

Configuration Guide

Point-to-Point Protocol

This configuration and troubleshooting guide will aid in the setup of Point-to-Point Protocol (PPP) and Multilink PPP (MLPPP) for ADTRAN Operating System (AOS) products. An overview of PPP/MLPPP general concepts combined with detailed command descriptions provide step-by-step assistance for configuration. The troubleshooting section outlines proper use of **show** and **debug** commands to verify that PPP/MLPPP has been configured properly on the AOS product(s).

This guide consists of the following sections:

- *PPP Overview on page 2*
- *Multilink PPP (MLPPP) Overview on page 6*
- *Hardware/Software Requirements/Limitations on page 9*
- *Advanced CLI Configuration on page 10*
- *GUI Configuration on page 23*
- *Example Configurations on page 36*
- *Quick Configuration Guide on page 50*
- *Troubleshooting on page 52*

PPP Overview

PPP operates at the data link layer of the open systems interconnection (OSI) model and provides end-to-end connectivity for devices across a point-to-point link. PPP is made up of a suite of protocols. (See Figure 1. AOS products support the protocols underlined in the illustration.) The PPP suite includes several types of protocols, and each one has a specific role in establishing and maintaining a PPP connection:

- Link Control Protocol (LCP)
- Authentication protocols
- Network Control Protocols (NCPs)
- PPP

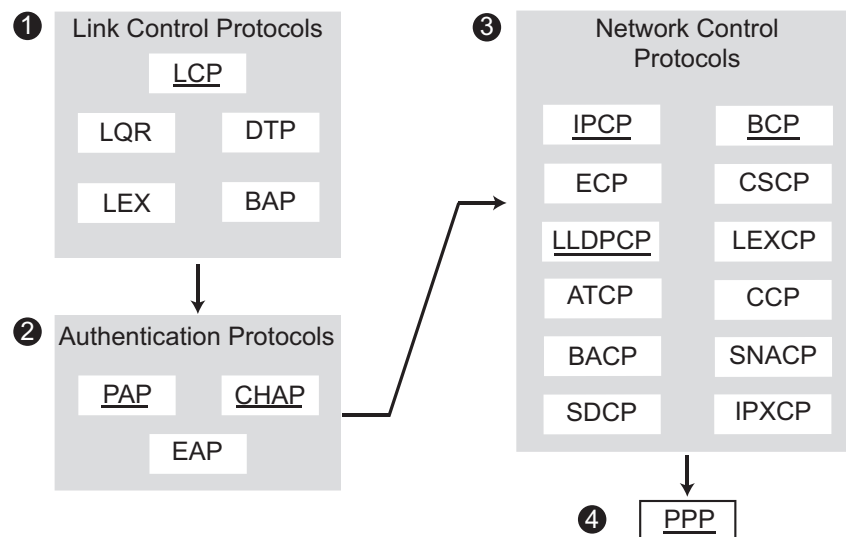


Figure 1. Protocols in the PPP Suite

Establishing a PPP Connection

When two peers try to establish a PPP connection, they must exchange protocols in the following order:

1. LCP
2. Authentication protocol (optional)
3. NCP
4. PPP

Exchanging authentication protocols is optional. Understanding how a PPP session is established can help with troubleshooting if problems occur (see Figure 2).

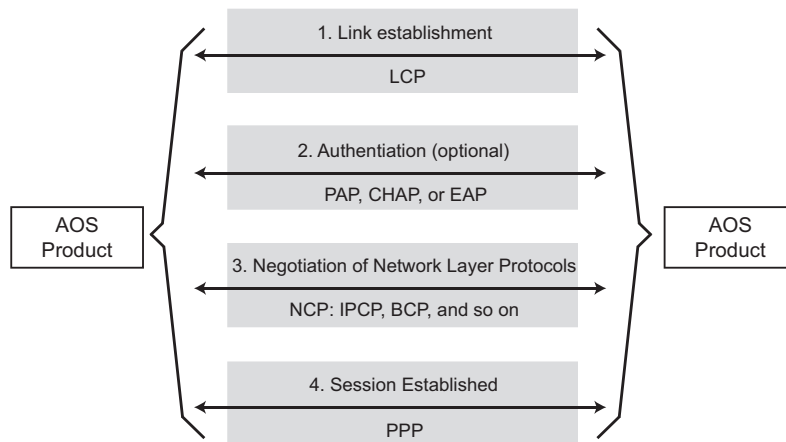


Figure 2. Establishing a PPP Link

Link Establishment

The two peers exchange LCP frames to establish, configure, and test the link. These frames allow the devices to determine if the link can accommodate the data they want to transfer. The LCP frames also contain a field called the configuration option, which informs the peer of the size of the PPP datagrams that will be sent and their degree of compression.

The two peers negotiate these settings. If the LCP frames do not contain a configuration option field, the peers use the default configurations.

Authentication Protocol

If authentication is configured, the two peers authenticate the link. Although authentication is optional, the peers pass through this phase whether or not authentication is chosen. PPP supports several authentication protocols:

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Extensible Authentication Protocol (EAP)



AOS products support PAP and CHAP.

PAP

PAP is the simplest possible authentication scheme. The protocol requires a two-way message exchange. One peer sends a previously agreed upon password to the other peer, called the authenticator. The authenticator looks up the password in its database. If the password matches, the router returns an authentication acknowledge; after the negotiation of network layer protocols, the link is established. PAP authentication requires that the two routers authenticate only once, and the user name and password are sent in clear text across the connecting private circuit. Since PAP sends the password unencrypted, anyone capable of tapping into the wire can intercept it.

CHAP

CHAP solves the security problem of PAP by hashing the password and sending the hash value instead of the password over the wire. CHAP follows the process shown in Figure 3.

1. The authenticator generates a challenge message with a random number and sends that to the peer requiring authentication.
2. The peer combines its password with the random number and other variables contained in the challenge message to calculate a hash value using the message digest 5 (MD5) algorithm. (In other words, the password has been irreversibly encrypted.) The peer sends the hash value to the authenticator in a response message.
3. The authenticator knows both the agreed upon random number and the peer's password. The authenticator performs the same hashing calculation with MD5 and compares its calculated hash value to the hash value sent by the peer in the response message.
4. If the hash values match, the authenticator acknowledges the peer, and the peers proceed to exchange NCPs. If the hash values do not match, the authenticator continues to issue challenges until the peer returns a matching hash value or runs out of retry attempts. Because the encryption prevents hackers from hijacking a password, CHAP provides increased security. In addition, CHAP requires peers to reauthenticate themselves from time to time.

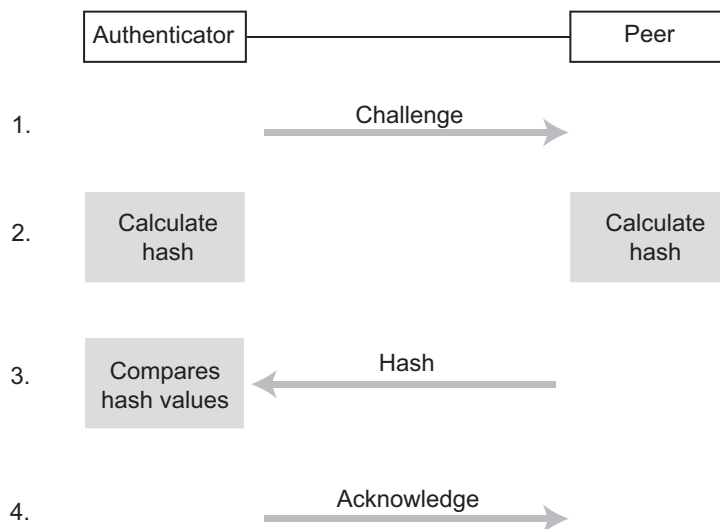


Figure 3. CHAP Process

NCP

PPP uses NCP to enable the exchange of network layer protocols across a link. The two local area networks (LANs) connected by a wide area network (WAN) link may use different network layer protocols. The two PPP peers that have established the WAN connection can use NCPs to encapsulate these network layer protocols so that they can exchange different higher level protocols without disrupting the WAN connection.

Applicable AOS products support the following NCPs:

- IP Control Protocol (IPCP)
- Bridging Control Protocol (BCP)
- Link-layer Discovery Protocol (LLDP) Control Protocol (LLDPCP)

PPP

PPP frames carry the actual information being transferred over the link. In PPP terminology, this information is called a datagram. After the two peers successfully exchange LCP frames, authenticate the link (if authentication is configured), and negotiate the network layer protocols, a PPP session is established. The devices can then exchange PPP datagrams.

Multilink PPP (MLPPP) Overview

Link Aggregation

PPP and other data link layer protocols establish point-to-point connections over a single carrier line. However, a single line may not provide sufficient bandwidth to meet a business' requirements. This lack of bandwidth can lead to congestion and dropped packets.

Purchasing a high-bandwidth T3 line to sidestep these limitations is not always feasible because some environments do not support them. In addition, a T3 line can be quite expensive. Often, an organization only wants to double or triple its bandwidth, rather than increase it twenty-eight fold. The purchase of a high-cost T3 line is difficult to justify when much of the bandwidth will not be used.

AOS products support link aggregation protocols, such as MLPPP, to address these problems. Such protocols treat multiple carrier lines as a single bundle, providing two advantages:

- Faster connections - Traffic can access the combined bandwidth of the bundle.
- More stable connections - If one line goes down, the other(s) can still carry traffic.

Theoretically, link aggregation is a simple idea: effectively double your available bandwidth by using two physical links to connect your endpoints instead of only one, triple your bandwidth by using three links, quadruple your bandwidth by using four links, and so on. For example, you could aggregate two 1.544 Mbps T1 connections into a virtual single network connection with an underlying bandwidth of 3.088 Mbps.

MLPPP takes advantage of multiple physical links by fragmenting frames into smaller pieces called frame fragments. These fragments are passed simultaneously over separate cables and then reassembled by the receiving peer (see Figure 4).

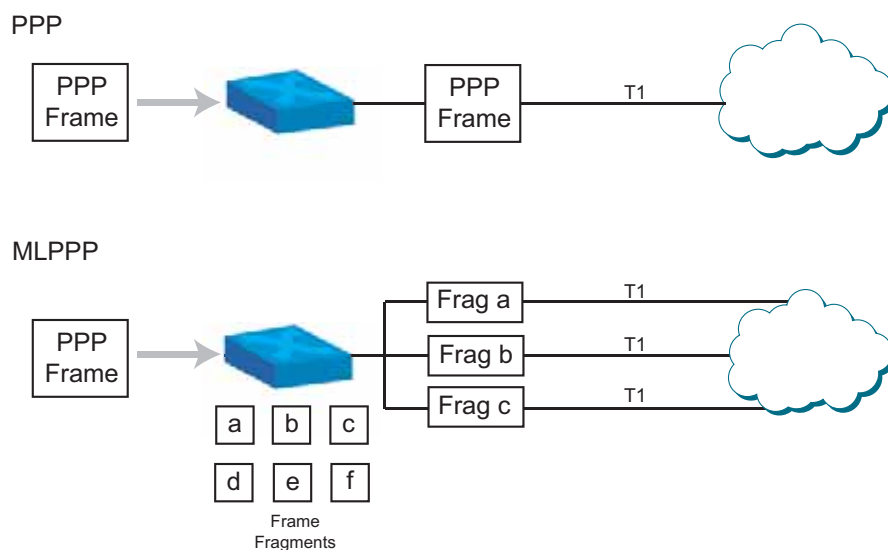


Figure 4. Fragmentation in MLPPP

Understanding MLPPP

Although using MLPPP to increase a connection's bandwidth does not require deep technical expertise, you should generally understand the following:

- How a PPP session is established (refer to the PPP overview at the beginning of this section)
- How MLPPP regulates the fragmentation and reconstruction of normal PPP frames

Such an understanding will help you troubleshoot MLPPP connections and regulate data flow.

MLPPP establishes a session between two peers using the same protocols and phases as typical PPP. However, MLPPP adds the following:

- Three option fields to the LCP frames
- A MLPPP header to the information field of the PPP frame

LCP Options

The receiving peer must know that the sending peer will be fragmenting PPP frames and transmitting them over multiple carrier lines. It must also be able to recognize that these fragmented frames originate from a single peer. Three LCP options prepare peers to exchange PPP frames over an MLPPP connection:

- **Maximum Receive Reconstructed Unit (MRRU)** - Including the MRRU option serves two functions: it indicates that the sending peer wants to, and that the receiving peer can, use MLPPP, and it specifies the size of the reconstructed frame.
- **Short Sequence Number Header Format** - A peer can request to use a 12-bit rather than a 24-bit sequence number in the MLPPP header. A 12-bit sequence number enables a frame to be split into a little less than 5,000 fragments, which is more than adequate for the typical bundle of lines.
- **Endpoint Discriminator (ED) Options** - Peers negotiate how the receiving peer will identify the sending peer. One of these methods is an ED, which can be generated from an IP address, MAC address, or PPP magic number. Every carrier line in the MLPPP bundle originates from the same endpoint and is given the same ED. The receiving peer recognizes that frames received from different carrier lines, but with the same ED, come from the same peer.

