ADTRAN

August 2007

AOS Quick Configuration Guide

Configuring PPP Authentication in AOS

Understanding PPP Authentication

The Point-to-Point Protocol (PPP) suite supports authentication protocols for increased security. Before establishing a PPP session, the AOS product can identify itself to its peer, force its peer to authenticate itself, or both.

PPP Authentication

Before two peers establish a PPP session, they pass through three phases:

1. Link Establishment – Peers exchange Link Control Protocol (LCP) frames to negotiate options for the session. One of these options is the authentication protocol, if any, that will be used.
2. Authentication – Peers exchange authentication information to ensure that they are connecting to an authorized peer.
3. Network Layer Protocol – Peers exchange Network Control Protocols (NCPs) to negotiate which Network Layer protocol (such as IP) Point-to- Point Protocol (PPP) frames will encapsulate, and the options for this protocol.

The PPP suite supports two authentication protocols. The AOS product supports Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Security of the WAN can be increased by requiring the peer at the other end of the link to vouch that it is, indeed, the authorized router at the remote site. The router can also be configured to provide its own authentication information. Many Internet service providers (ISPs) require their subscribers to authenticate themselves so that they only grant service to those who have paid for it.

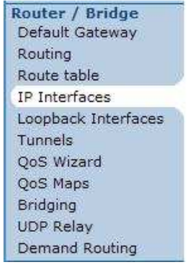
Hardware/Software Requirements/Limitations

PPP Authentication is supported in all AOS router platforms that support PPP.

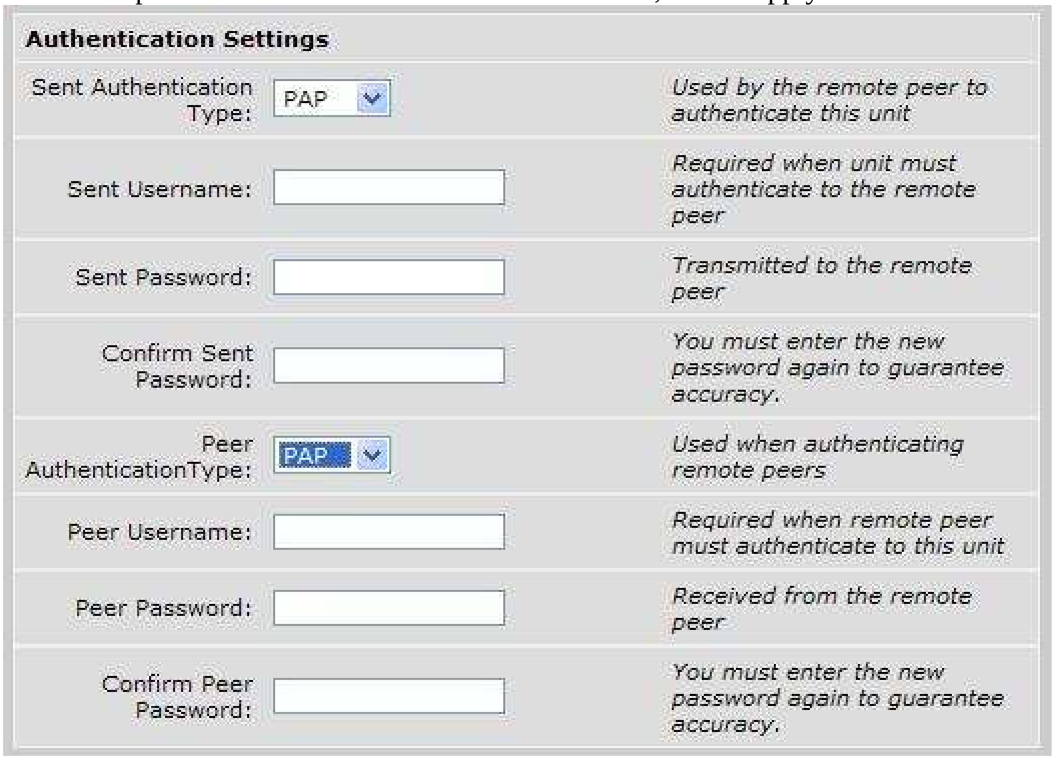
Configuring PPP Authentication

Configuring PPP Authentication in the GUI

First, navigate to IP Interfaces and select the desired PPP interface to use authentication.



