Overview of Access VPNs and Tunneling Technologies

Introduction

A virtual private network (VPN) is a network that extends remote access to users over a shared infrastructure. VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a point-to-point connection between remote users and an enterprise customer's network.

There are three main types of VPNs: access VPNs, intranet VPNs, and extranet VPNs.

- **Access VPNs**—Provide remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Access VPNs use analog, dial, ISDN, DSL, mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.
- **Intranet VPNs**—Link enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. Intranet VPNs differ from extranet VPNs in that they only allow access to the enterprise customer's employees.
- **Extranet VPNs**—Link outside customers, suppliers, partners, or communities of interest to an enterprise customer's network over a shared infrastructure using dedicated connections. Extranet VPNs differ from intranet VPNS in that they allow access to users outside the enterprise.

This document focuses solely on access VPNs.

Access VPNs

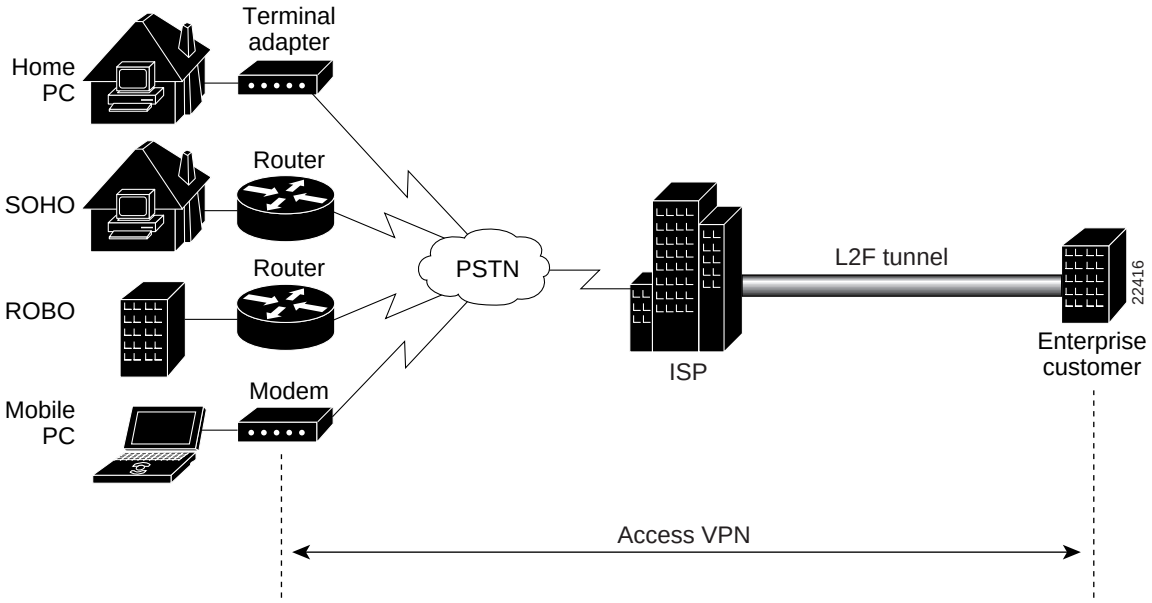
The main attraction of access VPNs is the way they delegate responsibilities for the network. The enterprise customer outsources the responsibility for the information technology (IT) infrastructure to an Internet service provider (ISP) that maintains the modems that the remote users dial into (called modem pools), access servers, and internetworking expertise. The enterprise customer is then only responsible for authenticating its users and maintaining its network.

Instead of connecting directly to the enterprise network by using the expensive public switched telephone network (PSTN), access VPN users only need to use the PSTN to connect to the ISP's local point of presence (POP). The ISP then uses the Internet to forward users from the POP to the enterprise customer network. Forwarding a user's call over the Internet provides dramatic cost saving for the enterprise customer. Access VPNs use layer 2 tunneling technologies to create a virtual point-to-point connection between users and the enterprise customer network. These tunneling technologies provide the same direct connectivity as the expensive PSTN by using the Internet. This means that users anywhere in the world have the same connectivity as they would at the enterprise customer's headquarters.

Access VPNs connect a variety of users: from a single, mobile employee to an entire branch office. Figure 1 illustrates the following methods of logging on to access VPNs:

- Home PC by using a terminal adapter
- Small office/home office (SOHO) by using a router
- Remote office/branch office (ROBO) by using a router
- Mobile PC by using a modem

Figure 1 Logging on to Access VPNs



The access VPN extends from the user to the enterprise customer. The Layer 2 Forwarding (L2F) tunnel is what makes access VPNs unique: Once the tunnel is established, the ISP is transparent to the user and the enterprise customer. The tunnel creates a secure connection between the user and the enterprise customer's network over the insecure Internet and is indistinguishable from a point-to-point connection.

This document describes three end-to-end access VPN case studies, which are primarily intended for ISPs who want to provide access VPN services to enterprise customers. The case studies are also useful to enterprise customers who want to establish access VPNs.

This document does not provide information on the entire spectrum of VPNs, nor does it cover all the details necessary to establish a network. Instead, this document focuses on three specific case studies:

- Layer 2 Forwarding Case Study
- Layer 2 Tunneling Protocol Case Study (under development)
- Layer 2 Tunneling Protocol with IPsec Case Study (under development)

Access VPN Architectures

Access VPNs are designed based on one of two architectural options: client-initiated or network access server (NAS)-initiated access VPNs. A NAS is an access server, maintained by the ISP, that users dial in to and that forwards the call to the enterprise network.

- **Client-initiated access VPNs**—Users establish an encrypted IP tunnel across the ISP's shared network to the enterprise customer's network. The enterprise customer manages the client software that initiates the tunnel. The main advantage of client-initiated VPNs is that they secure the connection between the client and the ISP. However, client-initiated VPNs are not as scalable and are more complex than NAS-initiated VPNs.
- **NAS-initiated access VPNs**—Users dial in to the ISP's NAS, which establishes an encrypted tunnel to the enterprise's private network. NAS-initiated VPNs are more robust than client-initiated VPNs, allow users to connect to multiple networks by using multiple tunnels, and do not require the client to maintain the tunnel-creating software. NAS-initiated VPNs do not encrypt the connection between the client and the ISP, but this is not a concern for most enterprise customers because the PSTN is much more secure than the Internet.

This document focuses solely on NAS-initiated access VPNs.

ISPs and Enterprise Customers

Access VPNs involve the cooperation of two partners: an internet service provider (ISP) and an enterprise customer.

- **ISP**—Responsible for maintaining the modem pool, access servers, and internetworking expertise. Often, the ISP will lease its IT infrastructure to smaller ISPs.
- **Enterprise Customer**—Responsible for maintaining its user database and private network. Often, the enterprise customer is a smaller ISP that does not want to take on the expense and commitment of establishing its own IT infrastructure.

In this document, ISP refers to the partner that is responsible for the IT infrastructure, and enterprise customer refers to the partner that leases the IT infrastructure.

Benefits

Access VPNs benefit both ISPs and enterprise customers as described in the following sections.

Benefits to the ISPs

- Offers end-to-end custom solutions that help differentiate the ISP in an increasingly competitive market
- Eliminates responsibility of managing the enterprise customer's user database
- Allows expansion to broadband technologies (such as DSL, cable, and wireless) as they become available

Benefits to the Enterprise Customers

- Allows enterprise customers to focus on their core business responsibilities
- Minimizes equipment costs
- Simplifies complexity of upgrading technology

- Eliminates need of maintaining internetworking expertise
- Reduces long distance and 800 number costs
- Increases flexibility and scalability of connecting and disconnecting branch offices, users, and external partners
- Prioritizes traffic to ensure bandwidth for critical applications

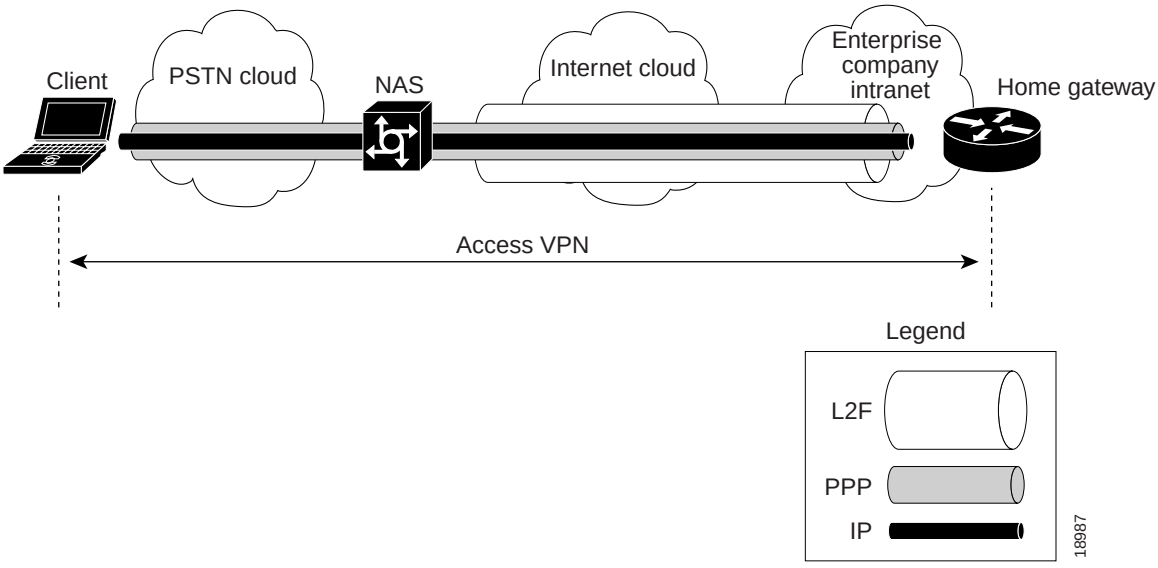
Access VPN Technologies

Access VPNs use L2F tunnels to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous High-Level Data Link Control). By using such tunnels, it is possible to detach the location of the ISP's NAS from the location of the enterprise customer's home gateway, where the dial-up protocol connection terminates and access to the enterprise customer's network is provided.

ISPs configure their NASs to receive calls from users and forward the calls to the enterprise customer's home gateway. The ISP only maintains information about the home gateway—the tunnel endpoint. The enterprise customer maintains the home gateway users' IP addresses, routing, and other user database functions. Administration between the ISP and home gateway is reduced to IP connectivity.

Figure 2 shows the PPP link running between a client (the user's hardware and software) and the home gateway. The NAS and home gateway establish an L2F tunnel that the NAS uses to forward the PPP link to the home gateway. The access VPN then extends from the client to the home gateway. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway.

Figure 2 End-to-End Access VPN Protocol Flow: L2F, PPP, and IP



The following sections give a functional description of the sequence of events that establish the access VPN:

- Protocol Negotiation Sequence
- L2F Tunnel Authentication Process
- Three-Way CHAP Authentication Process

The “Protocol Negotiation Sequence” section is an overview of the negotiation events that take place as the access VPN is established. The “L2F Tunnel Authentication Process” section gives a detailed description of how the NAS and home gateway establish the L2F tunnel. The “Three-Way CHAP Authentication Process” section gives a detailed description of how the NAS and home gateway authenticate a user.

Protocol Negotiation Sequence

When a user wants to connect to the enterprise customer’s home gateway, he or she first establishes a PPP connection to the ISP’s NAS. The NAS then establishes an L2F tunnel with the home gateway. Finally, the home gateway authenticates the client’s username and password, and establishes the PPP connection with the client.

Figure 3 describes the sequence of protocol negotiation events between the ISP’s NAS and the enterprise customer’s home gateway.

