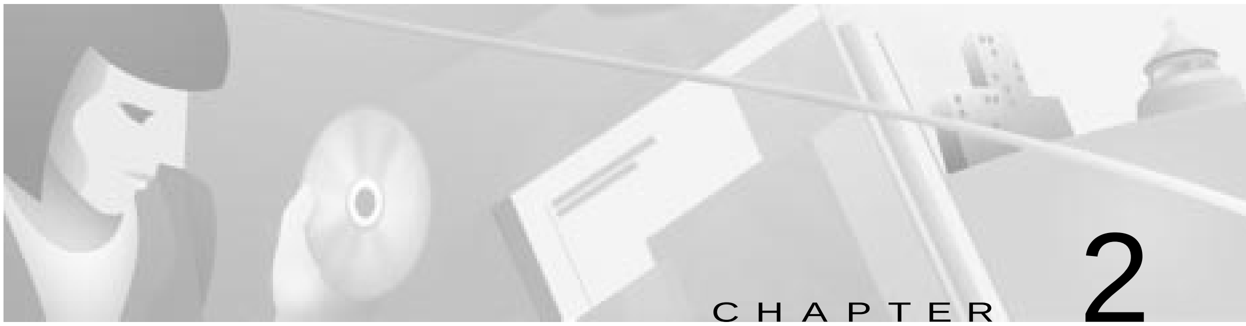

CHAPTER 2

Troubleshooting Tools

This chapter describes the tools available to assist you in troubleshooting your ATM switch router and contains the following sections:

- Using Diagnostic Commands
- Third-Party Troubleshooting Tools

Using Diagnostic Commands

You can use the **show**, **debug**, **ping**, and **traceroute** commands to monitor and troubleshoot your internetwork.

show Commands

You can use the **show** commands to perform many functions:

- Monitor switch router behavior during initial installation
- Monitor normal network operation
- Isolate problem interfaces, nodes, media, or applications
- Determine when a network is congested
- Determine the status of servers, clients, or other neighbors

Following are some of the most commonly used **show** commands:

Command	Purpose
show interfaces **show interfaces atm** **show interfaces atm-p** **show interfaces cbr** **show line**	Displays statistics for the network interfaces.
show controllers **show controllers atm** **show controllers ethernet**	Displays statistics for port adapter interface controllers.
show lane	Displays the LAN emulation configuration.
show running-config	Displays the switch router configuration currently running.

Command	Purpose
show startup-config	Displays the switch router configuration stored in nonvolatile RAM (NVRAM).
show flash	Displays the layout and contents of Flash memory.
show buffers	Displays statistics for the buffer pools on the switch router.
show memory	Shows statistics about the switch router memory, including free pool statistics.
show processes	Displays information about the active processes on the switch router.
show stacks	Displays information about the stack utilization of processes and interrupt routines, and the reason for the last system reboot.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

For further information about **show** commands, refer to the *ATM Switch Router Command Reference* publication for your specific software version.

debug Commands

The **debug** privileged EXEC commands provide a wealth of information about the traffic seen (or *not* seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets and cells, and other useful troubleshooting data.

Caution Exercise care when using **debug** commands. Many of these commands are processor intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded switch router. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

Appendix A, “Debugging an ATM Switch Router,” provides an overview of **debug** commands including how to use them when you are troubleshooting the ATM switch router.

In many situations, third-party diagnostic tools can be more useful and less intrusive than using **debug** commands. For more information, see the “Third-Party Troubleshooting Tools” section on page 2-3.

ping Commands

To check host reachability and network connectivity, use the **ping** user EXEC or privileged EXEC command. This command can be used to confirm basic network connectivity on IP networks.

For IP, the **ping** command sends Internet Control Message Protocol (ICMP) echo messages. If a station receives an ICMP echo message, it sends an ICMP echo reply message back to the source.

Using the extended command mode of the **ping** command, you can specify the supported IP header options, which allow the switch router to perform a more extensive range of test options. To enter **ping** extended command mode, enter **yes** at the extended commands prompt of the **ping** command.

Use the **ping** command when the network is functioning properly to see how the command works. When you are troubleshooting, you can see the difference between normal and abnormal operation.

For detailed information about using the **ping** and extended **ping** commands, refer to the *Configuration Fundamentals Command Reference* publication.

traceroute Commands

The **traceroute** user EXEC command discovers the routes packets follow when traveling to their destinations. With the **traceroute** privileged EXEC command, the supported IP header options are specified, and the switch router can perform a more extensive range of test options.

The **traceroute** command works by using the error message generated by ATM switch routers when a datagram exceeds its time-to-live (TTL) value. First, probe datagrams are sent with a TTL value of one. This causes the first switch router to discard the probe datagrams and send back “time exceeded” error messages. The **traceroute** command then sends several probes, and displays the round-trip time for each. After every third probe, the TTL increases by one.

