

Troubleshooting Guide

Troubleshooting Layer 2 Protocols over T1 Using the CLI

Troubleshooting network systems has grown more difficult as new, and more complex, technologies have been introduced. This troubleshooting guide provides insight into breaking these complex systems down into manageable pieces. Each individual piece becomes much easier to troubleshoot. This guide provides the tools for troubleshooting problems with the T1 circuit as well as the layer 2 protocol of the data riding on the T1, such as Point-to-Point Protocol (PPP) and Frame Relay using the AOS Command Line Interface (CLI).

This guide consists of the following sections:

- *T1 Technology Overview* on page 2
- *Troubleshooting T1 Interfaces* on page 5
- *Troubleshooting TDM Groups* on page 11
- *PPP Technology Overview* on page 13
- *Troubleshooting PPP Connections* on page 15
- *Frame Relay Technology Overview* on page 19
- *Troubleshooting Frame Relay Connections* on page 21
- *Appendix A* on page 25
- *Appendix B* on page 27

T1 Technology Overview

A T1 circuit is comprised of 24, eight-bit channels often referred to as timeslots or DS0s. Each DS0 is sampled 8000 times per second (8 kHz sampling) to provide a theoretical bandwidth of 64 kbps per DS0.

$$8 \text{ bits} \times 8000 \text{ samples per second} = 64,000 \text{ bits per second (64 kbps)}$$

T1 bandwidth is calculated by multiplying the 24 channels times the individual DS0 bandwidth (64 kbps). The resulting theoretical data bandwidth for the T1 is 1.536 Mbps.

$$24 \text{ DS0s} \times 64 \text{ kbps} = 1536 \text{ kbps (1.536 Mbps)}$$

In addition to data bandwidth, each T1 frame begins with a single framing bit for frame alignment (see Figure 1). The framing bit adds 8 kbps of overhead to the T1 giving a final data rate of 1.544 Mbps.

$$(1 \text{ frame bit} \times 8000 \text{ bps}) + 1.536 \text{ Mbps} = 1.544 \text{ Mbps}$$

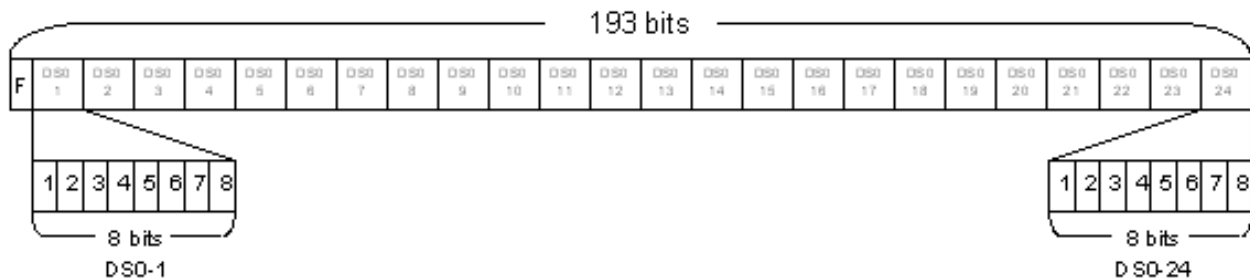


Figure 1. T1 Frame

T1 Interface Types

There are two types of T1 interfaces: DS1 and DSX (or DSX-1). Each interface type has an industry standard for transmission distance, receiver sensitivity, and interface pinout. DS1 interfaces are typically found on customer premises equipment (CPE) such as CSU/DSUs. DS1 interfaces have a maximum distance of 6000 feet, 3000 feet if a physical loop exists on the circuit. The receiver sensitivity is measured in millivolts. DS1 interfaces are supplied using an RJ-45 or RJ-48 (8-conductor) connector. Table 1 provides the DS1 interface pinout.

Table 1. DS1 Interface Pinout

Pin	Description
1	Receive Ring
2	Receive Tip
3	Unused
4	Transmit Ring
5	Transmit Tip
6-8	Unused

DSX interfaces are found on telco network interface unit (NIU)/Smart Jack interfaces (the connection to the T1 network provided by the network supplier) and on T1 devices designed specifically for connection to other T1 CPE equipment (like the T1/T1 + DSX-1 network interface module). The most common application for a DSX interface on CPE equipment is for connection to a phone system (PBX). DSX interfaces have a maximum distance of 655 feet. The receiver sensitivity is measured in volts. Just like DS1 interfaces, DSX interfaces are supplied using an RJ-45 or RJ-48 (8-conductor) connector, but the transmit and receive pairs are reversed. Table 1 provides the DSX interface pinout.

Table 2. DSX Interface Pinout

Pin	Description
1	Transmit Ring
2	Transmit Tip
3	Unused
4	Receive Ring
5	Receive Tip
6-8	Unused

Clocking

T1 is a synchronous technology, allowing one timing source on any single T1. All other T1 equipment must be configured to reference the same clock source. If multiple clock sources are present, or alternatively, if no clock source is present, the T1 will take errors in the form of clock slips, frame slips, or TDM group errors. Eventually, the T1 will lose synchronization altogether.

T1 equipment uses binary ones and zeros to transmit data. Binary ones are represented by a positive or negative 3 volts and binary zeros are represented by 0 volts (or the absence of voltage). Binary ones are used to maintain clock synchronization and if too many zeros are present in the datastream, the T1 equipment will lose synchronization and the T1 interface will go down. To avoid this, T1 data must contain a certain percentage of binary ones (the ones density rule). For T1 interfaces, the ones density rule states that 12.5 percent of data on the T1 must be binary ones. T1 line coding methods must compensate for data that does not meet the ones density rule specifications (refer to *Line Coding* on page 4 for more details).

Framing

T1 circuits use two types of framing: Extended Super Frame (ESF) and Super Frame (SF or D4). These framing formats provide the mechanism for equipment to distinguish between the individual DS0s and allocate additional overhead for error checking, alarm reporting, etc. The two framing formats are not compatible with one another. All equipment connected to the T1 circuit must be configured for the same framing format. A mismatch in framing format will produce a Red alarm.

Extended Super Frame (ESF)

ESF framing is more prevalent in the T1 network world. ESF framing uses framing bits to provide a facility data link (FDL), an out-of-band channel to use for alarm reporting or administration (such as loopbacks, testing, etc.). ESF framing is comprised of 24 T1 frames each containing a framing bit (see Figure 2). The framing bits are used for frame alignment (6 bits), the FDL (12 bits), and error checking (6 bits). Error checking is accomplished through Cyclic Redundancy Check-6 (CRC-6). CRC-6 checks data integrity by using the entire frame to calculate a CRC result. The receiver receives the frame and

calculates a CRC result and compares the result with the received result. This allows the receiver to ensure that there were no bit errors in the transmission of the frame.



Figure 2. ESF Frame

Super Frame (SF or D4)

SF (often referred to as D4) framing is comprised of 12 T1 frames each containing a framing bit. The 12 framing bits transmit a pattern of 1000 1101 1100 to aid in frame alignment in the T1 equipment. No additional features (such as the FDL or error checking) are provided using SF framing.

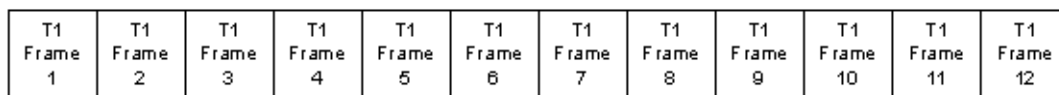


Figure 3. SF (D4) Frame

Line Coding

T1 line coding formats are fundamental for providing binary ones and zeros on the physical T1 medium as well as ensuring that undesirable conditions (such as a long string of zeros) do not cause transmission interruption. There are two T1 line coding methods: Alternate Mark Inversion (AMI) and Bipolar Eight Zero Substitution (B8ZS). The two line coding methods are not compatible with one another. A mismatch in line coding causes alarm conditions on the T1.

Alternate Mark Inversion (AMI)

AMI states that binary ones are represented by alternating polarity between +3 volts and -3 volts. The alternating polarity prevents the T1 signal from building a DC voltage on the physical line. This allows for a DC voltage to be applied on the T1 to power equipment (such as T1 repeaters). In addition, the alternating polarity provides a mechanism for error detection. Binary zeros are represented by the absence of voltage. AMI does not offer a solution for maintaining ones density across the network.

Figure 4 shows an example of AMI line coding.

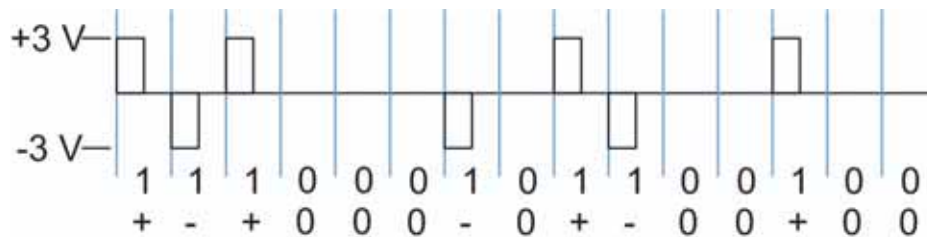


Figure 4. AMI Line Coding

AMI line coding provides error detection by checking for alternating polarities on sequential local ones in the transmission. When the polarities on two sequential logical ones are not reversed, a bipolar violation (BPV) is recorded. Figure 5 shows an example of an AMI BPV.

