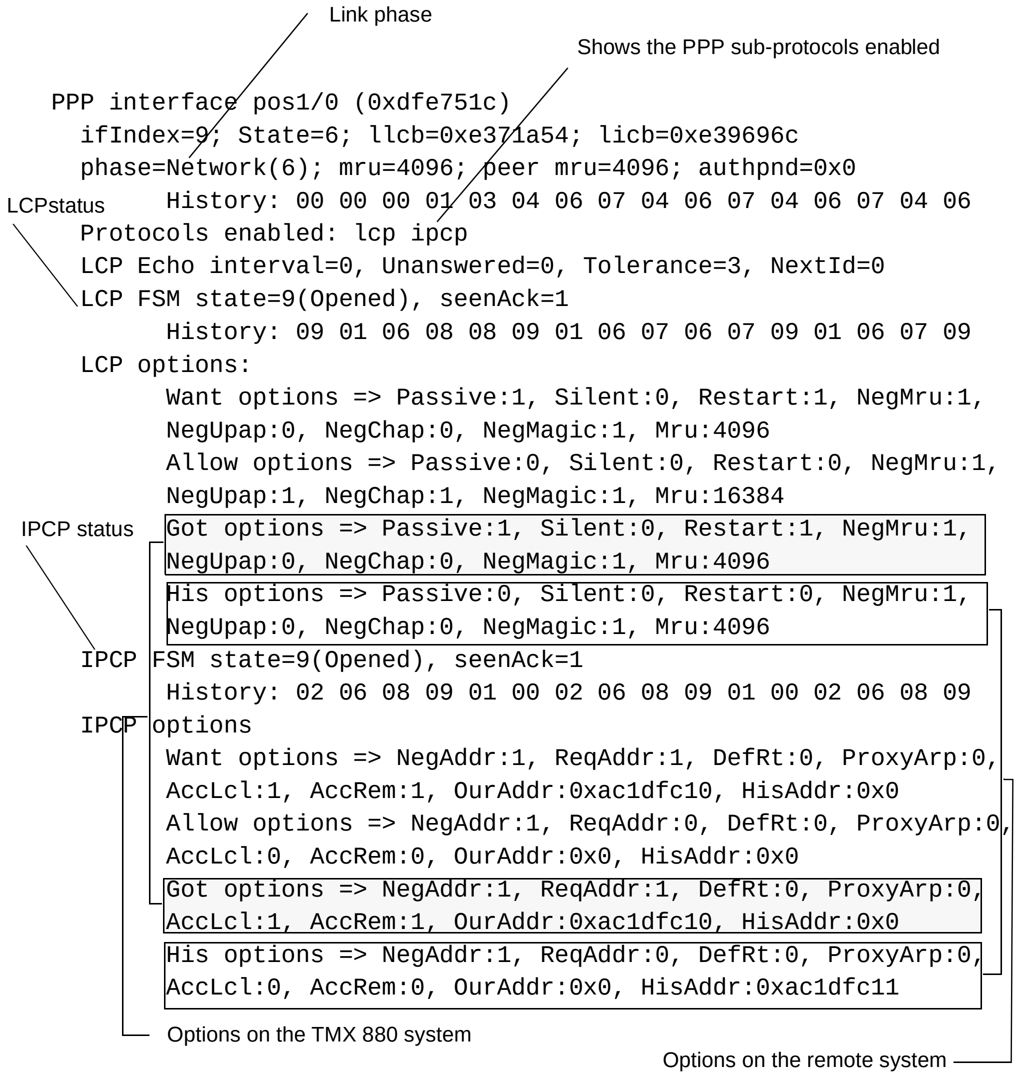
2. If the LCP is down, review the system messages stored in the system log utility to locate PPP messages for the interface such as:

   - Conditions that relate to the output of the **show interfaces** command
   - A configuration request that was rejected due to an unsupported option or unsupported protocol
   - An indication that the interface is going up and down. (In most instances this condition shows input packet errors in the output from the **show interfaces** command.)

   For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

3. Run the **show PPP** ***interface-name*** command to verify that LCP is open, and that IPCP and other network control protocols are open (if the associated network protocols are configured on the interface).

The following command output shows the status of LCP and IPCP for the interface. Sections for other network control protocols look similar to the one for IPCP.



```
PPP interface pos1/0 (0xdfe751c)
  ifIndex=9; State=6; llcb=0xe371a54; licb=0xe39696c
  phase=Network(6); mru=4096; peer mru=4096; authpnd=0x0
        History: 00 00 00 01 03 04 06 07 04 06 07 04 06 07 04 06
  Protocols enabled: lcp ipcp
  LCP Echo interval=0, Unanswered=0, Tolerance=3, NextId=0
  LCP FSM state=9(Opened), seenAck=1
        History: 09 01 06 08 08 09 01 06 07 06 07 09 01 06 07 09
  LCP options:
        Want options => Passive:1, Silent:0, Restart:1, NegMru:1,
        NegUpap:0, NegChap:0, NegMagic:1, Mru:4096
        Allow options => Passive:0, Silent:0, Restart:0, NegMru:1,
        NegUpap:1, NegChap:1, NegMagic:1, Mru:16384
        Got options => Passive:1, Silent:0, Restart:1, NegMru:1,
        NegUpap:0, NegChap:0, NegMagic:1, Mru:4096
        His options => Passive:0, Silent:0, Restart:0, NegMru:1,
        NegUpap:0, NegChap:0, NegMagic:1, Mru:4096
  IPCP FSM state=9(Opened), seenAck=1
        History: 02 06 08 09 01 00 02 06 08 09 01 00 02 06 08 09
  IPCP options
        Want options => NegAddr:1, ReqAddr:1, DefRt:0, ProxyArp:0,
        AccLcl:1, AccRem:1, OurAddr:0xac1dfc10, HisAddr:0x0
        Allow options => NegAddr:1, ReqAddr:0, DefRt:0, ProxyArp:0,
        AccLcl:0, AccRem:0, OurAddr:0x0, HisAddr:0x0
        Got options => NegAddr:1, ReqAddr:1, DefRt:0, ProxyArp:0,
        AccLcl:1, AccRem:1, OurAddr:0xac1dfc10, HisAddr:0x0
        His options => NegAddr:1, ReqAddr:0, DefRt:0, ProxyArp:0,
        AccLcl:0, AccRem:0, OurAddr:0x0, HisAddr:0xac1dfc11
```

Link phase
Shows the PPP sub-protocols enabled
LCPstatus
IPCP status
Options on the TMX 880 system
Options on the remote system

For this type of command output	Do this
For LCP	

`LCP FSM state =6` (or 7 or 8)	**1.** Make sure that the other side of the point-to-point link is correctly configured for PPP.
	2. Make sure the CRC value is the same at both ends of the link. Output from the **show interfaces details** command displays values for `Bad CRC` if the settings do not match.
	3. If the state remains in state 6, 7, or 8 for more than two minutes reset the link by shutting down then restarting an *interface*:
	– Use the **shutdown** command to shutdown a specified interface.
	– Then use the **no shutdown** command to restart the interface.
	– Run the **show ppp *interface-name*** command to verify that the protocol is up on the specified interface, and that the sub-protocols are open. For example:
	`LCP FSM state=9(Opened)`
	`IPCP FSM state=9(Opened)`

`LCP FSM state =3`	Make sure that the other side of the point-to-point link is correctly configured for PPP.
The values in: `History` bounce between states	Make sure that the link is not alternating between an operational and non-operational state: • Review the log messages to determine if the link is going up and down. • Review the output from the **show interfaces** command to see if there are input packet errors or drops. • Review the setting for the `LCP Echo interval` in the command output. The default value is 10 seconds. In some instances, you may need to increase this value. You use the **ppp echo-interval** command to do so.
A value greater than zero for: `LCP Echo Unanswered=` This output indicates the remote system is not acknowledging all packets.	

For this type of command output	Do this
For IPCP and other network control protocols	

`IPCP FSM state =3`
`OSICP` (or other network control protocol) `FSM state=3`
	Make sure that the protocol is correctly configured on the other side of the point-to-point link.

For IPCP	

`LCP FSM state=9 (Opened)`
AND
`IPCP` (or other network control protocol) `FSM state=6` (or 7 or 8)
	• **For IPCP only**:
	For interfaces on different subnets, verify that interfaces on both side of a PPP link are either numbered or unnumbered.
	On the TMX 880 MPLS Core Switch use the **ip unnumbered** command to establish an interface as unnumbered or the **ip address** command to assign an IP address to the interface.
	• **For all network control protocols:**
	If the state remains in 6, 7, or 8 for more than two minutes reset the link by shutting down then restarting an *interface*:
	– Use the **shutdown** command to shutdown a specified interface.
	– Then use the **no shutdown** command to restart the interface.
	– Run the **show ppp *interface-name*** command to verify that the protocol is up on the specified interface, and that the sub-protocols are open. For example:
	`LCP FSM state=9(Opened)`
	`IPCP FSM state=9(Opened)`

If after further debugging the protocol is still down and the configuration on the other side of the link is correct, you can try *reloading the card* using the **reload** command. For example to reload the IOP in slot 2:

```
TMX 880# cards
TMX 880(cards)# reload ioc 2
```

8

Troubleshooting ATM

This chapter describes the basic behavior for ATM running on the TMX 880 MPLS Core Switch, the configuration required to enable ATM on the system, and how to troubleshoot problems with ATM operation.

If you are troubleshooting ATM trunks running over MPLS, see Chapter 11, “Troubleshooting ATM Over MPLS”.

Before You Start

Before reading this chapter you should be sure that the interfaces configured to use ATM are up. When an ATM interface is up, the line protocol for the interface will also be up. For information about system interfaces, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

Basic ATM Behavior

A system with ATM interfaces correctly running ATM has:

- Each ATM interface and line protocol up
- ATM interfaces communicating with remote routers as configured

▶ For ATM, virtual circuits are typically configured on subinterfaces. Subinterfaces are logical interfaces on a physical port.

Output from the **show atm interfaces** and **show atm vc** commands provide information about the operating status of ATM interfaces.

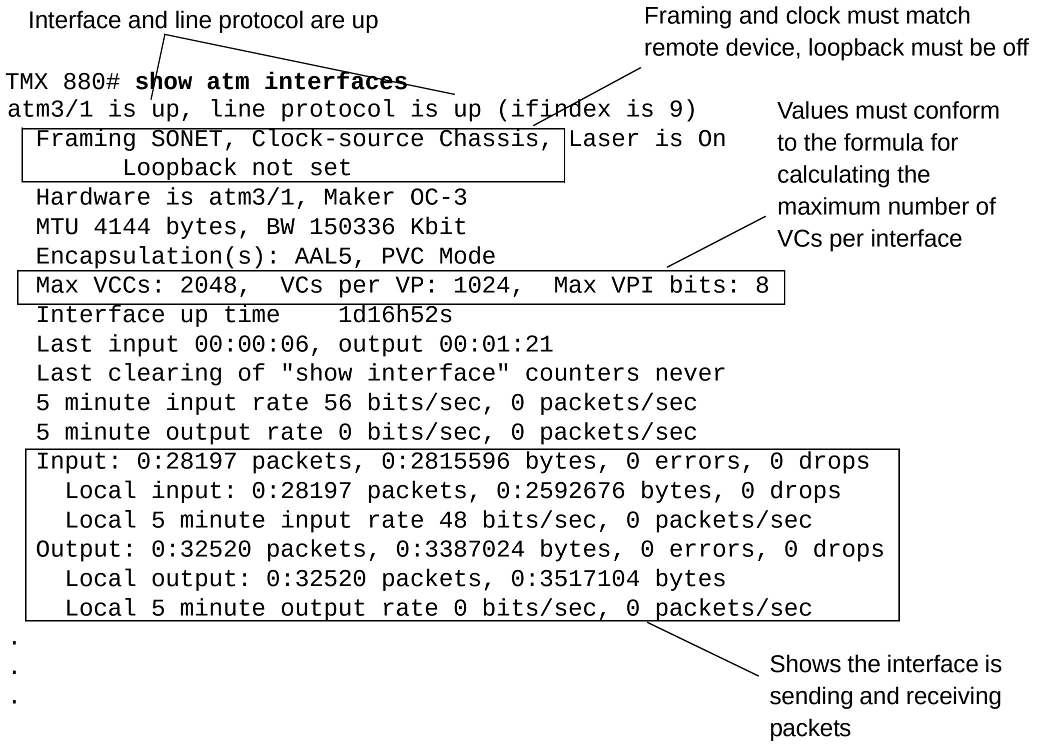
The **show atm interfaces** command shows whether:

- ATM is enabled on the appropriate interfaces
- Interfaces are sending and receiving packets

  When an interface is up, the system connects to the other end of the circuit.

  When the line protocol is up, the ATM configuration is correct and matches as needed with that at the other end of the circuit. If the line protocol is down, the configuration is incorrect, or the necessary parameters do not match the remote device, or both.
- The number of virtual paths (VPs) and virtual circuits (VCs) are within range allowed by the maximum number of virtual circuits for the interface

The following example shows output from one ATM interface:



Interface and line protocol are up

Framing and clock must match remote device, loopback must be off

Values must conform to the formula for calculating the maximum number of VCs per interface

Shows the interface is sending and receiving packets

```
TMX 880# show atm interfaces
atm3/1 is up, line protocol is up (ifindex is 9)
  Framing SONET, Clock-source Chassis, Laser is On
        Loopback not set
  Hardware is atm3/1, Maker OC-3
  MTU 4144 bytes, BW 150336 Kbit
  Encapsulation(s): AAL5, PVC Mode
  Max VCCs: 2048,  VCs per VP: 1024,  Max VPI bits: 8
  Interface up time    1d16h52s
  Last input 00:00:06, output 00:01:21
  Last clearing of "show interface" counters never
  5 minute input rate 56 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  Input: 0:28197 packets, 0:2815596 bytes, 0 errors, 0 drops
    Local input: 0:28197 packets, 0:2592676 bytes, 0 drops
    Local 5 minute input rate 48 bits/sec, 0 packets/sec
  Output: 0:32520 packets, 0:3387024 bytes, 0 errors, 0 drops
    Local output: 0:32520 packets, 0:3517104 bytes
    Local 5 minute output rate 0 bits/sec, 0 packets/sec
.
.
.
```

The **show atm vc** command displays the status of interfaces configured to use ATM.

Interfaces with a status of ACTIVE are operational on the system although they may not be passing traffic.

```
TMX 880# show atm vc
                               AAL/              Peak    Avg.   Burst
Interface      VCD  VPI  VCI  Encapsulation    Kbps    Kbps   cells Status
atm3/1.1         3    1   46  AAL5-SNAP           0       0       0 ACTIVE
atm3/2.1         4    1   47  AAL5-SNAP           0       0       0 ACTIVE
atm3/6.1         5    1   74  AAL5-SNAP           0       0       0 ACTIVE
atm3/6.13       24    0   47  AAL5-IP         15488       0       0 ACTIVE
```

An interface with a status of ENABLED indicates that the interface is configured and is administratively up, but is not available to traffic due to interface state or another physical problem.

ATM Configuration

This section summarizes how ATM should be configured on the system, and provides background information for troubleshooting ATM.

Basic ATM configuration requires:

- Specifying an IP address and netmask for an ATM interface (these must match the subnet and use the same netmask bounds as the peer router)
- Enabling ATM on an ATM interface by defining a permanent virtual circuit (PVC), configuring its virtual circuit descriptor (VCD) and virtual path identifier (VPI), virtual circuit identifier (VCI), and specifying an encapsulation type

► VCD is a system-specific term to refer to a VPI/VCI pair. ATM commands use this value. VCD is not an ATM Forum term.

- Defining a map-list, if needed
- Associating a map-list with an interface

► The TMX 880 system supports only IP and associated protocols over ATM.

The system requires aal5snap encapsulation for interfaces that run IS-IS or that use inverse ARP because both use non-IP frames.

Depending on the network configuration, the following may be set:

- Loopback mode for a specified interface
- A maximum number of VCs, and a corresponding number of VPIs and VCIs

Setting up VCs and VPs

You can use a VPI/VCI pair or a VCD only once on a physical port. The values set for VPIs and VCIs must:

- Conform to ATM Forum standards (to avoid network problems)
- Not conflict with combinations reserved by the ATM Forum
- Match at both ends of an ATM segment in order to establish a working connection

The number of VCs and VPs configured must also conform to the following formula:

(VCs per VP) x (VPs per interface) = Maximum total number of VCs per interface

Table 8-1 lists the values for **atm maxvc** and **atm vc-per-vp**, as well as the range of values for **atm maxvpi-bits**.

Table 8-1. VC and VP values

VC/VP Attribute	Set with this command	Values supported
Maximum number of VCs configured on an interface	**atm maxvc**	OC-3 default: 2048 OC-12 default: 8192 Value range: 16, 32, 64, 128, 256, 512, 1024, 2048 In addition on OC-12: 4096 and 8192
Range of VPIs that are available per interface	**atm maxvpi-bits**	The range is 0 to 8 bits, the default is 8, VPIs 0-255. 0 = VPI 0 1 = VPIs 0–1 2 = VPIs 0–3 3 = VPIs 0–7 4 = VPIs 0-15 5 = VPIs 0–31 6 = VPIs 0–63 7 = VPIs 0–127 8 = VPIs 0–255
Number of VCs that can use the same VPI number	**atm vc-per-vp**	OC-3 default: 1024 OC-12 default: 8192 Value range: 16, 32, 64, 128, 256, 512, 1024, 2048 In addition on OC-12: 4096 and 8192

For example, for an interface to support 256 VCs with an allowance of no more than 16-32 VCs per VP:

atm maxvc	=	**atm vc-per-vp**	x	number of VPs
256 VCs	=	16 VC\VP	x	16
256 VCs	=	32 VC\VP	x	8

In the second line of the example, **atm maxvpi-bits** set to 3 would limit the VPs to 0-7. If the interfaces uses the default value for **atm maxvpi-bits** (8), you can specify VPs of 0-255 but only a total of 8 VPs would be allowed from that range.

Configuration Examples

The following examples summarize basic ATM configurations on ATM interfaces.

Basic ATM Configuration

The following example enables ATM on the interface, creates a circuit, and sets the encapsulation type. It also associates the interface with a map group and map list:

```
TMX 880# configure terminal
TMX 880(config)# interface atm3/1.1 multipoint
TMX 880(config-if)# ip address 192.0.2.2 255.255.255.0
TMX 880(config-if)# atm pvc 4 1 46 aal5mux ip
TMX 880(config-if)# map-group gold
TMX 880(config-if)# exit
TMX 880(config)# map-list gold
TMX 880(map-list)# ip 192.0.2.4 atm-vc 4
TMX 880(map-list)# exit
```

► For smaller installations, a VCD should be unique within a TMX 880 system to avoid potential configuration problems. A VCD will equal a VPI/VCI pair in such cases. For large configurations, there should be a convention for re-use of VCDs.

VP/VC Configuration Example

This example shows interface atm 4/0 configured with the number of VPs and VCs within range for the 256 maximum number of circuits:

```
TMX 880# configure terminal
TMX 880(config)# interface atm4/0
TMX 880(config-if)# atm maxvc 256
TMX 880(config-if)# atm vc-per-vp 16
TMX 880(config-if)# atm maxvpi-bits 4
```

ATM with Inverse ARP Configuration Example

The following example enables ATM on the interface, creates a circuit, sets the encapsulation type, and inverse arp:

```
TMX 880# configure terminal
TMX 880(config)# interface atm3/6.1
TMX 880(config-if)# ip address 192.0.2.6 255.255.255.0
TMX 880(config-if)# atm pvc 5 1 74 aal5snap inarp 5
TMX 880(config-if)# exit
```

ATM Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with ATM running on a system:

Table 8-2. Commands to Troubleshoot ATM

To do this	Use this command
Enable or disable ATM ARP messages to be logged and displayed.	**debug atm arp** **undebug atm arp**
Set the severity level of the ATM messages, for either ATM interfaces or ATM VCs (virtual interfaces), sent to the logging utility. The **undebug atm errors** command returns the setting to the default of 3 (error-level logging).	**debug atm errors** **undebug atm errors**
Enable or disable the logging of protocol data units in packets that traverse a PVC. The first 88 bytes of each packet, including packet type, appears in hexadecimal format.	**debug atm packet** **undebug atm packet**
View the status of and summary information for ATM interfaces. View detailed interface statistics.	**show atm interfaces** **show atm interfaces details**
View the status and traffic data for interfaces configured to use ATM.	**show atm vc**
View a list of the IP address to VC mappings for the map lists configured on the system.	**show atm map**
View the system ARP table and check that addresses are correct and inverse ARP has set up properly.	**show ip arp**
Test connectivity to a remote system by sending an ICMP echo request.	**ping**

Anytime you suspect a problem with ATM, you should view the system messages stored in the system log utility. The **debug atm arp** command lets you receive ARP debugging messages. The **debug atm** errors command lets you set the severity level of messages logged for ATM interfaces or ATM VCs. For information about working with the log utility, see Chapter 2, "Reviewing System Messages."

► Interpreting the output for the **debug atm packets** command requires the expertise of qualified support or engineering personnel. The first 88 bytes of each packet, including packet type, are logged (or displayed) in hexadecimal format.

Troubleshooting ATM

The most common ATM problems are:

- Connectivity problems
- Inverse ARP issues
- Problems with amap list (a set of the static mappings)

Connectivity

A configuration problem on the TMX 880 system, on the remote router, or on both can disable communication between the two systems. Both the local and remote systems must have a PVC to the other system correctly configured. In addition, on the TMX 880 system the number of VCs and VPs set must conform to the formula discussed in "Setting up VCs and VPs" on page 8-3.

To troubleshoot connectivity:

1. Test the IP connectivity to the system at the other end of the link by using the **ping** command.
    - If the system receives an ICMP response to the **ping** command, the interface may have packet transmission problems. Run the **show atm interfaces details** command to view information about packet transmission on the interface.
    - If an interface had been up for some time and suddenly goes down, a problem most likely exists at the physical layer. For more information about troubleshooting at the physical layer, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
2. Run the **show atm vc** command to:
    - View if the interface is active.
    - Verify that the VCD, VPI, and VCI are correct for the interface.

```
TMX 880# show atm vc
                                AAL/              Peak    Avg.   Burst
Interface        VCD  VPI  VCI  Encapsulation     Kbps    Kbps   cells Status
atm3/1.1           3    1   46  AAL5-SNAP            0       0       0 ACTIVE
atm3/2.1           4    1   47  AAL5-SNAP            0       0       0 ACTIVE
atm3/6.1           5    1   74  AAL5-SNAP            0       0       0 ACTIVE
```

For this type of command output	Do this
`Status enabled` Indicates the circuit is administratively up, but down due to the interface state or other physical state.	**1.** Run the **show atm interfaces** command to make sure the interface is up. If the interface is not up, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols." **2.** Evaluate the number of VPIs and VCIs set, and make sure that the value of these two numbers multiplied together does not exceed the maximum number of VCs for the interface. If the VCs and VPs are configured after entering the **atm maxvc** command, the number should be within the acceptable range. The console displays a message if you try to configure VCs or VPs outside of the range. If, however, you have decreased the value of the **atm maxvc** after setting values for VPs and VCs, any of the VPs or VCs that fall outside the range will have a status of `ENABLED` and cannot be `ACTIVE`.
An interface does not have a `Status ACTIVE` within a few minutes	**1.** Verify the local VPI/VCI pair matches the remote VPI/VCI on the remote device. **2.** Verify that the encapsulation matches. **3.** Verify that the system at the other end of the link is operational.
`Status disabled` Indicates the interface is administratively down.	Identify why the interface was shutdown. Enable the interface when appropriate by running the **no shutdown** command.
`Status inactive` Indicates the circuit is administratively and operationally down.	Run the **show atm interfaces** command to make sure the interface is up. If the interface is not up, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

4. Verify that the netmask on the local interface is the same as used by other interfaces on the network.

Interfaces on the same network must use the same subnet mask. Packets are not routed correctly if different masks are configured.

5. Run the **show atm map** command to:

- Make sure that the IP address of the far-end mapping is correct for the specified VC.
- Make sure the VC is correctly specified.

You can change any incorrect mappings by using the **atm-vc** command.

The following example shows the IP address to VC mapping for the map lists `gold`, `silver`, and `bronze`:

```
TMX 880# show atm map
Map List gold:
      ip 192.0.2.6 maps to VC 3
      ip 192.0.2.10 maps to VC 4
Map List silver:
      ip 192.0.18.2 maps to VC 5
Map List bronze:
      ip 192.0.24.2 maps to VC 24
End of map-lists
```

6. Consider doing a shutdown of the suspect interface especially if there has been a succession of changes to its configuration.

   The **shutdown** command administratively disables the interface until you bring it back with a **no shutdown** command.

7. For an interface on a multimode ATM OC-3 card, make sure that the connectors are correctly attached.

To verify the appropriate number of VCs and VPs:

- Run the **show atm interfaces** command to verify the configuration for the number of VCs and VPs:

```
TMX 880# show atm interfaces atm4/0
atm4/0 is up, line protocol is up (ifindex is 124)
       •
       •
       •
Max VCCs: 256,  VCs per VP: 16,  Max VPI bits: 4
       •
       •
       •
```

For information about supported values for VCs and VPs, see “Setting up VCs and VPs.”

For information about interpreting the output for the **show atm interfaces** command, see “To troubleshoot connectivity:” on page 8-7.

Inverse ARP

Troubleshooting inverse ARP (address resolution protocol) relies on ARP messages for problem resolution. Reducing the interval between ARP messages makes it easier to capture messages that provide useful information for troubleshooting.

The default interval between ARP messages is 15 minutes. When troubleshooting ARP, consider reducing this interval to 2 to 3 minutes. Use the **atm pvc** command to change the ARP interval. For example, the following command sets the ARP interval to 2 minutes:

```
TMX 880# configure terminal
TMX 880(config)# interface atm14/1
TMX 880(config-if)# atm pvc 32 0 33 aal5snap inarp 2
TMX 880(config-if)#
```

To troubleshoot inverse ARP operations:

1. Run the **show atm vc** command to verify that all inverse ARP and IS-IS circuits use SNAP encapsulation.

```
TMX 880# show atm vc
                               AAL/             Peak    Avg.   Burst
Interface      VCD  VPI  VCI  Encapsulation    Kbps    Kbps   cells Status
atm3/1.1         3    1   46  AAL5-SNAP           0       0       0 ACTIVE
.
.
.
```

2. Run the **show ip arp** command to display the system ARP table to verify the destination addresses for the interfaces.

   The following example shows an ARP table with only ATM entries:

```
Host         Interface   MAC Address        Type   ARP Type          Age
-----------  ----------  ------------------ ----- ----------------- ---

172.12.0.21   atm12/0    0c:00:00:03:00:00  PTPT   Static
172.12.0.25   atm12/0    ff:ff:ff:ff:ff:ff  LAN    Local Broadcast
205.1.51.0    atm10/7.1  ff:ff:ff:ff:ff:ff  LAN    Local Broadcast
205.1.51.38   atm10/7.1  0a:07:00:01:00:00  PTPT   Local Pt-Pt
205.1.51.94   atm10/7.1  00:00:00:00:00:00  PTPT   Local
205.1.51.255  atm10/7.1  ff:ff:ff:ff:ff:ff  LAN    Local Broadcast
205.1.52.38   atm10/7.2  0a:07:00:09:00:00  PTPT   Dynamic Pt-Pt    355
205.1.52.94   atm10/7.2  00:00:00:00:00:00  PTPT   Local Pt-Pt
```

For this type of command output	Do this
The address of the remote system is in the ARP table	Troubleshoot IP. For information about troubleshooting IP, see Chapter 9, "Troubleshooting IP."
The address of the remote system is *not* in the ARP table	Update and view the ARP table: **1.** Run the **clear arp-cache** command to clear the ARP table. **2.** Run the **show ip arp** command while interfaces re-establish ARP to view the ARP table to see if expected addresses are still missing. This method has little if any effect on traffic unless there are large numbers of ARP circuits.

3. If you still do not see an entry listed, do the following:

   - Enable debug messages for ATM ARP.

     The **debug atm arp** command enables the logging of debug messages for ARP. You should activate debugging for the minimum amount of time required to retrieve the information you need to reduce the number of messages sent to the logging utility.

   - Run the **clear arp-cache** command to clear the ARP table.
   - Shutdown then restart the interface.
   - Turn the debugging off as soon as possible.

For example:

```
TMX 880# debug atm arp
TMX 880# clear arp-cache
TMX 880# configure terminal
TMX 880(config)# interface atm6/2
TMX 880(config-if)# shutdown
TMX 880(config-if)# no shutdown
```

As the interface becomes operational, the system generates messages:

```
2001-04-02 15:09:49    DEBUG SOURCE    ATM )              SLOT  RCP_1
IF_MGR: event PHY_ADMIN_UP in state PHY_DOWN, machine phyFsm10-07
.
.
.
2001-04-02 15:09:49    DEBUG SOURCE    ATM (tAtmVc)       SLOT  RCP_1
ATMARP: sent Inverse ARP request from IP port 25.3.3.96

2001-04-02 15:10:13    DEBUG SOURCE    ATM (tFpmData)     SLOT  RCP_1
ATMARP: received Inverse ARP request from IP 25.4.4.97 to 0.0.0.0
.
.
.
```

4. If the connection problem persists, remove (**no atm pvc**) and then recreate (**atm pvc**) the PVC.

   Recreating a PVC can correct a problem that does not have an obvious cause.

Map Lists

A map list is a set of the static mappings (associations) between upper-layer protocols (that is IP or ARP) and lower-level ATM VCs.

To troubleshoot map list and map group configuration:

1. Review assignment of map groups to appropriate interface.

   Make sure that each interface or subinterface has its own map list. Interfaces can not share lists.