Figure 3 Protocol Negotiation Events Between Access VPN Devices

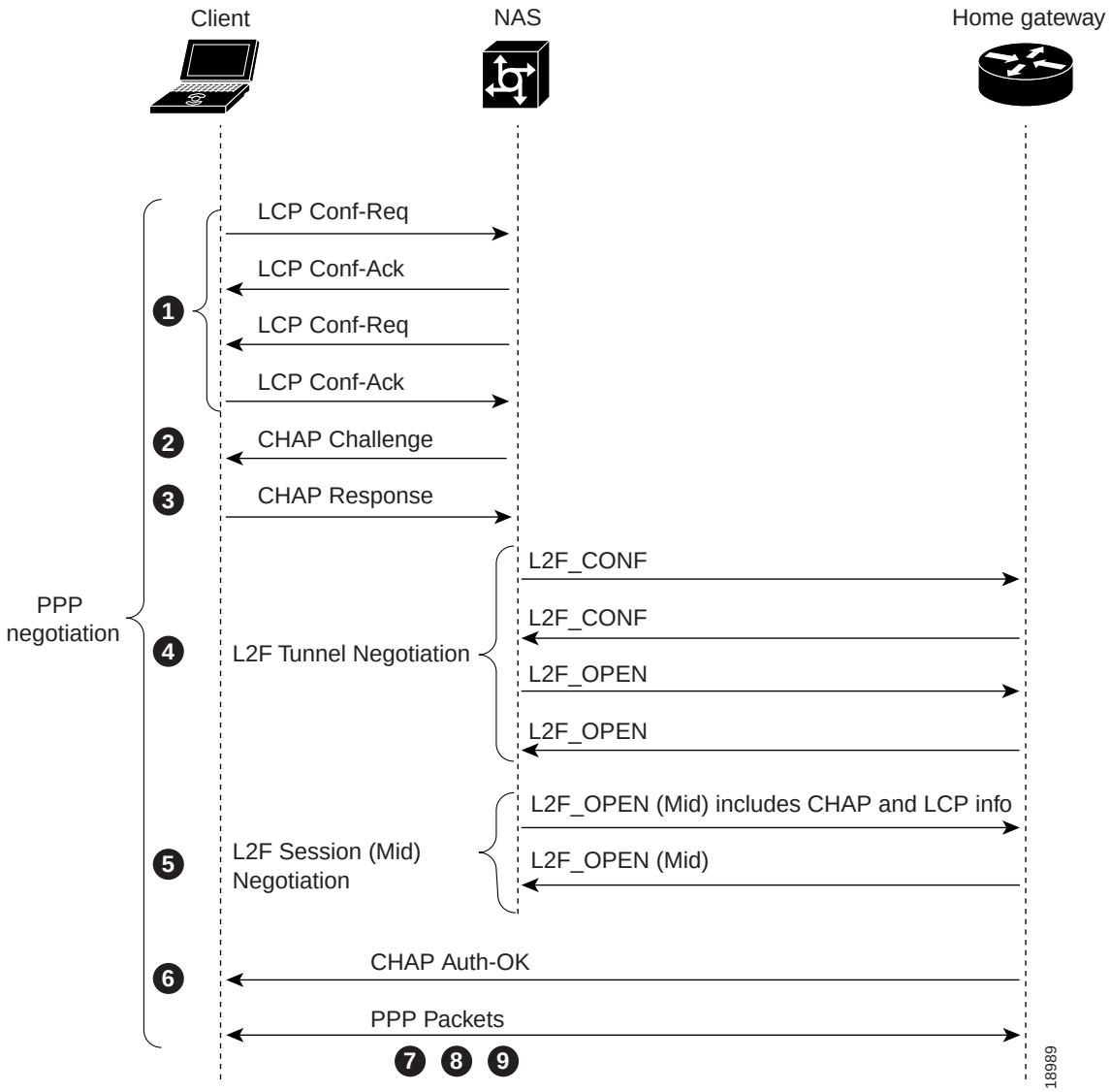


Table 1 explains the sequence of events shown in Figure 3.

Table 1 Protocol Negotiation Event Descriptions

Event	Description
1	The user's client and the NAS conduct a standard PPP link control protocol (LCP) negotiation.
2	The NAS begins PPP authentication by sending a Challenge Handshake Authentication Protocol (CHAP) challenge to the client.
3	The client replies with a CHAP response.
4	When the NAS receives the CHAP response, either the phone number the user dialed in from (when using DNIS-based authentication) or the user's domain name (when using domain name-based authentication) matches a configuration on either the NAS or its AAA server. This configuration instructs the NAS to create a VPN to forward the PPP session to the home gateway by using an L2F tunnel. Because this is the first L2F session with the home gateway, the NAS and the home gateway exchange L2F_CONF packets, which prepare them to create the tunnel. Then they exchange L2F_OPEN packets, which open the L2F tunnel.
5	Once the L2F tunnel is open, the NAS and home gateway exchange L2F session packets. The NAS sends an L2F_OPEN (Mid) packet to the home gateway that includes the client's information from the LCP negotiation, the CHAP challenge, and the CHAP response. The home gateway forces this information on to a virtual-access interface it has created for the client and responds to the NAS with an L2F_OPEN (Mid) packet.
6	The home gateway authenticates the CHAP challenge and response (using either local or remote AAA) and sends a CHAP Auth-OK packet to the client. This completes the three-way CHAP authentication.
7	When the client receives the CHAP Auth-OK packet, it can send PPP encapsulated packets to the home gateway.
8	The client and the home gateway can now exchange I/O PPP encapsulated packets. The NAS acts as a transparent PPP frame forwarder.
9	Subsequent PPP incoming sessions (designated for the same home gateway) do not repeat the L2F session negotiation because the L2F tunnel is already open.

L2F Tunnel Authentication Process

When the NAS receives a call from a client that instructs it to create an L2F tunnel with the home gateway, it first sends a challenge to the home gateway. The home gateway then sends a combined challenge and response to the NAS. Finally, the NAS responds to the home gateway's challenge, and the two devices open the L2F tunnel.

Before the NAS and home gateway can authenticate the tunnel, they must have a common "tunnel secret." A tunnel secret is a pair of usernames with the same password that is configured on both the NAS and the home gateway. By combining the tunnel secret with random value algorithms, which are used to encrypt to the tunnel secret, the NAS and home gateway authenticate each other and establish the L2F tunnel.

Figure 4 describes the tunnel authentication process.

Figure 4 L2F Tunnel Authentication Process

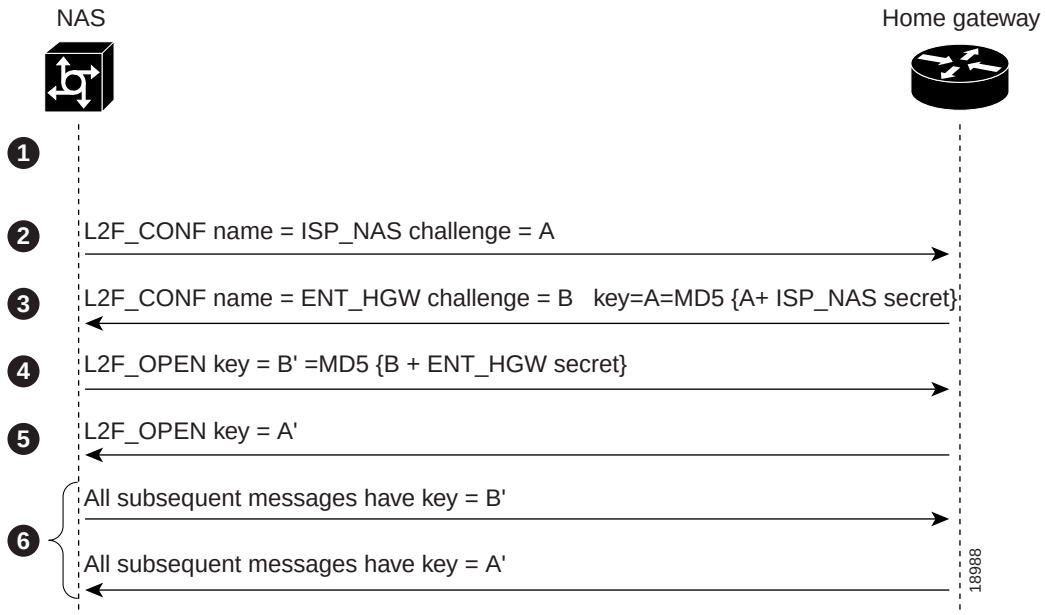


Table 2 explains the sequence of events shown in Figure 4.

Table 2 L2F Tunnel Authentication Event Descriptions

Event	Description
1	Before the NAS and home gateway open an L2F tunnel, both devices must have a common tunnel secret in their configurations.
2	The NAS sends an L2F_CONF packet that contains the NAS name and a random challenge value, A.
3	After the home gateway receives the L2F_CONF packet, it sends an L2F_CONF packet back to the NAS with the home gateway name and a random challenge value, B. This message also includes a key containing A' (the MD5 of the NAS secret and the value A).
4	When the NAS receives the L2F_CONF packet, it compares the key A' with the MD5 of the NAS secret and the value A. If the key and value match, the NAS sends an L2F_OPEN packet to the home gateway with a key containing B' (the MD5 of the home gateway secret and the value B).
5	When the home gateway receives the L2F_OPEN packet, it compares the key B' with the MD5 of the home gateway secret and the value B. If the key and value match, the home gateway sends an L2F_OPEN packet to the NAS with the key A'.
6	All subsequent messages from the NAS include key=B'; all subsequent messages from the home gateway include key=A'.

For more information on L2F, see RFC *Level Two Forwarding (Protocol) "L2F."*

Three-Way CHAP Authentication Process

When establishing an access VPN, the client, NAS, and home gateway use three-way CHAP authentication to authenticate the client's username and password. CHAP is a challenge/response authentication protocol in which the password is sent as a 64-bit signature instead of as plain text. This enables the secure exchange of the user's password between the user's client and the home gateway.

First, the NAS challenges the client, and the client responds. The NAS then forwards this CHAP information to the home gateway, which authenticates the client and sends a third CHAP message (either a success or failure message) to the client.

Figure 5 describes the three-way CHAP authentication process.

Figure 5 Three-Way CHAP Authentication Process

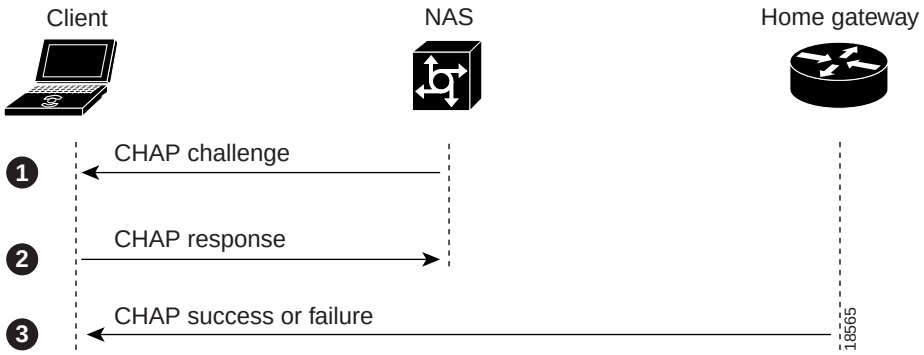


Table 3 explains the sequence of events shown in Figure 5.

Table 3 CHAP Event Descriptions

Event	Description
1	When the user initiates a PPP session with the NAS, the NAS sends a CHAP challenge to the client.
2	The client sends a CHAP response, which includes a plain text username, to the NAS. The NAS uses either the phone number the user dialed in from (when using DNIS-based authentication) or the user's domain name (when using domain name-based authentication) to determine the IP tunnel endpoint information. At this point, PPP negotiation is suspended, and the NAS asks its AAA server for IP tunnel information. The AAA server supplies the information needed to authenticate the tunnel between the NAS and the home gateway. Next, the NAS and the home gateway authenticate each other and establish an L2F tunnel. Then the NAS forwards the PPP negotiation to the home gateway.
3	The third CHAP event takes place between the home gateway and the client. The home gateway authenticates the client's CHAP response, which was forwarded by the NAS, and sends a CHAP success or failure to the client.

Once the home gateway authenticates the client, the access VPN is established. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway. The NAS acts as a transparent packet forwarder.

When subsequent clients dial in to the NAS to be forwarded to the home gateway, the NAS and home gateway do not need to repeat the L2F tunnel negotiation because the L2F tunnel is already open.

L2F Case Study Overview

Introduction

This case study describes how one Internet service provider (ISP) plans, designs, and implements an access virtual private network (VPN) by using Layer 2 Forwarding (L2F) as the tunneling protocol. L2F forwards Point-to-Point (PPP) sessions from one router to another router across a shared network infrastructure.