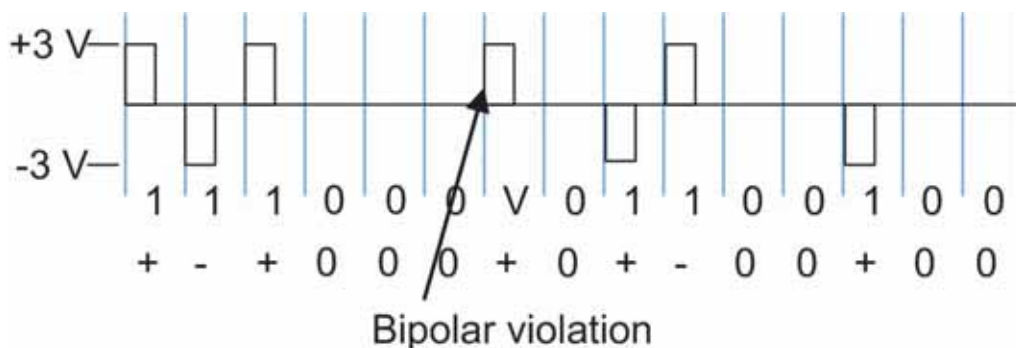


Figure 5. AMI Bipolar Violation

Bipolar Eight Zero Substitution (B8ZS)

Like AMI, B8ZS line coding also states that binary ones are represented by alternating polarity between +3 volts and -3 volts. Binary zeros are represented by the absence of voltage. B8ZS line coding maintains ones density by replacing eight consecutive zeros with a predetermined pattern of ones and zeros (00011011) that contain two bipolar violations. Error detection using the alternating polarities of binary ones is also available through B8ZS line coding. Invalid polarities between consecutive binary ones are recorded as BPVs. Figure 6 shows an example of B8ZS line coding. Bipolar violations are listed using a V in the example figure.

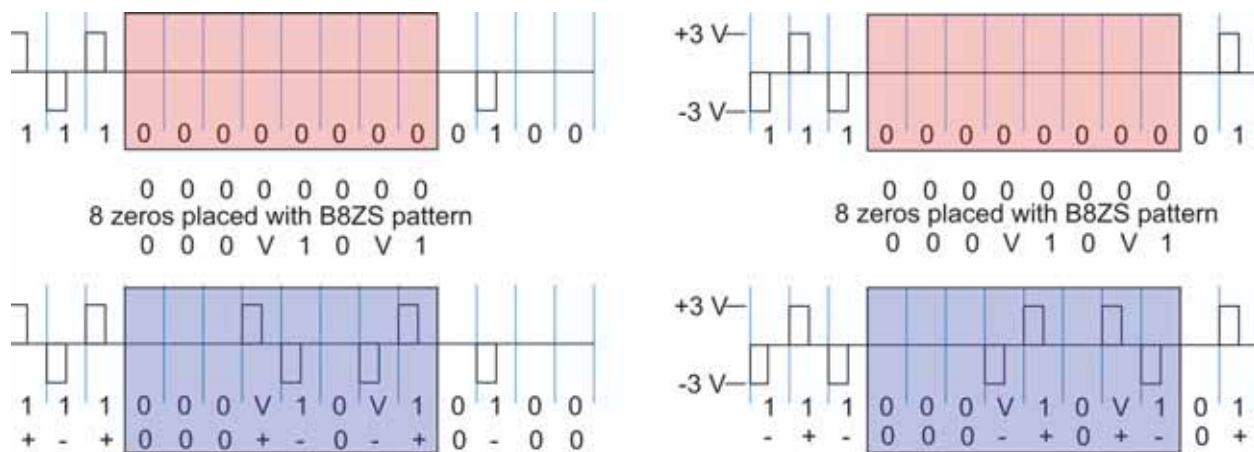


Figure 6. B8ZS Line Coding

Troubleshooting T1 Interfaces

The first step in troubleshooting a T1 problem is to check the T1 interface status using the **show interface t1 <slot/port>** command. AOS provides useful information for the T1 interface to help identify and correct problems. The following shows an example status printout for **show interface t1 1/1**. Critical information for troubleshooting is indicated with colored text and a brief description is provided.

#show interface t1 1/1

t1 1/1 is UP



T1 Physical Status indicates whether the physical T1 is UP or DOWN.

Description: Interface T1 1/1
 Receiver has no alarms
 T1 coding is B8ZS, framing is ESF
 Clock source is line, FDL type is ANSI
 Line build-out is 0dB
 No remote loopbacks, No network loopbacks
 Acceptance of remote loopback requests enabled
 Tx Alarm Enable: raid
 Last clearing of counters 00:00:01
 loss of frame: 0
 loss of signal: 0
 AIS alarm: 0
 Remote alarm: 0

DS0 Status: 123456789012345678901234
 NNNNNNNNNNNNNNNNNNNNNNNNNNNNN
 Status Legend: '-' = DS0 is unallocated
 'N' = DS0 is dedicated (nailed)

Line Status: -- No Alarms --



T1 Line Status displays current alarms (such as Red alarm, LOS, Blue alarm, etc.).

5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 Current Performance Statistics:
 0 Errored Seconds, 0 Bursty Errored Seconds
 0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
 0 Unavailable Seconds, 0 Path Code Violations
 0 Line Code Violations, 0 Controlled Slip Seconds
 0 Line Errored Seconds, 0 Degraded Minutes

TDM group 1, line protocol is UP



TDM Group Status displays information pertaining to the configured TDM group that is connected to the specified T1 interface.

Encapsulation PPP (ppp 1)
 0 packets input, 0 bytes, 0 no buffer
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame
 0 abort, 0 discards, 0 overruns
 0 packets output, 0 bytes, 0 underruns

!

Troubleshooting DOWN T1 Interfaces

If the **show interface t1 <slot/port>** command indicates that the T1 is DOWN, the next step is to check the line status (shown in **BLUE** in the following sample printout). The line status lists which alarm(s) are currently active for the T1. T1 alarms are used to help isolate where the issue lies on the T1 circuit. Several common alarm combinations and corrective actions are discussed in this section. Match the provided alarms to the status information for your T1 and follow the corrective action. Check the T1 interface line status after each corrective action until there are no alarms and the T1 is UP.

```
DS0 Status: 123456789012345678901234
           NNNNNNNNNNNNNNNNNNNNNNNNNNN
Status Legend: '.' = DS0 is unallocated
              'N' = DS0 is dedicated (nailed)

Line Status: ---- ACTIVE ALARMS (refer to the common alarm combinations below) ----
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
Current Performance Statistics:
  0 Errored Seconds, 0 Bursty Errored Seconds
  0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
  0 Unavailable Seconds, 0 Path Code Violations
  0 Line Code Violations, 0 Controlled Slip Seconds
  0 Line Errored Seconds, 0 Degraded Minutes
```

Line Status: LOS, Red, and Tx Yellow

Alarm Descriptions

- LOS** Loss of signal indicates that the unit is not receiving a T1 signal.
- Red** The received T1 signal is out of frame.
- Tx Yellow or RAI** The local unit transmits a Yellow or remote alarm indicator (RAI) alarm to the far-end unit indicating that there is a problem with the local receive path.

Network Failure Scenarios

Figure 7 and Figure 8 on page 8 illustrate possible network failures. T1 alarms are indicated above each unit. The red X signifies the location of a potential break in the line.

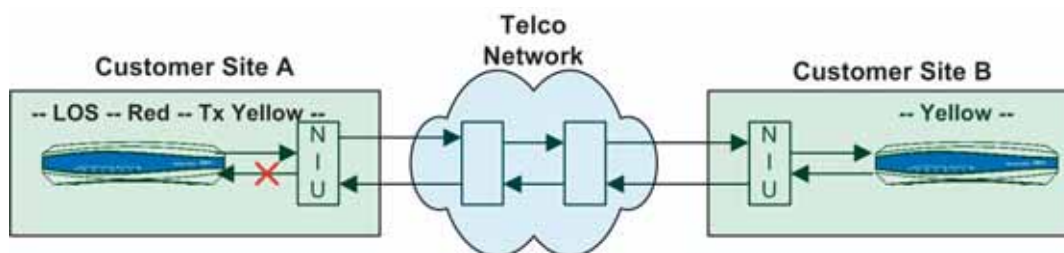


Figure 7. LOS, Red, and Tx Yellow (Scenario 1)

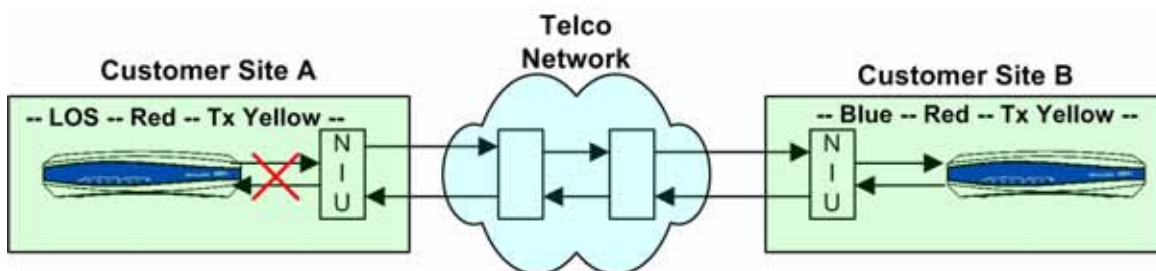


Figure 8. LOS, Red, and Tx Yellow (Scenario 2)

Corrective Action

1. Replace the T1 cable between the local unit and the Smart Jack (NIU).
2. Replace the T1 cable with a T1 cross-over cable. (Refer to *Appendix A* on page 25 for cross-over cable pinouts.)
3. Hard loop the unit’s T1 interface with a loopback plug. (Refer to *Appendix A* on page 25 for loopback plug pinouts.)
4. Call the T1 service provider and test with a loopback plug on the unit. (Refer to *Appendix B* on page 27 for instructions on troubleshooting with a loopback plug.)

