Configuring the Access VPN to Work with Remote AAA

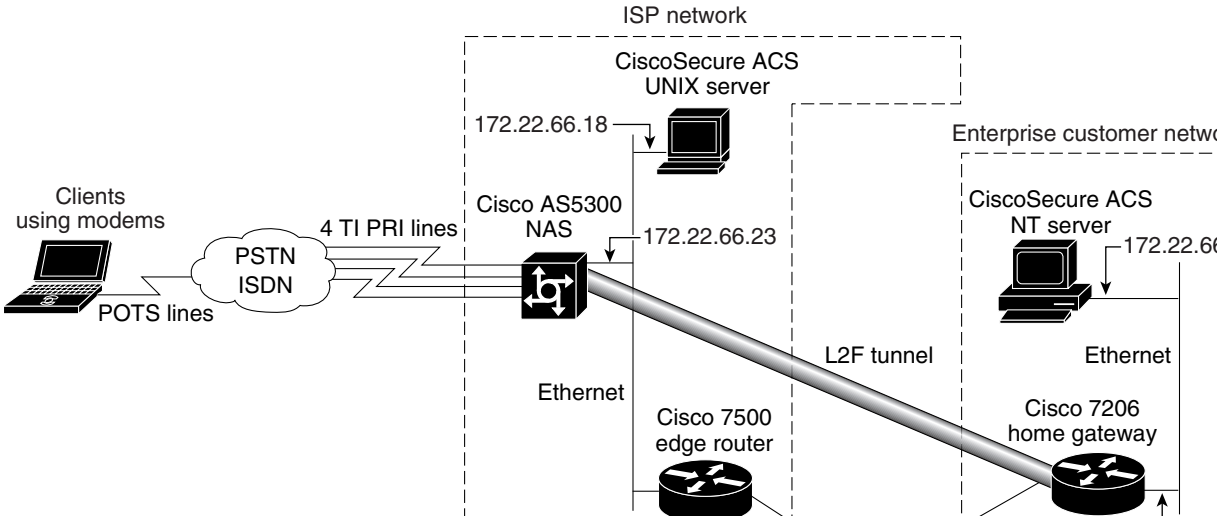
Introduction

In this third task, the ISP and the enterprise customer:

- Reconfigure the NAS and home gateway to work as an access VPN using remote AAA. To ensure that the access VPN is using remote AAA, the ISP and enterprise customer modify the AAA and VPN configurations on the NAS and home gateway.
- Configure CiscoSecure ACS on the UNIX and NT servers. The NAS uses CiscoSecure UNIX to authenticate the user's domain name and to determine the IP tunnel endpoint information. The home gateway uses CiscoSecure NT to authenticates the user's username and password. The NAS and home gateway continue to use their local username databases to authenticate the tunnel.
- Verify that the access VPN works properly.
- Troubleshoot the access VPN if there are problems.

The ISP configures the NAS and CiscoSecure UNIX. The enterprise customer configures the home gateway and CiscoSecure NT. Figure 17 shows the access VPN network topology.

Figure 17 Access VPN Topology Using Remote 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 CiscoSecure UNIX server authenticates the domain name, hgw.com, and supplies the NAS with the tunnel endpoint information.
- The NAS negotiates an L2F tunnel with the home gateway. The NAS and home gateway authenticate the tunnel by using their local username databases, which contain the tunnel secret. Once the tunnel is established, the NAS forwards the call to the home gateway.
- The CiscoSecure NT server 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 access VPN solution to work with remote AAA, follow these steps:

- Step 1—Configuring the NAS
- Step 2—Configuring the Home Gateway
- Step 3—Configuring the CiscoSecure ACS UNIX Server
- Step 4—Configuring the CiscoSecure ACS NT Server

Step 1—Configuring the NAS

In this step, the ISP:

- Moves the responsibilities for domain name authentication and tunnel endpoint determination from the NAS to the remote CiscoSecure UNIX server
- Points the NAS to the CiscoSecure UNIX server
- Removes unnecessary commands

Use this command	To do this
`ISP_NAS(config)# aaa authentication ppp default local radius`	Instruct AAA to first use the local database and then use the RADIUS server (CiscoSecure NT) for PPP and VPN authentication. The order of authentication methods is local first and RADIUS second because the tunnel is authenticated locally and the user's domain name is authenticated by the CiscoSecure UNIX server.
`ISP_NAS(config)# aaa authorization network default radius`	Instruct AAA to use the CiscoSecure UNIX server to authorize network-related service requests.
`ISP_NAS(config)# radius-server host 172.22.66.18`	Enter the CiscoSecure UNIX server's IP address.

Use this command	To do this
`ISP_NAS(config)# radius-server key cisco`	Define a key to decrypt the data that runs between the NAS and the CiscoSecure UNIX server. **Note** This key must be configured as "cisco." Cisco's RADIUS has a hard-coded password of "cisco"; this is separate from the NAS and home gateway passwords used to authenticate each other.
`ISP_NAS(config)# no vpdn-group 1`	Remove the VPN[1] group. All of the tunneling information will now be retrieved using RADIUS at the CiscoSecure UNIX server.

