Configuring the Access VPN to Work with Local AAA

Introduction

In this second task, the ISP and enterprise customer:

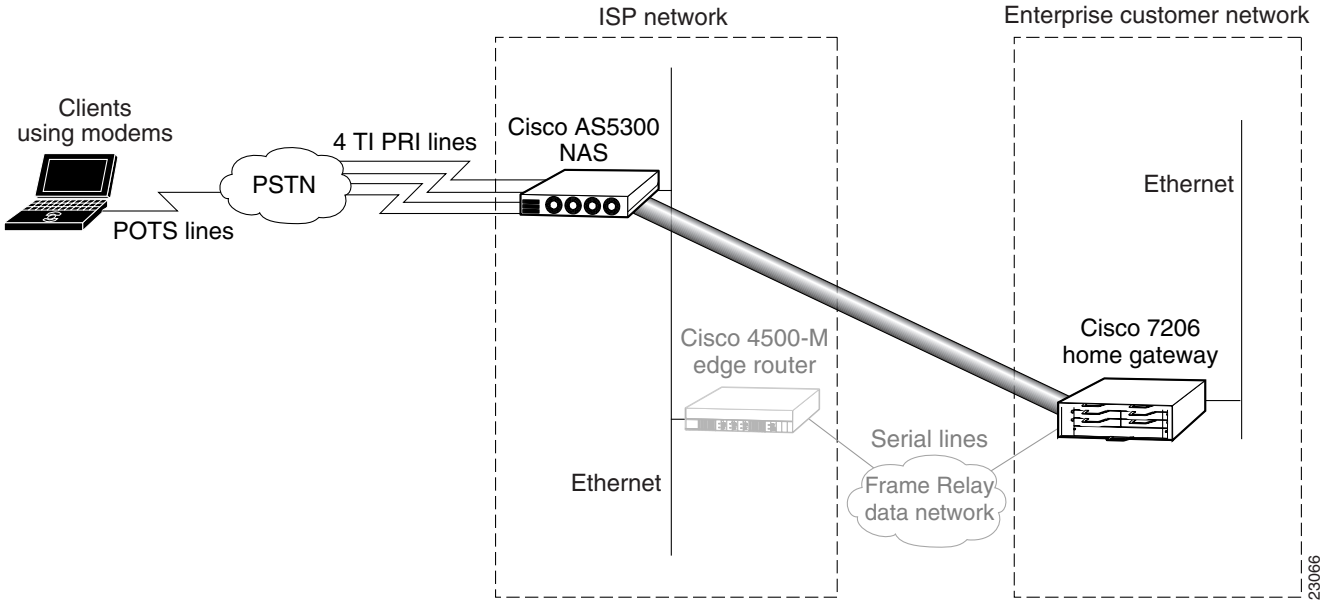
- Configure their network devices to work as an access VPN
- Use local AAA to authenticate the tunnel and the users
- Verify that the access VPN works properly
- Troubleshoot the access VPN if there are problems

The ISP configures the NAS, and the enterprise customer configures the home gateway.

After the ISP and enterprise customer verify that their access VPN works by using local AAA, they reconfigure their devices to use remote AAA servers. See "Configuring the Access VPN to Work with Remote AAA."

Figure 1 shows the access VPN network topology. The tunnel and user authentication occurs locally between the Cisco AS5300 NAS and the Cisco 7206 home gateway.

Figure 14 Access VPN Topology Using Local AAA



Once the ISP and enterprise customer have completed this task, the network will function as follows:

- When the user Jeremy wants to connect to the enterprise customer's network, he dials in to the NAS by using the username jeremy@hgw.com.
- The NAS and the client perform LCP negotiation.
- The NAS authenticates the domain name hgw.com and determines the tunnel endpoint information.
- The NAS negotiates an L2F tunnel with the home gateway. Once the tunnel is established, the NAS forwards the call to the home gateway.
- The home gateway authenticates the username, jeremy, and assigns the client an IP address. (It can optionally assign IP addresses for DNS and WINS servers.)
- The client and the home gateway can now exchange PPP packets. The NAS now acts as a transparent PPP frame forwarder.

Configuring the Access VPN

To configure the NAS and home gateway to work as an access VPN, follow these steps:

- Step 1—Configuring the NAS
- Step 2—Configuring the Home Gateway

Step 1—Configuring the NAS

In this step, the ISP configures the NAS for VPN using local AAA. This step contains the following sections:

- Enabling VPN to Send L2F Tunnels
- Authenticating and Authorizing the Tunnel
- Removing Unnecessary Commands

Note This step assumes that you already configured the NAS for basic dial access as described in "Configuring the NAS for Basic Dial Access." The access VPN described in this case study routes calls and builds tunnels based on domain name—not dialed number identification service (DNIS).

Enabling VPN to Send L2F Tunnels

In this section, the ISP:

- Turns on VPN
- Sends an L2F tunnel out to the home gateway
- Configures the NAS to first search for domain names before searching for DNIS

Use this command	To do this
`ISP_NAS(config)# vpdn enable`	Turn on VPN[1].
`ISP_NAS(config)# vpdn-group 1`	Create a VPN group. VPN group statements are not needed for remote AAA scenarios.
`ISP_NAS(config-vpdn)# request dialin l2f ip 172.22.66.25 domain hgw.com`	Request a tunnel to 172.22.66.25 by using L2F, IP, and the domain name hgw.com. To accept the tunnel, the home gateway is configured with the **accept dialin l2f virtual-template 1 remote ISP_NAS** command and **local name ENT_HGW** command. To create a DNIS based tunnel, replace the **domain** keyword with the **dnis** keyword and phone number. The domain name identifies which tunnel the user belongs to.
`ISP_NAS(config-vpdn)# local name ISP_NAS` `ISP_NAS(config-vpdn)# exit`	Turn on authentication for L2F. This name does not have to be the same as the hostname of the access server.
`ISP_NAS(config)# vpdn search-order domain dnis`	Configure the software to first search for the domain name before searching for DNIS. This command decreases connectivity time, which can reduce the number of system timeouts. By default, the Cisco IOS software first looks to see if it can build out a tunnel based on DNIS. If DNIS is not found, the software searches for a domain name. The **vpdn search-order domain dnis** command reverses the default.