MLPPP Header

The MLPPP header helps the receiving peer reconstruct frame fragments in the correct order. When a peer sends a PPP frame across an MLPPP connection, it first fragments the PPP frame. It then encapsulates fragments in new PPP frames and simultaneously sends them over each aggregated line. The new PPP frame includes the following:

- A new PPP header
- A four-field MLPPP header
- A fragment of the original PPP frame

The MLPPP header includes a flag and a sequence number. The sequence number indicates the fragment's place in the reconstructed PPP frame.

MLPPP Configuration Concerns

When you enable MLPPP for a connection, the LCP automatically negotiates the necessary options, such as the MRRU and ED. The extra carrier lines simply need to be cross connected in AOS to the PPP interface. MLPPP automatically adds them to the bundle. PPP keepalive signals are sent on each link in the bundle to verify when a link goes down. MLPPP automatically removes lines that go down from the bundle and adds lines that come back up. The PPP connection stays open as long as at least one line is up.

Hardware/Software Requirements/Limitations

PPP is supported in AOS products running version 7.1 or higher. Table 1 lists the types of PPP supported by each product platform.

Table 1. PPP Types Supported by AOS Products

AOS Product	PPP	MLPPP (maximum links per bundle)	PPPoE	PPPoA	PPPoE over ATM
NetVanta 300 Series				•	•
NetVanta 1000R Series	•	• (2)	•	•	•
NetVanta 1335	•	• (2)	•	•	•
NetVanta 2000 Series			•		
NetVanta 3120			•		
NetVanta 3130			•	•	•
NetVanta 3200 Series	•	• (2)	•	•	•
NetVanta 3300 Series	•	• (3)	•	•	•
NetVanta 3400 Series	•	• (2)	•	•	•
NetVanta 4000 Series	•	• (8)	•	•	•
NetVanta 5000 Series	•	• (48)	•		
NetVanta 6355	•	• (2)	•	•	•
NetVanta 7000 Series	•	• (2)	•	•	•
Total Access 900 Series	•		•		
Total Access 900e Series	•	• (4)	•		
Total Access 900 ADSL2+ Series				•	•

MLPPP is supported in AOS products running version 7.1 or higher. The maximum number of links per MLPPP bundle varies per platform and is listed in parentheses in the MLPPP column in Table 1.



PPPoA and PPPoE over ATM are supported on asymmetric digital subscriber line (ADSL) interfaces only. These interfaces are built-in to the NetVanta 340, 344, and 3130. An ADSL option module must be used for all other products listed that support PPPoA and PPPoE over ATM.

Advanced CLI Configuration

T1, E1, DDS, SHDSL, Serial, T3, and HSSI Interfaces

The physical T1, E1, DDS, SHDSL, serial, T3, and HSSI interfaces must be set up and activated in addition to configuring the virtual PPP interface. Table 2 shows the main physical settings that must be configured for an interface that uses PPP.

Table 2. Main Required Physical Settings

Interface Configuration Mode Context	Command	Explanation
t1	tdm-group <number> timeslots <range of DS0s>	Defines the number of channels (DS0s) used for the T1 connection.
	coding [ami b8zs]	Defines the line coding.
	framing [d4 esf]	Defines the frame format.
	clock source [internal line system]	Defines the clock source or timing for the T1.
	lbo [long short]	Line build out (LBO) sets the strength level of the transmit signal.
	no shutdown	Activates the interface.
e1	tdm-group <number> timeslots <range of DS0s>	Defines the number of channels (DS0s) used for the E1 connection.
	coding [ami hdb3]	Defines the line coding.
	framing [crc4]	Defines the frame format.
	clock source [internal line system]	Defines the clock source or timing for the E1.
	no shutdown	Activates the interface.
dds	clock source [internal line]	Defines the clock source for the DDS interface.
	clock rate [auto bps56k bps64k]	Defines the clock rate.
	no shutdown	Activates the interface.
shdsl	equipment-type [co cpe]	Specifies this unit as the master unit or as a slave unit.
	linerate <value>	Specifies the line rate for the SHDSL interface. Functional in CO mode only.
	no shutdown	Activates the interface.

Table 2. Main Required Physical Settings (*Continued*)

Interface Configuration Mode Context	Command	Explanation
serial*	serial-mode [EIA530 v35 x21]	Configures the interface to support the appropriate cable.
	et-clock-source [rxclock txclock]	Configures the serial interface to take the clock from the receive signal (rxclock) or from the transmit signal (txclock).
	no shutdown	Activates the interface.
t3**	clock source [local loop]	Defines the clock source or timing for the T3.
	coding [b3zs]	Defines the line coding.
	framing [cbit m13]	Defines the frame format.
	line-length [short long]	Sets the strength level of the transmit signal.
	no shutdown	Activates the interface.
hssi**	no shutdown	Activates the interface.
<p>* A serial connection on the WAN is typically used when the AOS device is placed behind an existing WAN access device.</p> <p>** T3 and HSSI are currently only supported in the NetVanta 5305.</p>		

Basic PPP Interface Setup

The first step to configuring PPP for an E1, T1, DDS, SHDSL, serial, T3, or HSSI interface is to create a virtual interface. Start from Global Configuration mode:

Step 1: Create a PPP Interface on the AOS Product

Create the virtual PPP interface and assign it a number. Every PPP interface must have a unique number.

```
(config)#interface ppp <number>
```

<number> Specifies the PPP interface number. Range is 1 to 1024. This value is only locally significant and does not need to match the identifier of the PPP interface on the other end of the point-to-point circuit.

Step 2: Configure an IP Address for the WAN Connection

The IP address for the E1, T1, or DDS WAN connection is configured on the PPP interface rather than on the physical interface. There are several ways to assign an IP address to the PPP interface:

- Assign a static IP address
- Configure the PPP interface to negotiate the IP address with your Internet service provider (ISP) or peer router.

- Configure the PPP interface as an unnumbered interface



*The peer IP address learned through IPCP is displayed as a 32-bit route in the routing table. The peer address will also be displayed in this manner in the output of the **show interface ppp** command.*

Static IP Address

The static IP address is a fixed address assigned to the PPP interface by a user.

```
(config-ppp 1)#ip address <ip address> <subnet mask>
```

<ip address> Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation.

<subnet mask> Specifies the subnet mask that corresponds to a range of IP addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation or as a prefix length following a forward slash (/).

For example, the IP address 192.22.73.101, assuming a 24-bit subnet mask, could be entered in either of the following ways:

```
(config-ppp 1)#ip address 192.22.73.101 255.255.255.0 (using dotted decimal notation)
```

or

```
(config-ppp 1)#ip address 192.22.73.101 /24 (using prefix length).
```

Negotiated IP Address

WAN connections used for Internet access often need to be configured so that the PPP interface will negotiate an IP address with the ISP's router. A user's ISP can confirm if this type of setup is needed. This option should also be selected if the peer router is configured to assign an IP address to the local router.

```
(config-ppp 1)#ip address negotiated
```

Unnumbered Interface

To conserve IP addresses on a network, users can create a PPP interface as an unnumbered interface. When a logical interface on the router is assigned an IP address, the address cannot overlap with the IP addresses assigned to other logical interfaces on the network. As a result, each interface that has an IP address represents an entire subnet. Depending on the subnetting scheme used, this could use more IP addresses than a network can spare.

By configuring a PPP interface as an unnumbered interface, the IP address of another interface (specified by the user) will also be used for the PPP interface. AOS then uses the IP address of the specified interface when routing updates are sent over the PPP interface.

```
(config-ppp 1)#ip unnumbered <interface>
```

<interface> Specifies the interface that has actually been assigned the IP address to be used as the source address for all packets transmitted on the ppp interface. For example, for an Ethernet interface, **eth 0/1** might be specified. Valid interface types include ATM, BVI, demand, Ethernet, Frame Relay, high level data link control (HDLC), loopback, and PPP. VLAN interfaces are also an option on integrated switch-router products. Type **ip unnumbered ?** for a list of valid interfaces on a specific product.

There is a potential disadvantage to configuring a PPP interface as an unnumbered interface. If the

interface to which the IP address is actually assigned goes down, the PPP interface will be unavailable. For example, suppose PPP 1 is configured as an unnumbered interface that takes its IP address from the Ethernet 0/1 interface. If the Ethernet 0/1 interface goes down, the PPP 1 interface will be unavailable as well.

A loopback interface can be used to minimize the chances that the actual interface with the specified IP address will not go down. Loopback interfaces rarely, if ever, go down.

```
Example: (config)#interface loopback 1
         (config-loop 1)#ip address 10.1.1.1/ 24
         (config-loop 1)#interface ppp 1
         (config-ppp 1)#ip unnumbered loopback 1
```

Step 3: (Optional) Configure Secondary IP Addresses

Depending on the network setup, secondary address configuration may or may not be needed. If secondary addresses do not need to be configured for this PPP connection, go to Step 4.

Additional IP addresses may be configured on PPP interfaces, as needed. The most common reason for adding secondary addresses to WAN interfaces is for the configuration of port forwarding. Port forwarding allows users to make servers on a private network available to the Internet via public IP addresses. The configuration requires the publicly available IP addresses to be added to the router's WAN interface, usually as secondary addresses.

```
(config-ppp 1)#ip address <ip address> <subnet mask> secondary
```

<ip address> Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

<subnet mask> Specifies the subnet mask that corresponds to a range of IP addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation or prefix length.

Step 4: (Optional) Configuring PPP Authentication

PPP authentication is optional. If authentication is not required by the ISP or needed for this PPP connection, go to Step 5.

```
(config-ppp 1)#ppp authentication [pap | chap]
```

Select either PAP or CHAP to set the authentication type. Refer to the appropriate section below to complete authentication configuration.



The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not necessarily mean it also has to authenticate itself to the peer.

PAP

PAP is used to verify that the PPP peer is a permitted device by checking a user name and password configured on the peer. The user name and password are both sent unencrypted across the connecting private circuit. PAP requires a two-way handshake between peers. First, the router that is required to be authenticated (for instance, the peer) sends an authentication request with its user name and password to the router requiring authentication (for instance, the local router). The local router then looks up the user name and password in the user name database for the PPP interface and, if they match, sends an authentication acknowledge back to the peer.

To configure a PAP user name and password into the database of a local router to which the peer must authenticate, execute the following command in the local router on the appropriate PPP interface:

```
(config-ppp 1)#username <username> password <password>
```

To configure the PAP user name and password credentials to be used by the peer router to authenticate itself to a local router, execute the following command in the peer router:

```
(config-ppp 1)#ppp pap-sent username <username> password <password>
```

An example scenario is given below for clarity.

Configuring PAP Example: Only the local router requires the peer to authenticate itself.

On the local router (host name Local):

```
Local(config-ppp 1)#ppp authentication pap  
Local(config-ppp 1)#username farend password same
```

On the peer (host name Peer):

```
Peer(config-ppp 1)#ppp pap sent-username farend password same
```

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the user name and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching user name and password.

CHAP

CHAP is a three-way handshake authentication protocol composed of a challenge, a response, and a success or failure. The MD5 hashing algorithm is used to protect the password in the response.

First, the local router (requiring its peer to be authenticated) sends a challenge containing a random number to the peer. The peer combines its password with the random number to calculate a hash value using the MD5 algorithm. This calculated hash is sent from the peer back to the local router for authentication. The local router then compares the hash value from the peer to the hash it calculated locally based on the random number and the password for the given host name configured on the PPP interface. If the hashes match, the local router sends a success message back to the peer, if not a failure message will be sent.

To configure a CHAP user name and password into the database of a local router to which the peer must authenticate, execute the following command in the local router on the appropriate PPP interface:

```
(config-ppp 1)#username <username> password <password>
```

<username> By default, CHAP authentication uses a router's host name for the user name. Therefore, the peer router's host name should be entered as the user name in this command.

<password> The password set in the local router must match the password programmed into the peer router.

To configure CHAP password credentials to be used by the peer router to authenticate itself to a local router, execute the following command in the peer router:

```
(config-ppp 1)#ppp chap password <password>
```

<password> The password set in the peer router must match the password programmed into the local router.



*By default, CHAP authentication uses a router's host name for the user name. This is specified with the **hostname** <name> command in the Global Configuration mode.*

The router can be programmed to send a specified host name instead of its default host name with the following command:

```
(config-ppp 1)#ppp chap hostname <hostname>
```

Example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name Local):

```
Local(config-1)#ppp authentication chap  
Local(config-1)#username Peer password secret
```

On the peer (host name Peer):

```
Peer(config-1)#ppp chap password secret
```

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the user name and password expected to be sent from the peer. The peer uses its host name and the **ppp chap password** command to send the proper authentication information.



*The password configured on the peer with the **ppp chap password** <password> command must be identical to the password configured with the **username** <username> **password** <password> command on the local router.*

Configuring CHAP Example 2: Using the **ppp chap hostname** command as an alternate solution.

On the local router (host name Local):

```
Local(config-ppp 1)#ppp authentication chap  
Local(config-ppp 1)#username farend password secret
```

On the peer (host name Peer):

```
Peer(config-ppp 1)#ppp chap hostname farend  
Peer(config-ppp 1)#ppp chap password secret
```

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct host name in the challenge.