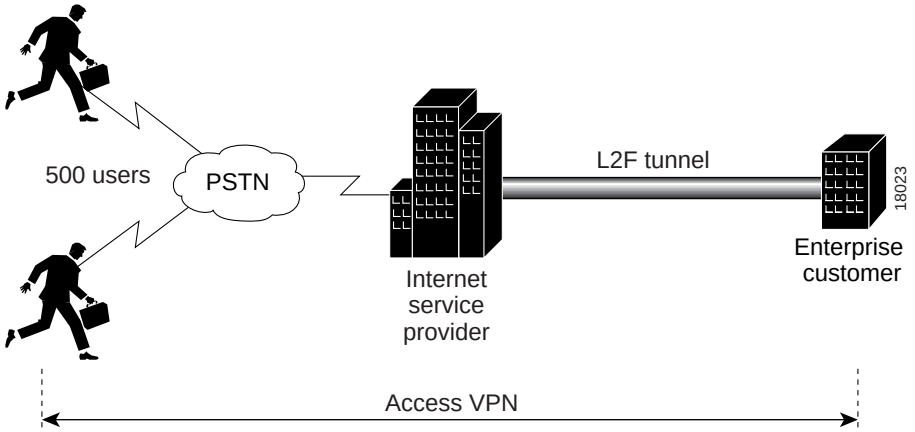
This case study is primarily intended for network administrators and operations teams working for ISPs who provide access VPN services to enterprise customers. This case study is also useful to enterprise customers who want to establish access VPNs.

This access VPN:

- Enables remote employees to access the enterprise customer's intranet resources when and where they want to
- Allows enterprise customer's networks to span from an intranet to remote clients who are connected to analog modems

Figure 6 shows an enterprise customer with a specific business objective. The enterprise customer wants to give 500 users dial-up modem access to intranet resources through the public switched telephone network (PSTN). To do this, the enterprise customer contracts with an ISP who is responsible for the required dial hardware and wide-area network (WAN) services. The ISP and enterprise customer decide to use L2F, because it is a stable tunneling protocol supported by many vendors and client software applications.

Figure 6 End-to-End Access VPN Solution



The ISP:

- Purchases, configures, and maintains the network access server (NAS). The NAS is the point-of-presence (POP) used to forward PPP sessions to the enterprise customer's network.
- Supports and maintains in-house modem pools.
- Maintains an authentication, authorization, and accounting (AAA) server that authenticates the IP tunnel endpoint and domain name assigned to the enterprise customer's home gateway.
- Maintains an edge router that connects the ISP's network to the enterprise customer's network.

The enterprise customer:

- Purchases, configures, and maintains a home gateway and clients.
- Authenticates and authorizes remote users' usernames and passwords by using a AAA server.

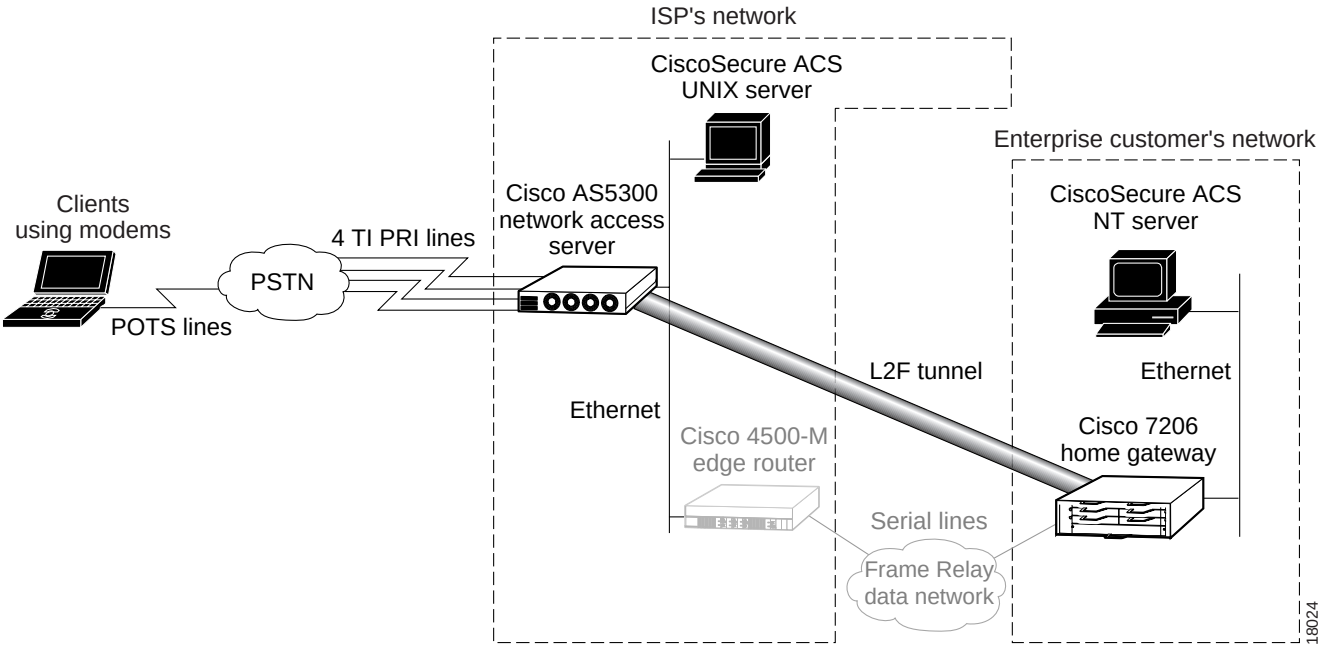
Note This case study illustrates one example of a NAS-initiated access VPN. Networks containing clients who initiate encrypted IP tunnels to home gateways are called client-initiated access VPNs.

Figure 7 shows the specific network devices used to build the access VPN in this case study.

- The ISP is responsible for a Cisco AS5300 network access server, a CiscoSecure ACS UNIX server, and a Cisco 4500-M edge router.
- The enterprise customer is responsible for a Cisco 7206 home gateway, a CiscoSecure ACS NT server, and the remote clients using modems.

The L2F tunnel runs between the Cisco AS5300 and Cisco 7206. The L2F tunnel is forwarded across a Frame Relay network.

Figure 7 Access VPN Case Study Network Topology



This case study does not describe how to configure the edge router, the Frame Relay data network, or the serial interfaces on the home gateway. Although these components are shown in Figure 7, they are not critical in understanding how to build an access VPN solution and are outside the scope of this case study. For more information about how to configure Frame Relay and serial interfaces, refer to the *Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.0.

See "Overview of Access VPNs and Tunneling Technologies" earlier in this document for an overview of access VPN solutions.

Device Characteristics

Table 4 provides a more detailed description of the hardware and software components used in the case study.

Table 4 Hardware and Software Used in the Case Study

	NAS	Home Gateway	CiscoSecure ACS UNIX Server	CiscoSecure ACS NT Server	Client
Chassis type	Cisco AS5300	Cisco 7206	Sun workstation	PC workstation	PC laptop
Physical interfaces	• 1 Ethernet interface • 4 T1 PRI ports • 96 terminal lines	• 1 Fast Ethernet interface • 4 serial interfaces	1 Ethernet interface	1 Ethernet interface	1 RJ-11 port
Hardware components	• Cisco AS5300 network access server • 96 MICA modems, 2 MICA CC and 1 Quad T1/PRI • T1 cable RJ45 to RJ45	• Cisco 7206, 6-slot chassis, 1 AC power supply • Cisco 7200 series input/output controller with Fast Ethernet • Cisco 7200 series network processing engine • 4-port serial port adapter, enhanced • V.35 cable, DTE, male, 10 feet	1 Ethernet card	1 Ethernet card	1 internal modem
Software loaded	• Cisco IOS Release 11.3(7)AA • Cisco AS5300 series IP	• Cisco IOS Release 12.0(2)T • Cisco 7200 series IP	• CiscoSecure ACS UNIX version 2.3.1 • Solaris 2.6	• CiscoSecure ACS NT version 2.1 • Windows NT 4.0	Windows 95
Telephone number or username	5550945[1]	N/A	N/A	N/A	jeremy@hgw.com password = subaru

Table 4 Hardware and Software Used in the Case Study (Continued)

	NAS	Home Gateway	CiscoSecure ACS UNIX Server	CiscoSecure ACS NT Server	Client
Memory	• Cisco AS5300 main DRAM upgrade (from 32 MB to 64 MB) • Cisco AS5300 system Flash upgrade (from 8 MB to 16 MB) • Cisco AS5300 boot Flash upgrade (from 4 MB to 8 MB)	• Cisco 7200 I/O PCMCIA Flash memory, 20 MB • Cisco 7200 NPE 64 MB DRAM upgrade kit	128 MB RAM 128 MB swap space	128 MB RAM	64 MB RAM
Ethernet IP Address	172.22.66.23 255.255.255.192	172.22.66.25 255.255.255.192	172.22.66.18 255.255.255.192	172.22.66.13 255.255.255.192	172.30.2.1[2]

1. This is the PRI telephone number assigned to the central site (NAS). The PRI number is often called the hunt group number, which distributes calls among the available B channels. Make sure your PRI provider assigns all four PRI trunks on the Cisco AS5300 to this number.
2. The home gateway dynamically assigns this IP address to the client in this case study.

Configuration Tasks

To build the access VPN, the ISP and enterprise customer must perform three major tasks to build the access VPN in this case study:

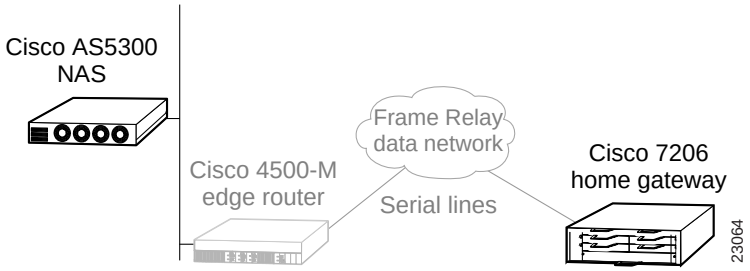
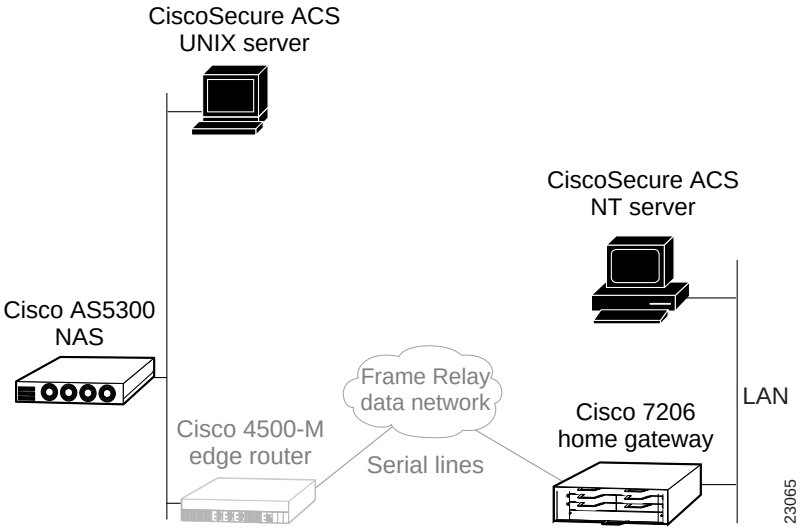
- Task 1—Configuring the NAS for Basic Dial Access
- Task 2—Configuring the Access VPN to Work with Local AAA
- Task 3—Configuring the Access VPN to Work with Remote AAA

Table 5 describes each task in more detail and identifies the devices related to each task.

A user named Jeremy with the username jeremy@hgw.com appears in many configurations, illustrations, and examples in this case study. The goal of the case study is to give Jeremy basic IP and modem services by forwarding his PPP session from the NAS to the home gateway. To help you understand how the various hardware and software components work together to forward the PPP session, follow Jeremy through the case study.

Note If you use this document to configure your own network, be sure to substitute your own IP addresses, passwords, usernames, hostnames, and telephone numbers.

Table 5 Relationship Between Configuration Tasks and Devices

Task	Description	Devices
1	Configuring the NAS for Basic Dial Access Performed by the ISP.	
2	Configuring the Access VPN to Work with Local AAA Performed by the ISP and the enterprise customer.	
3	Configuring the Access VPN to Work with Remote AAA Performed by the ISP and the enterprise customer.	

