CHAPTER 3

Troubleshooting Serial Line Problems

There are a variety of tools and techniques to troubleshoot serial line problems. This chapter includes the following sections that discuss a range of universally applicable tools for troubleshooting serial links:

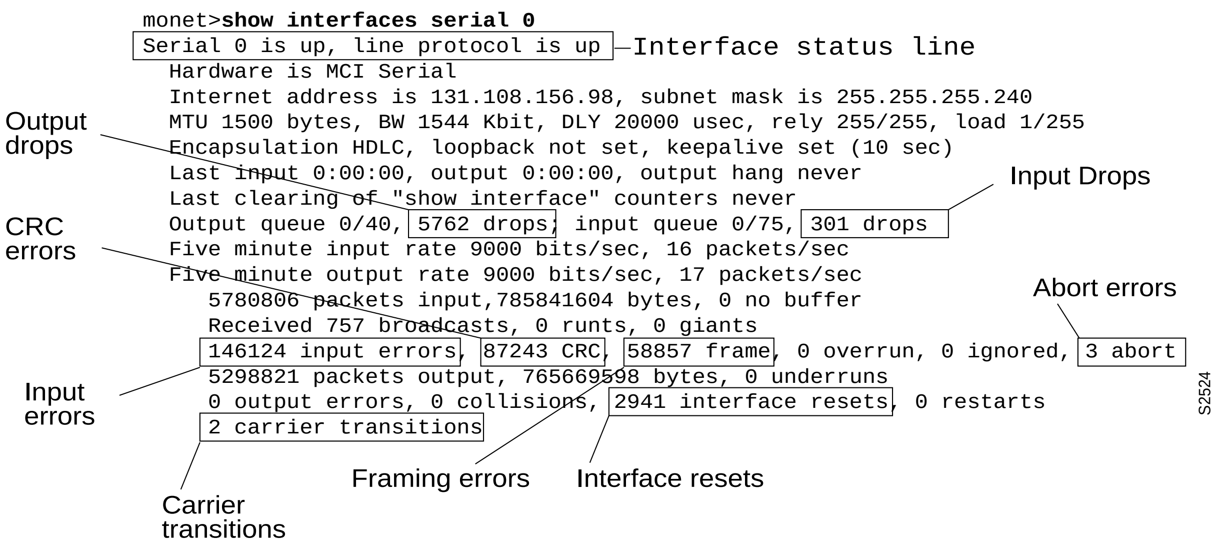
- Using the show interfaces Command to Troubleshoot Serial Lines—This section discusses the **show interfaces serial** *number* EXEC command and explains the various fields that appear in the output. For complete details about variables and options for **show** commands, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.
- Using the show controllers Command to Troubleshoot Serial Lines—This section discusses the various **show controllers** EXEC commands and provides an explanation of some of the important fields that appear in the output. For complete details about variables and options for **show** commands, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.
- Using debug Commands to Troubleshoot Serial Lines—This section describes important **debug** commands. Details about **debug** commands are provided in the *Debug Command Reference* publication.
- Troubleshooting Clocking Problems—This section discusses serial line clock issues and troubleshooting techniques.
- Using Extended ping Tests to Troubleshoot Serial Lines—This section discusses the use of extended **ping** tests.
- Adjusting Buffers to Ease Overutilized Serial Links—This section provides information on adjusting the size of buffers and queues.
- Special Serial Line Tests—This section discusses local and remote channel service unit (CSU) and data service unit (DSU) loopback tests.
- Troubleshooting Access Server to Modem Connectivity—This section discusses common modem connection problems and includes a number of symptom modules that address specific symptoms and suggest specific solutions.

Using the show interfaces Command to Troubleshoot Serial Lines

The **show interfaces** EXEC command is an important and useful show command. The specific information displayed depends on the interface type being examined (serial, Ethernet, Token Ring, or FDDI) and the type of encapsulation being used on the network (such as X.25 or Switched Multimegabit Data Service [SMDS]). This discussion focuses on information in the serial version of the display and outlines the specific fields used to diagnose serial line connectivity problems in a wide-area network (WAN) environment.

Figure 3-1 illustrates the **show interfaces serial** *number* EXEC command output for a High-Level Data Link Control (HDLC) serial interface. The interface is not running packet-switched software. The fields presented in this display are detailed in the *Router Products Configuration Guide* and *Router Products Command Reference* publications. This section describes the fields that are particularly important for diagnosing serial line problems.

Figure 3-1 Output from the HDLC Version of the show interfaces serial Command



Interface and Line Protocol Status

Five possible problem states can be identified in the interface status line (see Figure 3-1) of the **show interfaces serial** *number* display:

- 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 3-1 summarizes the causes associated with each of these conditions and suggests appropriate actions.

Table 3-1 Interface Status Conditions Displayed by the show interfaces serial Command

Status Line State	Possible Causes and Suggested Actions
Serial *x* is down, line protocol is down (data terminal equipment [DTE] mode)	This status indicates that the router is not sensing a carrier detect (CD) signal (that is, CD is not active). **Possible Causes:** **1** Telephone company problem—Line down; line not connected to CSU/DSU **2** Faulty or incorrect cabling **3** Faulty or incorrect applique (AGS/CGS/MGS only) **4** Hardware failure (CSU/DSU) **Suggested Actions:** **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** Check the applique. If it is incorrect, install the correct applique (AGS/CGS/MGS only). **Step 4** Insert a breakout box; check all control leads. **Step 5** Contact your leased-line or other carrier service. **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.

