Troubleshooting Serial Line Problems

This chapter presents general troubleshooting information and a discussion of tools and techniques for troubleshooting serial connections. The chapter consists of the following sections:

- Using the **show interfaces serial** Command
- Using the **show controllers** Command
- Using **debug** Commands
- Using Extended **ping** Tests
- Troubleshooting Clocking Problems
- Adjusting Buffers
- Special Serial Line Tests

Using the show interfaces serial Command

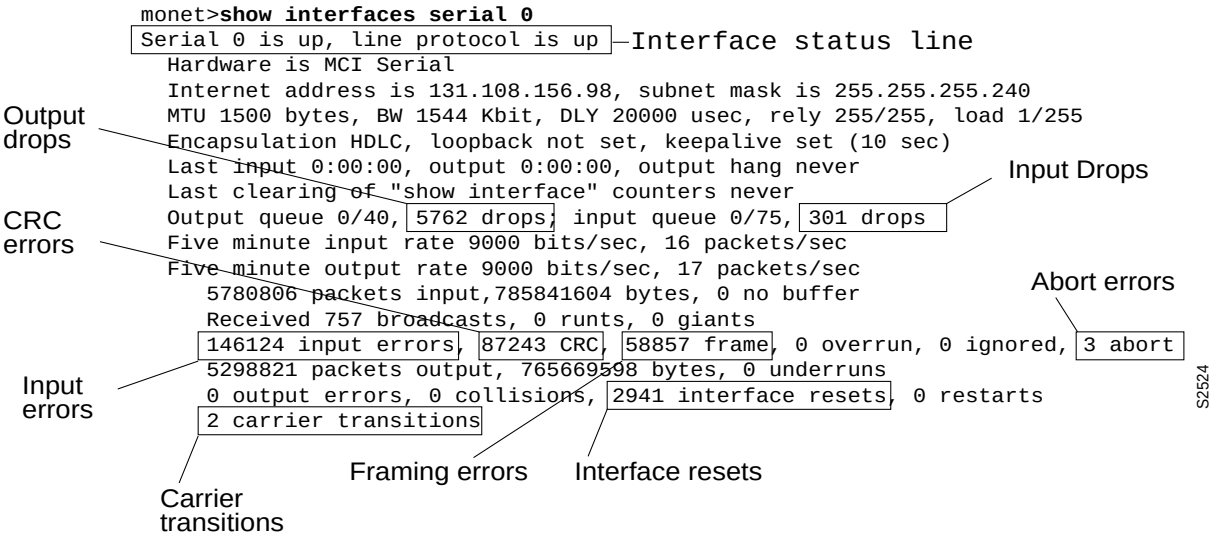
The output of the **show interfaces serial** EXEC command displays information specific to serial interfaces. Figure 13-1 shows the output of the **show interfaces serial** EXEC command for a High-Level Data Link Control (HDLC) serial interface.

This section describes how to use the **show interfaces serial** command to diagnose serial line connectivity problems in a WAN environment. The following sections describe some of the important fields of the command output.

- Interface and Line Protocol Status
- Output Drops
- Input Drops
- Input Errors
- Interface Resets
- Carrier Transitions

Other fields shown in the display are described in detail in the Cisco IOS *Configuration Fundamentals Command Reference*.

Figure 13-1 Output of HDLC show interfaces serial Command



Interface and Line Protocol Status

You can identify five possible problem states in the interface status line of the **show interfaces serial** display (see Figure 13-1):

- Serial *x* is down, line protocol is down
- Serial *x* is up, line protocol is down
- Serial *x* is up, line protocol is up (looped)
- Serial *x* is up, line protocol is down (disabled)
- Serial *x* is administratively down, line protocol is down

Table 13-1 shows the interface status condition, possible problems associated with the condition, and solutions to those problems.

Table 13-1 Serial Lines: show interfaces serial Status Line Conditions

Status Line Condition	Possible Problem	Solution
Serial *x* is up, line protocol is up	—	This is the proper status line condition. No action required.
Serial *x* is down, line protocol is down (DTE mode)	Typically indicates that the router is not sensing a CD[1] signal (that is, CD is not active). **1** Telephone company problem—Line is down or line is not connected to CSU/DSU **2** Faulty or incorrect cabling **3** Faulty or incorrect applique (AGS/CGS/MGS only) **4** Hardware failure (CSU/DSU)	**Step 1** Check the LEDs on the CSU/DSU to see if CD is active, or insert a breakout box on the line to check for the CD signal. **Step 2** Verify that you are using the proper cable and interface (see your hardware installation documentation). **Step 3** If appropriate, check the applique. If it is incorrect, install the correct applique (AGS/CGS/MGS only). **Step 4** Insert a breakout box and check all control leads. **Step 5** Contact your leased-line or other carrier service to see if there is a problem. **Step 6** Swap faulty parts. **Step 7** If you suspect faulty router hardware, change the serial line to another port or applique. If the connection comes up, the previously connected interface or applique has a problem.
Serial *x* is up, line protocol is down (DTE mode)	**1** Local or remote router is misconfigured **2** Keepalives are not being sent by remote router **3** Leased-line or other carrier service problem—noisy line, or misconfigured or failed switch **4** Timing problem on cable (SCTE[2] not set on CSU/DSU) **5** Failed local or remote CSU/DSU **6** Router hardware failure (local or remote)	**Step 1** Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** command to determine whether the line protocol comes up. If the line protocol comes up, a telephone company problem or a failed remote router is the likely problem. **Step 2** If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. **Step 3** Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct telephone company network termination point. Use the **show controllers** EXEC command to determine which cable is attached to which interface. **Step 4** Enable the **debug serial interface** EXEC command. **Step 5** If the line protocol does not come up in local loopback mode and if the output of the **debug serial interface** EXEC command shows that the keepalive counter is not incrementing, a router hardware problem is likely. Swap router interface hardware. **Step 6** If the line protocol comes up and the keepalive counter increments, the problem is *not* in the local router. Troubleshoot the serial line as described in the sections "Troubleshooting Clocking Problems" and "CSU and DSU Loopback Tests" later in this chapter. **Step 7** If you suspect faulty router hardware, change the serial line to an unused port or applique. If the connection comes up, the previously connected interface or applique has a problem.

