

ΔΡΟΜΟΛΟΓΗΤΕΣ

ΑΛΛΑΓΗ IOS

1. Δίνουμε IP σε ένα eth interface για να μπει στο δίκτυο του υπολογιστή στον οποίο είναι αποθηκευμένο το νέο IOS.
2. Τρέχουμε την εφαρμογή tftp.32 στον υπολογιστή που έχει το καινούργιο IOS. Στις ρυθμίσεις επιλέγουμε ``bind TFTP to this address: 192.150.160.76(την διεύθυνση του pc)
3. Αν θέλουμε να κρατήσουμε το παλιό IOS δίνουμε την εντολή router#copy flash:.....tftp.
4. Διαγράφουμε το παλιό IOS με την εντολή:
Router#delete flash:.....
5. Αντιγράφουμε το καινούργιο IOS από τον υπολογιστή: router# copy tftp:.....flash.
6. Κάνουμε reload.

ΕΝΕΡΓΟΠΟΙΗΣΗ E1 CONTROLLER

```
(config)#card type e1 00  
(config)#controller e1 0/0/0  
(config-if)#linecode hdb3  
(config-if)#framing crc4  
(config-if)#channel-group 0 timeslots 1-31 (για δομημένο κύκλωμα)  
(config-if)#channel-group 0 unframed (όταν το κύκλωμα είναι αδόμητο)
```

ΔΗΜΙΟΥΡΓΙΑ multilink

```
(config-if)# interface multilink xxx  
(config-if)# ip address xxxxxx  
(config-if)# ppp multilink  
(config-if)# ppp multilink group xxx
```

ΔΗΜΙΟΥΡΓΙΑ Tunnel

```
(config)# interface tunnel 0  
(config-if)# ip address 193.0.100.50 255.255.255.0  
(config-if)# ip pim sparse-dense mode  
(config-if)# cdp enable  
(config-if)# tunnel source gig 0/0  
(config-if)# tunnel destination 193.0.50.20
```

ΡΥΘΜΙΣΕΙΣ Console/vty

```
Line con 0  
Exec-timeout 5 0  
Authorization exec console  
Login authentication console  
Line vty 0 4 /5 15  
Access class xx in  
Exec-timeout 5 0  
Privilege level 15  
Password xxxxxx  
Authorization exec ssh  
Login authentication ssh  
Transport input ssh
```

ΡΥΘΜΙΣΕΙΣ ΘΥΡΑΣ Switch

```
(config)# switchport mode(access/trunk)
(config)# switchport access vlan xx
```

ΕΝΕΡΓΟΠΟΙΗΣΗ Vlan

```
(config)# int vlan xxx
(config-if)# ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
(config-if)# no shut
```

ΑΛΛΑΓΗ registry σε router

- 1) reload τον router
- 2) Κατά την εκκίνηση πατάμε break ή ctrl break
- 3) rommon 1 -> confreg 0x2142
rommon 2 -> reset
- 4) Αφού ξαναξεκινήσει ο router # copy startup – config running – config
(config)# enable secret.....
(config)# config – register 0x2102
router # copy running – config startup - config

Cisco Password Recovery

-Restart ο router και πατάμε Break για να μπει σε rommon

```
rommon 1>confreg 0x2142
rommon 2>reset (κάνει επανεκκίνηση)
router>en
router#copy startup-config running-config
router#conf t
(config)#username.....password.....
(config)#enable secret.....
(config)#config-register 0x2102
Router#copy running-config startup-config
Router reload
```

*Για να διαφημίσουμε τα στατικά routers:

```
Router(config-router)#redistribute static
```

*Για να διαφημίσουμε ένα default route:

```
Router(config)#router ospf1
Router(config-router)#default-information originate
```

*Για να μη διαφημίσουμε το πρωτόκολλο στο LAN:

```
Router(config)#router ospf1
Router(config router)#passive-interface fastethernet 0/0
```

*Για να σετάρουμε compression over ppp σ'ένα interface:

```
Router(config-if)#encapsulation ppp
Router(config-if)#compress predictor ή stac
```

*Για να δούμε τον Frame-relay:

```
Router#sh frame-relay map
```

*Για να ενεργοποιήσουμε το routing authentication σε ένα router με ospf:

```
Router(config-if)#ip ospf message-digest key 1 md5(cisco)
Router(config-if)#ip ospf authentication message digest
Router(config)#router ospf 10
Router(config-router)#area 0 authentication message digest
```

*Για να επιτρέπεται μόνο ένας χρήστης στις access lists:

```
Router(config)#access list 1 permit host.....
```

*Για να ορίσουμε subinterfaces σ' ένα router ώστε να δεχτεί VLANs:

```
Router(config)#int F0/0.10
Router(config-if)#encapsulation dot1q 10
Router(config-subif)#ip address 172.16.0.20 255.255.255.0
Router (config)#int P0/0.30
Router (config-subif)#ip address 172.16.2.20 255.255.255.0
Router(config)#int Fa 0/0
Router(config-if)#no shutdown
```

E1 ISDN PRI Τηλεφωνία

```
Conf t # isdn switch-type primary-qsig
Conf t # controller E1 0/0/0
Conf t - if # framing crc4
Conf t - if # linecode hdb3
Conf t - if # clock source internal
Conf t # pri- group timeslots 1-31
Conf t#int serial s0/0/0:15
Config-if# no ip address
        # no ip redirects
        # no ip unreachable
        # no ip proxy-arp
        # ip flow ingress
        # encapsulation ppp
        # isdn switch - type primary - gsig
        # isdn timer T310 12000
        # isdn overlap-receiving
        # isdn protocol-emulate network
        # isdn incoming-voice voice
        # isdn bchan-number-order descending
        # isdn sending-complete
        # no cdp enable
Conf t # voice port 0/0/0:15
Cont t # dialer-peer voice 301 VoIP
Conf t - if # destination-pattern 5399
Conf t - if # progress_ind setup enable 3
Conf t - if # session target ipv4: 193.193.104.0
Conf t -if # dtmf-relay cisco-rtp h245 - signal h245 alphanumeric


---


Conf t # dial - peer voice 2011 voip
Conf t - if # destination-pattern 8.....
Conf t - if # progress ind setup enable 3
Conf t - if # session target ip4:193.9.100.95
Conf t -if # dtmf relay cisco-rtp h245-signal h245-alphanumeric


---


Conf t # dial-peer voice 301 pots
Conf t - if # destination pattern 5399
Conf t - if # progress_ind setup enable 3
```

Conf t – if #port 0/0/0

Voice Ports Config

```
Conf t # voice port 0/0/0
Conf – if # connection plar opx 20
Conf t # dial – peer voice 20 voip
Conf – if # destination – pattern 20
Conf – if # session target ipv4: xxx.xxx.xxx.xxx (θύρα άλλου router)
Conf – if # destination – pattern 40
Conf – if # port 0/0/0
```

```
Conf t # voice port 0/1/0
Conf – if# connection plar 40
Conf t #dial – peer voice 40 voip
Conf – if # destination – pattern 40
Conf – if # session target ipv4: xxx.xxx.xxx.xxx
Conf t # dial-peer 20 pots
Conf – if #destination – pattern 20
Conf – if # port 0/1/0
```

IOS Load via rommon

```
Rommon 1> ip-address= xxx.xxx.xxx.xxx
Rommon 2> ip-subnet-mask= xxx.xxx.xxx.xxx
Rommon 3> default-gateway=xxx.xxx.xxx.xxx
Rommon 4> tftp-server=xxx.xxx.xxx.xxx
Rommon 5> tftp-file=c3725-ipvoice-mz.123-26.bin
Rommon 6> tftpdnld
Rommon 7> boot flash: c3725-ipvoice-mz.123-26.bin
Conf t # no boot system
Conf t # boot system flash : c3725-ipvoice-mz.123-26.bin
Conf t # config – register 0x2102
Conf t # wr
Conf t # reload
```

Connecting a Cisco router to internet using PPPOE

```
R1# conf t
R1(config)# int vlan1
R1(config-if)# ip address 192.168.50.1 255.255.255.0
R1(config-if)# no shutdown
```

```
R1# conf t
R1(config)# int ATM 0
R1(config-if)# pvc 8/35
R1(config-atm-vc)# pppoe-client dial-pool-number1
R1(config-if-atm-vc)#exit
R1(config-if)# no shut
R1(config-if)# exit
```

```
R1# conf t
R1(config)# int dialer 1
R1(config-if)# ip address negotiated
R1(config-if)# ip mtu 1492
```

```

R1(config-if)# encapsulation ppp
R1(config-if)# dialer pool 1
R1(config-if)# ppp pap sent-username XXXX(adsltest) password XXXX(1234)
R1(config-if)# exit

R1(config)# ip route 0.0.0.0 0.0.0.0 dialer1
R1(config)# exit
R1#sh ip int brief(check if the route has public IP address)
*ping www.google.com to see if it's working

R1(config)# access-list 1 permit any
R1 (config)# ip nat inside source list 1 interface dialer 1 overload
*ping DFG and then to 8.8.8.8 it doesn't work because NAT configuration is not
completed

R1(config)# int vlan 1
R1(config-if)# ip nat inside
R1(config-if)# exit
R1 (config)#int dialer 1
R1(config-if)#ip nat outside
R1(config – if)# exit
R1(config)#
*check if the pc goes out to the internet after NAT configuration ping 8.8.8.8(good)
R1(config)# no ip route 0.0.0.0 0.0.0.0 dialer 1
*check again the internet connection(won't work)
We want default route to be received directly from ISP.
R1(config)# int dialer 1
R1(config-if)#ppp ipcp route default
R1#sh ip route(there will be no route)
R1(config)# int dialer 1(shutdown and no shut to renegotiate)
R1#sh ip route(default route will be received by ISP)
*Ping 8.8.8.8 (It should ping it)
Check via browser if we can connect to the internet.No because of the absence of
DNS.We need to configure router as the DNS Server
R1(config)# ip dns server
R1(config)# int dialer 1
R1(config-if)# ppp ipcp dns request accept
R1(config-if)# shutdown and no shut
R1# sh ip int brief(check if the router got an ip from ISP)
*check again internet connection using a web browser.