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

Step 2—Configuring the Home Gateway

In this step, the enterprise customer:

- Moves the responsibility for username authentication from the NAS to the remote CiscoSecure NT server
- Points the home gateway to the CiscoSecure NT server
- Removes the client's username and password from the home gateways username database

Use this command	To do this
`ENT_HGW(config)# aaa authentication ppp default local radius`	Instruct AAA to first use the local database and then use the RADIUS server (CiscoSecure NT) for PPP and VPN authentication. The order of authentication methods is local first and RADIUS second because the tunnel is authenticated locally, and the user's username and password are authenticated by the CiscoSecure NT server.
`ENT_HGW(config)# aaa authorization network default radius`	Instruct AAA to use the CiscoSecure NT server to authorize network-related service requests.
`ENT_HGW(config)# aaa accounting network default start-stop radius`	Enable AAA accounting that sends a stop accounting notice at the end of the requested user process.
`ENT_HGW(config)# radius-server host 172.22.66.13 auth-port 1645 acct-port 1646`	Specify the CiscoSecure NT server's IP address and the ports to be used for authentication and accounting requests.
`ENT_HGW(config)# radius-server key cisco`	Set the authentication key and encryption key to "cisco" for all RADIUS communication.
`ENT_HGW(config)# no username jeremy@hgw.com`	Remove the jeremy@hgw.com username from the local database. This ensures that the home gateway uses CiscoSecure NT instead of the local username database to authenticate the username.

Step 3—Configuring the CiscoSecure ACS UNIX Server

In this step, the ISP configures CiscoSecure ACS UNIX to:

- Authenticate VPN
- Discover the IP tunnel endpoint information
- Track the accounting information relating to VPN usage

The following procedure shows how to configure CiscoSecure UNIX by using RADIUS as the security protocol.

The ISP can configure CiscoSecure UNIX by:

- Using the CiscoSecure UNIX server GUI-based interface
- Using the UNIX command line interface (CLI)

The following procedure shows the CLI method of configuring CiscoSecure UNIX.

Note The password "cisco" is used throughout the following configuration. There is only one place in the following configuration where using the password "cisco" is mandatory: the profile named "vpdn."

Use this command	To do this
`pagoda# cd /cs/CLI`	Change your working directory to the CLI directory in the CiscoSecure directory.

`pagoda# vi vpdn`
 	
`radius=Cisco11.3 {`
`check_items= {`
`2=cisco`
`6=5`
`}`
`reply_attributes= {`
`9,1="vpdn:gw-password=cisco"`
`9,1="vpdn:nas-password=cisco"`
`9,1="vpdn:tunnel-id=ISP_NAS"`
`9,1="vpdn:ip-addresses=172.22.66.25"`
`}`
	Open a vi editor session and create a file called vpdn.
	
	The vpdn file contains all the VPN RADIUS authentication and authorization attributes needed for the home gateway user. In this file:
	
	• **2=** defines the IETF RADIUS password attribute. In this instance, the password must be "cisco."
	
	Note In this particular file, you need to use the password "cisco." The vpdn profile is the one and only profile that actually interfaces directly with Cisco IOS software. Cisco's implementation of RADIUS needs a password to operate; for security reasons, that password should not reside on the NAS. Cisco has hard-coded the password "cisco" in Cisco IOS to address this security issue.
	
	• **6=** defines the IETF RADIUS user-service-type attribute. In this instance, 5 indicates a value of outbound user.
	
	Reply attributes send information from the RADIUS security server to the NAS. The following reply attributes need to be defined:
	
	• **gw-password=** defines the home gateway password as "cisco."
	
	• **nas-password=** defines the NAS password as "cisco."
	
	• **tunnel-id=** defines the name of the VPN tunnel as ISP_NAS.
	
	• **ip-addresses=** defines the IP address of the home gateway as 172.22.66.25.

`:wq!`	Exit the vi editor session and save the vpdn file.

Use this command	To do this
pagoda# **vi ENT_HGW** **radius=Cisco11.3 {** **check_items= {** **2=cisco** **}** **}**	Open a vi editor session and create a file called ENT_HGW that contains a password for the home gateway user. In this file: • **radius=** defines the version of RADIUS as being that contained in Cisco IOS Release 11.3. • **2=** defines the password for the home gateway user. In this instance, any password can be used.
:wq!	Exit the vi editor session and save the ENT_HGW file.
pagoda# **vi ISP_NAS** **radius=Cisco11.3 {** **check_items= {** **2=cisco** **}** **}**	Open a vi editor session and create a file called ISP_NAS that contains the password for the user created by the tunnel-id attribute. In this file: • **radius=** defines the version of RADIUS as being that contained in Cisco IOS Release 11.3. • **2=** defines the password for the home gateway user. In this instance, any password can be used.
:wq!	Exit the vi editor session and save the ISP_NAS file.
pagoda# **vi nas_list** **NAS.172.22.66.23**	Open a vi editor session and create a file named nas_list that adds 172.22.66.23 to the NAS list. **Note** In this case study, only one NAS is used: the NAS with the IP address of 172.22.66.23. If you have more than one NAS in your network, it is imperative that all NASs be added to the NAS list or authentication will fail.
:wq!	Exit the vi editor session and save the nas_list file.
pagoda# **vi nas1** **NASName="172.22.66.23"** **SharedSecret="cisco"** **RadiusVendor="Cisco"** **Dictionary="DICTIONARY.Cisco11.3"**	Open a vi editor session and create a profile for the NAS, which in this case is a file named nas1. This file identifies the RADIUS dictionary that the NAS uses, the NAS IP address, the applicable vendor, and the shared secret key. In this file: • **NASName=** defines nas1 as being the NAS identified by the IP address 172.22.66.23. • **SharedSecret=** defines the nas1 password as "cisco." • **RadiusVendor=** identifies the vendor code as "Cisco." • **Dictionary=** defines the version of the RADIUS dictionary as being that contained in Cisco IOS Release 11.3.
:wq!	Exit the vi editor session and save the nas1 file.
pagoda# **./DeleteProfile -p 9900 -u NAS_LIST** Profile Successfully Deleted pagoda#	The CLI does not support profile updates; you can only delete or add profiles. Because the ISP added a new NAS to the NAS_list, the ISP needs to delete the existing NAS list profile and create a new one. Delete the existing NAS_LIST profile where: • **-p 9900** indicates that Delete Profile uses this port to connect to the database. • **-u NAS_LIST** indicates the profile being deleted.