Status Line State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (DTE mode)	**Possible Causes:** **1** Local or remote router misconfigured **2** Keepalives not being sent by remote router **3** Leased-line or other carrier service problem—noisy line; misconfigured or failed switch **4** Timing problem on cable (serial clock transmit external [SCTE] not set on CSU/DSU) **5** Failed local or remote CSU/DSU **6** Router hardware failure (local or remote) **Suggested Actions:** **Step 1** Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** *number* command to determine whether the line protocol comes up. If the line protocol does come up, it is likely that there is a telephone company problem or that the remote router is down. **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 State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (data communications equipment [DCE] mode)	**Possible Causes:** **1** Missing **clockrate** interface configuration command **2** The 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 **Suggested Actions:** **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. See the section "Inverting the Transmit Clock" later in this chapter. **Step 3** Verify that the correct cable is being used. **Step 4** If 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)	**Possible Causes:** **1** 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. **Suggested Actions:** **Step 1** Use the **write terminal** privileged EXEC command to look for any instances of the **loopback** interface configuration command. **Step 2** If you find an occurrence of the **loopback** interface configuration command, 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 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.

Status Line State	Possible Causes and Suggested Actions
Serial *x* is up, line protocol is down (disabled)	**Possible Causes:** **1** High error rate due to telephone company service problem **2** CSU or DSU hardware problem **3** Bad router hardware (interface, applique) **Suggested Actions:** **Step 1** Troubleshoot with serial analyzer and breakout box; look for toggling Clear To Send (CTS) and Data Set Ready (DSR) 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	**Possible Causes:** **1** Router configuration includes the **shutdown** interface configuration command **2** Duplicate IP address **Suggested Actions:** **Step 1** Check 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 **write terminal** 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.

Evaluating Input Errors

When input errors appear in the **show interfaces serial** *number* output, you must consider several possibilities in order to determine the source of those errors. The most likely problems are summarized in the list of possible causes 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.

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

Possible Cause The following causes can result in this symptom:

- Faulty telephone company equipment
- Noisy serial line
- Incorrect clocking configuration (SCTE not set)
- Incorrect cable; 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 for this symptom:

Step 1 Use a serial analyzer to isolate the source of the 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 described later in this chapter to isolate the specific problem source.

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 3-2 details the meaning of CRC errors, framing errors, and aborts. These fields appear in the display shown in Figure 3-1.

Table 3-2 Meaning of Key Input Errors for Serial Line Troubleshooting

Input Error Type (Field Name)	Possible Causes and Suggested Actions
CRC errors (CRC)	**Meaning:** CRC calculation does not pass; some data is corrupted. **Possible Causes:** **1** Noisy serial line **2** Serial cable is too long; 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) **Suggested Actions:** **Step 1** Ensure that the line is clean enough for transmission requirements; shield 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 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 (for example, Extended Superframe Format [ESF]/Binary 8-Zero Substitution [B8ZS]) used by the leased-line or other carrier service. **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 Causes and Suggested Actions
Framing errors (frame)	**Meaning:** Detected packet does not end on an 8-bit byte boundary. **Possible Causes:** **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 span (incorrect framing or coding specification) **Suggested Actions:** **Step 1** Ensure that the line is clean enough for transmission requirements. Make certain you are using the correct cable. 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 to use 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 (for example, ESF/B8ZS) used by the leased-line or other carrier service. **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 Causes and Suggested Actions
Aborted transmission (abort)	**Meaning:** Illegal sequence of one bits (more than 7 in a row) **Possible Causes:** **1** SCTE mode is not enabled on DSU **2** CSU line clock is incorrectly configured **3** Serial cable is too long; 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, bad sending interface on remote router **Suggested Actions:** **Step 1** Ensure that all devices are properly configured to use 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.

Inverting the Transmit Clock

If you are attempting serial connections of 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.

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, check the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

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

Evaluating Output Drops

Output drops appear in the output of the **show interfaces serial** *number* command when the system is attempting to hand off a packet to a transmit buffer but no buffers are available. The output drops count is illustrated in Figure 3-1.

Symptom Increasing output drops

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

Recommended Action The following steps are suggested for this symptom:

Step 1 Minimize periodic broadcast traffic such as routing and SAP updates by using access lists or 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 of IP fast switching, enter the **no ip route-cache** interface configuration command. For the command syntax for other protocols, consult the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Step 4 Implement priority queuing on slower serial links by configuring priority lists. For information on configuring priority lists, see the *Router Products Configuration Guide* and the *Router Products Command Reference* publications.

Note Output drops are acceptable under certain conditions. For instance, if a link is known to be overused (with no opportunity or 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.

Evaluating Input Drops

Input drops appear in the **show interfaces serial** *number* EXEC command when too many packets from that interface are still being processed in the system. The input drops count is illustrated in Figure 3-1.

Symptom Increasing number of input drops

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, FDDI, and Token Ring) and serial interfaces. When traffic is light, there is no problem. As traffic rates increase, backups start occurring. By design, routers 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.

Evaluating Interface Resets

Interface resets that appear in the **show interfaces serial** *number* EXEC command are the result of missed keepalive packets. The interface resets count is illustrated in Figure 3-1.

Symptom Increasing interface resets

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 analyzing interface resets, you must examine other fields of the **show interfaces serial** *number* 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 3-1):

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

Step 2 Check the carrier transitions field in the **show interfaces serial** *number* 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/carrier service and swap faulty equipment as necessary.

Step 3 Examine the input errors field in the **show interfaces serial** *number* 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.