Status Line Condition	Possible Problem	Solution
Serial *x* is up, line protocol is down (DCE mode)	**1** Missing **clockrate** interface configuration command **2** DTE device does not support or is not set up for SCTE mode (terminal timing) **3** Failed remote CSU or DSU **4** Failed or incorrect cable **5** Router hardware failure	**Step 1** Add the **clockrate** interface configuration command on the serial interface. **Step 2** Set the DTE device to SCTE mode if possible. If your CSU/DSU does not support SCTE, you might have to disable SCTE on the Cisco router interface. Refer to the section "Inverting the Transmit Clock" later in this chapter. **Step 3** Verify that the correct cable is being used. **Step 4** If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. **Step 5** Replace faulty parts as necessary.
Serial *x* is up, line protocol is up (looped)	Loop exists in circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	**Step 1** Use the **show running-config** privileged EXEC command to look for any **loopback** interface configuration command entries. **Step 2** If you find a **loopback** interface configuration command entry, use the **no loopback** interface configuration command to remove the loop. **Step 3** If you do not find the **loopback** interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. **Step 4** Reset the CSU or DSU and inspect the line status. If the line protocol comes up, no other action is needed. **Step 5** If the CSU or DSU is not configured in manual loopback mode, contact the leased-line or other carrier service for line troubleshooting assistance.
Serial *x* is up, line protocol is down (disabled)	**1** High error rate due to telephone company service problem **2** CSU or DSU hardware problem **3** Bad router hardware (interface, applique)	**Step 1** Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS[3] and DSR[4] signals. **Step 2** Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a telephone company problem. **Step 3** Swap out bad hardware as required (CSU, DSU, switch, local or remote router).
Serial *x* is administratively down, line protocol is down	**1** Router configuration includes the **shutdown** interface configuration command **2** Duplicate IP address	**Step 1** Check the router configuration for the **shutdown** command. **Step 2** Use the **no shutdown** interface configuration command to remove the **shutdown** command. **Step 3** Verify that there are no identical IP addresses using the **show running-config** privileged EXEC command or the **show interfaces** EXEC command. **Step 4** If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

1. CD=Carrier Detect
2. SCTE=serial clock transmit external
3. CTS=Clear To Send
4. DSR=Data Set Ready

Output Drops

Output drops appear in the output of the **show interfaces serial** command (see Figure 13-1) when the system is attempting to hand off a packet to a transmit buffer but no buffers are available.

Symptom Increasing output drops on serial link

Possible Cause Input rate to serial interface exceeds bandwidth available on serial link

Recommended Action The following steps are suggested for this problem:

Step 1 Minimize periodic broadcast traffic such as routing and Service Advertising Protocol (SAP) updates by using access lists or by other means. For example, to increase the delay between SAP updates, use the **ipx sap-interval** interface configuration command.

Step 2 Increase the output hold queue size in small increments, using the **hold-queue out** interface configuration command.

Step 3 On affected interfaces, turn off fast switching for heavily-used protocols. For example, to turn off IP fast switching, enter the **no ip route-cache** interface configuration command. For the command syntax for other protocols, consult the Cisco IOS configuration guides and command references.

Step 4 Implement priority queuing on slower serial links by configuring priority lists. For information on configuring priority lists, see the Cisco IOS configuration guides and command references.

Note Output drops are acceptable under certain conditions. For instance, if a link is known to be overused (with no way to remedy the situation), it is often considered preferable to drop packets than to hold them. This is true for protocols that support flow control and can retransmit data (such as TCP/IP and Novell IPX). However, some protocols, such as DECnet and Local Area Transport (LAT) are sensitive to dropped packets and accommodate retransmission poorly, if at all.

Input Drops

Input drops appear in the output of the **show interfaces serial** EXEC command (see Figure 13-1) when too many packets from that interface are still being processed in the system.

Symptom Increasing number of input drops on serial link

Possible Cause Input rate exceeds the capacity of the router or input queues exceed the size of output queues.

Note Input drop problems are typically seen when traffic is being routed between faster interfaces (such as Ethernet, Token Ring, and FDDI) and serial interfaces. When traffic is light, there is no problem. As traffic rates increase, backups start occurring. Routers will drop packets during these congested periods.

Recommended Action The following steps are recommended when this symptom is encountered:

Step 1 Increase the output queue size on common destination interfaces for the interface that is dropping packets. Use the **hold-queue out** interface configuration command.

Step 2 Reduce the input queue size, using the **hold-queue in** interface configuration command, to force input drops to become output drops. Output drops have less impact on the performance of the router than do input drops.

Input Errors

If input errors appear in the **show interfaces serial** output (see Figure 13-1), there are several possible sources of those errors. The most likely sources are summarized in the list of possible problems that follows.

Note Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts above one percent of the total interface traffic suggests some kind of link problem that should be isolated and repaired.

Symptom Increasing number of input errors in excess of one percent of total interface traffic.

Possible Cause The following problems can result in this symptom:

- Faulty telephone company equipment
- Noisy serial line
- Incorrect clocking configuration (SCTE not set)
- Incorrect cable or cable too long

- Bad cable or connection
- Bad CSU or DSU
- Bad router hardware
- Data converter or other device being used between router and DSU

Note Cisco strongly recommends against the use of data converters when you are connecting a router to a WAN or serial network.

Recommended Action The following steps are suggested to resolve this problem:

Step 1 Use a serial analyzer to isolate the source of the input errors. If you detect errors, it is likely that there is a hardware problem or a clock mismatch in a device that is external to the router.

Step 2 Use the loopback and **ping** tests to isolate the specific problem source. For more information, see the sections "Using Extended **ping** Tests" and "CSU and DSU Loopback Tests," later in this chapter.

Step 3 Look for patterns. For example, if errors occur at a consistent interval, they could be related to a periodic function such as the sending of routing updates.

Table 13-2 describes the various types of input errors displayed by the **show interfaces serial** command (see Figure 13-1), possible problems that might be causing the errors, and solutions to those problems.

Table 13-2 Serial Lines: Troubleshooting Serial Line Input Errors

Input Error Type (Field Name)	Possible Problem	Solution
CRC errors (CRC)	CRC errors occur when the CRC calculation does not pass (indicating that data is corrupted). **1** Noisy serial line **2** Serial cable is too long or cable from the CSU/DSU to the router is not shielded **3** SCTE mode is not enabled on DSU **4** CSU line clock is incorrectly configured **5** Ones density problem on T1 link (incorrect framing or coding specification)	**Step 1** Ensure that the line is clean enough for transmission requirements. Shield the cable if necessary. **Step 2** Make sure the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for T1 link). **Step 3** Ensure that all devices are properly configured for a common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter. **Step 4** Make certain that the local and remote CSU/DSU are configured for the same framing and coding scheme as that used by the leased-line or other carrier service (for example, ESF[1]/B8ZS[2]). **Step 5** Contact your leased-line or other carrier service and have them perform integrity tests on the line.
Framing errors (frame)	A framing error occurs when a packet does not end on an 8-bit byte boundary. **1** Noisy serial line **2** Improperly designed cable; serial cable is too long; the cable from the CSU or DSU to the router is not shielded **3** SCTE mode is not enabled on the DSU; the CSU line clock is incorrectly configured; one of the clocks is configured for local clocking **4** Ones density problem on T1 link (incorrect framing or coding specification)	**Step 1** Ensure that the line is clean enough for transmission requirements. Shield the cable if necessary. Make certain you are using the correct cable. **Step 2** Make sure the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for T1 link) **Step 3** Ensure that all devices are properly configured to use a common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter. **Step 4** Make certain that the local and remote CSU/DSU is configured for the same framing and coding scheme as that used by the leased-line or other carrier service (for example, ESF/B8ZS). **Step 5** Contact your leased-line or other carrier service and have them perform integrity tests on the line.