Use this command	To do this

`pagoda# ./AddProfile -p 9900 -u NAS_LIST -s nas_list`
`Profile Successfully Added`
`pagoda#`
	Create a new user profile called NAS_LIST where
	• **-p 9900** indicates that Add Profile uses this port to connect to the database.
	• **-u NAS_LIST** indicates the profile name.
	• **-s nas_list** indicates the file used to create this user profile.

`pagoda# ./AddProfile -p 9900 -u NAS.172.22.66.23 -s nas1`
`Profile Successfully Added`
`pagoda#`
	For each entry on the NAS_LIST, there must be a user profile for the associated NAS. Create a user profile for the NAS itself called NAS.172.22.66.23 where
	• **-p 9900** indicates that Add Profile uses this port to connect to the database.
	• **-u NAS.172.22.66.23** indicates the profile name.
	• **-s nas1** indicates the file used to create this user profile.

`pagoda# ./AddProfile -p 9900 -g NAS_Group`	Organize your group structure so that all VPN-related elements (such as associated NAS and home gateways) are gathered together in one group by creating a group called NAS_Group.

`pagoda# ./AddProfile -p 9900 -u hgw.com -pr NAS_Group -s vpdn`
`Profile Successfully Added`
`pagoda#`
	Add the participants to the created NAS group by creating the following users for this group: VPDN, ENT_HGW, and ISP_NAS
	Create a domain-based VPN user called hgw.com under the group NAS_Group where
	• **-p 9900** indicates that Add Profile uses this port to connect to the database.
	• **-u hgw.com** indicates the domain name.
	• **-pr NAS_Group** indicates which group this user belongs to.
	• **-s vpdn** indicates the file used to create this user profile.

`pagoda# ./AddProfile -p 9900 -u ENT_HGW -pr NAS_Group -s ENT_HGW`
`Profile Successfully Added`
`pagoda#`
	Create a home gateway user called ENT_HGW under the group NAS_Group where
	• **-p 9900** indicates that Add Profile uses this port to connect to the database.
	• **-u ENT_HGW** indicates the profile name.
	• **-pr NAS_Group** indicates which group this user belongs to.
	• **-s ENT_HGW** indicates the file used to create this user profile.

`pagoda# ./AddProfile -p 9900 -u ISP_NAS -pr NAS_Group -s ISP_NAS`
`Profile Successfully Added`
`pagoda#`
	Create a tunnel user called ISP_NAS under the group NAS_Group where
	• **-p 9900** indicates that Add Profile uses this port to connect to the database.
	• **-u ISP_NAS** indicates the tunnel profile name.
	• **-pr NAS_Group** indicates the group which this user belongs to.
	• **-s ISP_NAS** indicates the file used to create this user profile.

Use this command	To do this
pagoda# **cd /cs/config**	Modify the file called CSU.cfg to support VPN accounting records. Change your working directory to config.
pagoda# **vi CSU.cfg** DOMAIN config_local_domain = **{** **{** **"hgw.com",** **"@",** **suffix** **}** **};**	Open a vi editor session to modify the file called CSU.cfg where: • **DOMAIN config_local_domain=** means that the accounting records generated are for hgw.com. • **hgw.com** defines the name of the domain. • @ defines the delimiter. • **suffix** defines that the domain name is placed after the username.
:wq!	Exit the vi editor session and save the modifications to the CSU.cfg file.
pagoda# **/etc/rc0.d/K80CiscoSecure**	Shut down the CiscoSecure UNIX server.
pagoda# **/etc/rc2.d/S80CiscoSecure**	Restart the CiscoSecure UNIX server.

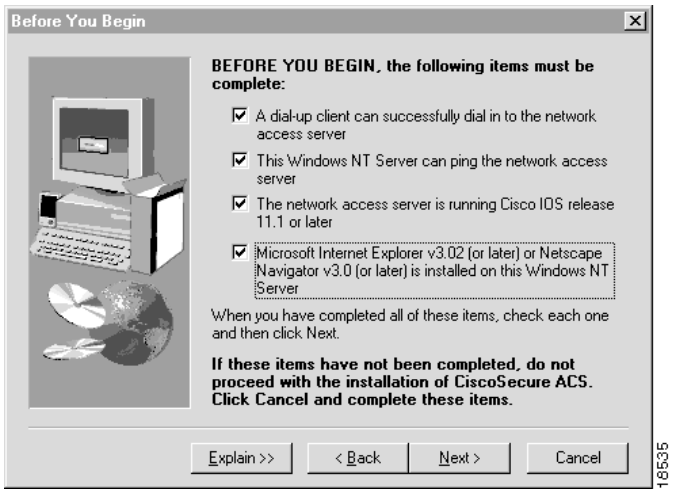
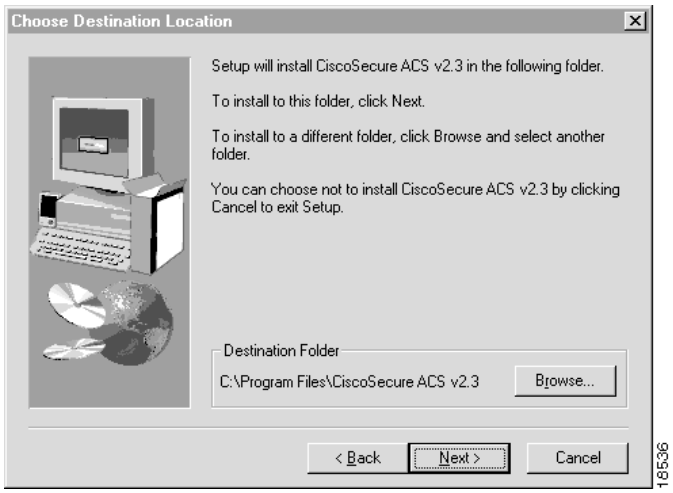
Step 4—Configuring the CiscoSecure ACS NT Server