Evaluating Carrier Transitions

Carrier transitions appear in the output of the **show interfaces serial** *number* EXEC command whenever there is an interruption in the carrier signal; for example, when there is an interface reset at the remote end of a link. The carrier transitions count is illustrated in Figure 3-1.

Symptom Increasing carrier transitions count

Possible Cause The following causes can result in this symptom:

- Line interruptions due to an external source (examples: physical separation of cabling; Red or Yellow T1 alarms; lightning strikes 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 breakout box or serial analyzer and test to determine source of problems).

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

Step 3 Swap faulty equipment as necessary.

Using the show controllers Command to Troubleshoot Serial Lines

The **show controllers** EXEC command is another important diagnostic tool. 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 3-2 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. Make certain that the cable to the CSU/DSU is attached to the proper interface. Check the microcode version to see if it is current.

Figure 3-2 show controllers cbus Command Output

```
Harold>show controllers cbus
Switch Processor 5, hardware version 11.1, microcode version 10.7
Microcode loaded from system
512 Kbytes of main memory, 128 Kbytes cache memory
4 256 byte buffers, 4 1024 byte buffers, 312 1520 byte buffers
1024 byte system buffer
Restarts: 0 line down, 0 hung output, 0 controller error
FSIP 0, hardware version 1.0, microcode version 175.0
Microcode loaded from system
Interface 0 - Serial 0/0, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 1 - Serial 0/1, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 2 - Serial 0/2, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
Interface 3 - Serial 0/3, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tql 23
Transmitter delay is 0 microseconds
```

Microcode version

Interface and attached cable information

S3397

The **show controllers** EXEC command is used on access products such as the Cisco 2000, Cisco 2500, Cisco 3000, and Cisco 4000 series. Figure 3-3 shows the **show controllers** command output from the basic-rate interface (BRI) and serial interfaces on a Cisco 2503. (Note that, in the interest of space, some output is not shown.) The **show controllers** output indicates the state of the interface channels and describes the whether a cable is attached to the interface. In Figure 3-3, serial interface 0 has an RS-232 DTE cable attached; serial interface 1 has no cable attached.

Figure 3-3 show controllers Command Output

```
Maude>show controllers
BRI unit 0
D Chan Info:
Layer 1 is DEACTIVATED
```

D channel is deactivated

```
[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B1 Chan Info:
Layer 1 is DEACTIVATED
```

B channel 1 is deactivated

```
[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B2 Chan Info:

[. . .]
LANCE unit 0, idb 0x9515C, ds 0x96F00, regaddr = 0x2130000, reset_mask 0x2
IB at 0x40163F4: mode=0x0000, mcfilter 0000/0000/0000/0000
station address 0000.0c0a.28a7  default station address 0000.0c0a.28a7
buffer size 1524

[. . .]
0 missed datagrams, 0 overruns, 0 late collisions, 0 lost carrier events
0 transmitter underruns, 0 excessive collisions,  0 tdr, 0 babbles
0 memory errors, 0 spurious initialization done interrupts
0 no enp status, 0 buffer errors, 0 overflow errors
0 one_col, 0 more_col, 3 deferred, 0 tx_buff
0 throttled, 0 enabled
Lance csr0 = 0x73

HD unit 0, idb = 0x98D28, driver structure at 0x9AAD0
buffer size 1524  HD unit 0, RS-232 DTE cable
```

Attached cable on serial interface 0

```
[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

HD unit 1, idb = 0x9C1B8, driver structure at 0x9DF60
buffer size 1524  HD unit 1, No DCE cable
```

No attached cable on serial interface 1

```
[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
```

S3398

Figure 3-4 illustrates the output for 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), a bad applique or a problem with the internal wiring of the card is likely. This might also indicate an improperly connected cable. In addition, the corresponding display for the **show interfaces serial** *number* EXEC command will show that the interface and line protocol are down. (See Figure 3-1.)

Figure 3-4 Output from the show controllers mci Command

Electrical interface identified as type
UNKNOWN, suggesting a hardware
failure or improperly connected cabl

```
MCI 1, controller type 1.1, microcode version 1.8
  128 Kbytes of main memory, 4 Kbytes cache memory
16 system TX buffers, largest buffer size 1520
  Restarts: 0 line down, 0 hung output, 0 controller error
  Interface 0 is Ethernet1, station address 0000.0c00.3b09
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
  Interface 1 is Serial2, electrical interface is UNKNOWN
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
  Interface 3 is Serial3, electrical interface is V.35 DTE
    22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
```

S2525

Using debug Commands to Troubleshoot Serial Lines

The output from **debug** privileged EXEC commands provides diagnostic information concerning a variety of internetworking events relating to protocol status and network activity in general.

Caution Throughout this and other chapters, the use of **debug** commands is suggested for obtaining information about network traffic and router status. Use these commands with great care. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems. Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions. When you finish using a **debug** command, remember to disable it with its specific **no debug** command or with the **no debug all** command (the **undebug** command is also accepted).

To minimize the impact of using **debug** commands, follow this procedure:

Step 1 Issue the **no logging console** global configuration command on your router. This command disables all logging to the console terminal.

Step 2 Telnet to a router port and enter the **enable** EXEC command.

Step 3 Issue the **terminal monitor** command and issue the necessary **debug** commands.

Following this procedure minimizes the load created by using **debug** commands because the console port no longer has to generate character-by-character processor interrupts.

Following are some **debug** commands that are useful when troubleshooting serial and WAN problems.