Configuring the NAS for Basic Dial Access

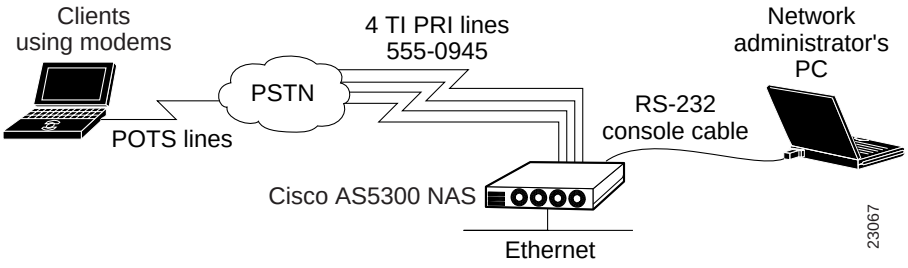
Introduction

In this first task, the ISP:

- Configures the Cisco AS5300 network access server (NAS) to support basic IP and modem services.
- Verifies that basic dial access works before the ISP starts forwarding PPP sessions to the enterprise customer's home gateway.
- Troubleshoots the NAS if there are problems.

Figure 8 shows the ISP's basic dial access topology. Clients using modems dial in to the NAS over four T1 PRI lines that are assigned to 555-0945.

Figure 8 Basic Dial Access Network Topology



After the ISP completes this task, basic dial access will function as follows:

- The client dials in to the NAS.
- The client and the NAS successfully complete PPP negotiation.
- The NAS assigns an IP address to the client.
- The client and NAS bidirectionally support IP services.

Configuring Basic Dial Access

To configure the NAS for basic dial access, the ISP completes the following steps:

- Step 1—Configuring the Host Name, Enable Password, and Service Time Stamps
- Step 2—Configuring Local AAA
- Step 3—Configuring the LAN Interface
- Step 4—Commissioning the T1 Controllers
- Step 5—Configuring the Serial Channels to Let Modem Calls Come In
- Step 6—Configuring the Modems and Asynchronous Lines
- Step 7—Specifying the IP Address Pool and DNS Servers
- Step 8—Configuring the Group-Async Interface

Step 1—Configuring the Host Name, Enable Password, and Service Time Stamps

In this step, the ISP:

- Assigns a host name to the NAS
- Sets up configuration privileges
- Turns on service time stamps

Use this command	To do this
`Router> enable`	Access privileged EXEC mode.
`Router# configure terminal` `Enter configuration commands, one per line. End with CNTL/Z.`	Access global configuration mode[1].
`Router(config)# hostname ISP_NAS`	Assign a host name to the access server. A host name distinguishes the NAS from other devices on the network.
`ISP_NAS(config)# enable secret letmein`	Enter a secret enable password, which secures privileged EXEC mode. An enable password allows you to prevent unauthorized configuration changes. Make sure to change **letmein** to your own secret password.
`ISP_NAS(config)# service password-encryption`	Encrypt passwords in the configuration file.
`ISP_NAS(config)# service timestamps debug datetime msec` `ISP_NAS(config)# service timestamps log datetime msec`	Apply millisecond time stamping to debug and logging output. These time stamps help identify debug output when there is a lot of activity on the router.

1. If the logging output generated by the NAS interferes with your terminal screen, redisplay the current command line by using the **Tab** key.

Step 2—Configuring Local AAA

In this step, the ISP:

- Enables the authentication, authorization, and accounting (AAA) access control system
- Creates a local username database

AAA provides the primary framework through which you set up access control on the NAS. Authentication identifies the client; authorization tells the client what it can do; accounting records what the client did do.

Use this command	To do this
`ISP_NAS(config)# aaa new-model`	Initiate the AAA access control system.
`ISP_NAS(config)# aaa authentication ppp default local`	Configure PPP authentication to use the local database.
`ISP_NAS(config)# username jane-admin password jane-password`	Create a local login database and username for yourself—the network administrator[1]. **Note** This step also prevents you from getting locked out of the access server.
`ISP_NAS(config)# username jeremy password subaru`	Create a local login username for the client. The username jeremy and password subaru are locally authenticated by the NAS. Later in the case study, jeremy is authenticated by the home gateway's CiscoSecure AAA server (not the NAS).

1. Make sure you use your own username and password.

Step 3—Configuring the LAN Interface

In this step, the ISP:

- Assigns an IP address to the Ethernet interface
- Brings up the interface

Use this command	To do this
`ISP_NAS(config)# interface ethernet 0` `ISP_NAS(config-if)# ip address 172.22.66.23 255.255.255.192`	Configure the IP address and subnet mask on the Ethernet interface. Do not forget to use your own IP address and subnet mask.

`ISP_NAS(config-if)# no shutdown`
`%LINK-3-UPDOWN: Interface Ethernet0, changed state to up`
`ISP_NAS(config-if)# exit`
	Bring up the interface.
	This command changes the state of the interface from administratively down to up[1].

1. The term administratively down means that the interface is intentionally shut down by the administrator. The **shutdown** command is applied to the interface.

Step 4—Commissioning the T1 Controllers

In this step, the ISP:

- Defines the ISDN switch type
- Commissions the T1 controllers to allow modem calls to come into the NAS. The ISP must specify the following information for each controller:
  - Framing type
  - Line code type
  - Clock source
  - Timeslot assignments

Use this command	To do this
`ISP_NAS(config)# isdn switch-type primary-5ess`	Enter the telco switch type, which is 5ESS in this case study. An ISDN switch type that is specified in global configuration mode is automatically propagated into the individual serial interfaces (for example, interface serial 0:23, 1:23, 2:23, and 3:23).
`ISP_NAS(config)# controller t1 0`	Access controller configuration mode for the first T1 controller, which is number 0. The controller ports are numbered 0 through 3 on the quad T1/PRI card.
`ISP_NAS(config-controller)# framing esf`	Enter the T1 framing type, which is extended super frame (ESF) in this case study.
`ISP_NAS(config-controller)# linecode b8zs`	Enter the T1 line code type, which is B8ZS in this case study.
`ISP_NAS(config-controller)# clock source line primary`	Configure the access server to get its primary clocking from the T1 line assigned to controller 0. Line clocking comes from the remote switch.
`ISP_NAS(config-controller)# pri-group timeslots 1-24`	Assign all 24 T1 timeslots as ISDN PRI channels. After you enter this command, a D-channel serial interface is instantly created (for example S0:23) as well as individual B-channel serial interfaces (for example S0:0, S0:1, S0:2, S0:3, and so on.). The D-channel interface functions like a dialer for all the 23 B channels using the controller. If this was an E1 interface, the PRI group range would be 1 to 31. The D-channel serial interfaces would be S0:15, S1:15, S2:15, and S3:15.
`ISP_NAS(config-controller)# exit`	Exit back to global configuration mode.

`ISP_NAS(config#) controller t1 1`
`ISP_NAS(config-controller)# framing esf`
`ISP_NAS(config-controller)# linecode b8zs`
`ISP_NAS(config-controller)# clock source line secondary`
`ISP_NAS(config-controller)# pri-group timeslots 1-24`
`ISP_NAS(config-controller)# exit`
	Configure the second controller, controller T1 1.
	Set the clocking to **secondary**. If the line clocking from controller T1 0 fails, the access server receives its clocking from controller T1 1.

Use this command	To do this

`ISP_NAS(config#) controller t1 2`
`ISP_NAS(config-controller)# framing esf`
`ISP_NAS(config-controller)# linecode b8zs`
`ISP_NAS(config-controller)# clock source internal`
`ISP_NAS(config-controller)# pri-group timeslots 1-24`
`ISP_NAS(config-controller)# exit`
`ISP_NAS(config#) controller t1 3`
`ISP_NAS(config-controller)# framing esf`
`ISP_NAS(config-controller)# linecode b8zs`
`ISP_NAS(config-controller)# clock source internal`
`ISP_NAS(config-controller)# pri-group timeslots 1-24`
`ISP_NAS(config-controller)# exit`
`ISP_NAS(config#)`
	Configure the remaining two controllers.
	Set both clocking entries to **internal** because the primary and secondary clock sources have already been assigned.

Step 5—Configuring the Serial Channels to Let Modem Calls Come In

In this step, the ISP:

- Configures the D channels to allow incoming voice calls to be routed to the integrated MICA modems. The D channel is the signaling channel.
- Uses the D channel to control the behavior of individual B channels

Use this command	To do this
`ISP_NAS(config)# interface serial 0:23`	Access configuration mode for the D-channel serial interface that corresponds to controller T1 0. The behavior of serial 0:0 through serial 0:22 is controlled by the configuration instructions provided for serial 0:23. This concept is also true for the other remaining D-channel configurations.
`ISP_NAS(config-if)# isdn incoming-voice modem`	Enable analog modem voice calls coming in through the B channels to be connected to the integrated modems.
`ISP_NAS(config-if)# exit`	Exit back to global configuration mode.

`ISP_NAS(config)# interface serial 1:23`
`ISP_NAS(config-if)# isdn incoming-voice modem`
`ISP_NAS(config-if)# exit`
`ISP_NAS(config)# interface serial 2:23`
`ISP_NAS(config-if)# isdn incoming-voice modem`
`ISP_NAS(config-if)# exit`
`ISP_NAS(config)# interface serial 3:23`
`ISP_NAS(config-if)# isdn incoming-voice modem`
`ISP_NAS(config-if)# exit`
	Configure the three remaining D channels with the same ISDN incoming-voice modem setting.

Step 6—Configuring the Modems and Asynchronous Lines

In this step, the ISP:

- Defines a range of modem lines
- Enables PPP clients to dial in, bypass the EXEC facility, and automatically start PPP.

Configure the modems and lines after the ISDN channels are operational. Each modem corresponds with a dedicated asynchronous line inside the access server. The modem speed 115200 bps and hardware flow control are default values for integrated modems.

Use this command	To do this
`ISP_NAS(config)# line 1 96`	Enter the range of modem lines that you want to configure. The NAS used in this case study has 96 integrated MICA modems.
`ISP_NAS(config-line)# autoselect ppp` `ISP_NAS(config-line)# autoselect during-login`	Enable PPP clients to dial in, bypass the EXEC facility, and automatically start PPP on the lines. The **autoselect during-login** command displays the username:password prompt as the modems connect. **Note** These two autoselect commands enable EXEC (shell) and PPP services on the same lines.
`ISP_NAS(config-line)# modem inout`	Support incoming and outgoing modem calls.

Step 7—Specifying the IP Address Pool and DNS Servers

In this step, the ISP:

- Creates an IP addresses pool that contains one IP address
- Specifies a primary and secondary domain name server (DNS)

Use this command	To do this
`ISP_NAS(config)# ip local pool default 1.1.1.1`	Create an IP pool containing one IP address to assign to one client[1].
`ISP_NAS(config)# async-bootp dns-server 171.68.10.70 171.68.10.140`	Specify the domain name servers on the network, which can be used for clients dialing in with PPP.

1. Later in the case study, the client is assigned an IP address from the local IP pool configured on the home gateway. The NAS, which is maintained by the ISP, does not assign IP addresses to the enterprise customer's clients when the network is configured as an access VPN.

Step 8—Configuring the Group-Async Interface

In this step, the ISP:

- Creates a group-async interface
- Projects protocol characteristics to 96 asynchronous interfaces

The group-async interface is a template that controls the configuration of all the asynchronous interfaces inside the NAS. Asynchronous interfaces are lines running in PPP mode.
An asynchronous interface uses the same number as its corresponding line. Configuring all the asynchronous interfaces as an async group saves you time by reducing the number of configuration steps.

Use this command	To do this
`ISP_NAS(config)# interface group-async 1`	Create the group-async interface.
`ISP_NAS(config-if)# ip unnumbered ethernet 0`	Use the IP address defined on the Ethernet interface.
`ISP_NAS(config-if)# encapsulation ppp`	Enable PPP.
`ISP_NAS(config-if)# async mode interactive`	Configure interactive mode on the asynchronous interfaces. Interactive mode means that clients can dial in to the NAS and get a router prompt or PPP session. Dedicated mode means that only PPP sessions can be established on the NAS. Clients cannot dial in and get an EXEC (shell) session.