Line Status: Red, Blue, and Tx Yellow

Alarm Descriptions

Blue or AIS Blue or alarm indication signal (AIS) alarm is sent by the telco equipment to maintain T1 timing as unframed ones.

Red The received T1 signal is out of frame.

Tx Yellow or RAI The local unit transmits a Yellow or remote alarm indicator (RAI) alarm to the far-end unit indicating that there is a problem with the local receive path.

Network Failure Scenarios

Figures 9 through 13 illustrate possible network failures. T1 alarms are indicated above each unit. The red X signifies the location of a potential break in the line.

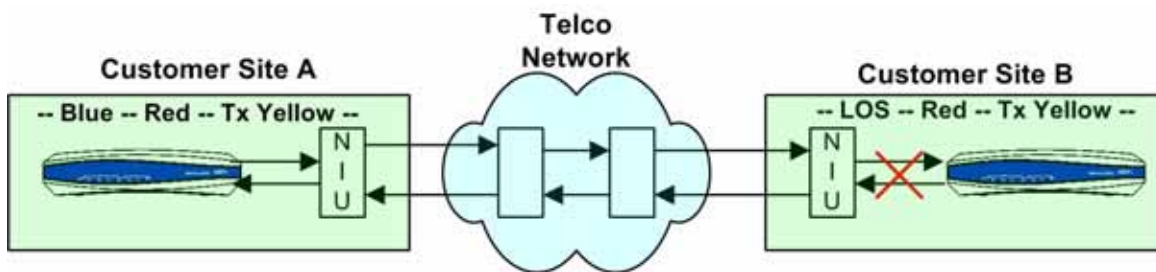


Figure 9. Red, Blue, and Tx Yellow (Scenario 1)

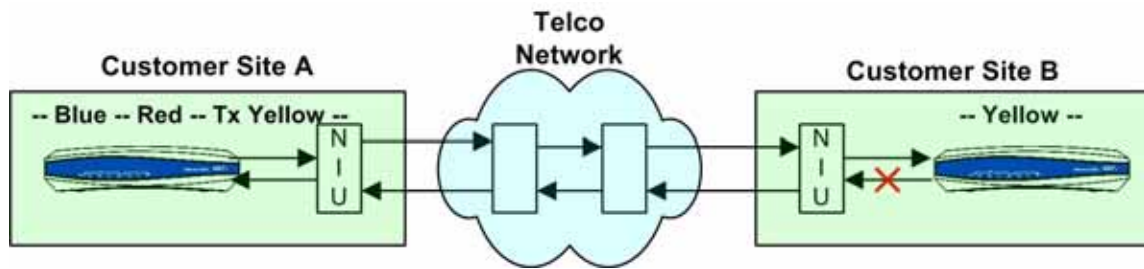


Figure 10. Red, Blue, and Tx Yellow (Scenario 2)

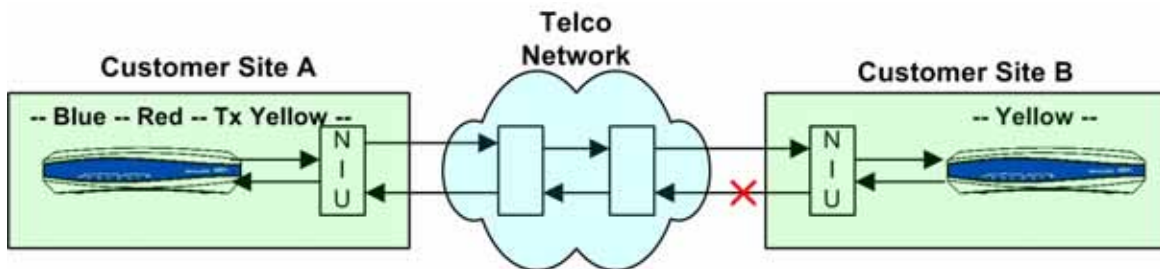


Figure 11. Red, Blue, and Tx Yellow (Scenario 3)

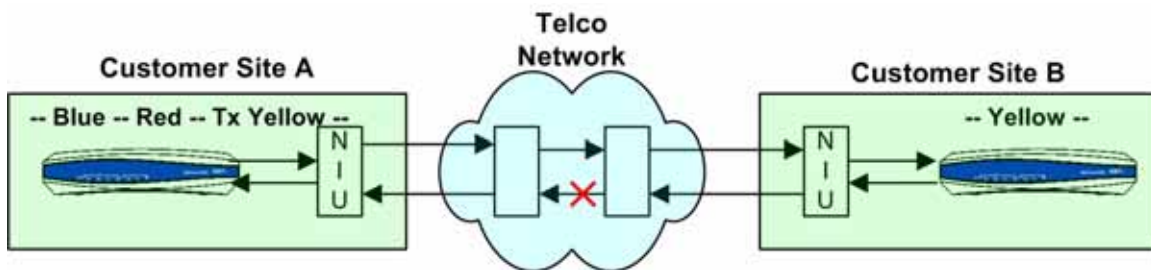


Figure 12. Red, Blue, and Tx Yellow (Scenario 4)

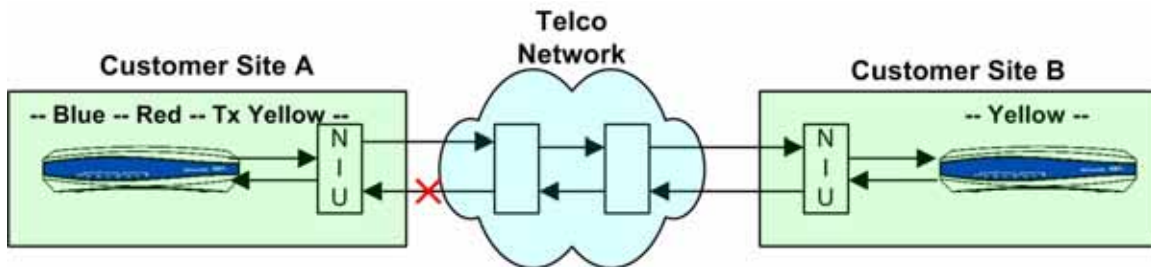


Figure 13. Red, Blue, and Tx Yellow (Scenario 5)

Corrective Action

1. Check the unit at Site B for alarms. If Site B is in LOS, troubleshoot accordingly.
2. Call the T1 service provider and inform them that the unit is receiving a Blue or AIS alarm.
3. Hard loop the unit’s T1 interface with a loopback plug. (Refer to *Appendix A* on page 25 for loopback plug pinouts.)
4. Call the T1 service provider and test with a loopback plug. (Refer to *Appendix B* on page 27 for instructions on troubleshooting with a loopback plug.)

Line Status: Red and Tx Yellow

Alarm Descriptions

Red The received T1 signal is out of frame. The NIU and the unit may have a framing mismatch.

Tx Yellow or RAI The local unit transmits a Yellow or RAI alarm to the far-end unit indicating that there is a problem with the local receive path. The remote unit could be in Blue alarm and also transmitting Yellow alarm.

Network Failure Scenarios

Figure 14 illustrates a possible network failure. T1 alarms are indicated above each unit.

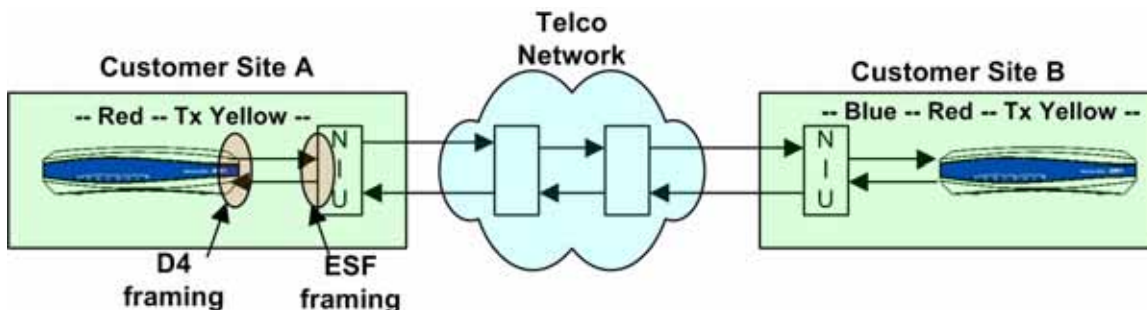


Figure 14. Red and Tx Yellow (Scenario 1)

Corrective Action

1. Verify that the unit’s T1 framing is set correctly for the T1 at this site.
2. Hard loop the unit’s T1 interface with a loopback plug. (Refer to *Appendix A* on page 25 for loopback plug pinouts.)
3. Call the T1 service provider and have them verify the T1 framing on the T1 circuit and that the telco equipment is properly configured.
4. Call the T1 service provider and test with a loopback plug on the unit. (Refer to *Appendix B* on page 27 for instructions on troubleshooting with a loopback plug.)

Line Status: Yellow Alarm

Alarm Descriptions

Tx Yellow or RAI The local unit transmits a Yellow or RAI alarm indicates there is an issue on the transmit path to the other site.

Network Failure Scenarios

Figure 15 illustrates a possible network failure. T1 alarms are indicated above each unit.