```

ΜΕΤΑΓΩΓΕΙΣ

Για να δούμε 10 τελευταίες εντολές που έχουμε δώσει:
Switch# sh history

Για να ενεργοποιήσουμε το ιστορικό:
Switch# terminal history

Για να απενεργοποιήσουμε το ιστορικό:
Switch# terminal no history

Για να δώσουμε IP address σ'ένα VLAN:
Switch# conf t

```
Switch(config)# interface VLAN 99
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)# no shutdown
```

Για να αντιστοιχίσουμε σ'ένα VLAN σε μια πόρτα του Switch:

```
Switch(config)# int Fa 0/18
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 99
```

Για να ορίσουμε default gateway για τα switch:

```
Switch (config)# ip default gateway 172.16.1.2
```

Για να αναγνωρίζει το interface αυτόματα τα καλώδια:

```
Switch(config-if)# mdix auto
```

Για να βάλουμε στο interface το auto duplex:

```
Switch(config-if)# duplex auto
```

Για να βάλουμε στο interface duplex speed και αυτόματη επιλογή ταχύτητας:

```
Switch(config-if)# speed auto
```

Για να ενεργοποιήσουμε ένα HTTP server ώστε να χειριζόμαστε τα WEB-Based εργαλεία :

```
Switch(config)# ip http server
```

Για να υπάρχει έλεγχος στο ποιός συνδέεται στο HTTP server του switch:

```
Switch(config)# ip http authentication enable
(για το enable password το οποίο είναι το default)
Switch(config)# ip http authentication local
(για local user database)
Switch(config)# ip http authentication tacacs
(όταν έχουμε server tacacs για να κάνει το authentication)
```

Για να δούμε τον πίνακα των mac-address:

```
Switch# sh mac-address table
```

Για να δημιουργήσουμε ένα στατικό στον πίνακα MAC-Address:

```
Switch# mac-address-table static «mac-address» vlan(1-4096)
Interface «fa 0/0»
```

Για να αποθηκεύσουμε το start up configuration σε άλλο σημείο στην flash memory:

```
Switch# copy startup config flash:«όνομα αρχείου»
```

Για να επαναφέρουμε κάποιο αποθηκευμένο startup configuration

```
Switch# copy flash: «όνομα αρχείου»start up-config και μετά με την εντολή reload.
```

Για να βάλουμε password στο console:

```
Switch(config)# line console 0
Switch(config-line)# password.....
Switch(config-line)# login
```

Για να βάλουμε password στο vty για remote:

```
Switch(config)#line vty 0 4
Switch(config-line)# password.....
```

Switch(config-line)# login

Για να βάλουμε password στο enable:

Switch(config)# enable password.....

Switch(config)# enable secret.....για κρυπτογραφημένο

Για να κρυπτογραφήσουμε όλα τα password στο switch:

Switch(config)# service password-encryption

Για να βάλουμε ένα login banner μήνυμα :

Switch(config)# banner login "μνμ"

Για να βάλουμε το πρωτόκολλο telnet να δουλεύει:

Switch(config)#line vty 0 15

Switch(config-line)# transport input telnet

Για να ενεργοποιήσουμε το port security:

Switch (config-if)# switchport mode access

Switch(config-if)# switchport port-security

Για να ορίσουμε ένα VLAN ως το native VLAN:

Switch(config)# int F0/1

Switch(config-if)# switchport mode trunk(Για να ανοίγει η πόρτα IEEE 802.1Qtrunk)

Switch(config-if)# switchport trunk native VLAN99

Για να δημιουργήσουμε ένα VLAN

Switch(config)#vlan (vlan 10)

Switch(config-vlan)#name (vlan name)

Για να αντιστοιχίσουμε μια πόρτα σ'ένα VLAN:

Switch(config)#int Fa/0/18

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 20

Troubleshooting Serial Lines

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

- Troubleshooting 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
- Detailed Information on the **show interfaces serial** Command
- Troubleshooting T1 Problems
- Troubleshooting E1 Problems

Troubleshooting Using the show interfaces serial Command

The output of the **show interfaces serial** exec command displays information specific to serial interfaces. Figure 15-1 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 wide-area network (WAN) environment. The following sections describe some of the important fields of the command output.

Other fields shown in the display are described in detail in the section "Detailed Information on the **show interfaces serial** Command," later in this chapter.

Serial Lines: show interfaces serial Status Line Conditions

You can identify five possible problem states in the interface status line of the **show interfaces serial** display (see Figure 15-1):

- 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

Figure 15-1 Output of the HDLC show interface serial Command

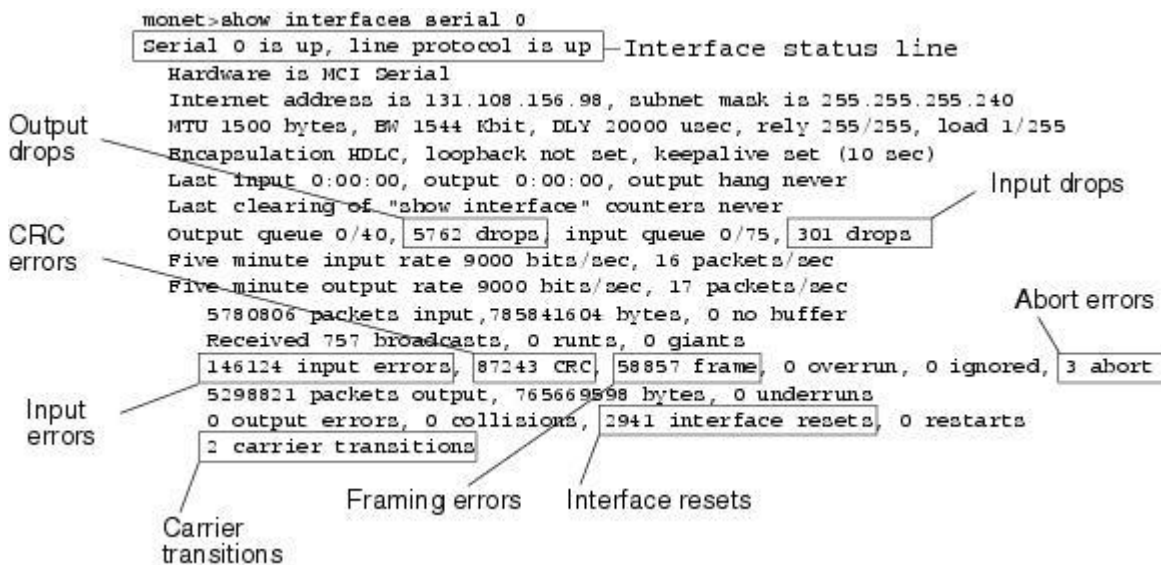


Table 15-1 shows the interface status conditions, possible problems associated with the conditions, and solutions to those problems.

Status Line Condition	Possible Problem	Solution
Serial x is up, line protocol is up	—	This is the proper status line condition. No action is required.
Serial x is down, line protocol is down (DTE ¹ mode)	<p>The router is not sensing a CD² signal (that is, the CD is not active).</p> <p>A telephone company problem has occurred—line is down or is not connected to CSU³/DSU⁴.</p> <p>Cabling is faulty or incorrect.</p> <p>Hardware failure has occurred (CSU/DSU).</p>	<ol style="list-style-type: none"> 1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that you are using the proper cable and interface (see your hardware installation documentation). 3. Insert a breakout box and check all control leads. 4. Contact your leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If you suspect faulty router hardware, change the serial line to another port. If the

		connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DTE mode)	<p>A local or remote router is misconfigured.</p> <p>Keepalives are not being sent by the remote router.</p> <p>A leased-line or other carrier service problem has occurred (noisy line or misconfigured or failed switch).</p> <p>A timing problem has occurred on the cable (SCTE⁵ not set on CSU/DSU).</p> <p>A local or remote CSU/DSU has failed.</p> <p>Router hardware (local or remote) has failed.</p>	<p>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.</p> <p>If the line protocol comes up, a telephone company problem or a failed remote router is the likely problem.</p> <p>2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU.</p> <p>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.</p> <p>4. Enable the debug serial interface exec command.mmm ,,,,</p>
Serial x is up, line protocol is down (DTE mode) (continued)		<p>Caution: Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system</p>