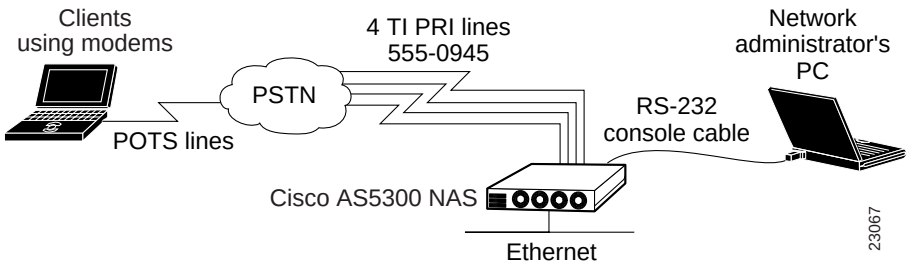
Use this command	To do this
`ISP_NAS(config-if)# ppp authentication chap pap`	Configure CHAP and PAP authentication to be used on the interface during LCP negotiation. The access server first authenticates with CHAP. If CHAP is rejected by the client, PAP authentication is used.
`ISP_NAS(config-if)# peer default ip address pool default`	Assign IP addresses to clients from the default IP address pool.
`ISP_NAS(config-if)# group-range 1 96` `Building configuration...`	Specify the range of asynchronous interfaces to include in the group, which is usually equal to the number of modems in the access server.

Verifying Basic Dial Access

This section describes how to verify that the following end-to-end connections function as shown in Figure 9:

- Step 1—Checking the NAS Running Configuration
- Step 2—Dialing in to the NAS
- Step 3—Pinging the NAS
- Step 4—Displaying Active Call Statistics on the NAS
- Step 5—Pinging the Client
- Step 6—Verifying That the Asynchronous Interface Is Up and That LCP Is Open

Figure 9 Basic Dial Access Network Topology



After you successfully test these connections, go to “Configuring the Access VPN to Work with Local AAA.” If you experience problems, see “Troubleshooting Basic Dial Access.”

Step 1—Checking the NAS Running Configuration

Enter the **show running-config** command in privileged EXEC mode to make sure that 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
```

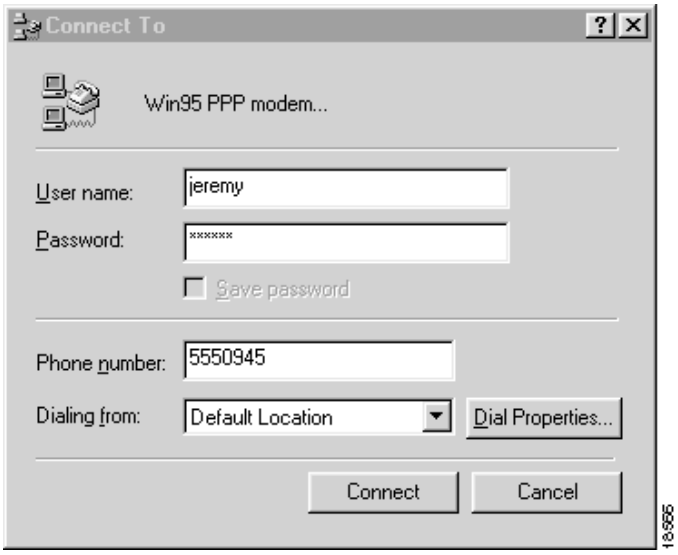
```
!
hostname ISP_NAS
!
aaa new-model
aaa authentication ppp default local
enable secret 5 $1$AXl/$27hOM6j51a5P76Enq.LCf0
!
!
username jeremy password 7 021511590A141A
username jane-admin password 7 0501090A6C5C4F1A0A1218000F
!
async-bootp dns-server 171.68.10.70 171.68.10.140
isdn switch-type primary-5ess
!
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
 peer default ip address pool default
 ppp authentication chap pap
 group-range 1 96
!
ip local pool default 1.1.1.1
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—Dialing in to the NAS

From the client, dial in to the NAS. Use the PRI telephone number assigned to the NAS' T1 trunks. Sometimes the PRI telephone is called the hunt group number. Figure 10 shows the username, password, and PRI telephone entered in the Windows 95 dial-up networking utility.

Figure 10 Windows 95 Dial-Up Networking Utility



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 47. The asynchronous interface is up.

```
*Jan  1 21:22:18.410: %LINK-3-UPDOWN: Interface Async47, 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 3—Pinging the NAS

Ping the NAS from the client. From the Windows 95 desktop:

(a) Click Start.

(b) Select Run.

(c) Enter **ping 172.22.66.23**. See Figure 11.

(d) Click OK.

(e) Look at the ping terminal screen and verify that the NAS is sending ping reply packets to the client. See Figure 12.

Figure 11 Windows 95 Ping Utility

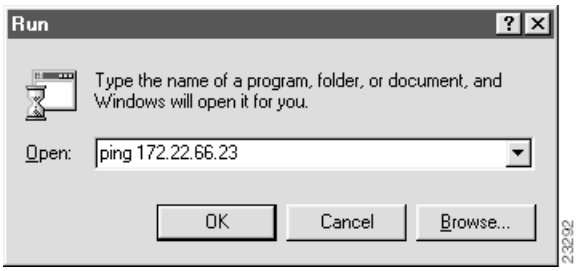
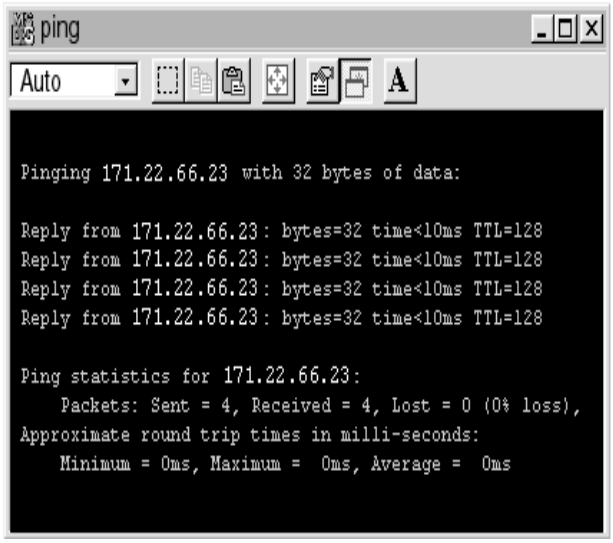


Figure 12 Ping Reply Packets Sent from the NAS to the Client



Step 4—Displaying Active Call Statistics on the NAS

From the NAS, 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 TTY line 47, asynchronous interface 47, and IP address 1.1.1.1. The network administrator jane-admin is using console 0.

```
ISP_NAS# show caller
  Line         User               Service       Active
  con 0        jane-admin          TTY           01:54:15
  tty 47       jeremy             Async         00:00:54
  As47         jeremy             PPP           00:00:50

ISP_NAS# show caller user jeremy

  User: jeremy, line tty 47, service Async, active 00:01:49
  TTY: Line 47, running PPP on As47, idle 00:00:00
  Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
  Status: Ready, Active, No Exit Banner, Async Interface Active
          HW PPP Support Active
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
                Modem Callout, Modem RI is CD,
                Line is permanent async interface, Integrated Modem
  Modem State: Ready
  Timeouts: Idle EXEC  Idle Session  Modem Answer   Session   Dispatch
             00:10:00         never             -     never   not set

  User: jeremy, line As47, service PPP, active 00:01:45
  PPP: LCP Open, CHAP (<- AAA), IPCP
  IP: Local 172.22.66.23, remote 1.1.1.1
  Counts: 29 packets input, 1690 bytes, 0 no buffer
          0 input errors, 0 CRC, 0 frame, 0 overrun
          12 packets output, 255 bytes, 0 underruns
          0 output errors, 0 collisions, 0 interface resets
```

Note The **show caller** command was added to the Cisco IOS software at Release 11.3(5)AA. If your software version of software does not support the **show caller** command, use the **show user** command.

Step 5—Pinging the Client

From the NAS, ping Jeremy's PC at IP address 1.1.1.1:

```
ISP_NAS# ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.22.66.55, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/136/160 ms
```

Step 6—Verifying That the Asynchronous Interface Is Up and That LCP Is Open

From the NAS, enter the **show interface async 47** command to verify that the interface is up, LCP is open, and no errors are reported:

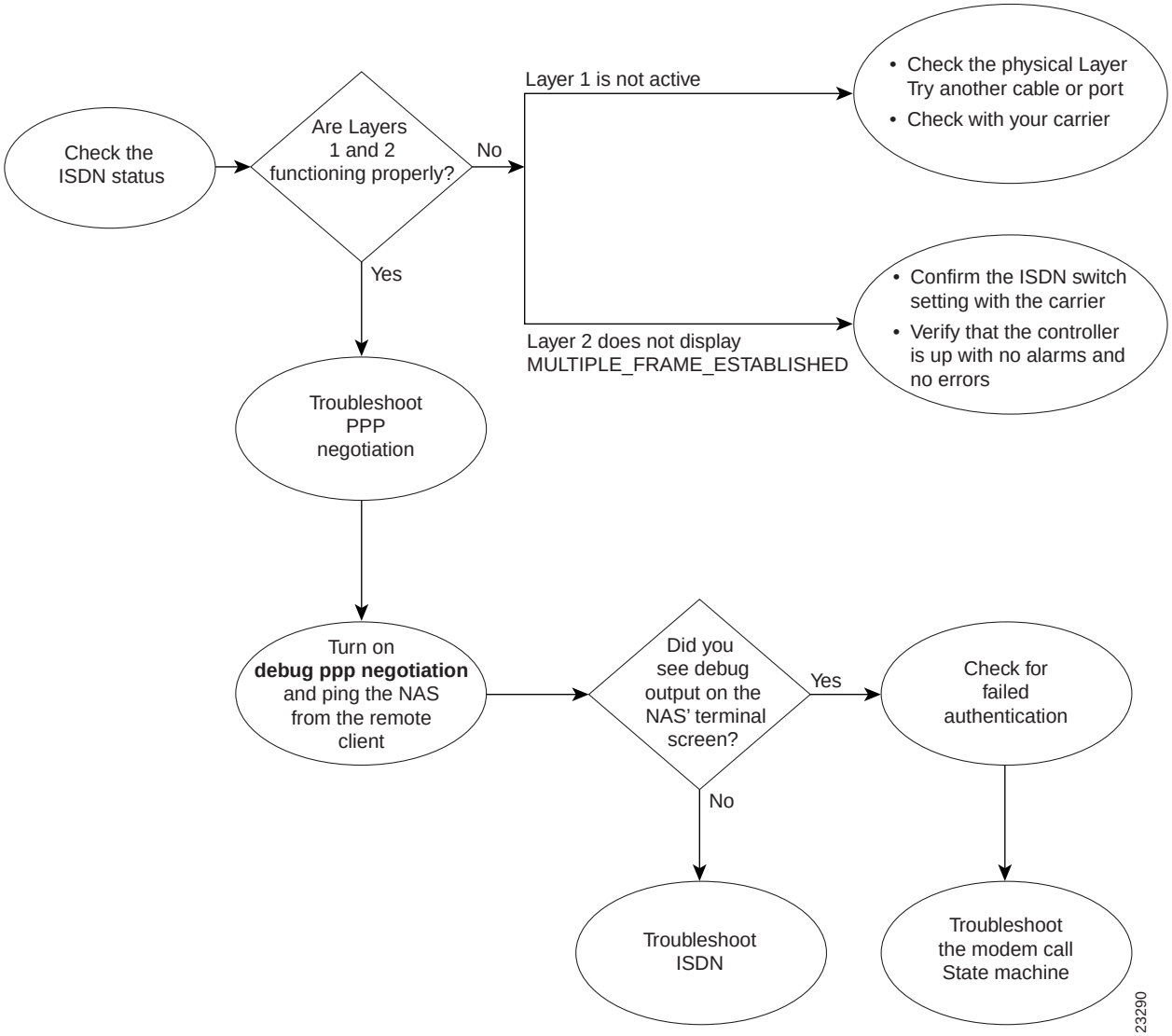
```
ISP_NAS# show interface async 47
Async47 is up, line protocol is up
  modem(slot/port)=1/46, state=CONNECTED
  dsx1(slot/unit/channel)=0/0/0, status=VDEV_STATUS_ACTIVE_CALL.VDEV_STATUS_ALL.
  Hardware is Async Serial
  Interface is unnumbered. Using address of Ethernet0 (172.22.66.23)
  MTU 1500 bytes, BW 115 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 5 seconds on reset
  LCP Open
  Open: IPCP
  Last input 00:00:46, output 00:02:42, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/10, 0 drops; input queue 1/10, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     37 packets input, 2466 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
     12 packets output, 255 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Troubleshooting Basic Dial Access

This section provides the ISP with a methodology for troubleshooting basic dial access as described in Figure 13. Complete the following steps to perform basic dial-up fault isolation. The bolded lines of output indicate important information.