1. The Cisco IOS command syntax uses the more specific term virtual private dialup network (VPDN) instead of VPN.

Authenticating and Authorizing the Tunnel

In this section, the ISP:

- Adds local usernames for bidirectional authentication between the NAS and home gateway
- Authenticates the tunnel between the remote peers and authorize the tunnel at the NAS

Use this command	To do this
`ISP_NAS(config)# username ISP_NAS password cisco` `ISP_NAS(config)# username ENT_HGW password cisco`	Add local usernames with the same password for bidirectional tunnel authentication between the NAS and the home gateway. These usernames and password are called the tunnel secret. **Note** The NAS and the home gateway must both have the same usernames with the same password. These usernames are not related to client authentication.
`ISP_NAS(config)# aaa authentication ppp default local` `ISP_NAS(config)# aaa authorization network default local`	Authenticate the tunnel between the remote peers and authorize the tunnel at the NAS. The tunnel authorization phase includes an authentication step. The tunnel must be *authenticated* before it can be *authorized*.

Removing Unnecessary Commands

In this section, the ISP:

- Removes the local IP address pool
- Deletes the client's username and password from the local database

Use this command	To do this

`ISP_NAS(config)# no ip local pool default 1.1.1.1`
`ISP_NAS(config)# interface group-async 1`
`ISP_NAS(config-if)# no peer default ip address pool default`
`ISP_NAS(config-if)# exit`
	Remove the local IP address pool from the NAS.
	The client is assigned an IP address from the home gateway's local IP address pool.

`ISP_NAS(config)# no username jeremy password subaru`	Remove the client's username and password from the local AAA database. The home gateway (not the NAS) now performs username authentication.

Step 2—Configuring the Home Gateway

In this step, the enterprise customer configures the home gateway for VPN using local AAA. This step contains the following sections:

- Configuring Basic Settings
- Configuring Local AAA
- Enabling VPN to Accept L2F Tunnels
- Creating the Virtual Template
- Specifying the IP Address Pool and BOOTP Servers

Configuring Basic Settings

In this section, the enterprise customer:

- Configures the basic global configuration settings
- Configures the Fast Ethernet interface
- Verifies connectivity with the NAS

We strongly recommend using the **service password-encryption** command so that your username passwords do not appear in the configuration output. The **service timestamps debug datetime msec** command includes millisecond dating on debug output. These time stamps help identify debug output when there is a lot of activity on the router.

Use this command	To do this
`Router> enable`	Enter privileged EXEC mode.
`Router# configure terminal` `Enter configuration commands, one per line. End with CNTL/Z.`	Enter global configuration mode.
`Router(config)# hostname ENT_HGW`	Change the hostname to ENT_HGW.
`ENT_HGW(config)# enable secret letmein`	Change the enable secret to letmein.
`ENT_HGW(config)# service password-encryption`	Encrypt passwords that appear as part of the configuration.
`ENT_HGW(config)# service timestamps debug datetime msec`	Set debug time stamps to include millisecond dating.
`ENT_HGW(config)# username jane-admin password jane-password`	Set the username and password for the administrator.
`ENT_HGW(config)# ip domain-name cisco.com`	Set the default domain name that the Cisco IOS software will use to complete unqualified host names.
`ENT_HGW(config)# ip name-server 171.68.10.70`	Set the IP address of the host that will supply Domain Name System (DNS) information.
`ENT_HGW(config)# interface fastethernet 0/0`	Enter interface configuration mode.
`ENT_HGW(config-if)# ip address 172.22.66.25 255.255.255.192`	Assign an IP address to the FastEthernet 0/0 interface.
`ENT_HGW(config-if)# no shutdown` `%LINK-3-UPDOWN: Interface FastEthernet0, changed state to up`	Bring up the interface.
`ENT_HGW(config-if)# exit`	Exit interface configuration mode.
`ENT_HGW(config)# exit`	Exit global configuration mode.

`ENT_HGW# ping 172.22.66.23`
`Type escape sequence to abort.`
`Sending 5, 100-byte ICMP Echos to 172.22.66.23, timeout is 2 seconds:`
`!!!!!`
`Success rate is 100 percent (5/5), round-trip min/avg/max = 128/131/144 ms`
	Verify connectivity between the home gateway and the NAS.

Configuring Local AAA

In this section, the enterprise customer configures local AAA and the usernames needed to authenticate the user and the tunnel:

Use this command	To do this
`ENT_HGW(config)# aaa new-model`	Enable the AAA access control system. This step immediately locks down login and PPP authentication.
`ENT_HGW(config)# aaa authentication login default local`	Specify that login users will be authenticated using the local database.
`ENT_HGW(config)# aaa authentication ppp default local`	Specify that PPP users will be authenticated using the local database.
`ENT_HGW(config)# aaa authorization network default local`	Specify that network-related service requests will be authorized by using the local database.
`ENT_HGW(config)# username jeremy@hgw.com password subaru`	Add the local username that is used to authenticate the remote user.
`ENT_HGW(config)# username ISP_NAS password cisco` `ENT_HGW(config)# username ENT_HGW password cisco`	Add local usernames and passwords for bidirectional tunnel authentication between the NAS and the home gateway. These usernames are called the tunnel secret. **Note** The NAS and the home gateway must both have the same usernames with the same password. These usernames are not related to client authentication.