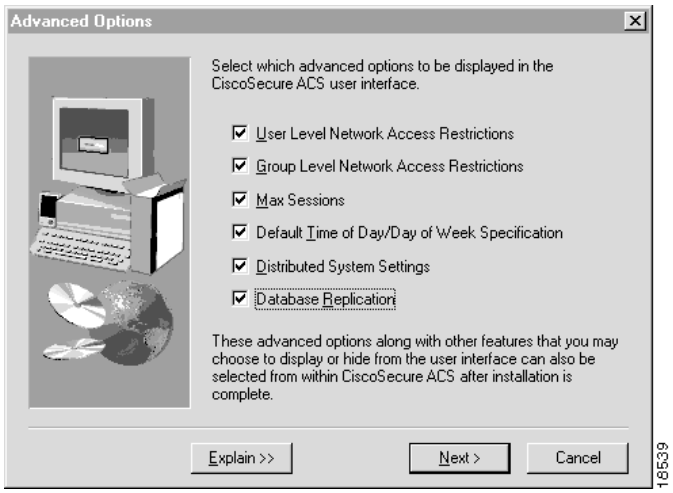
In this step, the enterprise customer:

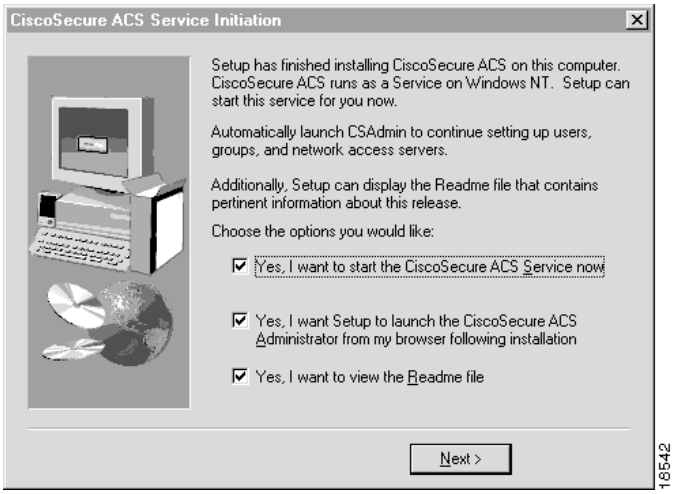
- Installs CiscoSecure NT, selecting RADIUS (Cisco) as the security protocol and identifying the access server by which authentication requests are transmitted
- Configures CiscoSecure NT to delete the domain name from incoming usernames so that the username matches the format CiscoSecure NT uses in its username/password database
- Creates a CiscoSecure NT user profile, which includes a username, password, and a description of the user

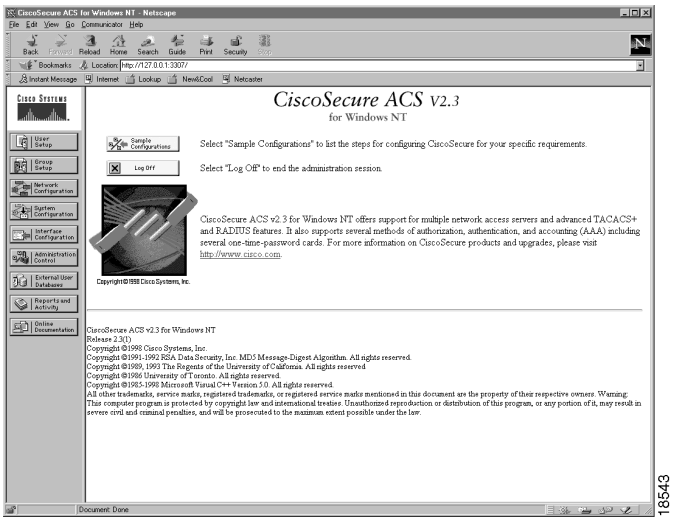
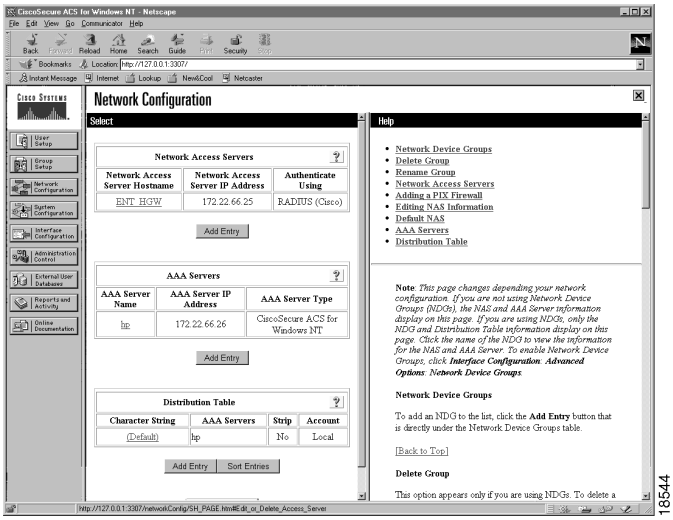
In CiscoSecure NT, basic accounting services are configured by default.