		<p>use.</p> <p>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.</p> <p>6. If the line protocol comes up and the keepalive counter increments, the problem is <i>not</i> 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.</p> <p>7. If you suspect faulty router hardware, change the serial line to an unused port. If the connection comes up, the previously connected interface has a problem.</p>
Serial x is up, line protocol is down (DCE ⁶ mode)	<p>The clockrate interface configuration command is missing.</p> <p>The DTE device does not support or is not set up for SCTE mode (terminal timing).</p> <p>The remote CSU or DSU has failed.</p>	<p>1. Add the clockrate interface configuration command on the serial interface.</p> <p>Syntax:</p> <p>clock rate <i>bps</i></p> <p>Syntax Description:</p> <ul style="list-style-type: none"> <i>bps</i>—Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000.
Serial x is up, line protocol is down (DCE mode)	The clockrate interface configuration command is missing.	<p>2. Set the DTE device to SCTE modem if possible. If your CSU/DSU does not support SCTE, you might have</p>

(continued)	<p>The DTE device does not support or is not set up for SCTE mode (terminal timing).</p> <p>The remote CSU or DSU has failed.</p>	<p>to disable SCTE on the Cisco router interface. Refer to the section "Inverting the Transmit Clock," later in this chapter.</p> <ol style="list-style-type: none"> 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. 5. Replace faulty parts, as necessary.
Serial x is up, line protocol is up (looped)	<p>A loop exists in the 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.</p>	<ol style="list-style-type: none"> 1. Use the show running-config privileged exec command to look for any loopback interface configuration command entries. 2. If you find a loopback interface configuration command entry, use the no loopback interface configuration command to remove the loop. 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. 4. Reset the CSU or DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 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)	<p>A high error rate has occurred due to a telephone company</p>	<ol style="list-style-type: none"> 1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS^z

	<p>service problem.</p> <p>A CSU or DSU hardware problem has occurred.</p> <p>Router hardware (interface) is bad.</p>	<p>and DSR⁸ signals.</p> <p>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.</p> <p>3. Swap out bad hardware, as required (CSU, DSU, switch, local or remote router).</p>
Serial x is administratively down, line protocol is down	<p>The router configuration includes the shutdown interface configuration command.</p> <p>A duplicate IP address exists.</p>	<p>1. Check the router configuration for the shutdown command.</p> <p>2. Use the no shutdown interface configuration command to remove the shutdown command.</p> <p>3. Verify that there are no identical IP addresses using the show running-config privileged exec command or the show interfaces exec command.</p> <p>4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.</p>

¹ DTE = data terminal equipment

² CD = carrier detect

³ CSU = channel service unit

⁴ DSU = digital service unit

⁵ SCTE = serial clock transmit external

⁶ DCE = data circuit-terminating equipment or data communications equipment

⁷ CTS = clear-to-send

⁸ DSR = data-set ready

Serial Lines: Increasing Output Drops on Serial Link

Output drops appear in the output of the **show interfaces serial** command (refer to Figure 15-1) 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

Table 15-2 outlines the possible problem that might cause this symptom and describes solutions to that problem.

Table 15-2 Serial Lines: Increasing Output Drops on Serial Link	
Possible Problem	Solution
Input rate to serial interface exceeds bandwidth available on serial link	<ol style="list-style-type: none"> 1. Minimize periodic broadcast traffic, such as routing and SAP¹ 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.
Input rate to serial interface exceeds bandwidth available on serial link (continued)	<ol style="list-style-type: none"> 2. Increase the output hold queue size in small increments (for instance, 25 percent), using the hold-queue out interface configuration command. 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. 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. <p>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 IPX²). However, some protocols, such as DECnet and local-area transport, are sensitive to dropped packets and accommodate retransmission poorly, if at all.</p>

¹ SAP = Service Advertising Protocol

² IPX = Internetwork Packet Exchange

Serial Lines: Increasing Input Drops on Serial Link

Input drops appear in the output of the **show interfaces serial** exec command (refer to Figure 15-1) when too many packets from that interface are still being processed in the system.

Symptom: Increasing number of input drops on serial link

Table 15-3 outlines the possible problem that might cause this symptom and describes solutions to that problem.

Table 15-3 Serial Lines: Increasing Input Drops on Serial Link	
Possible Problem	Solution
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 ¹) and serial interfaces. When traffic is light, there is no problem. As traffic rates increase, backups start occurring. Routers drop packets during these congested periods.
Input rate exceeds the capacity of the router, or input queues exceed the size of output queues (continued)	<ol style="list-style-type: none">1. Increase the output queue size on common destination interfaces for the interface that is dropping packets. Use the hold-queue number out interface configuration command. Increase these queues by small increments (for instance, 25 percent) until you no longer see drops in the show interfaces output. The default output hold queue limit is 100 packets.2. Reduce the input queue size, using the hold-queue number 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. The default input hold queue is 75 packets.

¹FDDI = Fiber Distributed Data Interface

Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic

If input errors appear in the **show interfaces serial** output (refer to Figure 15-1), there are several possible sources of those errors. The most likely sources are summarized in Table 15-4.

Note Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts above 1 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 1 percent of total interface traffic

Table 15-4 Serial Lines: Increasing Input Errors in Excess of 1 Percent of Total Interface Traffic	
Possible Problem	Solution
The following problems can result in this symptom: <ul style="list-style-type: none">Faulty telephone company equipmentNoisy serial lineIncorrect clocking configuration (SCTE not set)	Note: Cisco strongly recommends against the use of data converters when you are connecting a router to a WAN or a serial network. 1. Use a serial analyzer to isolate the source of the input errors. If you detect errors, there likely is a hardware problem or a clock mismatch in a device that is external to the router.
<ul style="list-style-type: none">Incorrect cable or cable that is too longBad cable or connectionBad CSU or DSUBad router hardwareData converter or other device being used between router and DSU	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. 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.

Serial Lines: Troubleshooting Serial Line Input Errors

Table 15-5 describes the various types of input errors displayed by the **show interfaces serial** command (see Figure 15-1), possible problems that might be causing the errors, and solutions to those problems.

Table 15-5 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) for one of the following	1. Ensure that the line is clean enough for transmission requirements. Shield the cable, if necessary. 2. Make sure that the cable is

	<p>reasons:</p> <ul style="list-style-type: none"> • The serial line is noisy. • The serial cable is too long, or the cable from the CSU/DSU to the router is not shielded • SCTE mode is not enabled on DSU. 	<p>within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link).</p> <p>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.</p> <p>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/B8ZS).</p>
CRC errors (CRC) (<i>continued</i>)	<ul style="list-style-type: none"> • The CSU line clock is incorrectly configured. • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). 	<p>5. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.</p>
Framing errors (frame)	<p>A framing error occurs when a packet does not end on an 8-bit byte boundary for one of the following reasons:</p> <ul style="list-style-type: none"> • The serial line is noisy • The cable is improperly designed; the serial cable is too long; the cable from the CSU or DSU to the router is not shielded. • SCTE mode is not enabled on the DSU; the CSU line clock is incorrectly configured; one of the clocks is configured for local 	<p>1. Ensure that the line is clean enough for transmission requirements. Shield the cable, if necessary. Make certain that you are using the correct cable.</p> <p>2. Make sure that the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link).</p> <p>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.</p> <p>4. Make certain that the local</p>

	<p>clocking.</p> <ul style="list-style-type: none"> • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). 	<p>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, ESF¹/B8ZS²).</p> <p>5. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.</p>
Aborted transmission (abort)	<p>Aborts indicate an illegal sequence of 1 bit (more than seven in a row)</p> <p>The following are possible reasons for this to occur:</p> <ul style="list-style-type: none"> • SCTE mode is not enabled on DSU. • The CSU line clock is incorrectly configured. • The serial cable is too long, or the cable from the CSU or DSU to the router is not shielded. • A ones density problem has occurred on the T1 link (incorrect framing or coding specification). • A packet terminated in middle of transmission (typical cause is an interface reset or a framing error). • A hardware problem has occurred (bad circuit, bad CSU/DSU, or bad sending interface on remote router). 	<p>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.</p> <p>2. Shield the cable, if necessary. Make certain that the cable is within the recommended length (no more than 50 feet [15.24 meters], or 25 feet [7.62 meters] for a T1 link). Ensure that all connections are good.</p> <p>3. Check the hardware at both ends of the link. Swap faulty equipment, as necessary.</p> <p>4. Lower data rates and determine whether aborts decrease.</p> <p>5. Use local and remote loopback tests to determine where aborts are occurring (see the section "Special Serial Line Tests," later in this chapter).</p> <p>6. Contact your leased-line or other carrier service, and have it perform integrity tests on the line.</p>

¹ESF = Extended Superframe Format

²B8ZS = binary eight-zero substitution

Serial Lines: Increasing Interface Resets on Serial Link

Interface resets that appear in the output of the **show interfaces serial** exec command (see Figure 15-1) are the result of missed keepalive packets.

Symptom: Increasing interface resets on serial link

Table 15-6 outlines the possible problems that might cause this symptom and describes solutions to those problems.