2. Run the **show atm map** command to verify the correct map list is associated with each PVC.

   Verify that the list includes the PVCs running inverse ARP.

3. Run the **show atm vc** command to verify VCD values and assignments.

9

Troubleshooting IP

This chapter describes basic Internet Protocol (IP) connectivity on the system, and describes how to troubleshoot IP problems. IP connectivity is basic to the operation of the router. The system uses the IP addresses to connect to other routers and to forward packets. Any interface with a valid IP address can connect to another system over an open communication path.

Before You Start

Before reading this chapter you should be sure that:

- The management Ethernet interface and the system interfaces are up.

  For more information about system interfaces, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
- The line protocol is running on each interface.

Before you start troubleshooting IP, you should also have a good understanding of the network topology, and of the routing and multi-protocol label switching (MPLS) configuration on the system and on the network.

IP Connectivity

System interfaces use IP addresses with associated netmasks to communicate within the system and to communicate with other systems. An interface and the line protocol for the interface must be up for IP to be operational on the interface. Connectivity to another system then relies on:

- Routing configuration — the local system must have a route to the remote system
- Packet transmission on the system

  Output from the **ping** command demonstrates whether the IP link between an interface and another system, or interface on a router, is up.

► If MPLS is configured on the system, **ping** requests succeed only over paths that have an inbound label-switched path (LSP) and an outbound LSP configured on the same tunnel interface. For information about troubleshooting MPLS LSPs, see Chapter 10, "Troubleshooting MPLS."

IP Configuration

This section summarizes how IP should be configured on the system, and provides background information for troubleshooting IP.

During initial system configuration:

- An IP address is assigned to the management Ethernet interface to support management applications such as Telnet and SNMP.
- An IP address is assigned to system interfaces, or an interface is configured as ip unnumbered.

  IP addresses are also configured on tunnel interfaces for MPLS configurations.

IP Address Configuration Examples

The following example sets an IP address and netmask for the Ethernet port:

```
TMX 880# configure terminal
TMX 880(config)# interface ethernet 0
TMX 880(config-if)# ip address 192.2.0.1 255.255.255.0
```

The following example sets an IP address and netmask for interface pos2/0:

```
TMX 880# configure terminal
TMX 880(config)# interface pos2/0
TMX 880(config-if)# ip address 192.2.0.2 255.255.255.0
```

IP Unnumbered Configuration Example

The following example specifies a point-to-point interface as IP unnumbered. As such it borrows its IP address from a lender interface:

```
TMX 880# configure terminal
TMX 880(config)# interface pos2/0
TMX 880(config-if)# encapsulation ppp
TMX 880(config-if)# ip unnumbered loopback 0
```

IP Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with IP running on a system.

Table 9-1. Commands to Troubleshoot IP

To do this	Use this command
Verify network connectivity.	**ping**
Trace the route of a packet from the local system to a remote destination.	**traceroute**
Display the system access defined in an access list.	**show access-list**

Table 9-1. Commands to Troubleshoot IP

To do this	Use this command
View configuration and status information for IP interfaces.	**show ip interface**
View the contents of the IP address resolution protocol (ARP) table.	**show ip arp**
View the contents of the entire routing table. You can limit the information displayed by specifying an address or routing protocol as an argument.	**show ip route**
View summary information from the routing table sorted by protocol or type.	**show ip route summary**
View IP traffic statistics.	**show ip traffic**

▶ At this time the IP component does not send log messages to the logging utility.

Troubleshooting IP

Typically, the failure to receive responses to **ping** commands (sent to a remote system) identify problems with IP connectivity.

▶ MPLS LSPs have special configuration requirements for **ping** requests sent over an LSP to succeed. For information about troubleshooting MPLS, see Chapter 10, “Troubleshooting MPLS.”

The most common IP problems on an operational interface are:

- The IP address or mask on the TMX 880 MPLS Core Switch is not configured correctly.
- Misconfigured routing protocols or access lists on the system resulting in inability to connect to another router.
- Faulty configuration on another router for IP addresses, routing protocols, or access lists.

Management Ethernet Interface Connections

The management Ethernet interface supports Telnet and SNMP connections from remote systems. A Telnet session to the system gives you remote access to the CLI. The management Ethernet interface uses the global routing table.

To troubleshoot IP connections to and from the management Ethernet interface:

1. Verify that the management Ethernet interface can connect to the network by entering a **ping** command with the IP address of a remote system you know to be operational and reachable.

   ► The **ping** command has both a line mode and an interactive mode, see the *TMX 880 Command Reference* for more information about the command.

   For example, the following example input connects to the system 192.0.2.25:

   ```
   TMX 880# ping 192.0.2.25
   8 bytes from 192.0.2.25: icmp_seq=0, time=4 ms
   8 bytes from 192.0.2.25: icmp_seq=1, time=2 ms
   8 bytes from 192.0.2.25: icmp_seq=2, time=2 ms
   8 bytes from 192.0.2.25: icmp_seq=3, time=2 ms
   8 bytes from 192.0.2.25: icmp_seq=4, time=2 ms

   ----10.0.100.69 PING Statistics----
   5 packets transmitted, 5 packets received, 0% packet loss
   round-trip (ms)  min/avg/max = 2/2/4
   ```

   ► The IP address and netmask for the management Ethernet port can be set in boot parameters and in the configuration file. Make sure that these addresses are *different*.

   When 2 RCPs are installed on a TMX 880 system, the ethernet0 IP address on RCP0 and RCP1 cannot be the same IP address as `inet on Ethernet` in the boot parameters for RCP0 or RCP1. Otherwise the console displays a message similar to the following:

   ```
   0x2d10bc0 (tNetTask): duplicate IP address!! sent from
   ethernet address: 08:00:3e:2a:cc:9e
   ```

2. If the **ping** command does not receive an ICMP response from the remote system, run the **traceroute** command to determine the last hop from which the system receives a response.

   ► The **traceroute** command has both a line mode and an interactive mode, see the *TMX 880 Command Reference* for more information about the command.

   You can then troubleshoot the connectivity from the last system that sends a traceroute response, and the next system in the path.

3. If you do not receive a response to the **traceroute** command, run the **show ip interface** command to verify that the management Ethernet port has the correct IP address and netmask, and that the interface is up.

System Interface Connections

No ICMP responses to a **ping** command sent to a system known to be operational and reachable usually results from configuration errors, but can also result from a problem with traffic transmission within the system.

Configuration

Configuration limitations can block access between a system interface to a remote system:

- An access list on the local system may not permit access to traffic received from a remote IP address.
- An access list on the remote system may not permit access by the IP address set on the system interface.
- Routing configuration may prevent a packet from reaching its destination.

Typically, you should be able to send packets out of a correctly configured management Ethernet interface with the result that **ping** commands to known IP addresses succeed.

To troubleshoot configuration problems:

1. Run the **ping** command to test the connection to a reachable, operational, remote system from an interface suspected to have an IP connectivity problem.

   Typically, the system sends packets to a specified address from a single interface. You can run the **show ip route** command to verify which interface sends packets to a destination IP address.

2. Review the access list on the local and remote systems to verify system access. On a TMX 880 system, run the **show access-list** command to view system access lists.

   In the following example, access list 1 permits access from any system, and access list 10 specifically permits access to system *x*.100.3.0:

```
TMX 880# show access-list
Standard IP Access List 1
        permit any

Standard IP Access List 10
        permit 172.100.3.0, wildcard bits 0.255.255.255
```

3. Run the **show ip interface** command to verify:

- The interface is up.
- The IP address is correct.
- The netmask is correct.

```
TMX 880# show ip interface

IP Interface Table
IP Cid Address          Mask             Type     Interface Name       State
------ ---------------- ---------------- -------- -------------------- ----
  1    192.0.0.20       255.255.255.255 Loopback loopback0             UP
  2    10.0.101.20      255.255.0.0      LAN      ethernet0             UP
  3    192.0.2.1        255.255.255.0    Pt-Pt    pos2/0                UP
  4    192.0.24.1       255.255.255.0    Pt-Pt    pos11/0               UP
  5    10.7.7.1         255.255.255.0    Pt-Pt    pos7/0                UP
  6    10.6.6.1         255.255.255.0    Pt-Pt    pos6/0                UP
  7    192.0.24.1       255.255.255.0    Pt-Pt    pos6/1                UP
```

For this type of command output	Do this
Interface state is DOWN	For information about how to troubleshoot an interface that is down, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
Incorrect Address or Mask	Use the **ip address** command to change an IP address for an interface. **Note:** Interfaces on the same network must use the same subnet netmask. If interfaces have different subnet netmasks configured, packets are not routed correctly.

4. Run the **show ip arp** command to view the arp table for the system.

If the command output does not show entries you expect, the system is not receiving broadcasts from systems not listed.

```
TMX 880# show ip arp

  Host           Interface     MAC Address       Type     ARP Type         Age

  -------------- ------------- ----------------- -------- ---------------- ---

  4.4.4.1        pos4/0        00:00:00:00:00:00 PTPT     Local Pt-Pt
  4.4.4.2        pos4/0        00:00:00:00:00:00 PTPT     Static
  10.0.0.0       ethernet0     ff:ff:ff:ff:ff:ff LAN      Local Broadcast
  10.0.0.1       ethernet0     00:60:3e:5e:7c:01 LAN      Dynamic Router   360
  10.0.3.9       ethernet0     08:00:3e:2e:93:95 LAN      Dynamic          355
  10.0.180.4     ethernet0     08:00:3e:2f:60:d0 LAN      Local
  10.0.180.7     ethernet0     00:50:19:00:7b:00 LAN      Dynamic          355
  10.0.180.180   ethernet0     00:a0:cc:5d:cd:d5 LAN      Dynamic          357
  10.0.255.255   ethernet0     ff:ff:ff:ff:ff:ff LAN      Local Broadcast
  10.1.180.22    pos2/0        00:00:00:00:00:00 PTPT     Local Pt-Pt
  172.100.3.1    atm5/0.1      00:00:00:00:00:00 PTPT     Local Pt-Pt
```

5. Run the **show ip route summary** command to see which routing protocols the system uses and the types of routes in the routing table.
6. Run the **show ip route** command to display the entire routing table.

   Evaluate the command output to:

   - Look for expected routes that are missing from the routing table.
   - Determine which routing protocol you expect to supply those routes.
   - Troubleshoot the routing protocol that does not appear to supply missing routes.

To troubleshoot this protocol	See this chapter
IS-IS	Chapter 13, "Troubleshooting IS-IS"
OSPF	Chapter 14, "Troubleshooting OSPF"
BGP	Chapter 15, "Troubleshooting BGP"

Traffic Activity

If the IP address, netmask, and routing protocol(s) for the interface appear to be configured correctly, but the **ping** command continues to fail the system may have packet forwarding problems such as the following:

- The system does not receive the packet.
- The system does not send a packet.
- A packet does not reach the next hop in the path to the destination host.
- A packet does not reach the destination host.
- The system drops packets.

Any of these conditions can indicate a problem with:

- The underlying link-layer protocol
- The route control processor (RCP)
- The local processor (LP) on an IOP
- The Forwarding Engine on an IOP

The following procedures describe how to troubleshoot traffic transmission.

To evaluate IP traffic:

1. Run the **show ip traffic** command to view statistics for the IP traffic on the router, and review the command output for the following error conditions.

   - Packets not being forwarded
   - Error counters incrementing
   - Packets being discarded

```
TMX 880# show ip traffic

IP Stats
ipInReceives         6658  ipInHdrErrors        0
ipInAddrErrors       0     ipForwDatagrams      4036
ipInUnknownProtos    0     ipInDiscards         4048
ipInDelivers         2562  ipOutRequests        901
ipOutDiscards        0     ipOutNoRoutes        0
ipReasmTimeout       60    ipReasmReqds         0
ipReasmOKs           0     ipReasmFails         0
ipFragOKs            0     ipFragFails          0
ipFragCreates        0     ipRoutingDiscards    0
cidrcnt              5


ICMP Stats
icmpInMsgs           47     icmpInErrors         0
icmpInDestUnreachs   0      icmpInTimeExcds      0
icmpInParmProbs      0      icmpInSrcQuenchs     0
icmpInRedirects      0      icmpInEchos          19
icmpInEchoReps       0      icmpInTimestamps     0
icmpInTimestampReps  0      icmpInAddrMasks      0
icmpInAddrMaskReps   0      icmpOutMsgs          19
icmpOutErrors        0      icmpOutDestUnreachs  0
icmpOutTimeExcds     0      icmpOutParmProbs     0
icmpOutSrcQuenchs    0      icmpOutRedirects     0
icmpOutEchos         0      icmpOutEchoReps      19
icmpOutTimestamps    0      icmpOutTimestampReps 0
icmpOutAddrMasks     0      icmpOutAddrMaskReps  0


UDP Stats
udpInDatagrams       1108   udpNoPorts           825
udpInErrors          0      udpOutDatagrams      0

IP Multicast Stats
ipmcForwDatagrams    0      ipmcInDiscards       0
ipmcInReceives       0

ARP Stats
arpreqtx             42     arprsptx             5
arpreqrx             0      arprsprx             0

IP Security stats
spooferrs            0      decaperrs            0
autherrs             0      esperrs              0
```

2. If packets are not being forwarded, or are being dropped, you should examine quality of service configuration for the interface. Run the **show queue statistics** command to get information about transmission statistics for priority queues configured on an interface.
3. If the system is not transmitting IP packets acceptably, run the **show interfaces** command to look for packet transmission problems. For information about troubleshooting transmission problems over an interface, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols.".
4. Verify that the interface is sending **ping** requests:
   - Run the **show ip traffic** command, and note the number for `icmpOutEchos`.
   - Enter a **ping** command.
   - Run the **show ip traffic** command again to see whether or not the counter for `icmpOutEchos` increases.

   ▶ You can use the **clear counters** command to reset the counters.

   If the counter for the `icmpOutEchos` does not change, it indicates a problem at the RCP. For information about troubleshooting system cards, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
5. Verify that the interface is sending **traceroute** packets:
   - Run the **show ip traffic** command, and note the number for `icmpInTimeExcds`.
   - Enter a **traceroute** command.
   - Run the **show ip traffic** command again to see whether or not the counter for `icmpInTimeExcds` increases.

   If the counter for the `icmpInTimeExcds does` not change, it indicates a problem at the RCP. For information about troubleshooting system cards, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

10

Troubleshooting MPLS

This chapter describes the basic behavior for MPLS running on a TMX 880 MPLS Core Switch, gives an overview of the configuration required to enable MPLS on the system, and describes how to troubleshoot problems with MPLS operation.

Before Your Start

Before reading this chapter you should be sure that the physical interfaces configured to use MPLS are operational. MPLS runs over POS interfaces configured to use PPP encapsulation. For information about system interfaces, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

Basic MPLS Behavior

A system with MPLS running correctly has:

- Operational MPLS-enabled interfaces and tunnel interfaces
- MPLS paths being established
- MPLS forwarding traffic over established paths

The **show mpls lsps all** command provides an overview of LSP configuration on systems that originate and terminate LSPs. The **show mpls cross-connects** command displays information about LSP configuration on transit LSRs.

To verify MPLS configuration on ingress and egress LSRs:

- Run the **show mpls lsps all** command:

```
TMX 880# show mpls lsps all
MPLS LSP 10: tunnel10, (IfIndex is 111, XC Index is 4, Owner is rsvp)
        Initiating on pos13/0 with label 17
MPLS LSP 11: tunnel11, (IfIndex is 113, XC Index is 5, Owner is rsvp)
        Initiating on pos13/1 with label 17
MPLS LSP 10001: tunnel11, (IfIndex is 49, XC Index is 1, Owner is static)
        Initiating on pos2/0 with label 100
MPLS LSP 10002: tunnel11, (IfIndex is 49, XC Index is 2, Owner is static)
        Terminating on pos2/0 with label 100
```

To verify MPLS configuration on transit LSRs:

- Run the **show mpls cross-connects** command:

```
TMX 880# show mpls cross-connects
MPLS Cross Connect
Index     In-I/F        In-Label         Out-I/F        Out-Label       Owner COS
-----   ----------      --------        ----------      ---------       ----- -----
    6       pos2/0           400            pos4/0           500        static 33
```

MPLS Configuration

You can configure MPLS to use signaled or static label switched paths (LSPs). Signaled paths may use an explicitly defined path or a path set up by the Constrained Shortest Path First (CSPF). CSPF requires an underlying OSPF configuration. The CSPF algorithm works with OSFP to select a path that meets setup requirements configured for a path.

The following table shows the differences between the configuration required to set up the two types of paths.

Table 10-1. Configuration Differences Between Signaled and Static LSPs

Signaled Paths	Static Paths
Configure the full path on the ingress LSR.	Explicitly configure each hop from each LSR in the path.
Enable MPLS and RSVP-TE on all interfaces in the path. For paths calculated by CSPF, also enable OSPF-TE and set interface attributes on all interfaces in the path.	Enable MPLS on all interfaces in the path.
RSVP-TE sets up the path.	The ingress LSR initiates path setup using the configuration on each system in the path.

The examples in this section give a *brief overview* of LSP configuration. Typically, MPLS configurations provide two LSPs with the same end points. These LSPs transmits traffic in opposite directions. Although this configuration is often referred to as a “bidirectional” LSP, two LSPs establish the bidirectional flow of traffic.

The MXOS software relies on logical interfaces, called tunnel interfaces, to originate and terminate an LSP. Each tunnel interface binds to a physical interface to transmit traffic. For static paths, you configure the binding, for signaled paths, the software establishes this binding (you can also explicitly configure the binding).

Typically, MPLS LSPs are part of a routing scheme that uses an IGP to route traffic. Integrating LSPs with IS-IS or OSPF routing requires additional configuration not shown in this brief configuration overview. Configuration for MPLS fast reroute to set up full secondary paths and local detour paths is also not shown. For more detailed information about MPLS configuration, including IGP configuration and fast-reroute configuration, see the *TMX 880 Configuration Guide*.

Signaled LSP Configuration

On an ingress LSR you configure the parameters used to set up a signaled path. A signaled LSP can set up a path calculated by CSPF or use a specified explicit path. Using CSPF requires MPLS, RSVP-TE and OSPF-TE enabled on all system interfaces that a path traverses. Paths set up over an explicit path require only MPLS and RSVP-TE enabled on interfaces in the path.

CSPF also require that an OSPF area be configured before you set up paths. For information about basic OSPF configuration see Chapter 14, “Troubleshooting OSPF.” For complete configuration information for OSPF, see the *TMX 880 Configuration Guide*.

The following examples set up a signaled LSP that uses traffic engineering. The following figure shows the system interfaces for the MPLS LSP:

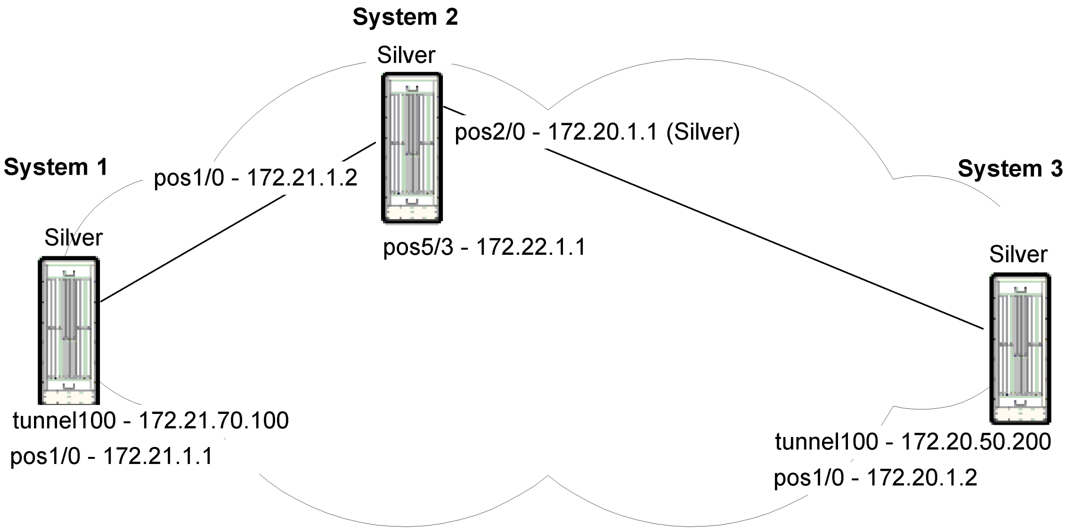


Figure 10-1. Signaled LSP Example Configuration

Signaled LSP Origination and Termination Example

To set up a bidirectional LSP, the configuration on the ingress LSR and the egress LSR is similar. The following examples show the configuration for System 1. The configuration for System 3 would be the same, with the exception of the system interfaces and associated IP addresses.

The following example sets up Silver as a color group on the system then configures a profile, named profile1. RSVP-TE uses the profile to set up an associated LSP.

```
System1(config)# color-group Silver 1

System1(config)# label-switched-profile rsvp-te profile1
System1(config-lsp-profile)# cspf max-delay 20
System1(config-lsp-profile)# cspf link-include-any Silver
System1(config-lsp-profile)# bandwidth 200
```

The following example enables OSPF-TE on a router that also has OSPF configured:

```
System1# configure terminal
System1(config)# router ospf
System1(config-router)# te-enable
```

This example originates a signaled LSP on System 1 using the attributes set in profile1.

```
System1(config)# interface pos1/0
System1(config-if)# encapsulation ppp
System1(config-if)# ip address 172.21.1.1 255.255.255.0
System1(config-if)# mpls enable
System1(config-if)# rsvp enable
System1(config-if)# ip ospf te-enable
System1(config-if)# exit
System1(config)# interface tunnel100
System1(config-if)# ip address 172.21.70.100 255.255.255.255
System1(config-if)# tunnel mode mpls
System1(config-if)# tunnel destination 172.20.1.1
System1(config-if)# mpls lsp signal lspid 0 lsp-profile profile1 to
172.20.1.2
```

► The tunnel destination is the router ID for IP routing. For MPLS LPSs used to transport ATM OPTimum cell trunks, the tunnel destination is the IP address of the tunnel interface at the opposite end of the LSP.

Signaled LSP Cross-connect Example

Signaled LSPs with traffic engineering require that RSVP-TE, MPLS, and OSPF-TE be enabled on interfaces on the transit systems. The interfaces have the link color attribute set to Silver to conform to the requirement set in profile1. The following example shows the configuration on System 2. If the path traversed other transit systems, configuration on those systems would be similar to that on System 2.

```
System2(config)# color-group Silver 1

System2(config)# router ospf
System2(config-router)# te-enable

System2(config)# interface pos1/0
System2(config-if)# encapsulation ppp
```

```
System2(config-if)# ip address 172.21.1.2 255.255.255.0
System2(config-if)# mpls enable
System2(config-if)# rsvp enable
System2(config-if)# ip ospf te-enable
System2(config-if)# maximum-mpls-bandwidth 500
System2(config-if)# link-color Silver
System2(config-if)# exit
System2(config)# interface pos2/0
System2(config-if)# encapsulation ppp
System2(config-if)# ip address 172.20.1.1 255.255.255.0
System2(config-if)# mpls enable
System2(config-if)# rsvp enable
System2(config-if)# ip ospf te-enable
System2(config-if)# maximum-mpls-bandwidth 500
System2(config-if)# link-color Silver
```

Static LSP Configuration

Configuring a static LSP requires that you explicitly configure both end points, including the labels assigned. For each cross-connect you specify the interfaces used for the cross-connect and assign labels for each interface.

The examples for a static LSP use the configuration shown in the following figure:

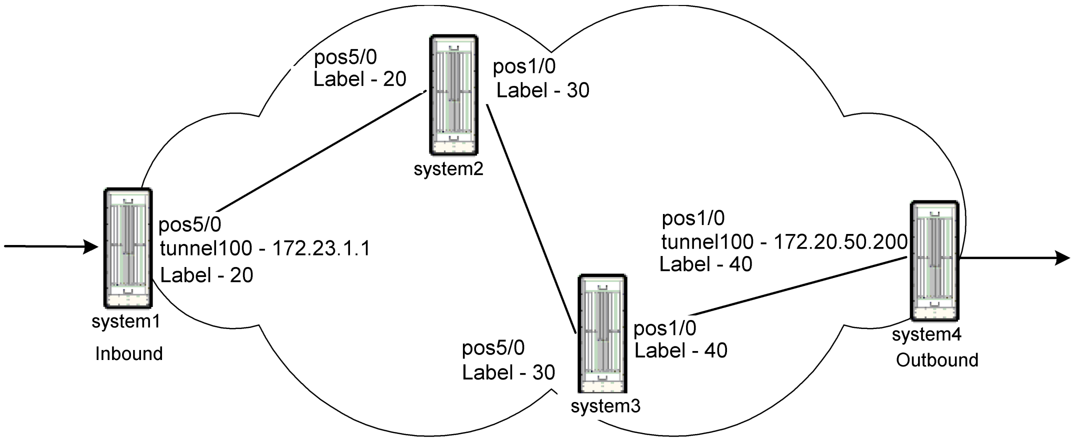


Figure 10-2. Static LSP Example Configuration

Static LSP Origination and Termination Examples

The following example configures a tunnel interface and binds it to a physical interface:

```
system1# configure terminal
system1(config)# interface pos5/0
system1(config-if)# encapsulation ppp
system1(config-if)# mpls enable
system1(config-if)# exit
system1(config)# interface tunnel100
system1(config-if)# ip address 172.23.1.1 255.255.255.255
system1(config-if)# tunnel mode mpls
system1(config-if)# tunnel bind pos5/0
```

The examples in this section require that a tunnel interface be configured and bound to a physical interface as described in the preceding example.

- The following command originates a *static LSP* with a label of 20 on a tunnel interface on an ingress LSR:

```
system1(config-if)# mpls lsp static ingress 20
system1(config-if)# exit
```

- The following syntax line terminates a *static LSP* with a label of 40 on a tunnel interface on an egress LSR.

```
system4(config-if)# mpls lsp static egress 40
system4(config-if)# exit
```

Static LSP Cross-connect Example

Static LSPs require explicit configuration of the cross-connect on a transit router. The following example shows the configuration of a static cross-connect from pos5/0 to pos1/0 LSP:

```
system2# configure terminal
system2(config)# interface pos5/0
system2(config-if)# encapsulation ppp
system2(config-if)# mpls enable
system2(config-if)# exit
system2(config)# interface pos1/0
system2(config-if)# encapsulation ppp
system2(config-if)# mpls enable
system2(config-if)# exit
system2(config)# mpls cross-connect pos5/0 20 pos1/0 30
system2(config)# exit
```

MPLS Troubleshooting Commands

The following table lists the commands you use to troubleshoot MPLS:

Table 10-2. Commands to Troubleshoot MPLS

To do this	On this type LSR	For this type LSP	Use this command
View the color, or administrative, groups configured on the system and the number of links using the group.	Ingress, egress, transit	Signaled	**show color-groups**
Verify network connectivity.	Ingress, egress for bidirectional LSP, that is an LSP that has the same end points	Signaled, static	**ping**

Table 10-2. Commands to Troubleshoot MPLS

To do this	On this type LSR	For this type LSP	Use this command
View interface configuration information for TE and bandwidth (including all bandwidth configurations).	Ingress, egress, transit	Signaled	**show bm-interface-info**
View traffic engineering database information specified.	Ingress, egress, transit	Signaled	**show ip ospf database te area**
View the list of interfaces that have OSPF-TE enabled.	Ingress, egress, transit	Signaled (CSPF-calculated path)	**show ip ospf interfaces**
View routing information for the system.	Ingress	Signaled, Static	**show ip route**
View information about the interfaces configured to form a cross-connect for an LSP.	Transit	Signaled, static	**show mpls cross-connects**
List information for incoming segments.	Egress, transit	Signaled, static	**show mpls in-segments**
View information for all interfaces on the system that have MPLS enabled.	Ingress, egress, transit	Signaled, static	**show mpls interfaces**
View information about each LSP that originates or terminates on this router.	Ingress, egress	Signaled, static	**show mpls lsps**
List information for outgoing segments.	Ingress, transit	Signaled, static	**show mpls out-segments**
View the list of interfaces that have RSVP-TE enabled.	Ingress, egress, transit	Signaled	**show rsvp interfaces**
View profile information for LSPs.	Ingress	Signaled	**show rsvp lsp-profiles**
View the status of signaled LSPs being set up by RSVP-TE.	Ingress, egress, transit	Signaled	**show rsvp session**

If you suspect a problem with MPLS, view messages stored in the system log utility for MPLS and for RSVP-TE and OSPF-TE (if appropriate). The Debug utility supports both RSVP-TE, and MPLS. For information about working with the log and debug utilities, see Chapter 2, "Reviewing System Messages."

Troubleshooting MPLS

The most common MPLS problems are:

- An IGP not routing traffic over an LSP
- An LSP that is not operational

These problems can be caused by

- Configuration errors
- Interfaces, configured to transmit MPLS traffic, that are not operational

If OSPF or IS-IS is not routing traffic over an LSP, you should troubleshoot the IGP configuration first, then troubleshoot the MPLS LSPs. To troubleshoot OSPF, see Chapter 14, "Troubleshooting OSPF." To troubleshoot IS-IS, see Chapter 13, "Troubleshooting IS-IS."

MPLS **show** commands provide information specific to static LSPs and signaled LSPs. The troubleshooting procedures you follow depends on which type of LSP you are troubleshooting. The commands you use also vary with the function of the LSR — one that originates an LSP, forms cross-connects, and/or terminates an LSP.

Viewing LSP Configuration for the System

Before you start troubleshooting LSPs, determine whether an LSP is signaled or static.

To view LSP configuration:

- Run the **show mpls lsps details** command to view configuration information for LSPs originating and terminating on the system.

To troubleshoot signaled LSPS, see "Troubleshooting MPLS Signaled LSPs" on page 10-8.