*For additional information and examples on configuring PAP and CHAP, please refer to the **AOS Command Reference Guide** available on the **AOS Documentation CD** shipped with your unit or online at www.adtran.com.*

Step 5: (Optional) Enable MLPPP

MLPPP is optional. If MLPPP is not used for this PPP connection, go to Step 6. More than one carrier line may be bundled to the same PPP interface for increased bandwidth and performance. MLPPP must be enabled on any PPP interface where multiple carrier lines will be bundled.

```
(config-ppp 1)#ppp multilink
```



*For additional MLPPP options, refer to **Enhancing MLPPP Performance** on page 21 of this document.*

Step 6: Activating the PPP Interface

Although this command activates the PPP interface, its status will not change until it is bound to the physical interface (refer to Step 7).

```
(config-ppp 1)#no shutdown
```


Step 7: Cross Connect the Physical Interface to the Virtual Interface

Next, associate the appropriate physical interface to the PPP interface, using the **cross-connect** command. The physical interface must be cross connected to the virtual interface so that the AOS device knows which data link layer protocol to use for that WAN connection. When a physical interface is cross connected to a virtual interface, the two are considered a single interface cross connect group. This guide assumes that the physical interface has already been configured.

If MLPPP is enabled, a **cross-connect** command should be issued for each carrier line that is to be bundled to the PPP interface (refer to example at the end of this step).

```
(config-ppp 1)#cross-connect <number> <from interface> <group number> <to interface>
```

<number> Identifies the cross connect using a number descriptor. Each cross connect within an AOS device must have a unique number. Range is 1 to 1024.

<from interface> Specifies the physical interface on one end of the cross connect. Specify an interface in the format *<interface type [slot/port | interface id]>*. To set up the PPP cross connect as outlined in this guide, it is likely that a T1, E1, DDS, serial, or SHDSL WAN interface will be specified as the from interface. For example, for a T1 interface, use **t1 1/1**. Enter **cross-connect 1 ?** for a list of all valid interfaces.

<group number> Optional. Specifies which configured TDM group to use for this cross connect. This subcommand only applies to T1 or E1 physical interfaces. To set up the PPP cross connect as outlined in this guide, use the same TDM group number assigned to the physical interface (see Table 2 or the *E1/T1 WAN Configuration Guide* for more details).

<to interface> Specifies the virtual interface on the other end of the cross connect. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. To set up the PPP cross connect as outlined in this guide, the interface number placed here should match the number assigned to the PPP interface in Step 1. Use the **?** to display a list of all valid interfaces.



You do not include a TDM group number when cross connecting a serial, HSSI, T3, SHDSL, or DDS interface to a virtual interface because they do not use TDM groups.

Multiple Cross Connect Statements for MLPPP

When issuing multiple cross connect statements for MLPPP, a new cross connect number should be used for each line. For example:

```
(config)#cross-connect 1 t1 1/1 1 ppp 1
```

```
(config)#cross-connect 2 t1 1/2 1 ppp 1
```



*Lines that will be aggregated may use the same or a different TDM group number. The bandwidth of each of the lines added to the MLPPP bundle does not have to be equal. However, varying transmission times across unequal links may cause bursty traffic. If it is necessary to bundle unequal bandwidth PPP lines, a better alternative would be load sharing across those lines with separate PPP interfaces versus multiple lines in a single MLPPP interface. Please refer to the document titled **Configuring IP Load Sharing in AOS** found at <http://kb.adtran.com> for more information on load sharing.*

The **cross-connect** command binds the virtual PPP interface to the physical WAN interface in the AOS product. The PPP interface can now attempt to negotiate a PPP session with its peer, and if that negotiation is successful, the status of the PPP interface will change to up. To view the status of or troubleshoot a PPP interface, please refer to *Troubleshooting* on page 52 of this guide.

Step 8: Exit the PPP Interface Configuration Menu and Save the Configuration

Issue the **exit** command once to leave the PPP interface configuration menu and return to the Global Configuration mode. Issue the **exit** command a second time to return to Enable mode, which is where the **copy running-config startup-config** command is issued to save the configuration.

```
(config-ppp 1)#exit
```

```
(config)#exit
```

```
#copy running-config startup-config
```



*The configuration may be saved directly from the PPP interface configuration menu or from the Global Configuration mode by typing the command **do copy running-config startup-config**.*

Additional Settings

Depending on the user's WAN environment, other settings may need to be configured on the PPP interface.

ACFC Accept-Compressed

Address and control field compression (ACFC) is a feature that can be applied during the LCP phase of PPP negotiation. When ACFC is negotiated, the HDLC header may be omitted on links that use HDLC encapsulation. By omitting the HDLC header, the framing overhead for each packet is reduced. The result is minor gains in bandwidth. ACFC must be used with caution, however, as the resulting re-alignment of data within the frame may impair the switching efficiency of the packets.

Use the **acfc accept-compressed** command to enable the AOS device to accept header compressed frames, even if compression is not negotiated. Compressed frames that are received are not dropped, but will still be logged as errors.

```
(config-ppp 1)#acfc-accept compressed
```

Bridging

Generally, routing should always be used across WAN links. However, some legacy equipment, such as point-of-sale devices and older medical equipment, do not support IP networking. AOS offers bridging as an option available for legacy applications that do not support IP routing.

Use the **bridge-group** *<number>* [**vlan-transparent**] command to assign an interface to the specified bridge group. This command is supported on all Ethernet interfaces, PPP virtual interfaces, and Frame Relay virtual subinterfaces. Use the **no** form of this command to remove an interface. Any two IP interfaces can be bridged (Ethernet to PPP virtual interface, VLAN to PPP virtual interface, etc.).

```
(config-ppp 1)#bridge-group <number>
```

<number> Specifies the bridge group (by number) this interface is to be assigned to. Range is 1 to 255.

The **vlan-transparent** parameter specifies that VLAN-tagged frames are passed across the PPP bridge link. For this function to work, it must be negotiated in BCP with the peer. If you are configuring the PPP bridge to pass VLAN-tagged frames, use the **bridge-group** *<number>* **vlan-transparent** command in conjunction with the **ppp bcp tagged-frame** command as follows:

```
(config-ppp 1)#bridge-group 1 vlan-transparent  
(config-ppp 1)#ppp bcp tagged-frame
```



*Several additional steps are needed to complete bridging configurations. Please refer to the document titled **Configuring Bridging in AOS** found at <http://kb.adtran.com> for more information on bridging.*

Description

You can add a description to the PPP interface if you want to document information about it. For example, if you have configured multiple PPP interfaces, you may want to document how each PPP interface is being used.

```
(config-ppp 1)#description <text>
```

<text> Identifies the specified interface using up to 80 alphanumeric characters. For example, you might enter:

```
(config-ppp 1)#description WAN link to Dallas office
```

This description is displayed when you enter the **show running-config** command or the **show interface ppp** command.

Keepalive

Use the **keepalive** command to enable the transmission of keepalive packets on the PPP interface and specify the time interval in seconds between transmitted packets. By default, the keepalive interval in AOS for PPP interfaces is 10 seconds.

```
(config-ppp 1)#keepalive <value>
```

<value> Defines the time interval (in seconds) between transmitted keepalive packets. Valid range is 0 to 32,767 seconds.

The keepalive interval must be set to the same value on devices at both ends of the PPP link. The shorter the keepalive interval, the faster an interface failure will be detected. The keepalive signal may be disabled by issuing the command **keepalive 0** on the PPP interface. However, this should only be done if the keepalive has also been disabled on the device at the other side of the point-to-point connection.



If five consecutive echo request keepalive messages are sent from the AOS device to a peer interface with no response, the interface is considered down and the PPP link will be terminated.

Maximum Transmission Unit (MTU)

The MTU defines the largest size that a PPP frame can be. If a frame exceeds this size, it must be fragmented. By default, the MTU for PPP interfaces is 1500 bytes.

(config-ppp 1)#**mtu** <size>

<size> Specifies the window size (in bytes) for transmitted packets. The valid range for PPP interfaces is 64 to 2100 except in the NetVanta 5305. The valid range for PPP interfaces in the NetVanta 5305 is 64 to 4600.



The valid MTU range for PPP interfaces to all interfaces was 64 to 1520 prior to AOS 14.1.

The MTU should be left at 1500 bytes for most environments. However, in some cases the MTU size may need to be adjusted. MTU size may need to be evaluated if:

- The interface is connected to another router that uses a different MTU size.
- The interface is used in a PPP over Ethernet (PPPoE) environment.

If the peer router uses a different MTU size across the PPP connection, transmissions and routing can be affected. For example, if the PPP peer is set to an MTU less than 1500 and the host router sends a packet that is 1500 bytes, the PPP peer will have to fragment the packet into separate PPP frames less than 1500 bytes. Furthermore, if the packet's IP header is tagged with the do not fragment field, then the peer router cannot forward the frame at all.

If open shortest path first (OSPF) routing has been enabled on the AOS product, caution should be exercised when setting the MTU. OSPF routers cannot become adjacent if their MTU sizes do not match. Ensure that the MTU is the same on both routers connected via PPP.



The negotiated maximum receive unit (MRU) in PPP is based on the MTU size configured for the PPP interface.

Peer Default IP

Use the **peer default ip address** command to specify the IP address of the remote peer of this interface. This command is useful if the peer does not send the IP address option during PPP negotiations.

```
(config-ppp 1)#peer default ip address <ip address>
```

<ip address> Specifies the default IP address for the remote end. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Use the **no** form of this command to remove an assigned IP address.

PPP BCP Tagged-Frame

Use the **ppp bcp tagged-frame** command to allow negotiation of IEEE 802.1Q-tagged packets over BCP. This option enables a VLAN identifier (VID) to be conveyed, facilitating consistent VLAN classification of the frame across the PPP link and enabling segregation of frames assigned to different VLANs.

```
(config-ppp 1)#ppp bcp tagged-frame
```

To pass VLAN-tagged frames across a bridged PPP link, the **ppp bcp tagged-frame** command must be used in conjunction with the **bridge-group <number> vlan-transparent** command in the PPP interface configuration to enable negotiation in BCP with the peer. Enter the commands as follows:

```
(config-ppp 1)#bridge-group 1 vlan-transparent  
(config-ppp 1)#ppp bcp tagged-frame
```

Enhancing MLPPP Performance

Several options are available to enhance the performance of MLPPP operation. A MLPPP bundle will remain active with a minimum of one physical link. Physical links are dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Fragmentation

Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. These data fragments are then transmitted simultaneously over each link and reassembled at the receiving end.

```
(config ppp-1)#ppp multilink fragmentation
```



The MRRU for MLPPP is hard set at 1520 bytes.

Interleave

If streaming protocols are used across the MLPPP connection, it may be beneficial to enable MLPPP interleave. Certain types of high priority packets may be adversely affected if they are transmitted over an MLPPP connection. When interleave is enabled, the interface handles high priority packets differently. Instead of being encapsulated as MLPPP traffic, high priority packets are encapsulated as PPP and sent to the next available link. Unlike multilink fragmentation, delivery is not guaranteed with multilink interleave operation.

High priority packets are defined at both the system level and user level in AOS. The priority of system level packets (e.g., OSPF Hello packets and Frame Relay signaling packets) is permanently set in AOS and cannot be changed by configuration. The priority of a user level packet (e.g., RTP traffic) is defined in AOS using a quality of service (QoS) map. A QoS map can be defined with a “Priority” flow and applied to the PPP interface. Packets that match the flow definition are marked as user level priority packets and are allowed to be interleaved as described above.



Since priority packets are encapsulated as regular PPP packets, they must be smaller than the configured MTU value for the PPP connection. Any priority packet larger than the MTU will be dropped.



*For more information on QoS maps, please refer to **Understanding AOS Queuing** available on the **AOS Documentation** CD shipped with your unit or online at <http://kb.adtran.com>.*

(config ppp-1)#**ppp multilink interleave**

Maximum Number of Links

Specifies the maximum number of links the user wants to allow in a PPP multilink bundle.

(config ppp-1)#**ppp multilink maximum** <number>

Table 1 on page 9 lists the maximum number of PPP links per bundle that are allowed per product.

GUI Configuration

The Web-based graphical user interface (GUI) is an especially useful tool for those who are less familiar with the command line interface (CLI) configuration. AOS products ship standard with a user-friendly GUI that can be used to perform many basic management and configuration functions on the AOS product. Some advanced options are configurable via the GUI as well.

Open a GUI session. If you need assistance, refer to the quick configuration guide specific to your AOS product available on the *AOS Documentation* CD shipped with your unit or online at www.adtran.com.

The screenshot shows the NetVanta 3200 GUI. The left-hand navigation menu is expanded to show the 'System' section, with 'Setup Wizard' highlighted. The main content area displays 'General System Information' with the following details:

General System Information	
Firmware Version	15.09.00.E
Part Number	1202860L1
Serial Number	LBADTN0453AA128
System Uptime	5 days, 12 hours, 21 minutes, 0 seconds
System Time	09:38:55 PM CST
System Date	April 28, 2008
Memory	Total Heap: 12,397,552 Bytes Free Heap: 5,704,688 Bytes
CPU Utilization	System Load: 9.88% 1 Min Avg Load: 19.18% 5 Min Avg Load: 14.13% Min Load: 0% Max Load: 79.42% Context Switch Load: 0.46%
File System	Total: 14,496,104 Bytes Used: 6,643,056 Bytes Free: 7,853,048 Bytes
SNTP Time Server	(Not Configured)


At the bottom of the main content area, there is a 'Clear CPU Max Load' button and a 'Refresh in 3 seconds...' indicator.

Figure 5. System Summary Menu

Once a successful connection to the GUI has been established, the main landing page appears.