Table 15-6 Serial Lines: Increasing Interface Resets on Serial Link	
Possible Problem	Solution
<p>The following problems can result in this symptom:</p> <ul style="list-style-type: none">• Congestion on link (typically associated with output drops)• Bad line causing CD transitions• Possible hardware problem at the CSU, DSU, or switch	<p>When interface resets are occurring, examine other fields of the show interfaces serial command output to determine the source of the problem. Assuming that an increase in interface resets is being recorded, examine the following fields:</p> <ol style="list-style-type: none">1. If there is a high number of output drops in the show interfaces serial output, see the section "Serial Lines: Increasing Output Drops on Serial Link," earlier in this chapter.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 a bad CSU or DSU. Contact your leased-line or carrier service, and swap faulty equipment, as necessary.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 a bad CSU/DSU. Contact your leased-line or other carrier service, and swap faulty equipment, as necessary.

Serial Lines: Increasing Carrier Transitions Count on Serial Link

Carrier transitions appear in the output of the **show interfaces serial** exec command 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

Table 15-7 outlines the possible problems that might cause this symptom and describes solutions to those problems.

Table 15-7 Serial Lines: Increasing Carrier Transitions Count on Serial Link	
Possible Problem	Solution
The following problems can result in this symptom: <ul style="list-style-type: none">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	<ol style="list-style-type: none">1. Check hardware at both ends of the link (attach a breakout box or a serial analyzer, and test to determine the source of problems).2. If an analyzer or breakout box is incapable of identifying any external problems, check the router hardware.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 15-2 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 channel service unit/digital service unit (CSU/DSU) is attached to the proper interface. You can also check the microcode version to see whether it is current.

Figure 15-2 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

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 15-3 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 15-3, serial interface 0 has an RS-232 DTE cable attached. Serial interface 1 has no cable attached.

Figure 15-4 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.

Figure 15-3 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:

[. . .]
LANC unit 0, idb 0x9515C, ds 0x96F00, regaddr = 0x2130000, reset_mask 0x2
IB at 0x40163F4: mode=0x0000, mcfiler 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

```

Figure 15-4 show controllers mci Command Output

```

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 Serial12, 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

```

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

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 Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use. 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 Link Access Procedure, Balanced (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 Switched Multimegabit Data Service (SMDS) packets being sent and received. This display also prints 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 is also 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 15-1.

Cisco internetworking devices provide a mechanism to automate the sending of many **ping** packets in sequence. Figure 15-5 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**. Also increase the datagram size to a larger number, such as 1500.

Figure 15-5 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]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0xffff
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

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 15-6 and Figure 15-7 illustrate two useful **ping** tests, an all-zeros 1500-byte **ping** and an all-ones 1500-byte **ping**, respectively.

Step 3 Examine the **show interfaces serial** command output (see Figure 15-1) and determine whether input errors have increased. If input errors have not increased, the local hardware (DSU, cable, router interface card) 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. See the section "Troubleshooting Clocking Problems," next.

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 a problem either 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.

Figure 15-6 All-Zeros 1500-Byte ping Test

```
youzers#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte — Datagram size [100]: 1500
packet size — 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]:
Validate reply data? [no]:
All zeros — Data pattern [0xABCD]: 0x0000
ping — 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
youzers#
```

Figure 15-7 All-Ones 1500-Byte ping Test

```

sounds#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte packet size — 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]:
Validate reply data? [no]:
All ones ping — Data pattern [0xABCD]: 0xffff
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
sounds#

```

Troubleshooting Clocking Problems

Clocking conflicts in serial connections can lead either to chronic loss of connection service or to degraded performance. This section discusses the important aspects of clocking problems: clocking problem causes, how to detect clocking problems, how to isolate clocking problems, and clocking problem solutions.

Clocking Overview

The CSU/DSU derives the data clock from the data that passes through it. 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 eight-zero substitution (B8ZS) coding. B8ZS provides a scheme by which a special code is substituted whenever eight 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 can better 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 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.

Step 3 If either of these steps indicates errors exceeding an approximate range of 0.5 percent 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, use the following procedure to 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 section "CSU and DSU Loopback Tests," earlier in this chapter.

Step 2 Determine which end of the connection is the source of the problem, or whether 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.

Aborts on one end suggest that the other end is sending bad information or that there is a line problem.

Note Always refer to the **show interfaces serial** command output (see Figure 15-1). Log any changes in error counts, or note if the error count does not change.

Clocking Problem Solutions

Table 15-8 outlines suggested remedies for clocking problems, based on the source of the problem.

Table 15-8 Serial Lines: Clocking Problems and Solutions	
Possible Problem	Solution
Incorrect CSU configuration	<ol style="list-style-type: none">1. Determine whether the CSUs at both ends agree on the clock source (local or line).2. If the CSUs do not agree, configure them so that they do agree (usually the line is the source).3. Check the LBO¹ 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	<ol style="list-style-type: none">1. Determine whether the DSUs at both ends have SCTE mode enabled.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 <i>must</i> be enabled. If your DSU does not support SCTE, see the section "Inverting the Transmit Clock," later in this chapter.)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

	<p>on its framing and coding schemes.</p> <p>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.</p>
Cable to router out of specification	<p>If the cable is longer than 50 feet (15.24 meters), use a shorter cable.</p> <p>If the cable is unshielded, replace it with shielded cable.</p>

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 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 greater than 70 percent results in reduced overall performance and can cause intermittent failures. For example, DECnet file transmissions might be failing because of 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

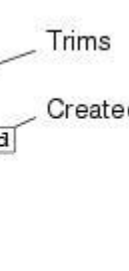
There are two general buffer types on Cisco routers: *hardware buffers* and *system buffers*. Only the system buffers are directly configurable by system administrators. The hardware buffers are specifically used as the receive and transmit buffers associated with each interface and (in the absence of 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 15-8 shows the output from the **show buffers** command.

Figure 15-8 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) Failures
```



In the **show buffers** output, the following is true:

- **total** identifies the total number of buffers in the pool, including used and unused buffers.
- **permanent** identifies the permanent number of allocated buffers in the pool. These buffers are always in the pool and cannot be trimmed away.
- **in free list** identifies the number of buffers currently in the pool that are available for use.
- **min** identifies the minimum number of buffers that the route processor (RP) should attempt to keep in the free list:
 - The **min** parameter is used to anticipate demand for buffers from the pool at any given time.
 - If the number of buffers in the free list falls below the **min** value, the RP attempts to create more buffers for that pool.
- **max allowed** identifies the maximum number of buffers allowed in the free list:
 - The **max allowed** parameter prevents a pool from monopolizing buffers that it doesn't need anymore, and frees this memory back to the system for further use.
 - If the number of buffers in the free list is greater than the **max allowed** value, the RP should attempt to trim buffers from the pool.
- **hits** identifies the number of buffers that have been requested from the pool. The hits counter provides a mechanism for determining which pool must meet the highest demand for buffers.
- **misses** identifies the number of times that a buffer has been requested and that the RP detected that additional buffers were required. (In other words, the number of buffers in the free list has dropped below **min**.) The misses counter represents the number of times that the RP has been forced to create additional buffers.
- **trims** identifies the number of buffers that the RP has trimmed from the pool when the number of buffers in the free list exceeded the number of **max allowed** buffers.
- **created** identifies the number of buffers that has been created in the pool. The RP creates buffers when demand for buffers has increased until the number of buffers in the free list is less than **min** buffers or a miss occurs because of zero buffers in the free list.
- **failures** identifies the number of failures to grant a buffer to a requester even after attempting to create an additional buffer. The number of failures represents the number of packets that have been dropped due to buffer shortage.
- **no memory** identifies the number of failures caused by insufficient memory to create additional buffers.

The **show buffers** command output in Figure 15-8 indicates high numbers in the Trims and Created fields for large buffers. If you are receiving high numbers in these fields, you can increase your serial link performance by increasing the **max free** value configured for your system buffers. **trims** identifies the number of buffers that the RP has trimmed from

the pool when the number of buffers in free list exceeded the number of **max allowed** buffers.

Use the **buffers max free** *number* global configuration command to increase the number of free system buffers. The value that 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 15-8), 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. Increase these queues by small increments (for instance, 25 percent) until you no longer see drops in the **show interfaces** output. The default output hold queue limit is 100 packets.

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

Use the **hold-queue** 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 capable of tolerating longer delays. DECnet is an example of a protocol that meets both criteria. Local-area transport (LAT) does not meet this criteria 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, a variety of traffic types are 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), and priority queuing will help 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 that 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). The default **queue-limit** arguments are 20 packets for the high-priority queue, 40 for medium, 60 for normal, and 80 for low.

Note When bridging Digital Equipment Corporation (Digital) 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 Digital LAT is LAT compression. You can implement LAT compression with the interface configuration command **bridge-group group lat-compression**.

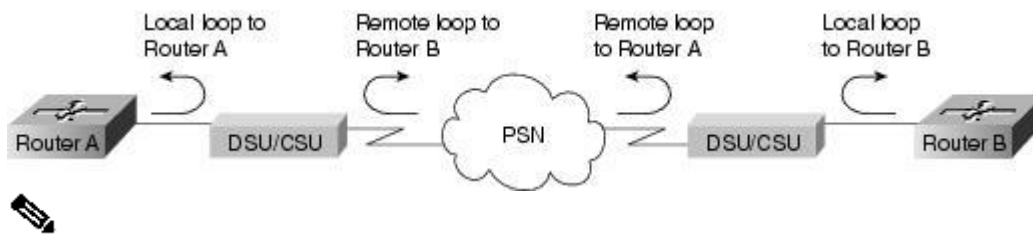
Special Serial Line Tests

In addition to the basic diagnostic capabilities available on routers, a variety of supplemental tools and techniques 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, and then perform the remote test. Figure 15-9 illustrates the basic topology of the CSU/DSU local and remote loopback tests.