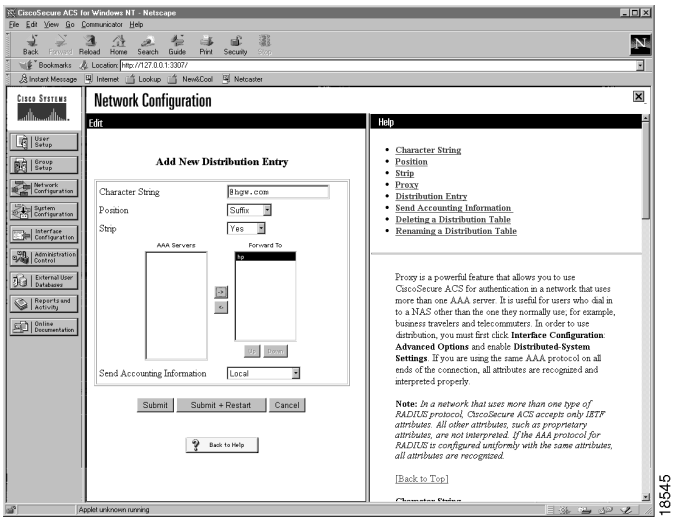
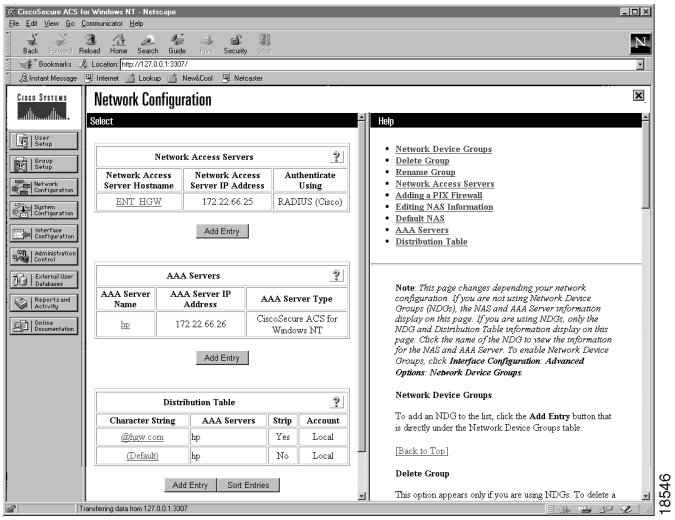
Note CiscoSecure NT refers to the home gateway as the network access server or just the access server. Make sure that when CiscoSecure NT prompts you to enter information about what it calls the access server, you enter the corresponding information about the home gateway. CiscoSecure NT does not communicate with the NAS. Therefore, the only server CiscoSecure NT refers to is the home gateway.

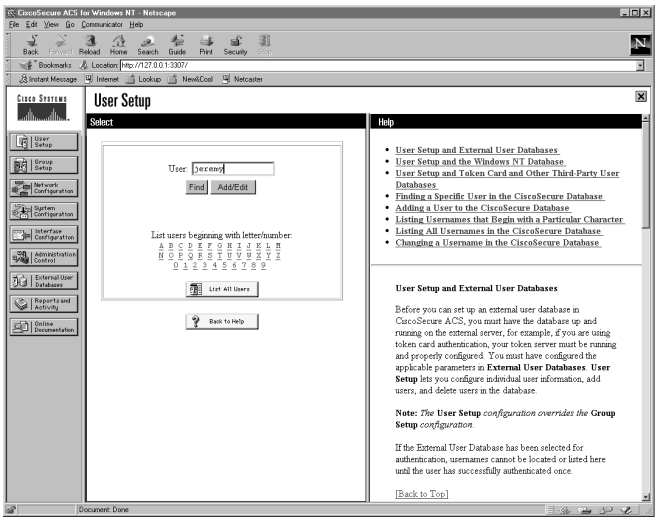
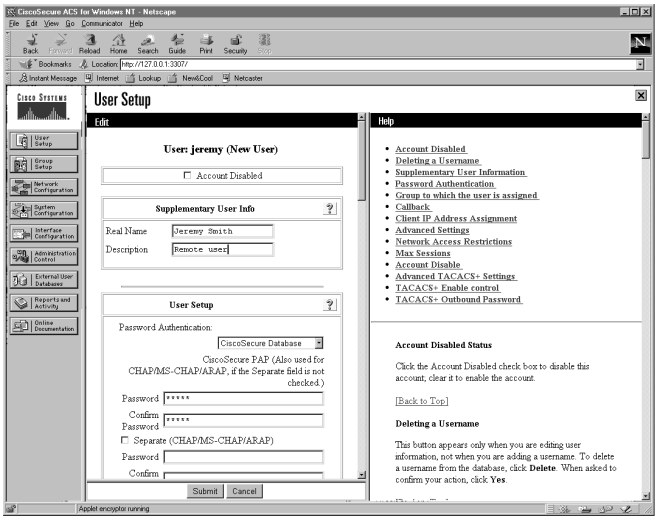
Use this display	To do this
	Install CiscoSecure NT. Before you can successfully install CiscoSecure NT, make sure you meet the following criteria: • A client can successfully dial in to the NAS. If you have successfully configured the access VPN to work with local AAA, you have met this criterion. • This Windows NT server can ping the NAS. If you have successfully configured the access VPN to work with local AAA, you have met this criterion. • The NAS is running Cisco IOS Release 11.1 or later release. • A compatible browser is installed on the Windows NT server. • On the Before You Begin screen, check all the corresponding boxes when the requirements are met. • Click **Next**.
	In the Choose Destination Location screen: • Select the folder where Setup will install CiscoSecure NT. • Click **Next**.
	In the Authentication Database Configuration screen, define the database where CiscoSecure NT authenticates users. You have the option to use either the: • Local CiscoSecure database or • Local CiscoSecure database and the Windows NT user database. In this scenario, only the local CiscoSecure database is queried for user accounts. • Click **CiscoSecure ACS database only**. • Click **Next**.