- **debug serial interface—**Verifies whether HDLC keepalive packets are incrementing; if 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. Refer to the *Debug Command Reference* publication for more information concerning this command.
- **debug lapb**—Obtains 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 for determining whether a Frame Relay switch and 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 the 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 necessary error messages to indicate why a packet was not sent or was received erroneously. For SMDS, dumps the entire SMDS header and some payload data when an SMDS packet is transmitted or received.

More information about the output of each debug command is provided in the *Debug Command Reference* publication.

Troubleshooting Clocking Problems

Clocking conflicts in serial connections can lead to either chronic loss of connection service or generally degraded performance. The following discussion addresses five issues regarding clocking problems:

- Clocking Overview
- Clocking Problem Causes
- Detecting Clocking Problems
- Isolating Clocking Problems
- Suggested Clocking Problem Remedies

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). 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) framing and Alternate Mark Inversion (AMI) coding. AMI requires that the sending device maintain ones density, because it 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. The 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 the 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" earlier in this chapter.

Clocking Problem Causes

In general, clocking problems in serial WAN interconnections can be attributed to one of the following basic 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 your serial interface, look for input errors as follows:

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

Step 2 Examine the display output for CRC, framing errors, and aborts.

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 next procedure, "Isolating Clocking Problems."

Step 5 Bypass or repair faulty patch panel.

Isolating Clocking Problems

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

Step 1 Perform a series of loopback and **ping** tests, both local and remote, as described in the section "CSU and DSU Loopback Tests" later 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 Issue the **show interfaces serial** *number* 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 likely problem.

If only one end is experiencing input errors, there is likely to be 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** *number* display output and log any changes in error counts or note if the error count does not change.

Suggested Clocking Problem Remedies

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

Table 3-3 Serial Lines: Clocking Problems and Suggested Remedies

Clocking Problem Cause	Suggested Actions
Incorrect CSU configuration	**Step 1** Determine whether the CSUs at both ends are in agreement regarding the clock source (local or line). **Step 2** Configure both to agree if not already correctly configured (usually the line is the source). **Step 3** Check Line Build Out (LBO) setting on CSU/DSU 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** Enable SCTE on both ends of the connection if not already correctly configured. (For any interface that is connected to a line of 128 kbps or faster, SCTE *must* be enabled. If your CSU/DSU does not support SCTE, see the section "Inverting the Transmit Clock" earlier 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. **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	**Step 1** Use shorter cable if longer than 50 feet (15.24 meters). **Step 2** Replace with shielded cable.

Using Extended ping Tests to Troubleshoot Serial Lines

The *ping* function is one of the useful tests available on Cisco internetworking systems (as well as on many host systems). In TCP/IP terminology, this diagnostic tool also is known as the "Internet Control Message Protocol (ICMP) Echo Request."

Note The ping function is particularly useful when high levels of input errors are being registered in the **show interfaces serial** *number* display (see Figure 3-1).

Cisco internetworking systems provide a mechanism to automate the sending of many ping packets in sequence. Figure 3-5 illustrates the menu used to specify extended ping options. This example specifies only 20 successive pings; however, when testing the components on your serial line, you should specify a much larger number, such as 1000 pings.

Figure 3-5 Extended ping Specification Menu

```
Betelgeuse# ping
Protocol [ip]:
Target IP address: 129.44.12.7
Repeat count [5]: 20
Datagram size [100]: 64
Timeout in seconds [2]:
Extended commands [n]: yes
Source address:
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]: ffff
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 64-byte ICMP Echos to  129.44.12.7, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

ping count specification

Extended commands selected option

Data pattern specification

S2526

In general, perform serial line ping tests as follows:

Step 1 Put CSU or DSU into local loopback mode.

Step 2 Configure the extended **ping** command to send different data patterns and packet sizes. Figure 3-6 and Figure 3-7 illustrate two useful **ping** tests, an all-zeros 1500 byte **ping** and an all-ones 1500 byte **ping**, respectively.

Figure 3-6 All-Zeros 1500 Byte ping Test

1500 byte packet size

All zeros ping

```
yowzers#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]: 0000
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0x0000
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
yowzers#
```

S3391

Figure 3-7 All-Ones 1500 Byte ping Test

1500 byte packet size

All ones ping

```
zounds#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]: ffff
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
zounds#
```

S3392

Step 3 Examine the **show interfaces serial** *number* statistics and determine whether input errors have increased. If input errors have not increased, the local hardware (DSU, cable, router interface card, and applique) is likely to be good.

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 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, consult your router technical support representative.

Adjusting Buffers to Ease Overutilized Serial Links

Excessively high bandwidth utilization results in reduced overall performance and can cause intermittent failures. For example, DECnet file transmissions may be failing due to packets being dropped somewhere in the network. If the situation is bad enough, you *must* add bandwidth; however, adding bandwidth may 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, you should *not* adjust system buffers unless you are working closely with your router 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.

You have 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 (called "hold queues")
- Prioritize how traffic is queued for transmission (also called "priority output queuing")

The configuration commands associated with these options are fully described in the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

The following discussion 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. Commands are discussed as appropriate.

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 3-8 shows an example of the output from the **show buffers** command.

Figure 3-8 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)                Trims
     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)                  Created
     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)  Failures                     S3405
```

The **show buffers** command output in Figure 3-8 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 3-8), 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 router 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 stand 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. (Low bandwidth and/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 network administrators to prioritize traffic transmitted into networks on an interface-by-interface basis. In a manner that is analogous to Cisco's access list traffic control mechanisms, 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 (with the keywords **protocol** and **interface**, as appropriate). 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 details about command syntax associated with priority queuing, refer to the *Router Products Configuration Guide* and *Router Products Command Reference* publications.