Figure 15-9 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 tests are 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 whether it remains down.

Step 3 If the line protocol comes up when the CSU or DSU is in local loopback mode, this 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 that 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 that the cables are attached to the proper ports. Swap faulty equipment, as necessary.

Figure 15-10 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 15-10 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
1 missed
keepalive
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
3 missed
keepalives
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
Line goes
down,
interface
resets
```

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's 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.

The following are the steps required to perform loopback testing:

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 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 one's 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.

Detailed Information on the show interfaces serial Command

This section covers the **show interfaces serial** command's parameters, syntax description, sample output display, and field descriptions.

show interfaces serial

To display information about a serial interface, use the **show interfaces serial** privileged exec command:

show interfaces serial [*number*] [**accounting**]

show interfaces serial [*number* [:*channel-group*]] [**accounting**] (Cisco 4000 series)

show interfaces serial [*slot* | *port* [:*channel-group*]] [**accounting**] (Cisco 7500 series)

show interfaces serial [*type slot* | *port-adaptor* | *port*] [**serial**] (ports on VIP cards in the Cisco 7500 series)

show interfaces serial [*type slot* | *port-adaptor* | *port*] [:*t1-channel*] [**accounting** | **crb**] (CT3IP in Cisco 7500 series)

Syntax Description

- *Number*—(Optional) Port number.
- **accounting**—(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
- *:channel-group*—(Optional) On the Cisco 4000 series with an NPM or a Cisco 7500 series with a MIP, specifies the T1 channel-group number in the range of 0 to 23, defined with the channel-group controller configuration command.

- *slot*—Refer to the appropriate hardware manual for slot information.
- *port*—Refer to the appropriate hardware manual for port information.
- *port-adaptor*—Refer to the appropriate hardware manual for information about port adaptor compatibility.
- *:t1-channel*—(Optional) For the CT3IP, the T1 channel is a number between 1 and 28.

T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

- **crb**—(Optional) Shows interface routing and bridging information.

Command Mode

Privileged exec

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0 for the Cisco 4000 series. It first appeared in Cisco IOS Release 11.0 for the Cisco 7000 series, and it was modified in Cisco IOS Release 11.3 to include the CT3IP.

Sample Displays

The following is sample output from the **show interfaces** command for a synchronous serial interface:

```
Router# show interfaces serial
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 150.136.190.203, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:07, output 0:00:00, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    16263 packets input, 1347238 bytes, 0 no buffer
    Received 13983 broadcasts, 0 runts, 0 giants
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
1 carrier transitions
    22146 packets output, 2383680 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets, 0 restarts
```

Table 15-9 describes significant fields shown in the output.

Table 15-9 Show Interfaces Serial Field Descriptions	
Field	Description
Serial...is {up 	Indicates whether the interface hardware is

<i>down</i> }...is administratively down	currently active (whether carrier detect is present) or whether it has been taken down by an administrator.
line protocol is { <i>up</i> <i>down</i> }	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful), or whether it has been taken down by an administrator.
Hardware is	Specifies the hardware type.
Internet address is	Specifies the Internet address and subnet mask.
MTU	Specifies the maximum transmission unit of the interface.
BW	Indicates the value of the bandwidth parameter that has been configured for the interface (in kilobits per second). The bandwidth parameter is used to compute IGRP metrics only. If the interface is attached to a serial line with a line speed that does not match the default (1536 or 1544 for T1, and 56 for a standard synchronous serial line), use the bandwidth command to specify the correct line speed for this serial line. <i>continues</i>
DLY	Gives the delay of the interface in microseconds.
rely	Expresses reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Expresses load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes.
Encapsulation	Gives the encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
keepalive	Indicates whether keepalives are set.
Last input	Gives the number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
Last output	Gives the number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.

output hang	Gives the number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the last fields exceeds 24, the number of days and hours is printed. If that field overflows, asterisks are printed.
Output queue, drops input queue, drops	Gives the number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets because the queue is full.
5 minute input rate 5 minute output rate	<p>Gives the average number of bits and packets transmitted per second in the past 5 minutes.</p> <p>The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.</p>
packets input	Gives the total number of error-free packets received by the system.
bytes	Gives the total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Gives the number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Gives the total number of broadcast or multicast packets received by the interface.
runts	Gives the number of packets that are discarded because they are smaller than the medium's minimum packet size.
Giants	Gives the number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Gives the total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so this sum might not balance with the other counts.

CRC	The Cyclic Redundancy Check (CRC) counter is incremented by the originating station or far-end device when the checksum calculated from the data received does not match the checksum from the transmitted data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Gives the number of packets received incorrectly, having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Gives the number of times that the serial receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the receiver's capability to handle the data.
ignored	Gives the number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Indicates an illegal sequence of 1 bit on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
carrier transitions	Gives the number of times that the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. This indicates modem or line problems if the carrier detect line is changing state often.
packets output	Gives the total number of messages transmitted by the system.
bytes output	Gives the total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Gives the number of times that the transmitter has been running faster than the router can handle. This might never be reported on some interfaces.
output errors	Gives the sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors because some

	datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Gives the number of messages retransmitted because of an Ethernet collision. This usually is the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). Some collisions are normal. However, if your collision rate climbs to around 4 percent or 5 percent, you should consider verifying that there is no faulty equipment on the segment, or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Gives the number of times that an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Gives the number of times that the controller was restarted because of errors.
alarm indications, remote alarms, rx LOF, rx LOS	Gives the number of CSU/DSU alarms, and the number of occurrences of receive loss of frame and receive loss of signal.
BER inactive, NELR inactive, FELR inactive	Shows the status of G.703-E1 counters for bit error rate (BER) alarm, near-end loop remote (NELR), and far-end loop remote (FELR). Note that you cannot set the NELR or FELR.

Troubleshooting T1 Problems

This section describes the techniques and procedures to troubleshoot T1 circuits for dial-in customers.

Troubleshooting Using the show controller t1 Command

The **show controller t1** exec command provides information to logically troubleshoot physical layer and data link layer problems. This section describes how to logically troubleshoot using the **show controller t1** command.

This command displays the controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel.

The NPM or MIP can query the port adapters to determine their current status. Issue a **show controller t1** command to display statistics about the T1 link.

If you specify a slot and port number, statistics for each 15-minute period will be displayed.

Most T1 errors are caused by misconfigured lines. Ensure that linecoding, framing, and clock source are configured according to what the service provider recommends.

show controller t1 Conditions

The t1 controller can be in three states:

- Administratively down
- Down
- Up

Is the Controller Administratively Down?

The controller is administratively down when it has been manually shut down. You should restart the controller to correct this error.

Step 1 Enter enable mode.

```
maui-nas-03>en
Password:
maui-nas-03#
```

Step 2 Enter global configuration mode.

```
maui-nas-03#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#
```

Step 3 Enter controller configuration mode.

```
maui-nas-03(config)#controller t1 0
maui-nas-03(config-controller)#
```

Step 4 Restart the controller.

```
maui-nas-03(config-controlle)#shutdown  
maui-nas-03(config-controlle)#no shutdown
```

Is the Line Up?

If the T1 controller and line are not up, check to see if you are seeing one of the following messages in the **show controller t1** exec output:

Receiver has loss of frame.

or

Receiver has loss of signal.

If Receiver Has Loss of Frame

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. You can check the framing format of the controller from the running configuration or the **show controller t1** command output.

To change the framing format, use the **framing {SF | ESF}** command in the controller configuration mode, as shown here:

```
maui-nas-03#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
  
maui-nas-03(config)#controller t1 0  
maui-nas-03(config-controlle)#framing esf
```

Step 2 Try the other framing format to see if the alarm clears.

Step 3 Change the line build out setting using the **cablelength {long | short}** command.

Line build out (LBO) compensates for the loss in decibels based on the distance from the device to the first repeater in the circuit. A longer distance from the device to the repeater requires that the signal strength on the circuit be boosted to compensate for loss over that distance.

To configure transmit and receive levels for a cable length (line build out) longer than 655 feet for a T1 trunk with a channel service unit (CSU) interface, use the **cablelength long** controller configuration command. To configure transmit attenuation for a cable length (line build out) of 655 feet or shorter for a T1 trunk with a DSX-1 interface, use the **cablelength short** controller configuration command.

Consult your service provider and the Cisco IOS command reference for details on buildout settings.

If this does not fix the problem, proceed to the next section.

If Receiver Has Loss of Signal

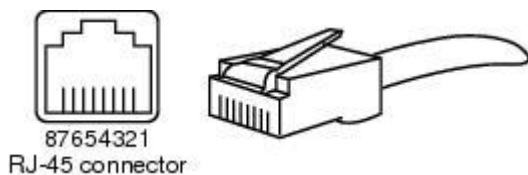
Step 1 Make sure that the cable between the interface port and the T1 service provider's equipment or T1 terminal equipment is connected correctly. Check to see if the cable is hooked up to the correct ports. Correct the cable connections, if necessary.

Step 2 Check cable integrity. Look for breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. If necessary, replace the cable.

Step 3 Check the cable connectors. A reversal of the transmit and receive pairs or an open receive pair can cause errors. Set the receive pair to lines 1 and 2; the transmit pair should be lines 4 and 5.

The pins on an RJ-48 jack are numbered from 1 through 8. Pin 1 is the leftmost pin when looking at the jack with the metal pins facing you. Refer to Figure 15-11.

Figure 15-11 RJ-45 Cable



Step 4 Try using a rollover cable.

Run the **show controller t1** exec command after each step to see whether the controller exhibits any errors.

If the Line Is in Loopback Mode

Check to see whether the line is in loopback mode from the **show controller t1** output. A line should be in loopback mode only for testing purposes.

To turn off loopback, use the **no loopback** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#no loopback
```

If the Controller Displays Any Alarms

Check the **show controller** command output to see if there are alarms displayed by the controller.