Once inside the PPP interface configuration, scroll to Authentication Settings and enter the desired authentication information. “Sent” authentication will be the username and password sent to the remote router. “Peer” authentication will be the username and password that the router is expecting to receive from the remote peer. After the information has been entered, click “Apply”.



Authentication Settings		
Sent Authentication Type:	PAP	*Used by the remote peer to authenticate this unit*
Sent Username:		*Required when unit must authenticate to the remote peer*
Sent Password:		*Transmitted to the remote peer*
Confirm Sent Password:		*You must enter the new password again to guarantee accuracy.*
Peer AuthenticationType:	PAP	*Used when authenticating remote peers*
Peer Username:		*Required when remote peer must authenticate to this unit*
Peer Password:		*Received from the remote peer*
Confirm Peer Password:		*You must enter the new password again to guarantee accuracy.*

Configuring PPP Authentication in the CLI

1. Move to the PPP interface that will be authenticated and choose the type of authentication.

   Syntax: **ppp authentication** <*chap* | *pap*>
   EX: (config-ppp 1)# **ppp authentication pap**

2. Enter the peer’s username and password. If CHAP is being used, then the username should be the hostname of the remote router.

   Syntax: **username** <*username*> **password** <*password*>
   EX: (config-ppp 1)# **username Remote password Netvanta**

3. Enter the username and password that will be sent to the remote router, or in the case of CHAP, the password that will be sent along with the hostname.

   Syntax: **ppp pap sent-username** <*username*> **password** <*password*>
   Syntax: **ppp chap password** <*password*>
   EX: (config-ppp 1)# **ppp pap sent-username Host password Netvanta**
   EX: (config-ppp 1)# **ppp chap password Netvanta**

Command Summary Table

	Command	Description
Step 1	(config-ppp 1)# **ppp authentication** <pap | chap>	Navigate to the PPP interface and specify the authentication type
Step 2	(config-ppp 1)# **username** <username> **password** <password>	Specify the username and password expected from the remote router. If using CHAP, specify the hostname of the remote router
Step 3	(config-ppp 1)# **ppp pap send-username** <usename> **password** <password> (config-ppp 1)# **ppp chap password** <password>	Enter the username and password that will be sent to the remote router. In the case of CHAP, enter the password that will be sent along with the hostname.

Example configuration

PAP Example

Router 1	Router 2
(config-ppp 1)# **ppp authentication pap**	(config-ppp 1)# **ppp authentication pap**
(config-ppp 1)# **username Router2 password PW**	(config-ppp 1)# **username Router1 password PW**
(config-ppp 1)# **ppp pap send-username Router1 password PW**	(config-ppp 1)# **ppp pap send-username Router2 password PW**

CHAP Example

Router 1	Router 2
(config)# **hostname Router1**	(config)# **hostname Router2**
(config-ppp 1)# **ppp authentication chap**	(config-ppp 1)# **ppp authentication chap**
(config-ppp 1)# **username Router2 password PW**	(config-ppp 1)# **username Router1 password PW**
(config-ppp 1)# **ppp chap password PW**	(config-ppp 1)# **ppp chap password PW**

Troubleshooting

When a PPP connection will not go up, view the status of the PPP interface (**show int ppp <*interface number*>**). If the LCP state is continually going up and down, it is possible that one or both of the peers cannot authenticate themselves.

Authentication debug messages can be viewed to determine whether the local or the remote router has failed to authenticate itself. When troubleshooting PAP, the usernames and passwords the routers are sending can also be viewed.

Syntax: **debug ppp authentication**