- Step 1—Checking the ISDN Status
- Step 2—Troubleshooting PPP Negotiation
- Step 3—Troubleshooting ISDN
- Step 4—Checking the Error Status of the T1 Controllers
- Step 5—Troubleshooting the Modem Call State Machine

Figure 13 Troubleshooting Flow Diagram for Basic Dial Access



If you use a Telnet session to connect to the NAS, enable the **terminal monitor** command, which ensures that your EXEC session is receiving the logging and debug output from the NAS.

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

Step 1—Checking the ISDN Status

Enter the **show isdn status** command to confirm that Layer 1 is active and the display field MULTIPLE_FRAME_ESTABLISHED appears at Layer 2. This example shows that each serial interface is functioning properly:

```
ISP_NAS# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 1
        CCB:callid=11E, sapi=0, ces=0, B-chan=12, calltype=DATA
ISDN Serial1:23 interface
        dsl 1, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 1
        CCB:callid=12A, sapi=0, ces=0, B-chan=2, calltype=VOICE
ISDN Serial2:23 interface
        dsl 2, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
    Activated dsl 2 CCBs = 1
        CCB:callid=143, sapi=0, ces=0, B-chan=7, calltype=DATA
ISDN Serial3:23 interface
        dsl 3, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        4 Active Layer 3 Call(s)
    Activated dsl 3 CCBs = 4
        CCB:callid=160, sapi=0, ces=0, B-chan=14, calltype=VOICE
        CCB:callid=162, sapi=0, ces=0, B-chan=17, calltype=VOICE
        CCB:callid=167, sapi=0, ces=0, B-chan=22, calltype=VOICE
        CCB:callid=168, sapi=0, ces=0, B-chan=23, calltype=VOICE
    Total Allocated ISDN CCBs = 7
```

If Layer 1 is not active:

- Check the physical layer connectivity. Try using another port or cable.
- Check with your PRI provider.

If the display field MULTIPLE_FRAME_ESTABLISHED does not appear at Layer 2:

- Verify that the ISDN switch setting is correct.
- Enter the **show controller** command to verify that the controller is up without any alarms or errors. For an example, see "Step 4—Checking the Error Status of the T1 Controllers."

Note If you isolated the problem to Layers 1 or 2 and you think that you fixed it, go back to the verification steps and confirm that the problem is resolved. If the client still cannot dial in to the NAS, go to Step 2.

Step 2—Troubleshooting PPP Negotiation

Troubleshoot PPP negotiation by:

(a) Turning on the **debug ppp negotiation** command.

(b) Pinging the NAS from the client.

(c) Observing the debug output messages that appear on the NAS' terminal screen. If you do not see debug output, turn off the **debug ppp negotiation** command and go to Step 3.

It is important to understand what a successful debug PPP sequence looks like before you troubleshoot PPP negotiation. In this way, comparing a faulty PPP debug session against a successfully completed debug PPP sequence saves you time and effort.

Following is an example of a successful PPP sequence. See Table 6 for a detailed description of the output fields.

```
ISP_NAS# debug ppp negotiation
PPP protocol negotiation debugging is on
ISP_NAS# show debug
PPP:
  PPP protocol negotiation debugging is on

ISP_NAS#
Mar 13 10:57:13.415: %LINK-3-UPDOWN: Interface Async1, changed state to up
Mar 13 10:57:15.415: As1 LCP: O CONFREQ [ACKrcvd] id 2 len 25
Mar 13 10:57:15.415: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.415: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.415: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.415: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.415: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:15.543: As1 LCP: I CONFACK [REQsent] id 2 len 25
Mar 13 10:57:15.543: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.543: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.543: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.543: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.547: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP: I CONFREQ [ACKrcvd] id 4 len 23
Mar 13 10:57:16.919: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:16.919: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:16.919: As1 LCP:    PFC (0x0702)
Mar 13 10:57:16.919: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:16.919: As1 LCP: O CONFREJ [ACKrcvd] id 4 len 7
```

```
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:17.047: As1 LCP: I CONFREQ [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: O CONFACK [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: State is Open
Mar 13 10:57:17.047: As1 PPP: Phase is AUTHENTICATING, by this end
Mar 13 10:57:17.047: As1 CHAP: O CHALLENGE id 1 len 28 from "ISP_NAS"
Mar 13 10:57:17.191: As1 CHAP: I RESPONSE id 1 len 30 from "jeremy"
Mar 13 10:57:17.191: As1 CHAP: O SUCCESS id 1 len 4
Mar 13 10:57:17.191: As1 PPP: Phase is UP
Mar 13 10:57:17.191: As1 IPCP: O CONFREQ [Closed] id 1 len 10
Mar 13 10:57:17.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:17.303: As1 IPCP: I CONFREQ [REQsent] id 1 len 40
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x020
6002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.303: As1 IPCP: O CONFREJ [REQsent] id 1 len 22
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x020
6002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.319: As1 CCP: I CONFREQ [Not negotiated] id 1 len 15
Mar 13 10:57:17.319: As1 CCP:    MS-PPC supported bits 0x00000001 (0x12060000000
1)
Mar 13 10:57:17.319: As1 CCP:    Stacker history 1 check mode EXTENDED (0x110500
0104)
Mar 13 10:57:17.319: As1 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
Mar 13 10:57:17.319: As1 LCP:  (0x80FD0101000F12060000000111050001)
Mar 13 10:57:17.319: As1 LCP:  (0x04)
Mar 13 10:57:17.319: As1 IPCP: I CONFACK [REQsent] id 1 len 10
Mar 13 10:57:17.319: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:18.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, cha
nged state to up
Mar 13 10:57:19.191: As1 IPCP: TIMEout: State ACKrcvd
Mar 13 10:57:19.191: As1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
Mar 13 10:57:19.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:19.315: As1 IPCP: I CONFACK [REQsent] id 2 len 10
Mar 13 10:57:19.315: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:20.307: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
Mar 13 10:57:20.307: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.307: As1 IPCP: O CONFREJ [ACKrcvd] id 2 len 16
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.419: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.419: As1 IPCP: O CONFNAK [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
```

```
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.543: As1 IPCP: I CONFREQ [ACKrcvd] id 4 len 22
Mar 13 10:57:20.543: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: O CONFACK [ACKrcvd] id 4 len 22
Mar 13 10:57:20.547: As1 IPCP:    Address 1.1.1.1 (0x030601010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: State is Open
Mar 13 10:57:20.551: As1 IPCP: Install route to 1.1.1.1
```

Table 6 Time Stamps and Descriptions for Debug PPP Negotiation Events

Time Stamp	Description
10:57:15.415	Outgoing configuration request (O CONFREQ). The NAS sends an outgoing PPP configuration request packet to the client.
10:57:15.543	Incoming configuration acknowledgment (I CONFACK). The client acknowledges the NAS' PPP request.
10:57:16.919	Incoming configuration request (I CONFREQ). The client wants to negotiate the callback protocol.
10:57:16.919	Outgoing configuration reject (O CONFREJ). The NAS rejects the callback option.
10:57:17.047	Incoming configuration request (I CONFREQ). The client requests a new set of options. Notice that Microsoft Callback is not requested this time.
10:57:17.047	Outgoing configuration acknowledgment (O CONFACK). The NAS accepts the new set of options.
10:57:17.047	PPP LCP negotiation is completed successfully (LCP: State is Open). Both sides have acknowledged (CONFACK) the other side's configuration request (CONFREQ).
10:57:17.047 to 10:57:17.191	PPP authentication is completed successfully. After LCP negotiates, authentication starts. Authentication must take place before any network protocols, such as IP, are delivered. Both sides authenticate with the method negotiated during LCP. The Cisco AS5300 is authenticating the client using CHAP.
10:57:20.551	The state is open for IP Control Protocol (IPCP). A route is negotiated and installed for the IPCP peer, which is assigned IP address 1.1.1.1.

Failed authentication is a common occurrence. Misconfigured or mismatched usernames and passwords create error messages in debug output.

The following example shows that the username sam-admin does not have permission to dial in to the NAS, which does not have a local username configured for this user. To fix the problem, use the **username** *name* **password** *password* command to add the username sam-admin to the NAS' local AAA database:

```
Mar 13 11:01:42.399: As2 LCP: State is Open
Mar 13 11:01:42.399: As2 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:01:42.399: As2 CHAP: O CHALLENGE id 1 len 28 from "ISP_NAS"
Mar 13 11:01:42.539: As2 CHAP: I RESPONSE id 1 len 30 from "sam-admin"
Mar 13 11:01:42.539: As2 CHAP: Unable to validate Response.  Username sam-admin not
found
Mar 13 11:01:42.539: As2 CHAP: O FAILURE id 1 len 26 msg is "Authentication fail
ure"
Mar 13 11:01:42.539: As2 PPP: Phase is TERMINATING
```

The following example shows that the username sam-admin is configured on the NAS. However, the password comparison failed. To fix this problem, use the **username** *name* **password** *password* command to specify sam-admin's correct login password:

```
Mar 13 11:04:06.843: As3 LCP: State is Open
Mar 13 11:04:06.843: As3 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:04:06.843: As3 CHAP: O CHALLENGE id 1 len 28 from "ISP_NAS"
Mar 13 11:04:06.987: As3 CHAP: I RESPONSE id 1 len 30 from "sam-admin"
Mar 13 11:04:06.987: As3 CHAP: O FAILURE id 1 len 25 msg is "MD/DES compare failed"
Mar 13 11:04:06.987: As3 PPP: Phase is TERMINATING
```

Note If you isolated the problem to PPP negotiation and you think that you fixed it, go back to the verification steps and confirm that the problem is resolved. If you are still having problems, go to Step 3.

Step 3—Troubleshooting ISDN

Troubleshoot ISDN if no debug output appeared when you tried debugging PPP negotiation. Turn on ISDN Q.931 debugging and verify that no other debug commands are enabled:

```
ISP_NAS# debug isdn q931
ISDN Q931 packets debugging is on
ISP_NAS# show debug
ISDN:
  ISDN Q931 packets debugging is on
```

Send a PPP modem call into the NAS. As the call enters the access server, the following successful call setup messages appear on the NAS' terminal screen. Refer to Table 7 for a detailed description of the output fields.

```
ISP_NAS#
Mar 13 11:06:01.715: ISDN Se0:23: RX <-  SETUP pd = 8  callref = 0x02AD
Mar 13 11:06:01.715:         Bearer Capability i = 0x8090A2
Mar 13 11:06:01.719:         Channel ID i = 0xA98381
Mar 13 11:06:01.719:         Progress Ind i = 0x8283 - Origination address is no
n-ISDN
Mar 13 11:06:01.719:         Calling Party Number i = '!', 0x83, '4089548021'
Mar 13 11:06:01.719:         Called Party Number i = 0xC1, '5550945'
Mar 13 11:06:01.719: ISDN Se0:23: TX ->  CALL_PROC pd = 8  callref = 0x82AD
Mar 13 11:06:01.719:         Channel ID i = 0xA98381
Mar 13 11:06:01.719: ISDN Se0:23: TX ->  ALERTING pd = 8  callref = 0x82AD
Mar 13 11:06:01.867: ISDN Se0:23: TX ->  CONNECT pd = 8  callref = 0x82AD
Mar 13 11:06:01.895: ISDN Se0:23: RX <-  CONNECT_ACK pd = 8  callref = 0x02AD
Mar 13 11:06:33.619: %LINK-3-UPDOWN: Interface Async4, changed state to up
Mar 13 11:06:38.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4, cha
nged state to up
```

If this debug output is not displayed on your terminal screen, confirm that the client is dialing the correct telephone number. If the number is correct, troubleshoot the problem with your PRI provider. If you are still having problems, go to Step 4.