We will now discuss various alarms and the procedure necessary to correct them.

Receive (RX) Alarm Indication Signal (AIS) (Blue)

A received alarm indication signal (AIS) means that an alarm is occurring on the line upstream of the equipment connected to the port. The AIS failure is declared when an AIS defect is detected at the input and still exists after the loss of frame failure is declared

(caused by the unframed nature of the "all-ones" signal). The AIS failure is cleared when the loss of frame failure is cleared.

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. If not, change the framing format on the controller to match that of the line.

Step 2 Contact your service provider to check for misconfiguration within the telco.

Receive (Rx) Remote Alarm Indication (Yellow)

A received remote alarm indication means that the far-end equipment has a problem with the signal that it is receiving from its upstream equipment.

For SF links, the far-end alarm failure is declared when bit 6 of all the channels has been zero for at least 335 ms. The failure is cleared when bit 6 of at least one channel is not zero for a period usually less than 1 second and always less than 5 seconds. The far-end alarm failure is not declared for SF links when a loss of signal is detected.

For ESF links, the far-end alarm failure is declared if the yellow alarm signal pattern occurs in at least seven out of ten contiguous 16-bit pattern intervals. The failure is cleared if the yellow alarm signal pattern does not occur in ten contiguous 16-bit signal pattern intervals.

Step 1 Insert an external loopback cable into the port. To create a loopback plug, refer to the section "Performing Hardware Loopback Plug Test," later in this chapter.

Step 2 Check to see if there are any alarms. If you do not see any alarms, then the local hardware is probably in good condition. In that case, do the following:

- Check the cabling. Refer to the section "If Receiver Has Loss of Signal" for more information.
- Check the settings at the remote end, and verify that they match your port settings.
- If the problem persists, contact your service provider.

Step 3 Remove the loopback plug, and reconnect your T1 line

Step 4 Check the cabling. Refer to the section "Loss of Signal" for more information.

Step 5 Power-cycle the router.

Step 6 Connect the T1 line to a different port. Configure the port with the same settings as that of the line. If the problem does not persist, then the fault lies with the one port:

- Reconnect the T1 line to the original port.
- Proceed to the "Troubleshooting Error Events" section, later in this chapter.

If the problem persists, then do the following:

- Perform a hardware loop test, as described in the section "Performing Hardware Loopback Plug Test."
- Replace the T1 controller card.
- Proceed to "Troubleshooting Error Events," the next section.

Transmitter Sending Remote Alarm (Red)

A red alarm is declared when the CSU cannot synchronize with the framing pattern on the T1 line.

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. If not, change the framing format on the controller to match that of the line.

Step 2 Check the settings at the remote end, and verify that they match your port settings.

Step 3 Contact your service provider.

Transmit (Tx) Remote Alarm Indication (Yellow)

A transmitted remote alarm indication at the interface indicates that the interface has a problem with the signal it is receiving from the far-end equipment.

Step 1 Check the settings at the remote end, and verify that they match your port settings.

Step 2 A Tx RAI should be accompanied by some other alarm that indicates the nature of the problem that the T1 port/card is having with the signal from the far-end equipment.

Troubleshoot that condition to resolve the Tx RAI.

Transmit (Tx) AIS (Blue)

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. If not, correct the mismatch.

Step 2 Power-cycle the router.

Step 3 Connect the T1 line to a different port. Configure the port with the same settings as that of the line.

If the problem persists, then do the following:

- Perform a hardware loop test, as described in the section "Performing a Hardware Loop Test."
- Replace the T1 controller card.
- Proceed to the "Troubleshooting Error Events" section, next.

Troubleshooting Error Events

The **show controller t1** exec command provides error messages that can be used to troubleshoot problems. We will now discuss several error messages and how to correct the errors.

To see whether the error counters are increasing, execute the **show controller t1** command repeatedly. Note the values of the counters for the current interval.

Consult your service provider for framing and linecoding settings. A good rule of thumb is to use B8ZS linecoding with ESF framing and AMI linecoding with SF framing.

Slip Secs Counter Is Increasing

The presence of slips on a T1 line indicates a clocking problem. The T1 provider (telco) will provide the clocking that the customer premises equipment (CPE) will need to synchronize to.

Step 1 Verify that the clock source is derived from the network. This can be ascertained by looking for "Clock Source Is Line Primary."

Note: If there are multiple T1s into an access server, only one can be the primary, while the other T1s derive the clock from the primary. In that case, verify that the T1 line designated as the primary clock source is configured correctly.

Step 2 Set the T1 clock source correctly from the controller configuration mode.

```
maui-nas-03(config-controller)#clock source line primary
```

Framing Loss Seconds Counter Is Increasing

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. You can check this by looking for "Framing is {ESF|SF}" in the show controller t1 output.

Step 2 To change the framing format, use the **framing {SF | ESF}** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#framing esf
```

Step 3 Change the line build out using the **cablelength {long | short}** command.

Consult your service provider and the Cisco IOS command reference for details on buildout settings.

Line Code Violations Are Increasing

Step 1 Check to see whether the linecoding configured on the port matches the framing format of the line. You can check this by looking for "Line Code is {B8ZS|AMI}" in the **show controller t1** output.

Step 2 To change the linecoding, use the **linecode {ami | b8zs}** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#linecode b8zs
```

Step 3 Change the line build out using the **cablelength {long | short}** command.

Consult your service provider and the Cisco IOS command reference for details on buildout settings.

Verify that isdn switchtype and pri-group Are Configured Correctly

Use the **show running-config** command to check if isdn switchtype and pri-group timeslots are configured correctly. Contact your service provider for correct values.

To change the isdn switchtype and pri-group, enter these lines:

```
maui-nas-03#configure terminal
```

```
maui-nas-03(config)#isdn switch-type primary-5ess
```

```
maui-nas-03(config)#controller t1 0
```

```
maui-nas-03(config-controller)#pri-group timeslots 1-24
```

Verifying the Signaling Channel

If the error counters do not increase but the problem persists, verify that the signaling channel is up and configured correctly.

Step 1 Run the **show interface serial x:23** command, where x should be replaced by the interface number.

Step 2 Check to see if the interface is up. If the interface is not up, use the **no shutdown** command to bring the interface up.

```
maui-nas-03#config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
maui-nas-03(config)#interface serial 0:23
```

```
maui-nas-03(config-if)#no shutdown
```


Step 3 Ensure that encapsulation is PPP. If the interface is not using PPP, then use the **encapsulation ppp** command in the interface configuration mode to correct it.

```
maui-nas-03(config-if)#encapsulation ppp
```

Step 4 Check to see whether loopback is set. Loopback should be set only for testing purposes. Use the **no loopback** command to remove loopbacks.

```
maui-nas-03(config-if)#no loopback
```

Step 5 Power-cycle the router.

Step 6 If the problem persists, contact your service provider or Cisco TAC.

Troubleshooting a PRI

Whenever troubleshooting a PRI, you need to check whether the T1 is running cleanly on both ends. If Layer 1 problems have been resolved, as described previously, we must look to Layer 2 and 3 problems.

Troubleshooting Using the show isdn status Command

The **show isdn status** command is used to display a snapshot of all ISDN interfaces. It displays the status of Layers 1, 2, and 3.

Step 1 Verify that Layer 1 is active.

The Layer 1 status should always say ACTIVE unless the T1 is down.

If **show isdn status** indicates that Layer 1 is DEACTIVATED, then there is a problem with the physical connectivity on the T1 line. Refer to the previous section "Is the Controller Administratively Down?"

Also verify that the T1 is not administratively down. Use the **no shutdown** command to bring up the T1 controller.

Step 2 Check whether Layer 2 state is MULTIPLE_FRAME_ESTABLISHED.

The desired Layer 2 State is MULTIPLE_FRAME_ESTABLISHED, which indicates that we are exchanging Layer 2 frames and have finished Layer 2 initialization.

If Layer 2 is not MULTIPLE_FRAME_ESTABLISHED, use the **show controller t1 exec** command to diagnose the problem. Refer to the section "Troubleshooting Using the show controller t1 Command."

Because **show isdn status** is a snapshot of the current status, it is possible that Layer 2 is bouncing up and down despite indicating MULTIPLE_FRAME_ESTABLISHED. Use **debug isdn q921** to verify that Layer 2 is stable.

Using debug q921

The **debug isdn q921** command displays data link layer (Layer 2) access procedures that are taking place at the router on the D-channel.

Ensure that you are configured to view **debug** messages by using the logging console or terminal monitor command as necessary.