Input Error Type (Field Name)	Possible Problem	Solution
Aborted transmission (abort)	Aborts indicate an illegal sequence of one bits (more than 7 in a row) **1** SCTE mode is not enabled on DSU **2** CSU line clock is incorrectly configured **3** Serial cable is too long or cable from the CSU or DSU to the router is not shielded **4** Ones density problem on T1 link (incorrect framing or coding specification) **5** Packet terminated in middle of transmission (typical cause is an interface reset or a framing error) **6** Hardware problem—bad circuit, bad CSU/DSU, or bad sending interface on remote router	**Step 1** Ensure that all devices are properly configured to use a common line clock. Set SCTE on the local and remote DSU. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter. **Step 2** Shield the cable if necessary. Make certain the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for T1 link). Ensure that all connections are good. **Step 3** Check the hardware at both ends of the link. Swap faulty equipment as necessary. **Step 4** Lower data rates and determine if aborts decrease. **Step 5** Use local and remote loopback tests to determine where aborts are occurring (see the section "Special Serial Line Tests" later in this chapter.) **Step 6** Contact your leased-line or other carrier service and have them perform integrity tests on the line.

1. ESF=Extended Super Frame
2. B8ZS=binary eight-zero substitution

Interface Resets

Interface resets that appear in the output of the **show interfaces serial** EXEC command (see Figure 13-1) are the result of missed keepalive packets.

Symptom Increasing interface resets on serial link

Possible Cause The following causes can result in this symptom:

- Congestion on link (typically associated with output drops)
- Bad line causing CD transitions
- Possible hardware problem at the CSU, DSU, or switch

Recommended Action When interface resets are occurring, examine other fields of the **show interfaces serial** command output to determine the source of the problem. Assuming an increase in interface resets is being recorded, examine the following fields (illustrated in Figure 13-1):

Step 1 If there are a high number of output drops in the **show interfaces serial** output, see the section "Output Drops" earlier in this chapter.

Step 2 Check the carrier transitions field in the **show interfaces serial** display. If carrier transitions are high while interface resets are being registered, the problem is likely to be a bad link or bad CSU or DSU. Contact your leased line or carrier service and swap faulty equipment as necessary.

Step 3 Examine the input errors field in the **show interfaces serial** display. If input errors are high while interface resets are increasing, the problem is probably a bad link or bad CSU/DSU. Contact your leased line or other carrier service and swap faulty equipment as necessary.

Carrier Transitions

Carrier transitions appear in the output of the **show interfaces serial** EXEC command (see Figure 13-1) whenever there is an interruption in the carrier signal (such as an interface reset at the remote end of a link).

Symptom Increasing carrier transitions count on serial link

Possible Cause The following causes can result in this symptom:

- Line interruptions due to an external source (such as physical separation of cabling, Red or Yellow T1 alarms, or lightning striking somewhere along the network)
- Faulty switch, DSU, or router hardware

Recommended Action The following steps are suggested when this symptom is encountered:

Step 1 Check hardware at both ends of the link (attach a breakout box or a serial analyzer and test to determine source of problems).

Step 2 If an analyzer or breakout box is unable to identify any external problems, check the router hardware.

Step 3 Swap faulty equipment as necessary.

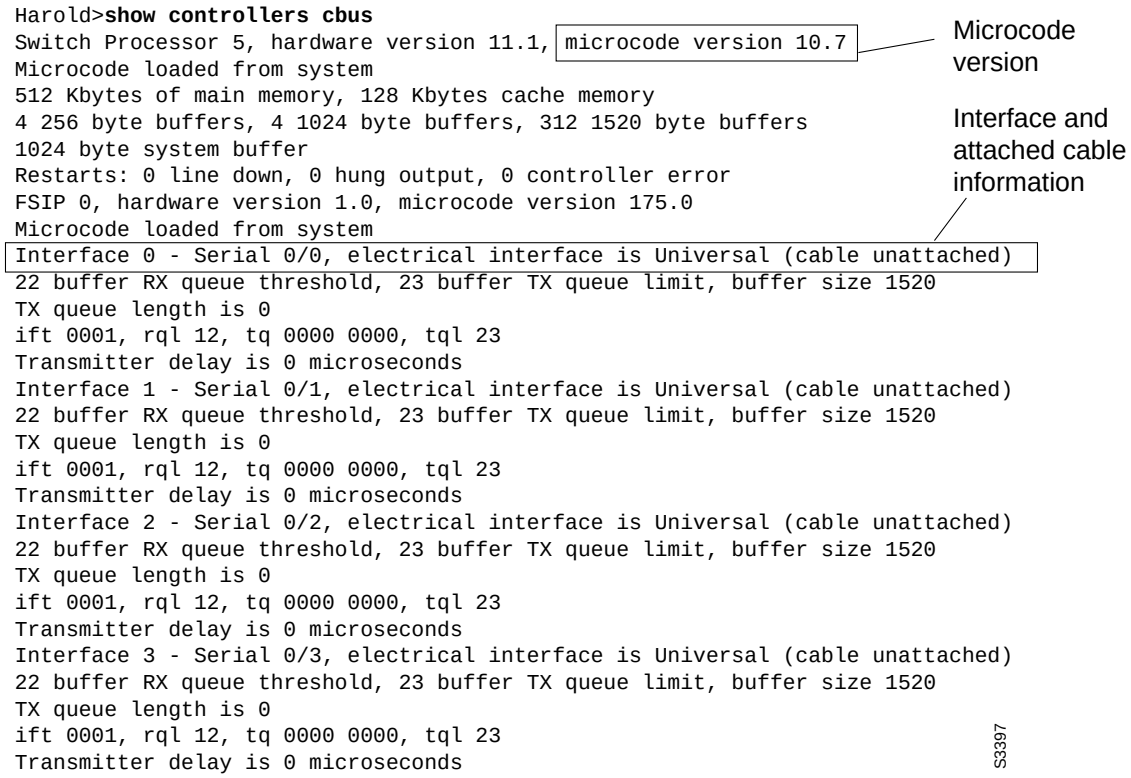
Using the show controllers Command

The **show controllers** EXEC command is another important diagnostic tool when troubleshooting serial lines. The command syntax varies depending on platform:

- For serial interfaces on Cisco 7000 series routers, use the **show controllers cbus** EXEC command
- For Cisco access products, use the **show controllers** EXEC command
- For the AGS, CGS, and MGS, use the **show controllers mci** EXEC command

Figure 13-2 shows the output from the **show controllers cbus** EXEC command. This command is used on Cisco 7000 series routers with the Fast Serial Interface Processor (FSIP) card. Check the command output to make certain that the cable to the CSU/DSU is attached to the proper interface. You can also check the microcode version to see if it is current.

Figure 13-2 show controllers cbus Command Output



On access products such as the Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series access servers and routers, use the **show controllers** EXEC command. Figure 13-3 shows the **show controllers** command output from the basic-rate interface (BRI) and serial interfaces on a Cisco 2503 access server. (Note that some output is not shown.)