Table 7 Time Stamps and Descriptions for Debug ISDN Q.931 Events

Time Stamp	Description
11:06:01.715	The NAS receives (RX) the ISDN setup message for an incoming call. Call characteristics appear.
11:06:01.719	The NAS transmits (TX) a call-proceeding message. The NAS has not answered the call as yet.
11:06:01.867	The NAS transmits a connect message and answers the call.
11:06:01.895	The NAS receives a connect acknowledgment, and the connection is established.

Step 4—Checking the Error Status of the T1 Controllers

Enter the **show controller t1** command to display the error status of the T1 controllers. A properly functioning T1 0 controller displays "T1 0 is up" and "No alarms detected." The following example shows four T1 controllers in good working condition:

```
ISP_NAS# show controller t1
T1 0 is up.
  Applique type is Channelized T1
  No alarms detected.
  Version info of slot 0:  HW: 4, Firmware: 16, PLD Rev: 0

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
 Board Hardware Version 1.32, Item Number 800-2540-2,
 Board Revision A0, Serial Number 11488142,
 PLD/ISP Version 0.0, Manufacture Date 10-Nov-1998.

  Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
  Data in current interval (748 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 30 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
T1 1 is up.
  Applique type is Channelized T1
  No alarms detected.
  Version info of slot 0:  HW: 4, Firmware: 16, PLD Rev: 0

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
 Board Hardware Version 1.32, Item Number 800-2540-2,
 Board Revision A0, Serial Number 11488142,
 PLD/ISP Version 0.0, Manufacture Date 10-Nov-1998.

  Framing is ESF, Line Code is B8ZS, Clock Source is Line Secondary
.
  Data in current interval (751 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 30 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

```
T1 2 is up.
  Applique type is Channelized T1
  No alarms detected.
  Version info of slot 0:  HW: 4, Firmware: 16, PLD Rev: 0

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
 Board Hardware Version 1.32, Item Number 800-2540-2,
 Board Revision A0, Serial Number 11488142,
 PLD/ISP Version 0.0, Manufacture Date 10-Nov-1998.

  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Data in current interval (755 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 30 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
T1 3 is up.
  Applique type is Channelized T1
  No alarms detected.
  Version info of slot 0:  HW: 4, Firmware: 16, PLD Rev: 0

Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
 Board Hardware Version 1.32, Item Number 800-2540-2,
 Board Revision A0, Serial Number 11488142,
 PLD/ISP Version 0.0, Manufacture Date 10-Nov-1998.

  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Data in current interval (757 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 30 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

If counters increase on a specific T1 controller, look closely at the error statistics. Focus on the current interval that is indented under the display field “Data in current interval.”

Error counters are recorded over a 24-hour period in 15-minute intervals. You must specify a specific controller number to see this detailed information. Enter the **clear controller t1** *number* command before you look for current error statistics. Error counters stop increasing when the controller is configured correctly.

Step 5—Troubleshooting the Modem Call State Machine

Troubleshoot the modem’s call state machine (CSM) by using the **debug modem csm** command. Troubleshoot the CSM if you do not see PPP debug output, and the **show isdn status** command and **debug isdn q931** command demonstrate good working status:

```
ISP_NAS# debug modem csm
Modem Management Call Switching Module debugging is on
ISP_NAS# show debug
Modem Management:
  Modem Management Call Switching Module debugging is on
```

Send a PPP modem call into the NAS. Transition states in the debug output signify that everything is operating properly. If you do not see transition states, look at the disconnect reason for the modem. For example, enter the **show modem log 1/4** command.

See the following example of successful debug output for the **debug modem csm** command:

```
ISP_NAS#
Mar 13 11:13:12.487: EVENT_FROM_ISDN::dchan_idb=0x60EA108C, call_id=0x1D, ces=0x
1bchan=0x0, event=0x1, cause=0x0
Mar 13 11:13:12.487: VDEV_ALLOCATE: slot 1 and port 4 is allocated.
Mar 13 11:13:12.487: EVENT_FROM_ISDN:(001D): DEV_INCALL at slot 1 and port 4
Mar 13 11:13:12.487: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 4
Mar 13 11:13:12.487: Mica Modem(1/4): Configure(0x1 = 0x0)
Mar 13 11:13:12.487: Mica Modem(1/4): Configure(0x23 = 0x0)
Mar 13 11:13:12.487: Mica Modem(1/4): Call Setup
Mar 13 11:13:12.611: Mica Modem(1/4): State Transition to Call Setup
Mar 13 11:13:12.611: Mica Modem(1/4): Went offhook
Mar 13 11:13:12.611: CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 4
Mar 13 11:13:12.631: EVENT_FROM_ISDN::dchan_idb=0x60EA108C, call_id=0x1D, ces=0x1
bchan=0x0, event=0x4, cause=0x0
Mar 13 11:13:12.631: EVENT_FROM_ISDN:(001D): DEV_CONNECTED at slot 1 and port 4
Mar 13 11:13:12.631: CSM_PROC_IC4_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at slot 1,
port 4
Mar 13 11:13:12.631: Mica Modem(1/4): Link Initiate
Mar 13 11:13:13.751: Mica Modem(1/4): State Transition to Connect
Mar 13 11:13:18.903: Mica Modem(1/4): State Transition to Link
ISP_NAS#
Mar 13 11:13:37.051: Mica Modem(1/4): State Transition to Trainup
Mar 13 11:13:38.731: Mica Modem(1/4): State Transition to EC Negotiating
Mar 13 11:13:39.387: Mica Modem(1/4): State Transition to Steady State
Mar 13 11:13:42.007: %LINK-3-UPDOWN: Interface Async5, changed state to up
Mar 13 11:13:46.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async5, cha
nged state to up
Mar 13 11:14:41.803: Mica Modem(1/4): State Transition to Steady State Speedshif ting
Mar 13 11:14:44.139: Mica Modem(1/4): State Transition to Steady State
Mar 13 11:17:30.475: %SYS-5-CONFIG_I: Configured from console by vty0 (171.68.20
1.22)
```

Note If you are still experiencing problems, contact your escalation support personnel.

Configuring the Access VPN to Work with Local AAA

Introduction

In this second task, the ISP and enterprise customer:

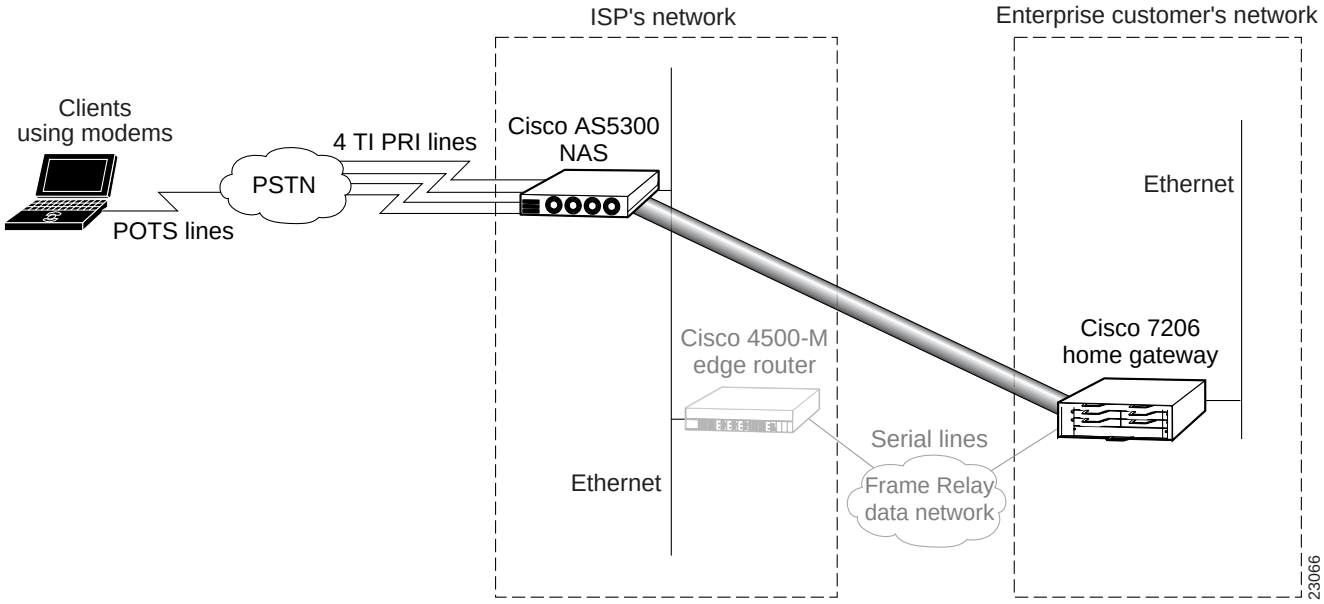
- Configure their network devices to work as an access VPN
- Use local AAA to authenticate the tunnel and the users
- Verify that the access VPN works properly
- Troubleshoot the access VPN if there are problems

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.