Each outgoing packet can result in one of two error messages. A “time exceeded” error message indicates that an intermediate switch router has seen and discarded the probe. A “port unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet to an application. If the timer goes off before a response comes in, **traceroute** displays an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the **traceroute** with the escape sequence.

Use the **traceroute** command when the network is functioning properly to see how the command works under normal conditions. Then when you are troubleshooting you can see the difference between normal and abnormal operation.

For detailed information about using the **traceroute** and extended **traceroute** commands, refer to the *ATM Switch Router Command Reference* publication.

Third-Party Troubleshooting Tools

In many situations, third-party diagnostic tools can be helpful. For example, attaching a network analyzer to a network is less intrusive and is more likely to yield useful information without interrupting the operation of the switch router than using the **debug** commands, which are processor intensive.

Some typical third-party tools used for troubleshooting internetworks are described in the following sections:

- Volt-Ohm Meters, Digital Multimeters, and Cable Testers
- TDRs and OTDRs
- Network Monitors
- Network Analyzers

Volt-Ohm Meters, Digital Multimeters, and Cable Testers

Volt-ohm meters and digital multimeters measure parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity. They check physical connectivity.

Using cable testers (scanners), you can also check physical connectivity. Cable testers are available for foil twisted-pair (FTP), unshielded twisted-pair (UTP), 10BaseT, and coaxial and twinax cables. A given cable tester can perform any of the following functions:

- Test and report on cable conditions, including near-end crosstalk (NEXT), attenuation, and noise
- Perform time domain reflectometer (TDR) functions, traffic monitoring, and wire map functions
- Display media access control (MAC)-layer information about LAN traffic, provide statistics such as network utilization and packet error rates, and perform limited protocol testing (for example, TCP/IP tests such as **ping**)

Similar testing equipment is available for fiber-optic cable. Due to the relatively high cost of fiber cable and its installation, test fiber-optic cable both before installation (on-the-reel testing) and after installation. Continuity testing of the fiber requires either a visible light source or a reflectometer. Light sources capable of providing light at the three predominant wavelengths, 850 nanometers (nm), 1300 nm, and 1550 nm, are used with power meters that can measure the same wavelengths and test attenuation and return loss in the fiber.

TDRs and OTDRs

TDRs quickly locate open circuits, short circuits, crimps, kinks, sharp bends, impedance mismatches, and other defects in metallic cables.

A TDR reflects a signal off the end of the cable. Opens, shorts, and other problems reflect back the signal at different amplitudes, depending on the problem. A TDR measures the time it takes for the signal to reflect and calculates the distance to a fault in the cable. TDRs can also measure the length of a cable, and some TDRs can calculate the rate of propagation based on a configured cable length.

Fiber-optic measurement is performed by an optical time domain reflectometer (OTDR). OTDRs can accurately measure the length of the fiber, locate cable breaks, measure the fiber attenuation, and measure splice or connector losses. An OTDR can take the signature of a particular installation, noting attenuation and splice losses. This baseline measurement can then be compared with future signatures when you suspect a problem in the system.

Network Monitors

Network monitors continuously track packets crossing a network, providing an accurate picture of network activity. Network monitors do not decode the contents of frames. They are useful for creating a baseline of normal performance.

Monitors collect information such as packet sizes, the number of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. This data can be used to create profiles of LAN traffic and assist in locating traffic overloads, planning for network expansion, detecting intruders, and distributing traffic more efficiently.

Network Analyzers

To accurately troubleshoot your ATM network, you should have the following analyzers:

- Simple cell generators and analyzers to test high-speed ATM and Broadband Integrated Services Digital Network (BISDN) transmission and protocols.
- Signaling generators to test ATM equipment, service installation, and the interworking of broadband services. They help manage the performance of broadband networks, and guarantee end-to-end quality of service (QoS).
- Physical layer analyzers to provide physical, convergence, and ATM cell testing capabilities and transmission test functionality.

  Most physical layer analyzers can perform many of the following functions:

  - Traffic generation
  - Cell error and cell loss measurements
  - Cell delay measurements
  - Traffic capture and playback
- Network analyzers (or protocol analyzers) decode the various protocol layers in a recorded frame and present them as readable abbreviations or summaries, detailing which layer is involved (physical, data link, and so forth) and what function each bit or byte content serves.

  Most network analyzers can perform many of the following functions:

  - Filter traffic that meets certain criteria so that, for example, all traffic to and from a particular device is captured
  - Time-stamp captured data
  - Present protocol layers in an easily readable form
  - Generate frames and transmit them to the network
  - Incorporate an “expert” system in which the analyzer uses a set of rules, combined with information about the network configuration and operation, to diagnose, solve, or offer potential solutions to network problems