The **show controllers** output indicates the state of the interface channels and whether a cable is attached to the interface. In Figure 13-3, serial interface 0 has an RS-232 DTE cable attached. Serial interface 1 has no cable attached.

Figure 13-3 show controllers Command Output

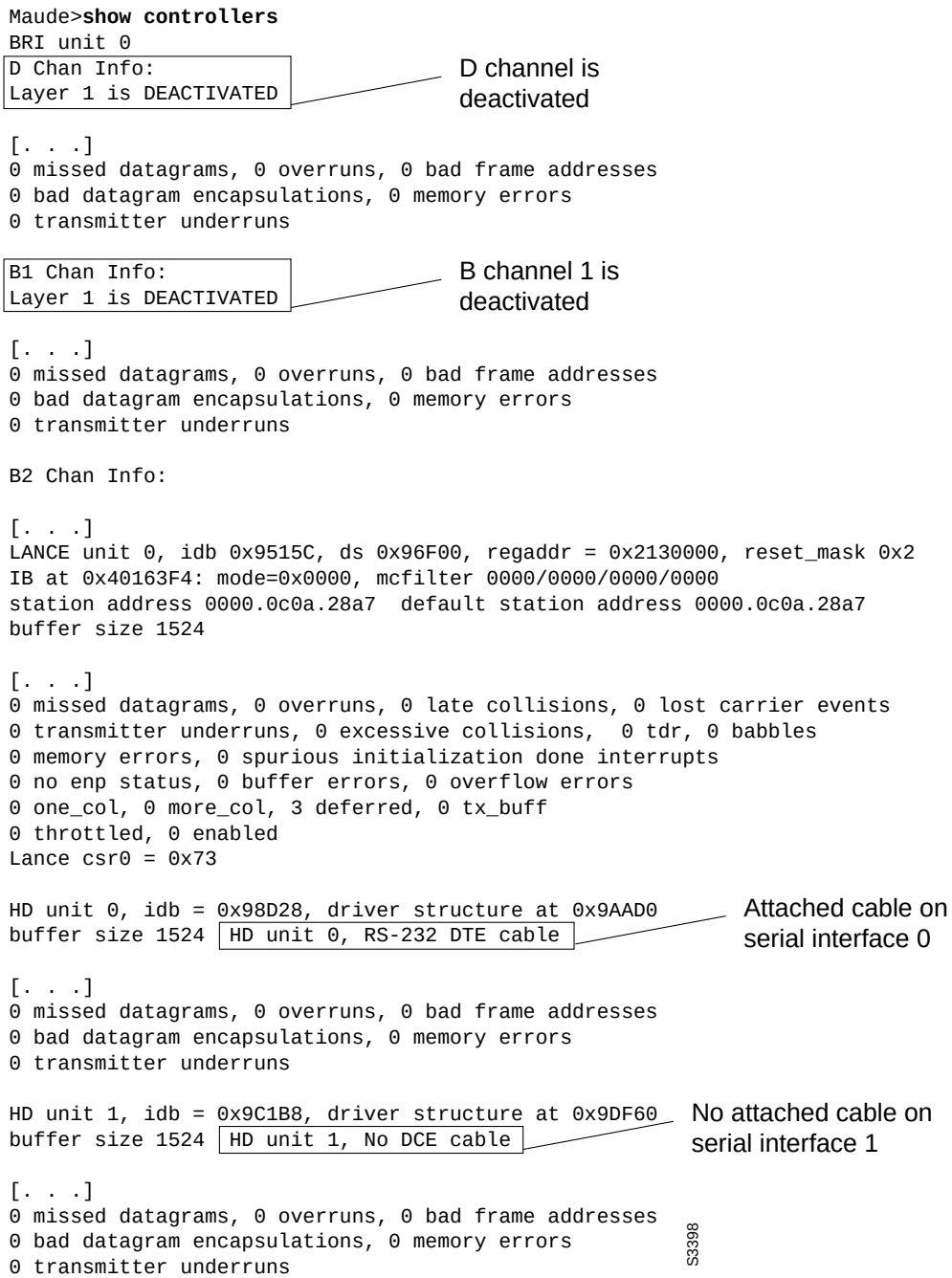
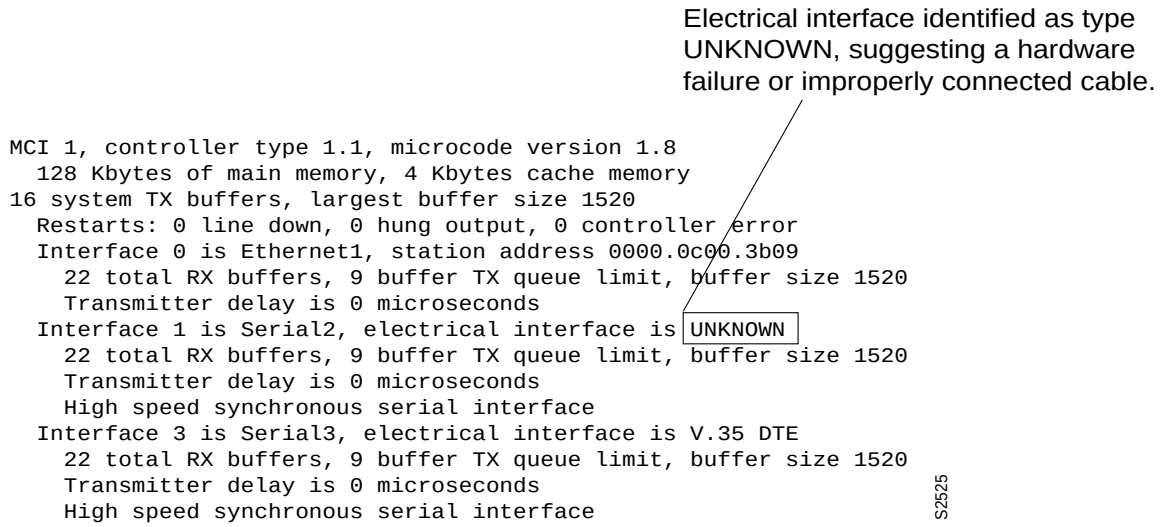


Figure 13-4 shows the output of the **show controllers mci** command. This command is used on AGS, CGS, and MGS routers only. If the electrical interface is displayed as "UNKNOWN" (instead of V.35, EIA/TIA-449, or some other electrical interface type), an improperly connected cable is the likely problem. A bad applique or a problem with the internal wiring of the card is also possible. If the electrical interface is unknown, the corresponding display for the **show interfaces serial** EXEC command will show that the interface and line protocol are down. (See Figure 13-1.)

Figure 13-4 show controllers mci Command Output



Using debug Commands

The output of the various **debug** privileged EXEC commands provides diagnostic information relating to protocol status and network activity for many internetworking events.

Caution In general, **debug** commands should be used with care. Enabling debugging can significantly disrupt the operation of a heavily loaded router. When you finish using a **debug** command, remember to disable it with its specific **no debug** command or with the **no debug all** command.