To troubleshoot static LSPs, see "Troubleshooting MPLS Static LSPs" on page 10-16.

Troubleshooting MPLS Signaled LSPs

You start troubleshooting a signaled LSP (that you suspect is not operational) from the system that originates the LSP.   The originating system provides the LSP setup configuration.

Before you start troubleshooting a signaled LSP, you should have available a topology map for the network MPLS configuration. With traffic engineered paths, many variables effect path setup such as bandwidth availability, transmission delay, and administrative groups.

To troubleshoot a signaled LSP:

1. If the LSP is bidirectional, run the **ping** command, specifying the IP address of the tunnel interface at the other end of the LSP as the destination.

   If the **ping** command shows connectivity between the two end points, the LSPs in each direction are operational.

2. If the **ping** command does not succeed

   or:

   If you are troubleshooting an LSP that is unidirectional:

   On the ingress LSR, run the **show rsvp session** command to view the status of signaled LSPs that traverse the system:

```
TMX 880# show rsvp session
MPLS Signaled Label Switch Path(s).

Sender          Receiver        TnlID   LspID   InLbl   OutLbl  LspStatus
-------------------------------------------------------------------------
192.141.141.1    31.31.31.2       140     0       0       33      Down
171.114.114.1    31.31.31.3       150     0       0       44      Up
```

3. If the LSP status is Down, run the command again, specifying the **details** argument for the specified tunnel to view configuration and profile information for the LSP:

```
TMX 880# show rsvp session details 140
MPLS Signaled Label Switch Path(s).
Sender         Receiver        TnlID   LspID   InLbl   OutLbl   LspStatus
-------------------------------------------------------------------------
192.141.141.1  31.31.31.2       140    0       0       17       Down
Profile and Bandwidth for this tunnel
-------------------------------------
Profile : profile1
Bandwidth : 15 bytes/sec
Explicit Path Hop List for this tunnel
--------------------------------------
1 : 200.10.1.6 /32 strict
2 : 200.10.1.5 /32 strict
3 : 200.10.2.2 /32 strict
4 : 200.12.21.2 /32 strict
Actual Path Hop List for this tunnel
------------------------------------
1 : 200.10.1.6 /32 loose
2 : 200.10.2.1 /32 loose
3 : 200.12.21.1 /32 loose
4 : 200.12.21.2 /32 loose
```

4. For detailed information for the profile, run the **show rsvp lsp-profiles** command.

```
TMX 880# show rsvp profiles
profile2:
        Explicit Path Id: 0
        Bandwidth: 50 Mbps
        Priority: 6
        Cspf: Enabled
                Max Delay: 0
                Include All Affinity: 0x0
                        Colors :
                Exclude All Affinity: 0x0
                        Colors :
                Include Any Affinity: 0x0
                        Colors :
                Include Hop List: 0
                Exclude Hop List: 0
        Fast Reroute by Detour LSPs: Enabled
                Hop Limit: 10
                Bandwidth: 20% (= 10 Mbps)
                Exclude Any Affinity: 0x0
                        Colors :
                Include Any Affinity: 0x0
                        Colors :
```

5. View LSP-related log messages at the errors (3) level.

   For information about using the log utility to set the log level and to view log messages for a module, see Chapter 2, “Reviewing System Messages.”

Working with Error Messages

RSVP returns error messages to the system initiating the LSP whenever RSVP cannot set up a path. The most common error conditions indicate that:

- RSVP cannot find a route to the destination
- There is no MPLS resource

The following table lists the steps to take for specified types of error messages:

Error message indicates this	Next steps
The LSP does not have a route to the LSP destination.	Run the **show ip route** command to show whether the specified system has a route to the destination. If the command output does not list a route using the tunnel interface, troubleshoot the routing configuration. On the TMX 880 MPLS Core Switch: • For static routes, troubleshoot the route configuration and the state of the remote interface. • For troubleshooting OSPF routes, see Chapter 14, “Troubleshooting OSPF.” • For troubleshooting IS-IS routes, see Chapter 13, “Troubleshooting IS-IS.”

Error message indicates this	Next steps
There is no MPLS resource This probably indicates that MPLS or RSVP-TE is not enabled on the router interface for a specified IP address.	**1.** Run the **show mpls interfaces** command to verify whether MPLS is enabled on the specified interface. To enable MPLS on an interface, use the **mpls enable** command. **2.** Run the **show rsvp interfaces** command to verify whether RSVP-TE is enabled on the specified interface. To enable RSVP-TE on an interface, use the **rsvp enable** command. **3.** For LSPs calculated by CSPF, run the **show ip ospf interfaces command** to verify whether OSPF-TE is enabled on the interface. To enable OSPFP-TE on an interface, use the **ip ospf te-enable** command. OSPF-TE must also be enabled on the router. Use the **te-enable** commands to enable OSPF-TE on the system.
• The path is being initialized RSVP-TE is setting up the LSP. The ingress LSR has not received a response from the downstream routers. A prolonged initialization time indicates a configuration problem (typically for a newly configured LSP). • A problem with the explicit route object (ERO). The ERO defines the addresses in the LSP. • An unrecognized address of the next hop in the path	**1.** Review the configuration as described in the section "Troubleshooting Path Configuration" on page 10-12. **2.** If the configuration is correct, and the associated interfaces operational, remove the path then reconfigure it. To remove the path, run the **no mpls signal lsp** command. **Note:** If troubleshooting systems in the path is time-consuming, remove the path configuration to prevent RSVP-TE from sending messages every 30 seconds to set up the path.
A path error or a reservation error	Remove the path then reconfigure it. To remove the path, run the **no mpls signal lsp** command.

► RSVP-TE sends path messages every 30 seconds to set up a path. It then sends refresh messages every 30 seconds to maintain the path.

If the path goes down, the ingress LSR receives messages that contain information about the problem.

You can use the **rsvp refresh-interval** command to increase the time between refresh messages.

Troubleshooting Path Configuration

Typically, signaled LSPs also use traffic engineering. In this case, there be may a configuration problem with:

- LSP profiles
- Interface resource configuration

Configuring traffic engineering across an MPLS domain requires coordination between the resource requirements for an LSP, and the interface resources available.

► For paths calculated by CSPF, troubleshoot OSPF before troubleshooting LSPS. For information about troubleshooting OSPF, see Chapter 14, “Troubleshooting OSPF.”

Configuration on the Ingress LSR

Most troubleshooting for signaled LSPs is done on the ingress LSR because this system signals path setup to other systems in the path.

To troubleshoot configuration on the ingress LSR:

1. Verify that MPLS, RSVP-TE, and OSPF-TE (for CSPF) are enabled on the interface initiating the LSP:

To verify that this component is enabled on an interface	Use this command
MPLS	**show mpls interfaces**
RSVP-TE	**show rsvp interfaces**
OSPF-TE	**show ip ospf interfaces**

2. Run the **show rsvp session details** command to identify the IP addresses being used to set up the LSP.

   If the profile references an explicit path, verify that the configuration for the explicit path is correct.

   ```
   TMX 880# show rsvp session details 140
   MPLS Signaled Label Switch Path(s).
   Sender         Receiver        TnlID   LspID   InLbl   OutLbl   LspStatus
   -------------------------------------------------------------------------
   192.141.141.1  31.31.31.2       140    0       0       17       Down
   Profile and Bandwidth for this tunnel
   -------------------------------------
   Profile : profile1
   Bandwidth : 15 bytes/sec
   Explicit Path Hop List for this tunnel
   --------------------------------------
   1 : 200.10.1.6 /32 strict
   2 : 200.10.1.5 /32 strict
   3 : 200.10.2.2 /32 strict
   4 : 200.12.21.2 /32 strict
   Actual Path Hop List for this tunnel
   ------------------------------------
   1 : 200.10.1.6 /32 loose
   2 : 200.10.2.1 /32 loose
   3 : 200.12.21.1 /32 loose
   4 : 200.12.21.2 /32 loose
   ```

3. Run the **show ip ospf database te link details** command to evaluate the parameters required top set up the path.

   For each IP address listed in the `Actual Path Hop List for this tunnel` section of the output from the **show rsvp session details** command, evaluate the interface settings and bandwidth. Note that the `TE metric` in the command output is either the link delay or the OSPF interface cost.

```
TMX 880# show ip ospf database te link details

                 OSPF Router with id (202.26.26.26)

                Opaque (Area Scope) Link States (Area 0.0.0.0)

LS age: 1297
Options: (No TOS-capabilities)
LS Type: Area Scope Opaque Links
Link State ID: 1.0.2.51
Advertising Router: 202.20.20.20
LS Seq Number: 0x80000037
Checksum: 0x5dd0
Length: 124
opaque type is link type
        Link type: point to point
        Link ID: 202.10.10.10
        Local IP: 200.10.1.2
        Remote IP: 200.10.1.1
        TE metric: 3
        Max bandwidth: 19375000.0 Bytes/sec (155 Mbits/sec)
        Max Reservable bandwidth: 9750000.0 Bytes/sec (78.0 Mbits/sec)
        Color: 4  <>

LS age: 1314
Options: (No TOS-capabilities)
LS Type: Area Scope Opaque Links
Link State ID: 1.0.2.52
Advertising Router: 202.20.20.20
LS Seq Number: 0x80000013
Checksum: 0x7bd1
Length: 124
opaque type is link type
        Link type: point to point
        Link ID: 202.10.10.10
        Local IP: 200.10.1.6
        Remote IP: 200.10.1.5
        TE metric: 1
        Max bandwidth: 19375000.0 Bytes/sec (155 Mbits/sec)
        Max Reservable bandwidth: 9750000.0 Bytes/sec (78.0 Mbits/sec)
        Color: 2  <>.
.
.
.
```

Link resource requirements

► The value for the reservable bandwidth changes in response to the links traversing the interface. Note the age of the link-state advertisement, the reservable bandwidth may be different from the value listed in the link state advertisement.

Troubleshooting Systems in a Path

If an error message indicates a problem with path setup, you troubleshoot each interface in the path starting with the downstream system adjacent to the ingress LSR. The **show rsvp session details** command run on the ingress LSR shows the IP addresses in the path that RSVP is trying to set up.

To evaluate configuration on each system in the path:

1. Run the **show ip interfaces** command to verify that the interface is up.

If an interface is not up, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

▶ If the LSP uses fast reroute, then RSVP-TE should set up a detour LSP if an interface is down.

2. Verify that MPLS, RSVP-TE, and OSPF-TE (for CSPF) are enabled on the interface initiating the LSP:

To verify that this component is enabled on an interface	Use this command
MPLS	**show mpls interfaces**
RSVP-TE	**show rsvp interfaces**
OSPF-TE	**show ip ospf interfaces**

3. For paths calculated by CSPF, run the **show color-groups** command to ensure that the system has the correct color groups configured.

4. Ensure that interfaces meets the resource requirements defined in the profile.

Run the **show bm-interface-info** command for each interface to review resource configuration and compare the interface configuration with the profile configuration on the ingress LSR (see “To troubleshoot configuration on the ingress LSR:” on page 10-12.

```
TMX 880# show bm-interface-info atm14/0

Interface Information on Interface (slot 14/port 0).

Link Color                              :
Link Delay                              :   0 us
Maximum Number of LSPs                  :   100
Number of LSPs                          :   4
Programmed Line Rate                    :   622 Mbps (100%)
Maximum MPLS Bandwidth                  :   0 Mbps
Scaling Factor                          :   100%
MPLS Bandwidth Allocation               :   0 Mbps
MPLS Reserved Bandwidth                 :   0 Mbps
MPLS Overbooked Bandwidth               :   0 Mbps
ATM Reserved Bandwidth                  :   0 Mbps
Queue Bandwidth Allocation              :  96 Mbps
```

5. Make any configuration changes needed.
6. If RSVP does not set up the path after you corrected interface configuration errors on one system, continue troubleshooting other interfaces in the path by following step 3 through step 5 above.

Troubleshooting MPLS Static LSPs

Static LSPs have each hop in the path explicitly configured. Before you start troubleshooting a static LSP, you should be familiar with the configured hops in the path.

For static LSPs, the label values are also explicitly configured. The outgoing label on an outgoing segment must be the same as the incoming label on the adjacent incoming segment for an LSP to be operational. The following illustration shows how label values are configured on adjacent LSRs:

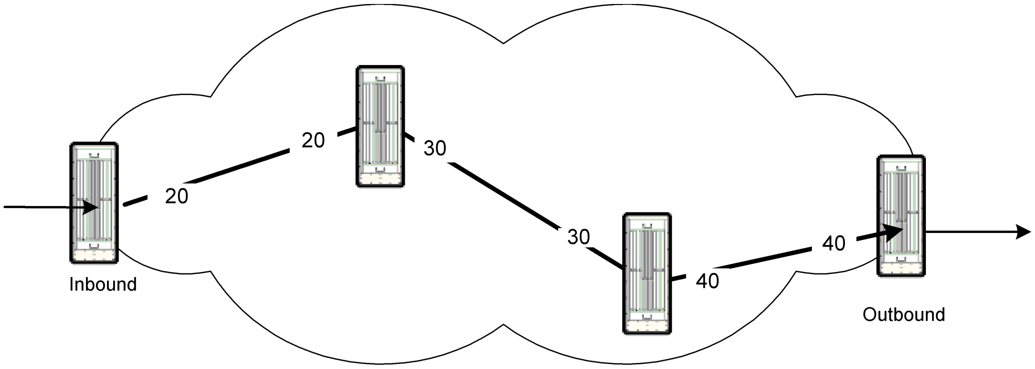


Figure 10-3. Label Values on an LSP

You start troubleshooting a static LSP from the ingress LSR, then troubleshoot subsequent systems in the path.

► If an LSP has the same end points, you can simultaneously troubleshoot the origination of one LSP and the termination of the associated LSP returning to the system.

To troubleshoot static LPSs on the ingress LSR:

1. If the LSP is bidirectional, run the **ping** command, specifying the IP address of the tunnel interface at the other end of the LSP as the destination.

   If the **ping** command shows connectivity between the two end points, the LSPs in each direction are operational.

   If the **ping** command does not succeed, or if you are troubleshooting an LSP that is not configured as bidirectional go to step 2.

2. Run the **show mpls lsps static** command and review configuration information for LSPs that originate (initiate) on the system.

   ► The output for the show mpls LSPs command displays information about LSP originating *and terminating* on the system.

   ```
   TMX 880# show mpls lsps static
   MPLS LSP 10001: tunnel11, (IfIndex is 49, XC Index is 1, Owner is static)
           Initiating on pos2/0 with label 100
   MPLS LSP 10002: tunnel11, (IfIndex is 49, XC Index is 2, Owner is static)
           Terminating on pos2/0 with label 100
   ```

   - If any configuration errors exist, correct them and go back to step 1.
   - Record the outgoing label value. You will need this value if you troubleshoot the next system in the path.

3. Run the **show mpls interfaces detail** command, and review statistics for packets transmitted by interfaces that have bindings to tunnel interfaces originating LSPs.

   ```
   TMX 880# show mpls interfaces detail

   pos1/0 (ifindex 6) has MPLS enabled
           MPLS Ingress: 0 labels in use,
           MPLS Egress:  0 labels in use, 0 packets, 0:0 bytes
             0 errors, 0 discards

   pos2/0 (ifindex 9) has MPLS enabled
           MPLS Ingress: 2 labels in use,
           MPLS Egress:  1 labels in use, 0 packets, 0:0 bytes
             0 errors, 0 discards

   pos4/0 (ifindex 52) has MPLS enabled
           MPLS Ingress: 0 labels in use,
           MPLS Egress:  1 labels in use, 3330344367 packets, 1:1221893472
                bytes
             0 errors, 0 discards
   ```

4. If the **show mpls interfaces detail** command shows the interface is not transmitting traffic, or is discarding packets, run the **show mpls out-segments static detail** command to determine if the interface is operationally and administratively up.

   ```
   TMX 880# show mpls out-segments static detail
   MPLS OutSegments
   ----------------
   OutSegment 1 with label 100 on interface pos2/0 (ifIndex 9) is UP
         MPLS traffic:  0 packets, 0:0 bytes, 0 errors, 0 packets discarded

   OutSegment 5 with label 500 on interface pos4/0 (ifIndex 52) is UP
         MPLS traffic:  3371924558 packets, 3:1280638608 bytes, 0 errors, 0
            packets discarded
   ```

   If an interface is operationally or administratively down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols” to get information about troubleshooting the interface.

To test connectivity to other interfaces in the route:

1. Make sure the LSP has a route to the interface that forwards traffic from the LSP by setting up a static route to that interface.

   For example, to set up a static route to a tunnel interface on the 10.10.10.10 subnet:

   ```
   TMX 880# ip route 10.10.10.0 255.255.255.255 tunnel 200
   ```

2. From the ingress LSR, run the **ping** command specifying the IP address of the tunnel interface that terminates the LSP:

   ```
   TMX 880# ping 10.10.10.3
   ```

   By default, the **ping** command sends 5 packets to the specified address.

3. Determine whether each interface in the path is receiving the ICMP echo request packets.

   On the TMX 880 MPLS Core Switch, the **show mpls interfaces** command shows packet statistics for an interface.

   The interface statistics should show the 5 packets sent by the **ping** command.

4. If an interface did not send the 5 ping packets, run the **show mpls out-segments static detail** command to determine if the interface is operationally and administratively up.

   ```
   TMX 880# show mpls out-segments static detail
   MPLS OutSegments
   ----------------
   OutSegment 1 with label 100 on interface pos2/0 (ifIndex 9) is UP
         MPLS traffic:  0 packets, 0:0 bytes, 0 errors, 0 packets discarded

   OutSegment 5 with label 500 on interface pos4/0 (ifIndex 52) is UP
         MPLS traffic:  3371924558 packets, 3:1280638608 bytes, 0 errors, 0
            packets discarded
   ```

   - Record the value of the label to compare this value with the value of the incoming label on the next LSR in the path.
   - If an interface is operationally or administratively down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols” to get information about troubleshooting the interface.

After you identify the system or interface where the LSP fails, you troubleshoot the configuration and connection status on that system. On transit LSRs, you verify the status of the two interfaces forming the cross connect.

To troubleshoot connection problems on a transit LSR:

1. Run the **show mpls cross-connects static** command to view the configuration for cross-connects on the system.

   ```
   TMX 880# show mpls cross-connects static
   MPLS Cross Connect
   Index     In-I/F        In-Label         Out-I/F        Out-Label       Owner COS
   -----   ----------      --------        ----------      ---------       ----- -----
       6       pos2/0           400            pos4/0           500        static 33
   ```

2. Run the **show mpls in-segments static** command to verify the status of the interface and value of the incoming label.
   - Compare the value of the label to the outgoing label on the upstream LSR to insure that the labels have the same value.
   - If an interface is operationally or administratively down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols” to get information about troubleshooting the interface.
3. Run the **show mpls out-segments static** command to verify the status of the interface and value of the outgoing label.
   - Record the value of the label to compare this value with the value of the incoming label on the next LSR in the path.
   - If an interface is operationally or administratively down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols” to get information about troubleshooting the interface.

11

Troubleshooting ATM Over MPLS

This chapter describes the basic behavior for ATM over MPLS running on the TMX 880 MPLS Core Switch, the configuration required to enable ATM on the system, and how to troubleshoot problems with ATM over MPLS operation.

ATM over MPLS enables you to create an MPLS network deploying the TMX 880 MPLS Core switches at the core of an existing ATM network of Lucent CBX 500® and GX 550TM switches. Lucent ATM OPTimum cell trunks connect CBX 550 and GX 500 switches, as well as the two GX 550 switches on each end of the MPLS domain. MPLS tunnels encapsulate incoming aggregated cell traffic for transport over high-speed POS links through the MPLS domain.

ATM to MPLS mapping greatly enhances the switching capacity of Lucent ATM networks by providing high bandwidth and transport speed at the MPLS core of the ATM network.

Before Your Start

Before reading this chapter be sure that:

- Interfaces configured to use ATM and MPLS are up

  When an ATM interface is up, the line protocol for the interface will also be up. You must also be sure that the physical interfaces configured to use MPLS are operational. MPLS runs over POS interfaces configured to use PPP encapsulation. For information about system interfaces, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

- LSPs are operational

  For information about troubleshooting MPLS LSPs, see Chapter 10, “Troubleshooting MPLS.”

Basic ATM Over MPLS Behavior

A system with ATM interfaces correctly running ATM has:

- ATM OPTimum cell trunk connections over an MPLS domain of TMX 880 MPLS Core switches.

- Label-switched paths (LSPs) and tunnel interfaces on the TMX 880 MPLS Core switches at the MPLS core.
- ATM-MPLS cross connects between ATM virtual paths (VPs) and MPLS Label Switched Paths (LSPs) for encapsulating and forwarding ATM OPTimum cell trunk traffic over the MPLS domain.

Output from the **show atm interfaces** command shows whether VP trunking is enabled on an interface. The following example shows output from one ATM interface:

```
TMX 880# show atm interfaces atm2/1
atm2/1 is up, line protocol is up (ifindex is 71)
  Framing SONET, Clock-source Line, Laser is On
        Loopback not set
  Hardware is atm2/1, Maker OC-12
  MTU 4144 bytes, BW 601334 Kbit
  VP Trunking enabled
  Max VCCs: 8192,  VCs per VP: 1024,  Max VPI bits: 8
  Max Vps: 14,  Control Vp Opened: 255
  Interface up time 16:36:54
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 1800 bits/sec, 4 packets/sec
  5 minute output rate 2240 bits/sec, 5 packets/sec
  Input: 0:260442 packets, 0:12501216 bytes, 0 errors, 0 drops
    Local input: 0:0 packets, 0:0 bytes, 0 drops
    Local 5 minute input rate 0 bits/sec, 0 packets/sec
  Output: 0:267079 packets, 0:13854512 bytes, 0 errors, 0 drops
    Local output: 0:0 packets, 0:0 bytes
    Local 5 minute output rate 0 bits/sec, 0 packets/sec
```

Interface and line protocol are up

VP trunking enabled

Output from the **show atm pvp** command provides information about all the permanent virtual path (PVP) trunking enabled on the interface.

```
TMX 880# show atm pvp
Interface     VPI     Service      CoS     Rate (Kbps)
---------     ---     -------      ---     -----------
   atm6/4       4        aal5      cbr           69903
   atm6/4       5        aal5      ubr               0
   atm6/6       1        aal5      ubr               0
   atm2/0       3        aal5      cbr          298714
   atm2/0       4        aal5      ubr               0
   atm2/1       2        cell      cbr          298714
   atm2/1       3        aal5      ubr               0
```

Interfaces enabled as PVPs

Service assigned to the PVP

Class of service assigned to the PVP

Output from the **show atm vp-trunking** command provides information all virtual path (VP) trunking enabled interfaces.

```
TMX 880# show atm vp-trunking
Interface     VP Trunk     VPI bits      # VPI's     # Xconnects
---------     --------     --------      -------     -----------
   atm6/4          yes            8            2               2
   atm6/6          yes            8            1               1
   atm2/0          yes            8            2               2
   atm2/1          yes            8            2               2
```

VP trunking status

Number of cross connects from this interface

Output from the **show atm xconnect** command provides information about all valid ATM PVP to MPLS tunnel cross connections and their current state.

```
TMX 880# show atm xconnect
Intf       Type         VPI       XC Type       Tunnel        XC        State
                                                 Name      Priority
-------   -------      -----      -------      -------    ---------    ------
 atm6/4    ATM_PVP       4         MPLS       tunnel700      6       ACTIVE
 atm6/4    ATM_PVP       5         MPLS       tunnel880      7       ACTIVE
 atm6/6    ATM_PVP       1         MPLS       tunnel710      7       ACTIVE
 atm2/0    ATM_PVP       3         MPLS       tunnel9010     3       ACTIVE
 atm2/0    ATM_PVP       4         MPLS       tunnel9000     7       ACTIVE
 atm2/1    ATM_PVP       2         MPLS       tunnel800      1       ACTIVE
 atm2/1    ATM_PVP       3         MPLS       tunnel810      7       ACTIVE
```

Type of cross connection

Tunnel interface for the cross connect

ATM Over MPLS Configuration

ATM over MPLS enables you to create an MPLS network of TMX 880 switches at the core of an existing ATM network of Lucent CBX 500 and GX 550 Multiservice Wide Area Network (WAN) switches using Lucent ATM OPTimum cell trunks.

► Typically, you configure ATM over MPLS through Navis TMX 880 EMS. For information about configuring ATM over MPLS through the EMS, see *Navis TMX 880 Element Management System User's Guide*.

ATM Over MPLS Configuration Example

The following example sets up a VP trunk over the MPLS tunnel interface 100.

```
System1# configure terminal
System1(config)# interface atm10/0
System1(config-if)# atm vp-trunking
System1(config-if)# atm pvp 10 aal5 cbr 10000
System1(config-if)# atm xconnect vp 10 mpls tunnel100
```

ATM Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with ATM over MPLS running on a system:

Table 11-1. Commands to Troubleshoot ATM Over MPLS

To do this	Use this command
View all virtual paths (VPs).	**show atm pvp**
View the status of interfaces with VP trunking enabled.	**show atm vp-trunking**
View the status of all ATM to MPLS cross-connections.	**show atm xconnect**
View the status of and summary information for ATM interfaces. View detailed interface statistics.	**show atm interfaces** **show atm interfaces *interface-name* details**
Display information for all interfaces on the system that have MPLS enabled.	**show mpls interfaces**

Anytime you suspect a problem with ATM over MPLS, you should view the system messages stored in the system log utility. For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

Troubleshooting ATM over MPLS

The most common ATM over MPLS problems are:

- An MPLS LSP is not operational. For information about troubleshooting LSPs, see Chapter 10, “Troubleshooting MPLS”.
- A VCC or VPC is not operational. For information about VCCs and VPCs, see the *Navis TMX 880 Element Management System User’s Guide*.
- The OPTimum call trunk is not operational. For information about troubleshooting OPTimum cell trunks, see the *NavisCore Troubleshooting Guide*.

These problems can be caused by

- Configuration errors
- Interfaces, configured to transmit ATM over MPLS traffic, that are not operational

A configuration problem on the TMX 880 system, on the remote router, or on both can disable communication between the two systems. Both the local and remote systems must have a PVC to the other system correctly configured.

If an interface had been up for some time and suddenly goes down, a problem most likely exists at the physical layer. For more information about troubleshooting at the physical layer, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

To troubleshoot connectivity:

1. For information about interruption of Operations Administration and Maintenance (OAM) cells from NavisCore^{TM}, see the *NavisCore Troubleshooting Guide* for more information.

2. Run the **show atm interfaces** command to make sure the interface is up.

   If the interface is not up, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

3. Run the **show atm pvp** command to verify which interfaces are enabled for permanent virtual path (PVP) trunking.

```
TMX 880# show atm pvp
Interface     VPI     Service      CoS     Rate (Kbps)
---------     ---     -------      ---     -----------
   atm6/4       4        aal5      cbr           69903
   atm6/4       5        aal5      ubr               0
   atm6/6       1        aal5      ubr               0
   atm2/0       3        aal5      cbr          298714
   atm2/0       4        aal5      ubr               0
   atm2/1       2        cell      cbr          298714
   atm2/1       3        aal5      ubr               0
```

4. Run the **show atm vp-trunking** command to view all virtual path (VP) trunking enabled interfaces.

```
TMX 880# show atm vp-trunking
Interface     VP Trunk     VPI bits      # VPI's     # Xconnects
---------     --------     --------      -------     -----------
   atm6/4          yes            8            2               2
   atm6/6          yes            8            1               1
   atm2/0          yes            8            2               2
   atm2/1          yes            8            2               2
```

5. Run the **show atm xconnect** command to display all valid ATM PVP to MPLS tunnel cross connections and their current state.

```
TMX 880# show atm xconnect
Intf      Type      VPI    XC Type   Tunnel           XC        State
                                      Name        Priority
-------   -------   -----  -------   -------      ---------    ------
atm6/4    ATM_PVP   4      MPLS      tunnel700         6         ACTIVE
atm6/4    ATM_PVP   5      MPLS      tunnel880         7         ACTIVE
atm6/6    ATM_PVP   1      MPLS      tunnel710         7         ACTIVE
atm2/0    ATM_PVP   3      MPLS      tunnel9010        3         ACTIVE
atm2/0    ATM_PVP   4      MPLS      tunnel9000        7         ACTIVE
atm2/1    ATM_PVP   2      MPLS      tunnel800         1         ACTIVE
atm2/1    ATM_PVP   3      MPLS      tunnel810         7         ACTIVE
```

6. Run the **show mpls interface details** command to display all valid MPLS interfaces and their current status.

   If the interface is not up, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

7. Consider doing a shutdown of the suspect interface especially if there has been a succession of changes to its configuration.

   The **shutdown** command administratively disables the interface until you bring it back with a **no shutdown** command.

To verify the permanent virtual paths (PVPs) configured:

- Run the **show atm pvp** command to verify that PVPs were created.

To verify that VP trunking is enabled:

- Run the **show atm vp-trunking** command to verify that VP trunking is enabled.

To verify the ATM over MPLS cross connects:

- Run the **show atm xconnect** command to verify the cross connects are enabled.

12

Troubleshooting Internet Protocol (IP) Multicast

This chapter describes the basic behavior of Internet Protocol (IP) Multicast, hereafter referred to as Protocol Independent Multicast (PIM), running on the TMX 880 MPLS Core Switch, the configuration required to enable PIM on the system, and how to troubleshoot PIM problems.

Before You Start

Before reading this chapter you should be sure that the interfaces configured to use PIM are up, are running the associated line protocols, and are sending and receiving packets. For information about system interfaces, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols.".