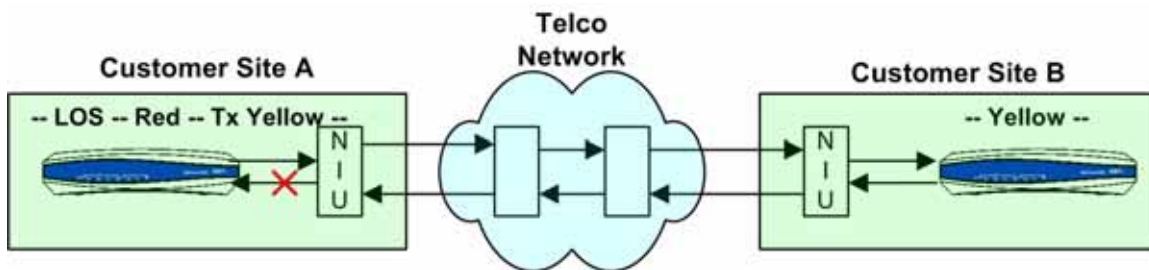


Figure 15. Yellow Alarm (Scenario 1)

Corrective Action

1. Check the unit at the remote site for alarms and troubleshoot accordingly.

Troubleshooting TDM Groups

The second step in troubleshooting a PPP or Frame Relay issue over T1 is to check the TDM group status using the **show interface t1 <slot/port>** command (shown in **PURPLE** in the following sample printout). The TDM group status lists pertinent information about the TDM group assigned to the T1 interface including the line protocol assigned to the group, the status of the protocol, and data statistics for the protocol. Several common TDM group status messages and their corresponding corrective actions are discussed in this section (see Table 3 on page 12). Match the example information to the status information for your TDM group and follow the applicable corrective action. These examples use encapsulation PPP, but encapsulation Frame Relay is also an option. Check the TDM group status after each corrective action until the TDM group is UP.

TDM group 1, line protocol is UP

```
Encapsulation PPP (ppp 1)
 0 packets input, 0 bytes, 0 no buffer
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame
 0 abort, 0 discards, 0 overruns
 0 packets output, 0 bytes, 0 underruns
```

Table 3. TDM Group Status Messages

TDM Group Status Message	Corrective Action
<p>No TDM group is listed</p> <p>A TDM group has NOT been configured on the T1 interface</p>	<p>Add a TDM group with the correct time slots to the T1 interface configuration. For example,</p> <pre>! interface t1 1/1 tdm-group 1 timeslots 1-24 speed 64 no shutdown !</pre>
<p>TDM group 1, line protocol is not set</p> <p>Encapsulation is not set</p>	<p>Check that the cross-connect command is entered with the correct information linking the PPP or Frame Relay interface to the T1 interface TDM group. For example,</p> <pre>! interface ppp 1 ip address 10.19.2.61 255.255.255.252 no shutdown cross-connect 1 t1 1/1 ppp 1 !</pre> <p>Or,</p> <pre>! interface fr 1 ip address 10.19.2.61 255.255.255.252 no shutdown cross-connect 1 t1 1/1 fr 1 !</pre>
<p>TDM group 1, line protocol is DOWN</p> <p>Encapsulation PPP (ppp x)</p> <p>or</p> <p>TDM group 1, line protocol is DOWN</p> <p>Encapsulation FRAME-RELAY IETF (fr x)</p>	<p>First, check the speed and time slots allocated in the TDM group on the T1 interface. Compare settings with T1 provisioning and with the peer device. For example,</p> <pre>! interface t1 1/1 tdm-group timeslots 1-24 speed 64 no shutdown !</pre> <p>Continue to <i>Troubleshooting PPP Connections</i> on page 15 for PPP troubleshooting or <i>Troubleshooting Frame Relay Connections</i> on page 21 for Frame Relay troubleshooting.</p>
<p>TDM group1, line protocol is UP</p> <p>Encapsulation PPP (ppp x)</p> <p>or</p> <p>TDM group 1, linen protocol is UP</p> <p>Encapsulation FRAME-RELAY IETF (fr x)</p>	<p>Layer 2 has been properly negotiated. Proceed to <i>Troubleshooting PPP Connections</i> on page 15 to verify the appropriate PPP protocols are open or <i>Troubleshooting Frame Relay Connections</i> on page 21 to verify active PVC status.</p>

PPP Technology Overview

PPP is a set of protocols (link management, authentication, and network control protocols) that allow routers to negotiate parameters to establish and maintain a connection. PPP protocol messages are exchanged between the peer routers that specify the preferred PPP parameters for each router. If the peer router accepts the information, the router responds by sending an acknowledgement. This request and acknowledgement exchange must be bidirectional for the protocol to properly negotiate. It is possible to have an instance when a peer router fails to successfully negotiate PPP parameters because it does not understand a protocol, does not like a parameter offered in a request, or is configured to refuse a particular PPP option. Special PPP messages exist to help identify these instances.

The entire PPP negotiation can be monitored to determine why a PPP link is not coming up and at which step the PPP negotiation is failing. PPP requires the peer routers to acknowledge (ACK) every request (REQ) before the negotiation is complete and the protocol is said to be OPEN.

Below are descriptions of protocols used for establishing and maintaining a PPP link.

Link Control Protocol (LCP)

LCP is a required protocol that negotiates the data transmission parameters between two peers to initially establish, configure, and test the PPP link. LCP negotiation must be successful for the PPP link process to continue. The LCP protocol contains the following information:

- Peer router identification. During the LCP process, a router either accepts or rejects the peer device as a valid or invalid peer.
- Magic number. The magic number is used to identify the presence of a loop.
- Maximum receive unit (MRU). The MRU specifies the maximum packet size that the interface is willing to accept.
- Maximum reconstruct receive unit (MRRU). The MRRU is used on multilink PPP circuits to negotiate the maximum size of a reconstructed packet that the interface is willing to accept.
- Authentication protocol (AP). The AP is optional information that identifies which type of authentication to use.

Authentication Protocols (CHAP, PAP, and EAP)

Two peers can specify authentication of the link during the LCP process. Both peers must agree not only to authenticate the link, but also on the chosen method of authentication. There are three authentication protocols available: Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Extensible Authentication Protocol (EAP).

CHAP uses a three-way handshake to authenticate the identity of a peer. During this handshake process the authenticator sends a challenge message to the peer requesting an identity verification. The peer then uses a one-way hash function, such as Message Digest 5 (MD5), to calculate and return a response. The authenticator uses the same hash method to determine the expected value of the response and compares the two. The link is only authenticated if the values match. A mismatch in values causes the authenticator to terminate the connection.

In PAP authentication, an unencrypted ASCII password is transmitted and validated between the peers. This lack of security makes PAP authentication the least desirable of the three authentication protocols. PAP should generally be reserved as a last resort in the event that other authentication protocols are unavailable on the peer device.

EAP supports a wide variety of authentication mechanisms (such as MD5, RADIUS servers, etc.). This authentication method is for advanced users and is beyond the scope of this document.

Network Control Protocols (LLDP, IPCP, and BCP)

Network control protocols are used to negotiate the exchange of network layer data across a PPP link. Two peers negotiate necessary parameters for each type of network layer (layer 3) protocol that will travel over the link. Three common network control protocols are Link Layer Discovery Protocol (LLDP), Internet Protocol Control Protocol (IPCP), and Bridging Control Protocol (BCP). Multiple network control protocols can be used for a single link, allowing MORE flexible handling of heterogeneous traffic. LLDP allows peer routers to exchange information about one another for administrative purposes. LLDP transmissions advertise a peer's abilities and capabilities. This protocol is not required, so a negotiation with a peer that does not support LLDP will not necessarily fail. IPCP exchanges IP information between peers to facilitate IP routing across the link. BCP identifies that the peer is set to bridge traffic. BCP is not required for IP routing across PPP links.

PPP Message Types

Understanding the purpose of each PPP message type allows a user to determine why a PPP link or a particular protocol is failing to negotiate successfully. PPP messages indicate at what point a protocol is failing negotiation. Table 4 describes some common PPP message types found during PPP debugging.

Table 4. Common PPP Message Types

Message	Description
Conf-Req	Configuration request (Conf-Req) is a message that is sent when a unit wishes to open a connection. A Conf-Req includes options specific to desire protocol.
Conf-Ack	Configuration acknowledgement (Conf-Ack) is a message that acknowledges information received in the Conf-Req as acceptable.
Conf-Nak	Configuration negative acknowledgement (Conf-Nak) is a messages that acknowledges a received Conf-Req , but indicates that the peer has requested to use a supported option. The Conf-Nak includes alternative supported options.
Conf-Rej	Configuration reject (Conf-Rej) is a message that is sent to indicate that the peer has requested to use an unsupported option. Conf-Rej does not offer alternative options for the unsupported feature.
Prot-Rej	Protocol reject (Prot-Rej) is a message sent to inform a peer that it is attempting to use an unsupported protocol.
Term-Req	Termination request (Term-Req) is a message sent to terminate a PPP connection.

Table 4. Common PPP Message Types (Continued)

Message	Description
Term-Ack	Termination acknowledgement (Term-Ack) is a message sent to acknowledge a received Term-Req .
Echo-Req/Echo-Rpl	Echo request (Echo-Req) and echo reply (Echo-Rpl) are messages used as PPP keepalives.

Troubleshooting PPP Connections

The first step in troubleshooting a PPP problem is to check the status of the PPP link using the **show interface ppp <interface id>** command. The AOS CLI output shows the interface status as UP or DOWN, the local PPP interface configuration, the current state of the various protocols, and the traffic and queuing statistics. This information is vital in identifying the PPP problem.