Enabling VPN to Accept L2F Tunnels

In this section, the enterprise customer enables and configure the home gateway for VPN using L2F tunnels:

Use this command	To do this
`ENT_HGW(config)# vpdn enable`	Enable VPN[1].
`ENT_HGW(config)# vpdn-group 1`	Create VPN group 1.
`ENT_HGW(config-vpdn)# accept dialin l2f virtual-template 1 remote ISP_NAS`	Specify that the home gateway will accept L2F tunnels from the client, ISP_NAS, and clone the new virtual-access interface from virtual template 1. To accept the tunnel, the home gateway is configured with the **request dialin l2f ip 172.22.66.25 domain hgw.com** command and **local name ENT_HGW** command.
`ENT_HGW(config-vpdn)# local name ENT_HGW`	Specify that the L2F tunnel identifies itself with the local hostname, ENT_HGW.

1. The Cisco IOS command syntax uses the more specific term virtual private dialup network (VPDN) instead of VPN.

Creating the Virtual Template

In this section, the enterprise customer creates the virtual template that is used to clone virtual-access interfaces:

Output	Purpose
`ENT_HGW(config)# interface virtual-template 1`	Create virtual template 1 that is used to clone virtual-access interfaces.

`ENT_HGW(config-if)# ip unnumbered fastethernet0/0`	Specify that the virtual-access interfaces use the Fast Ethernet 0/0 interface's IP address.
`ENT_HGW(config-if)# ppp authentication chap`	Enable CHAP authentication using the local username database.
`ENT_HGW(config-if)# peer default ip address pool default`	Return an IP address from the default pool to the client.
`ENT_HGW(config-if)# encapsulation ppp`	Enable PPP encapsulation.

Specifying the IP Address Pool and BOOTP Servers

In this section, the enterprise customer specifies the IP address pool and the BOOTP servers.

The IP address pool is the addresses that the home gateway assigns to clients. You must configure an IP address pool. You can also provide BOOTP servers. DNS servers translate hostnames to IP addresses. WINS servers, which are specified using the **async-bootp nbns-server** command, provide dynamic NetBIOS names that Windows devices use to communicate without IP addresses.

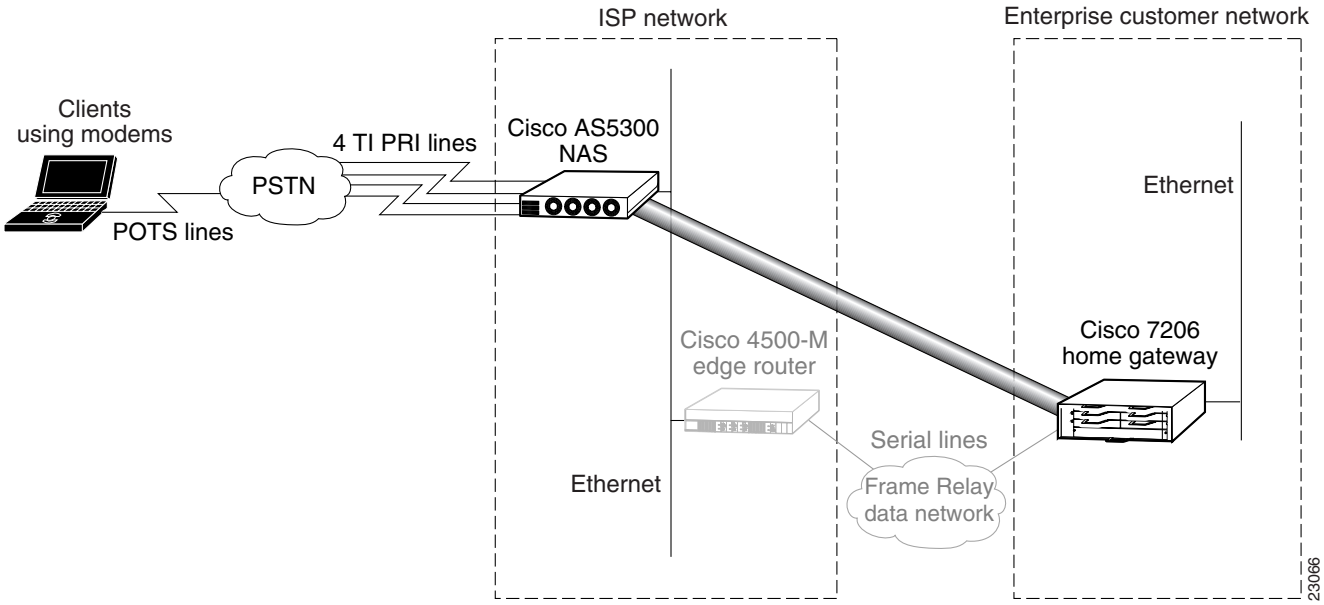
Use this command	To do this
`ENT_HGW(config)# ip local pool default 172.30.2.1 172.30.2.96`	Configure the default local pool of IP address that will be used by clients.
`ENT_HGW(config)# async-bootp dns-server 172.23.1.10 172.23.2.10`	(Optional) Return the configured addresses of Domain Name Servers in response to BOOTP requests.
`ENT_HGW(config)# async-bootp nbns-server 172.23.1.11 172.23.2.11`	(Optional) Return the configured addresses of Windows NT servers in response to BOOTP requests.

Verifying the Access VPN

This section describes how to verify that the following end-to-end connections function as shown in Figure 15:

- Step 1—Checking the NAS Running Configuration
- Step 2—Checking the Home Gateway Running Configuration
- Step 3—Dialing in to the NAS
- Step 4—Pinging the Home Gateway
- Step 5—Displaying Active Call Statistics on the Home Gateway
- Step 6—Pinging the Client
- Step 7—Verifying That the Virtual-Access Interface Is Up and That LCP Is Open
- Step 8—Viewing Active L2F Tunnel Statistics

Figure 15 Access VPN Topology Using Local AAA



After you successfully test these connections, go to "Configuring the Access VPN to Work with Remote AAA." If you experience problems, see "Troubleshooting the Access VPN."