Also verify that unicast routes are set up. These can include any of the following types of routes, alone or in combination with one another:

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)
- Static routes

Basic PIM Behavior

A system correctly running Protocol Independent Multicast (PIM) has:

- The PIM module installed and enabled
- Specified interfaces running the PIM protocol
- A configured bootstrap router (BSR)
- A configured rendezvous point (RP)
- PIM adding all expected routes to the routing table (Routes appear in the table only after the receivers and/or sources are active and sending traffic.)

Output from the **show ip pim summary** command shows whether PIM is running properly on the system. The command output provides a summary of the current status of all configured Protocol Independent Multicast (PIM) settings:

```
TMX 880# show ip pim summary
Candidate BSR Settings:
  Address:  172.100.4.1(atm1/4.1)
  Priority: 0     Hash Mask Len: 30
  Frag Tag: 28168
Candidate RP Settings:
  Address:  172.100.4.1(atm1/4.1)
  Priority:       0     Group List:     0
  Interval(secs): 60    Holdtime(secs): 150
Timer Settings (seconds):
  Join/Prune Interval:    60    Holdtime: 210
  State Refresh Interval: 0
Inter-Operation Settings:
  Register Checksum: standard
TMX 880#
```

This section shows BSR candidate settings

This section shows RP candidate settings

This section shows configured timer settings

This section shows configured operational settings

You must ensure that PIM is establishing neighbors and that there is at least one unicast method of routing up and running. The **show ip mroute** command shows the multicast routes.

```
TMX 880# show ip mroute summary
Flags: S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
       M - MSDP created entry

(*, 224.0.1.39), 00:01:51/00:00:00, RP 10.152.18.2, flags:   SC

(*, 225.55.55.55), 00:01:49/00:00:00, RP 10.152.18.2, flags: SC
  (172.100.1.2, 225.55.55.55), 00:03:20/00:03:26, flags:     SCFT
```

PIM Configuration

This section summarizes how PIM should be configured on the system, and provides background information for troubleshooting PIM. Basic PIM configuration requires:

- Ensuring the Protocol Independent Multicast (PIM) module is loaded on the system
- Enabling Internet Protocol (IP) Multicast routing
- Configuring a bootstrap router (BSR) and rendezvous point (RP)
- Configuring one or more interfaces to use PIM
- Configuring the system and enabling Internet Group Management Protocol (IGMP) and Multicast Source Discovery Protocol (MSDP) (IGMP and MSDP are enabled automatically with PIM.)

Verifying the PIM Module is Loaded

In most cases the PIM module is already loaded, but you should verify that the system has loaded it.

To verify that the PIM module is loaded:

- Run the **show modules** command, and look for output similar to the following:

  ```
  pim nxPim           active     MAY-04-2001 12:36:45
  ```

  Active indicates that the system loaded the PIM module `pim`.

If the module is not active (not loaded), you must load it.

To load the PIM module:

1. Load the module by entering the following commands:

   ```
   TMX 880# configure terminal
   TMX 880(config)# load pim
   ```

2. Run the **show modules** command to verify that the module is loaded.

Reviewing Basic PIM Configuration

Setting up PIM on a system requires the following:

- Configuring IP interfaces
- Enabling IP multicast routing
- Configuring global PIM parameters
- Enabling PIM on the required interfaces
- Configuring PIM interface parameters

PIM Configuration Example

The following example loads PIM, specifies PIM sparse mode, enables multicast routing, and designates a bootstrap router (BSR) and rendezvous point (RP):

```
TMX 8801# configure terminal
TMX 8801(config)# hostname TMX 8801
TMX 8801(config)# load pim
TMX 8801(config)# interface atm0/0.19 point-to-point
TMX 8801(config-if)# ip address 1.1.19.1 255.255.255.0
TMX 8801(config-if)# atm pvc 14 10 19 aal5snap inarp
TMX 8801(config-if)# exit
TMX 8801(config)# ip multicast-routing
TMX 8801(config)# ip pim bsr-candidate atm0/0.19 30 80
TMX 8801(config)# access-list 10 permit 224.1.1.1
TMX 8801(config)# ip pim rp-candidate atm0/0.19 group-list 10 60 50
TMX 8801(config)# interface atm0/0.19 point-to-point
TMX 8801(config-if)# ip pim sparse-mode
```

Bootstrap Router (BSR) Candidate Configuration

You must designate at least one router in the network as a Bootstrap Router candidate. It is recommended that you designate at least two routers as BSRs for redundancy. The following example designates the bootstrap router (BSR).

```
TMX 880# configure terminal
TMX 880(config)# ip multicast-routing
TMX 880(config)# ip pim bsr-candidate atm0/0.19 30 80
```

Rendezvous Point (RP) Candidate Configuration

You must designate at least one router in the network as a Rendezvous Point (RP) candidate. It is recommended that you designate at least two routers as RPs for redundancy. The following example designates a rendezvous point (RP).

```
TMX 880# configure terminal
TMX 880(config)# ip multicast-routing
TMX 880(config)# ip pim rp-candidate atm0/0.19 group-list 10 60 50
```

IGMP Configuration

The TMX 880 MPLS Core Switch automatically enables or disables IGMP when PIM is enabled or disabled on an interface. Normally, no additional configuration is required but you can modify the parameters to tune IGMP behavior.

MSDP Configuration

You enable MSDP by configuring an MSDP peer to the local router. You must configure Border Gateway Protocol (BGP) before enabling MSDP. MSDP is not required for PIM operation, but is used for sharing PIM information between autonomous systems (ASs).

You normally configure BSR borders when using MSDP. The BSRs send out information that the PIM enabled routers in the network use to locate RP candidates. MSDP is used to communicate between RPs.

MSDP Peer Configuration

The following example designates a peer and assigns a description to it:

```
TMX 880# configure terminal
TMX 880(config)# ip msdp peer 1.1.19.1 connect-source 1.14.2.1 remote-as 4
TMX 880(config)# ip msdp description 1.1.19.1 labrouter
```

Default MSDP Peer Configuration

An MSDP peer of the local router can also be a BGP peer. You must have already configured an MSDP peer to use it as the default MSDP peer. If you specify a standard access list, the peer will be a default peer only for the prefixes in the specified list.

```
TMX 880# configure terminal
TMX 880(config)# ip msdp default-peer 1.1.19.1 list 10
TMX 880(config)#
```

PIM Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with PIM running on a system.

Table 12-1. Commands to Troubleshoot PIM

To do this	Use this command
Display the contents of the IP fast switching cache.	**show ip mcache**
Display the contents of the IP multicast routing table.	**show ip mroute**
Display Bootstrap Router (BSR) information.	**show ip pim bsr-router**
Display interface information.	**show ip pim interface**
Display a list of the PIM neighbors.	**show ip pim neighbor**
Display active Rendezvous Points (RPs).	**show ip pim rp**
Display which Rendezvous Points (RP) are associated with a specified group.	**show ip pim rp-hash**
Display the details about the group prefixes of all of the candidate Rendezvous Points (RPs).	**show ip pim rp-set**
Display information regarding the configured shortest path source-tree (SPT) threshold.	**show ip pim spt-threshold**
Display a summary of the current status of all locally configured Protocol Independent Multicast (PIM) settings.	**show ip pim summary**
Verify that the PIM module is loaded.	**show modules**

Troubleshooting PIM

The most common PIM problems on an operational interface are:

- The protocol is not enabled on the system.
- The system is not configured correctly.
- The rendezvous point (RP) is not configured.
- The boot strap router (BSR) is not correctly configured.

If PIM is not running correctly on the system:

1. Verify IP connections.

   For information about troubleshooting IP connections, see Chapter 9, “Troubleshooting IP.”

2. Review log messages for PIM messages.

3. Check the PIM configuration on the system.
4. Verify that all routers agree on the same BSR and RP.
5. Verify connections to PIM neighbors.
6. Verify that all senders and receivers are configured and active.

Before evaluating other PIM problems, make sure that the basic PIM configuration on the system is correct.

To evaluate PIM configuration problems:

1. Run the **show ip pim interface** command to verify that the PIM protocol is enabled and configured with valid values for:
   - The system address
   - Interface name
   - Version and Mode

```
TMX 880# show ip pim interface
Address      Interface  Version/Mode   Nbr    Query    DR         Pri
                                       Count  Intvl
10.152.10.18   pos7/3     v2/Sparse     1      30      0.0.0.0       -
10.152.18.2    atm1/7.1   v2/Sparse     1      30      0.0.0.0       -
172.100.4.1    atm1/4.1   v2/Sparse     0      30      0.0.0.0       -
```

2. Run the **show ip pim summary** command to verify that a BSR and RP candidate are configured.

   If the TMX 880 system is correctly configured for PIM, the output for the command is similar to the following:

```
TMX 880# show ip pim summary
Candidate BSR Settings:
  Address:  172.100.4.1(atm1/4.1)
  Priority: 0     Hash Mask Len: 30
  Frag Tag: 28168
Candidate RP Settings:
  Address:  172.100.4.1(atm1/4.1)
  Priority:      0     Group List:     0
  Interval(secs): 60    Holdtime(secs): 150
Timer Settings (seconds):
  Join/Prune Interval:    60    Holdtime: 210
  State Refresh Interval: 0
Inter-Operation Settings:
  Register Checksum: standard
TMX 880#
```

This section shows BSR candidate settings

This section shows RP candidate settings

This section shows configured timer settings

This section shows configured operational settings

For this type of command output	Do this
Interface state is DOWN	For information about how to troubleshoot an interface that is down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

For this type of command output	Do this
The CLI displays the following message when you enter a PIM command: `<(Unknown option,? for list)>` This indicates that the PIM module is not enabled or is not loaded.	• Verify whether the PIM module is loaded. For information about how to verify whether the module is loaded and how to load the module, see "Verifying the PIM Module is Loaded" on page 12-3. • If the module is loaded, use the **ip multicast-routing** command to enable PIM on the system.
No items listed under `Interfaces supported by PIM` (indicating that none of the interfaces are configured to run PIM)	Run the **ip pim** command (at the `config-if` prompt) to enable PIM on the specified interface.
No bootstrap router (BSR) is configured	Run the show **ip pim bsr-router** command to verify whether the BSR is configured. Run the **ip pim bsr-candidate** command to configure the BSR candidate if none exists.
No rendezvous point (RP) is configured	Run the show **ip pim rp-set** command to verify whether an RP is configured. Run the **ip pim rp-candidate** command to configure the RP candidate if none exists.

3. Ensure that PIM is enabled on the interface.

   To enable PIM issue the **ip pim** interface command.

4. Ensure that IP Mulitcasting is enabled on the system. To enable IP Multicasting issue the **ip multicast-routing** global configuration command.

To troubleshoot Bootstrap Router (BSR) problems:

1. Run the **show ip pim summary** command to verify that a BSR candidate is configured.
2. Run the **show ip pim bsr-router** command to verify that a BSR is configured.

   The command output provides information about the BSR, the address, uptime and configured priority:

```
TMX 880# show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.100.4.1
  Uptime: 01:52:27, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:02 seconds
```

For this type of command output	Do this
`No BSR information displays, indicating that a BSR is not configured.`	Configure a BSR using the **ip pim bsr-candidate** command.

To troubleshoot Rendezvous (RP) problems:

1. Run the **show ip pim summary** command to verify that an RP candidate is configured.
2. Run the **show ip pim rp-set** command to verify that an RP is configured.

   The command output provides information about the RP, including the address, priority, uptime and the source the information comes from:

```
TMX 880# show ip pim rp-set
RP: 172.100.1.1, Priority: 0
  Info source: 172.100.4.1 via bootstrap
  Uptime: 03:25:26, Expires: 00:02:17, Holdtime: 00:02:30
  Is Candidate for:
    224.0.0.0/4

RP: 172.100.4.1, Priority: 0
  Info source: 172.100.4.1 via management
  Uptime: 02:00:48, Expires: 00:00:00, Holdtime: 00:02:30
  Is Candidate for:
    224.0.0.0/4
```

For this type of command output	Do this
`No RP information displays, indicating that an RP is not configured.`	Configure a BSR using the **ip pim rp-candidate** command.

IGMP Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with PIM running on a system.

Table 12-2. Commands to Troubleshoot IGMP

To do this	Use this command
Display IGMP multicast-related information about interfaces.	**show ip igmp interface**
Display the groups that have directly connected members that were learned via IGMP.	**show ip igmp groups**

Troubleshooting IGMP

The TMX 880 MPLS Core Switch automatically enables or disables IGMP when PIM is enabled or disabled on an interface. Normally, no additional configuration is required but you can modify the IGMP parameters in order to tune the behavior.

The most common IGMP problems are:

- IGMP is not enabled on the interface.
- IGMP group connections are lost.

If IGMP is not running correctly on the system:

1. Check the IGMP configuration on the system.
2. Verify the IGMP group connections.

Before evaluating other IGMP problems, make sure the basic IGMP configuration is correct.

To evaluate IGMP configuration problems:

1. Run the **show igmp interface** command to verify IGMP configuration on the interface:

```
TMX 880# show igmp interface
pos7/3 is up, line protocol is up (ifindex is 79)
  IGMP is enabled on this interface
  Query interval is 125 seconds
  Current IGMP version is 2
  Querying router is 10.152.10.7
  Query max. response time is 10.0 seconds
  Querier uptime is 00:00:04
  Querier expiry is 00:04:11
  Wrong version queries: 0
  Activity: 0 joins, 0 groups
  Robustness variable is 2
  Last member query response interval is 1.0 seconds
```

2. Run the **show igmp groups** command to display IGMP related information about groups:

```
TMX 880# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface           Uptime    Expires   Last Reporter
224.2.217.45     atm1/4.1            05:37:03  00:02:34  172.100.4.2
224.2.255.155    atm1/4.1            05:37:07  00:02:34  172.100.4.2
```

MSDP Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with MSDP:

Table 12-3. Commands to Troubleshoot MSDP

To do this	Use this command
Display the number of MSDP sources and groups originated in SA messages from each AS.	**show ip msdp count**
Display a list of local sources that are sending traffic and being announced in SA messages sent to other MSDP peers.	**show ip msdp local-sources**
Display detail information about the MSDP peer.	**show ip msdp peer**
Display the information stored in cache about MSDP peers.	**show ip msdp sa-cache**
Display a summary of the current status of all MSDP peers.	**show ip msdp summary**

Troubleshooting MSDP

The most common MSDP problems are:

- Peers are not correctly configured.
- Connections to peers are lost.

If MSDP is not running correctly on the system:

1. Check the MSDP configuration on the system.
2. Verify the peer connections.
3. Review log messages for MSDP messages.

Before evaluating other MSDP problems, make sure that the basic MSDP configuration on the system is correct.

To evaluate MSDP configuration problems:

1. Run the **show ip msdp summary** command to display a summary of the current status of all MSDP peers.

```
TMX 880# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS        State     Uptime/   Reset     Peer Name
                                  Downtime  Count
*1.4.67.8         0        Up     00:14:27     9      PeerToASN-300
L*6.0.1.1         0        Up     00:00:04     3
A*10.254.0.19     0        Up     02:09:16     1
```

2. Run the **show ip msdp count** command to display the number of MSDP sources and groups originated in SA messages from each AS:

```
TMX 880# show ip msdp count
   State per ASN Counters, <asn>: <#sources>/<# groups>
      Total entries: 3
      200:3/3
```

3. Run the **show ip msdp local-sources** command to display a list of local sources that are sending traffic and being announced in SA messages sent to other MSDP peers.

```
TMX 880# show ip msdp local-sources
MSDP Local-Sources - 3 entries
(4.4.6.2,192.0.4.1), RP 4.4.6.1, BGP/AS 200, 00:00:35/00:02:55
(4.4.6.2,192.0.4.2), RP 4.4.6.1, BGP/AS 200, 00:00:35/00:03:00 (Blocked)
(4.4.6.2,192.0.4.3), RP 4.4.6.1, BGP/AS 200, 00:00:35/00:03:00
```

4. Run the **show ip msdp peer** command to display detail information about the MSDP peer.

```
TMX 880# show ip msdp peer
MSDP Peer 4.4.3.3, AS 100
Description: PeerToASN-100
   Connection status:
      State: Up, Times Up: 1, Connection source: ethernet1 (4.4.3.5)
      Uptime(Downtime): 00:17:19, Messages sent/received: 24/18
      Output messages discarded: 0
   SA Filtering:
      Input (S,G) filter: none
      Input RP filter: none
      Output (S,G) filter: none
      Output RP filter: none
   SA Requests:
      Input filter: none
      Sending SA-Requests to peer: disabled
   Peer ttl threshold: 0
MSDP Peer 4.4.4.1, AS 200
Description:
   Connection status
   Connection status:
      State: Up, Times Up: 1, Connection source: ethernet3 (4.4.4.2)
      Uptime(Downtime): 00:18:23, Messages sent/received: 14/19
      Output messages discarded: 0
   SA Filtering:
      Input (S,G) filter: none
      Input RP filter: none
      Output (S,G) filter: none
      Output RP filter: none
   SA Requests:
      Input filter: none
      Sending SA-Requests to peer: disabled
   Peer ttl threshold: 0
```

5. Run the **show ip msdp sa-cache** command to display the information stored in cache about MSDP peers.

```
TMX 880# show ip msdp sa-cache
DP Source-Active Cache - 3 entries
(4.4.6.2,192.0.1.1), RP 4.4.6.1, BGP/AS 200, 00:07:25/00:01:05
(4.4.6.2,192.0.1.2), RP 4.4.6.1, BGP/AS 200, 00:07:20/00:01:05
(4.4.6.2,192.0.1.3), RP 4.4.6.1, BGP/AS 200, 00:07:20/00:01:05
TMX 880#
```

6. Run the **show ip pim rp-hash** command to verify that all TMX 880 systems agree which RP is active for a specified class D network.

13

Troubleshooting IS-IS

This chapter describes the basic behavior for IS-IS running on an TMX 880 MPLS Core Switch, the configuration required to enable IS-IS on the system, and how to troubleshoot IS-IS routing problems.

Before You Start

Before reading this chapter verify that the interfaces configured to use IS-IS and the associated line protocols for those interfaces are up, and that the interfaces are sending and receiving packets. For information about system interfaces, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

Basic IS-IS Behavior

A system correctly running IS-IS has:

- IS-IS enabled
- Specified interfaces running the IS-IS protocol, and forming adjacencies with other systems as configured
- IS-IS adding all expected routes to the routing table
- The system redistributing routes as specified

Output from the **show clns protocols** and **show ip route isis** commands shows whether IS-IS is running properly on the system. If the output from these commands shows that IS-IS is correctly configured and adding routes, you do not need to continue troubleshooting IS-IS, unless you see a problem with redistribution of routes.

The **show clns protocols** command shows whether IS-IS is running on the system.

The command output provides summary information such as configuration values, addresses, and routes:

System ID must be a value other than zero

```
TMX 880# show clns protocol
IS-IS Router:
  System Id: 2222.2222.2222  IS-Type: level-1-2
  Image built on Thu Nov  9 10:10:13 EST 2000 (Version B 1.6.0 (BL
69).^ISIS.^)
  Manual area address(es):
        47.0004.004D
  Routing for area address(es):
        47.0004.004D
  Interfaces supported by IS-IS:
        Port gigabitethernet8/1 - IP
  Summary address(es):
```

This section should show configured values

This section should show areas learned from another router

This section shows interfaces configured to run IS-IS

The **show ip route isis** command shows whether IS-IS is adding routes to the routing table.

In the command output `i` identifies the IS-IS routes:

```
TMX 880# show ip route isis
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       T - route in transitional state
  i L2 172.16.21.0/24 [110/20] via 172.16.55.111, 02:09:28,
gigabitethernet8/1
  i L2 172.16.22.0/24 [110/20] via 172.16.55.111, 02:09:28,
gigabitethernet8/1
```

IS-IS Configuration

This section summarizes how IS-IS should be configured on the system, and provides background information for troubleshooting IS-IS.

Basic IS-IS configuration requires:

- Ensuring the IS-IS module is loaded on the system
- Configuring the system, including setting the system id and area
- Configuring one or more interfaces to use IS-IS

Verifying the IS-IS Module is Loaded

In most cases the IS-IS module is already loaded, but you should verify that the system is loading it.

To verify if the IS-IS module is loaded:

- Run the **show modules** command, and look for output similar to the following:

  ```
  isi nxIsi          active     MAY-19-2001 19:43:06
  ```

  Active indicates that the system loaded the IS-IS module `isi`.

If the module is not active (not loaded), you must load it.

To load the IS-IS module:

1. Load the module by entering the following commands:

   ```
   TMX 880# configure terminal
   TMX 880(config)# load isi
   ```

2. Run the **show modules** command to verify that the module is loaded.

Reviewing Basic IS-IS Configuration

Setting up IS-IS requires configuring the following on the system:

- The network address and system ID
- IS-IS on an IP circuit
- IS-IS on a point-to-point circuit

Router IS-IS Configuration Example

The following example enables IS-IS, specifies a network entity title (net), and sets a loopback address (to support interoperability with BGP). In the net, the first 13 bytes are the area ID, the next 6 bytes are the system ID, the last byte is an entity ID. Note that all systems within an area must have the same area ID, but a system ID must be unique within an area. The entity ID is always 00. In this example the net is comprised of:

- Area ID — **47.0005.0102.0304.0000.0001.0001**
- System ID — **0200.6660.0304**
- Entity ID — **00**

```
TMX 880(config)# router isis
TMX 880(router-config)#
   net 47.0005.0102.0304.0000.0001.0001.0200.6660.0304.00
TMX 880(router-config)# passive loopback0
TMX 880(router-config)# exit
```

► Until the **net** command is used to enable ISIS, interface configurations are ignored.

IS-IS Interface Configuration Examples

The following example specifies an IP address for an interface; then enables IS-IS on the interface:

```
TMX 880(config)# interface ethernet1
TMX 880(if-config)# ip address 192.3.104.23 255.255.255.0
TMX 880(if-config)# ip router isis
TMX 880(if-config)# exit
```

The following example configures a gigabit Ethernet interface and enables IS-IS on it:

```
TMX 880(config)# interface gigabitethernet8/1
TMX 880(if-config)# ip address 192.3.104.23 255.255.255.0
TMX 880(if-config)# ip router isis
TMX 880(if-config)# exit
```

If you want to redistribute routes from another protocol, such as OSPF, into IS-IS you do so by running the **redistribute** command for IS-IS. If you are running IS-IS to provide routes for another protocol such as BGP, you may need to redistribute them into that protocol.

▶ IS-IS runs only on point-to-point or LAN circuits.

IS-IS Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with IS-IS running on a system:

Table 13-1. Commands to Troubleshoot IS-IS

To do this	Use this command
Turn on or off IS-IS debugging messages to view IS-IS debugging messages through the logging utility.	**debug isis** **undebug isis**
Verify that the IS-IS module is loaded.	**show modules**
Verify that the system is configured to redistribute routes.	**show running-config**
Verify that an interface is up and configured correctly.	**show clns interface *interface-name***
Verify that a peer is visible. View information about the state of adjacencies.	**show clns neighbors**
Verify detailed information about neighbors such as areas and IP addresses.	**show clns neighbors detail**
Verify that the IS-IS protocol is enabled and running on the system.	**show clns protocol**
View summary information for packets, including the numbers and types of packets sent and received.	**show clns traffic**

Table 13-1. Commands to Troubleshoot IS-IS

To do this	Use this command
Verify whether IS-IS is adding routes to the table. View data (from the routing table) about IS-IS routes.	**show ip route isis**
View information about link state packets for each circuit type (level).	**show isis database**
View detailed information from the link state database, such as learned area addresses and connected subnets.	**show isis database detail**

If you suspect a problem with IS-IS routing, you should view log messages using the **show logging** command, and enable debugging by using the **debug isis** command to make debugging messages available from the logging utility. See Chapter 2, "Reviewing System Messages."

Troubleshooting IS-IS

The most common causes of IS-IS problems are:

- The protocol is not enabled on the system.
- The TMX 880 system or a neighbor is not configured correctly.
- The system does not form an adjacency with another system.
- IS-IS is not adding routes to the routing table.
- The system is not redistributing routes correctly.

If IS-IS is not running correctly on the system:

1. Check the IS-IS configuration on the system.
2. Make sure IS-IS is forming adjacencies with other routers.
3. Look for routing problems (including redistribution of routes into IS-IS).

The following sections discuss the specific steps you take to isolate and remedy problems running IS-IS on the system.

Configuration

Before evaluating other IS-IS problems, make sure that the basic IS-IS configuration on the system is correct.

To evaluate IS-IS configuration problems:

- Run the **show clns protocol** command to verify that the IS-IS protocol is enabled and configured with valid values for:
  - The system id
  - A (manual) area shared with another system
  - One or more interfaces supporting IS-IS

If the TMX 880 system and the system at the other end are correctly configured and operational, the output for the command should list addresses learned from another system:

```
TMX 880# show clns protocol
IS-IS Router:
  System Id: 2222.2222.2222  IS-Type: level-1-2
  Image built on Thu Nov  9 10:10:13 EST 2000 (Version B 1.6.0 (BL
69).^ISIS.^)
  Manual area address(es):
        47.0004.004D
  Routing for area address(es):
        47.0004.004D
  Interfaces supported by IS-IS:
        Port gigabitethernet8/1 - IP
  Summary address(es):
```

Shows the system is learning addresses from a connected peer

For this type of command output	Do this
The CLI displays the following message when you enter an IS-IS command: `<(Unknown option, ? for list)>` This indicates that the IS-IS module is not enabled or is not loaded.	• Verify whether the IS-IS module is loaded. For information about how to verify whether the module is loaded and how to load the module, see "Verifying the IS-IS Module is Loaded" on page 13-3. • If the module is loaded, use the **router isis** command to enable IS-IS on the system; then the **net** command to set the system ID and area.
Missing or invalid System ID	Set the value using the **net** command.
Missing or invalid manual area address	Set the address using the **net** command. **Note:** The TMX 880 system and another system must share at least one area to establish an L1 adjacency.
Missing entries (adjacencies) under `Routing for area addresses`	Determine if the system is forming an adjacency. For information about how to troubleshoot adjacencies, see "Adjacencies" on page 13-7.
No items listed under `Interfaces supported by IS-IS` (indicating that none of the interfaces are configured to run IS-IS)	Run the **ip router isis** command (at the `config-if` prompt) to configure a specified interface.

Adjacencies

To exchange routing information with another IS-IS system, the TMX 880 MPLS Core Switch must form an adjacency with the other router. Forming an adjacency requires that both systems:

- Use the same circuit type.

  Although the systems could be configured with one using Level 1 (or Level 2), and the other using Level 1-2, it is advisable to configure both systems to use the same level.

- Have at least one area configured that is the same for L1 adjacencies.
- Use the same password (if any).

To troubleshoot adjacency problems:

1. If log-adjacency-changes is enabled on the system, review the log file to get information about the state of adjacencies.

   Entries in the log file have the following form:

   ```
   Adjacency to system-id (interface-name) Up, new adjacency
   Adjacency to system-id (interface-name) Down, hold time expired
   ```

2. Run the **show clns neighbors detail** command to verify that the system recognizes a connection to another router.

   The command output provides information about the state of neighbor adjacencies and how long they have been up:

   ```
   TMX 880# show clns neighbor detail
   System Id      Interface      SNPA           State  Holdtime Type Protocol
   1111.1111.1111 gigabitethernet8/10060.1D28.C843  Up     26      L1L2 IS-IS
     Area Address(es): 47.0004.004D
     IP Address: 172.16.55.111
     Uptime: 00:59:07
   ```

For this type of command output	Do this
A peer is not listed in the list of system IDs, indicating the system does not have an adjacency with that router.	Proceed to the next step.

For this type of command output	Do this
`Type`	Make sure the circuit type is compatible between the two systems. The **show clns protocol** command provides this information for the system. For example: `System Id: 6666.6666.6666  IS-Type: level-1-2` To change the level, use the **is-type** command. **Note:** The TMX 880 system establishes a Level 1 adjacency if there is at least one common area address with a neighbor. Otherwise, if both sides are either Level 2 or Level 1-2 routers, the routers establish a Level 2 adjacency.

3. Run the **show clns interface** command to verify that the interface is up:

```
TMX 880# show clns interface
gigabitethernet8/1 is Up, line protocol is Up
  Checksums enabled, MTU 8192, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: level-1-2  Circuit State: Up
    Interface number 0x7, local circuit ID 0x7
    Level-1 Metric: 10, Priority: 64, Circuit ID: 2222.2222.2222
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: 2222.2222.2222
    Number of active level-2 adjacencies: 1
    Level-1 Hello Interval 10
    Level-2 Hello Interval 10
    ReTx Interval 5
    Hello Multiplier 3
```

If the interface is down, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

4. Run the **show clns traffic** command to see if the system is sending and receiving IS-IS packets.

Keep in mind this command displays output only for fields that have a value. For example, it would not display a field for `LSPs sourced` if none were sent or received.

The following example output shows the activity of IS-IS packets on the interface `gigabitethernet8/1`:

```
TMX 880# show clns traffic
Interface gigabitethernet8/1
IS-IS: Level-1 Hellos (sent/rcvd): 369/432
IS-IS: Level-2 Hellos (sent/rcvd): 369/439
IS-IS: Level-1 LSPs sourced (new/refresh): 12/0
IS-IS: Level-2 LSPs sourced (new/refresh): 20/0
IS-IS: Level-1 LSPs flooded (sent/rcvd): 3/15
IS-IS: Level-2 LSPs flooded (sent/rcvd): 1/15
IS-IS: Level-1 CSNPs (sent/rcvd): 431/30
IS-IS: Level-2 CSNPs (sent/rcvd): 428/0
```

```
IS-IS: Level-1 PSNPs (sent/rcvd): 0/2
IS-IS: NSAP L1 Area Address mismatches (sent/received): 0/27
```

For this type of command output	Do this
The interface is not sending IS-IS packets.	Verify if the interface is sending any packets by running the **show interfaces** command. If the interface is not sending packets, or if the output of the **show interfaces** command indicates a packet transmission problem, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
The interface is sending Hello packets, but not receiving them	Verify the following information: • The remote system is up. • IS-IS is correctly configured on the remote system. • The remote system is sending IS-IS packets.
Mismatched passwords	If the output shows a mismatched password, set the same password on both systems. Use the **show running-config** command to view the password assigned to an interface. To change the password use the **isis password** command (at the `config-if` prompt).
Mismatched areas	Change the system configuration to share at least one area with the other system. To set the area use the **net** command.