Use this display	To do this
	In the CiscoSecure ACS Network Access Server Details screen, select the security protocol. **Note** Remember that CiscoSecure NT calls the home gateway the network access server. • Select **RADIUS (Cisco)** in the security protocol box. • Type **ENT_HGW** in the Access Server Name box. • Type **172.22.66.25** in the Access Server IP Address box. • Type **172.22.66.13** in the Windows NT Server IP Address box. • Click **Next**.
	In the Advanced Options screen, define the advanced options that will appear in the CiscoSecure NT user interface. Click the following advanced options: • User level network access restrictions • Group level network access restrictions • Max sessions • Default time of day/day of week specification • Distributed system settings • Database replication • Click **Next**.
	In the Active Service Monitoring screen: • Click **Enable Log-in Monitoring** • Select Script to execute: *Restart All. • Click **Next**.

Use this display	To do this
	In the Network Access Server Configuration screen, click **Next**. Because you have already configured the home gateway, you do not need to use this automated configuration feature. **Note** Remember, CiscoSecure NT calls the home gateway the network access server. The installation is now complete.
	In the CiscoSecure ACS Service Initiation screen, you are asked if you want to start CiscoSecure NT service immediately and if you want Setup to launch the CiscoSecure NT Administrator from the installed browser immediately. To do so: • Click **Yes, I want to start CiscoSecure ACS Service now** • Click **Yes, I want Setup to launch the CiscoSecure ACS Administrator from my browser following installation** • Click **Next**.

Use this display	To do this
	In the CiscoSecure ACS Welcome screen, click **Network Configuration**. **Note** The address 127.0.0.1 is a loopback address. If you run the browser from the same system that CiscoSecure NT is installed on, this IP address appears in the HTTP browser field. However, if you want to run the browser on a system that is different than the one on which CiscoSecure NT has been installed, then the actual IP address of the device appears in the box.
	For CiscoSecure NT to authenticate a user, you must strip the domain name from the incoming username, so that the username matches the form that CiscoSecure NT uses in its username/password database. In the Network Configuration screen: Click **Add Entry** below the Distribution Table.

Use this display	To do this
	In the Add New Distribution Entry frame of the Network Configuration window, create a distribution entry: • Type **@hgw.com** in the Character string box. • Select **Suffix** in the Position box. • Select **Yes** in the Strip box. • Select **ENT_HGW** in the Forward to: box and click the right arrow to move it to the "Forward To" column. • Click **Submit and Restart**.
	After you click Submit and Restart, a summary of the information you have configured appears. Click **User Setup**.

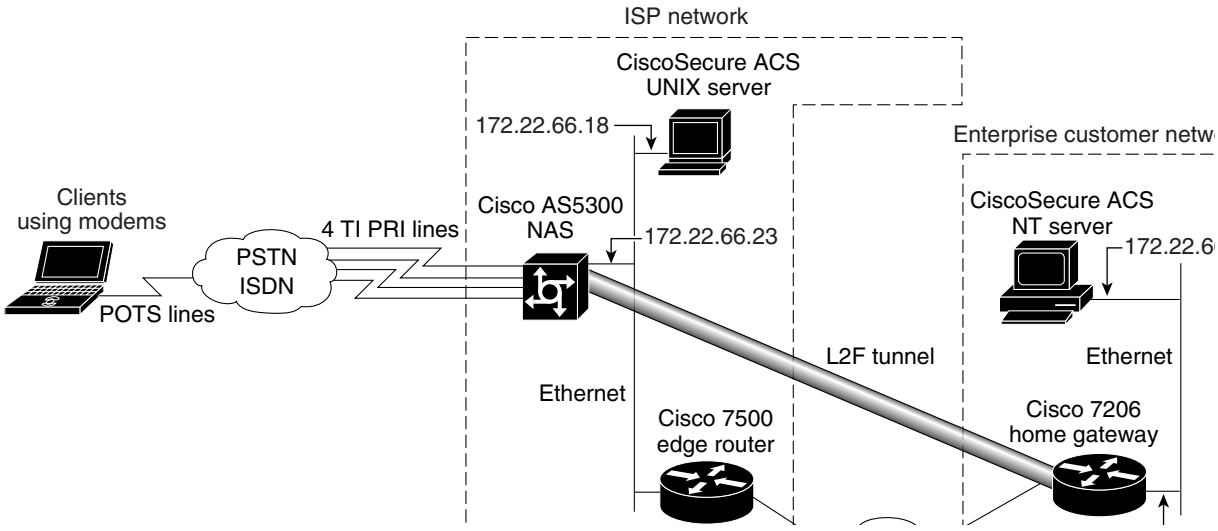
Use this display	To do this
	In the User Setup window, to create a user: • Type **jeremy** in the User box. • Click **Add/Edit**.
	In the User Setup screen, add the following supplementary user information: • Type **Jeremy Smith** in the Real Name box. • Type **Remote User** in the Description box. • Select **CiscoSecure Database** in the Password Authentication box. • Type **subaru** in the Password box. • Type **subaru** in the Confirm box. • Click **Submit**. You have now created a user named Jeremy.

Verifying the Access VPN

This section describes how to verify that the end-to-end connections function as shown in Figure 18:

- Step 1—Checking the NAS Final Running Configuration
- Step 2—Checking the Home Gateway Final 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 18 Access VPN Topology Using Remote AAA



After you successfully test these connections, the final end-to-end solution is built. If you experience problems, see "Troubleshooting the Access VPN."

Step 1—Checking the NAS Final 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 radius
aaa authorization network default radius
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
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
!
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
!
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 Final 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 radius
aaa authorization network default radius
aaa accounting network default start-stop radius
enable secret 5 $1$44oH$gZlAZLwylZJSNKGDk.BKb0
!
username jane-admin password 7 00001C05
username ISP_NAS password 7 070C285F4D06
username ENT_HGW password 7 104D000A0618
```

```
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
!
radius-server host 172.22.66.13 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password 7 045F0405
!
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 this 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 this 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 the **ping 172.22.66.25** command.