Step 1—Checking the NAS Running Configuration

Enter the **show running-config** command in privileged EXEC mode to make sure the NAS accepted the commands you entered:

```
ISP_NAS# show running-config
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP_NAS
!
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
enable secret 5 $1$AXl/$27hOM6j51a5P76Enq.LCf0
!
username jane-admin password 7 0501090A6C5C4F1A0A1218000F
username ENT_HGW password 7 104D000A0618
username ISP_NAS password 7 13061E010803
vpdn enable
!
vpdn search-order domain dnis
vpdn-group 1
 request dialin l2f ip 172.22.66.25 domain hgw.com
 local name ISP_NAS
!
```

```
async-bootp dns-server 171.68.10.70 171.68.10.140
isdn switch-type primary-5ess
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-24
!
!
interface Ethernet0
 ip address 172.22.66.23 255.255.255.192
!
interface Serial0:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial1:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial2:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial3:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface FastEthernet0
 no ip address
 shutdown
!
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 async mode interactive
 no peer default ip address
```

```
 ppp authentication chap pap
 group-range 1 96
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.66.1
!
!
line con 0
 transport input none
line 1 96
 autoselect during-login
 autoselect ppp
 modem InOut
line aux 0
line vty 0 4
!
end
```

Step 2—Checking the Home Gateway Running Configuration

Enter the **more system:running-config** command in privileged EXEC mode to make sure the home gateway accepted the commands you entered:

```
ENT_HGW# more system:running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
!
hostname ENT_HGW
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authorization network default local
enable secret 5 $1$44oH$gZlAZLwylZJSNKGDk.BKb0
!
username jane-admin password 7 00001C05
username ISP_NAS password 7 070C285F4D06
username ENT_HGW password 7 107249D900E4
username jeremy@hgw.com password 7 140407090D163F
ip subnet-zero
ip domain-name cisco.com
ip name-server 171.68.10.70
!
vpdn enable
!
vpdn-group 1
 accept dialin l2f virtual-template 1 remote ISP_NAS
 local name ENT_HGW
!
async-bootp dns-server 172.23.1.10 172.23.2.10
async-bootp nbns-server 172.23.1.11 172.23.2.11
!
!
!
interface FastEthernet0/0
 ip address 172.22.66.25 255.255.255.192
 no ip directed-broadcast
```

```
!
.
.
.
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 peer default ip address pool default
 ppp authentication chap
!
ip local pool default 172.30.2.1 172.30.2.96
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.66.1
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password 7 045F0405
 login local
!
end
```

Step 3—Dialing in to the NAS

From the client, dial in to the NAS by using the PRI telephone number assigned to the NAS' T1 trunks. Sometimes the PRI telephone number is called the hunt group number.

As the call comes into the NAS, a LINK-3-UPDOWN message automatically appears on the NAS' terminal screen. In this example, the call comes in to the NAS on asynchronous interface 14. The asynchronous interface is up.

```
*Jan  1 21:22:18.410: %LINK-3-UPDOWN: Interface Async14, changed state to up
```

Note No debug commands are turned on to display this log message. Start troubleshooting the NAS if you do not see the above message after 30 seconds of when the client first transmits the call.

Step 4—Pinging the Home Gateway

From the client, ping the home gateway. From the client's Windows 95 desktop:

(a) Click Start.

(b) Select Run.

(c) Enter **ping 172.22.66.25**.

(d) Click OK.

(e) Look at the terminal screen and verify that the home gateway is sending ping reply packets to the client.

Step 5—Displaying Active Call Statistics on the Home Gateway

From the home gateway, enter the **show caller** command and **show caller user** *name* command to verify that the client received an IP address. This example shows that Jeremy is using interface virtual-access 1 and is assigned IP address 172.30.2.1. The network administrator jane-admin is using console 0.

```
ENT_HGW# show caller
  Line         User               Service       Active
  con 0        jane-admin          TTY           00:00:25
  Vi1          jeremy@hgw.com     PPP   L2F     00:01:28

ENT_HGW# show caller user jeremy@hgw.com

  User: jeremy@hgw.com, line Vi1, service PPP L2F, active 00:01:35
  PPP: LCP Open, CHAP (<- AAA), IPCP
  IP: Local 172.22.66.25, remote 172.30.2.1
  VPDN: NAS ISP_NAS, MID 1, MID open
        HGW  ENT_HGW, NAS CLID 36, HGW CLID 1, tunnel open
  Counts: 105 packets input, 8979 bytes, 0 no buffer
          0 input errors, 0 CRC, 0 frame, 0 overrun
          18 packets output, 295 bytes, 0 underruns
          0 output errors, 0 collisions, 0 interface resets
```

Note The **show caller** command was introduced in Cisco IOS Release 11.3(5)AA. If your Cisco IOS software does not include the **show caller** command, use the **show user** command instead.