Routing

Before you start troubleshooting routes, ensure that:

- IS-IS is configured correctly on the system, see "Configuration" on page 13-5 for more information.
- The system has an adjacency with the other router, see "Adjacencies" on page 13-7 for more information.

Router Connections

Troubleshooting routes requires a good understanding of the network topology and information about which IS-IS routes should be in the system's routing table. Work with the network administrator to obtain the available information about how the network routes should handle traffic.

To troubleshoot problems with routes:

1. Run the **show ip route isis** command to verify whether IS-IS is adding routes to the routing table.

   IS-IS routes in the command output would look similar to the following:

   ```
   i L2 172.16.21.0/24 [110/20] via 172.16.55.111, 02:09:28,
   gigabitethernet8/1
     i L2 172.16.22.0/24 [110/20] via 172.16.55.111, 02:09:28,
   gigabitethernet8/1
   ```

   If you do not see the expected routes:

   - Verify the type of circuit (Level 1, Level2, or Level1-2) the systems forming the adjacency use. The **show clns neighbors** command displays this information for the system.
   - If IS-IS is redistributing routes from another protocol, see "Routes Redistributed from Another Protocol" for information about troubleshooting redistribution.

2. Run the **show isis database** command to determine with which routers the system is communicating.

   The LSPID indicates which router created the packet:

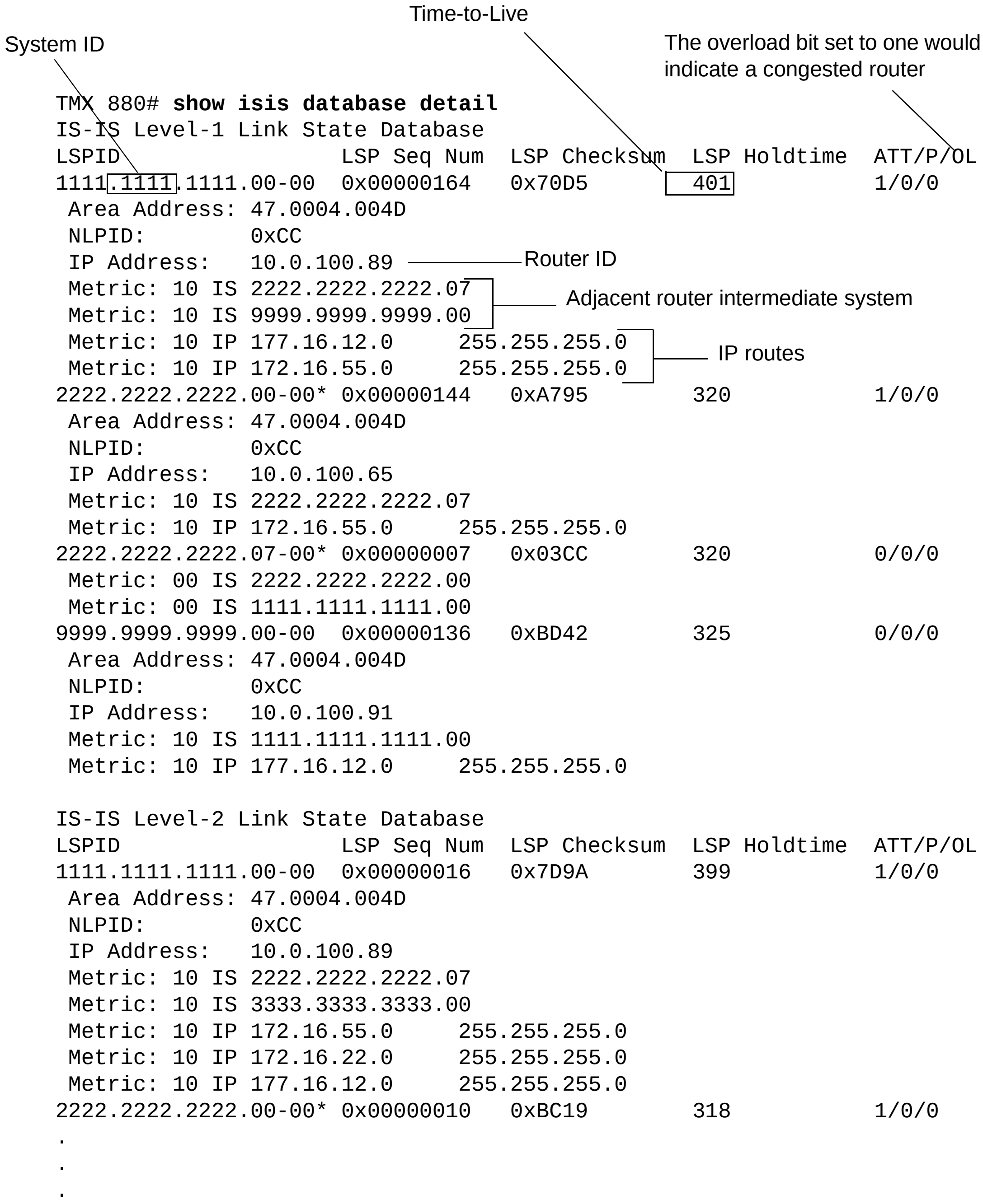
   ```
   TMX 880# show isis database
   IS-IS Level-1 Link State Database
   LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
   1111.1111.1111.00-00   0x00000162   0x74D3        1021          1/0/0
   2222.2222.2222.00-00*  0x00000142   0xAB93        940           1/0/0
   2222.2222.2222.07-00*  0x00000005   0x07CA        940           0/0/0
   9999.9999.9999.00-00   0x00000134   0xC140        945           0/0/0

   IS-IS Level-2 Link State Database
   LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
   1111.1111.1111.00-00   0x00000014   0x8198        1021
     1/0/0
   2222.2222.2222.00-00*  0x0000000E   0xC017        940           1/0/0
   2222.2222.2222.07-00*  0x00000007   0x03CC        940           0/0/0
   3333.3333.3333.00-00   0x0000000E   0x6512        321           1/0/0
   ```

3. Run the **show isis database detail** command to view information acquired from the control content of LSPs.

   The command output displays information from the link state database including the following:

   - Routers that are congested and may be unreliable
   - Area addresses IS-IS recognizes
   - Routes IS-IS recognizes

► The system assigns a router identifier. If this system router identifier is identical to another one in the same network area, you can use the **system-router-id** command to change it.


Time-to-Live
System ID
The overload bit set to one would indicate a congested router
Router ID
Adjacent router intermediate system
IP routes

```
TMX 880# show isis database detail
IS-IS Level-1 Link State Database
LSPID                  LSP Seq Num   LSP Checksum  LSP Holdtime  ATT/P/OL
1111.1111.1111.00-00   0x00000164    0x70D5         401          1/0/0
 Area Address: 47.0004.004D
 NLPID:         0xCC
 IP Address:    10.0.100.89
 Metric: 10 IS 2222.2222.2222.07
 Metric: 10 IS 9999.9999.9999.00
 Metric: 10 IP 177.16.12.0      255.255.255.0
 Metric: 10 IP 172.16.55.0      255.255.255.0
2222.2222.2222.00-00* 0x00000144    0xA795         320          1/0/0
 Area Address: 47.0004.004D
 NLPID:         0xCC
 IP Address:    10.0.100.65
 Metric: 10 IS 2222.2222.2222.07
 Metric: 10 IP 172.16.55.0      255.255.255.0
2222.2222.2222.07-00* 0x00000007    0x03CC         320          0/0/0
 Metric: 00 IS 2222.2222.2222.00
 Metric: 00 IS 1111.1111.1111.00
9999.9999.9999.00-00  0x00000136    0xBD42         325          0/0/0
 Area Address: 47.0004.004D
 NLPID:         0xCC
 IP Address:    10.0.100.91
 Metric: 10 IS 1111.1111.1111.00
 Metric: 10 IP 177.16.12.0      255.255.255.0

IS-IS Level-2 Link State Database
LSPID                  LSP Seq Num   LSP Checksum  LSP Holdtime  ATT/P/OL
1111.1111.1111.00-00   0x00000016    0x7D9A         399          1/0/0
 Area Address: 47.0004.004D
 NLPID:         0xCC
 IP Address:    10.0.100.89
 Metric: 10 IS 2222.2222.2222.07
 Metric: 10 IS 3333.3333.3333.00
 Metric: 10 IP 172.16.55.0      255.255.255.0
 Metric: 10 IP 172.16.22.0      255.255.255.0
 Metric: 10 IP 177.16.12.0      255.255.255.0
2222.2222.2222.00-00* 0x00000010    0xBC19         318          1/0/0
.
.
.
```

Routes Redistributed from Another Protocol

If the network redistributes routes from one routing protocol to another, IS-IS or another routing protocol can drop routes if not correctly configured. This section discusses routing redistribution from another protocol into IS-IS. For information about redistributing routes into OSPF, see Chapter 14, “Troubleshooting OSPF,” and for information about redistributing routes into BGP see Chapter 15, “Troubleshooting BGP.”

You need a good understanding of how redistribution is configured on the various systems on the network before you begin troubleshooting those systems.

To troubleshoot route redistribution:

1. If IS-IS is redistributing routes from another protocol, for example from OSPF, run the **show running-config** command to determine if the system is configured to redistribute routes.

   If the system is not redistributing routes, you can configure redistribution with the IS-IS **redistribute** command.

2. Run the **show isis database detail** command to decide which routes are missing from the routing table, and which routers are not advertising routes. For more information about output from this command, see "Adjacencies" on page 13-7.
3. Compare the routes listed in the routing table with a list of routes you expect to see.

   If routes redistributed from BGP into IS-IS Level 1 do not appear in the list, see "To troubleshoot redistributing BGP routes into IS-IS Level 1:" on page 13-12.

   Identifying the source of missing routes can be a time-consuming process.
4. Make sure a system that is dropping routes is up and configured correctly both for IS-IS and for redistribution.
5. Make any configuration changes needed.
6. Repeat step 3 and step 4 for other routers as needed.

To troubleshoot redistributing BGP routes into IS-IS Level 1:

1. Run the **show running-config** command to make sure that redistribution is configured to import the specified route map.
2. Run the **show route-map** command to verify that the level for the route map is set to Level 1.

Refer to the *TMX 880 Command Reference* for information about redistributing BGP routes into IS-IS Level 1.

14

Troubleshooting OSPF

This chapter describes the basic behavior of the Open Shortest Path First protocol (OSPF) running on the TMX 880 MPLS Core Switch, the configuration required to enable OSPF on the system, and how to troubleshoot OSPF routing problems.

Before You Start

Before reading this chapter you should be sure that the interfaces configured to use OSPF are up, are running the associated line protocols, and are sending and receiving packets. For information about system interfaces, see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."

Basic OSPF Behavior

A system correctly running OSPF has:

- OSPF enabled on it
- Specified interfaces running the OSPF protocol, becoming neighbors with OSPF neighbors in the AS, and forming adjacencies with the designated and backup designated routers
- OSPF adding all expected routes to the routing table
- The system redistributing routes as specified

To implement OSPF successfully on a network requires:

- The OSPF protocol running on all routers in a defined autonomous system
- The link-state databases running on each router in the autonomous system synchronized with each other
- The links required for routing advertised from each link-state database

Output from the **show ip ospf** and the **show ip route ospf** commands shows whether OSPF is running as configured on the TMX 880 MPLS Core Switch. The output provides information about configuration, OSPF neighbors, the link-state advertisement (LSA) database, and routing data for OSPF areas.

The **show ip ospf** command shows whether OSPF is running on the system. The command output provides summary information such as configuration values and area data:

Required ID

```
TMX 880# show ip ospf
Routing Process 'ospf' with ID 10.0.100.65
Supports only single TOS(TOS0) routes
It is an autonomous system boundary router
External Link Update interval is 00:30:00 and update due in 00:06:47
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs.
Type 5 Ext. LSAs in the LSDB: 2       LS Checksum of ext-LSAs: 14232
New LSAs Transmitted         : 612       New LSAs Received: 630
Table limit for non-default AS-ext-LSAs: unlimited
Number of Areas in this router is 1
Area 0.0.0.0
        Number of interfaces in this area is 2
        SPF algorithm executed 11 times
        Area ranges/summaries are:

        Link State Update Interval is 00:30:00 and due in 00:18:00
        Link State Age Interval is 00:59:58 and due in 00:47:58
```

Link state summary information

Area summary information

The **show ip route ospf** command shows whether OSPF is adding routes to the routing table. In the command output `O` identifies the OSPF routes:

```
TMX 880# show ip route ospf
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       T - route in transitional state
  O    172.16.9.0/24 [50/30] via 172.16.15.55, 00:42:04, pos2/0
  O    172.16.24.0/24 [50/20] via 172.16.15.55, 00:42:04, pos2/0
```

OSPF Configuration

This section summarizes how OSPF should be configured on the system, and provides background information for troubleshooting OSPF.

Basic OSPF configuration requires:

- Ensuring the OSPF module is loaded on the system
- Configuring the system

Verifying the OSPF Module is Loaded

In most cases the OSPF module is already loaded, but you should verify that the system is loading it.

To verify if the OSPF module is loaded:

- Run the **show modules** command, and look for the following output:

  ```
  spf nxSpf           active MAY-19-2000 19:53:09
  ```

  Active indicates that the system loaded the OSPF module `spf`.

If the module is not active (not loaded), you must load it.

To load the OSPF module:

1. Load the module by entering the following commands:

   ```
   TMX 880# configure terminal
   TMX 880(config)# load spf
   ```

2. Run the **show modules** command to verify that the module is loaded.

Reviewing Basic OSPF Configuration

The following examples summarize a basic OSPF configuration.

The following example configures OSPF for a broadcast or non-broadcast multi-access (NBMA) network. The sample input enables OSPF, and assigns the IP addresses on network 192 to area 0. If area 0 does not already exist, OSPF creates it.

```
TMX 880(config)# router ospf
TMX 880(router-config)# network 192.100.10.90 0.255.255.255 area 0
TMX 880(router-config)#
```

The following example configures OSPF for a point-to-point, point-to-multipoint network, or non-broadcast network. The sample input enables OSPF, assigns the IP addresses on network 192 to area 1. It also configures interface pos4/1 as a point-to-point network type for OSPF:

```
TMX 880(config)# router ospf
TMX 880(router-config)# network 192.100.10.90 0.255.255.255 area 1
TMX 880(router-config)# exit
TMX 880# configure terminal
TMX 880(config)# interface pos4/1
TMX 880(config-if)# ip ospf network point-to-point
TMX 880(config-if)# exit
TMX 880(config)#
```

If you want to redistribute routes from another protocol, such as BGP, into OSPF you do so by running the **redistribute** command for OSPF. If you are running OSPF to provide routes for another protocol, you may need to redistribute them into that protocol.

To enable graceful restart:

OSPF graceful restart (OSPF-GR) is a proprietary implementation in the TMX 880 system that allows for failover from the primary RCP to the secondary RCP without affecting the OSPF routing capabilities of the switch. The OSPF-GR feature temporarily retains OSPF routes when the primary RCP switches to the secondary RCP.

The following example enables OSPF graceful restart.

```
TMX 880 # configure terminal
TMX 880(config)# router ospf
TMX 880(config-router)# graceful-restart
```

You must enable OSPF-GR on all neighboring TMX 880 systems to take advantage of the OSPF-GR capability. Other routers will ignore the OSPF graceful restart feature.

OSPF Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with OSPF running on a system:

Table 14-1. Commands to Troubleshoot OSPF

To do this	Use this command
Turn on or off OSPF debugging messages to view OSPF debugging messages through the logging utility.	**debug ip ospf all** **undebug ip ospf**
View information about changes to neighbor connections.	**log-adjacency-changes**
Verify that the OSPF module is loaded.	**show modules**
Verify that the system is configured to redistribute routes.	**show running-config**
Verify that the OSPF protocol is enabled and running on the system. View summary information about OSPF.	**show ip ospf**
View the content of the system's link state database.	**show ip ospf database**
View summary information for each OSPF interface, including timer intervals.	**show ip ospf interface**
View summary information for a neighbor recognized by specified interfaces.	**show ip ospf neighbor**
View the list of virtual links for OSPF that the system maintains in its routing table.	**show ip ospf virtual-links**

Anytime you suspect a problem with OSPF routing, you should view log messages using the **show logging** command.

You can enable debugging by using the **debug ip ospf all** command to make debugging messages available to you through the log utility. For information about working with the log utility, see Chapter 2, "Reviewing System Messages."

⚠ Use caution when turning on debugging. The large number of messages generated by OSPF places a heavy load on system resources and can slow system performance.

For information about neighbor connections, run the **log-adjacency-changes** details command to view information about all state changes. Use this command prior to running the **debug ip ospf adjacency** command.

Troubleshooting OSPF

The most common causes of OSPF problems are:

- The protocol is not enabled on the system.
- The TMX 880 system or a neighbor is not configured correctly.
- The system does not form the appropriate neighbor or adjacency connections.
- OSPF does not add routes to the routing table.
- OSPF drops routes.
- The system does not redistribute routes correctly.

If OSPF is not running correctly on the system:

1. Check the OSPF configuration on the TMX 880 system.
2. Verify that the system forms neighbor connections with other routers, and an adjacency with the designated router and with the backup designated router.
3. Investigate routing problems such as dropped routes and faulty redistribution of routes into OSPF.

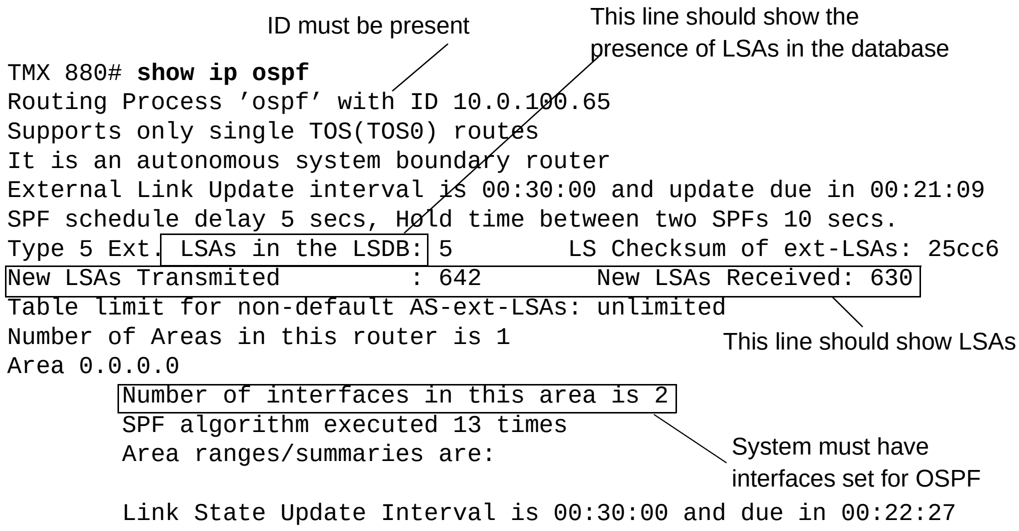
Configuration

Before evaluating other OSPF problems, make sure that the basic OSPF configuration on the system is correct.

To evaluate OSPF configuration problems:

- Run the **show ip ospf** command to verify that the OSPF protocol is enabled and configured.

  In the following example output, all of the interfaces running OSPF were assigned to area `0.0.0.0` (a backbone area) by using the **network** command.



ID must be present

This line should show the presence of LSAs in the database

```
TMX 880# show ip ospf
Routing Process 'ospf' with ID 10.0.100.65
Supports only single TOS(TOS0) routes
It is an autonomous system boundary router
External Link Update interval is 00:30:00 and update due in 00:21:09
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs.
Type 5 Ext. LSAs in the LSDB: 5        LS Checksum of ext-LSAs: 25cc6
New LSAs Transmitted          : 642        New LSAs Received: 630
Table limit for non-default AS-ext-LSAs: unlimited
Number of Areas in this router is 1
Area 0.0.0.0
        Number of interfaces in this area is 2
        SPF algorithm executed 13 times
        Area ranges/summaries are:

        Link State Update Interval is 00:30:00 and due in 00:22:27
```

This line should show LSAs

System must have interfaces set for OSPF

For this type of command output	Do this
The CLI displays the following message when you enter an OSPF command: `<(Unknown option, ? for list)>` This indicates that the OSPF module is not enabled or is not loaded.	• Verify whether the OSPF module is loaded. For information about how to verify whether the module is loaded and how to load the module, see "Verifying the OSPF Module is Loaded" on page 14-2. • If the module is loaded, use the **router ospf** command to enable OSPF on the system, and the **network** command to enable OSPF on interfaces and assign those interfaces to an area.
The router id as identified by the line: `Routing Process 'ospf with ID` *`id-number`*	Make sure that the router id is unique on the AS. The system assigns a router identifier. If this system router identifier is identical to another one in the same network area, you can use the **system-router-id** command to change it.
No area set	Set the area with one of the area commands.

For this type of command output	Do this
LSAs are not being received: New LSAs Received: 0	**1.** Verify that the interface is up by running the **show ip ospf interface** command. If the interface is down, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.” **2.** Determine if the system is forming an adjacency. For information about how to troubleshoot adjacencies, see “Neighbors and Adjacencies” on page 14-8, then evaluate routing problems discussed in “Routing” on page 14-11.
No LSAs in the link state database: LSAs in the LSDB: 0	Determine if the system is forming an adjacency with the designated router and the backup designated router. For information about how to troubleshoot adjacencies, see “Neighbors and Adjacencies” on page 14-8, then evaluate routing problems discusses in “Routing” on page 14-11.
LSAs are not being sent: New LSAs Transmitted : 0	Verify if the interface is sending any packets by running the **show interfaces** command. • If the interface is not sending packets, or if the output of the **show interfaces** command indicates a packet transmission problem, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.” • If the interface is sending packets, determine if the system is forming an adjacency with the designated router, see “Neighbors and Adjacencies” on page 14-8.
The number of areas defined for the router is greater than one: Number of Areas in this router is 2	In many cases, all of the interfaces on the router belong to the same area. If the output shows more than one area, make sure that the areas are configured correctly. Run the **show ip ospf interface** command to see which interfaces belong to which area.
The number of interfaces defined for the area, indicated by: `Number of interfaces in this area is`	Verify if this number matches the number of interfaces expected to run OSPF.

For this type of command output	Do this
Values in the `SPF algorithm executed` counter	If after booting, the `SPF algorithm executed` counter steadily increases: **1.** Evaluate if another router in the AS is going up and down. This behavior would cause the system to recalculate the SPF each time the state of the flapping router changed. **2.** Make sure that two systems in the AS do not have duplicate router IDs. Two routers with the same ID would cause ongoing SPF recalculations.

Neighbors and Adjacencies

To exchange routing information from the link state database, the router must form an adjacency with the designated router for the area. The system can form an adjacency with the designated router only after the system forms adjacent neighbor connections with other routers in the area.

To communicate with each other, all neighbors sharing a common OSPF interface definition must have the same values set for:

- The hello timer interval
- The dead timer interval
- Classification as a stub area (for those areas that are stub areas) or nssa (for those areas that are nssa)
- Area ID
- Authentication type (if any)

For all neighbors that are TMX 880 systems, run the commands discussed in the following procedure and save the command output to a file (from a Telnet session save the terminal output to a Telnet log file). You can then examine the output from the systems to compare configuration values.

To troubleshoot neighbor and adjacency problems:

1. Run the **show ip ospf neighbor** command to view the list of neighbors recognized by specified interfaces.

   The following example output shows that all neighbors have a primary state of `Full`, meaning that they are adjacent. As adjacent neighbors the systems have the same (or similar) data in their link state databases.

   ```
   TMX 880# show ip ospf neighbor

   ID               Pri State  Dead Time Address         Interface
   192.0.100.91      1 FULL/    00:00:35 192.24.10.20    pos2/0.409
   192.0.100.91      1 FULL/    00:00:35 192.24.9.20     pos2/0.408
   192.0.100.91      1 FULL/    00:00:35 192.24.8.20     pos2/0.407
   ```

```
192.0.100.91     1 FULL/    00:00:35 192.24.7.20     pos2/0.406
192.0.100.91     1 FULL/    00:00:35 192.24.6.20     pos2/0.405
192.0.100.91     1 FULL/    00:00:35 192.24.5.10     pos2/0.404
```

For this type of command output	Do this
No neighbors listed	Verify that the system is using the correct netmask to configure interfaces. The **show ip ospf interface** command provides this information.
An OSPF interface does not appear in the list.	Verify that the interface is up and is configured to use OSPF by running the **show ip ospf interface *interface-name*** command.
The primary state is `DOWN`.	**1.** Verify the following information for the remote system: – The system is up. – OSPF is correctly configured on the remote system. – The remote system is sending OSPF packets. **2.** Go to Step 2 to continue troubleshooting the neighbor relationship.

3. Run the **show ip ospf interface** command to:

- Verify the value for the Hello timer.

  Make sure this value is the same as other systems in the AS.

- Verify the value for the Dead interval timer.

  Make sure this value is the same as other systems in the AS.

- Verify the IP address and netmask.

- Determine if the system is a designated router, or a backup designated router, or neither.

  The command output displays the following as appropriate:

  ```
  We are the designated router
  We are the backup designated router
  ```

```
TMX 880# show ip ospf interface

Interface (loopback0) type: LAN Emulation (NBMA) State: Up  Router ID:
10.0.100.65
 IP Address/Mask: 172.16.16.222/255.255.255.0, Area 0.0.0.0
 Interface Cost:                        10
 Router Priority:                       1
 DR election state:                 We are Designated Router
 Designated Router ID  10.0.100.65, Interface IP address 172.16.16.222
 Timer intervals configured, Hello 30, Dead 120, Wait 120, retransmit 5
 Hello due in 12 seconds
 Neighbor count 0, Adjacent Neighbor count 0

Interface (pos2/0) type: Point-to-Point State: Up  Router ID:
10.0.100.65
 IP Address/Mask: 172.16.15.222/255.255.255.0, Area 0.0.0.0
 Interface Cost:                        10
 Router Priority:                       1
```

For this type of command output	Do this

`We are the designated router`
or:
`We are the backup designated router`
	Make sure the system has adjacencies with all of the other neighbors in the area. Verify that the `Adjacent neighbor count` in the output is correct.

`We are neither the designated router or the backup designated router`	**1.** Make sure the system recognizes the other neighbors in the area. Verify that the `Neighbor count` is correct. **2.** Make sure the system is adjacent with both the designated router and the backup designated router. Verify that the `Adjacent Neighbor count` is 2.
`IP Address/Mask`	Verify that the settings are correct. If they are not, you can change the settings by using the **network** command.

3. Verify that the following settings are the same on the routers in the AS:

- Area ID

  The **show ip ospf** command gives you this information for the TMX 880 MPLS Core Switch

- Area as a stub area or nssa

  The **show ip ospf** command gives you this information for the TMX 880 MPLS Core Switch.

- Authentication type (if any)

  The **show running-config** command gives you this information for the TMX 880 MPLS Core Switch.

Routing

Before you start troubleshooting routes, ensure that:

- OSPF is configured correctly on the system, see "Configuration" on page 14-5 for more information.
- The system has adjacencies appropriate for its designated router state, see "Neighbors and Adjacencies" on page 14-8 for more information.

Troubleshooting routes requires a good understanding of the network topology and the OSPF routes that should appear in system's routing table. Work with the network administrator to obtain the available information about how the network routes should handle traffic.

To view OSPF routes:

- Run the **show ip route ospf** command to verify if OSPF adds routes to the routing table.

  The command displays data from the routing table. OSPF routes in the command output would look similar to the following:

  ```
  O    172.16.9.0/24 [50/30] via 172.16.15.55, 00:25:10, pos2/0
  O    172.16.24.0/24 [50/20] via 172.16.15.55, 00:25:10, pos2/0
  ```

  If the **show ip route ospf** command does not display the routes you expect to see, troubleshoot router connections (see "Router Connections" on page 14-11) and redistribution configuration (see "Routes Redistributed from Another Protocol" on page 14-12).

Router Connections

Troubleshooting communication with routers beyond their OSPF area requires an understanding of OSPF configuration within the AS:

- The system communication with an area border router (if present in the network configuration and if the system is not one)
- The link type at both ends of a link
- Virtual links

To troubleshoot connections to other routers:

1. If the router does not have interfaces on an OSPF backbone (Area 0), verify whether the area has an area border (ABR) configured to communicate with the backbone. The ABR is a router connected to Area 0 and at least one other area.

   If the router does not have any interfaces in Area 0, make sure there is another router in its area that is an ABR.

2. If the system is an area border router, and uses a virtual link to another router, ensure that the systems are forming the virtual route by running the **show ip ospf virtual-links** command.

For this type of command output	Do this
The link is not listed in the command output.	Set the virtual link on the system using the **area virtual-link** command.
The link is listed as down. For example: `Virtual link to router 1.1.1.2 is Down`	Verify whether the remote system is operational and has the virtual link configured.

3. If one side of the link is configured as point-to-point, verify that the system on the other side of the link is also configured as point-to-point.

   The **show ip ospf interface** command gives you this information for an TMX 880 MPLS Core Switch. For example:

   ```
   Interface (pos2/0) type: Point-to-Point State: Up  Router ID: 10.0.100.65
   ```

   The **ip ospf network** command can be used to set the OSPF network type for an interface.