(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 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
```

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:

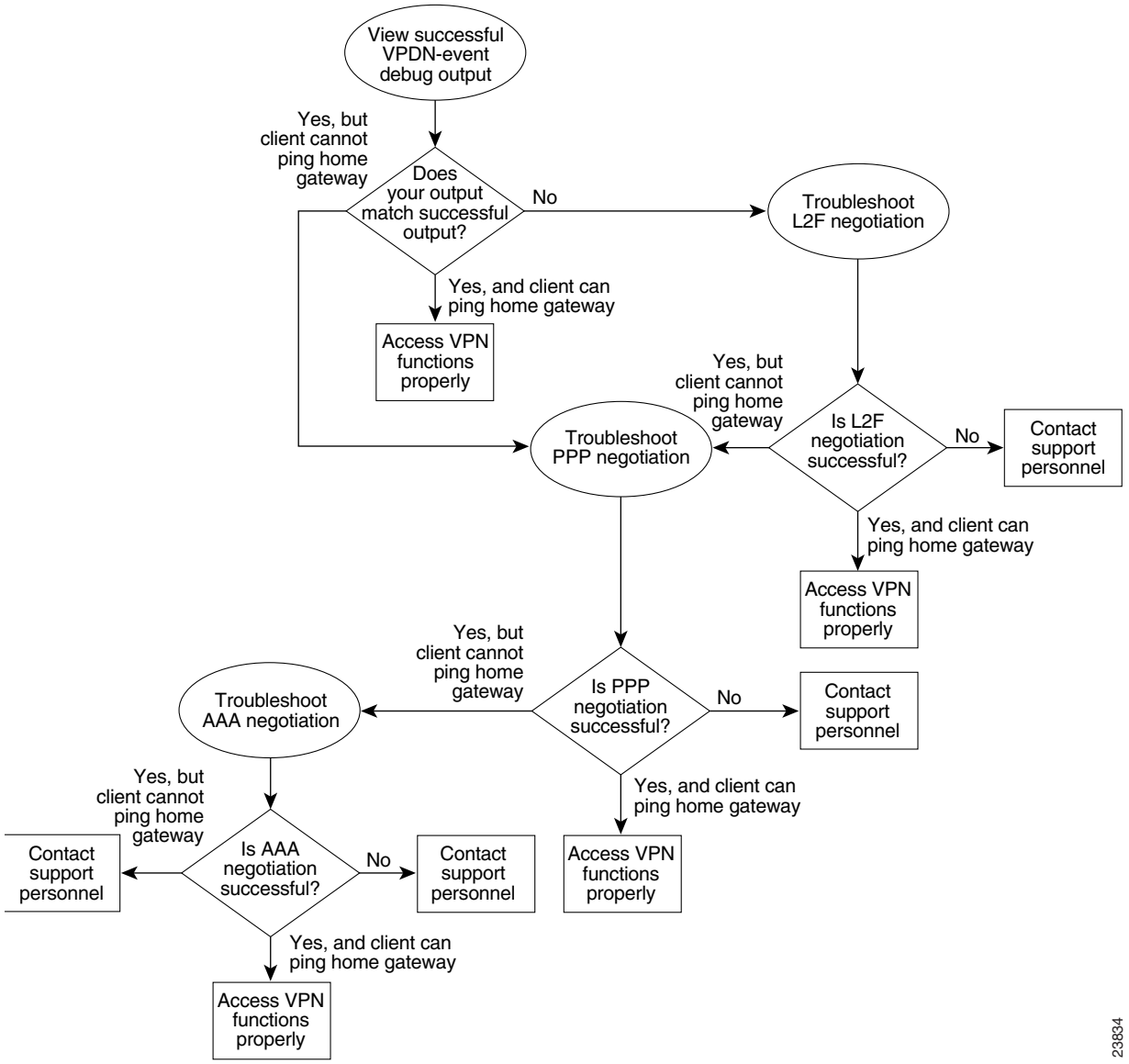
```
ENT_HGW# show vpdn

% 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 19. 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 19 Troubleshooting Flow Diagram for Access VPN with Remote AAA



If you are accessing the NAS and home gateway through a Telnet connection, you need to enable the **terminal monitor** command. This command 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 and dial in to the NAS. 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

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 of 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 tunnel secret usernames with the same password.

Misconfigured Home Gateway Tunnel Secret

If one of the tunnel secret usernames on the home gateway is incorrect, the following debug output appears 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

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 username. This time you see the phrase "Packet has bogus1 key" on the NAS instead of the home gateway. This tells you that the home gateway has an incorrect tunnel secret username.

To avoid this problem, make sure that you configure both the NAS and home gateway for the same two tunnel secret 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. On the home gateway, these tunnel names are configured under the **vpdn-group 1** command by using the **local name** command. On the NAS, these names are configured on the CiscoSecure UNIX server.