A setup wizard option is available in the NetVanta 340, 3200, 3430, and 3448. Select **Setup Wizard** from the left-hand menu in the GUI. The same wizard is available in the Total Access 900(e) Series and NetVanta 6355, but it is called a **Configuration Wizard**. The wizard will guide a system administrator through setup of the most common PPP configurations. However, if the system administrator prefers to configure PPP without going through the wizard, the following step-by-step process mimics the configuration outlined in *Advanced CLI Configuration* on page 10 of this document.



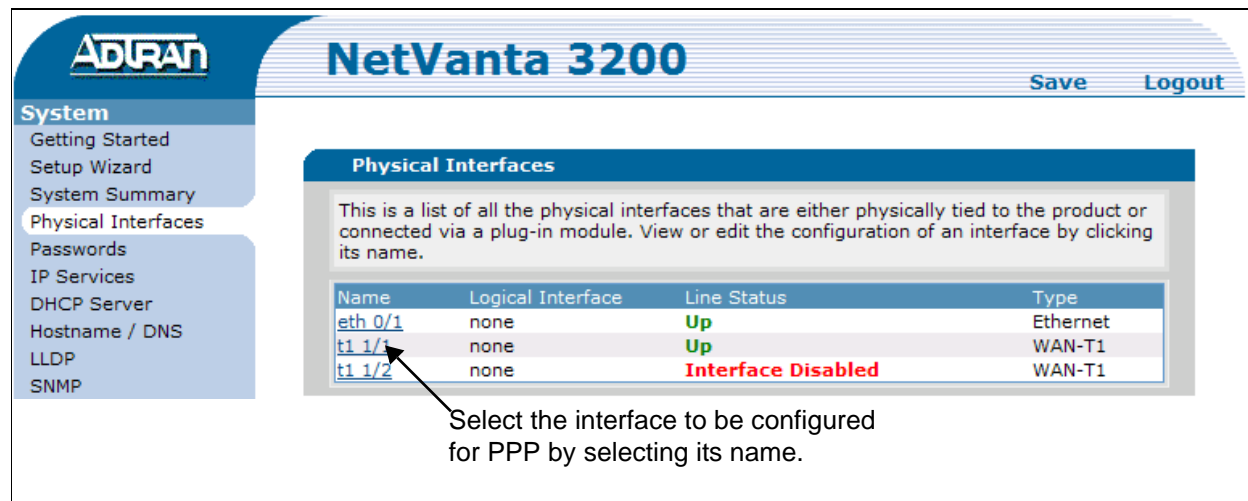
While navigating the GUI you will notice question mark  symbols that indicate additional information is available. Simply place your cursor over the symbol to view the additional information.

Step 1

Select **Physical Interfaces** from the left-hand menu in the GUI. A list of all the physical interfaces on the AOS product is available. Select the interface to be configured for PPP by selecting its name (see Figure 6). For example purposes only, this tutorial will demonstrate the configuration of the interface **t1 1/1**.



A virtual interface (i.e., PPP 1) that has already been created will appear as a hyperlink listed under the **Logical Interface** heading. This link will allow direct access to configuration menus for the virtual interface.



ADTRAN NetVanta 3200 Save Logout

System

- Getting Started
- Setup Wizard
- System Summary
- Physical Interfaces**
- Passwords
- IP Services
- DHCP Server
- Hostname / DNS
- LLDP
- SNMP

Physical Interfaces

This is a list of all the physical interfaces that are either physically tied to the product or connected via a plug-in module. View or edit the configuration of an interface by clicking its name.

Name	Logical Interface	Line Status	Type
eth 0/1	none	Up	Ethernet
t1 1/1	none	Up	WAN-T1
t1 1/2	none	Interface Disabled	WAN-T1

Select the interface to be configured for PPP by selecting its name.

Figure 6. Physical Interfaces Menu

Step 2



The physical interface GUI menu in the Total Access 900(e), NetVanta 6355, and NetVanta 7000 Series is different than the NetVanta 3200 GUI menu shown in Figure 7 on page 26. Please refer to the latter part of this step to find information applicable to the GUI in the products listed above.

The GUI now displays the physical interface configuration options for **t1 1/1** (see *Figure 7 on page 26*). Select the number of **Data DS0s** on this T1 that are to be mapped to the ppp interface. All DS0s or a contiguous fraction of DS0s may be activated for data. Select the button next to **PPP** to set the encapsulation type. To enable the interface, ensure that a check mark appears in the box next to **Enable**.



This page is a good place to double check all other physical parameters (e.g., clocking, framing, coding, etc.) for the interface.

MLPPP

If more than one carrier line will be bundled to this PPP interface for increased bandwidth, then select the box to the right of **Multilink** and ensure that a green check mark appears.



MLPPP is only available on units that allow more than one physical interface to be connected (see Table 1 on page 9).

Select **Apply** to apply the settings. The PPP Configuration menu (see page 29) appears.

The screenshot displays the NetVanta 3200 GUI configuration page for the Physical Interfaces section, specifically for interface T1 1/1. The page title is "NetVanta 3200" and the breadcrumb is "Physical Interfaces > T1 1/1". The left sidebar shows a navigation menu with categories: System, Physical Interfaces, Router / Bridge, Firewall, VPN, and Utilities. The main configuration area is titled "Configuration for 'T1 1/1'" and contains the following settings:

Field	Value	Description / Note
Description:	To ISP	Description label (optional)
Enable:	<input checked="" type="checkbox"/>	Enable or disable this interface.
Clocking:	Line	Select the source timing for this interface
Framing:	ESF	Select the framing that matches the network provider framing format.
Coding:	B8ZS	Select the coding that matches the network provider line coding.
FDL:	ANSI	Select the format for the facility data link channel.
Data DS0s:	1 to 24	Select the DS0s to map to the Router.
DSX-1 Map:	None	DS0s mapped to the DSX-1 port
DS0 Speed:	64Kbps	Select the speed for the DS0s in the DS0 Map.
Encapsulation:	<input checked="" type="radio"/> PPP <input type="radio"/> Frame Relay <input type="radio"/> HDLC	Interface connects to a PPP, Frame Relay, or HDLC circuit
Multilink:	<input type="checkbox"/>	Enable multilink for the selected encapsulation.

Buttons for "Reset" and "Apply" are located at the bottom of the configuration area.

Figure 7. Physical Interfaces Configuration Menu (NetVanta 3200)

Total Access 900(e), NetVanta 6355, and NetVanta 7000 Series GUI

In Figure 8 on page 27, the physical interface configuration options are displayed for **t1 0/1**. The top part of the page lists various physical parameters that should have already been configured for the T1 interface. However, it is always recommended to double check the settings.

The next section contains options for configuring PPP. Select **PPP** from the **Connect To** drop-down menu. Next, select the number of data DS0s on this T1 that are to be mapped to the PPP interface. All DS0s or a contiguous fraction of DS0s may be activated for data. Finally, choose the speed of the DS0s in the **Speed** drop-down menu.

MLPPP

If more than one carrier line will be bundled to this PPP interface for increased bandwidth, then select the box to the right of **Multilink** and ensure that a green check mark appears.



MLPPP is only available on units that allow more than one physical interface to be connected (see Table 1 on page 9).

Select **Add** to add a connection. The PPP Configuration menu (see page 29) appears.

The screenshot displays the ADTRAN Total Access 904 configuration interface. The left sidebar contains a navigation menu with categories: System (Config Wizard, System Summary, Physical Interfaces, Passwords, IP Services, DHCP Server, Hostname / DNS, LLDP, SNMP), Voice, Data, and Utilities. The main content area is titled 'Physical Interfaces > t1 0/1' and includes 'Save' and 'Logout' buttons.

Configuration for "t1 0/1"

Basic configuration for the T1 interface.

Description:	<input type="text"/>	Description label (optional)
Enable:	<input checked="" type="checkbox"/>	Enable or disable this interface
Clocking:	Line	
Framing:	ESF	Select the framing that matches the network provider framing format
Coding:	B8ZS	Select the coding that matches the network provider line coding
FDL:	ANSI	Select the format for the facility data link channel

Buttons: Reset, Apply

Configured DS0 Connections for "t1 0/1"

Use this dialog to connect a group of DS0's to a particular interface or service provided by this unit. To configure a connected interface's settings, click on the item in the list below. To remap a group of DS0's that are currently in use, click the delete button to remove the connections group.

Add a Connection

Connect To:	PPP	Select an interface type to map to the DS0s
Available DS0 Range:	1-24	
DS0 Range:	1 to 20	Set the range of DS0s to be mapped
Speed:	64kbps	Select the speed for the DS0s being mapped

Button: Add

Connected Interface	DS0's Used	Group Number	Speed
There are no connections configured			

Figure 8. Physical Interfaces Configuration Menu (Total Access 904)

Step 3

The top part of the **PPP Configuration** menu (see Figure 9 on page 29) contains basic PPP control settings, such as whether or not the interface is enabled, choice of queuing method, MTU size, etc. An optional description of this PPP link may be entered.

Authentication Settings (Optional)

If authentication is required for a PPP connection to the remote peer (such as your ISP), choose the type of authentication (**PAP** or **CHAP**) next to **Sent Authentication Type**. Next, enter the appropriate **Sent Username** and **Sent Password** credentials. Depending on whether the PPP connection is between two office locations or an ISP and a user, user name and password credentials will either be previously agreed upon or simply supplied by the ISP.

By selecting **PAP** or **CHAP** for **Peer Authentication Type**, the unit can also be set up to require authentication from peers before a PPP connection is allowed to be established. The **Peer Username** and **Peer Password** entered into the fields that follow are placed into the PPP database and referenced when verifying PAP or CHAP peer credentials.



*For more in-depth explanations on PPP authentication types, refer to Step 3 in the section **Advanced CLI Configuration** on page 10 of this document.*

The screenshot displays the configuration interface for a NetVanta 3200 router. The breadcrumb path is "Physical Interfaces > t1 1/1 > PPP Config". The main content area is titled "PPP Configuration for 'ppp 1'" and is divided into two sections: "Basic configuration for the PPP interface" and "Authentication Settings".

Basic configuration for the PPP interface:

- Description: [Text Input] *Description label (optional)*
- Enabled: *Enable data flow for this interface.*
- Weighted Fair Queuing: *If disabled, FIFO queuing method will be used.*
- MTU: [1500] *Maximum Transmit Unit*
- Physical Interface: **t1 1/1** *Physical interface connection for this interface.*
- Qos-policy: **None** *Outbound QoS-Policy map.*
- Default Peer IP Address: *Set an IP address for the remote end of this interface (optional).*

Authentication Settings:

- Sent Authentication Type: [None] *Used by the remote peer to authenticate this unit*
- Sent Username: [Text Input] *Required when unit must authenticate to the remote peer*
- Sent Password: [Text Input] *Transmitted to the remote peer*
- Confirm Sent Password: [Text Input] *You must enter the new password again to guarantee accuracy.*
- Peer AuthenticationType: [None] *Used when authenticating remote peers*
- Peer Username: [Text Input] *Required when remote peer must authenticate to this unit*
- Peer Password: [Text Input] *Received from the remote peer*
- Confirm Peer Password: [Text Input] *You must enter the new password again to guarantee accuracy.*

Figure 9. PPP Configuration Menu

Step 4

IP Settings

The **IP Settings** configuration is located toward the bottom of the page (displayed after selecting **Apply** in Step 2, or simply scrolling further down from the **Authentication Settings** in Step 3). Choose the type of IP address the AOS device will have: **none**, **static**, **unnumbered**, or **negotiated**. Each IP address type displays a different set of options that accompany the setting. Secondary IP addresses for the PPP interface are entered here by selecting on the link that says **Add a new Secondary IP Address**.

NOTE

*The option to add secondary IP addresses in the Total Access 900(e), NetVanta 6355, and NetVanta 7000 Series menus does not appear until you have configured the initial **IP Settings** and selected **Apply**.*

NOTE

*Refer to Step 2 in **Basic PPP Interface Setup** on page 11 under the **Advanced CLI Configuration** section of this document for detailed information on each of the different IP settings and how they are used.*

None

The **Address Type** should be set to **None** if you are connecting to a bridge with IP routing disabled.

The screenshot shows the 'IP Settings' configuration page. The 'Address Type' dropdown menu is set to 'None'. To the right of this dropdown is a note: 'Set to 'None' if connecting to a Bridge with IP routing disabled.' Below this, the 'Dynamic DNS' dropdown is set to '<disabled>', with a note: 'Used to register this interface's IP address with a DNS Name.' The 'Secondary IP Settings' section contains a table with columns 'IP Address' and 'Mask'. Below the table is a link: 'Add a new Secondary IP Address'. At the bottom of the form are 'Reset' and 'Apply' buttons.

Figure 10. IP Address Type None

Static

The **Address Type Static** is a fixed address assigned to the PPP interface by a user.

The screenshot shows the 'IP Settings' configuration window. The 'Address Type' is set to 'Static'. The IP Address is 208.61.209.1 and the Subnet Mask is 255.255.255.248. Dynamic DNS is set to '<disabled>'. The 'Secondary IP Settings' section is empty. There are 'Reset' and 'Apply' buttons at the bottom.