Figure 16 displays sample output of the **show interface ppp** command. The output consists of two parts. The first contains configuration information about the PPP interface and the second part shows the state of the various protocols negotiated through the PPP and interface statistics.

```
#show interface ppp 1
ppp 1 is UP
Configuration:
  Keep-alive is set (10 sec)
  No multilink
  MTU = 1520
  Peer authentication with PAP
  Bridge group 1 is configured
  IP is configured
10.10.1.2 255.255.255.252
Link thru t1 2/1 is UP; LCP state is OPENED, MTU is 1520
Receive: bytes=708, pkts=67, errors=0
Transmit: bytes=889, pkts=44, errors=0
5 minute input rate 88 bits/sec, 1 packets/sec
5 minute output rate 48 bits/sec, 1 packets/sec
Bundle Information
Queueing method: weighted fair
HDLC tx ring limit: 2
Output queue: 0/1/0/64/0 (size/highest/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Available Bandwidth 1536 kilobits/sec
IP is UP, IPCP state is OPENED
Address=10.10.1.2 Mask=255.255.255.252
Peer address=10.10.1.1
IP MTU=1500, Bandwidth=1536 Kbps
Bridging is UP, bridging state is OPENED
Bridge group 1
```

This portion displays the current configuration of the local PPP interface.

This portion displays information on the negotiated protocols and link statistics.

Figure 16. Sample show interface ppp Output



When confirming the PPP link is UP, it is important to check all configured protocols. Only LCP is required to be OPEN for the PPP interface to be UP. IPCP or BCP need not be in the OPEN state.

Troubleshooting DOWN PPP Interfaces

If the **show interface ppp** <interface id> command indicates the PPP interface is DOWN, the next step is to check the LCP state. The LCP state appears in **GREEN** in the sample output below. Table 5 lists the various LCP states and provides a description for each.

```
# show interface ppp 1
ppp 1 is UP
Configuration:
  Keep-alive is set (10 sec.)
  Queue-type weighted-fair
  No multilink
  MTU = 1500
  No authentication
  IP is configured
    10.19.2.14 255.255.255.252
Link thru t1 1/1 is UP; LCP state is OPENED, MTU is 1500
Receive: bytes=25187017, pkts=96, errors=0
Transmit: bytes=25185253, pkts=17192, errors=0
5 minute input rate 591680 bits/sec, 50 packets/sec
5 minute output rate 591624 bits/sec, 50 packets/sec
Bundle information
  Queueing method: weighted fair
  HDLC tx ring limit: 2
  Output queue: 0/1/0/64/0 (size/highest/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Available Bandwidth 1344 kilobits/sec
```

Table 5. LCP State Descriptions

LCP State	Description
INITIAL	This is the first state of LCP negotiation.
REQSENT	The unit has sent a Conf-Req to the peer router. When the router is stuck in this state, it is an indication that one of the following may be occurring: <ol style="list-style-type: none"> 1. The timeslots or speed configured for the TDM group are mismatched with the peer router. or <ol style="list-style-type: none"> 2. The peer router is not set for PPP protocol.
ACKRCVD	The unit has received a Conf-Ack from the peer router.
LOOPBACK	The unit received its own packet on the PPP interface. This indicates a loopback is in place towards the unit somewhere on the T1 line. Check the T1 to verify that there are no hard loopback plugs connected. Call the T1 service provider to have them check their equipment for active loops.
OPENED	LCP has been fully negotiated.

Use the PPP debug commands to monitor PPP negotiation, authentication, and errors. These commands display all PPP information sent and received from the peer router. Information within the debug display will identify why a link or protocol is not being properly negotiated. Table 6 on page 17 provides a list of available PPP debug commands and a description of each.

Table 6. PPP Debug Commands

Command	Description
debug ppp negotiation	Displays protocol parameter negotiation.
debug ppp authentication	Displays PAP and CHAP authentication.
debug ppp verbose	Displays detailed messages related to PPP events.
debug ppp errors	Displays protocol errors and statistics.

Understanding PPP Debug Messages

Figure 17 is an example of a successful PPP negotiation monitored on the unit using the **debug ppp negotiation** command. For each **Conf-Req** a response is sent in the opposite direction. This example does not provide information for all PPP protocols, but the subset configured on the example unit.

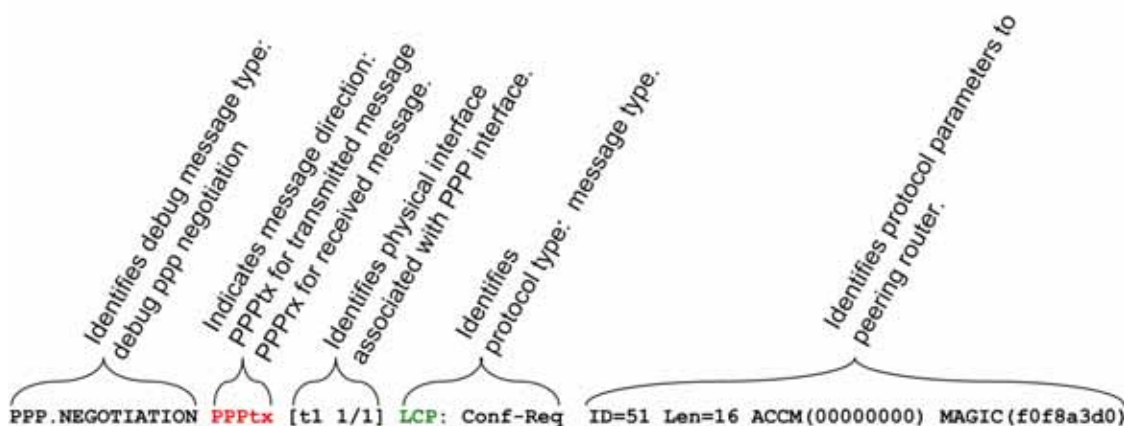


Figure 17. PPP Debug Message

The following is a complete, successful PPP negotiation debug captured from a NetVanta router.

```
Router# debug ppp negotiation
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=51 Len=16 ACCM(00000000) MAGIC(f0f8a3d0)
PPP.NEGOTIATION PPPrx[t1 1/1] LCP: Conf-Ack ID=51 Len=16 ACCM(00000000) MAGIC(f0f8a3d0)
PPP.NEGOTIATION PPPrx[t1 1/1] LCP: Conf-Req ID=242 Len=16 ACCM(00000000) MAGIC(3df92758)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Ack ID=242 Len=16 ACCM(00000000) MAGIC(3df92758)
PPP.NEGOTIATION PPPFSM: layer up, Protocol=c021
PPP.NEGOTIATION t1 1/1: LCP up
PPP.NEGOTIATION PPPtx[t1 1/1] LLDPCP: Conf-Req ID=1 Len=4
PPP.NEGOTIATION PPPrx[t1 1/1] LLDPCP: Conf-Req ID=1 Len=4
PPP.NEGOTIATION PPPtx[t1 1/1] LLDPCP: Conf-Ack ID=1 Len=4
PPP.NEGOTIATION PPPrx[t1 1/1] LLDPCP: Conf-Ack ID=1 Len=4
PPP.NEGOTIATION PPPFSM: layer up, Protocol=82cc
PPP.NEGOTIATION LLDPCP up
PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Req ID=1 Len=22 IP(10.19.2.14) PriDNS(0.0.0.0)
SecDNS(0.0.0.0)
```

```

PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Req ID=1 Len=22 IP(10.19.2.13) PriDNS(0.0.0.0)
SecDNS(0.0.0.0)
PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Rej ID=1 Len=16 PriDNS(0.0.0.0) SecDNS(0.0.0.0)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Rej ID=1 Len=16 PriDNS(0.0.0.0) SecDNS(0.0.0.0)
PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Req ID=2 Len=10 IP(10.19.2.14)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Req ID=2 Len=10 IP(10.19.2.13)
PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Ack ID=2 Len=10 IP(10.19.2.13)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Ack ID=2 Len=10 IP(10.19.2.14)
PPP.NEGOTIATION PPPFSM: layer up, Protocol=8021
PPP.NEGOTIATION IPCP up
INTERFACE_STATUS.ppp 1 changed state to up

```

Routers can also reject (**Rej**) or negative acknowledge (**Nak**) a portion of a configuration request. During the IPCP negotiation illustrated above, both routers send an IPCP configuration request (**Conf-Req**) and each reply with a **Conf-Rej** specifying the options each router rejected from the original request. After the **Conf-Rej** is received, each router then sends another **Conf-Req** without the information previously rejected by the peer. The IPCP negotiation can be broken down as follows:

1. Both routers send an IPCP **Conf-Req**.

```

PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Req ID=1 Len=22 IP(10.19.2.14) PriDNS(0.0.0.0)
SecDNS(0.0.0.0)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Req ID=1 Len=22 IP(10.19.2.13) PriDNS(0.0.0.0)
SecDNS(0.0.0.0)

```

2. Both routers respond with an IPCP **Conf-Rej** specifying what they are rejecting.

```

PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Rej ID=1 Len=16 PriDNS(0.0.0.0) SecDNS(0.0.0.0)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Rej ID=1 Len=16 PriDNS(0.0.0.0) SecDNS(0.0.0.0)

```

3. Both routers send another IPCP **Conf-Req** omitting the previously rejected information.

```

PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Req ID=2 Len=10 IP(10.19.2.14)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Req ID=2 Len=10 IP(10.19.2.13)

```

4. Both routers send an IPCP **Conf-Ack**.

```

PPP.NEGOTIATION PPPtx[t1 1/1] IPCP: Conf-Ack ID=2 Len=10 IP(10.19.2.13)
PPP.NEGOTIATION PPPrx[t1 1/1] IPCP: Conf-Ack ID=2 Len=10 IP(10.19.2.14)

```

5. Both routers agreed on the information and IPCP is now UP.

```

PPP.NEGOTIATION PPPFSM: layer up, Protocol=8021
PPP.NEGOTIATION IPCP up

```

One common issue identified using PPP debug messages is PPP **Conf-Req** messages with no **Conf-Ack** replies. In the following sample output, only **PPPtx Conf-Req** are seen on the router.

```

PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=91 Len=16 ACCM(00000000) MAGIC(2fead23f)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=92 Len=16 ACCM(00000000) MAGIC(2fead23f)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=93 Len=16 ACCM(00000000) MAGIC(2fead23f)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=94 Len=16 ACCM(00000000) MAGIC(2fead23f)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=95 Len=16 ACCM(00000000) MAGIC(2fead23f)
PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Req ID=96 Len=16 ACCM(00000000) MAGIC(2fead23f)

```

This is an indication that one of the following may be occurring:

1. The timeslots or speed configured for the TDM group are mismatched with the peer router.
2. The peer router is not configured for PPP protocol.