The home gateway must be configured to accept tunnels from the name the NAS sends it. This is done using the **accept dialin l2f virtual-template 1 remote ISP_NAS** command, where **ISP_NAS** is the name. The name it returns to the NAS is configured 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
```

On the CiscoSecure UNIX server, the tunnel names are configured by adding profiles to the **NAS_Group** group with the names **ISP_NAS** and **ENT_HGW**.

In the following debug output, the NAS attempted to open a tunnel 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 CiscoSecure UNIX server.

If you fixed the problem in your configuration, go back to the section "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 several common misconfigurations that prevent successful AAA negotiation.

- Successful AAA Negotiation
- Incorrect User Password
- Error Contacting RADIUS Server
- Misconfigured AAA Authentication

Successful AAA Negotiation

Enable the **debug aaa authentication** and **debug aaa authorization** commands on the home gateway and dial in to the NAS.

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

```
ENT_HGW#
Jan  7 19:29:44.132: AAA/AUTHEN: create_user (0x612D550C) user='ENT_HGW' ruser='
' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.132: AAA/AUTHEN/START (384300079): port='' list='default' action
=SENDAUTH service=PPP
Jan  7 19:29:44.132: AAA/AUTHEN/START (384300079): found list default
Jan  7 19:29:44.132: AAA/AUTHEN/START (384300079): Method=LOCAL
Jan  7 19:29:44.132: AAA/AUTHEN (384300079): status = PASS
Jan  7 19:29:44.132: AAA/AUTHEN: create_user (0x612D550C) user='ISP_NAS' ruser='
' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.132: AAA/AUTHEN/START (2545876944): port='' list='default' actio
n=SENDAUTH service=PPP
Jan  7 19:29:44.132: AAA/AUTHEN/START (2545876944): found list default
Jan  7 19:29:44.132: AAA/AUTHEN/START (2545876944): Method=LOCAL
Jan  7 19:29:44.132: AAA/AUTHEN (2545876944): status = PASS
Jan  7 19:29:44.228: AAA/AUTHEN: create_user (0x612F1F78) user='jeremy@hgw.com'
ruser='' port='Virtual-Access1' rem_addr='408/5550945' authen_type=CHAP service=
PPP priv=1
Jan  7 19:29:44.228: AAA/AUTHEN/START (101773535): port='Virtual-Access1' list=''
action=LOGIN service=PPP
Jan  7 19:29:44.228: AAA/AUTHEN/START (101773535): using "default" list
Jan  7 19:29:44.228: AAA/AUTHEN/START (101773535): Method=LOCAL
Jan  7 19:29:44.228: AAA/AUTHEN (101773535): status = ERROR
Jan  7 19:29:44.228: AAA/AUTHEN/START (101773535): Method=RADIUS
Jan  7 19:29:44.692: AAA/AUTHEN (101773535): status = PASS
Jan  7 19:29:44.692: Vi1 AAA/AUTHOR/LCP: Authorize LCP
Jan  7 19:29:44.692: AAA/AUTHOR/LCP Vi1 (3630870259): Port='Virtual-Access1' list=''
service=NET
Jan  7 19:29:44.692: AAA/AUTHOR/LCP: Vi1 (3630870259) user='jeremy@hgw.com'
Jan  7 19:29:44.692: AAA/AUTHOR/LCP: Vi1 (3630870259) send AV service=ppp
Jan  7 19:29:44.692: AAA/AUTHOR/LCP: Vi1 (3630870259) send AV protocol=lcp
Jan  7 19:29:44.692: AAA/AUTHOR/LCP (3630870259) found list "default"
Jan  7 19:29:44.692: AAA/AUTHOR/LCP: Vi1 (3630870259) Method=RADIUS
Jan  7 19:29:44.692: AAA/AUTHOR (3630870259): Post authorization status = PASS_REPL
Jan  7 19:29:44.696: Vi1 AAA/AUTHOR/FSM: We can start IPCP
6w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
up
```

```
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we want
172.30.2.1
```

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

If you did not see the debug output above, you need to 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
```

Error Contacting RADIUS Server

If the **aaa authorization** command on the home gateway is configured with the **default radius none** keywords, the home gateway may allow unauthorized access to your network.

This command is an instruction to first use RADIUS for authorization. The home gateway first contacts the RADIUS server (because of the **radius** keyword). If an error occurs when the home gateway contacts the RADIUS server, the home gateway does not authorize the user (because of the **none** keyword).

To see the following debug output, enable the **debug aaa authorization** command on the home gateway and dial in to the NAS:

```
ENT_HGW#
*Feb  5 17:27:36.166: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP Vi1 (3192359105): Port='Virtual-Access1' list=''
service=NET
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP: Vi1 (3192359105) user='jeremy@hgw.com'
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP: Vi1 (3192359105) send AV service=ppp
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP: Vi1 (3192359105) send AV protocol=lcp
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP (3192359105) found list "default"
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP: Vi1 (3192359105) Method=RADIUS
*Feb  5 17:27:36.166: AAA/AUTHOR (3192359105): Post authorization status = ERROR
*Feb  5 17:27:36.166: AAA/AUTHOR/LCP: Vi1 (3192359105) Method=NONE
*Feb  5 17:27:36.166: AAA/AUTHOR (3192359105): Post authorization status = PASS_ADD
*Feb  5 17:27:36.166: Vi1 CHAP: O SUCCESS id 1 len 4
```

Caution Using the **none** keyword can allow unauthorized access to your network. Because of the risk of such errors occurring, we strongly suggest that you do not use the **none** keyword in your **aaa** commands.

Misconfigured AAA Authentication

If you reverse the order of the **local** and **radius** keywords in the **aaa authentication ppp** command on the home gateway, the L2F tunnel cannot be established. The command should be configured as **aaa authentication ppp default local radius**.

If you configure the command as **aaa authentication ppp default radius local**, the home gateway first tries to authenticate the L2F tunnel using RADIUS. The RADIUS server sends the following message to the home gateway. To see this message, enable the **debug radius** command.

```
ENT_HGW#
Jan  1 01:34:47.827: RADIUS: SENDPASS not supported (action=4)
```

The RADIUS protocol does not support inbound challenges. This means that RADIUS is designed to authenticate user information, but it is not designed to be authenticated by others. When the home gateway requests the tunnel secret from the RADIUS server, it responds with the “SENDPASS not supported” message.

To avoid this problem, use the **aaa authentication ppp default local radius** command on the home gateway.

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