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 (altered with the **queue-limit** keyword option of the **priority-list** global configuration command) when implementing priority queues. After enabling priority queuing, monitor output drops with the **show interfaces serial** *number* 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.

Note When bridging DEC LAT traffic, your router must drop very few packets, or LAT will not function correctly (that is, sessions will 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**.

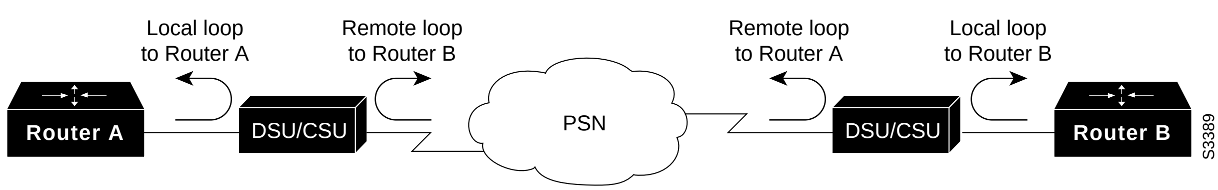
Special Serial Line Tests

In addition to the basic diagnostic capabilities provided with routers, there are a variety of supplemental tools and techniques that can be used to determine the conditions of cables, switching gear, modems, hosts, and remote internetworking hardware. Although complete discussions of these tools are beyond the scope of this publication, some hints about using these alternative tools are provided here. 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** *number* 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 3-9 illustrates the topology of the CSU/DSU local and remote loopback tests.

Figure 3-9 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

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

Step 1 Place the CSU/DSU in local loop mode. 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** *number* 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, issue the **debug serial interface** privileged EXEC command.

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

Step 6 Again place the CSU/DSU in local loop mode. 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 T1 link). Make certain the cables are attached to the proper ports. Swap faulty equipment as necessary.

Figure 3-10 shows the output from the **debug serial interface** command for an HDLC serial connection, with missed keepalives eventually causing the line to go down and the interface to reset.

Figure 3-10 debug serial interface Command Output

```
router# debug serial interface

Serial1: HDLC myseq 636119, mineseen 636119, yourseen 515032, line up
Serial1: HDLC myseq 636120, mineseen 636120, yourseen 515033, line up
Serial1: HDLC myseq 636121, mineseen 636121, yourseen 515034, line up
Serial1: HDLC myseq 636122, mineseen 636122, yourseen 515035, line up
Serial1: HDLC myseq 636123, mineseen 636123, yourseen 515036, line up
Serial1: HDLC myseq 636124, mineseen 636124, yourseen 515037, line up
Serial1: HDLC myseq 636125, mineseen 636125, yourseen 515038, line up
Serial1: HDLC myseq 636126, mineseen 636126, yourseen 515039, line up

Serial1: HDLC myseq 636127, mineseen 636127, yourseen 515040, line up
Serial1: HDLC myseq 636128, mineseen 636127, yourseen 515041, line up
Serial1: HDLC myseq 636129, mineseen 636129, yourseen 515042, line up

Serial1: HDLC myseq 636130, mineseen 636130, yourseen 515043, line up
Serial1: HDLC myseq 636131, mineseen 636130, yourseen 515044, line up
Serial1: HDLC myseq 636132, mineseen 636130, yourseen 515045, line up
Serial1: HDLC myseq 636133, mineseen 636130, yourseen 515046, line down
```

1 missed keepalive

3 missed keepalives

Line goes down, interface resets

S3390

CSU and DSU Remote Loopback Tests for HDLC or PPP Links

If you are able to 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 that follows 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.

Step 2 Using the **show interfaces serial** *number* 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 (for example, ESF and B8ZS) used by the leased-line or other carrier service.

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

Troubleshooting Access Server to Modem Connectivity

This section offers recommended procedures for properly setting up an access server-to-modem connection, and presents a number of symptom modules that describe access server-to-modem connectivity problems and suggested actions for resolving them. This section does not cover hardware problems. For information on troubleshooting your hardware, see the "Troubleshooting Router Startup Problems" chapter. See the "Troubleshooting AppleTalk Connectivity" chapter for modem troubleshooting information that is directly related to AppleTalk Remote Access (ARA) dial-in sessions.

The first part of this section, "Initiating a Reverse Telnet Session to a Modem," describes the procedure for establishing a reverse Telnet session with your modem in order to set the proper speed and configure it at that speed. The rest of the section includes the following troubleshooting symptom modules:

- No Connectivity Between Access Server and Modem
- Remote Dial-In Sees "Garbage"
- High Rate of Data Loss Over Modem Connection
- Modem Does Not Disconnect Properly
- Remote Dial-In Client Receives No EXEC Prompt
- Remote Dial-In Interrupts Existing Sessions

Initiating a Reverse Telnet Session to a Modem

Establishing a reverse Telnet session with your modem allows you to configure the modem at the speed at which you want it to communicate with the Cisco device. As long as you lock the DTE-side speed of the modem (see Table 3-6 for information on locking the modem speed), the modem will always speak to the access server or router at the desired speed. Be certain that the speed of the Cisco device is configured prior to issuing commands to the modem via a reverse Telnet session. (See Table 3-6 for information on configuring the speed of the access server or router.)