Step 6—Pinging the Client

From the home gateway, ping Jeremy's PC at IP address 172.30.2.1:

```
ENT_HGW# ping 172.30.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/132/152 ms
```

Step 7—Verifying That the Virtual-Access Interface Is Up and That LCP Is Open

From the home gateway, enter the **show interface virtual-access 1** command to verify that the interface is up, LCP is open, and no errors are reported:

```
ENT_HGW# show interface virtual-access 1
Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of FastEthernet0/0 (172.22.66.25)
  MTU 1500 bytes, BW 115 Kbit, DLY 100000 usec,
     reliablility 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open
  Open: IPCP
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters 3d00h
  Queueing strategy: fifo
  Output queue 1/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
114 packets input, 9563 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
27 packets output, 864 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Step 8—Viewing Active L2F Tunnel Statistics

From the home gateway, display active tunnel statistics by entering the **show vpdn** command and **show vpdn tunnel all** command:

```
ENT_HGW# show vpdn
% No active L2TP tunnels

L2F Tunnel and Session

 NAS CLID HGW CLID NAS Name        HGW Name        State
 36       1        ISP_NAS         ENT_HGW         open
                   172.22.66.23    172.22.66.25

 CLID   MID    Username                  Intf   State
 36     1      jeremy@hgw.com            Vi1    open

ENT_HGW# show vpdn tunnel all
% No active L2TP tunnels

L2F Tunnel
NAS name: ISP_NAS
NAS CLID: 36
NAS IP address 172.22.66.23
Gateway name: ENT_HGW
Gateway CLID: 1
Gateway IP address 172.22.66.25
State: open
Packets out: 52
Bytes out: 1799
Packets in: 100
Bytes in: 7143
```

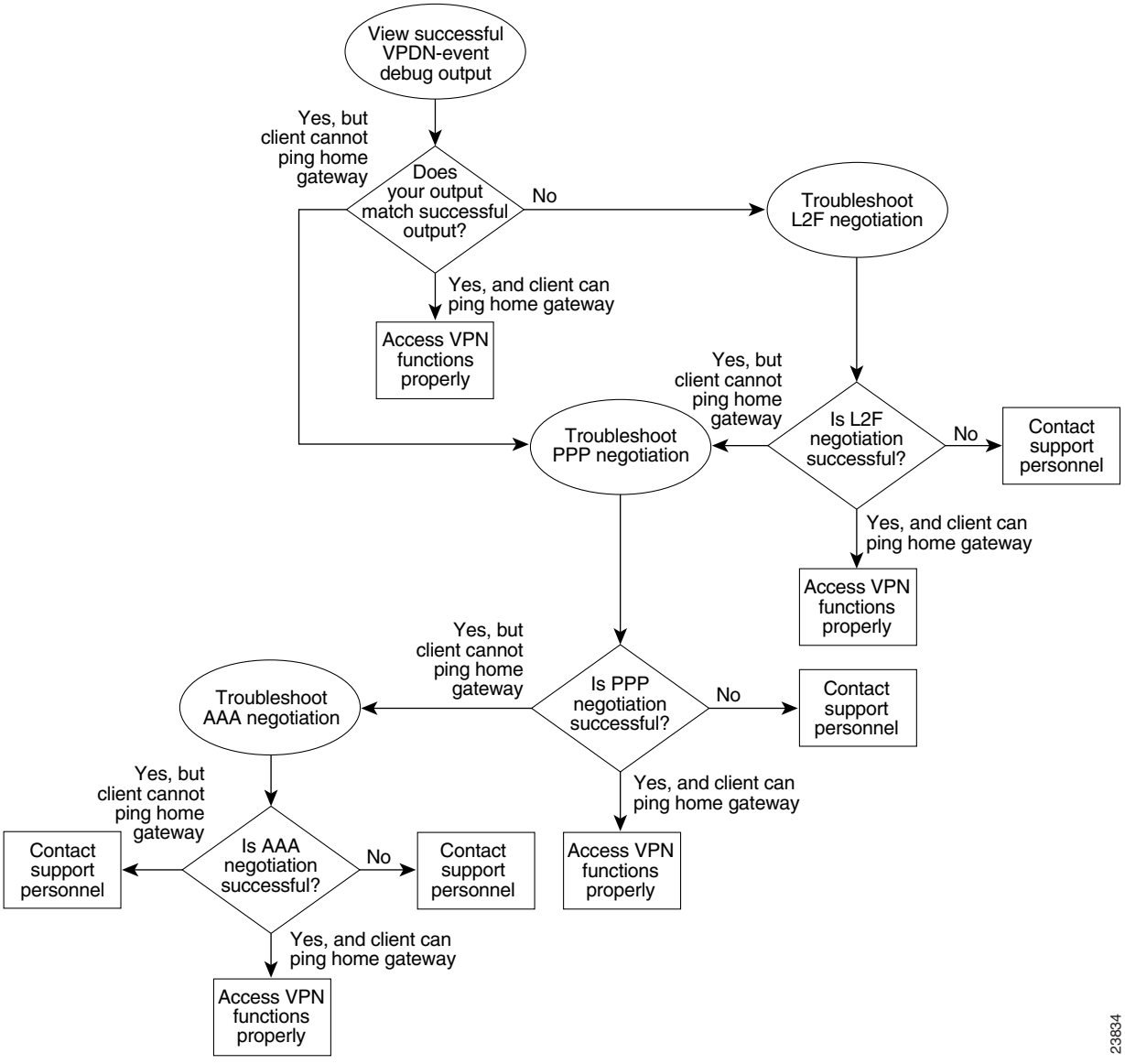
Troubleshooting the Access VPN

This section provides the ISP and enterprise customer with a methodology for troubleshooting the access VPN as described in Figure 16. Step 1 shows debug output from a successful call. If your debug output does not match the successful output, follow the remaining steps to begin troubleshooting the network. The bolded lines of debug output indicate important information.

- Step 1—Comparing Your Debug Output to the Successful Debug Output
- Step 2—Troubleshooting L2F Negotiation
- Step 3—Troubleshooting PPP Negotiation
- Step 4—Troubleshooting AAA Negotiation

Figure 16 describes the methodology used to troubleshoot the Access VPN.

Figure 16 Troubleshooting Flow Diagram for Access VPN with Local AAA



If you are accessing the NAS and home gateway through a Telnet connection, enable the **terminal monitor** command, which ensures that your EXEC session is receiving the logging and debug output from the devices.

When you finish troubleshooting, use the **undebug all** command to turn off all debug commands. Isolating debug output helps you efficiently build a network.

Step 1—Comparing Your Debug Output to the Successful Debug Output

Enable the **debug vpdn-event** command on both the NAS and the home gateway. The following debug output shows successful VPN negotiation on the NAS and home gateway:

```
ISP_NAS#
Jan  7 00:19:35.900: %LINK-3-UPDOWN: Interface Async9, changed state to up
Jan  7 00:19:39.532: sVPDN: Got DNIS string As9
Jan  7 00:19:39.532: As9 VPDN: Looking for tunnel -- hgw.com --
Jan  7 00:19:39.540: As9 VPDN: Get tunnel info for hgw.com with NAS ISP_NAS,
IP172.22.66.25
Jan  7 00:19:39.540: As9 VPDN: Forward to address 172.22.66.25
Jan  7 00:19:39.540: As9 VPDN: Forwarding...
Jan  7 00:19:39.540: As9 VPDN: Bind interface direction=1
Jan  7 00:19:39.540: As9 VPDN: jeremy@hgw.com is forwarded
Jan  7 00:19:40.540: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async9, changed
state to up
ISP_NAS#

ENT_HGW#
Jan  7 00:19:39.967: VPDN: Chap authentication succeeded for ISP_NAS
Jan  7 00:19:39.967: Vi1 VPDN: Virtual interface created for jeremy@hgw.com
Jan  7 00:19:39.967: Vi1 VPDN: Set to Async interface
Jan  7 00:19:39.971: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
6w5d: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan  7 00:19:40.051: Vi1 VPDN: Bind interface direction=2
Jan  7 00:19:40.051: Vi1 VPDN: PPP LCP accepted rcv CONFACK
Jan  7 00:19:40.051: Vi1 VPDN: PPP LCP accepted sent CONFACK
6w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
up
```

If you see the above debug output but cannot ping the home gateway, go on to "Step 3—Troubleshooting PPP Negotiation."

If you do not see the above debug output, go on to "Step 2—Troubleshooting L2F Negotiation."

Step 2—Troubleshooting L2F Negotiation

This step describes several common misconfigurations that prevent successful L2F negotiation.

- Misconfigured NAS Tunnel Secret
- Misconfigured Home Gateway Tunnel Secret
- Misconfigured Tunnel Name

Misconfigured NAS Tunnel Secret

The NAS and the home gateway must both have the same usernames with the same password to authenticate the L2F tunnel. These usernames are called the tunnel secret. In this case study, these usernames are ISP_NAS and ENT_HGW. The password is "cisco" for both usernames on both systems.

If one of the tunnel secrets on the NAS is incorrect, you will see the following debug output when you dial in to the NAS and the **debug vpdn l2x-errors** command is enabled on the NAS and home gateway:

```
ISP_NAS#
Jan  1 00:26:49.899: %LINK-3-UPDOWN: Interface Async3, changed state to up
Jan  1 00:26:54.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async3, cha
nged state to up
Jan  1 00:27:00.559: L2F: Resending L2F_OPEN, time #1
Jan  1 00:27:05.559: L2F: Resending L2F_ECHO, time #1
Jan  1 00:27:05.559: L2F: Resending L2F_OPEN, time #2
Jan  1 00:27:10.559: L2F: Resending L2F_ECHO, time #2
Jan  1 00:27:10.559: L2F: Resending L2F_OPEN, time #3
Jan  1 00:27:15.559: L2F: Resending L2F_ECHO, time #3
Jan  1 00:27:15.559: L2F: Resending L2F_OPEN, time #4
Jan  1 00:27:20.559: L2F: Resending L2F_ECHO, time #4
Jan  1 00:27:20.559: L2F: Resending L2F_OPEN, time #5
Jan  1 00:27:25.559: L2F: Resending L2F_ECHO, time #5
Jan  1 00:27:25.559: L2F: Resend packet (type 2) around too long, time to kill off the
tunnel
ISP_NAS#

ENT_HGW#
Jan  1 00:26:53.645: L2F: Packet has bogus2 key C8353FAB B6369121
5w6d: %VPDN-6-AUTHENFAIL: L2F HGW , authentication failure for  tunnel ISP_NAS; Invalid
key
5w6d: %VPDN-5-UNREACH: L2F NAS 172.22.66.23 is unreachable
Jan  1 00:27:00.557: L2F: Gateway received tunnel OPEN while in state closed
ENT_HGW#
```

The phrase “time to kill off the tunnel” in the NAS debug output indicates that the tunnel was not opened. The phrase “Packet has bogus2 key” in the home gateway debug output indicates that the NAS has an incorrect tunnel secret.

To avoid this problem, make sure that you configure both the NAS and home gateway for the same two usernames with the same password.

Misconfigured Home Gateway Tunnel Secret

If one of the tunnel secrets on the home gateway is incorrect, you will see the following debug output when you dial in to the NAS and the **debug vpdn l2x-errors** command is enabled on the NAS and home gateway:

```
ISP_NAS#
Jan  1 00:45:27.123: %LINK-3-UPDOWN: Interface Async7, changed state to up
Jan  1 00:45:30.939: L2F: Packet has bogus1 key B6C656EE 5FAC6B3
Jan  1 00:45:30.939: %VPDN-6-AUTHENFAIL: L2F NAS ISP_NAS, authentication failure
 for  tunnel ENT_HGW; Invalid key
Jan  1 00:45:31.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, cha
nged state to up
Jan  1 00:45:35.559: L2F: Resending L2F_OPEN, time #1
Jan  1 00:45:35.559: L2F: Packet has bogus1 key B6C656EE 5FAC6B3
ISP_NAS#