IP Settings		
Address Type:	Static	Set to 'None' if connecting to a Bridge with IP routing disabled.
IP Address:	208 . 61 . 209 . 1	IP address for this numbered interface
Subnet Mask:	255 . 255 . 255 . 248	Subnet Mask for this numbered interface
Dynamic DNS:	<disabled>	Used to register this interface's IP address with a DNS Name.
Secondary IP Settings		
IP Address	Mask	
Add a new Secondary IP Address		
		Reset Apply

Figure 11. IP Address Type Static

Unnumbered

The **Address Type Unnumbered** allows the IP address of another interface on the AOS device to also be used as the IP address of the PPP interface. See *Unnumbered Interface* on page 12 for more information on the use of unnumbered interfaces.

The screenshot shows the 'IP Settings' configuration window. The 'Address Type' is set to 'Unnumbered'. The 'Interface' is set to 'eth 0/1'. Dynamic DNS is set to '<disabled>'. The 'Secondary IP Settings' section is empty. There are 'Reset' and 'Apply' buttons at the bottom.

IP Settings		
Address Type:	Unnumbered	Set to 'None' if connecting to a Bridge with IP routing disabled.
Interface:	eth 0/1	The 'eth 0/1' interface will be associated with this unnumbered IP interface.
Dynamic DNS:	<disabled>	Used to register this interface's IP address with a DNS Name.
Secondary IP Settings		
IP Address	Mask	
Add a new Secondary IP Address		
		Reset Apply

Figure 12. IP Address Type Unnumbered

Negotiated

The **Address Type Negotiated** allows WAN connections used for Internet access to be configured so that the PPP interface will negotiate an IP address with the ISP's router. The user's ISP can confirm if this type of setup is needed. This should also be selected if the peer router is configured to assign an IP address to the local router.

The screenshot displays the 'IP Settings' configuration window. The 'Address Type' dropdown menu is set to 'Negotiated'. To the right of this dropdown is a help text: 'Set to 'None' if connecting to a Bridge with IP routing disabled.' Below this, the 'Default Route' checkbox is unchecked, with a help text: 'Add a default route to the route table.' The 'Dynamic DNS' dropdown is set to '<disabled>', with a help text: 'Used to register this interface's IP address with a DNS Name.'

Below the 'IP Settings' section is the 'Secondary IP Settings' section. It contains a table with two columns: 'IP Address' and 'Mask'. The first row of the table is a blue header. The second row is a text input field containing the text 'Add a new Secondary IP Address'. At the bottom of the 'Secondary IP Settings' section are two buttons: 'Reset' and 'Apply'.

Figure 13. IP Address Type Negotiated

Media Gateway

The option to designate the PPP interface as a **Media Gateway** is available in the **IP Settings** menu for for voice products as well as a number of data products. Refer to the AOS Feature Matrix, article #2272, found at <http://kb.adtran.com> for the most current listing of products that support this option.

The Media Gateway option is used in conjunction with the SIP Transparent Proxy feature. If the PPP interface is the outbound interface used to connect to the Session Initiation Protocol (SIP) server, then the media gateway option should be set to **primary**. This setting should be enabled for all interfaces on the unit where voice traffic sourcing is desired. Refer to *Configuring SIP Transparent Proxy in AOS*, article #2183, found at <http://kb.adtran.com> for more information on SIP Transparent Proxy.

The screenshot shows a configuration window with two main sections: **Media-Gateway** and **Monitoring**. In the **Media-Gateway** section, the 'IP Address Type' is set to 'None' in a dropdown menu. To the right of this dropdown is the text: 'RTP traffic will flow over the selected IP address.' In the **Monitoring** section, the 'RTP Monitoring' checkbox is unchecked. To the right of this checkbox is the text: 'Enables RTP monitoring on this interface.' At the bottom of the window are two buttons: 'Reset' and 'Apply'.

Figure 14. Media Gateway

Step 5

Upon completing all applicable fields for **PPP Authentication** and **IP Settings**, select **Apply**. Basic PPP interface configuration is now complete. The GUI menu will refresh itself. Scroll to the bottom of the menu to view the status of the PPP interface (see Figure 15). If the peer end of the PPP connection has already been properly configured, the PPP interface's **Link State** and **LCP State** status should change to **Up**.

Status for "ppp 1"	
Port Status	
Connected Interface	t1 1/1
Link State	Up
LCP State	UP
IP Address	65.162.109.202
Peer IP Address	65.162.109.201
Queueing method	weighted fair queue
HDLC tx ring limit	2
Output queue (size/highest/max total/threshold/drops)	0/1/460/64/0
Conversations (active/max active/max total)	0/1/256
Line Statistics	
Five Minute Input Rate in bits/s (pkts/sec)	80 (0)
Five Minute Output Rate in bits/s (pkts/sec)	72 (0)
Input Packets (bytes)	244 (6594)
Input Errors	0
Input Discards	0
Output Packets (bytes)	864 (14728)
Output Errors	0
Output Discards	0
<input type="button" value="Clear Statistics"/>	
Refresh in 3 seconds...	

Figure 15. Status Menu

Upon completion of PPP configuration in the GUI, be sure to save all changes to nonvolatile random access memory (NVRAM). This is accomplished by selecting the word **Save** in the upper right-hand corner of the screen.

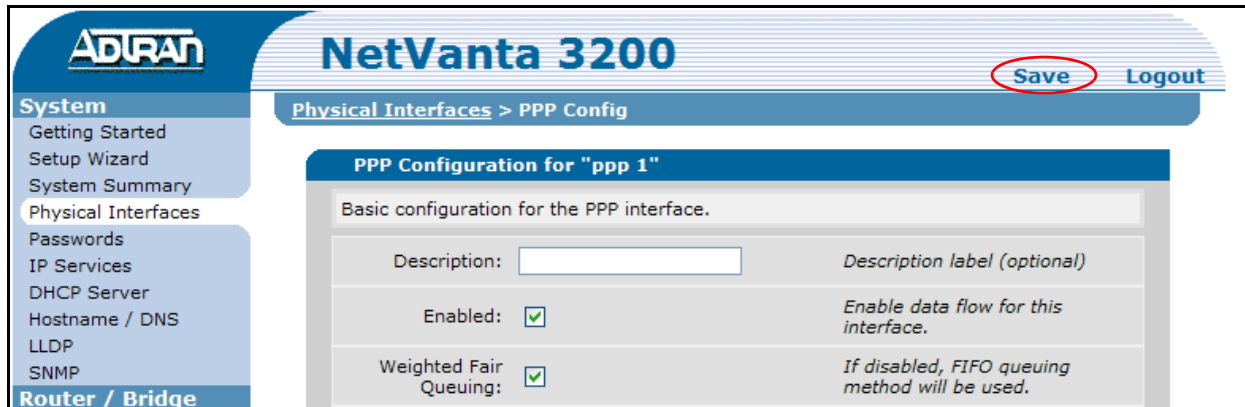


Figure 16. Save the Configuration

Example Configurations

The example scenarios contained within this section are designed to enhance understanding of PPP and MLPPP configurations on AOS products.

Some commands shown in the example configurations in this guide are already enabled as the default setting in the unit. These commands will not appear in the output when the **show running-config** command is issued. Issue the **show run verbose** command to see all commands (including those that do not appear when the **show running-config** command is issued).

Integrated Switch-Router Configuration Versus Nonintegrated Switch-Router

Configuration of the IP address and firewall access policies on the private LAN interface differs slightly depending on the type of AOS product. The IP address and firewall commands are placed on the private LAN Ethernet interface on nonintegrated switch-router products, such as the NetVanta 3200 and 3430. The *Advanced CLI Configuration* outlined in this guide, as well as the majority of the examples provided in the *Example Configurations* section, applies to nonintegrated switch-router products. Configuration of the IP address and firewall access policies on integrated switch-router products, such as the NetVanta 6355 varies in that the commands are issued on the appropriate VLAN interface(s) as opposed to the private Ethernet interface. An additional step is required to associate switchport* interfaces to the appropriate VLAN that corresponds with the physical setup of the network. The example configuration below assigns the switchport 0/1 interface to VLAN 1.

```
!  
interface vlan 1  
    ip address 192.168.0.1 255.255.255.0  
    access-policy Private  
    no shutdown  
!  
interface switchport 0/1  
    switchport access vlan 1  
    no shutdown  
!
```

* Some switch-router AOS products, such as the NetVanta 1224R Series, label the switchport interfaces *interface ethernet 0/x* instead of *interface switchport 0/x*, where x is a variable from 1 to 24 depending on the product.



Refer to Example 2 to see an integrated switch-router product example configuration for the NetVanta 3448.

Example 1: PPP to an ISP with AOS Device and External Firewall

PPP is commonly used across a T1 connection between an ISP and its customer. The following configuration example has an external firewall that is connected to Ethernet 0/1 on the AOS product. The external firewall will perform all security functions, including network address port translation (NAPT) and port forwarding. A virtual interface, PPP 1, defines parameters for the PPP connection, such as how the IP address is assigned and any authentication options. The customer's WAN IP address (65.162.109.202 /30) is statically assigned and no authentication will be required for the PPP connection. All 24 DS0s on the WAN connection will be used for this PPP connection. One public IP address (208.61.209.1 /29) will be assigned to Ethernet port 0/1 on the AOS product. Another public IP address from the public block (208.61.209.2 /29) will be assigned to the external firewall. A default route that points to interface PPP 1 is added to the route table in the AOS product. The external firewall will need to have its default route pointing to the public IP address assigned to the AOS product's Ethernet 0/1 interface (208.61.209.1).

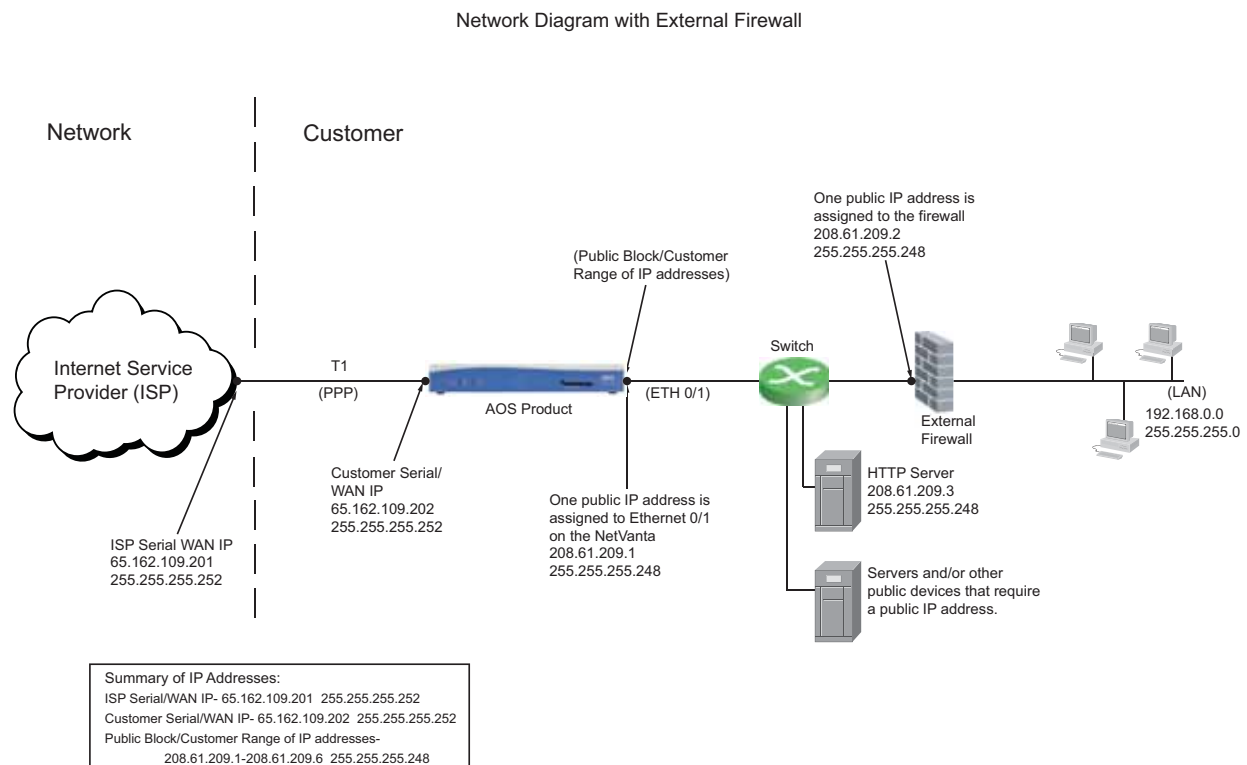


Figure 17. A PPP Connection to an ISP with an External Firewall on the Customer's LAN

The following configuration applies to Example 1:

```
!  
interface eth 0/1  
    ip address 208.61.209.1 255.255.255.248  
    no shutdown  
!  
interface t1 1/1  
    clock source line  
    tdm-group 1 timeslots 1-24 speed 64  
    no shutdown  
!  
interface ppp 1  
    ip address 65.162.109.202 255.255.255.252  
    no shutdown  
    cross-connect 1 t1 1/1 1 ppp 1  
!  
ip route 0.0.0.0 0.0.0.0 ppp 1  
!
```

Example 2: PPP to an ISP with AOS Device (Utilizing the Internal Firewall Capabilities)

PPP is commonly used across a T1 connection between an ISP and its customer. The following configuration example utilizes the built-in firewall capabilities of the AOS product to perform security functions, including NAPT, 1:1 NAT, and port forwarding. The customer's WAN IP address will be negotiated from the ISP's router. Through the internal firewall, 1:1 NAT or port forwarding is used for any public IP addresses that are assigned to servers and/or public devices that sit on the private side of the AOS product. This example shows an HTTP server with a private IP address (192.168.0.2 /24) receiving port forwards from public IP address 208.61.209.1 /29. The public IP address is entered as a secondary IP address on the WAN PPP interface. NAPT is also used to provide Internet access to devices on the LAN. CHAP authentication is used by the ISP to verify the PPP connection from the customer. The customer is provided a CHAP user name (USERNAME) and password (PASSWORD) to be programmed into the AOS product. The ISP router will not need to authenticate itself to the customer's router. All 24 DSOs on the WAN connection will be used for the PPP connection.