Frame Relay Technology Overview

Frame Relay is a layer 2 packet-switched protocol used primarily for connecting remote offices over long distances. The Frame Relay network switches packets from one location to another using addressing information contained in the Frame Relay header. It is important to become familiar with some common Frame Relay acronyms before beginning a Frame Relay technology overview. Table 7 provides some common acronyms along with a description for each.

Table 7. Common Frame Relay Terms

Acronym	Description
CPE	Customer premises equipment (CPE). The NetVanta router is an example of a CPE device terminating a Frame Relay circuit.
DCE	Data communications equipment (DCE) in the form of the Frame Relay service provider's Frame Relay switch.
DLCI	Data link connection identifier (DLCI). DLCIs are used to identify a virtual circuit between the CPE and local DCE. DLCIs are only locally significant between the CPE and DCE.
PVC	Permanent virtual circuit (PVC). PVCs identify a permanent circuit linking two locations.
CIR	Committed information rate (CIR). The CIR is the amount of bandwidth the user is guaranteed on the circuit by the provider.
LMI	Link management interface (LMI). LMI is used to notify the CPE of active and present DLCIs and if DLCIs are removed. It is also used to monitor the connection between the CPE and DCE using keepalive messages.
FECN	Forward error congestion notification (FECN). FECNs are sent by a congested device to the destination CPE to inform the device of the current congestion situation.
BECN	Backwards error congestion notification (BECN). BECNs are sent by a congested device to the sending CPE device to inform the device of the current congestion situation.
DE	Discard eligible (DE). Discard eligible bits are set to identify non-critical packets. The network has the option to drop DE packets during congestion periods.

Figure 18 illustrates three locations that are interconnected using Frame Relay circuits. The solid line between the DCE and the CPE represents the physical T1. The dotted line represents the PVC connecting each remote site back to the main site.

NOTE *The DLCIs for Remote 1 and Remote 2 are both 16. This example illustrates that the DLCI is only locally significant. DLCI 16 is used at each remote site to connect back to the main site. At the main site, the DLCI for Remote 1 is 100 and Remote 2 is 101.*

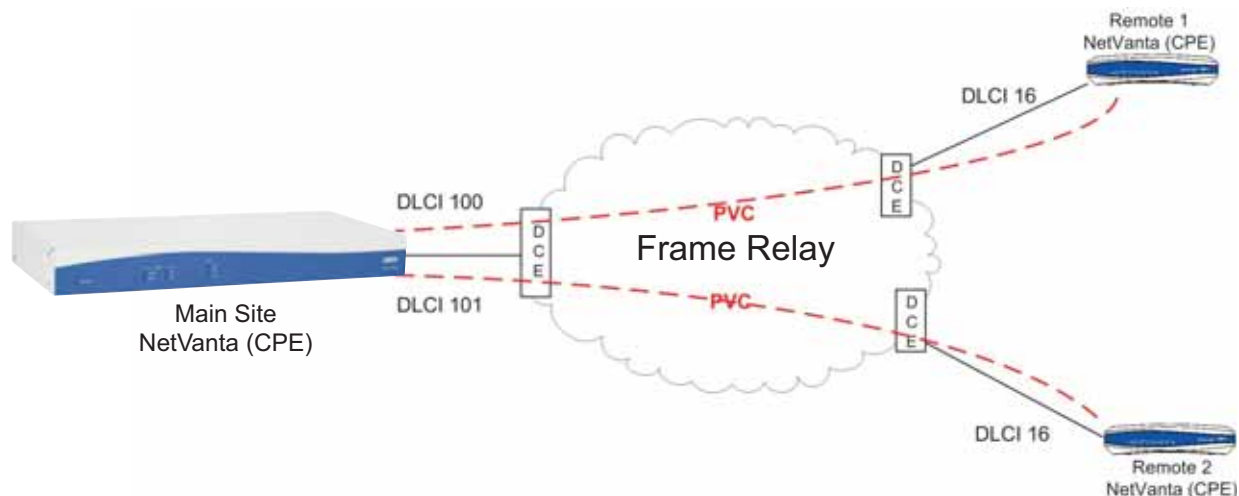


Figure 18. Frame Relay Network Example Diagram

LMI Overview

LMI plays a very important role in Frame Relay networks. LMI has three main purposes:

1. Notify the CPE of present DLCIs.
2. Notify the CPE if a DLCI is removed.
3. Monitor the connection between the CPE and DCE using keepalives called link status inquiry messages.

Link status inquiries are sent every 10 seconds. The CPE sends a request and the DCE responds. The DCE sends a full status update (including all the DLCIs the switch has configured for the connected CPE) in every sixth status inquiry response. Frame Relay PVCs are not considered active on the CPE until the full status update is received from the DCE. Table 8 on page 20 lists supported LMI types.

Table 8. LMI Types


LMI Type	Description
AUTO	Detects the LMI type automatically. This is the default setting.
ANSI (Annex D)	North American LMI standard.
Cisco	Cisco proprietary LMI signaling.

Table 8. LMI Types (Continued)

LMI Type	Description
Q933a (Annex A)	International LMI standard.
None	No LMI signaling. Links without LMI signaling are assumed to be UP.

Understanding Signaling Roles

Frame Relay calls for connected equipment to have set signaling roles. The CPE is typically configured in a user role, while the DCE is generally performing a network role. The roles identify how messages are sent from the device and what messages a device should expect from connected equipment. For example, a user expects to receive an LMI full status update from the DCE before declaring the PVC active. If two users are connected, neither will provide the full status update and the PVC will remain inactive. User equipment must be connected to network equipment and vice versa for LMI messages to be properly exchanged.



CPE equipment is set to perform a user role while the Frame Relay provider equipment (DCE) should be set to network.

PVC States

PVCs (the links between routers across the Frame Relay cloud) are identified at each location using a local DLCI. PVCs can be in one of three states. Each PVC state provides unique information for identifying Frame Relay issues and where the problem is occurring. Table 9 provides a list of the PVC state and description of each.

Table 9. PVC States

PVC State	Description
ACTIVE	LMI is active between both sites. Correct DLCI information is being advertised from the local frame switch (DCE).
INACTIVE	LMI at the remote site is DOWN.
DELETED	Local DLCI configured on the router is not being advertised as valid by the local frame switch (DCE).

Troubleshooting Frame Relay Connections

The first step in troubleshooting a Frame Relay problem is to check the status of the Frame Relay link using the **show interface frame-relay <interface number>** command. The AOS CLI output identifies the interface status as UP or DOWN, the main Frame Relay interface configuration (not the sublink

information), and the traffic and queuing statistics. This information is vital in isolating a Frame Relay issue.

Figure 19 illustrates the **show interface frame-relay** output. The output consists of two parts. The first part contains configuration information about the main Frame Relay interface and the second part shows the state of the Frame Relay link and the interface statistics.

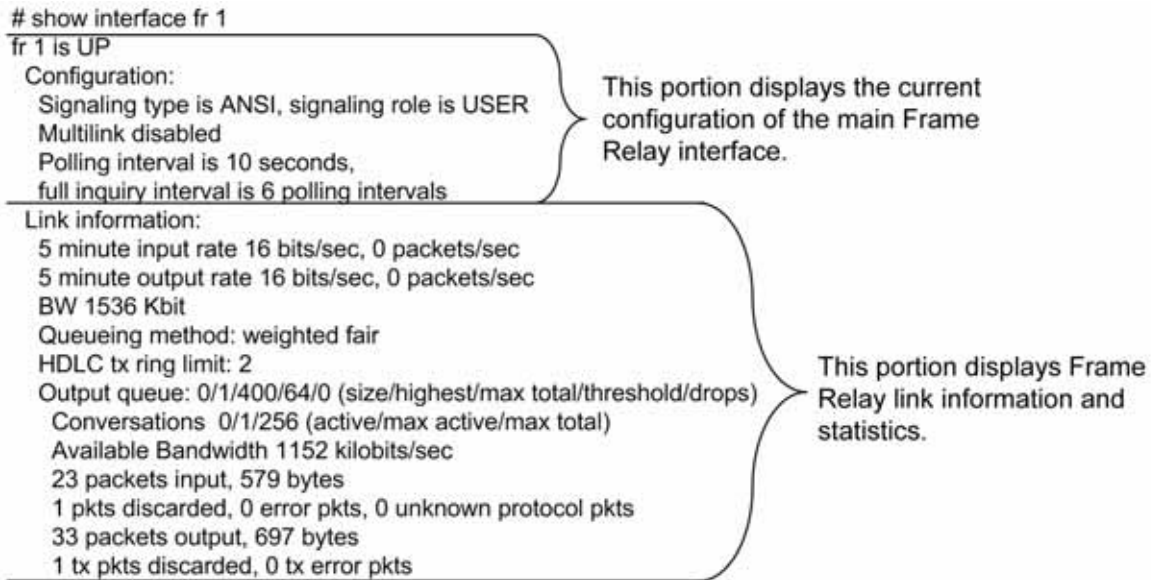


Figure 19. Sample 'show interface fr' (main interface) Output

Use the **show frame-relay lmi** command to display LMI statistics for all configured Frame Relay interfaces. The output from this command shows the number of LMI messages sent, received, and the ones that timed out. The **show frame-relay lmi** command can be used to identify if the switch is responding to the CPE sent LMI messages. The CPE must receive three concurrent LMI messages, one of which must be a full status, before the Frame Relay LMI is considered to be UP. Figure 20 shows a sample output from the **show frame-relay lmi** command.