Note In a production environment, verify that console logging is disabled. Enter the **show logging** command. If logging is enabled, the access server might intermittently freeze up as soon as the console port gets overloaded with log messages. Enter the **no logging** console command.

Note If **debug isdn q921** is turned on and you do not receive any **debug** outputs, place a call or reset the controller to get **debug** outputs.

Step 1 Verify that Layer 2 is stable. You should observe the **debug** outputs for messages indicating that the service is not bouncing up and down. If you see the following types of debug outputs, the line is not stable:

```
Mar 20 10:06:07.882: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:23, TEI 0
changed
to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:23, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected
as
clock source
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:23, TEI 0 changed
to
up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller T1 0, changed state to
up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:23, changed state to up
```

If Layer 2 does not appear to be stable, refer to the section "Troubleshooting Error Events."

Step 2 Verify that you are seeing only SAPI messages in both transmit (TX) and receive (RX) sides.

```
Mar 20 10:06:52.505: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:23: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
```

Step 3 Verify that you are not seeing SABME messages, which indicates that Layer 2 is trying to reinitialize. This is usually seen when we are transmitting poll requests (RRp) and not getting a response from the switch (RRf), or vice versa. The following are example of SABME messages:

```
Mar 20 10:06:21.702: ISDN Se0:23: RX <- SABMEp sapi = 0 tei = 0
Mar 20 10:06:22.494: ISDN Se0:23: TX -> SABMEp sapi = 0 tei = 0
```

If you are seeing SABME messages, do the following:

- Use the **show running-config** command to check whether **isdn switchtype** and **pri-group timeslots** are configured correctly. Contact your service provider for correct values.
- To change the **isdn switchtype** and **pri-group**, enter these lines:

```
maui-nas-03#configure terminal
maui-nas-03(config)#isdn switch-type primary-5ess
maui-nas-03(config)#controller t1 0
maui-nas-03(config-controller)#pri-group timeslots 1-24
```

Step 4 Verify that the D-channel is up using the **show interfaces serial x:23** command.

If the D-channel is not up, then use **no shutdown** command to bring it up:

```
maui-nas-03(config)#interface serial 0:23
maui-nas-03(config-if)#no shutdown
```

Step 5 Check to see whether encapsulation is PPP. If not, use the **encapsulation ppp** command to set encapsulation.

```
maui-nas-03(config-if)#encapsulation ppp
```

Step 6 Check to see whether the interface is in loopback mode. For normal operation, the interface should not be in loopback mode.

```
maui-nas-03(config-if)#no loopback
```

Step 7 Power-cycle the router.

Step 8 If the problem persists, contact your service provider or Cisco TAC.

Performing Hardware Loopback Plug Test

The hardware loopback plug test can be used to test whether the router has any faults. If a router passes a hardware loopback plug test, then the problem exists elsewhere on the line.

To create a loopback plug, follow these steps:

Step 1 Use wire cutters to cut a working RJ-45 or RJ-48 cable so that there are 5 inches of cable and the connector attached to it.

Step 2 Strip the wires.

Step 3 Twist the wires from pins 1 and 4 together.

Step 4 Twist the wires from pins 2 and 5 together.

Leave the rest of the wires alone.

The pins on an RJ-45/48 jack are numbered from 1 through 8. Pin 1 is the left-most pin when looking at the jack with the metal pins facing you.

Performing the Loopback Plug Test

Step 1 Insert the plug into the T1 port in question.

Step 2 Save your router configuration using the **write memory** command.

```
maui-nas-03#write memory
Building configuration...
[OK]
```

Step 3 Set the encapsulation to HDLC.

```
maui-nas-03#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#interface serial 0
maui-nas-03(config-if)#enc
maui-nas-03(config-if)#encapsulation HDLC
maui-nas-03(config-if)#^Z
```

Step 4 Use the **show running-config** command to check whether the interface has an IP address.

If the interface does not have an IP address, obtain a unique address and assign it to the interface with a subnet mask of 255.255.255.0

```
maui-nas-03(config)#ip address 172.22.53.1 255.255.255.0
```

Step 5 Clear the interface counters using the **clear counters** command.

```
maui-nas-03#clear counters
Clear "show interface" counters on all interfaces [confirm]
maui-nas-03#
```

Step 6 Perform the extended **ping** test as described in the "Using Extended ping Tests" section, earlier in this chapter.

Troubleshooting E1 Problems

This section describes the techniques and procedures to troubleshoot E1 circuits for dial-in customers.

Troubleshooting Using the **show controller e1** Command

The **show e1 controller** exec command provides information to logically troubleshoot physical layer and data link layer problems. This section describes how to logically troubleshoot using the **show controller e1** command.

This command displays the controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

The NPM or MIP can query the port adapters to determine their current status. Issue a **show controller e1** command to display statistics about the E1 link.

If you specify a slot and port number, statistics for each 15-minute period will be displayed.

Most E1 errors are caused by misconfigured lines. Ensure that linecoding, framing, clock source, and line termination (balanced or unbalanced) are configured according to what the service provider recommended.

Show controller e1 Conditions

The E1 controller can be in three states:

- Administratively down
- Down
- Up

Is the Controller Administratively Down?

The controller is administratively down when it has been manually shut down. You should restart the controller to correct this error.

Step 1 Enter enable mode.

```
maui-nas-03>en
Password:
maui-nas-03#
```

Step 2 Enter global configuration mode.

```
maui-nas-03#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#
```

Step 3 Enter controller configuration mode.

```
maui-nas-03(config)#controller e1 0
maui-nas-03(config-controller)#
```

Step 4 Restart the controller.

```
maui-nas-03(config-controller)#shutdown
maui-nas-03(config-controller)#no shutdown
```

Is the Line Up?

If the E1 line is not up, check to see that the line configuration is correct and matches the settings of the remote end.

Check the framing of the line and the remote end. For E1 lines, the framing is either CRC4 or noCRC4.

Check the linecoding of the line and the remote end. The linecoding is either AMI or HDB3.

Check whether the line termination is set for balanced or unbalanced (75 ohm or 120 ohm).

Consult your service provider for more information regarding the correct settings. Make any changes as necessary to both local or remote end devices.

If the E1 controller and line are not up, check to see whether you are seeing one of the following messages in the **show controller e1** exec output:

Receiver has loss of frame.

or

Receiver has loss of signal.

If Receiver Has Loss of Frame

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. You can check the framing format of the controller from the running configuration or the **show controller e1** command output.

To change the framing format, use the **framing {CRC4 | no CRC4}** command in the controller configuration mode, as shown here:

```
maui-nas-03#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
maui-nas-03(config)#controller E1 0  
maui-nas-03(config-controller)#framing CRC4
```

Step 2 Try the other framing format to see if the alarm clears.

If this does not fix the problem, proceed to the receiver has loss of signal section below.

Step 3 Check the framing format on the remote end.

Step 4 Check the linecoding on the remote end.

If Receiver Has Loss of Signal

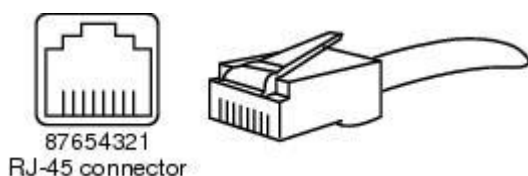
Step 1 Make sure that the cable between the interface port and the E1 service provider's equipment or E1 terminal equipment is connected correctly. Check to see whether the cable is hooked up to the correct ports. Correct the cable connections if necessary.

Step 2 Check cable integrity. Look for breaks or other physical abnormalities in the cable. Ensure that the pinouts are set correctly. If necessary, replace the cable.

Step 3 Check the cable connectors. A reversal of the transmit and receive pairs or an open receive pair can cause errors. Set the receive pair to lines 1 and 2; the transmit pair should be lines 4 and 5.

The pins on a RJ-48 jack are numbered from 1 through 8. Pin 1 is the leftmost pin when looking at the jack with the metal pins facing you. Refer to Figure 15-12 for more information.

Figure 15-12 RJ-45 Cable



Step 4 Try using a rollover cable.

Step 5 Check to see whether there are far-end block errors. If so, the problem exists with the receive lead on the local end. Contact TAC for more assistance.

Run the **show controller e1** exec command after each step to check whether the controller exhibits any errors.

If the Line Is in Loopback Mode

Check to see whether the line is in loopback mode from the **show controller e1** output. A line should be in loopback mode only for testing purposes.