4. Run the **show ip ospf** command to verify whether the system is calculating the shortest paths (SPFs).

   The following example output for the area summary provides this information:

   ```
   SPF algorithm executed 99 times
   ```

   This number should increment by at least once every 30 minutes.

   For information about troubleshooting suspected problems with SPF calculations, see "Configuration" on page 14-5.

Routes Redistributed from Another Protocol

If the network redistributes routes from one routing protocol to another, OSPF or another routing protocol can drop routes if not correctly configured. This section discusses routing redistribution from another protocol into OSPF. For information about redistributing routes into IS-IS, see Chapter 13, "Troubleshooting IS-IS," and for information about redistributing routes into BGP see Chapter 15, "Troubleshooting BGP."

You need a good understanding of how redistribution is configured on the various systems on the network before you begin troubleshooting those systems.

To troubleshoot route redistribution:

1. If OSPF is redistributing routes from another protocol, for example from BGP, run the **show running-config** command to determine if the system is configured to redistribute routes.

The following output from the **show running-config** command shows that OSPF is configured to redistribute routes from BGP:

```
redistribute bgp 4229
```

If the system is not redistributing routes, you can configure redistribution with the OSPF **redistribute** command.

▶ OSPF cannot redistribute routes into a stub area.

2. Run the **show IP ospf database** command to decide which routes are missing from the routing table, and which routers are not advertising routes.

- For each section, identify which routers are advertising routes. The following example output show two ADV Routers:

```
Displaying Router Link States(Area 0.0.0.0)

  Link ID          ADV Router        Age          Seq#     Checksum   Link
count
10.0.100.65       10.0.100.65      1627     0x80000090    0xb661        3
10.0.100.66       10.0.100.66      1629     0x80000090    0x2e9a        3
```

- Determine if all of the links expected to other routing domains are listed.

3. View the remaining link states in the command output, and compare those values to expected values.

Comparing command output, with the type of routing data expected for the network topology lets you identify the source of missing routes. This process can be time-consuming.

4. Make sure a system that is dropping routes is up and configured correctly both for OSPF and for redistribution.

5. Make any configuration changes needed.

6. Repeat step 3 and step 4 for other routers as needed.

15

Troubleshooting BGP

This chapter describes the basic behavior of BGP running on the TMX 880 MPLS Core Switch, the configuration required to enable BGP on the system, and how to troubleshoot BGP routing problems.

The system supports version 4 of BGP which provides extensions to the earlier version, such as supernetting through classless inter-domain routing (CIDR). Ideally, the other systems in the AS and systems that are external neighbors should also run BGP version 4.

Before You Start

Before reading this chapter you should be sure that the interfaces configured to use BGP are up, are running the associated line protocols, and are sending and receiving packets. For information about system interfaces, see Chapter 5, “Getting Started Troubleshooting Interfaces and Protocols.”

You should also have a good understanding of route filtering before you try to troubleshoot BGP routing problems. Route filtering is complex to implement and troubleshoot.

Basic BGP Behavior

A system correctly running BGP has:

- BGP enabled on it
- Specified interfaces running the BGP protocol
- Connections to configured neighbors, within the autonomous system (AS), or external to the AS
- BGP routes in the routing table
- Routes resulting from policies that are correctly configured
- The system redistributing routes as specified

To implement BGP successfully on a network requires:

- BGP running on the border routers in an AS
- BGP communicating between ASs

- BGP receiving update information, and advertising routes as configured
- BGP maintaining the same routing information among systems in the AS

Output from the **show ip bgp summary** and the **show ip route summary** commands shows whether BGP is running as configured on the system. The output provides information about configuration and about BGP routes.

The **show ip bgp summary** command shows whether BGP is running on the system, is sending and receiving packets, and is establishing neighbors. (When a number is displayed in the "PfxRcvd" category, the state is ESTABLISHED.) The command output also provides general information about status of BGP on the system:

```
TMX 880# show ip bgp summary
BGP table version is 38250, main routing table version is 39010
2063 network entries (2063/3063 paths) using 295560 bytes of memory
3 BGP path attribute entries using 377 bytes of memory
1 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Neighbor        V    AS MsgRcvd MsgSent OutQ  Up/Down Type     State/  Fid
                                                              PfxRcvd
192.23.252.17   4 65300    6669    6733    0  0:37:58 ext        1000  51(p)
172.25.252.17   4 65300     313     323    0  0:37:41 ext        1000  69(a)
192.28.111.6    4 64531   11031   13781    0    4d03h ext        1000  38(a)
```

Shows that prefixes were received

The **show ip route summary** command shows whether BGP is adding routes to the routing table. The command output shows the number routes added by BGP, and other routing protocols. (The following sample output is truncated to show only the networks and subnets added.)

```
TMX 880# show ip route summary

Route Source Networks     Subnets     ...
isis         0            0           ...
rip          0            0           ...
ospf         1            2           ...
static       2            0           ...
local        0            56          ...
bgp          2            50,000      ...
fpm          0            0           ...
(null)       0            0           ...
Total        3            58          ...
```

BGP Configuration

Basic BGP configuration requires:

- Ensuring the BGP module is loaded on the system
- Configuring the system

BGP provides route filtering for management. To take full advantage of BGP routing, systems running BGP typically have filters configured for incoming and outgoing route updates.

Verifying the BGP Module is Loaded

In most cases the BGP module is already loaded, but you should verify that the system is loading it.

To verify if the BGP module is loaded:

- Run the **show modules** command, and look for the following output:

  ```
  bgp nxBgp           active MAY-19-2001 16:31:56
  ```

  Active indicates that the system loaded the BGP module bgp.

If the module is not active (not loaded), you must load it.

To load the BGP module:

1. Load the module by entering the following commands:

   ```
   TMX 880# configure terminal
   TMX 880(config)# load bgp
   ```

2. Run the **show modules** command to verify that the module is loaded.

Reviewing Basic BGP Configuration

The following examples summarize very basic BGP configurations. Typically, BGP configuration is complex and includes filters to manage routes.

This example enables BGP on the system, assigns the router to AS 500, allows internal peers to receive internal routing advertisements, specifies which network the router can announce to its neighbors, and configures a neighbor and route filters:

```
TMX 880# configure terminal
TMX 880(config)# router bgp 500
NOTE: newly configured neighbors will be activated only
   after top-level configuration mode is exited or
   ’commit’ command is executed
TMX 880(router-bgp)# permit-internal-into-ibgp
TMX 880(router-bgp)# network 192.0.2.10 mask 255.255.255.255
TMX 880(router-bgp)# neighbor 192.0.24.20 remote-as 500
TMX 880(router-bgp)# neighbor 192.0.24.20 distribute-list 1 in
TMX 880(router-bgp)# neighbor 192.0.24.20 distribute-list 1 out
TMX 880(router-bgp)# commit
TMX 880(router-bgp)# exit
TMX 880(config)# access-list 1 permit 192.0.2.10
```

The following example, in BGP router configuration mode, configures dampening and fall-over for BGP. Dampening helps to avoid excessive routing updates produced by a system that repeatedly becomes available then unavailable. Fall-over lets the system reset a BGP connection if the link between the TMX 880 MPLS Core Switch and an adjacent external peer is down.

```
TMX 880(router-bgp)# bgp dampening
TMX 880(router-bgp) # bgp fast-external-fallover
TMX 880(router-bgp)# commit
TMX 880(router-bgp)#
```

The **redistribute** command allows you to redistribute routes from another protocol, such as OSPF, into BGP.

Graceful restart allows the RCP to temporarily retain BGP routes when TCP sessions between BGP peers are briefly interrupted. With graceful restart, peer routers re-establish connections and restore their BPG routes without having to relearn them. Both peers must support graceful restart and capabilities advertisement (the mechanism used to communicate support of the graceful restart functionality) for the RCP to implement the feature.

Graceful restart is enabled by default for all peers. You can control graceful restart at both the frame and the peer level. If disabled for the chassis, then graceful restart is disabled for every peer; however, any configuration at the peer level is saved and reapplied if and when the feature is re-enabled at the chassis level.

You can configure graceful restart for unicast IPv4 address family or for no address families.

- The following example configures graceful restart on the local router in autonomous system 100 for the unicast IPv4 address family for this peer.

```
TMX 880# configure terminal
TMX 880(config)# router bgp 100
TMX 880router-bgp)# neighbor 128.109.33.2 restart-family uni-ipv4
TMX 880(router-bgp)#
```

- The following example configures graceful restart for the unicast IPv4 address family as the global default in this router.

```
TMX 880# configure terminal
TMX 880(config)# router bgp 100
TMX 880(router-bgp)# restart-family uni-ipv4
TMX 880(router-bgp)#
```

BGP Troubleshooting Commands

The following table lists the commands you use to troubleshoot problems with BGP running on a system:

Table 15-1. Commands to Troubleshoot BGP

To do this	Use this command
Turn on BGP event messages to view BGP debugging messages through the log utility.	**debug ip bgp events**
Turn off BGP event messages to view BGP debugging messages through the log utility.	**undebug ip bgp events**
Test the IP access to a remote system.	**ping**
Verify that the BGP module is loaded.	**show modules**
View configured IP address access lists, which display IP address filtering criteria.	**show access-list**

Table 15-1. Commands to Troubleshoot BGP

To do this	Use this command
View configured AS-path access lists, which display AS-path filtering criteria.	**show ip as-path-access-list**
View the BGP routing table.	**show ip bgp**
View the date and time of the latest build.	**show ip bgp build-info**
View paths that are not recognized because a system was changing states between operational and not operational (that is the routes are in a dampened state).	**show ip bgp dampened-paths**
View history and route filtering information for systems that change state from operational to not operational (that is flapping).	**show ip bgp flap-statistics**
View information about the TCP and BGP connections to neighbors.	**show ip bgp neighbors**
View KeepAlive and HoldTime timer information.	**show ip bgp neighbors timers**
View received routes that are rejected (not installed as valid routes) by filters for incoming routes.	**show ip bgp rejected**
View summary status of all BGP connections.	**show ip bgp summary**
View the IP routing table.	**show ip route**
View details of configured route maps.	**show route-map**

Troubleshooting BGP

The most common causes of BGP problems are:

- The protocol is not enabled on the system.
- The system does not form appropriate neighbor connections.
- BGP does not add configured routes to the routing table.
- Incorrectly configured packet filters.
- Incorrectly configured route filters.
- The system does not redistribute routes correctly.

If BGP is not running correctly on the system:

1. Verify IP connections.

   For information about troubleshooting IP connections, see Chapter 9, “Troubleshooting IP.”

2. Review log messages for BGP messages.

3. Check the BGP configuration on the system.
4. Verify that the system forms neighbor connections with other routers within the AS, as well as any neighbor connections with external routers (if configured).
5. Investigate routing problems such as dropped routes and faulty redistribution of routes into BGP.

► If you need to contact Network Care for support when troubleshooting a BGP problem, make sure that you have the version information for BGP available by running the **show ip bgp build-info** command.

Reviewing Log Messages

Anytime you suspect a problem with BGP routing, you should view log messages using the **show logging** command. You can also enable debugging by using the **debug ip bgp events** command to make events messages available to you through the log utility. For information about working with the log utility, see Chapter 2, "Reviewing System Messages."

BGP notification messages usually provide an error code, and when applicable, an error subcode. The following table lists these error codes and the associated type of messages.

Table 15-2. BGP Notification Codes

Error Code	Error subcode	Description of error
1		**Error in message header**
	1	The connection is not synchronized. The message header does not contain the expected values for an open message, or for an Authentication Information Optional Parameter.
	2	The Length field in a message header is invalid. The type of message determines the defined range of values for the Length field.
	3	The message header contains an invalid type.

Table 15-2. BGP Notification Codes

Error Code	Error subcode	Description of error
2		**Error in open message**
	1	The version number is not supported.
	2	The open message contains an invalid peer AS number.
	3	The open message contains an invalid IP address from a remote host.
	4	The open message contains an unsupported optional parameter.
	5	Authentication failed.
	6	The system rejects the HoldTime value received from the remote system.
3		**Error in update message**
	1	The update message contains a path attribute (unfeasible route length and/or total attribute length) that is too long.
	2	The update message contains a data field that the system does not recognize.
	3	The update message does not contain a mandatory well-known attribute.
	4	An update message contains attribute flags that conflict with the attribute type code.
	5	The update message contains an attribute length that conflicts with the attribute type code.
	6	The update message contains an invalid origin attribute.
	7	The update message indicates an AS routing loop.
	8	The update message contains an invalid next hop IP address. **Note:** This error applies only to external BGP connections.
	9	The system detects (and discards) an error in an optional attribute in an update message.
	10	The network field in the update message is invalid.
	11	An update message contains incorrect syntax for the AS path.

Table 15-2. BGP Notification Codes

Error Code	Error subcode	Description of error
4		The system did not receive a KeepAlive, update, or notification message within the time specified for the HoldTimer.
5		The system detected an error, such as unexpected event.
6		A BGP peer closes a BGP connection by sending a Cease message.

Configuration

Before evaluating other BGP problems:

- Make sure that the basic BGP configuration on the TMX 880 MPLS Core Switch is correct.
- Assess how routing in general (access lists, route maps and so forth) is configured on the system to determine how to proceed.

► The system assigns a router identifier. If this system router identifier is identical to another one in the same network area, you can use the **system-router-id** command to change it.

To evaluate BGP configuration problems:

1. Run the **show ip bgp summary** command to verify the protocol is enabled and configured:

```
TMX 880# show ip bgp summary
BGP table version is 709013, main routing table version is 709010
82567 network entries (82567/82567 paths) using 9908040 bytes of memory
10295 BGP path attribute entries using 1516312 bytes of memory
9 BGP route-map cache entries using 288 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Neighbor        V    AS MsgRcvd MsgSent OutQ  Up/Down Type     State/  Fid
                                                              PfxRcvd
10.0.0.1        4 65534   88292    3200    1    1d22h ext        82559  15(p)
10.0.100.65     4   174       0       0    0    never           ACTIVE   0(p)
```

► The `state/PfxRcvd` identifies the status of the connection: `Idle`, `Connect`, `Active`, `OpenSent`, `OpenConfirm`, or `Established`. If it is established it displays the number of prefixes received instead of “ESTABLISHED.”

For this type of command output	Do this
`Error: BGP is not active`	BGP is not enabled on the system. **1.** Enable BGP by using the **router bgp** command. **2.** Configure the protocol if it is not already configured.
The `Neighbor` column does not list a neighbor system you expect to see on the list.	Troubleshoot neighbor connections, see "Neighbors" on page 15-10.
The `MsgRcvd` column does not show any messages received from a listed neighbor.	Make sure that the system can connect to the remote router by running the **ping** command. If the **ping** command fails, determine if the system is communicating over the Internet Protocol, see Chapter 9, "Troubleshooting IP."
Number of messages listed in the `OutQ` column is large.	Check traffic flow on system interfaces, for information about evaluating packet transmission see Chapter 5, "Getting Started Troubleshooting Interfaces and Protocols."
The State is `Idle`. An `Idle` state indicates the connection is closed and that BGP deleted all routes to the connection from the routing table.	Troubleshoot neighbor connections, see "Neighbors" on page 15-10.
The state is `Active`. An `Active` state indicates the system is attempting to form a connection after initially failing to make the connection.	Wait to see if the state becomes established. If it does not, troubleshoot neighbor connections, see "Neighbors" on page 15-10.

3. Run the **show running-config** command to get information about BGP configuration on the system. The command output shows neighbor configuration and BGP routing configuration entries such as the following:

   - Filtering IP addresses with access lists on the local router, for example:

     ```
     access-list 1 deny 172.24.22.20
     access-list 2 permit any
     ```

     and applying them to a neighbor:

     ```
     neighbor 172.29.252.16 distribute-list 2 out
     ```

   - Sharing routes through redistribution, for example:

     ```
     redistribute static
     ```

- Use of route maps on the local router, for example:

  ```
  route-map TEST permit 10
  ```

  and applying them to a neighbor:

  ```
  neighbor 172.29.252.16 route-map all in
  ```

- Filters used by route maps, for example:

  ```
  route-map TEST permit 10
  match ip address 2
  ```

  set metric 66

Neighbors

For BGP to share routing information with other systems, the remote systems must be established neighbors. Establishing a neighbor relationship requires that:

- The systems have a TCP/IP connection.
- For internal neighbors, each system is in the same AS. For external neighbors, each system is configured to be a neighbor with the remote AS.

  Note that systems internal to an AS can use route reflectors or confederations to simplify communication between the systems within the AS.
- The routes have access to the systems (that is, BGP route filters allow routes from the other system).

  The TMX 880 system must have route filters or distribute lists configured to grant access to routes. By default, a TMX 880 system denies route access.
- Settings for HoldTime and KeepAlive be compatible — the KeepAlive messages must have sufficient time to reach another system before the HoldTime interval expires.

  Typically, the HoldTime interval is three times longer than the KeepAlive interval.

To troubleshoot neighbor connections:

1. Run the **show ip bgp summary** command to view a list of the neighbors (identified by IP address and AS) that BGP recognizes.

   In the command output, look for neighbors that do not show the number of prefixes received, or neighbors that you expect to be in the list not listed.
2. Verify that the system can connect to the neighbor system by running the **ping** command.

   If the **ping** command fails, troubleshoot the IP connection, see Chapter 9, “Troubleshooting IP.”
3. Run the **show ip bgp neighbors** ***ip-address*** command to get information about the neighbor configuration.

   Neighbor connections should show the state as `BGP state = ESTABLISHED`.
4. Compare the configuration on the two systems that are not establishing a neighbor relationship. Run the **show running-config** command on the local system, and obtain the same information for the remote system.

Make sure that the output identifies the AS for a neighbor, and verify that the value for that AS is correct. The following example shows the file entry for a neighbor in AS 4290:

```
neighbor 192.0.24.16 remote-as 4290
```

5. Run the **show ip bgp neighbors timers** command to verify that the HoldTime interval and the KeepAlive interval are compatible between the local system and neighbor system.

   The command output shows the configured timers, and the timer values set on neighbors.

```
TMX 880# show ip bgp neighbors timers
Globally configured: HoldTime 180, KeepAlive: 60
Neighbor                   PeerGroup       State      Hold        Keep
Fid
                                                     conf neg    conf neg
192.25.252.16                               IDLE   180    0    60     0
0
192.27.252.16                             ACTIVE   180    0    60     0
0
192.28.111.2                          ESTABLISHED   180   90    60    30
63
192.31.252.18                         ESTABLISHED   180  180    60    60
65
```

   Typically, BGP negotiates the timer value between systems that have different timers configured, using the smaller configured values.

6. Run the **show ip bgp dampened-paths** and **show ip bgp flap-statistics** commands to see whether the path to the remote system has been unreliable due to operational state.

Routing

Troubleshooting BGP routing problems is painstaking and time-consuming. This process requires a good understanding of the network topology and of the BGP routes that should appear in a system’s routing table. Work with the system administrator to obtain the available information about how the network routes should handle traffic. As a first step, determine if any routes are missing from the routing table, then evaluate the potential causes of a missing route.

Before you start troubleshooting routes, ensure that:

- BGP is configured correctly on the system, see “Configuration” on page 15-8 for more information.
- The system is establishing neighbors, see “Neighbors” on page 15-10 for more information.

You should also be familiar with how the system filters routes:

- BGP on an TMX 880 system applies only a single filter to a route, using the following order of precedence if more than one filter is specified:
  - Route map
  - Filter list
  - Distribution list

- When route filters are changed on the system, the **clear ip bgp** command must be executed for the new filters to take effect. This command should be run each time a filter is changed.
- MXOS access lists deny all routes by default. If you want a system to have access, you must explicitly configure access for that system.

In addition, filters configured on different systems in the path need to be compatible with each other, for example one system should not deny access to an AS, while another system in the path permits it.

To view BGP routes:

1. Run the **show ip bgp summary** command to view information about access configuration:

```
TMX 880# show ip bgp summary
BGP table version is 38250, main routing table version is 39010
2063 network entries (2063/3063 paths) using 295560 bytes of memory
3 BGP path attribute entries using 377 bytes of memory
1 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Neighbor        V    AS MsgRcvd MsgSent OutQ  Up/Down Type     State/  Fid
                                                              PfxRcvd
172.23.252.17   4 65300    6669    6733    0  0:37:58 ext         1000  51(p)
.
.
.
```

2. Run the **show ip route** command to see which routes BGP and other routing protocols are adding to the routing table.

   You should probably save this information to a telnet log file. Typically, command output is lengthy.

   If a BGP route is missing from the routing table, determine if another protocol has that route specified. A protocol that has a better distance might insert the route into the routing table.

3. Run the **show running-config** command to get an overview of routine configuration for route maps, access lists, filters, and so forth.

4. Run the **show ip bgp** command to display the BGP routing table. In the command output look for a network preceded by an x, indicating that the next-hop is unreachable.

   For networks marked as unreachable:

   - Try to **ping** the remote system. If the **ping** command fails, see Chapter 9, "Troubleshooting IP."
   - Examine the BGP configuration on the remote system to make sure that the remote system provides access to the system you are troubleshooting.

5. If BGP was previously routing traffic correctly, check whether any route filters changed on the local system or on the remote system. If a filter did change, review the changes to see whether the change caused the current routing problem.

   The **show ip bgp summary** command gives you this information for the TMX 880 MPLS Core Switch. In the command output, an asterisk (*) signifies a changed policy.

6. Run the **show ip bgp rejected** command to view routes rejected by the inbound filter configuration.

- An r indicates that the system administratively rejected a route due to inbound filter configuration. Review the filter for the rejected route, and make changes as needed.
- A d indicates that a route was dampened because it was becoming operational then non-operational (flapping). Identify the flapping route (**show ip bgp flap-statistics**), and, if possible, remedy the problem that is causing it to frequently change operational states.

7. To troubleshoot specific route filters, use the following commands:

- **show access- list**
- **show ip as-path-access-list**
- **show route map**

Examine the filters to try to isolate any that might cause the routing problem identified. You can then modify or disable these filters to see whether the change fixes the problem.

8. If you are unable to resolve routing problems on a system that is using route filters, collect information from the output commands in step 6 and step 7, then call Network Care for further assistance.

Routes Redistributed from Another Protocol

If the network redistributes routes from one routing protocol to another, BGP or another routing protocol can drop routes if not correctly configured. This section discusses routing redistribution from another protocol into BGP. For information about redistributing routes into IS-IS, see Chapter 13, “Troubleshooting IS-IS,” and for information about redistributing routes into OSPF see Chapter 14, “Troubleshooting OSPF.”

You need a good understanding of how redistribution is configured on the various systems on the network before you begin troubleshooting those systems. Typically routes are redistributed into BGP from an interior gateway protocol, such as IS-IS or OSPF. Redistribution should be configured within the same AS, not from an external AS.

To troubleshoot route redistribution:

1. If BGP is redistributing routes from another protocol, for example from OSPF, run the **show running-config** command to determine if the system is configured to redistribute routes.

The following output from the **show running-config** command shows that BGP is configured to redistribute static routes:

```
redistribute static
```

If the system is not redistributing routes, you can configure redistribution with the BGP **redistribute** command.

2. Make sure a system that is dropping routes is up and configured correctly both for BGP and for redistribution.

3. Make any configuration changes needed.

4. Repeat step 2 and step 3 for other routers as needed.

16

Troubleshooting SNMP

This chapter describes how to troubleshoot problems with SNMP associated operations on the TMX 880 MPLS Core Switch. SNMP is responsible for:

- Communicating with a network management station (as configured)
- Communicating between tasks running on the system

Basic SNMP Behavior

A system correctly running SNMP displays the following behavior:

- **Remote communication** — Sends SNMP traps and messages to a remote network management station. The network management station monitors network systems to gather information about system performance and status.
- **Local communication** — Provides interprocessor communication within the system including sending correct messages from the CLI to a task to execute a command.

SNMP Configuration for Remote Access

At a minimum, the system must have the following configured to communicate with a network management station:

- An SNMP community

  The system must provide read and write access to the community shared with the network management station, and be configured to send trap messages compatible with the version expected by the management station.
- An SNMP server host
- System access compatible with the way systems permit access on the associated network

The following example configures SNMP on an TMX 880 system. The input specifies the community **manager** for the system and the network management station. The community configuration allows read/write permission, and specifies version2 for trap messages:

```
TMX 880# configure terminal
TMX 880(config)# snmp-server community manager rw trapv2
TMX 880(config)# snmp-server host 192.0.2.10 manager
TMX 880(config)# exit
```

SNMP Troubleshooting Commands

The following table lists the commands you use to troubleshoot SNMP:

Table 16-1. Commands to Troubleshoot SNMP

To do this	Use this command
View SNMP communities and host addresses configured for the system.	**show communities**
View a list of the tasks running on the system.	**show process**
View errors associated with SNMP MIBs.	**show snmp**
Display the views configured for a host.	**show views**

Troubleshooting SNMP

The most common cause of SNMP problems are:

- **Remote** — SNMP configuration on the TMX 880 system or on the network management station
- **Local** — An internal system task not receiving an SNMP message

Anytime you suspect a problem with SNMP, you should set the log severity level to debugging and view log messages using the **show logging** command. For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

Troubleshooting Remote Communication Problems

A network management station not receiving SNMP messages from an TMX 880 system can result from:

- A configuration problem on the TMX 880 MPLS Core Switch
- A configuration on the management server
- A communication problem between the systems

The following procedures describe how to examine system configurations. If there is a configuration error, correct it. If the configuration appears to be correct on the local and on the remote system, you should troubleshoot the connection between the two systems. For information about troubleshooting IP connections, see Chapter 9, “Troubleshooting IP.”

To troubleshoot the configuration on the local system:

1. Run the **show communities** command to verify that:
    - The TMX 880 system belongs to the same community as the network management station.
    - The community has read/write access to the system.

- The trap version is the same as the one used by the network management station.
- The community has access to the TMX 880 system.

The following example output shows that the community manager has read/write permission, uses version 2 traps, with a host 192.0.2.10:

```
TMX 880# show communities
Community        View             Type    Traps  Access  Hosts
                                                 List
all-traps        default          RO      V2             192.168.1.250
private          default          RW                     0.0.0.0
manager          default          RW      V2             192.0.2.10
```

For information about how to configure a community and a host see "SNMP Configuration for Remote Access."

2. Make sure that the network management system has access through the access mechanism used on the network:

    - **Access lists** — You can display the access list for the system to get this information. Based on the system configuration, use the appropriate command:

For access lists defined by	Use this command
BGP **ip as-path access-list** command	**show ip as-path-access-list**
access-list command	**show access-list**

    - **Views** — Use the **show views** command to examine the views configured.

3. Run the **show snmp** command to look for any error conditions:

```
TMX 880# show snmp
Route Control Card, Thu May  8 03:49:57 EST 2001, D 1.7
.0 (BL 51).^RCP Image.^Built by  on daedalus.^.
Contact:
Location:
625 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    2558 Number of requested variables
    36 Number of altered variables
    211 Get-request PDUs
    373 Get-next PDUs
    41 Set-request PDUs
624 SNMP packets output
    0 Too big errors
    16 No such name errors
    0 Bad value errors
    0 General errors
    624 Get-response PDUs
    0 SNMP trap PDUs
```

If the command output shows errors, use the log utility to view messages created by command execution:

- Make sure that the log level is set to debug.

- Run a CLI command.
- Review the debug messages generated.

For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

To troubleshoot the configuration on the remote system:

- Make sure that the following are configured on the network management station:
  - A community that is the same as the community specified by the TMX 880 system, with the read/write access, and the correct trap version set.
  - The correct server hostname.

Troubleshooting Local Communication Problems

SNMP underlies interprocessor communication on the system; it provides the communication between the CLI and other tasks running on the system. The following conditions indicate a local problem with SNMP:

- Running a CLI command does not produce the expected behavior.
- Running a CLI configuration command does not make the expected change to the running configuration file.

The troubleshooting steps are the same to remedy either of these situations.

Troubleshooting Command Execution

You can run CLI commands to get information about what happens on the system when a command executes, and whether or not changes are written to the running configuration file as designed.

To troubleshoot command execution:

1. Run the **show snmp** command to look for any error conditions.

   If the command output shows errors:

   - Make sure that the log level is set to debug.
   - Run the problematic CLI command again.
   - Review the debug messages generated.

   For information about working with the log utility, see Chapter 2, “Reviewing System Messages.”

17

Removing and Replacing Field Replaceable Units

This chapter describes how to remove and replace system hardware Field Replaceable Units (FRUs).

The *TMX 880 Installation Guide* describes the system hardware modules; refer to the installation guide for more information.

Before You Begin

⚠ Review the safety guidelines in Appendix C, “Safety Instructions” before working with system components.

TMX 880 components can be damaged by static electricity. Static voltages as high as 35,000 volts can build from handling plastic or foam packing material, or sliding an electronic assembly across plastic or carpeting. Intermittent or complete component failures can result.

Before handling the modules and to minimize the chance of ESD damage, do the following:

- Always wear an ESD wrist/ankle strap with good contact to the skin.
- Insert the equipment end of your ESD strap (the banana plug) into any of the ESD sockets in front or back of the *grounded* chassis before handling a module.
- Avoid contact between cards and your clothing. The wrist strap protects cards from ESD voltages on the body only; EDS voltages on clothing can still cause electronic-component damage.
- Always place a card component-side up on an antistatic surface, in an antistatic card rack, or in a static-shielding bag. If you are returning a card to the factory, immediately place it in a static-shielding bag.
- Use the ejector levers to properly seat the card connectors to the chassis when you are installing modules and tighten all captive screws.

Systems Chassis Configuration

Figure 17-1 and Figure 17-2 show front and rear view of the TMX 880 system to help you identify and locate the systems hardware components. The system is shown as it is shipped with filler panels in place. The front view is with the chassis trim panels removed.