Following are some **debug** commands that are useful when troubleshooting serial and WAN problems. More information about the function and output of each of these commands is provided in the *Debug Command Reference* publication.

- **debug serial interface**—Verifies whether HDLC keepalive packets are incrementing. If they are not, a possible timing problem exists on the interface card or in the network.
- **debug x25 events**—Detects X.25 events, such as the opening and closing of switched virtual circuits (SVCs). The resulting "Cause and Diagnostic" information is included with the event report.
- **debug lapb**—Outputs LAPB or Level 2 X.25 information.
- **debug arp**—Indicates whether the router is sending information about or learning about routers (with ARP packets) on the other side of the WAN cloud. Use this command when some nodes on a TCP/IP network are responding but others are not.
- **debug frame-relay lmi**—Obtains Local Management Interface (LMI) information useful for determining whether a Frame Relay switch and a router are sending and receiving LMI packets.
- **debug frame-relay events**—Determines whether exchanges are occurring between a router and a Frame Relay switch.

- **debug ppp negotiation**—Shows Point-to-Point Protocol (PPP) packets transmitted during PPP startup, where PPP options are negotiated.
- **debug ppp packet**—Shows PPP packets being sent and received. This command displays low-level packet dumps.
- **debug ppp errors**—Shows PPP errors (such as illegal or malformed frames) associated with PPP connection negotiation and operation.
- **debug ppp chap**—Shows PPP Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) packet exchanges.
- **debug serial packet**—Shows SMDS packets being sent and received. This display also prints out error messages to indicate why a packet was not sent or was received erroneously. For SMDS, the command dumps the entire SMDS header and some payload data when an SMDS packet is transmitted or received.

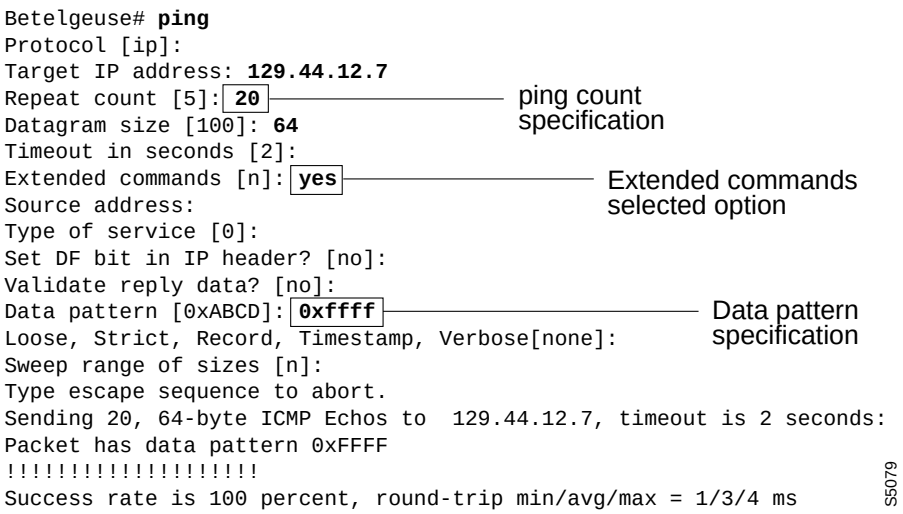
Using Extended ping Tests

The **ping** command is a useful test available on Cisco internetworking devices as well as on many host systems. In TCP/IP, this diagnostic tool also is known as an Internet Control Message Protocol (ICMP) Echo Request.

Note The **ping** command is particularly useful when high levels of input errors are being registered in the **show interfaces serial** display (see Figure 13-1).

Cisco internetworking devices provide a mechanism to automate the sending of many **ping** packets in sequence. Figure 13-5 illustrates the menu used to specify extended **ping** options. This example specifies 20 successive **pings**. However, when testing the components on your serial line, you should specify a much larger number, such as 1000 **pings**.

Figure 13-5 Extended ping Specification Menu



In general, perform serial line **ping** tests as follows:

Step 1 Put the CSU or DSU into local loopback mode.

Step 2 Configure the extended **ping** command to send different data patterns and packet sizes. Figure 13-6 and Figure 13-7 illustrate two useful **ping** tests, an all-zeros 1500 byte **ping** and an all-ones 1500 byte **ping**, respectively.

Figure 13-6 All-Zeros 1500 Byte ping Test

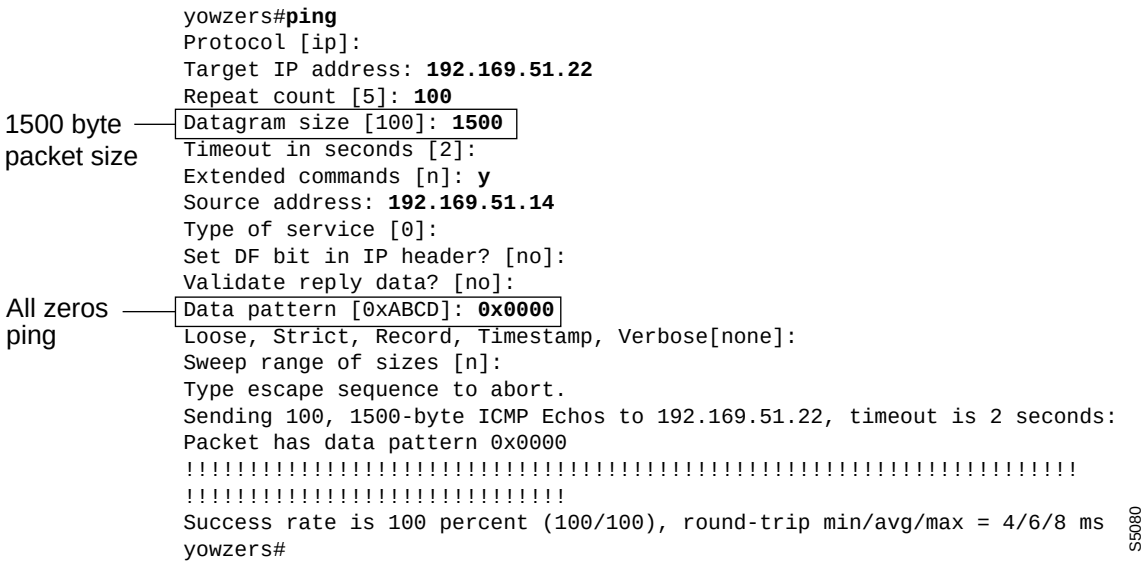
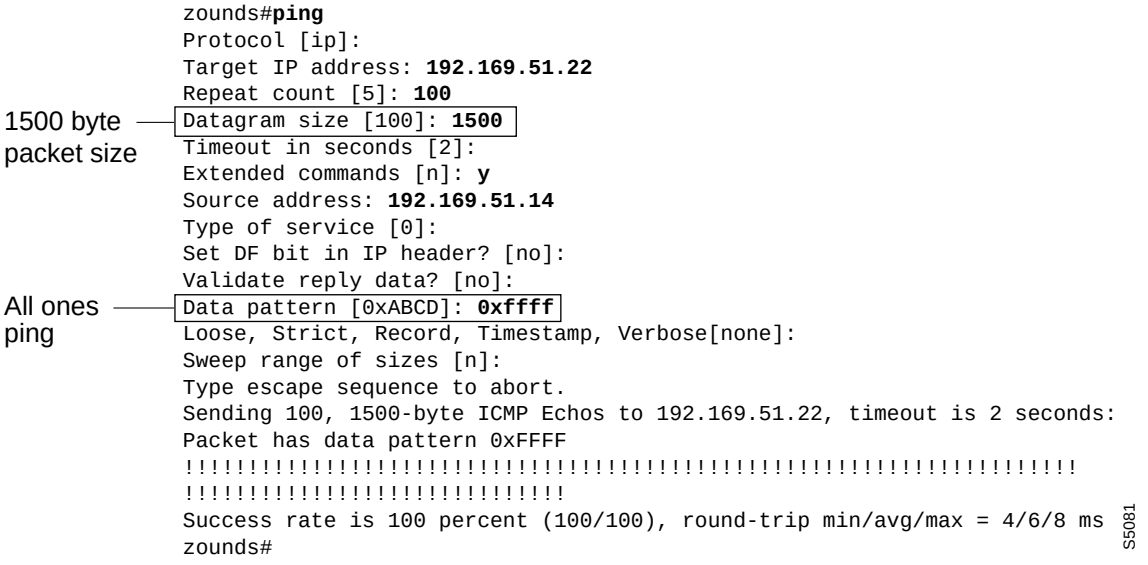