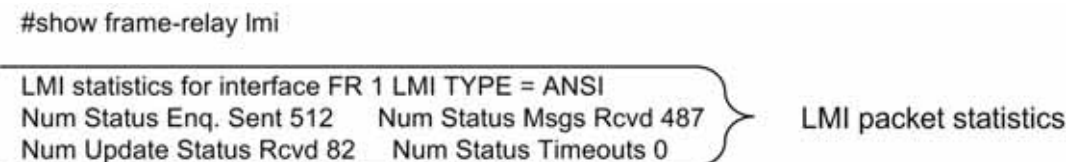


Figure 20. Sample 'show frame-relay lmi' Output

The AOS CLI provides more detailed information about the Frame Relay link by using the **show interface frame-relay <port.sublink>** command and specifying the Frame Relay sublink (for example, fr 1.100). This command identifies the state of the sub-interface (or PVC). Possible states are ACTIVE, INACTIVE, and DELETED. Refer to *PVC States* on page 21 for more information concerning PVC states. Figure 21 shows a sample output from the **show interface frame-relay** command specifying a particular PVC.

```
# show interface fr 1.100
fr 1.100 is Active
Ip address is 10.10.2.1, mask is 255.255.255.252
Interface-dlci is 100
MTU is 1500 bytes, BW is 1536 Kbit
Average utilization is 0%
```

Displays Frame Relay sub-interface status and statistics.

Figure 21. Sample 'show interface frame-relay 1.100' Output

You can use the **show frame-relay pvc** command to show information for all configured PVCs. All PVCs on the same Frame Relay interface are grouped together. Figure 22 shows a sample output from the **show frame-relay pvc** command.

```
#show frame-relay pvc
Frame Relay Virtual Circuit Statistics for interface FR 1
Active Inactive Deleted Static
local 2 0 0 2
DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = FR 1.100
MTU: 1500
input pkts: 6 output pkts: 8 in bytes: 834
out bytes: 1120 dropped pkts: 0 in FECN pkts: 0
in BECN pkts: 0 in DE pkts: 0 out DE pkts: 0
Creation time: 03-07-2005 17:17:05 Last status change: 00W:00D:00H:02M:45S
DLCI = 101, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = FR 1.101
MTU: 1500
input pkts: 6 output pkts: 7 in bytes: 834
out bytes: 980 dropped pkts: 0 in FECN pkts: 0
in BECN pkts: 0 in DE pkts: 0 out DE pkts: 0
Creation time: 03-07-2005 17:17:11 Last status change: 00W:00D:00H:02M:36S
```

This portion displays a summary of PVCs states.

This portion displays statistics on each individual PVC.

Figure 22. Sample 'show frame-relay pvc' Output

Troubleshooting DOWN Frame Relay Interfaces

If the **show interface frame-relay <port>** command indicates the Frame Relay interface is DOWN, verify that the signaling type is properly configured to match the Frame Relay circuit. The configured signaling type is displayed in the configuration section of the **show interface frame-relay** command output. If the signaling type is properly configured, check the Frame Relay LMI statistics using the **show frame-relay lmi** command. For example,

#show frame-relay lmi

```
LMI statistics for interface FR 1 LMI TYPE = ANSI
Num Status Enq. Sent 24   Num Status Msgs Rcvd 0
Num Update Status Rcvd 0   Num Status Timeouts 0
```

If the output indicates that the interface is transmitting LMI messages (**Num Status Enq Sent**) but not receiving LMI messages (**Num Status Msgs Rcvd** and **Num Update Status Rcvd**), contact your Frame Relay service provider and inform them that the CPE is not receiving LMI from the frame switch. Service providers frequently disable the switch frame interface until the customer notifies them that a CPE device is installed.

Checking the PVC Status

When the Frame Relay interface shows UP, check the PVC status for each sub-interface using the **show frame-relay pvc** command. Compare the PVC status with the information provided in Table 10 and follow the corrective action. The following is sample output from the **show frame-relay pvc** command.

#show frame-relay pvc

Frame Relay Virtual Circuit Statistics for interface FR 1

```
      Active  Inactive Deleted  Static
local    2      0      0      2
```

DLCI = 100, DLCI USAGE = LOCAL, **PVC STATUS = ACTIVE**, INTERFACE = FR 1.100

MTU: 1500

```
input pkts: 5   output pkts: 5   in bytes: 256
out bytes: 245   dropped pkts: 0   in FECN pkts: 0
in BECN pkts: 0   in DE pkts: 0   out DE pkts: 0
```

Creation time: 03-07-2005 17:17:06 Last status change: 00W:00D:00H:07M:34S

DLCI = 101, DLCI USAGE = LOCAL, **PVC STATUS = ACTIVE**, INTERFACE = FR 1.101

Table 10. Troubleshooting PVCs

PVC State	Description	Corrective Action
ACTIVE	PVC is active between the sites.	No corrective action necessary.
INACTIVE	LMI at the remote site is DOWN.	Check the remote site(s) and troubleshoot accordingly.
DELETED	Local frame switch is not advertising a DLCI that is configured on the interface.	Contact the Frame Relay service provider and verify the DLCI information for the local site.

Appendix A

Making a T1 Loopback Plug

A T1 loopback plug is made by shorting the transmit pins to the receive pins. This allows the user to verify that the T1 interface transmitter and receiver are operating properly. Follow the steps outlined below to make a T1 loopback plug. Refer to *Appendix B* on page 27 for more information on troubleshooting with a T1 loopback plug.



You will need a set of RJ-45/RJ-48 crimpers, an RJ-45 (or RJ-48) connector, and two pieces of conductor to make the loopback plug.

Making a T1 Loopback Plug	
Step	Action
1	Hold the RJ-45 (or RJ-48) connector so that the end is pointing away from you and the locking lever is pointed toward the floor.
2	The connector pins are numbered 1 through 8 counting from left to right. Locate pins 1, 2, 4, and 5.
3	Use a jumper conductor to connect pin 1 to pin 4 and pin 2 to pin 5 (see Figure 1).

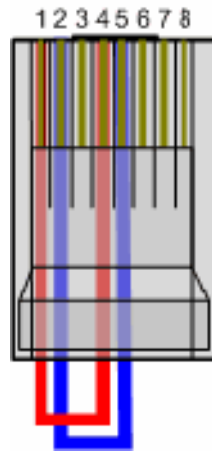


Figure 1. T1 Loopback Plug

Making a T1 Cross-over Cable

A T1 cross-over cable is used when connecting two T1 devices together with like interfaces (DS1 to DS1). For example, NetVanta routers can be connected back to back if you use a cross-over cable. A cross-over cable is required because both NetVanta T1 interfaces are DS1 interfaces. Use the wiring pinouts provided in Table 1 to make a T1 cross-over cable.



You will need a set of RJ-45/RJ-48 crimpers, 4-conductor wire, and two RJ-45 (or RJ-48) connectors to make a T1 cross-over cable.

Making a T1 Cross-over Cable	
Step	Action
1	Hold the RJ-45 (or RJ-48) connector so that the end is pointing away from you and the locking lever is pointed toward the floor.
2	The connector pins are numbered 1 through 8 counting from left to right. Locate pins 1, 2, 4, and 5 and insert a conductor in each pin location. Follow the wiring pinouts in Table 1 to connect the conductors.

Table 1. T1 Cross-over Cable Wiring Pinouts

Side A	Side B
1	4
2	5
4	1
5	2

Appendix B

Troubleshooting with a T1 Loopback Plug

A T1 loopback plug provides a means to test and troubleshoot T1 circuits and interfaces in an unbiased manner to locate potential issues. The T1 loopback plug can be used to test the physical T1 interface (transmitter and receiver), the T1 line, and the internal wiring independently.

Testing a NetVanta T1 Interface Using a Loopback Plug

To test the T1 interface, insert the loopback plug into the WAN T1 port and check the interface status (see Figure 1). The T1 interface should show UP and the PPP interface should show LCP status is IN LOOPBACK. You can check the Frame Relay interface using the **show frame-relay pvc** command. The LMI sent messages and received messages should be the same.

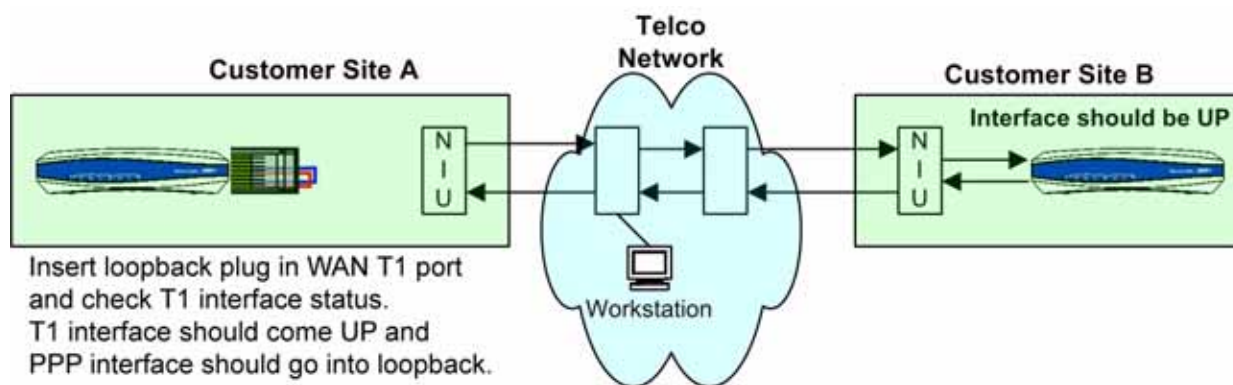


Figure 1. Testing the T1 Interface Using a Loopback Plug

Testing Internal Wiring Using a Loopback Plug

T1 service providers generally test a T1 line by sending loop-up codes to the NIU and then running a test pattern to the looped NIU. The pattern will report any errors (see Figure 2).