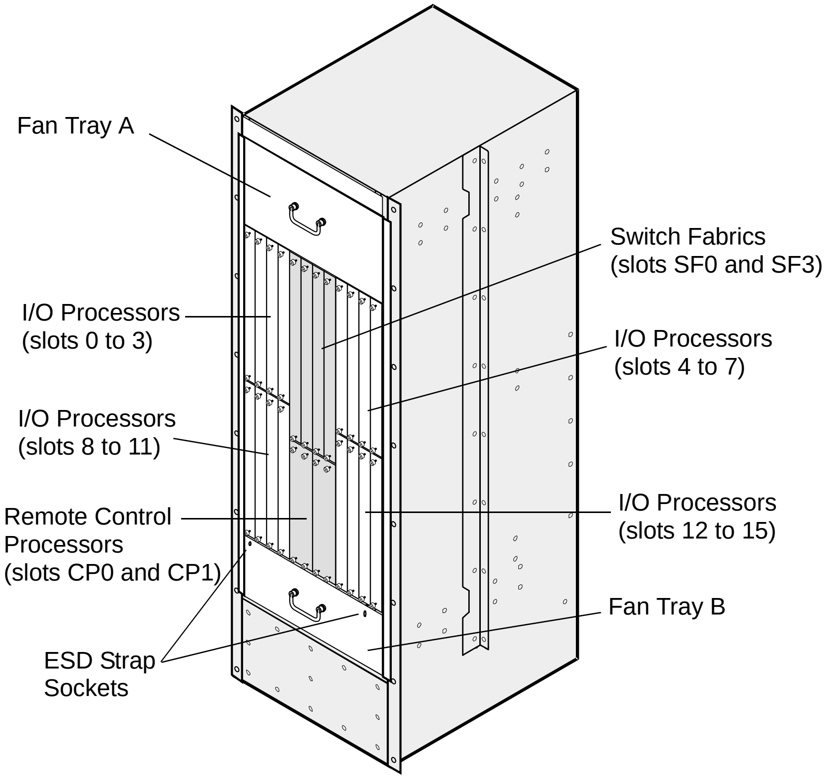

Fan Tray A
Switch Fabrics (slots SF0 and SF3)
I/O Processors (slots 0 to 3)
I/O Processors (slots 4 to 7)
I/O Processors (slots 8 to 11)
I/O Processors (slots 12 to 15)
Remote Control Processors (slots CP0 and CP1)
Fan Tray B
ESD Strap Sockets

Figure 17-1. TMX 880 MPLS Core Switch Front View

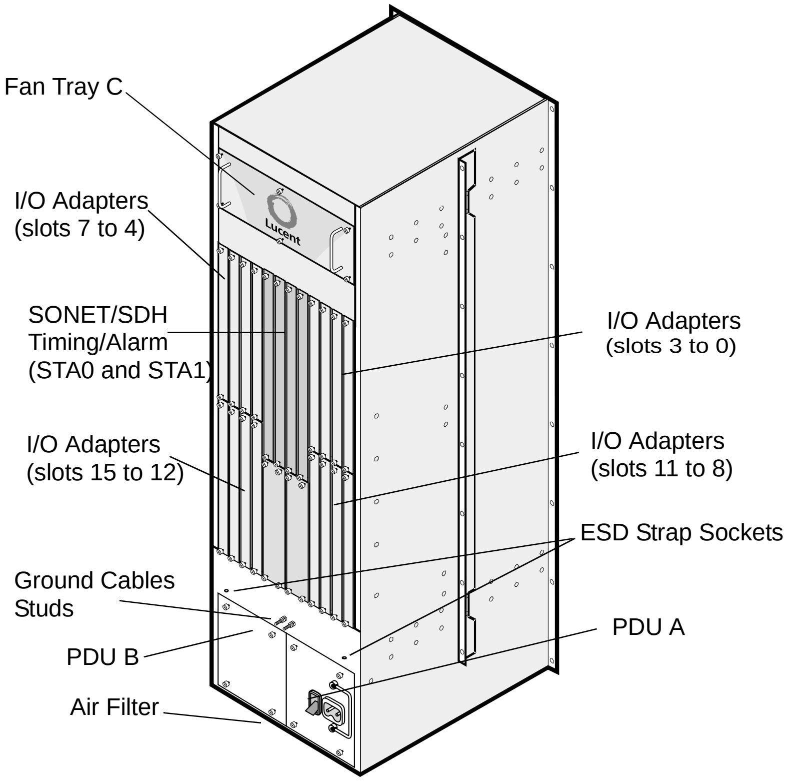

Fan Tray C
I/O Adapters (slots 7 to 4)
SONET/SDH Timing/Alarm (STA0 and STA1)
I/O Adapters (slots 15 to 12)
Ground Cables Studs
PDU B
Air Filter
I/O Adapters (slots 3 to 0)
I/O Adapters (slots 11 to 8)
ESD Strap Sockets
PDU A
Lucent

Figure 17-2. TMX 880 MPLS Core Switch Rear View

Card Modules Removal and Replacement

This section describes important operational procedures for card modules and how to remove and replace these modules, which include:

- I/O Processors (IOPs)
- I/O Adapters (IOAs)
- Switch Fabric modules
- SONET Timing/Alarm (STAs)
- Route Control Processors (RCPs)

Removal and Replacement of IOPs, IOAs, STAs, and SFs

This section describes how to remove and replace IOPs, IOAs, STAs, and SFs. Use Figure 17-3 as a reference for this operation. These cards are hot-swappable, which means you can remove and replace the modules while the system is powered on. See “Removing and Replacing the Route Control Processor” on page 17-8 for removal and replacement of RCPs.

If you remove an IOA or IOP from a slot and replace it with a different type of card (for example, if you reconfigure the system and replace an OC-3 ATM IOP with an OC-3 POS IOP or an OC-3 ATM IOA with a OC-12 ATM IOA), you must remove the old configuration for the slot for the new card to function properly. The following procedure explains how to do this.

► We suggest that you remove and replace only one module at the time to ensure that each module is installed in the correct slot.

⚠ When handling modules, always attach the ESD (electro-static discharge) strap to your wrist and connect the banana plug end of the strap into the ESD socket in the chassis. Refer to Figure 17-1 and Figure 17-2 for location of ESD sockets.

⚠ This equipment is a Class 1 Laser Product and is intended for connection to Class 1 devices only. Lasers used in this equipment meet the regulatory requirements for casual exposure to the eye, however it is recommended that you do not look directly into the laser light source.

⚠ When an IOP slide latch is opened and then immediately closed, it causes the card to remain in a quiescent state. To put the card back into an operational state either:

- Re-open the card’s slide latch and then wait 10 seconds before closing it again

or:

- at the CLI card-level prompt, enter:

```
TMX 880(cards)# shutdown ioc #
TMX 880(cards)# no shutdown ioc #
```

(where # is the slot number of the card to be enabled)

► Running commands to manually deactivate a card results in an alarm condition. The physical removal of a card deactivates the associated card alarm. See the Chapter 3, “Reviewing System Alarms and Status Indicators” for more information on working with the alarm subsystem.

To remove a card module from the chassis:

1. To remove a card from the chassis, first shutdown the card following the instructions in the table below, then proceed to step 2.

For this type card	Do this
I/O Processors (IOP) and/or I/O Adapters (IOA) (The CLI refers to IOPs as IOCs, I/O Controllers)	• If the RUN LED is illuminated on the card, shutdown the card from the CLI using a command in the form: `TMX 880(cards)#` **`shutdown ioc`** ***`slot-number`*** Wait for the card to be in the **Quiescent** state. You can check the card's state by executing the **show all** command. `TMX 880(cards)#` **`show all`** • If you are *changing an IOA or IOP* from one type to another, for example from OC-3 to OC-12, remove the configuration for the existing card: `TMX 880#` **`configure terminal`** `TMX 880(config)#` **`no interface`** ***`interface_name`*** At the prompt, press **`y`** to confirm erasing the old configuration. • If the RUN LED is not illuminated on the card, proceed to step 2.
SONET Timing and Adapter (STA)	• If the RUN LED is illuminated on the card, shutdown the card from the CLI using a command in the form: `TMX 880(cards)#` **`shutdown sta`** ***`slot-number`*** Wait for the card to be in the **Quiescent** state. You can check the card's state by executing the **show all** command. `TMX 880(cards)#` **`show all`** • If the RUN LED is not illuminated on the card, proceed to step 2.
Switch Fabric (SF. The CLI refers to it as SFC, Switch Fabric Controller.)	• If the RUN LED is illuminated on the card, shutdown the card from the CLI using a command in the form: `TMX 880(cards)#` **`shutdown sfc`** ***`slot-number`*** Wait for the card to be in the **Quiescent** state. You can check the card's state by executing the **show all** command. `TMX 880(cards)#` **`show all`** • If the RUN LED is not illuminated on the card, proceed to step 2.

⚠ The cards have three sates during shutdown: **`goingdown`**, **`buffermanagement`**, and **`quiescent`**. If the cards are removed from the chassis while in the **`buffermanagement`** state, they may not reboot without doing a chassis reload.

2. Remove all cables from the faceplate connectors.

⚠ Before removing the SONET and Ethernet cables from the adapter ports make sure that the cables are labeled so you can reconnect them to the correct ports.

3. Using a number 2 Phillips-head screwdriver, loosen the captive screws at both ends of the faceplate.
4. Slide the latch down or up depending on the card location in the chassis.

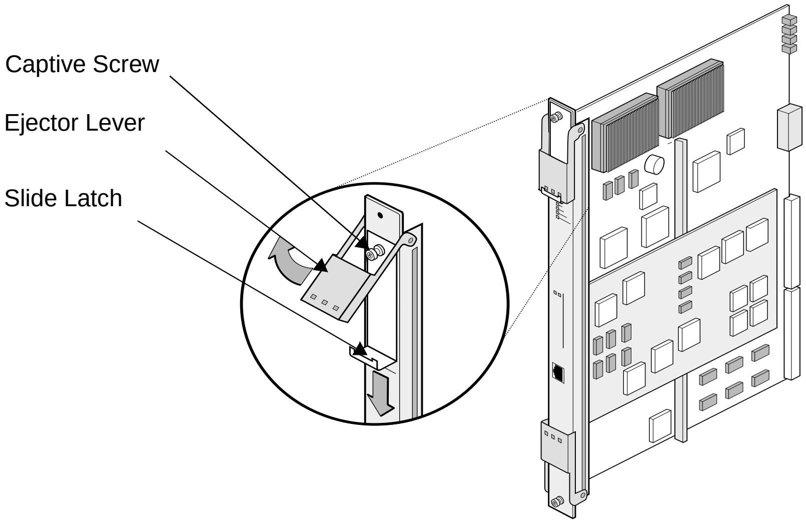


Figure 17-3. Card Latch Mechanism

5. Open the ejector levers at both ends of the faceplate. Carefully slide the card out by initially pulling on the ejector levers and then holding it by its sides.

To install a card module into the chassis:

1. Remove the new module from its antistatic bag observing the proper ESD precautions.

⚠
- To maintain proper airflow through the system, make sure to install all IOPs in the slot sequence described in the installation guide for the system.
- Retain filler panels over all unused card slots.

2. Before inserting the board into the slot, make sure that the board is oriented properly as indicated in Table 17-1.

Table 17-1. System Module Orientation in Chassis

Switch/Router	IOP and SF Latch Orientation	IOA and STA Latch Orientation
Top row	Toward top of chassis	Toward bottom of chassis
Bottom row	Toward bottom of chassis	Toward top of chassis

3. With the ejector levers up (open), hold the module on opposite ends of the faceplate, and carefully guide it into the top and bottom card cage rails. Slowly slide the module along the tracks until the ejector levers contact the chassis.

4. When the ejector-lever hooks catch the lip of the card cage, push both levers down until they are flush with the faceplate. The LEDs on the card illuminate.

⚠ The chassis has a key mechanism to prevent incompatible card installation. It is critical that if you feel any resistance when seating a card, you remove it and double check that you have the correct card type and orientation (depending on top or bottom slots). Do not force a card into a slot.

5. Lock the slide-latch into place (up or down depending on slot location). This activates the card.

6. Tighten the captive screws at the top and bottom of card.

7. Re-connect all cables.

⚠ If you have replaced an IOA, ensure that you reconnect each cable to the correct port.

8. If you have replaced a card with the same type of card, follow the steps outlined in the table below.

For this type card	Do this

I/O Processor (IOP)
I/O Adapters (IOA)
	Reload the card by executing the card **reload** command as shown below:
	`TMX 880#` **`cards`**
	`TMX 880(cards)#` **`reload`** ***`ioc slot_number`***
	`TMX 880(cards)#`

SONET Timing/Alarm (STA)	No action required. When you replace the card, it should automatically reload. When you add a second STA, the system automatically recognizes the card.

For this type card	Do this

Switch Fabric (SF)	• If you remove and replace a SF in a system that has a single SF, you must reload the chassis by executing the router **reload chassis** command as shown below:
	`TMX 880# cards`
	`TMX 880(cards)# reload chassis`
	`Reload the entire chassis ? [Y/N]y`
	`Confirm reload? <yes|no>y`
	`        The system is being rebooted...`
	`.`
	`.`
	`.`
	• If you remove and replace a SF in a system that has more than one SF, the SF will become active as soon as you close the latch. The new SF buffers are allocated in minutes and the card becomes fully operational.

Refer to the *TMX 880 Command Reference* for further details about the **reload** command available at the `TMX 880(cards)#` prompt.

Removing and Replacing the Route Control Processor

The TMX 880 system supports one (primary) route control processor (RCP) or two RCPs, a primary and a secondary RCP. In a redundant configuration, a system with two RCPs, if the primary RCP should fail the secondary RCP will run the system.

► In a system with two RCPs, if a primary RCP fails so that the secondary RCP takes over, you should replace the primary RCP.

The system displays the switchover logging messages whenever an RCP becomes active, fails, or in a redundant system when the secondary RCP takes over for the primary RCP. See the section on configuring cards and interfaces in the *TMX 880 Configuration Guide* for more information on switchover logging messages.

Systems with a Single RCP

If you need to replace a single RCP in the system, follow the steps below to remove it and replace it. You do not need to shutdown and reload the RCP. After you install the new RCP, the system reboots automatically.

To remove the RCP from the chassis:

1. Disconnect the Ethernet and console cables from the RCP.
2. Remove the PCMCIA card from the slot.
3. Using a number 2 Phillips-head screwdriver, loosen the 4 captive screws (2 at the top and 2 at the bottom) that fasten the RCP to the chassis.
4. Pull the RCP out of the chassis by first pulling on its handle and then by holding it securely on both sides by the metal carrier.

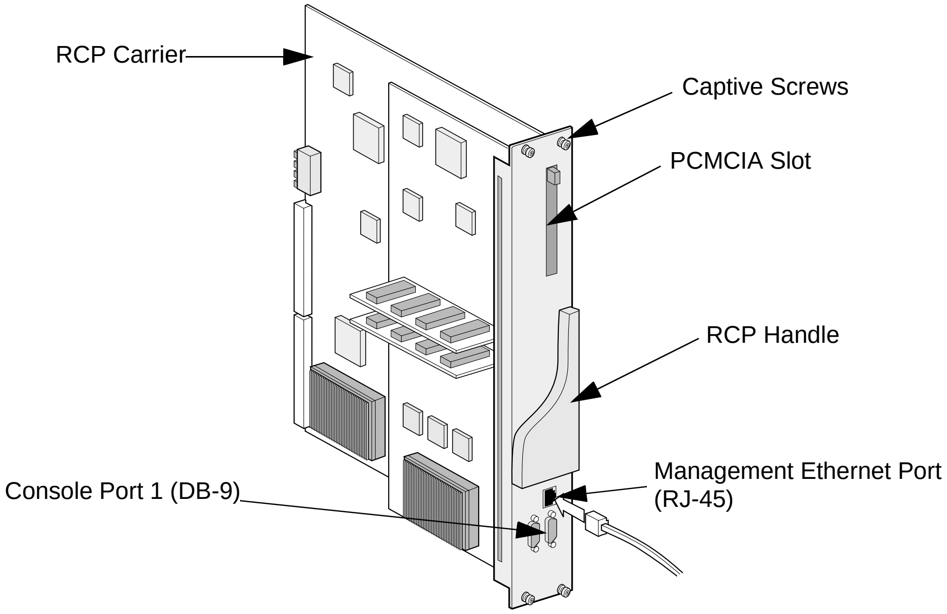


Figure 17-4. Route Control Processor Module

To install an RCP into the chassis:

1. Remove the replacement RCP from its anti-static bag.
2. Insert the PCMCIA card into its slot.
3. Orient the RCP module so that the PCMCIA slot is at the top (see Figure 17-4).
4. If you are installing the RCP in the CP0 slot, align the RCP carrier with the second rail from the left. If you are installing the RCP in the CP1 slot, align the RCP carrier with the first rail from the right.
5. Slide the card in gently until it is seated completely in the slot.

   The system now reboots.
6. Reinstall the Ethernet and console cables.
7. Using a Phillips-head screwdriver tighten the captive screws.

Systems with Two RCPs

The TMX 880 system is configurable with one or two RCP modules (primary and secondary). You can add a second (redundant) RCP to the system dynamically, without rebooting, and with no data loss or degradation in performance. In a redundant configuration, if the primary RCP should fail the secondary RCP will run the system. With BGP graceful restart and OSPF graceful restart support, the RCP disperses the routing data to each line card, allowing the system to provide uninterrupted service should an RCP failure occur.

In a redundant system, you execute CLI commands from the primary RCP. After the system has booted, a TMX 880 system with one RCP, has the default prompt, `TMX 880#,` displayed on the RCP management console. For systems with two RCPs, the management console of the primary RCP also displays the default prompt, `TMX 880#`. The management console of the second RCP displays the prompt `standbyRCP#`.

To do this	Use this command
Reload a specific RCP controller.	**reload rcp {0 | 1}**
Reload the RCP in a system running a single RCP	**reload rcp-primary**
In a redundant system, to determine which RCP is the secondary and reboot that RCP, which then remains in standby mode.	**reload rcp-secondary**

► If you manually switch RCPs, (by running the **reload** command for example) wait until the default prompt is displayed on the CLI before switching back to the original RCP.

To add a secondary RCP to a system running with one RCP:

1. Before adding the RCP, save the running configuration file to the PCMCIA card on the primary RCP as follows:

```
TMX 880# copy running-config startup-config
```

2. Remove the second RCP from its anti-static bag.
3. Insert the PCMCIA card into its slot.

► Make sure that the PCMCIA card, in the secondary RCP, is of equal size to the PCMCIA card in the primary RCP before running the **copy sync** command.

► When coping the configuration file to the secondary RCP PCMCIA card, the primary RCP and the secondary RCP must contain the same version of the MXOS software.

4. Orient the RCP module so that the PCMCIA slot is at the top (see Figure 17-4).
5. If you are installing the RCP in the CP0 slot, align the RCP carrier with the second rail from the left. If you are installing the RCP in the CP1 slot, align the RCP carrier with the first rail from the right.
6. Slide the card in gently until it is seated completely in the slot.
7. Install the Ethernet and console cables.
8. Using a Phillips-head screwdriver tighten the captive screws.
9. Copy the running configuration file to the PCMCIA card on the second RCP as follows:

```
TMX# copy sync file config
```

10. Run the **reload rcp-secondary** command to run the updated image file on the secondary RCP. The secondary RCP does not take over for the primary RCP when you run the **reload rcp-secondary** command. For example:

```
TMX 880# cards
TMX 880(cards)# reload rcp-secondary
Working...DONE
TMX 880(cards)#
```

To remove one of the two RCPs installed in the system:

► You can remove and replace either the primary or secondary RCP while the system is powered on.

1. Before replacing an RCP, save the running configuration file to the PCMCIA card on the primary RCP as follows:

```
TMX 880# copy running-config startup-config
```

► When a redundant RCP is present in the system and you issue the **copy running-config startup-config** command, the system automatically copies both the startup configuration file and the backup file of the startup configuration to the secondary RCP.

2. Disconnect the Ethernet and console cables from the RCP you want to remove.
3. Remove the PCMCIA card from the slot.
4. Using a number 2 Phillips-head screwdriver, loosen the 4 captive screws (2 at the top and 2 at the bottom) that fasten the RCP to the chassis.
5. Pull the RCP out of the chassis by first pulling on its handle and then by holding it securely on both sides by the metal carrier.

To install a replacement RCP into a redundant system:

1. Remove the replacement RCP from its anti-static bag.
2. Insert the PCMCIA card into its slot.
3. Orient the RCP module so that the PCMCIA slot is at the top (see Figure 17-4).
4. If you are installing the RCP in the CP0 slot, align the RCP carrier with the second rail from the left. If you are installing the RCP in the CP1 slot, align the RCP carrier with the first rail from the right.
5. Slide the card in gently until it is seated completely in the slot.
6. Reinstall the Ethernet and console cables.
7. Using a Phillips-head screwdriver tighten the captive screws.

PCMCIA Card Backup

By executing the **copy sync *all*** command, you can copy the contents of the entire PCMCIA card to a secondary RCP as a backup in case of failure of the original RCP. For example:

```
TMX 880# copy sync all
```

When executing this command, the PCMCIA card in the second RCP is reformatted and thus deletes all the old files on the card. Although this command means “duplicate the card”, the following files and directories will not be copied:

- The .del files which are the deleted files
- The “inet on Ethernet” boot parameter.

Setting the Location of the Startup Configuration File

If the name or location of the startup configuration is different from the default file and path names, pcmcia0/startup.cfg, you need to set the location of the startup configuration file for the RCP.

You set the location of the boot configuration file by running the **boot config** command:

```
TMX 880(config)# boot config full-path-name-of-the-configuration-file
```

For example:

```
TMX 880(config)# boot config /pcmcia0/startupnew.cfg
```

If this is not done, subsequent **write memory** or **copy running-config startup-config** commands complete with no error, but do not save the running configuration anywhere.

Fan Tray Removal and Replacement

To remove a fan tray assembly from the chassis:

⚠ Do not operate the TMX 880 MPLS Core Switch with one of the fan trays removed for more than one (1) minute.

1. Locate the replacement fan, unpack it, and have it ready for immediate installation.

The table below can help you make sure that you have the correct replacement fan tray.

Fan Tray	How to recognize it
Top front fan tray	At the bottom of the front panel there is a strip with chassis slot numbers.
Bottom front fan tray	At the top of the front panel there is a strip with chassis slot numbers. The strip has two holes in it for the ESD Strap sockets to show through them.
Top rear fan tray	Fan tray front panel has Lucent logo and 2 fixed handles.

2. Notice the slides on each side of the fan tray so you will be able to quickly match these slides with the ones in the chassis.
3. Depending on the fan tray to be replaced, if necessary, remove the top or bottom bezel from the front of the chassis.
4. Using a Phillips-head screwdriver, loosen the 6 captive screws on fan tray to be replaced.
5. Pull the fan tray towards you then, holding it firmly by the sides, pull it out of the chassis. (A stout pull may be necessary to disengage the connectors at the rear of the fan tray from the chassis connectors.)

To replace a fan tray assembly into the chassis:

1. Align the fan tray with its designated bay and insert it into the bay as shown in Figure 17-5.

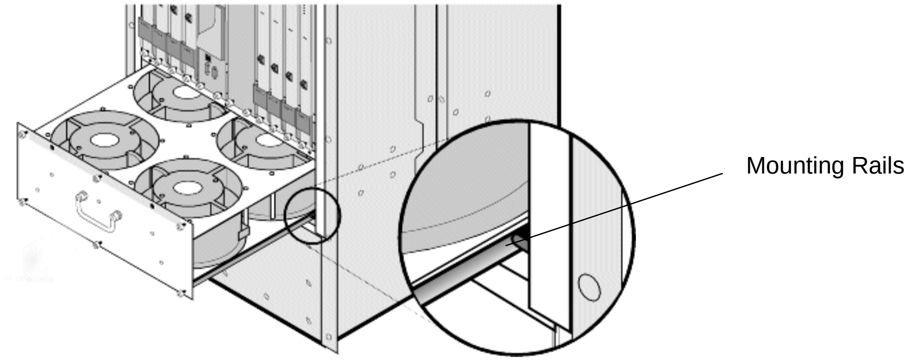


Figure 17-5. TMX 880 MPLS Core Switch Fan Tray

2. Carefully push the fan tray into place to seat the connector at the rear of the assembly into its mating chassis connector.

⚠ Do not force the connector at the back of the assembly into the mating chassis connector because you could damage the connector.

3. The fan green LED should now be on.
4. With the faceplate of the fan tray assembly flush with the chassis, tighten the 6 captive screws to secure the assembly into place.

PDU Removal and Replacement

This section describes how to remove and replace a PDU. Use Figure 17-6 as a reference for this operation.

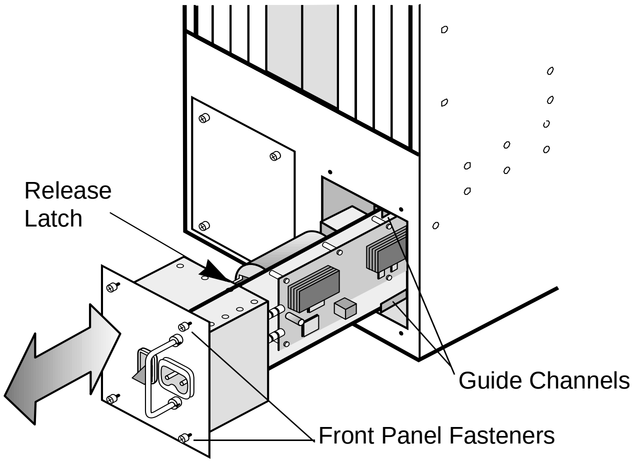


Figure 17-6. PDU Removal

To remove the PDU from the chassis:

⚠ A PDU displaying a green LED must not be removed from an operating system unless the second PDU is also displaying a green LED. A single green LED indicates that only a single PDU is operational. If this PDU is removed the system will crash.

1. Turn off power to the PDU by setting the PDU front-panel circuit breaker switch to the OFF position.

   ⚠ After the PDU is switched off, the amber light comes on. Wait until the amber light is totally extinguished again before unlatching and removing the power connector from the PDU. (It takes about two minutes for the amber light to be totally extinguished.)

2. Unlatch the DC input line connector by turning the **T** handle on the connector counter-clockwise and remove the connector from the PDU socket.
3. Loosen and disengage the four captive screws on the faceplate of the PDU.
4. Pull the PDU forward until the mechanical latch prevents further travel. Depress the mechanical latch and pull the PDU past the latch point and out of the chassis. (A stout pull may be necessary to disengage the interface connectors at the rear of the PDU from the chassis connector.)

To install a PDU into the chassis:

1. Ensure that the circuit breaker switch on the PDU that you are about to install in the chassis is in the OFF position.

2. Align the PDU with the guide channel(s) at the top and bottom of the PDU bay in the chassis.

3. Slide the PDU into the bay and ensure that the mating connectors on the PDU and chassis are fully engaged.

> ⚠ Do not use excessive force in mating the PDU connector to the system connector since this may damage the connector pins.

4. Engage and tighten the 4 front-panel captive screws.

5. Plug the DC line cord into the PDU socket and turn the **T** handle clockwise to fully engage the connection.

6. With the PDU circuit breaker in the OFF position, apply power at the DC source.

7. Use a voltmeter to check the voltage at the test points on the top of the power connector (see Figure 17-7) to ensure a nominal -48 volts DC source.

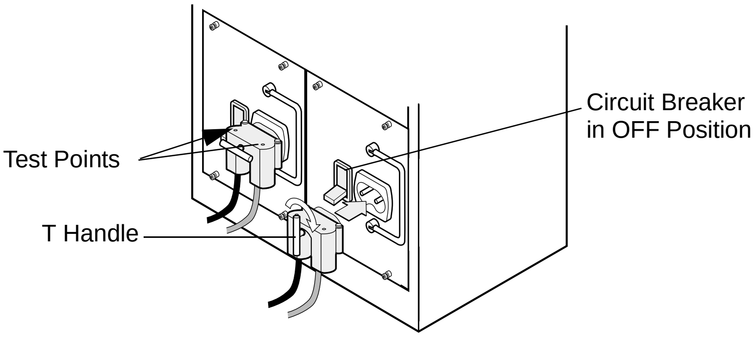


Figure 17-7. PDU Circuit Breaker Position

8. Power up the PDU by turning the circuit breaker to the ON position.

   After approximately 30 seconds the front panel LED labeled “Power OK” should be illuminated.

Inspecting and Replacing the Air Filter

The air filter in the TMX 880 MPLS Core Switch should be inspected every 3 months and should be replaced if it appears quite dirty. Filters should be replaced at least every 6 months.

The air filter is located at the bottom of the chassis and is accessed from the rear of the system, refer to Figure 17-8. To remove or replace the filter, lift the power cables out of the way and pull the filter toward you or insert it into the filter slots. Install the filter with the metal mesh side up.

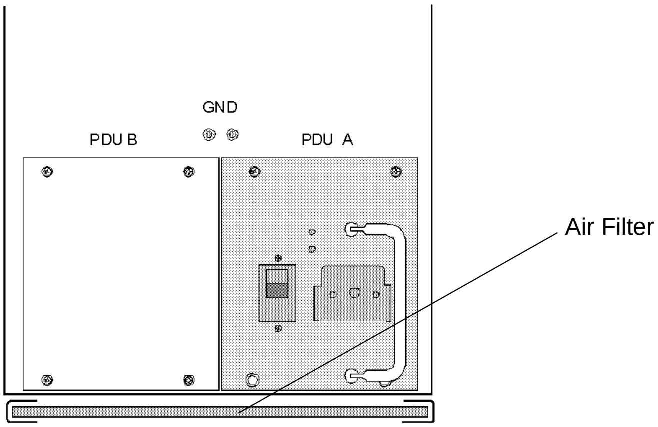


Figure 17-8. TMX 880 MPLS Core Switch Air Filter

A

Power Requirements and Optical Specifications

The tables in this appendix provide IOP and IOA DC and optical power requirements and optical specifications.