Figure 13-7 All-Ones 1500 Byte ping Test



Step 3 Examine the **show interfaces serial** command output (see Figure 13-1) and determine whether input errors have increased. If input errors have not increased, the local hardware (DSU, cable, router interface card, and applique) is probably in good condition.

Assuming that this test sequence was prompted by the appearance of a large number of CRC and framing errors, a clocking problem is likely. Check the CSU or DSU for a timing problem. Refer to the section "Troubleshooting Clocking Problems" later in this chapter.

Step 4 If you determine that the clocking configuration is correct and is operating properly, put the CSU or DSU into remote loopback mode.

Step 5 Repeat the **ping** test and look for changes in the input error statistics.

Step 6 If input errors increase, there is either a problem in the serial line or on the CSU/DSU. Contact the WAN service provider and swap the CSU or DSU. If problems persist, contact your technical support representative.

Troubleshooting Clocking Problems

Clocking conflicts in serial connections can lead either to chronic loss of connection service or to degraded performance. The following sections discuss the important aspects of clocking problems:

- Clocking Overview
- Clocking Problem Causes
- Detecting Clocking Problems
- Isolating Clocking Problems
- Clocking Problem Solutions

Clocking Overview

The CSU/DSU derives the data clock from the data that passes through it. In order to recover the clock, the CSU/DSU hardware *must* receive at least one 1-bit value for every 8 bits of data that pass through it (this is known as ones density.) Maintaining ones density allows the hardware to recover the data clock reliably.

Newer T1 implementations commonly use Extended Superframe Format (ESF) framing with Binary 8-Zero Substitution (B8ZS) coding. B8ZS provides a scheme by which a special code is substituted whenever 8 consecutive zeros are sent through the serial link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream.

Older T1 implementations use D4 (also known as Superframe Format [SF]) framing and Alternate Mark Inversion (AMI) coding. AMI does not utilize a coding scheme like B8ZS. This restricts the type of data that can be transmitted because ones density is not maintained independent of the data stream.

Another important element in serial communications is serial clock transmit external (SCTE) terminal timing. SCTE is the clock echoed back from the data terminal equipment (DTE) device (for example, a router) to the data communications equipment (DCE) device (for example, the CSU/DSU).

When the DCE device uses SCTE instead of its internal clock to sample data from the DTE, it is better able to sample the data without error even if there is a phase-shift in the cable between the CSU/DSU and the router. Using SCTE is highly recommended for serial transmissions faster than 64 kbps. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter.

Clocking Problem Causes

In general, clocking problems in serial WAN interconnections can be attributed to one of the following causes:

- Incorrect DSU configuration
- Incorrect CSU configuration
- Cables out of specification (longer than 50 feet [15.24 meters] or unshielded)
- Noisy or poor patch panel connections
- Several cables connected together in a row

Detecting Clocking Problems

To detect clocking conflicts on a serial interface, look for input errors as follows:

Step 1 Use the **show interfaces serial** EXEC command on the routers at both ends of the link.

Step 2 Examine the command output for CRC, framing errors, and aborts (see Figure 13-1).

Step 3 If either of these steps indicates errors exceeding an approximate range of 0.5 to 2.0 percent of traffic on the interface, clocking problems are likely to exist somewhere in the WAN.

Step 4 Isolate the source of the clocking conflicts as outlined in the following section, "Isolating Clocking Problems."

Step 5 Bypass or repair any faulty patch panels.

Isolating Clocking Problems

After you determine that clocking conflicts are the most likely cause of input errors, the following procedure will help you isolate the source of those errors:

Step 1 Perform a series of **ping** tests and loopback tests (both local and remote), as described in the sections "Using Extended **ping** Tests" and "CSU and DSU Loopback Tests" elsewhere in this chapter.

Step 2 Determine which end of the connection is the source of the problem, or if the problem is in the line. In local loopback mode, run different patterns and sizes in the **ping** tests (for example, use 1500-byte datagrams). Using a single pattern and packet size may not force errors to materialize, particularly when a serial cable to the router or CSU/DSU is the problem.

Step 3 Use the **show interfaces serial** EXEC command and determine whether input errors counts are increasing and where they are accumulating.

If input errors are accumulating on both ends of the connection, clocking of the CSU is the most likely problem.

If only one end is experiencing input errors, there is probably a DSU clocking or cabling problem.

If you see aborts on one end, it suggests that the other end is sending bad information or that there is a line problem.

Note Always refer back to the **show interfaces serial** command output (see Figure 13-1) and log any changes in error counts or note if the error count does not change.

Clocking Problem Solutions

Table 13-3 outlines suggested remedies for clocking problems, based on the source of the problem.

Table 13-3 Serial Lines: Clocking Problems and Solutions

Possible Problem	Solution
Incorrect CSU configuration	**Step 1** Determine whether the CSUs at both ends agree on the clock source (local or line). **Step 2** If the CSUs do not agree, configure them so that they do (usually the line is the source). **Step 3** Check the LBO[1] setting on the CSU to ensure that the impedance matches that of the physical line. For information on configuring your CSU, consult your CSU hardware documentation.
Incorrect DSU configuration	**Step 1** Determine whether the DSUs at both ends have SCTE mode enabled. **Step 2** If SCTE is not enabled on both ends of the connection, enable it. (For any interface that is connected to a line of 128 kbps or faster, SCTE *must* be enabled. If your DSU does not support SCTE, see the section "Inverting the Transmit Clock" later in this chapter.) **Step 3** Make sure that ones density is maintained. This requires that the DSU use the same framing and coding schemes (for example, ESF and B8ZS) used by the leased-line or other carrier service. Check with your leased line provider for information on their framing and coding schemes. **Step 4** If your carrier service uses AMI coding, either invert the transmit clock on both sides of the link or run the DSU in bit-stuff mode. For information on configuring your DSU, consult your DSU hardware documentation.
Cable to router out of specification	If the cable is longer than 50 feet (15.24 meters), use a shorter cable. If the cable is unshielded, replace it with shielded cable.