To initiate a reverse Telnet session to your modem, perform the following steps:

Step 1 From your terminal, issue the command

telnet *x.x.x.x* **20***yy*

where *x.x.x.x* is the IP address of any active, connected interface on the Cisco device that is currently up, and *yy* is the line number to which the modem is connected. For example, the following command

```
telnet 192.169.53.52 2001
```

would connect you to the auxiliary port on a Cisco router with IP address 192.169.53.52. A Telnet command of this kind can generally be issued from anywhere on the network that can **ping** IP address *x.x.x.x*.

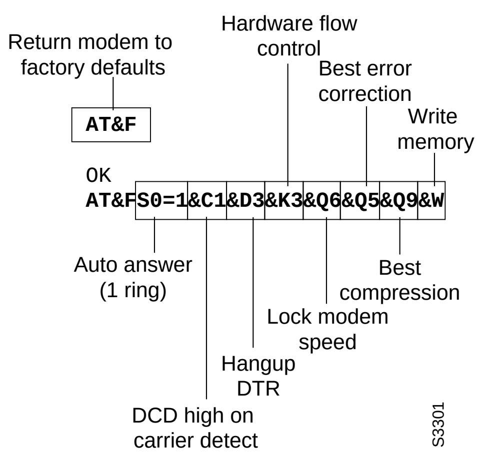
Note On a Cisco router, port 01 is the auxiliary port. On a Cisco access server, the auxiliary port is *last_tty+1*, so on a 16-port access server, the auxiliary port is port 17. Use the **show line** EXEC command to make certain you are working with the correct line.

Step 2 If the connection is refused, there may already be a user connected to that port. Issue the **show users** EXEC command to determine if the line is being used. If desired, the line can be cleared from the console using the **clear line** privileged EXEC command. When you are certain the line is not in use, attempt the Telnet connection again.

Step 3 If the connection is again refused, confirm that you have set modem control to **modem inout** for that line. See Table 3-4 for information on configuring a line on a Cisco device for modem control.

Step 4 After successfully making the Telnet connection, you are ready to configure the modem. Make sure that when you enter **AT**, the modem replies with OK. Figure 3-11 shows a typical Hayes-compatible modem command string. Again, be certain to check the documentation for your specific modem to verify the exact syntax of these commands.

Figure 3-11 Typical Hayes-Compatible Modem Command String



No Connectivity Between Access Server and Modem

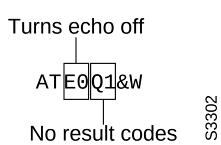
Symptom: Connectivity between a modem and a Cisco access server or router is nonexistent. Attempts to initiate a reverse Telnet session to the modem have no result, or the user receives a "Connection Refused by Foreign Host" message. Table 3-4 describes possible causes and suggests actions when modem to access server connections are unresponsive.

Table 3-4 Modem: No Connectivity Between Access Server and Modem

Possible Causes	Suggested Actions
Modem control is not enabled on the access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** Issue the **show line** EXEC command on the access server or router. The output for the auxiliary port should show inout or RIisCD in the Modem column. This indicates that modem control is enabled on the line of the access server or router. For an explanation of the **show line** output, see the "Interpreting show line Output" section later in this chapter. **Step 2** If you are running software prior to Software Release 9.21, and therefore do not have modem control, perform these steps and do not proceed to Step 3: • Disable echo on the modem. This is typically done with the **E0** modem command. Check your modem documentation for the exact syntax of modem commands. • Disable result codes on the modem. This is typically done using the **Q1** modem command. Check your modem documentation for the exact syntax. See Figure 3-12 for a modem command string that disables echo and result codes on a Hayes-compatible modem. • On the access server or router, configure the line to which the modem is connected with the **exec timeout** line configuration command. This command tells the access server to end the EXEC session after a specified period of time of no activity. **Step 3** If you are running Software Release 9.21 or later, configure the line for modem control using the **modem inout** line configuration command. Modem control is now enabled on the access server. The **debug modem** output should indicate the change. NOTE: Be certain to use the **modem inout** command in favor of the **modem ri-is-cd** command while the connectivity of the modem is in question. The latter command allows the line to accept incoming calls only. Outgoing calls will be refused, making it impossible to establish a Telnet session with the modem to configure it. If you want to enable the **modem ri-is-cd** command, do so only after you are certain the modem is functioning correctly.

Possible Causes	Suggested Actions
Incorrect cabling configuration	**Step 1** Check the cabling between the modem and the access server or router. Confirm that the modem is connected to the auxiliary port on the access server or router with a rolled RJ-45 cable and an MMOD DB-25 adapter. This cabling configuration is recommended and supported by Cisco for RJ-45 ports. **Step 2** If you are using a rolled RJ-45 cable with an MDCE DB-25 adapter, or a straight RJ-45 cable with an MDTE DB-25 adapter, you must dismantle the connector on the EIA/TIA-232 side and move pin 6 to pin 8. This turns the MDCE or MDTE adapter into an MMOD adapter by wiring the DCD output of the modem to the DSR input of the access server or router. **Step 3** Use the **show line** *line-number* EXEC command to verify that the cabling is correct. See the explanation of the **show line** command output in the section "Interpreting show line Output," following.
Hardware problem	**Step 1** Verify that you are using the correct cabling and that all connections are good. **Step 2** Check all hardware for damage, including cabling (broken wire), adapters (loose pin), access server ports, and modem. **Step 3** See the "Troubleshooting Router Startup Problems" chapter for more information on hardware troubleshooting.

Figure 3-12 Hayes-Compatible Modem Command String for Pre-Modem Control Software



Interpreting show line Output

The output from the **show line** *line-number* EXEC command is useful when troubleshooting a modem-to-access server or router connection. Figure 3-13 shows the output from the **show line** *line-number* command. Important fields and their meanings are noted following.