System Power Requirements

The TMX 880 MPLS Core Switch uses nominal -48VDC distributed power. The system electrical rating has a range of -42VDCto -60VDC (150A). However, the system uses only the power necessary to support the modules in use. Table 2-3 lists the TMX 880 system and module power requirements.

Table A-1. TMX 880 System and Module Power Requirements

System/Module	Current Draw (Amps)	Power Consumption (Watts)
Base Chassis - 1 PDU, 3 Fans	3.6	155
Route Control Processor	0.7	30
SONET Timing/Alarm	0.4	17
Switch Fabric	4.1	176
IOP-OC3-POS with IOA	4.3	186
IOP-OOC3-ATM with IOA	5.3	228
IOP-DOC12-ATM with IOA	5.2	224
IOP-QOC12-POS with IOA	4.5	193.5
IOP-SOC48-POS with IOA	4.8	206
IOP-QOC-48c POS with IOA	4.6	197.8
IOP-SOC192-POS with IOA	5.2	224

Table A-1. TMX 880 System and Module Power Requirements

System/Module	Current Draw (Amps)	Power Consumption (Watts)
IOP D-Gigabit Ethernet with IOA	4.5	193.5
IOP Q-Gigabit Ethernet with IOA	5.2	250.0
Notes: *Power calculations are based on a -43V input power source.* *IOP designations use the following conventions: S = single or 1-port; D = dual or 2-port; Q = quad or 4-port; O = octal or 8-port.*		

► Lucent recommends that you increase the total power-consumption number by 10% - 15% when provisioning power to the chassis to allow for module-to-module variation.

Optical Specifications

Table A-2. "Line Card SIgnal Levels" lists optical specifications for the system:

Table A-2. Line Card SIgnal Levels

Line Card	Min. Output Power(dBm)	Max. Output Power(dBm)	Min. Input Power(dBm)	Max. Input Power(dBm)
8-port OC-3c ATM Short Reach, Multimode Maximum Distance: 2 km	-23.5	-14	-30	-14
8-port OC-3c POS Short Reach Multimode Maximum Distance: 2 km	-23.5	-14	-30	-14
2-port OC-12c ATM Intermediate Reach, Single-mode Maximum Distance: 15 km	-15	-8	-31	-8
4-port OC-12c POS Intermediate Reach, Single-mode Maximum Distance: 15 km	-15	-8	-31	-8
1-port OC-48c POS Short Reach, Single-mode Maximum Distance: 2 km	-10	-3	-18	0
4-port OC-48c POS Short Reach, Single-mode Maximum Distance: 2 km	-10	-3	-18	-3

Line Card	Min. Output Power(dBm)	Max.Output Power(dBm)	Min. Input Power(dBm)	Max. Input Power(dBm)
1-port OC-192c POS Very Short Reach, Single-mode, (VSR-1) Maximum Distance: 600 m	-6	-1	-11	-1
1-port OC-192c POS Short Reach, Single-mode, (SR-1) Maximum Distance: 12 km	-6	-0	-11	-1
1-port OC-192c POS Intermediate Reach, Single-mode, (IR-1) Maximum Distance: 40 km	-1	2	-14	-3
2-port Gigabit Ethernet Short Reach, Multimode (SX) Maximum Distance: 500 m	-9.5	-4	-17	0
2-port Gigabit Ethernet Long Reach, Single-mode (LX) Maximum Distance: 10 km	-9.5	-3	-20	-3
8-port Gigabit Ethernet Short Reach, Multimode (SX) Maximum Distance: 1 km	-17	-9.5	-4	-3
8-port Gigabit Ethernet Long Reach, Multimode (LXS) Maximum Distance: 10 km	-9	-3	-20	-3
8-port Gigabit Ethernet Long Reach, Single-mode (LXL) Maximum Distance: 25 km	-20	-9.0	-3.0	-3.0
8-port Gigabit Ethernet Ultra Long Haul Reach, Single-mode (ZX) Maximum Distance: 70 km	-23.0	-3.0	-3.0	2.0

B

Adapter Card Connections

This appendix lists the types of connectors used on the TMX 880 MPLS Core Switch.

Connector Types

The TMX 880 system uses SC, LC, MTRJ, and SMB connectors to connect the line cards to the network. The following table lists the connectors required by each card:

Table B-1. Adapter Cable Connectors Usage

Connector type	For this card
MTRJ connector multimode duplex	• 8 port OC-3c IOA ATM • 8 port OC-3c IOA POS • 2 port Gigabit Ethernet IOA Lucent recommends using Volex, FCI or Computer Crafts MTRJ connector.
SC connector single-mode duplex	• 1 port OC-48c IOA POS • 4 port OC-48 IOA POS • 1 port OC-192c IOA POS
LC connector single-mode duplex	• 2 port OC-12 IOA ATM • 4 port OC-12 IOA POS • 8-port Gigabit Ethernet IOA

C

Safety Instructions

Important Safety Instructions

Observe the following safety guidelines to prevent physical injury and to prevent damage to the equipment when installing or operating the Lucent TMX$^{\text{TM}}$ 880 MPLS Core Switch.

⚠ This symbol notifies the reader to proceed carefully to avoid possible equipment damage or data loss.

⚡ This symbol notifies the reader to proceed carefully to avoid possible personal injury.

- The Lucent TMX 880 MPLS Core Switch must be installed in a *restricted access* location by authorized customer or Lucent personnel and must be installed on a dry, non-flammable surface, preferably concrete.
- Before installing the system, locate the emergency power switch or breaker for the equipment on which you are working and make sure it is set to OFF.
- Disconnect all power and external cables *before* moving a chassis.
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check.
- Do not do anything that creates a potential hazard to people or makes the equipment unsafe.
- Carefully examine your work area for possible hazards such as wet floors, ungrounded power extension cables, and missing safety grounds.

Laser Class 1

This equipment is a Class 1 Laser Product and is intended for connection to Class 1 devices only. Lasers used in this equipment meet the regulatory requirements for casual exposure to the eye, however it is recommended that you do not look directly into the laser light source.

Consignes de sécurité importantes

Respectez les consignes de sécurité suivantes pour prévenir les dommages physiques et les dégâts qui pourraient être occasionnés à l'équipement lors de l'installation ou du fonctionnement du commutateur TMX 880 MPLS Core Lucent:

⚠ Ce symbole avertit le lecteur de procéder prudemment afin de prévenir les risques d'endommagement du matériel ou d'altération des données.

⚡ Ce symbole invite le lecteur à procéder prudemment afin d'éviter les risques de blessures corporelles.

- Le commutateur TMX 880 MPLS Core Lucent doit être installé à un emplacement dont *l'accès est limité* au client autorisé ou au personnel Lucent et doit être installé sur un sol sec, non-inflammable et de préférence en béton.
- Avant de procéder à l'installation, identifiez le commutateur de marche-arrêt d'urgence ou le coupe-circuit de l'équipement sur lequel vous travaillez et assurez-vous qu'il est en position OFF.
- Mettez hors tension tous les câbles électriques et externes *avant* de déplacer un châssis.
- Veillez à ne pas travailler seul en présence de conditions de danger potentielles.
- Vérifiez TOUJOURS que le circuit est effectivement hors tension; ne vous limitez jamais à le supposer.
- Ne procédez jamais à aucune opération pouvant être à l'origine de dangers potentiels pour les personnes ou pouvant rendre l'équipement dangereux.
- Examinez soigneusement la zone de travail et considérez les sources de danger éventuelles telles que les sols mouillés, les câbles de rallonge non mis à la terre et les masses de sécurité manquantes.

Laser de Classe 1

Cet équipement est un Produit Laser de Classe 1; il doit par conséquent être raccordé exclusivement à des appareils de Classe 1. Les lasers utilisés dans cet équipement sont conformes aux normes réglementaires en cas d'exposition accidentelle des yeux, il est toutefois recommandé de ne pas regarder directement la source d'émission laser.

Wichtige Sicherheitshinweise

Bitte beachten Sie die folgenden Sicherheitsrichtlinien, um Körperverletzungen und Geräteschäden zu vermeiden, wenn Sie den TMX 880 MPLS Core Schalter von Lucent:

⚠ Dieses Symbol weist den Leser darauf hin, vorsichtig fortzufahren, um möglichen Geräteschaden oder Datenverlust zu vermeiden.

⚡ Dieses Symbol weist den Leser darauf hin, vorsichtig fortzufahren, um möglichen Körperverletzungen vorzubeugen.

- Der TMX 880 MPLS Core Schalter von Lucent muß von vom Kunden autorisierten oder Lucent-Personal an einem Ort mit *beschränktem Zugang* auf einer trockenen, nicht brennbaren Oberfläche, bevorzugt Zement, installiert werden.
- Vor der Installation vergewissern Sie sich, wo sich der Notstromschalter bzw. Notunterbrecher befindet und daß er sich in der abgeschalteten Position (OFF) befindet.
- Stecken Sie alle Strom- und externen Kabel aus, *bevor* Sie ein Chassis verschieben.
- Arbeiten Sie unter potentiell gefährlichen Bedingungen nicht alleine.
- Gehen Sie niemals davon aus, daß keine Spannung am Schaltkreis anliegt, prüfen Sie dieses immer nach.
- Unternehmen Sie nichts, was für andere Personen zur Gefahr werden könnte oder die Anlage unsicher machen könnte.
- Überprüfen Sie Ihren Arbeitsplatz sorgfältig auf mögliche Gefahren wie z.B. feuchte Böden, nicht geerdete Stromverlängerungskabel und fehlende Schutzleiter.

Laser Klasse 1

Diese Anlage ist ein Produkt der Laser Klasse 1 und ist ausschließlich für den Anschluß an Geräte der Klasse 1 vorgesehen. Die mit dieser Anlage verwendeten Laser erfüllen die Vorschriften für versehentliches Exponieren der Augen, es wird jedoch empfohlen, nicht direkt in die Laserlichtquelle zu schauen.

Importantes instrucciones de seguridad

Observe las siguientes pautas de seguridad para prevenir daños personales y al equipo al instalar u operar TMX™ 880 MPLS Core Switch de Lucent:

⚠ Este símbolo le indica al lector que debe proceder con cuidado para evitar pérdida de datos o daño al sistema.

⚡ Este símbolo le indica al lector que debe proceder con cuidado para evitar daño personal.

- TMX™ 880 MPLS Core Switch de Lucent lo debe instalar en un *área de acceso restringido* el personal de Lucent o personal autorizado por el cliente y debe instalarse en una superficie seca y no inflamable, preferiblemente de cemento.
- Antes de instalar el sistema, busque dónde se encuentra el interruptor de corriente de emergencia para el equipo en el que está trabajando y asegúrese que esté en la posición OFF (apagado).
- Desconecte la corriente eléctrica y los cables externos *antes* de mover cualquier chasis.
- No trabaje solo si existen condiciones potencialmente peligrosas.
- Nunca asuma que la corriente eléctrica está desconectada, siempre debe comprobarlo antes de ponerse a trabajar.
- No haga nada que cree un riesgo potencial para otras personas o que comprometa la seguridad del equipo.
- Examine con cuidado su área de trabajo para comprobar que no haya peligros, tales como suelos mojados, cables de extensión de corriente no conectados a tierra y la falta de conexiones a tierra de seguridad.

Láser clase 1

Este equipo es un producto Láser de clase 1 y tiene como objetivo su conexión a dispositivos de la clase 1 solamente. Los láseres usados en este equipo cumplen los requisitos necesarios para la exposición a los ojos. Sin embargo, se recomienda que no mire directamente a la fuente de luz del láser.

重要的安全说明

在安装或操作 Lucent TMX^{TM} 880 MPLS Core Switch 时，请遵循如下安装指南以避免造成人身伤害和设备损坏：

⚠ 本符号提醒读者小心操作，以免损坏设备或丢失数据。

⚠ 本符号提醒读者小心操作，以免造成可能的人身伤害。

- 必须将 Lucent TMX^{TM} 880 MPLS Core Switch 安装在一“禁止入内”的区域。必须由授权客户或朗讯工作人员实施安装，且必须安装在干燥、不易燃的地面上，最好是混凝土地面。
- 在安装该系统前，请查看设备的电源或断路器，确保其已被设置为 “关闭”。
- 在移动底板以前，断开所有电源和外接电缆。
- 如果存在潜在的危险情况，切勿单独工作。
- 在亲自进行查看以前，切勿臆断已经断开电源。
- 不要进行可能伤害他人或损坏设备的任何操作。
- 仔细检查工作区，确保没有潜在危险，如湿地板、未接地的电源扩展电缆和没有安全接地。

类激光

本设备属于 1 类激光产品，只能用于 1 类设备的连接。本设备所使用的激光符合对人眼辐照的规定要求，不过，请最好不要直视激光光源。

安全上の重要注意事項

ルーセント TMX$^{\text{TM}}$ 880 MPLS Coreスイッチを設置または操作する際、人体の怪我および装置の損傷を予防するため、以下の安全ガイドラインを守ってください。

⚠ このシンボルは、装置の損傷あるいはデータの損失を予防するため、注意して先へ進むよう警告するためのものです。

⚠ このシンボルは、人体の怪我を予防するため、注意して先へ進むよう警告するためのものです。

- ルーセント TMX$^{\text{TM}}$ 880 MPLS Core スイッチは、許可されたお客様またはルーセントの作業員が、*入室制限*ロケーションに設置すること。また、乾燥した非可燃性の床（できればコンクリート）上に設置すること。
- システムを設置する前に、作業する装置の非常用電源スイッチまたはブレーカの位置を確認し、それがオフになっているのを確認すること。
- シャーシを移動する*前に*、すべての電源および外部ケーブルを切断すること。
- 危険な状況が潜在する場合には、一人で作業しないこと。
- 電源が回線から切断されていると思い込まずに、常にチェックすること。
- 人体に潜在的な危険を及ぼしたり、装置を安全でない状態にするようなことはしないこと。
- 床が濡れている、電源延長ケーブルがアースされていない、安全なアースがない等、作業エリアに危険が潜在していないかどうか、注意深く調べること。

レーザクラス1

この装置はクラス１のレーザ製品であり、クラス１機器接続専用です。この装置で使用されているレーザは、軽度の目への照射についての規定要件は満たしていますが、レーザ光源を直接見つめないことをお勧めします。

Laser Safety Guidelines

General Laser Information

Optical fiber telecommunication systems, their associated test sets, and similar operating systems use semiconductor laser transmitters that emit infrared (IR) light at wavelengths between approximately 800 nanometers (nm) and 1600 nanometers. The emitted light is above the red end of the visible spectrum, which is normally not visible to the human eye. Although radiant energy at near-IR wavelengths is officially designated invisible, some people can see the shorter wavelength energy even at power levels several orders of magnitude below any that have been shown to cause injury to the eye.

Conventional lasers can produce an intense beam of monochromatic light. The term monochromaticity means a single wavelength output of pure color that may be visible or invisible to the eye. A conventional laser produces a small-size beam of light, and because the beam size is small the power density (also called irradiance) is very high. Consequently, lasers and laser products are subject to federal and applicable state regulations as well as international standards for their safe operation.

A conventional laser beam expands very little over distance, or is said to be very well collimated. Thus, conventional laser irradiance remains relatively constant over distance. However, lasers used in lightwave systems have a large beam divergence, typically 10 to 20 degrees. Here, irradiance obeys the inverse square law (doubling the distance reduces the irradiance by a factor of 4) and rapidly decreases over distance.

Lasers and Eye Damage

The optical energy emitted by laser and high-radiance LEDs in the 400-1400 nm range may cause eye damage if absorbed by the retina. When a beam of light enters the eye, the eye magnifies and focuses the energy on the retina magnifying the irradiance. The irradiance of the energy that reaches the retina is approximately 10^5 or 100,000 times more than at the cornea and, if sufficiently intense, may cause a retinal burn.

The damage mechanism at the wavelengths used in an optical fiber telecommunications is thermal in origin, that is, damage caused by heating. Therefore, a specific amount of energy is required for a definite time to heat an area of retinal tissue. Damage to the retina occurs only when one looks at the light sufficiently long that the product of the retinal irradiance and the viewing time exceeds the damage threshold. Optical energies above 1400 nm cause corneal and skin burns but do not affect the retina. The thresholds for injury at wavelengths greater than 1400 nm are significantly higher than for wavelengths in the retinal hazard region.

Classification of Lasers

Manufacturers of lasers and laser products in the U.S. are regulated by the Food and Drug Administration’s Center for Devices and Radiological Health (FDA/CDRH) under 21 CFR 1040. These regulations require manufacturers to certify each laser or laser product as belonging to one of four major Classes: I, II, lla, IlIa, lllb, or IV. The International Electro-technical Commission is an international standards body that writes laser safety standards under IEC-60825. Classification schemes are similar with Classes divided into Classes 1, 2, 3A, 3B, and 4. Lasers are classified according to the accessible emission limits and their potential for causing injury. Optical fiber telecommunication systems are generally classified as Class I/1, because, under normal operating conditions, all energized laser transmitting circuit packs are terminated on optical fibers which enclose the laser energy with the fiber sheath forming a protective housing. Also, a protective housing / access panel is typically installed in front of the laser circuit pack shelves. The circuit packs themselves, however, may be FDA/CDRH Class I or IIIb or IEC Class 1, 3A, or 3B.

Laser Safety Precautions for Optical Fiber Telecommunication Systems

In its normal operating mode, an optical fiber telecommunication system is totally enclosed and presents no risk of eye injury. It is a Class I/1 system under the FDA and IEC classifications.

The fiber optic cables that interconnect various components of an optical fiber telecommunication system can disconnect or break, and may expose people to laser emissions. Also, certain measures and maintenance procedures may expose the technician to emission from the semiconductor laser during installation and servicing. Unlike more familiar laser devices, such as solid-state and gas lasers, the emission pattern of a semiconductor laser results in a highly divergent beam. In a divergent beam, the irradiance (power density) decreases rapidly with distance. The greater the distance, the less energy will enter the eye, and the less potential risk for eye injury. Inadvertently viewing an unterminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches normally will not cause eye injury provided the power in the fiber is less than a few milliwatts at the near IR wavelengths and a few tens of milliwatts at the far IR wavelengths. However, damage may occur if an optical instrument such as a microscope, magnifying glass or eye loupe is used to stare at the energized fiber end.

⚠ Use of controls, adjustments and procedures other than those specified herein may result in hazardous laser radiation exposure.

Laser Safety Precautions for Enclosed Systems

Under normal operating conditions, optical fiber telecommunication systems are completely enclosed; nonetheless, the following precautions shall be observed:

1. Because of the potential for eye damage, technicians should not stare into optical connectors or broken fibers.
2. Under no circumstance shall laser/fiber optic operations be performed by a technician before satisfactorily completing an approved training course.
3. Since viewing laser emissions directly in excess of Class I/1 limits with an optical instrument such as an eye loupe greatly increases the risk of eye damage, appropriate labels must appear in plain view, in close proximity to the optical port on the protective housing/access panel of the terminal equipment.

Laser Safety Precautions for Unenclosed Systems

During service, maintenance, or restoration, an optical fiber telecommunication system is considered unenclosed. Under these conditions, follow these practices:

1. Only authorized, trained personnel shall be permitted to do service, maintenance and restoration. Avoid exposing the eye to emissions from unterminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters, Automatic Power Reduction (APR), and Automatic Power Shut Down (APSD) are engineering controls that are also used to limit the emissions. However, technicians removing or replacing laser circuit packs should not stare or look directly into the optical port with optical instruments or magnifying lenses (Normal eyewear or indirect viewing instruments such as Find-R-Scopes are not considered magnifying lenses or optical instruments).
2. Only authorized, trained personnel shall use optical test equipment during installation or servicing since this equipment contains semiconductor lasers (Some examples of optical test equipment are Optical Time Domain Reflectometers (OTDR's), Hand-Held Loss Test Sets, and Feature Finders).
3. Under no circumstances shall any personnel scan a fiber with an optical test set without verifying that all laser sources on the fiber are turned off.
4. All unauthorized personnel shall be excluded from the immediate area of the optical fiber telecommunication systems during installation and service.

Consult ANSI Z136.2 American National Standard for Safe Use of Lasers in the U.S. or outside the U.S., IEC-60825, Part 2 for guidance on the safe use of optical fiber optic communication systems in the workplace.

Internal Laser Circuit Packs Optical Specifications

Laser Circuit Pack Code	Wavelength (nm)	Output Power (mW)	Fiber Type (μm)	Connector Type	FDA Class /IEC Class
OC-3c POS 8-port (LED)	1300	0.04	MM(62.5)	MT-RJ	I/1
OC-3c ATM 8-port (LED)	1300	0.04	MM(62.5)	MT-RJ	I/1
OC-12c POS 4-port	1310	0.158	SM(8.8)	LC	I/1
OC-12c ATM 2-port	1310	0.158	SM(8.8)	LC	I/1
OC-48c POS 4-port	1300	0.5	SM(8.8)	SC Duplex	I/1
OC-48c POS 1-port	1300	1.0	SM(8.8)	SC	I/1
OC-192c POS 1-port					
• Very Short Reach	1310	0.794	SM(9.5)	SC	I/1
• Short Reach, single-mode	1550	1.0	SM(8.8)	SC	I/1
• Intermediate Reach, single-mode	1550	1.58	SM(8.8)	SC	I/1
Gigabit Ethernet 2-port					
• SX	850	0.398	MM(62.5)	MT-RJ	I/1
• LX	1310	0.500	SM(8.8)	MT-RJ	I/1
Gigabit Ethernet 8-port					
• SX	850	0.398	MM(62.5)	Duplex LC	I/1
• LXS	1310	0.500	SM(8.8)	Duplex LC	I/1
• LXL	1310	1.258	SM(8.8)	Duplex LC	I/1
• ZX	1550	1.585	SM(8.8)	Duplex LC	I/1

SX = 1 km typical	LXS = 10 km typical	ZX = 70 km typical
LX = 5 km typical	LXL = 25 km typical	

► Lucent Technologies TMX 880 systems comply with 21CFR 1040.10 and 1040.11 as Class I and IEC 60825-1 Class 1 laser products. They are assessed as IEC-60825-2 Hazard Level 1 Optical Fiber Communication Systems as per Part 4.1.1.

Acronyms

This appendix lists the acronyms used in the documentation.

Acronyms

Acronym	Meaning
AAL	ATM adaptation layer
ABR	area border router *Also:* available bit rate
ACR	allowable cell rate
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	autonomous system
ASBR	autonomous system border router
ASE	autonomous system external
ASP	autonomous system path
ATM	asynchronous transfer mode
Bc	committed burst size
Be	excess burst size
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
BSR	bootstrap router
CAC	connection access control

Acronym	Meaning
CBR	constant bit rate
CDV	cell delay variation
CIDR	classless interdomain routing
CIR	committed information rate
CLI	Command Line Interface
CLNS	connectionless network service
CP	control processor *Usually called* the RCP (route control processor) *Also referred to as* RCC (route control card)
CRC	cyclic redundancy check
CSNP	complete sequence number packets
CSPF	Constrained Shortest Path First
CSU	channel service unit
CTA	Clock Timing Adapter *Also referred to as* TAC (Timing Adapter Controller) *Now referred to as* STA (SONET Timing/Alarm module)
dBm	decibles per milliwatt
DCE	data communications equipment
DF	don’t fragment bit
DIS	designated intermediate system
DLCI	Data Link Connection Identifier
DNS	domain name service
DR	designated router
DS	differential service *Also*: digital signal
DSU	data service unit
DTE	data terminal equipment
DWDM	dense wave division multiplexing

Acronym	Meaning
EBGP	External Border Gateway Protocol
ECMP	equal cost multipath
EGP	External Gateway Protocol
EMS	Element Management System
ESD	electrostatic discharge
ES-IS	End System-to-Intermediate System
FCS	Frame Check Sequence
FEAC	far end alarm control
FECN	forward explicit congestion notification
FPGA	Field Programmable Gate-Array
FR	Frame Relay
FRU	field replacement unit
FTP	File Transfer Protocol
HDLC	high level data link control
IARP	Inverse Address Resolution Protocol
IARP	Inverse Address Resolution Protocol
IBGP	Internal Border Gateway Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
ILMI	Integrated Local Management Interface *Aso*: Interim Local Management Interface
IOA	input/output adapter card
IOC	input/output card *Usually referred to as* IOP (input/output processor)
IOD	input/output daughter card
IOP	input/output processor *Also referred to* as IOC

Acronym	Meaning
IP	Internet Protocol
IPCP	IP Control Protocol
IRP	Interdomain Routing Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-to-Intermediate System
KA	keep alive
Kbps	kilobits per second
LAN	local area network
LAP	Link Access Protocol
LCP	link control protocol
LLC	logical link control
LMI	local management interface
LP	local processor
LSA	link state advertisement
LSP	link state packet *Also:* label switched path
LSR	label switched router
MAC	Media Access Control
Mbps	megabits per second
MBS	maximum burst size
MED	multi-exit discriminator
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MPLS-TE	MPLS traffic engineering
MRU	Maximum Receive Unit
MSDP	Multicast Source Discovery Protocol
MTU	Maximum Transfer Unit

Acronym	Meaning
NAS-IP	network access server IP
NBMA	non-broadcast multiple access
NCP	Network Control Protocol
NET	network entity title
NIC	network interface card
NNI	Network-to-Network Interface
NPDU	network protocol data unit
NRT-VBR	non-real time variable bit rate
NSAP	Network Service Access Point
NSSA	not so stubby area
OAM	operation, administration, and maintenance
OC	Optical Carrier
OL	overload bit
OPT(imum)	Open Packet Trunking
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
PCR	peak cell rate
PDU	protocol data unit *Also:* power distribution unit
PIM	Protocol Indepentent Multicast
PMP	point-to-multipoint
POS	Packet over SONET (Synchronous Optical Network)
PPP	Point-to-Point Protocol
PSNP	partial sequence numbers protocol data unit
PVC	permanent virtual circuit
PVP	permanent virtual path

Acronym	Meaning
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RCC	route control card *Usually referred to as* RCP (route control processor) *Also referred to as* CP (control processor)
RCP	route control processor *Also referred to as* CP (control processor) and RCC (route control card)
RFC	request for comments
RIP	Routing Information Protocol
RP	rendezvous point
RSVP	resource reservation protocol
RSVP-TE	RSVP traffic engineering
SA	source-active
SAAL	signaling ATM adaptation layer
SAR	segmentation and reassembly
SCR	sustained cell rate
SDH	synchronous digital hierarchy
SFC	switch fabric card
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SNPA	subnet point of attachment
SONET	Synchronous Optical Network
SPF	Shortest Path First
SQE	signal quality error
STA	SONET Timing/Alarm module *Also referred to as* CTA (Clock Timing Adapter) *and* TAC (Timing Adapter Controller)
SVC	switched virtual circuit

Acronym	Meaning
TAC	Timing Adapter Controller *Also referred to as* CTA (Clock Timing Adapter) *Now referred to as* STA (SONET Timing/Alarm module)
TCP	Transmission Control Protocol
TE	traffic engineering
TE-LSAI	traffic engineering link state advertisement identifier
TTL	Time to Live (threshhold)
TOS	type of service
UBR	unspecified bit rate
UDP	User Datagram Protocol
UNI	User-to-Network Interface
VBR	variable bit rate
VC	virtual circuit
VCC	virtual circuit connection
VCD	virtual circuit descriptor
VCI	virtual channel identifier
VNN	Virtual Network Navigator
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPN	virtual private network
WAN	wide area network
WRED	weighted random early detection

Index

Technical Support

The Lucent Technical Assistance Center (TAC) is available to assist you with any problems encountered while using this Lucent product. Call the appropriate number in the following table, or log on to our Customer Support web site (www.lucent.com/support) to obtain numbers for the Lucent TAC in your region.

Country/Region		Telephone Number
United States, Canada, United Kingdom, and Europe www.lucent.com/support	United States and Canada	1-866-LUCENT8 (1-866-582-3688)
	United Kingdom	0-800-96-2229
	Europe	Toll-free calls from most European countries: 00-800-0058-2368 Toll calls from other countries: 353-1-692-4579
Asia-Pacific www.lucent.com/support	Australia	1-800-458-236
	China	(00) 800-5823-6888 Hotline: 86-10-8518 8275
	Hong Kong	(001) 800-5823-6888 Hotline: (852) 2596-4110
	Japan	+81-3-5325-7397
	Malaysia	(00) 800-5823-6888
	New Zealand	(00) 800-5823-6888
	Singapore	(001) 800-5823-6888
	South Korea	Via Telecom: (001) 800-5823-6888 Via Dacom: (002) 800-5823-6888
	Taiwan	(00) 800-5823-6888
	Thailand	(00) 800-5823-6888
	All other AP Countries	+61-3-9614-8530
Central America and Latin America www.lucent.com/support	Argentina	0-800-222-8537
	Brazil	Within Brazil: 0800-55-6400 Outside Brazil: +55-19-3707-7900
	Colombia	54-11-4340-8681
	Mexico	Within Mexico: 800-2-658588 (01 800 26 LT LTT) *or* 800-3-158588 (01 800 31 LT LTT) Outside Mexico: 52 5 278 7005
	Puerto Rico	888-866-8537
	Venezuela	800-5287683

Problem Reporting Information

To expedite the troubleshooting process, please have available and provide the following information. Note any deviations from initially installed component version information.

Source Information	Description
Primary Contact Name:	
Location:	
Phone/Pager:	
Availability:	
Secondary Contact Name:	
Location:	
Phone/Pager:	
Availability:	
System type:	
Installed HW components / versions:	
Installed SW modules / versions:	
Affected component (SW module, HW component, etc.):	
Question/Problem:	
Severity of impact:	
Supporting documentation (configuration files, log files, topology diagrams, trace files, etc.):	