1. LBO=Line Build Out

Inverting the Transmit Clock

If you are attempting serial connections at speeds greater than 64 kbps with a CSU/DSU that does not support serial clock transmit external (SCTE), you might have to invert the transmit clock on the router. Inverting the transmit clock compensates for phase-shifts between the data and clock signals.

The specific command used to invert the transmit clock varies between platforms. On a Cisco 7000 series router, enter the **invert-transmit-clock** interface configuration command. For Cisco 4000 series routers, use the **dte-invert-txc** interface configuration command.

To ensure that you are using the correct command syntax for your router, refer to the user guide for your router or access server and to the Cisco IOS configuration guides and command references.

Note On older platforms, inverting the transmit clock might require that you move a physical jumper.

Adjusting Buffers

Excessively high bandwidth utilization results in reduced overall performance and can cause intermittent failures. For example, DECnet file transmissions might be failing due to packets being dropped somewhere in the network.

If the situation is bad enough, you *must* increase the bandwidth of the link. However, increasing the bandwidth might not be necessary or immediately practical. One way to resolve marginal serial line overutilization problems is to control how the router uses data buffers.

Caution In general, do *not* adjust system buffers unless you are working closely with a Cisco technical support representative. You can severely affect the performance of your hardware and your network if you incorrectly adjust the system buffers on your router.

Use one of the following three options to control how buffers are used:

- Adjust parameters associated with system buffers
- Specify the number of packets held in input or output queues (hold queues)
- Prioritize how traffic is queued for transmission (priority output queuing)

The configuration commands associated with these options are described in the Cisco IOS configuration guides and command references.

The following section focuses on identifying situations in which these options are likely to apply and defining how you can use these options to help resolve connectivity and performance problems in serial/WAN interconnections.

Tuning System Buffers

There are two general buffer types on Cisco routers. These are referred to as hardware buffers and system buffers. Only the system buffers are directly configurable by system administrators.

The hardware buffers are specifically used as the receive and transmit buffers associated with each interface and (in the absence of any special configuration) are dynamically managed by the system software itself.

The system buffers are associated with the main system memory and are allocated to different size memory blocks. A useful command for determining the status of your system buffers is the **show buffers** EXEC command. Figure 13-8 shows the output from the **show buffers** command.

Figure 13-8 show buffers Command Output

```
Cookie-Monster>show buffers
Buffer elements:
     401 in free list (500 max allowed)
     87777499 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 120, permanent 120):
     114 in free list (20 min, 250 max allowed)
     70005538 hits, 6 misses, 2 trims, 2 created
Middle buffers, 600 bytes (total 90, permanent 90):
     88 in free list (10 min, 200 max allowed)
     25696696 hits, 27 misses, 27 trims, 27 created
Big buffers, 1524 bytes (total 90, permanent 90):
     90 in free list (5 min, 300 max allowed)
     8214530 hits, 15 misses, 366 trims, 366 created
Large buffers, 5024 bytes (total 5, permanent 5):
     5 in free list (0 min, 30 max allowed)
     15017 hits, 12 misses, 16354 trims, 16354 created
Huge buffers, 18024 bytes (total 3, permanent 0):
     2 in free list (0 min, 4 max allowed)
     297582 hits, 17 misses, 30 trims, 33 created

0 failures (0 no memory)
```

Trims

Created

Failures

S3405

The **show buffers** command output in Figure 13-8 indicates high numbers in the trims and created fields for Large Buffers. If this is the case, you can increase your serial link performance by increasing the max-free value configured for your system buffers.

Use the **buffers max-free** *number* global configuration command to increase the number of free system buffers. The value you configure should be approximately 150 percent of the figure indicated in the Total field of the **show buffers** command output. Repeat this process until the **show buffers** output no longer indicates trims and created buffers.

If the **show buffers** command output shows a large number of failures in the "(no memory)" field (see the last line of output in Figure 13-8), you must reduce the usage of the system buffers or increase the amount of shared or main memory (physical RAM) on the router. Call your technical support representative for assistance.

Implementing Hold Queue Limits

Hold queues are buffers used by each router interface to store outgoing or incoming packets. Use the **hold-queue** interface configuration command to increase the number of data packets queued before the router will drop packets.

Note The **hold-queue** command is used for process-switched packets and periodic updates generated by the router.

Use this command to prevent packets from being dropped and to improve serial-link performance under the following conditions:

- You have an application that cannot tolerate drops and the protocol is able to tolerate longer delays. DECnet is an example of a protocol that meets both criteria. LAT does not because it does not tolerate delays.
- The interface is very slow (bandwidth is low or anticipated utilization is likely to sporadically exceed available bandwidth).

Note When you increase the number specified for an output hold queue, you might need to increase the number of system buffers. The value used depends on the size of the packets associated with the traffic anticipated for the network.

Using Priority Queuing to Reduce Bottlenecks

Priority queuing is a list-based control mechanism that allows traffic to be prioritized on an interface-by-interface basis. Priority queuing involves two steps:

Step 1 Create a priority list by protocol type and level of priority.

Step 2 Assign the priority list to a specific interface.

Both of these steps use versions of the **priority-list** global configuration command. In addition, further traffic control can be applied by referencing **access-list** global configuration commands from **priority-list** specifications. For examples of defining priority lists and for details about command syntax associated with priority queuing, refer to the Cisco IOS configuration guides and command references.

Note Priority queuing automatically creates four hold queues of varying size. This overrides any hold queue specification included in your configuration.

Use priority queuing to prevent packets from being dropped and to improve serial link performance under the following conditions:

- When the interface is slow, there are a variety of traffic types being transmitted, and you want to improve terminal traffic performance.
- If you have a serial link that is intermittently experiencing very heavy loads (such as file transfers occurring at specific times), you can use priority lists to select which types of traffic should be discarded at high traffic periods.

In general, start with the default number of queues when implementing priority queues. After enabling priority queuing, monitor output drops with the **show interfaces serial** EXEC command. If you notice that output drops are occurring in the traffic queue you have specified to be high priority, increase the number of packets that can be queued (using the **queue-limit** keyword option of the **priority-list** global configuration command).

Note When bridging DEC LAT traffic, the router must drop very few packets, or LAT sessions can terminate unexpectedly. A high priority queue depth of about 100 (specified with the **queue-limit** keyword) is a typical working value when your router is dropping output packets and the serial lines are subjected to about 50 percent bandwidth utilization. If the router is dropping packets and is at 100 percent utilization, you need another line.