To turn off loopback, use the **no loopback** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#no loopback
```

If the Controller Displays Any Alarms

Check the **show controller** command output to see whether any alarms are displayed by the controller.

We will now discuss various alarms and the procedure necessary to correct them.

Receiver (Rx) Has Remote Alarm

A received remote alarm means that an alarm is occurring on the line upstream of the equipment connected to the port.

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. If not, change the framing format on the controller to match that of the line.

Step 2 Check the linecoding setting on the remote-end equipment. Contact your service provider for the correct settings. Correct any misconfigurations, as necessary.

Step 3 Insert an external loopback cable into the port. To create a loopback plug, refer to the section "Performing Hardware Loopback Plug Test," earlier in the chapter.

Step 4 Check to see whether there are any alarms. If you do not see any alarms, then the local hardware is probably in good condition. In that case, do the following:

- Check the cabling. Refer to the section "Loss of Signal" for more information.
- Check the settings at the remote end, and verify that they match your port settings.
- If the problem persists, contact your service provider.

Step 5 Remove the loopback plug and reconnect your E1 line.

Step 6 Check the cabling. Refer to the section "Loss of Signal" for more information.

Step 7 Power-cycle the router.

Step 8 Connect the E1 line to a different port. Configure the port with the same settings as that of the line. If the problem does not persist, then the fault lies with the port:

- Reconnect the E1 line to the original port.
- Proceed to the "Troubleshooting E1 Error Events" section.

If the problem persists, then do the following:

- Perform a hardware loop test, as described in the section "Performing a Hardware Loop Test,"
- Replace the E1 controller card.
- Proceed to the "Troubleshooting E1 Error Events" section.

Transmitter Sending Remote Alarm (Red)

A red alarm is declared when the CSU cannot synchronize with the framing pattern on the E1 line.

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. If not, change the framing format on the controller to match that of the line.

Step 2 Check the settings at the remote end, and verify that they match your port settings.

Step 3 Insert an external loopback cable into the port. To create a loopback plug, refer to the section "Performing Hardware Loopback Plug Test," earlier in the chapter.

Step 4 Check to see whether there are any alarms. If you do not see any alarms, then the local hardware is probably in good condition. In that case, do the following:

- Check the cabling. Refer to the section "Loss of Signal" for more information.
- If the problem persists, contact your service provider.

Step 5 Connect the E1 line to a different port. Configure the port with the same settings as that of the line. If the problem does not persist, then the fault lies with the port:

- Reconnect the E1 line to the original port.
- Proceed to the "Troubleshooting E1 Error Events" section.

If the problem persists, then do the following:

- Perform a hardware loop test, as described in the section "Performing a Hardware Loop Test."
- Replace the E1 controller card.
- Proceed to the "Troubleshooting E1 Error Events" section.
- Contact your service provider.

Troubleshooting E1 Error Events

The **show controller e1** exec command provides error messages that can be used to troubleshoot problems. We will now discuss several error messages and how to correct the errors.

To see whether the error counters are increasing, execute the **show controller e1** command repeatedly. Note the values of the counters for the current interval.

Consult your service provider for framing and linecoding settings.

Slip Secs Counter Is Increasing

The presence of slips on E1 lines indicates a clocking problem. The E1 provider (telco) will provide the clocking that the customer premises equipment (CPE) will need to synchronize to.

Step 1 Verify that the clock source is derived from the network. This can be ascertained by looking for "Clock Source is Line Primary."

Note If there are multiple E1s into an access server, only one can be the primary, while the other E1s derive the clock from the primary. In that case, verify that the E1 line designated as the primary clock source is configured correctly.

Step 2 Set the E1 clock source correctly from the controller configuration mode.

```
maui-nas-03(config-controller)#clock source line primary
```

Framing Loss Seconds Counter Is Increasing

Step 1 Check to see whether the framing format configured on the port matches the framing format of the line. You can check this by looking for "Framing is {CRC4|no CRC4}" in the **show controller e1** output.

Step 2 To change the framing format, use the **framing {CRC4 | no CRC4}** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#framing crc4
```

Line Code Violations Are Increasing

Step 1 Check to see whether the linecoding configured on the port matches the framing format of the line. You can check this by looking for "Line Code is {AMI/HDB3}" in the **show controller e1** output.

Step 2 To change the linecoding, use the **linecode {ami | hdb3}** command in the controller configuration mode, as shown here:

```
maui-nas-03(config-controller)#linecode ami
```

Verifying That isdn switchtype and pri-group Are Configured Correctly

Use the **show running-config** command to check whether **isdn switchtype** and **pri-group timeslots** are configured correctly. Contact your service provider for correct values.

To change the **isdn switchtype** and **pri-group**, use these lines:

```
maui-nas-03#configure terminal
```

```
maui-nas-03(config)#isdn switch-type primary-net5
```

```
maui-nas-03(config)#controller e1 0
```

```
maui-nas-03(config-controller)#pri-group timeslots 1-31
```

Verifying the Signaling Channel

If the error counters do not increase but the problem persists, verify that the signaling channel is up and configured correctly.

Step 1 Run the **show interface serial x:15** command, where x should be replaced by the interface number.

Step 2 Check to see whether the interface is up. If the interface is not up, use the **no shutdown** command to bring up the interface.

```
maui-nas-03#config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
maui-nas-03(config)#interface serial 0:15
```

```
maui-nas-03(config-if)#no shutdown
```

Step 3 Ensure that encapsulation is PPP. If the interface is not using PPP, then use the **encapsulation ppp** command in the interface configuration mode to correct it.

```
maui-nas-03(config-if)#encapsulation ppp
```

Step 4 Check to see whether loopback is set. Loopback should be set only for testing purposes. Use the **no loopback** command to remove loopbacks.

```
maui-nas-03(config-if)#no loopback
```

Step 5 Power-cycle the router.

Step 6 If the problem persists, contact your service provider or Cisco TAC.

Troubleshooting a PRI

Whenever troubleshooting a PRI, you need to check whether the E1 is running cleanly on both ends. If Layer 1 problems have been resolved, as described previously, we must look to Layer 2 and 3 problems.

Troubleshooting Using the **show isdn status** Command

The **show isdn status** command is used to display a snapshot of all ISDN interfaces. It displays the status of Layers 1, 2, and 3.

Step 1 Verify that Layer 1 is active.

The Layer 1 status should always say ACTIVE unless the E1 is down.

If **show isdn status** indicates that Layer 1 is DEACTIVATED, then there is a problem with the physical connectivity on the E1 line. Refer to the section "Is the Controller Administratively Down?"

Also verify that the E1 is not administratively down. Use the **no shutdown** command to bring up the E1 controller.

Step 2 Check whether Layer 2 state is MULTIPLE_FRAME_ESTABLISHED.

The desired Layer 2 state is MULTIPLE_FRAME_ESTABLISHED, which indicates that the startup protocol between ISDN switch and end device has been established and that we are exchanging Layer 2 frames.

If Layer 2 is not MULTIPLE_FRAME_ESTABLISHED, use the **show controller E1** exec command to diagnose the problem. Refer to the previous section "Troubleshooting Using the show controller e1 Command," and the upcoming section "Troubleshooting E1 Error Events."

Because **show isdn status** is a snapshot of the current status, it is possible that Layer 2 is bouncing up and down despite indicating Multiple_Frame_Established. Use **debug isdn q921** to verify that Layer 2 is stable.

Using **debug q921**

The **debug isdn q921** command displays data link layer (Layer 2) access procedures that are taking place at the router on the D-channel.

Ensure that you are configured to view **debug** messages by using the **logging console** or **terminal monitor** commands, as necessary.

Note In a production environment, verify that console logging is disabled. Enter the **show logging** command. If logging is enabled, the access server might intermittently freeze up as soon as the console port gets overloaded with log messages. Enter the **no logging** console command.

Note If **debug isdn q921** is turned on and you do not receive any **debug** outputs, place a call or reset the controller to get **debug** outputs.

Step 1 Verify that Layer 2 is stable. You should observe the **debug** outputs for messages indicating that the service is not bouncing up and down. If you see the following types of **debug** outputs, the line is not stable:

```
Mar 20 10:06:07.882: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:15, TEI 0
changed
to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:15, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected
as
clock source
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:15, TEI 0 changed
to
up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller E1 0, changed state to
up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:15, changed state to up
```

If Layer 2 does not appear to be stable refer to the "Troubleshooting Error Events" section, earlier in this chapter.

Step 2 Verify that you are seeing only SAPI messages in both transmit (TX) and receive (RX) sides.

```
Mar 20 10:06:52.505: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:15: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0
```

Step 3 Verify that you are not seeing SABME messages, which indicates that Layer 2 is trying to reinitialize. This is usually seen when we are transmitting poll requests (RRp) and not getting a response from the switch (RRf), or vice versa. The following are examples of SABME messages. We should get a response from ISDN switch for our SABME messages (UA frame received):

```
Mar 20 10:06:21.702: ISDN Se0:15: RX <- SABMEp sapi = 0 tei = 0
Mar 20 10:06:22.494: ISDN Se0:15: TX -> SABMEp sapi = 0 tei = 0
```

If you are seeing SABME messages, do the following:

- Use the **show running-config** command to check whether **isdn switchtype** and **pri-group timeslots** are configured correctly. Contact your service provider for correct values.
- To change the **isdn switchtype** and **pri-group**, use these lines:

```
maui-nas-03#configure terminal
maui-nas-03(config)#isdn switch-type primary-net5
maui-nas-03(config)#controller e1 0
maui-nas-03(config-controller)#pri-group timeslots 1-31
```

Step 4 Verify that the D-channel is up using the **show interfaces serial x:15** command.

If the D-channel is not up, then use **no shutdown** command to bring it up:

```
maui-nas-03(config)#interface serial 0:15
maui-nas-03(config-if)#no shutdown
```

Step 5 Check to see whether encapsulation is PPP. If not, use the **encapsulation ppp** command to set encapsulation.

```
maui-nas-03(config-if)#encapsulation ppp
```

Step 6 Check to see whether the interface is in loopback mode. For normal operation, the interface should not be in loopback mode.

```
maui-nas-03(config-if)#no loopback
```

Step 7 Power-cycle the router.

Step 8 If the problem persists, contact your service provider or Cisco TAC.