NOTE *Sample configurations for this example are provided for both the NetVanta 3430, a nonintegrated switch-router product and NetVanta 3448, an integrated switch-router product. Refer to the beginning of this section for more information on the configuration differences between these two types of products.*

NOTE *Please refer to the document titled **Configuring Port Forwarding in AOS**, found at <http://kb.adtran.com>, for information on port forwarding, 1:1 NAT, and other firewall features.*

Network Diagram with NetVanta Firewall

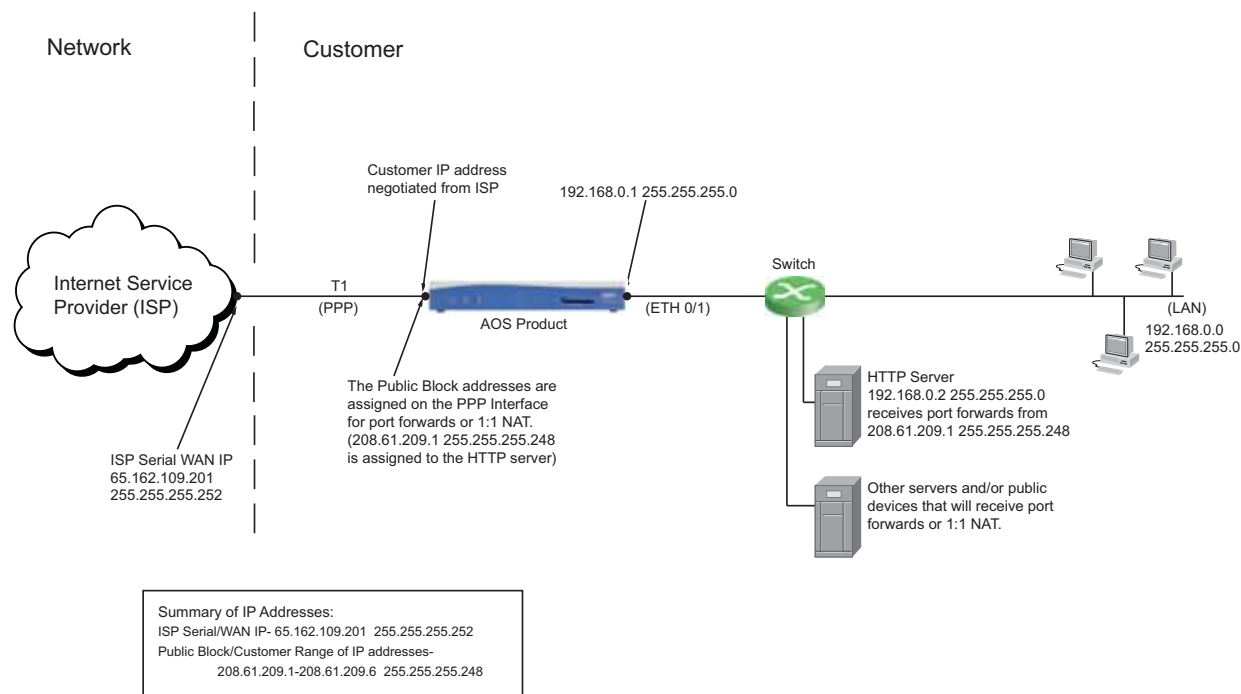


Figure 18. A PPP Connection to an ISP with the Built-in Firewall of the AOS Device

The following configuration applies to Example 2:

NetVanta 3430

```
!  
ip firewall  
ip firewall nat-preserve-source-port  
!  
interface eth 0/1  
    ip address 192.168.0.1 255.255.255.0  
    access-policy Private  
    no shutdown  
!  
interface t1 1/1  
    clock source line  
    tdm-group 1 timeslots 1-24 speed 64  
    no shutdown  
!  
interface ppp 1  
    ip address negotiated  
    ip address 208.61.209.1 255.255.255.248 secondary  
    access-policy Public  
    ppp chap hostname USERNAME  
    ppp chap password PASSWORD  
    no shutdown  
    cross-connect 1 t1 1/1 1 ppp 1  
!  
ip access-list standard MATCHALL  
    permit any  
!  
ip access-list extended WEB-IN  
    permit tcp any host 208.61.209.1 eq www  
!  
ip access-list extended WEB-OUT  
    permit ip host 192.168.0.2 any  
!  
ip policy-class Private  
    allow list MATCHALL self  
    nat source list WEB-OUT address 208.61.209.1 overload  
    nat source list MATCHALL interface ppp 1 overload  
!  
ip policy-class Public  
    nat destination list WEB-IN address 192.168.0.2  
!
```




The default route will be learned from the ISP when an IP address is assigned to the PPP interface.



*The commands **ip firewall nat-preserve-source-port** and **clock source line** are enabled by default. Therefore, these commands will not appear in the output when the **show running-config** command is issued.*



*If the unit terminating the PPP connection at the ISP is an AOS device, then the customer's WAN IP address is configured into the ISP's unit using the following command: **peer default IP address <ip address>**. This assignment will be transparent to the customer; however, the system administrator only needs to enter the command **ip address negotiated** into the local unit, as shown in the configuration example above.*

NetVanta 3448

```
!  
ip firewall  
ip firewall nat-preserve-source-port  
!  
interface switchport 0/1  
    switchport access vlan 1  
    no shutdown  
!  
interface t1 1/1  
    clock source line  
    tdm-group 1 timeslots 1-24 speed 64  
    no shutdown  
!  
!  
interface vlan 1  
    ip address 192.168.0.1 255.255.255.0  
    access-policy Private  
    no shutdown  
!  
interface ppp 1  
    ip address negotiated  
    ip address 208.61.209.1 255.255.255.248 secondary  
    access-policy Public  
    ppp chap hostname USERNAME  
    ppp chap password PASSWORD  
    no shutdown  
    cross-connect 1 t1 1/1 1 ppp 1  
!  
ip access-list standard MATCHALL  
    permit any  
!  
ip access-list extended WEB-IN  
    permit tcp any host 208.61.209.1 eq www  
!  
ip access-list extended WEB-OUT  
    permit ip host 192.168.0.2 any  
!  
ip policy-class Private  
    allow list MATCHALL self  
    nat source list WEB-OUT address 208.61.209.1 overload  
    nat source list MATCHALL interface ppp 1 overload  
!  
ip policy-class Public  
    nat destination list WEB-IN address 192.168.0.2  
!
```



The default route will be learned from the ISP when an IP address is assigned to the PPP interface.



The commands **switchport access vlan 1**, **ip firewall nat-preserve-source-port**, and **clock source line** are enabled by default. Therefore, these commands will not appear in the output when the **show running-config** command is issued.



If the unit terminating the PPP connection at the ISP is an AOS device, then the customer's WAN IP address is configured into the ISP's unit using the following command: **peer default IP address <ip address>**. This assignment will be transparent to the customer; however, the system administrator only needs to enter the command **ip address negotiated** into the local unit, as shown in the configuration example above.

Example 3: PPP from Central Corporate to a Branch Office

PPP can be used across the connection between a central corporate office and a remote branch office. The distance between the two locations is transparent, with clients on the remote LAN operating seamlessly with clients and resources on the corporate LAN. Internet access for the remote office is also funneled through the corporate office and across the PPP connection. The following configuration example utilizes private static IP addresses at each end of the PPP link (10.0.0.1 /30 at corporate and 10.0.0.2 /30 at the branch office). No authentication is used for this PPP connection. Clocking on the T1 interface is provided by the AOS product at the corporate location. Each LAN is assigned a different subnet (192.168.1.0 /24 at corporate and 192.168.2.0 /24 at the branch office). The remote office is programmed with a default route that points to the PPP interface. This route ensures that Internet and other traffic destined for the corporate LAN is directed to the proper place. The default route programmed into the corporate AOS product points toward the corporate Internet router connected to the ISP (192.168.1.254). A static route programmed into the corporate router ensures that traffic destined for the remote LAN (192.168.2.0 /24) is directed toward the PPP interface on the remote router (10.0.0.2).

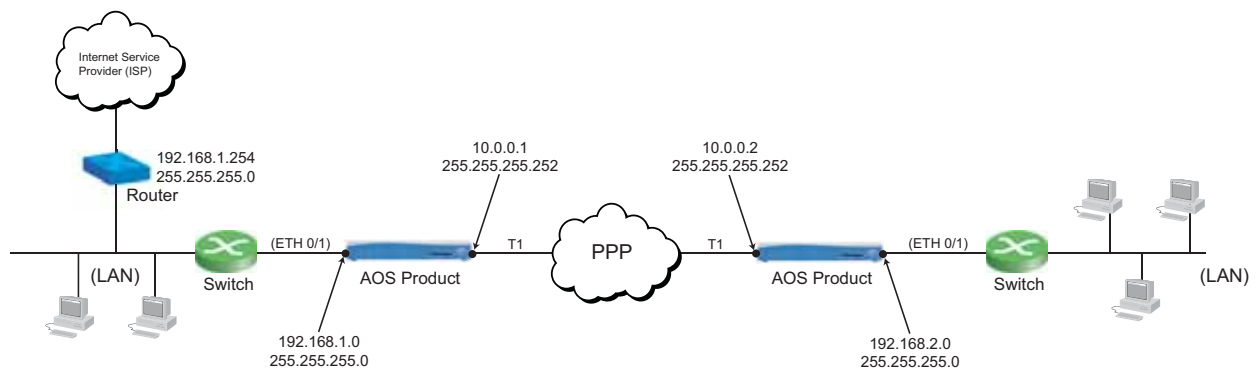


Figure 19. A PPP Connection from Central Corporate to a Branch Office

The following configuration applies to Example 3:

Central Office

```
!
interface eth 0/1
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
interface t1 1/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.0.0.1 255.255.255.252
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.2.0 255.255.255.0 ppp 1
!
```

Remote Office

```
!
interface eth 0/1
  ip address 192.168.2.1 255.255.255.0
  no shutdown
!
interface t1 1/1
  clock source line
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.0.0.2 255.255.255.252
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
```

The corporate Internet router (192.168.1.254) must be configured with the following routes:

```
ip route 192.168.2.0 255.255.255.0 192.168.1.1
ip route 10.0.0.0 255.255.255.252 192.168.1.1
```



*The command **clock source line** is enabled by default. Therefore, this command will not appear in the output when the **show running-config** command is issued.*

Example 4: MLPPP to an ISP with AOS Device and External Firewall

MLPPP is used to achieve higher bandwidth across multiple T1 connections to an ISP. In the following example, virtual interface, **PPP 1**, defines parameters for the PPP connection, such as how the IP address is assigned, authentication options, and the MLPPP settings. The customer's WAN IP address (65.162.109.202 /30) is statically assigned and no authentication is required for the PPP connection. All 24 DS0s on the WAN connection are used for this PPP connection. MLPPP is enabled with no enhancements.

Commands are issued on interfaces T1 1/1 and 1/2 to ensure that clocking is only recovered from the T1 line on interface T1 1/1. As shown in Example 1, this configuration example utilizes an external firewall that is connected to Ethernet 0/1 on the AOS product. The external firewall performs all security functions, including NAT and port forwarding. One public IP address (208.61.209.1 /29) is assigned to Ethernet port 0/1 on the AOS product. Another public IP address from the public block (208.61.209.2 /29) is assigned to the external firewall. A default route that points to interface **PPP 1** is added to the route table in the AOS product. The external firewall needs to have its default route pointing to the public IP address assigned to the AOS product's Ethernet 0/1 interface (208.61.209.1).