Another tool to relieve congestion when bridging DEC LAT is LAT compression. You can implement LAT compression with the interface configuration command **bridge-group** *group* **lat-compression**.

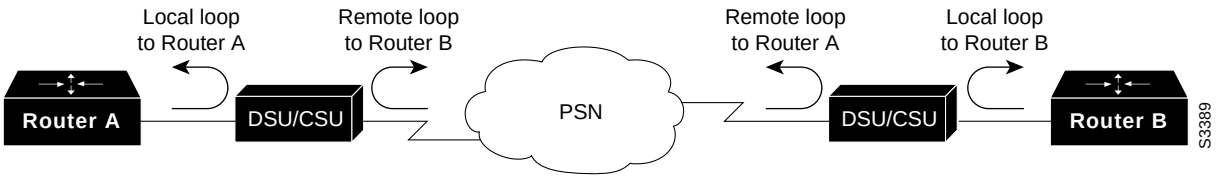
Special Serial Line Tests

In addition to the basic diagnostic capabilities available on routers, there are a variety of supplemental tools and techniques that can be used to determine the conditions of cables, switching equipment, modems, hosts, and remote internetworking hardware. For more information, consult the documentation for your CSU, DSU, serial analyzer, or other equipment.

CSU and DSU Loopback Tests

If the output of the **show interfaces serial** EXEC command indicates that the serial line is up but the line protocol is down, use the CSU/DSU loopback tests to determine the source of the problem. Perform the local loop test first, then the remote test. Figure 13-9 illustrates the basic topology of the CSU/DSU local and remote loopback tests.

Figure 13-9 CSU/DSU Local and Remote Loopback Tests



Note These tests are generic in nature and assume attachment of the internetworking system to a CSU or DSU. However, the test is essentially the same for attachment to a multiplexer with built-in CSU/DSU functionality. Because there is no concept of a loopback in X.25 or Frame Relay packet-switched network (PSN) environments, loopback tests do not apply to X.25 and Frame Relay networks.

CSU and DSU Local Loopback Tests for HDLC or PPP Links

Following is a general procedure for performing loopback tests in conjunction with built-in system diagnostic capabilities.

Step 1 Place the CSU/DSU in local loop mode (refer to your vendor documentation). In local loop mode, the use of the line clock (from the T1 service) is terminated, and the DSU is forced to use the local clock.

Step 2 Use the **show interfaces serial** EXEC command to determine whether the line status changes from "line protocol is down" to "line protocol is up (looped)," or if it remains down.

Step 3 If the line protocol comes up when the CSU or DSU is in local loopback mode, it suggests that the problem is occurring on the remote end of the serial connection. If the status line does not change state, there is a possible problem in the router, connecting cable, or CSU/DSU.

Step 4 If the problem appears to be local, use the **debug serial interface** privileged EXEC command.

Step 5 Take the CSU/DSU out of local loop mode. When the line protocol is down, the **debug serial interface** command output will indicate that keepalive counters are not incrementing.

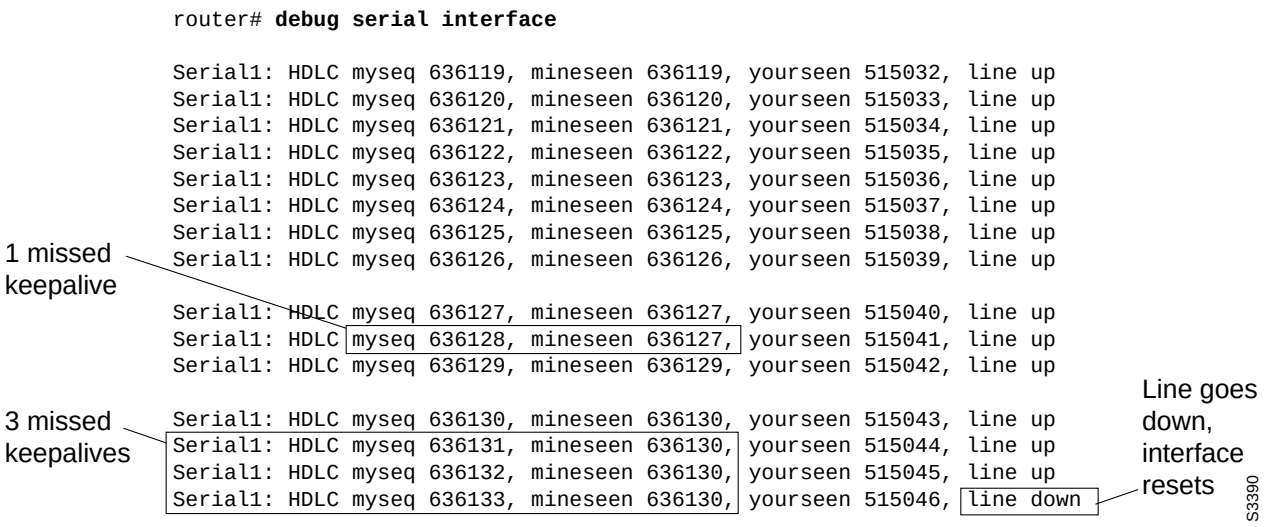
Step 6 Place the CSU/DSU in local loop mode again. This should cause the keepalive packets to begin to increment. Specifically, the values for *mineseen* and *yourseen* keepalives will increment every 10 seconds. This information will appear in the **debug serial interface** output.

If the keepalives do not increment, there may be a timing problem on the interface card or on the network. For information on correcting timing problems, refer to the section "Troubleshooting Clocking Problems," earlier in this chapter.

Step 7 Check the local router and CSU/DSU hardware, and any attached cables. Make certain the cables are within the recommended lengths (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). Make certain the cables are attached to the proper ports. Swap faulty equipment as necessary.

Figure 13-10 shows the output from the **debug serial interface** command for an HDLC serial connection, with missed keepalives causing the line to go down and the interface to reset.

Figure 13-10 debug serial interface Command Output



CSU and DSU Remote Loopback Tests for HDLC or PPP Links

If you determine that the local hardware is functioning properly but you still encounter problems when attempting to establish connections over the serial link, try using the remote loopback test to isolate the problem cause.

Note This remote loopback test assumes that HDLC encapsulation is being used and that the preceding local loop test was performed immediately before this test.

Step 1 Put the remote CSU or DSU into remote loopback mode (refer to the vendor documentation).

Step 2 Using the **show interfaces serial** EXEC command, determine whether the line protocol remains up with the status line indicating "Serial *x* is up, line protocol is up (looped)," or if it goes down with the status line indicating "line protocol is down."

Step 3 If the line protocol remains up (looped), the problem is probably at the remote end of the serial connection (between the remote CSU/DSU and the remote router). Perform both local and remote tests at the remote end to isolate the problem source.

Step 4 If the line status changes to "line protocol is down" when remote loopback mode is activated, make certain that ones density is being properly maintained. The CSU/DSU must be configured to use the same framing and coding schemes used by the leased-line or other carrier service (for example, ESF and B8ZS).

Step 5 If problems persist, contact your WAN network manager or the WAN service organization.