Figure 3-13 show line Command Output

Line speed

Modem control enabled

Hardware flow control enabled

Modem state

EXEC timeout configured

Modem hardware state

```
Choncie# show line 1
 Tty Typ    Tx/Rx       A Modem  Roty AccO AccI  Uses    Noise   Overruns
   1 AUX  38400/38400   - inout     -    -    -     0        0        0/0

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 38400/38400, no parity, 2 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
  Modem Callout, Modem RI is CD
Modem state: Idle
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               0:10:00        never                        none     not set
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
Full user help is disabled
Allowed transports are pad telnet mop.  Preferred is telnet.
No output characters are padded
No special data dispatching characters
Modem hardware state: CTS noDSR  DTR RTS
Choncie#
```

S3309

When connectivity problems occur, important output appears in the Modem State and the Modem Hardware State fields.

Note The Modem Hardware State field does not appear in the **show line** *line-number* output for every platform. In certain cases, the indications for signal states will be shown in the Modem State field instead.

Table 3-5 shows typical Modem State and Modem Hardware State strings from the output of the **show line** *line-number* command and explains the meaning of each state.

Table 3-5 Modem and Modem Hardware States in show line Output

<table>
<tr><th>Modem State</th><th>Modem Hardware State</th><th>Meaning</th></tr>
<tr><td>Idle</td><td>CTS noDSR DTR RTS</td><td>These are the proper modem states for connections between an access server or router and a modem. Output of any other kind generally indicates a problem.</td></tr>
<tr><td>Ready</td><td>–</td><td>If the Modem State is Ready instead of Idle, there are three possibilities:
1 Modem control is not configured on the access server or router. Configure the access server or router with the modem inout line configuration command.
2 A session exists on the line. Issue the show users EXEC command and use the clear line privileged EXEC command to kill the session if desired.
3 DSR is high. There are two possible reasons for this:
— Cabling problems—The DSR signal from the modem is connected to DSR from the access server. The proper signalling is DCD (modem) to DSR (access server).
Check the cabling configuration as described in Table 3-4.
— Modem configured for DCD always high—The modem should be reconfigured to have DCD high only on carrier detect (CD). This is usually done with the &C1 modem command (see Figure 3-11), but check your modem documentation for the exact syntax for your modem.
You might have to configure the access server line to which the modem is connected with the no exec line configuration command. Clear the line with the clear line privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD.
End the Telnet session by entering disconnect and reconfigure the access server line with the exec line configuration command.</td></tr>
</table>

<table>
<tr><th>Modem State</th><th>Modem Hardware State</th><th>Meaning</th></tr>
<tr><td>Ready</td><td>noCTS noDSR DTR RTS</td><td>There are four possibilities for the noCTS string appearing in the Modem Hardware State field:
1 Modem is turned off.
2 Modem is not connected to the access server properly. Check the cabling connections from the modem to the access server.
3 Incorrect cabling configuration (either rolled MDCE or straight MDTE, but without the pins moved). See Table 3-4 for information on the recommended cabling configuration.
4 Modem is not configured for hardware flow control. Disable hardware flow control on the access server with the no flowcontrol hardware line configuration command. Enable hardware flow control on the modem via a Reverse Telnet session. (Consult your modem documentation and see the section “Initiating a Reverse Telnet Session to a Modem,” earlier in this chapter.) Reenable hardware flow control on the access server with the flowcontrol hardware line configuration command.</td></tr>
<tr><td>Ready</td><td>CTS DSR DTR RTS</td><td>There are two possibilities for the presence of the DSR string instead of the noDSR string in the Modem Hardware State field:
1 Incorrect cabling configuration (either rolled MDCE or straight MDTE, but without the pins moved). See Table 3-4 for information on the recommended cabling configuration.
2 The modem is configured for DCD always high. Reconfigure the modem so that DCD is only high on CD. This is usually done with the &C1 modem command (see Figure 3-11), but check your modem documentation for the exact syntax for your modem.
Configure the access server line to which the modem is connected with the no exec line configuration command. Clear the line with the clear line privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD.
End the Telnet session by entering disconnect. Reconfigure the access server line with the exec line configuration command.</td></tr>
<tr><td>Ready</td><td>CTS* DSR* DTR RTS</td><td>If this string appears in the Modem Hardware State field, it is likely that modem control is not enabled on the access server. Use the modem inout line configuration command to enable modem control on the line.
See Table 3-4 for more information on configuring modem control on an access server or router line.</td></tr>
</table>

Remote Dial-In Sees "Garbage"

Symptom: Attempts to establish remote dial-in sessions over a modem to a Cisco access server or router return "garbage" and ultimately result in no connection to the remote site. User might see a "Connection Closed by Foreign Host" message. Table 3-6 describes possible causes and suggests actions for remote dial-in sessions seeing "garbage."