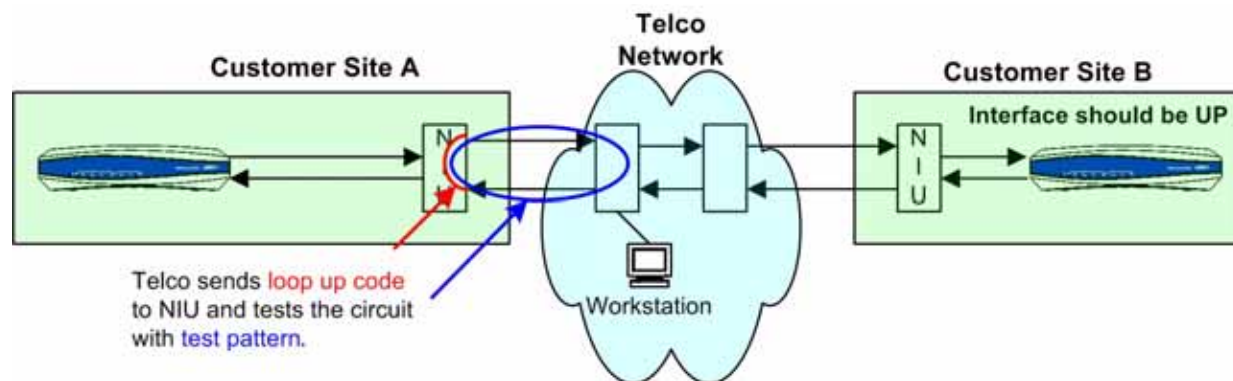


Figure 2. Telco Loop to the NIU

If the circuit runs error-free with the NIU in loopback, the provider can then send a loop-up code to the CPE CSU/DSU (NetVanta) to loop the T1 interface towards the network. The provider again runs a test pattern, but this time to the looped CSU/DSU (see Figure 3).

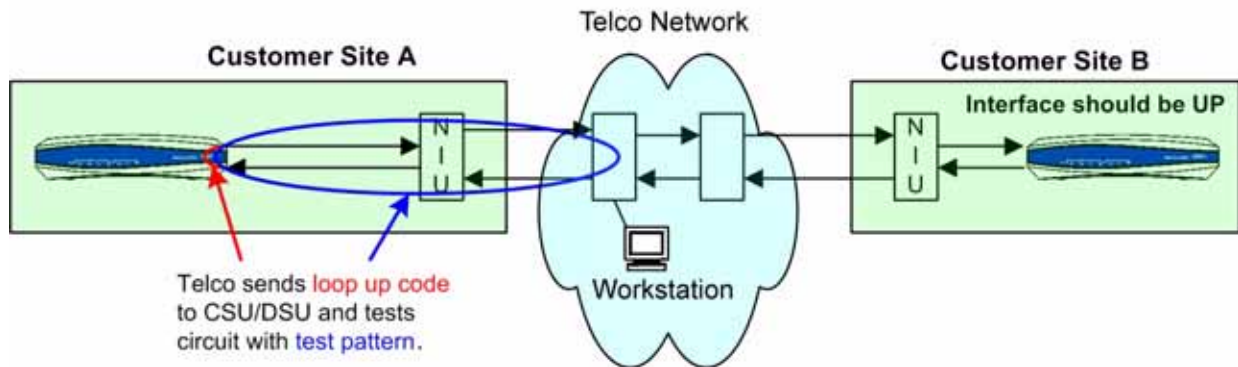


Figure 3. Telco Loop to the CSU/DSU

If the provider is unable to loop the CSU/DSU, or if the test indicated that there were errors, use a loopback plug to remove the CSU/DSU from the circuit and isolate the internal wiring.

1. Insert the loopback plug into the unit's T1 WAN interface and check the T1 status (see Figure 4). Verify that the T1 interface is UP and no errors are incrementing.

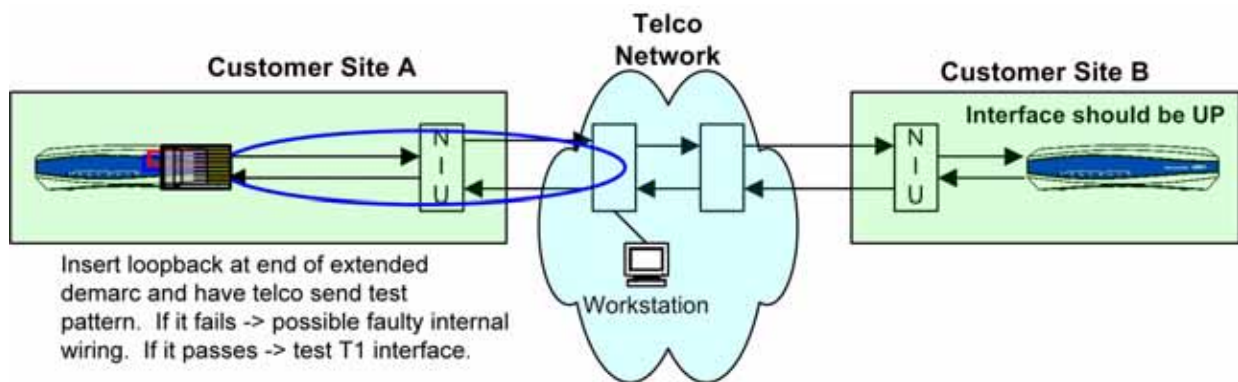


Figure 4. Loopback Plug on WAN T1 Interface

2. Insert the loopback plug into the NIU and have the provider run a test pattern to test the line (see Figure 5 on page 29).

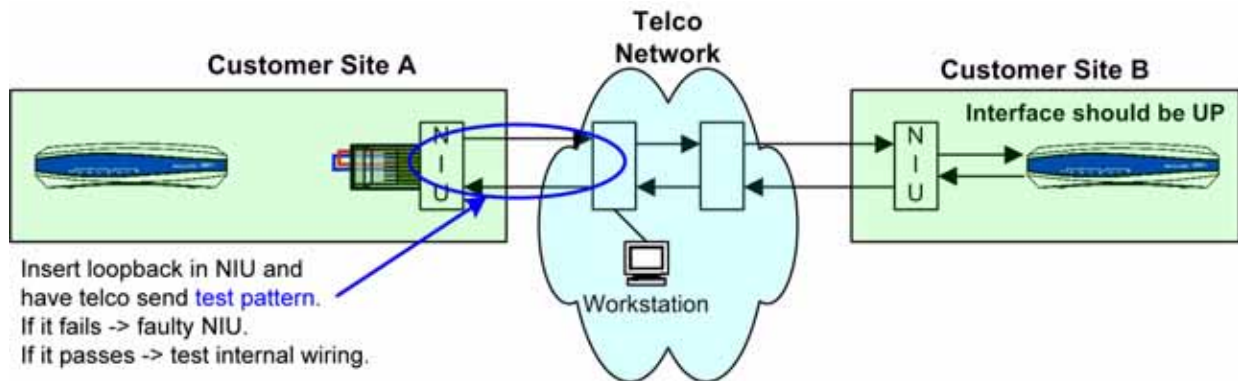


Figure 5. Telco Line Test to NIU with Loopback Plug

3. Insert the loopback plug into the T1 jack where the router is attached (see Figure 6). Have the provider repeat the line test.

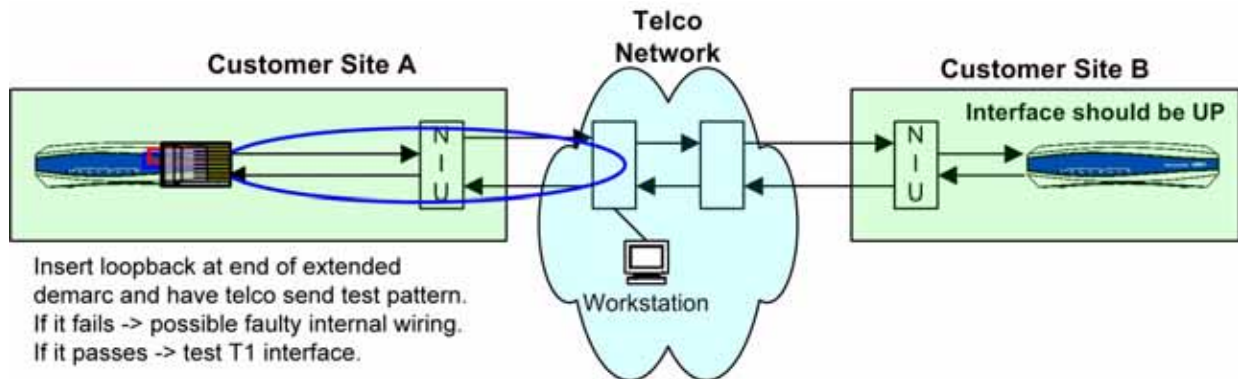


Figure 6. Telco Line Test to T1 Jack with Loopback Plug

If the line test fails when the loopback plug is in the NIU, then the NIU could be faulty. If the line test is clean to the NIU but fails to the T1 jack (with the loopback plug connected to the T1 jack), then there is an issue with the wiring between the NIU and the T1 jack.