ENT_HGW#
Jan  1 00:45:30.939: L2F: Tunnel authentication succeeded for ISP_NAS
Jan  1 00:45:35.559: L2F: Gateway received tunnel OPEN while in state open
Jan  1 00:45:40.559: L2F: Gateway received tunnel OPEN while in state open
Jan  1 00:45:45.559: L2F: Gateway received tunnel OPEN while in state open
Jan  1 00:45:50.559: L2F: Gateway received tunnel OPEN while in state open
```

Notice how this output is similar to the debug output you see when the NAS has a misconfigured tunnel secret. This time you see the phrase "Packet has bogus1 key" on the NAS instead of on the home gateway. This tells you that the home gateway has an incorrect tunnel secret.

To avoid this problem, make sure that you configure both the NAS and home gateway for the same two usernames with the same password.

Misconfigured Tunnel Name

If the NAS and home gateway do not have matching tunnel names, they cannot establish an L2F tunnel. These tunnel names are configured under the **vpdn-group 1** command on both the NAS and the home gateway by using the **local name** command.

The home gateway must be configured to accept tunnels from the name the NAS sends it. This is done by using the **accept dialin l2f virtual-template 1 remote ISP_NAS** command, where **ISP_NAS** is the name. The name the home gateway returns to the NAS is configured by using the **local name ENT_HGW** command where **ENT_HGW** is the name. These commands appear in the running configuration as follows:

```
vpdn-group 1
 accept dialin l2f virtual-template 1 remote ISP_NAS
 local name ENT_HGW
```

In the following debug output, the NAS attempted to open a tunnel by using the name isp. Because the home gateway did not know this name, it did not open the tunnel. To see the following debug output, enable the **debug vpdn l2x-events** and **debug vpdn l2x-errors** commands on the home gateway:

```
ENT_HGW#
Jan  1 01:28:54.207: L2F: L2F_CONF received
Jan  1 01:28:54.207: L2X: Never heard of isp
Jan  1 01:28:54.207: L2F: Couldn't find tunnel named isp
```

To avoid the above problem, make sure that the tunnel names match on the home gateway and on the NAS.

If you fixed the problem in your configuration, go back to "Verifying the Access VPN."

If your call still cannot successfully complete L2F negotiation, contact your support personnel.

Step 3—Troubleshooting PPP Negotiation

Enable the **debug ppp negotiation** command on the home gateway and dial in to the NAS. You should not need to enable this command on the NAS, because you already verified dial up connectivity to the NAS in "Configuring the NAS for Basic Dial Access."

The following debug output shows successful PPP negotiation on the home gateway:

```
1d02h: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Feb  4 14:14:40.505: Vi1 PPP: Treating connection as a dedicated line
*Feb  4 14:14:40.505: Vi1 PPP: Phase is ESTABLISHING, Active Open
*Feb  4 14:14:40.505: Vi1 PPP: Treating connection as a dedicated line
*Feb  4 14:14:40.505: Vi1 PPP: Phase is AUTHENTICATING, by this end
*Feb  4 14:14:40.509: Vi1 PPP: Phase is UP
```

If your call successfully completed PPP negotiation, but you still cannot ping the home gateway, go on to "Step 4—Troubleshooting AAA Negotiation."

If your call cannot successfully complete PPP negotiation, contact your support personnel.

Step 4—Troubleshooting AAA Negotiation

This section first shows debug output of successful AAA negotiation. It then explains a common misconfiguration that prevents successful AAA negotiation.

- Successful AAA Negotiation
- Incorrect User Password

Successful AAA Negotiation

Enable the **debug aaa authentication** and **debug aaa authorization** commands on the home gateway.

The following debug output shows successful AAA negotiation on the home gateway. This output has been edited to exclude repetitive lines.

```
Jan 15 21:35:10.902: AAA/AUTHEN: create_user (0x612C5DE4) user='ENT_HGW' ruser='
' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 15 21:35:10.902: AAA/AUTHEN/START (1765780899): port='' list='default' actio
n=SENDAUTH service=PPP
Jan 15 21:35:10.902: AAA/AUTHEN/START (1765780899): found list default
Jan 15 21:35:10.902: AAA/AUTHEN/START (1765780899): Method=LOCAL
Jan 15 21:35:10.902: AAA/AUTHEN (1765780899): status = PASS
Jan 15 21:35:10.902: AAA/AUTHEN: create_user (0x612C5DE4) user='ISP_NAS' ruser='
' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 15 21:35:10.906: AAA/AUTHEN/START (990949917): port='' list='default' action
=SENDAUTH service=PPP
Jan 15 21:35:10.906: AAA/AUTHEN/START (990949917): found list default
Jan 15 21:35:10.906: AAA/AUTHEN/START (990949917): Method=LOCAL
Jan 15 21:35:10.906: AAA/AUTHEN (990949917): status = PASS
8w0d: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 15 21:35:10.994: AAA/AUTHEN: create_user (0x612E4234) user='jeremy@hgw.com'
ruser='' port='Virtual-Access1' rem_addr='408/5550945' authen_type=CHAP service=
PPP priv=1
Jan 15 21:35:10.994: AAA/AUTHEN/START (2063987649): port='Virtual-Access1' list=
'' action=LOGIN service=PPP
Jan 15 21:35:10.994: AAA/AUTHEN/START (2063987649): using "default" list
Jan 15 21:35:10.994: AAA/AUTHEN/START (2063987649): Method=LOCAL
Jan 15 21:35:10.994: AAA/AUTHEN (2063987649): status = PASS
Jan 15 21:35:10.994: Vi1 AAA/AUTHOR/LCP: Authorize LCP
Jan 15 21:35:10.994: AAA/AUTHOR/LCP Vi1 (2975944584): Port='Virtual-Access1' lis
t='' service=NET
Jan 15 21:35:10.994: AAA/AUTHOR/LCP: Vi1 (2975944584) user='jeremy@hgw.com'
Jan 15 21:35:10.998: AAA/AUTHOR/LCP: Vi1 (2975944584) send AV service=ppp
Jan 15 21:35:10.998: AAA/AUTHOR/LCP: Vi1 (2975944584) send AV protocol=lcp
Jan 15 21:35:10.998: AAA/AUTHOR/LCP (2975944584) found list "default"
Jan 15 21:35:10.998: AAA/AUTHOR/LCP: Vi1 (2975944584) Method=LOCAL
Jan 15 21:35:10.998: AAA/AUTHOR (2975944584): Post authorization status = PASS_REPL
Jan 15 21:35:10.998: Vi1 AAA/AUTHOR/FSM: We can start IPCP
8w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed s
tate to up
Jan 15 21:35:14.094: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we want 1
72.30.2.1
```

If this debug output appears, but you still cannot ping the home gateway, contact your support personnel and troubleshoot your network's backbone.

If you do not see this debug output, troubleshoot AAA negotiation.

Incorrect User Password

If the user password is incorrect (or it is incorrectly configured), the tunnel will be established, but the home gateway will not authenticate the user. If the user password is incorrect, the following debug output appears on the NAS and home gateway when you dial in to the NAS and the **debug vpdn l2x-errors** and **debug vpdn l2x-events** commands are enabled:

```
ISP_NAS#
Jan  1 01:00:01.555: %LINK-3-UPDOWN: Interface Async12, changed state to up
Jan  1 01:00:05.299:  L2F: Tunnel state closed
Jan  1 01:00:05.299:  L2F: MID  state closed
Jan  1 01:00:05.299: L2F: Open UDP socket to 172.22.66.25
Jan  1 01:00:05.299:  L2F: Tunnel state opening
Jan  1 01:00:05.299: As12 L2F: MID jeremy@hgw.com state waiting_for_tunnel
Jan  1 01:00:05.303: L2F: L2F_CONF received
Jan  1 01:00:05.303: L2F: Removing resend packet (L2F_CONF)
Jan  1 01:00:05.303: ENT_HGW L2F: Tunnel state open
Jan  1 01:00:05.307: L2F: L2F_OPEN received
Jan  1 01:00:05.307: L2F: Removing resend packet (L2F_OPEN)
Jan  1 01:00:05.307: L2F: Building nas2gw_mid0
Jan  1 01:00:05.307: L2F: L2F_CLIENT_INFO: CLID/DNIS 4089548021/5550945
Jan  1 01:00:05.307: L2F: L2F_CLIENT_INFO: NAS-Port Async12
Jan  1 01:00:05.307: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
Jan  1 01:00:05.307: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/26400/28800
Jan  1 01:00:05.307: As12 L2F: MID jeremy@hgw.com state opening
Jan  1 01:00:05.307: L2F: Tunnel authentication succeeded for ENT_HGW
Jan  1 01:00:05.391: L2F: L2F_OPEN received
Jan  1 01:00:05.391: L2F: Got a MID management packet
Jan  1 01:00:05.391: L2F: Removing resend packet (L2F_OPEN)
Jan  1 01:00:05.391: As12 L2F: MID jeremy@hgw.com state open
Jan  1 01:00:05.391: As12 L2F: MID synced NAS/HG Clid=47/12 Mid=1
Jan  1 01:00:05.523: L2F: L2F_CLOSE received
Jan  1 01:00:05.523: %VPDN-6-AUTHENERR: L2F HGW ENT_HGW cannot locate a AAA server for
As12 user jeremy@hgw.com; Authentication failure

ENT_HGW#
Jan  1 01:00:05.302: L2F: L2F_CONF received
Jan  1 01:00:05.302: L2F: Creating new tunnel for ISP_NAS
Jan  1 01:00:05.302:  L2F: Tunnel state closed
Jan  1 01:00:05.302: L2F: Got a tunnel named ISP_NAS, responding
Jan  1 01:00:05.302: L2F: Open UDP socket to 172.22.66.23
Jan  1 01:00:05.302: ISP_NAS L2F: Tunnel state opening
Jan  1 01:00:05.306: L2F: L2F_OPEN received
Jan  1 01:00:05.306: L2F: Removing resend packet (L2F_CONF)
Jan  1 01:00:05.306: ISP_NAS L2F: Tunnel state open
Jan  1 01:00:05.306: L2F: Tunnel authentication succeeded for ISP_NAS
Jan  1 01:00:05.310: L2F: L2F_OPEN received
Jan  1 01:00:05.310: L2F: L2F_CLIENT_INFO: CLID/DNIS 4089548021/5550945
Jan  1 01:00:05.310: L2F: L2F_CLIENT_INFO: NAS-Port Async12
Jan  1 01:00:05.310: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
Jan  1 01:00:05.310: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/26400/28800
Jan  1 01:00:05.310: L2F: Got a MID management packet
Jan  1 01:00:05.310:  L2F: MID  state closed
Jan  1 01:00:05.310: L2F: Start create mid intf process for jeremy@hgw.com
5w6d: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan  1 01:00:05.390: Vi1 L2X: Discarding packet because of no mid/session
Jan  1 01:00:05.390: Vi1 L2F: Transfer NAS-Rate L2F/26400/28800 to LCP
Jan  1 01:00:05.390: Vi1 L2F: Finish create mid intf for jeremy@hgw.com
Jan  1 01:00:05.390: Vi1 L2F: MID jeremy@hgw.com state open
5w6d: %VPDN-6-AUTHENERR: L2F HGW ENT_HGW cannot locate a AAA server for Vi1 user
jeremy@hgw.com; Authentication failure
```

If the access VPN now works by using local AAA, go on to "Configuring the Access VPN to Work with Remote AAA." If you do not see this debug output, contact your support personnel.