Table 3-6 Modem: Remote Dial-In Sessions Seeing "Garbage"

Possible Causes	Suggested Actions
Modem speed setting is not locked.	**Step 1** Issue the **show line** EXEC command on the access server or router. The output for the auxiliary port should indicate the currently configured transmit (Tx) and receive (Rx) speeds. For an explanation of the output from the **show line** command, see the "Interpreting show line Output" section earlier in this chapter. **Step 2** If the line speed is not configured to the speed you desire, you must reconfigure the line. Use the **speed** line configuration command to set the line speed on the access server or router line. Set the value to the highest speed in common between the modem and the access server or router port. NOTE: If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data. **Step 3** Issue the **show line** EXEC command again and confirm that the line speed is set to the desired value. **Step 4** When you are certain that the access server or router line is configured for the desired speed, initiate a reverse Telnet session to the modem via that line. For more information, see the section "Initiating a Reverse Telnet Session to a Modem." **Step 5** Issue a modem command string that includes the lock DTE speed command for your modem. See your modem documentation for exact configuration command syntax. NOTE: The lock DTE speed command, which might also be referred to as *port rate adjust* or *buffered mode*, is often related to the way in which the modem handles error correction. This command varies widely between modems. Locking the modem speed ensures that the modem always communicates with the Cisco access server or router at the speed configured on the Cisco auxiliary port. If this command is not used, the modem will revert to the speed of the data link (the telephone line) instead of communicating at the speed configured on the access server.

High Rate of Data Loss Over Modem Connection

Symptom: Remote sessions over a modem connection experience a high rate of data loss. Table 3-7 shows possible causes and suggests actions when there is a high rate of data loss over a modem connection.

Table 3-7 Modem: High Rate of Data Loss Over Modem Connection

Possible Causes	Suggested Actions
Error correction is not configured on the modem.	**Step 1** Make certain the modem is configured for error correction. For the exact syntax of the command, see your modem documentation.
Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured.	**Step 1** Display detailed information about the auxiliary line using the **show line** *aux-line-number* EXEC command. In the Capabilities field (see Figure 3-13), look for the following: `Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out...` If there is no mention of hardware flow control in this field, hardware flow control is not enabled on the line. Cisco recommends hardware flow control for access server-to-modem connections. For an explanation of the output from the **show line** command, see the “Interpreting show line Output” section earlier in this chapter. **Step 2** Configure hardware flow control on the line using the **flowcontrol hardware** line configuration command. NOTE: If for some reason you cannot use flow control, limit the line speed to 9600 bps. Faster speeds are likely to result in lost data. **Step 3** After enabling hardware flow control on the access server or router line, initiate a reverse Telnet session to the modem via that line. For more information, see the section “Initiating a Reverse Telnet Session to a Modem.” **Step 4** Issue a modem command string that includes the RTS/CTS Flow command for your modem. This command ensures that the modem is using the same method of flow control (that is, hardware flow control) as the Cisco access server or router. See your modem documentation for exact configuration command syntax. Figure 3-11 shows the hardware flow control command string for a Hayes-compatible modem.

Modem Does Not Disconnect Properly

Symptom: Modem does not disconnect properly. Connection to modem does not terminate when **quit** command is entered. Table 3-8 describes possible causes and suggests actions for a modem that does not disconnect properly.

Table 3-8 Modem: Modem Not Disconnecting Properly

Possible Causes	Suggested Actions
Modem is not sensing DTR.	**Step 1** Enter the Hangup DTR modem command string. This command tells the modem to drop carrier when the DTR signal is no longer being received. On a Hayes-compatible modem the **&D3** string is commonly used, as shown in Figure 3-11. For the exact syntax of this command, see the documentation for your modem.
Modem control is not configured on the router or access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** See Table 3-4 for instructions on configuring modem control on a router or access server port.

Remote Dial-In Client Receives No EXEC Prompt

Symptom: Remote dial-in client opens a session and appears to be connected, but the user does not receive an EXEC prompt (for example, a Username or Router> prompt). Table 3-9 describes possible causes and suggests actions for a remote dial-in client that is not receiving an EXEC prompt.

Table 3-9 Modem: Remote Dial-In Client Is Not Receiving an EXEC Prompt

Possible Causes	Suggested Actions
Autoselect is enabled on the line.	**Step 1** Attempt to access EXEC mode by issuing a carriage return.
Line is configured with the **no exec** command.	**Step 1** Use the **show line** *line-number* EXEC command to view the status of the appropriate line. Check the Capabilities field to see if it says "EXEC suppressed." If this is the case, the **no exec** line configuration command is enabled. **Step 2** Configure the **exec** line configuration command on the line to allow EXEC sessions to be initiated.
Flow control is not enabled, is enabled only on one device (either DTE or DCE), or is misconfigured.	**Step 1** For information on configuring flow control, see Table 3-7.
Modem speed setting is not locked.	**Step 1** For information on setting the speed of your access server or modem, see Table 3-6.

Remote Dial-In Interrupts Existing Sessions

Symptom: Remote dial-in session interrupts an already existing session initiated by another user. Table 3-10 describes possible causes and suggests actions for remote dial-in sessions interrupting existing sessions.

Table 3-10 Modem: Remote Dial-In Interrupts Existing Sessions

Possible Causes	Suggested Actions
Modem configured for DCD always high.	**Step 1** The modem should be reconfigured to have DCD high only on carrier detect (CD). This is usually done with the **&C1** modem command string (see Figure 3-11), but check your modem documentation for the exact syntax for your modem. **Step 2** You might have to configure the access server line to which the modem is connected with the **no exec** line configuration command. Clear the line with the **clear line** privileged EXEC command, initiate a reverse Telnet session with the modem, and reconfigure the modem so that DCD is high only on CD. **Step 3** End the Telnet session by entering **disconnect** and reconfigure the access server line with the **exec** line configuration command.
Modem control is not configured on the router or access server (modem control on auxiliary ports is only available in Software Release 9.21 and later).	**Step 1** See Table 3-4 for instructions on configuring modem control on a router or access server port.
Incorrect cabling configuration	**Step 1** See Table 3-4 for information on the recommended cabling configuration.