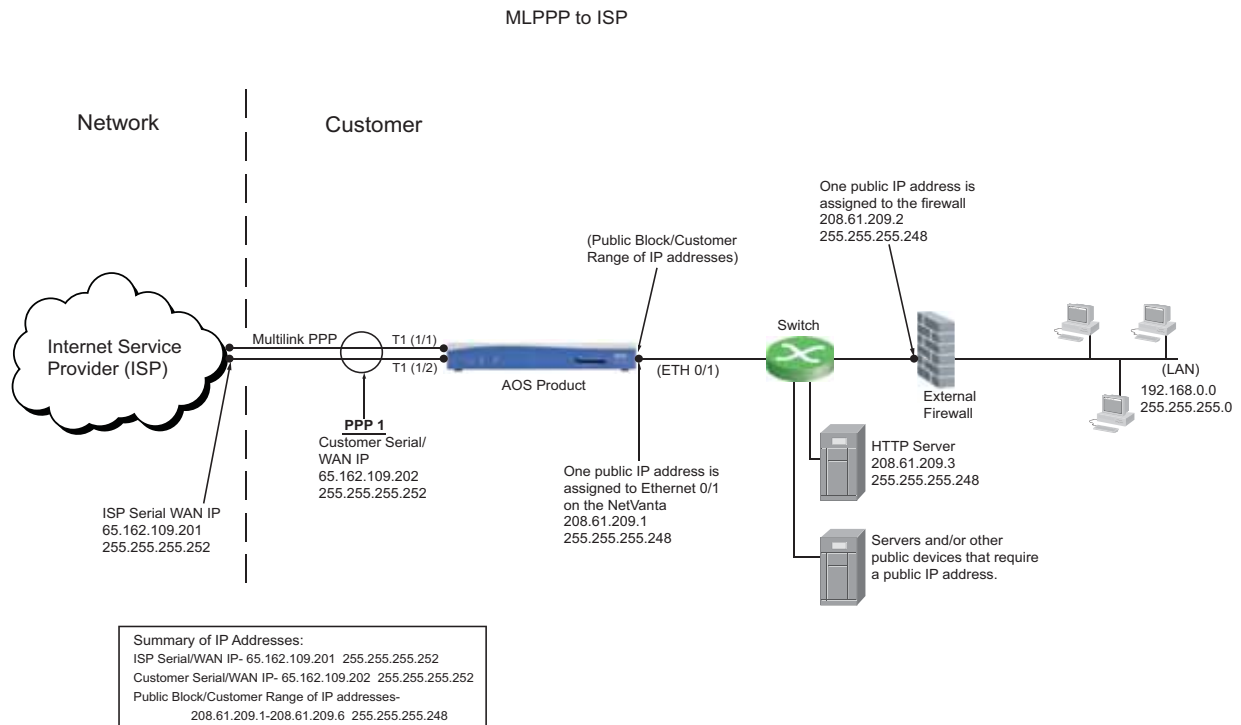


Figure 20. An MLPPP Connection to an ISP with an Ethernet Firewall

The following configuration applies to Example 4:

```
!  
interface eth 0/1  
    ip address 208.61.209.1 255.255.255.248  
    no shutdown  
!  
interface t1 1/1  
    clock source line  
    tdm-group 1 timeslots 1-24 speed 64  
    no shutdown  
!  
interface t1 1/2  
    clock source through  
    tdm-group 2 timeslots 1-24 speed 64  
    no shutdown  
!  
interface ppp 1  
    ip address 65.162.109.202 255.255.255.252  
    ppp multilink  
    no shutdown  
    cross-connect 1 t1 1/1 1 ppp 1  
    cross-connect 2 t1 1/2 2 ppp 1  
!  
ip route 0.0.0.0 0.0.0.0 ppp 1  
!
```



The command **clock source line** is enabled by default. Therefore, this command will not appear in the output when the **show running-config** command is issued.



When using a dual T1 interface card, only one clocking source is allowed between interface T1 1/1 and interface T1 1/2. If interface T1 1/1 is set to source the clock from the line or internally, then interface T1 1/2 will automatically set to **clock source through**. Conversely, if interface T1 1/2 is set to source the clock from the line or internally, then interface T1 1/1 will automatically set to **clock source through**.

Example 5: MLPPP from a Central to a Remote Location

MLPPP can be used to achieve higher bandwidth across multiple T1 connections between a central corporate office and a remote branch office. The distance between the two locations is transparent, with clients on the remote LAN operating seamlessly with clients and resources on the corporate LAN. Internet access for the remote office is also funneled through the corporate office and across the MLPPP connection. The following configuration example utilizes private static IP addresses at each end of the MLPPP connection (10.0.0.1 /30 at corporate and 10.0.0.2 /30 at the branch office). No authentication is required to establish the MLPPP session. Clocking on the T1 interface is provided by the AOS product at the corporate location. Each LAN is assigned a different subnet (192.168.1.0 /24 at corporate and 192.168.2.0 /24 at the branch office). The remote office is programmed with a default route that points to the PPP interface. This route ensures that Internet and other traffic destined for the corporate LAN is directed to the proper place. The default route programmed into the corporate AOS product points toward the corporate Internet router connected to the ISP (192.168.1.254). A static route programmed into the corporate router ensures that traffic destined for the remote LAN (192.168.2.0 /24) is directed toward the PPP interface on the remote router (10.0.0.2).

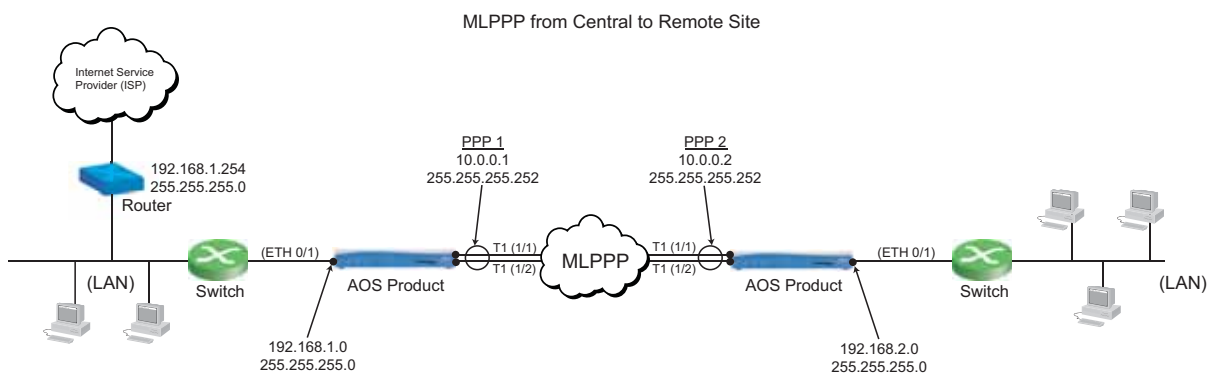


Figure 21. An MLPPP Connection from Central HQ to a Branch Office

The following configuration applies to Example 5:

Central Office

```
!
interface eth 0/1
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
interface t1 1/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.0.0.1 255.255.255.252
  ppp multilink
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
  cross-connect 2 t1 1/2 2 ppp 1
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.2.0 255.255.255.0 ppp 1
!
```

Remote Office

```
!
interface eth 0/1
  ip address 192.168.2.1 255.255.255.0
  no shutdown
!
interface t1 1/1
  clock source line
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface t1 1/2
  clock source through
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.0.0.2 255.255.255.252
  ppp multilink
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
  cross-connect 2 t1 1/2 2 ppp 1
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
```

Separate Internet router (192.168.1.254) will need the following routes added:

```
ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

```
ip route 10.0.0.0 255.255.255.252 192.168.1.1
```



The command **clock source line** is enabled by default. Therefore, this command will not appear in the output when the **show running-config** command is issued.

Quick Configuration Guide

Table 3. PPP Configuration Command Summary

	Command	Description
Step 1	(config)# interface ppp <number>	Create a virtual PPP interface.
Step 2	(config ppp x)# ip address <ip address> <subnet mask>	Configure the PPP interface with a static IP address.
(or)	(config-ppp x)# ip address negotiated	Configure the PPP interface to negotiate the IP address with your Internet Service Provider (ISP).
(or)	(config-ppp x)# ip unnumbered <interface>	Configure the PPP interface as an unnumbered interface.
Step 3 (Optional)	(config-ppp x)# ip address <ip address> <subnet mask> secondary	Configure secondary IP addresses on the PPP interface.
Step 4 (Optional)	(config-ppp x)# ppp authentication [pap chap]	Require PAP or CHAP authentication on the PPP interface.
PAP (Optional)	(config-ppp x)# username <username> password <password>	Configure the PAP user name and password into the database of the (local) router.
	(config-ppp x)# ppp pap-sent username <username> password <password>	Configure the PAP user name and credentials into the (peer) router.
CHAP (Optional)	(config-ppp x)# username <username> password <password>	Configure the CHAP user name and password into the database of the (local) router.
	(config-ppp x)# ppp chap password <password>	Configure the CHAP password into the (peer) router.
	(config-ppp x)# ppp chap hostname <hostname>	Change the host name that is sent during the challenge for CHAP authentication.
Step 5 (Optional)	(config-ppp x)# ppp multilink	Enable MLPPP.
Step 6	(config-ppp x)# no shutdown (config-ppp x)# exit	Activate the PPP interface. Exit the PPP interface configuration menu.
Step 7	(config)# cross-connect <number> <from interface> <group number> <to interface>	Cross connect the physical WAN interface to the virtual PPP interface. When MLPPP is used, a cross-connect command should be issued for each carrier line that is to be bundled to the PPP interface.
	(config)# exit	Exit the configuration menu.
Step 8	(config)# copy running-config startup-config	Save the configuration.

Table 4. Additional PPP Interface Settings

Command	Description
acfc accept-compressed	Enable the AOS device to accept header compressed frames even if compression is not negotiated.
bridge-group <number> [vlan-transparent]	Assign an interface to a specified bridge group. Any two interfaces may be bridged together. Optionally allows VLAN-tagged frames to cross a bridged PPP link (if this option is configured, it must be used in conjunction with the ppp bcp tagged-frame command).
description <text>	Add a text description that describes this PPP interface.
keepalive <value>	Enable the transmission of keepalive packets on the interface and/or specify the time interval between transmitted packets.
mtu <size>	Specify the MTU for this PPP connection.
peer default ip address <ip address>	Specify the default IP address for the remote end of this interface.
ppp bcp tagged-frame	Allow negotiation of 802.1Q-tagged packets over Bridging Control Protocol (BCP). If VLAN-tagged frames are going to be passed over a bridged PPP link, this command must be used in conjunction with the bridge-group <number> vlan-transparent command.

Table 5. Enhancing MLPPP Performance

Command	Description
ppp multilink fragmentation	Enable multilink fragmentation to reduce serialization delays of large packets.
ppp multilink interleave	Enable multilink interleave if streaming protocols are used across the MLPPP connection.
ppp multilink maximum <number>	Specify the maximum number of links allowed in the MLPPP bundle.

Troubleshooting

Network issues observed across a PPP connection are commonly caused by problems on the physical transmission medium. Therefore, troubleshooting should begin with examination of the status of the Layer 1 interface to which the PPP interface is bound. T1 is the physical layer used for the troubleshooting examples that follow. The underlined output below shows that the physical layer is up and there are no alarms:

#show interfaces t1 1/1

t1 1/1 is UP

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: rai
 Last clearing of counters 00:09:24

loss of frame	: 0
loss of signal	: 0
AIS alarm	: 0
Remote alarm	: 0

DS0 Status: 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
 NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
 Status Legend: '-' = DS0 is unallocated
 'N' = DS0 is dedicated (nailed)

Line Status: -- No Alarms --

5 minute input rate 72 bits/sec, 0 packets/sec
 5 minute output rate 120 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

Encapsulation PPP (ppp 1)

131 packets input, 4897 bytes, 0 no buffer
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame
 0 abort, 0 discards, 0 overruns
 150 packets output, 8174 bytes, 0 underruns

The statistics listed under the TDM group 1 section all pertain to the PPP interface. Ideally, all error indicators (runs, giants, throttles, input errors, CRC, frame, abort, discards, overruns, and underruns) should be 0. It is normal to have a few errors if the interface has been active for an extended period of time. Any error value that increments over a short period of time is a good indicator that there are Layer 1 problems on the transmission medium.



The command **show interfaces t1 1/1** displays all cumulative errors for the TDM group since the last time the **clear counters** command was issued. The errors displayed under **Current Performance Statistics** only reflect what has occurred during the last 15 minutes. To view all performance statistics errors that have occurred over the last 24 hours, enter the following command: **show interfaces t1 1/1 performance-statistics total-24-hour** or **show interfaces t1 1/1 p t**.

If Layer 1 is up and transmitting properly, the next step 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 10 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 = 1500
  Peer authenticates with CHAP
  IP is configured
    IP address negotiated
  Secondary IP:
    208.61.209.1, 255.255.255.248
-----
Link thru t1 1/1 is UP; LCP state is OPENED, negotiated MTU is 1500
  Receive: bytes=15359, pkts=827, errors=0
  Transmit: bytes=25716, pkts=1372, errors=0
  5 minute input rate 112 bits/sec, 1 packets/sec
  5 minute output rate 104 bits/sec, 1 packets/sec
Bundle information
  Queueing method: weighted fair
  HDLC tx ring limit: 2
  Output queue: 0/1/460/64/0 (size/highest/max total/threshold/drops)
    Conversations 0/1/256 (active /max active/max total)
    Available Bandwidth 1152 kilobits/sec
  IP is UP, IPCP state is OPENED
    Negotiated Address=65.162.109.202 Mask=255.255.255.255
  Peer address=65.162.109.201
    IP MTU=1500, Bandwidth=1536 Kbps
  LLDPCP State is OPENED
  
```

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

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

Figure 22. 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 does not need to be in the OPEN state for the PPP interface to be UP, however, they must be open in order to transport data across the PPP link.

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 is underlined 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 DOWN

Configuration:

Keep-alive is set (10 sec.)

No multilink

MTU = 1500

Peer authenticates with CHAP

IP is configured

IP address negotiated

Secondary IP:

208.61.209.1, 255.255.255.248

Link thru t1 1/1 is DOWN; LCP state is REQSENT

Receive: bytes=4290, pkts=234, errors=0

Transmit: bytes=7176, pkts=390, errors=0

5 minute input rate 112 bits/sec, 1 packets/sec

5 minute output rate 88 bits/sec, 1 packets/sec

Bundle information

Queuing method: weighted fair

HDLC tx ring limit: 0

Output queue: 0/0/460/64/0 (size/highest/max total/threshold/drops)

Conversations 0/0/256 (active/max active/max total)

Available Bandwidth 1152 kilobits/sec

Table 6. LCP State Descriptions

LCP State	Description
INITIAL	This is the first state of LCP negotiation.
REQSENT	<p>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:</p> <ol style="list-style-type: none"> 1. The timeslots or speed configured for the TDM group are mismatched with the peer device. 2. The peer router is not set for PPP protocol. 3. The authentication user name and/or password does not match what has been programmed into the peer device. 4. There are severe errors on the physical interface preventing PPP frames from being sent and received intact between peers.
ACKRCVD	The unit has received a Conf-Ack from the peer device.
LOOPBACK	The unit received its own PPP frame, which is determined by inspecting the magic number of the frame received and comparing it to the one transmitted. When this number is the same, it indicates a loopback is in place toward 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.

Debug Commands

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. Debug commands are issued from enable mode. The commands may also be entered from global or interface configuration mode when preceded by the delimiter **do** (e.g. (config)#**do debug ppp errors**). Table 7 provides a list of available PPP **debug** commands and a description of each.


 **NOTE** *Some **debug** commands will produce data that will quickly fill up the screen. Due to continuous scrolling of incoming debug messages, it may become difficult to execute the **no** form of the **debug** command to turn debug messages off. A shortcut command can be issued to turn all debug messages off. This command is **#undebug all** or **#u** for short.*

Table 7. PPP Debug Commands

Command	Description
debug ppp authentication	Activates debug messages pertaining to PAP or CHAP authentication.
debug ppp errors	Activates debug messages that indicate a PPP error was detected (encapsulation error, etc.).
debug ppp negotiation	Activates debug messages associated with PPP negotiation (LCP, IPCP, BCP negotiation, etc.).
debug ppp verbose	Displays all PPP debug messages in real time to the terminal or Telnet screen.

Various PPP messages can be generated when **debug** commands are issued. 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 8. 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 the desired 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 message that acknowledges a received Conf-Req , but indicates that the peer has requested to use an option that is not supported. The Conf-Nak includes alternative options that are supported.
Conf-Rej	Configuration reject (Conf-Rej) is a message that is sent to indicate that the peer has requested to use an option that is not supported. 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 a protocol that is not supported.
Term-Ack	Termination acknowledge (Term-Ack) is a message sent to acknowledge a termination request from the peer.
Term-Req	Termination request (Term-Req) is a message sent to terminate a PPP connection.

The **debug ppp authentication** command displays authentication messages pertaining to PAP and CHAP. The following example output shows a successful CHAP negotiation. The output was captured on a unit that received and responded to a CHAP challenge from its peer.

#debug ppp authentication

```
2007.10.26 15:46:06 PPP.AUTHENTICATION PPPrx [t1 1/1] CHAP: Challenge ID=1 Len=27
ValLen=16 Name (Router)
2007.10.26 15:46:06 PPP.AUTHENTICATION PPPtx [t1 1/1] CHAP: Response ID=1 Len=27
ValLen=16 Name (Router)
2007.10.26 15:46:06 PPP.AUTHENTICATION PPPrx [t1 1/1] CHAP: Success ID=1 Len=4
Message( )
```

The following output shows a failed CHAP challenge. The output was captured on a unit that received a CHAP challenge from its peer. An incorrect password supplied by this unit caused the authentication failure.

#debug ppp authentication

```
2007.10.26 16:04:27 PPP.AUTHENTICATION PPPrx[t1 1/1] CHAP: Challenge ID=1 Len=27
ValLen=16 Name(Router)
2007.10.26 16:04:27 PPP.AUTHENTICATION PPPtx[t1 1/1] CHAP: Response ID=1 Len=27
ValLen=16 Name(Router)
2007.10.26 16:04:27 PPP.AUTHENTICATION PPPrx[t1 1/1] CHAP: Failure ID=1 Len=4
Message( )
```

The **debug ppp errors** command activates debug messages that indicate a PPP error was detected. Many different types of error messages are possible. The following example output shows an error message that was generated due to an incorrect password supplied for a CHAP challenge by this unit.

#debug ppp errors

2007.10.26 16:09:23 PPP.NEGOTIATION PPPFSM: layer up, Protocol=c021

The **debug ppp negotiation** command monitors PPP negotiation that takes place on any interface of the unit. PPP negotiation messages are displayed in real time as a PPP link is established or torn down.

Figure 23 shows the breakdown of a sample PPP negotiation message.

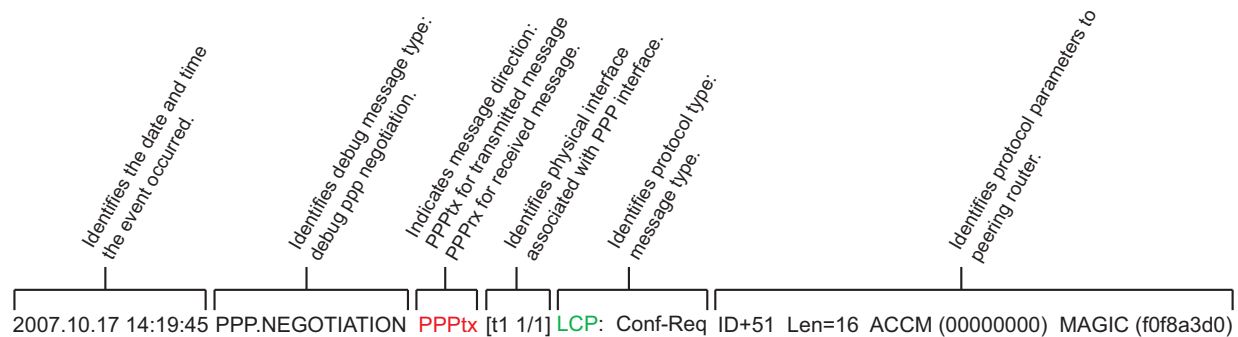


Figure 23. Breakdown of a PPP Debug Message

The following sample debug output shows a successful PPP negotiation (the date/time stamp has been omitted from this output):

#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 may 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:

- 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)

```
- 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)

```
- 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)

```
- 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)

```
- Both routers agreed on the information and IPCP is now up.

```

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

```

A 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:

- The timeslots or speed configured for the TDM group are mismatched with the peer device.
- The peer device is not configured for PPP protocol.

The **debug ppp verbose** command displays all possible PPP debug messages. Use this command with care as it may generate a heavy amount of output.

Once a PPP link has been established, PPP keepalive messages can be observed in the output of **debug ppp verbose**.

```
2006.11.24 12:20:55 PPP PPPtx[t1 1/1] LCP: Echo-Req MAGIC(8e8e18a8)
2006.11.24 12:20:55 PPP PPPrx[t1 1/1] LCP: Echo-Rpl MAGIC(3dcf4bc1)
2006.11.24 12:20:55 PPP PPPrx[t1 1/1] LCP: Echo-Req MAGIC(3dcf4bc1)
2006.11.24 12:20:55 PPP PPPtx[t1 1/1] LCP: Echo-Rpl MAGIC(8e8e18a8)
```

A common observance when an AOS device is connected to a Cisco device is Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) LCP protocol reject messages in the output of the **debug ppp verbose** command. CDP is a protocol that is proprietary to Cisco devices. If a Cisco device is programmed to use CDP with its neighbors, then it will attempt to communicate with the AOS device using the proprietary protocol. The AOS device does not understand CDP and will reject any attempts to communicate via this protocol. LLDP is a standards-based protocol that is equivalent to CDP and is supported by AOS devices. However, if the AOS device is connected to a Cisco device that has been programmed to use CDP, the Cisco device will reject LLDP messages received from the AOS device. Additionally, LLDP LCP protocol reject messages may also be observed when the AOS device is connected to any non-AOS device that does not support LLDP. *It is important to note that the discovery protocol does not affect the ability of the devices to establish a successful PPP connection.* Even though there may be CDP and/or LLDP LCP protocol reject messages in the output of the **debug ppp verbose** command, these messages do not indicate that there is a problem with the PPP link.

The following sample output was generated on an AOS device that is connected to a Cisco device. The AOS device transmits an LLDP configuration request in the first line. The second line shows a CDP configuration request received from the Cisco device. The AOS device then transmits a CDP LCP protocol reject message to the Cisco device (8207). Subsequently, an LLDP LCP protocol reject message is received from the Cisco device (82cc). After this, the AOS device continues to transmit LLDP configuration requests and receive LLDP LCP protocol reject messages.

```
2007.12.30 08:40:15 PPP.NEGOTIATION PPPTx[t1 1/1] LLDPCP: Conf-Req ID=1 Len=4
2007.12.30 08:40:15 PPP PPPrx[t1 1/1] PID=8207Conf-Req ID=1 Len=4
2007.12.30 08:40:15 PPP.NEGOTIATION PPPTx[t1 1/1] LCP: ProtoRej (8207)
2007.12.30 08:40:15 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: ProtoRej (82cc)
```

```
2007.12.30 08:40:19 PPP.NEGOTIATION PPPTx[t1 1/1] LLDPCP: Conf-Req ID=2 Len=4
2007.12.30 08:40:19 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: ProtoRej (82cc)
```

```
2007.12.30 08:40:23 PPP.NEGOTIATION PPPTx[t1 1/1] LLDPCP: Conf-Req ID=3 Len=4
2007.12.30 08:40:23 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: ProtoRej (82cc)
```

```
2007.12.30 08:40:27 PPP.NEGOTIATION PPPTx[t1 1/1] LLDPCP: Conf-Req ID=4 Len=4
2007.12.30 08:40:27 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: ProtoRej (82cc)
```

```
2007.12.30 08:40:31 PPP.NEGOTIATION PPPTx[t1 1/1] LLDPCP: Conf-Req ID=5 Len=4
2007.12.30 08:40:31 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: ProtoRej (82cc)
```

Reduce the number of negative acknowledge or protocol reject messages by turning LLDP off on the AOS device. This can be accomplished by issuing the **no lldp send-and-receive** command on the appropriate PPP interface or by unchecking TX/RX on the appropriate PPP interface from the LLDP link in the AOS GUI interface.

Troubleshooting MLPPP

The most important consideration for troubleshooting MLPPP is determining whether a peer device supports the protocol.

Turn on PPP negotiation debug messages:

```
#debug ppp negotiation
```

Look for the two following fields in the negotiation messages:

- Maximum receive reconstructed unit (MRRU)
- Endpoint discriminator (ED)

```

2007.10.24 10:39:19 PPP.NEGOTIATION PPPrx[t1 1/2] LCP: Conf-Req ID=1
Len=23 MAGIC (dcede7e3) MRRU (1520) ED (3:00a0c812b91d)
2007.10.24 10:39:19 PPP.NEGOTIATION PPPtx[t1 1/2] LCP: Conf-Ack ID=1
Len=23 MAGIC (dcede7e3) MRRU (1520) ED (3:00a0c812b91d)
2007.10.24 10:39:19 PPP.NEGOTIATION PPPrx[t1 1/1] LCP: Conf-Req ID=1
Len=23 MAGIC (56139827) MRRU (1520) ED (3:00a0c812b91d)
2007.10.24 10:39:19 PPP.NEGOTIATION PPPtx[t1 1/1] LCP: Conf-Ack ID=1
Len=23 MAGIC (56139827) MRRU (1520) ED (3:00a0c812b91d)
2007.10.24 10:39:22 PPP.NEGOTIATION PPPFSM: layer up, Protocol=c021
2007.10.24 10:39:22 PPP.NEGOTIATION t1 1/2: LCP up
2007.10.24 10:39:22 PPP.MULTILINK Links bundled
.
.
.
2007.10.24 10:46:28 PPP.NEGOTIATION PPPFSM: layer up, Protocol=82cc
2007.10.24 10:46:28 PPP.NEGOTIATION ppp 1: LLDPCP up
.
.
.
2007.10.24 10:46:28 PPP.NEGOTIATION PPPFSM: layer up, Protocol=8021
2007.10.24 10:46:28 PPP.NEGOTIATION ppp 1: IPCP up
2007.10.24 10:46:28 INTERFACE _STATUS.ppp 1 changed state to up

```

The MRRU field indicates MLPPP support.

The identical ED indicates that T1 1/1 and T2 1/2 are the same link.

Figure 24. MLPPP Debug Messages

MRRU

An MRRU field automatically signals MLPPP support. In Figure 24, the AOS device receives a message (**Conf-Req**) with an MRRU option, which indicates that the peer supports MLPPP. If the AOS device did not support MLPPP or was not configured for MLPPP, then it would reject (**Conf-Rej**) the request. Similarly, if the peer at the other end of the link rejects the MRRU field, the AOS product will terminate the link because it assumes its peer cannot support MLPPP.



The MRRU of an AOS device is hard set at 1520 bytes.

ED

The ED field is present in messages pertaining to MLPPP. This field identifies the device transmitting the packet and allows the receiving peer to recognize that frame fragments received on different carrier lines belong together. The ED should be the same for each line in the bundle. For example, in Figure 24 on page 61, the ED for the T1 1/1 interface and the T1 1/2 interface are the same.