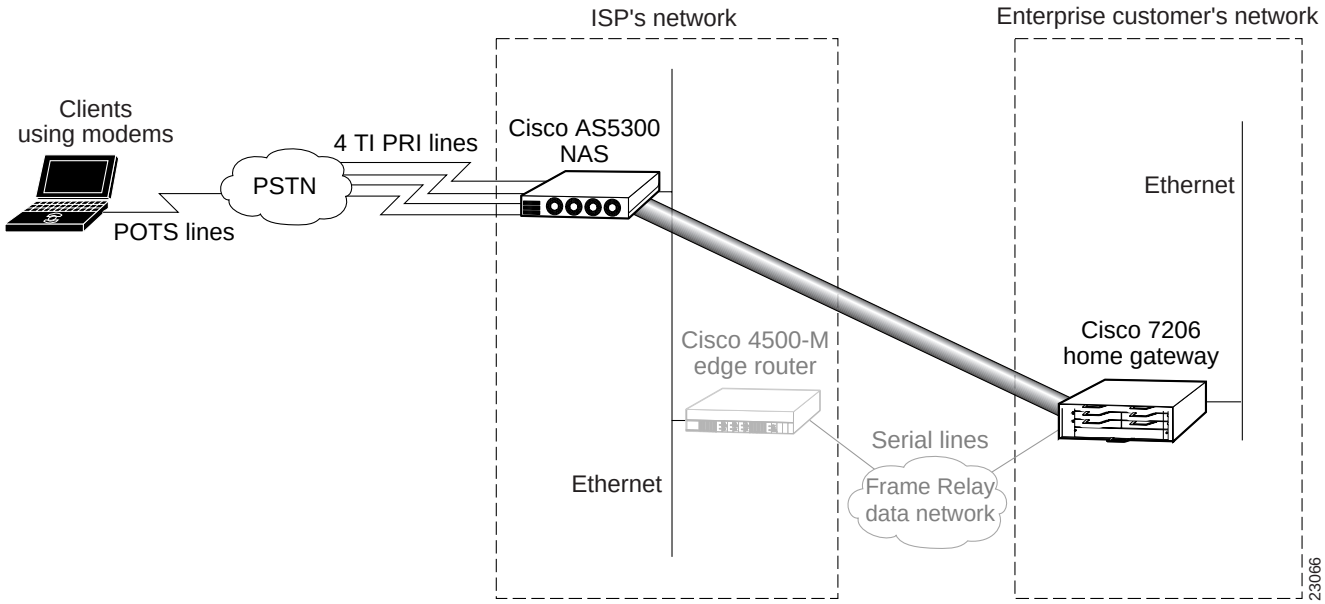
Use this command	To do this
`ENT_HGW(config)# ip local pool default 172.30.2.1 172.30.2.96`	Configure the default local pool of IP address that will be used by clients.
`ENT_HGW(config)# async-bootp dns-server 172.23.1.10 172.23.2.10`	(Optional) Return the configured addresses of Domain Name Servers 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
```

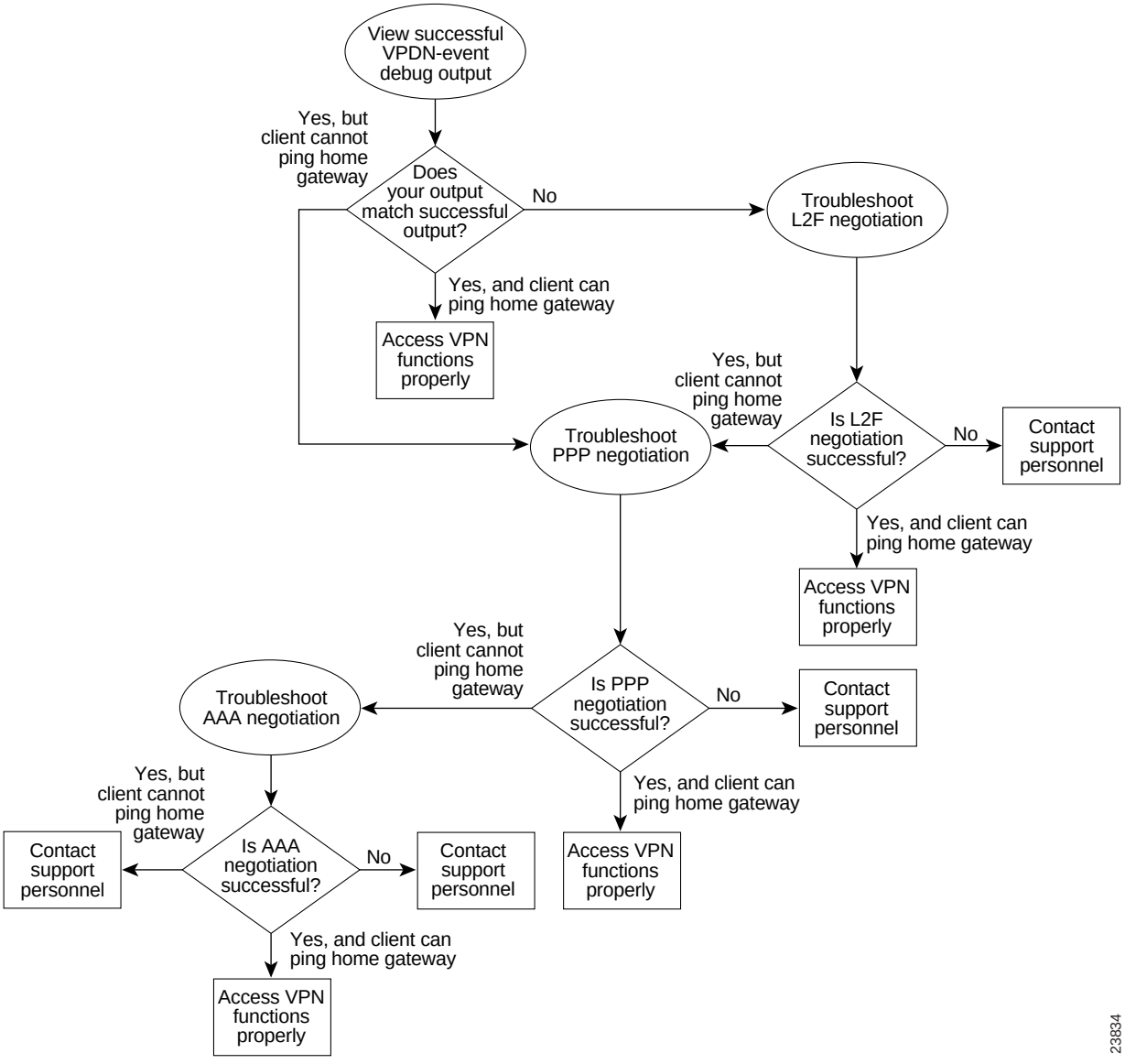
Troubleshooting the Access VPN

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.

Configuring the Access VPN to Work with Remote AAA

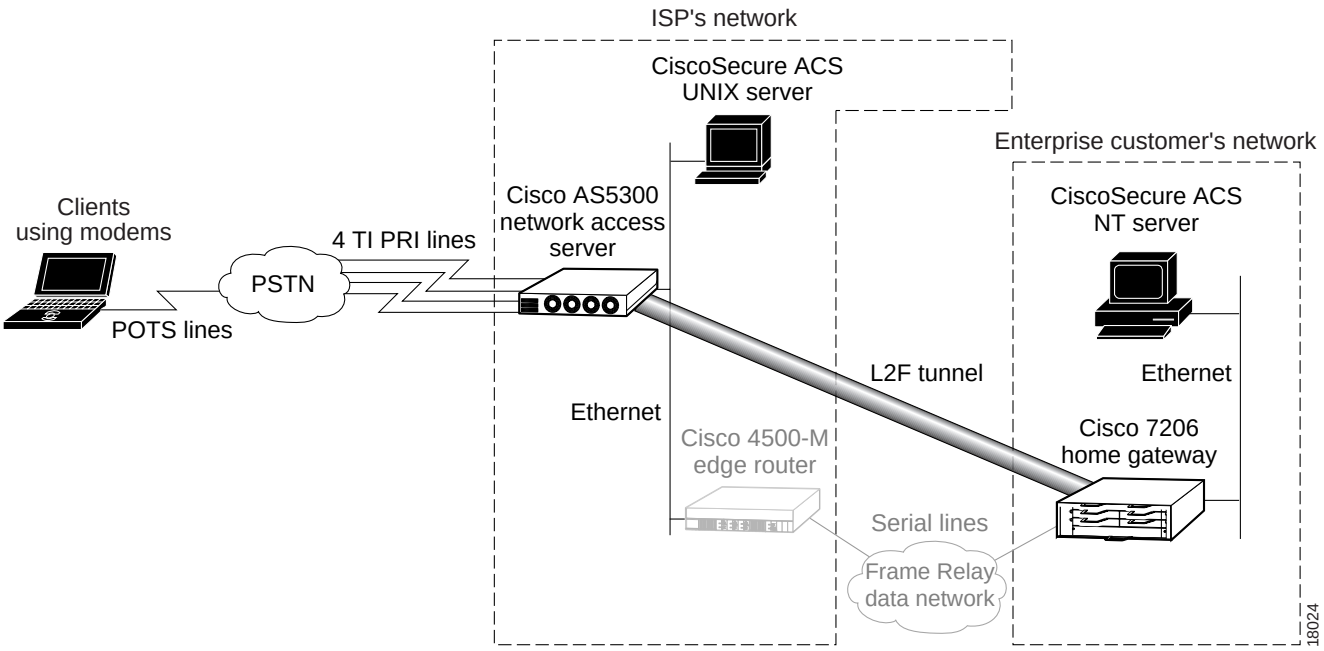
Introduction

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.

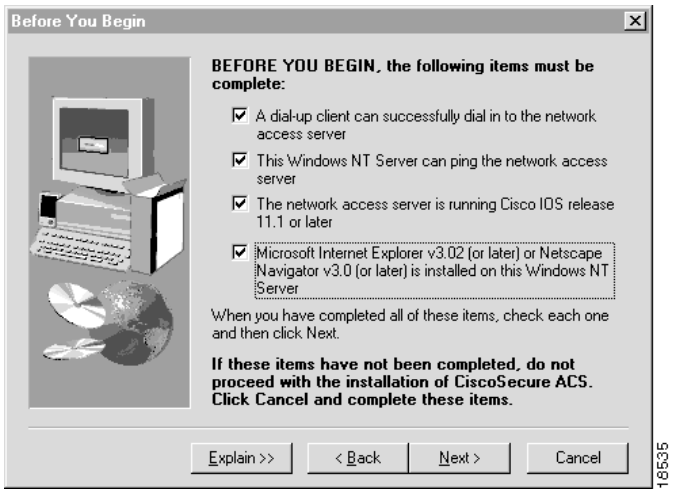
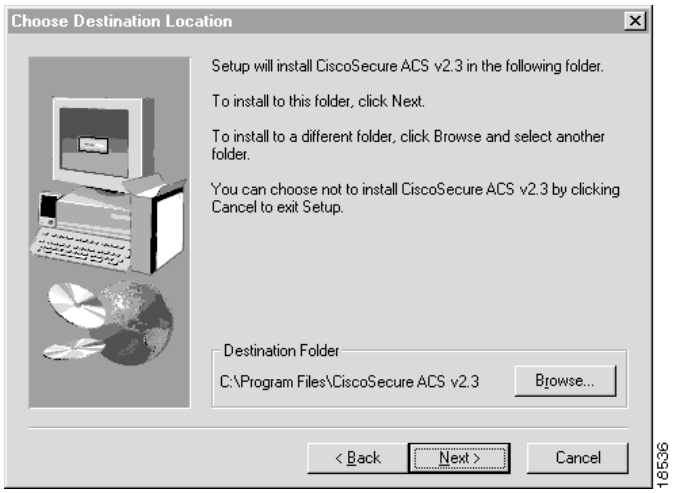
Step 4—Configuring the CiscoSecure ACS NT Server

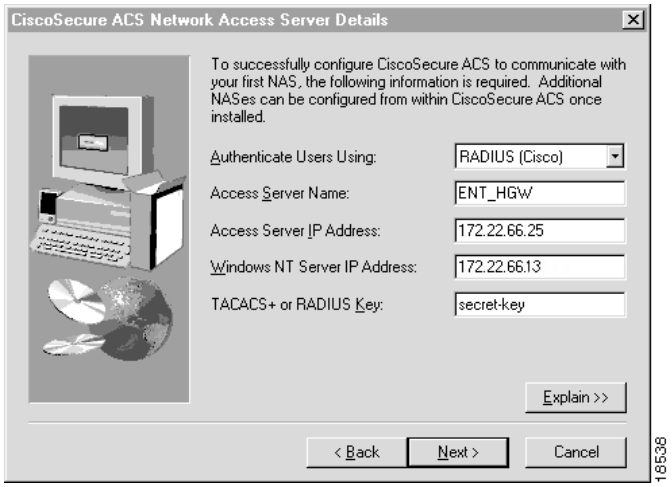
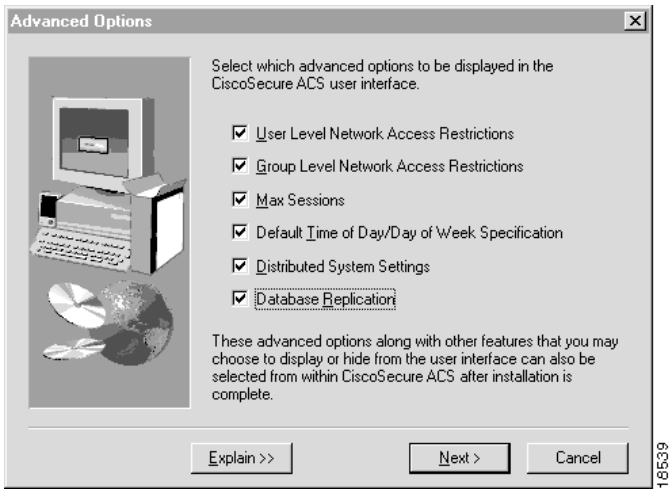
In this step, the enterprise customer:

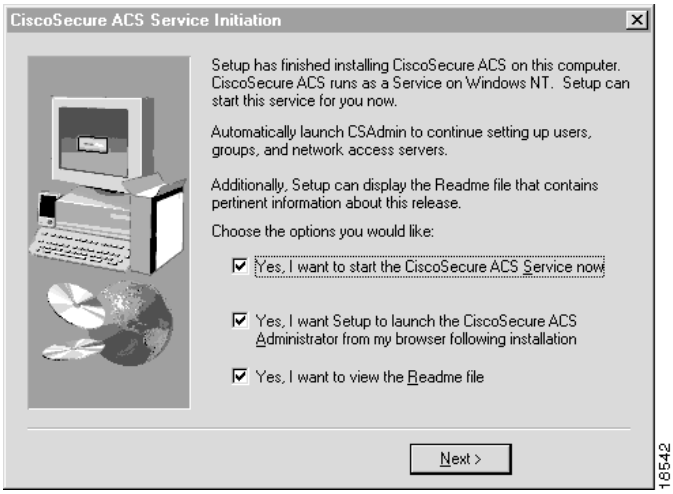
- Installs CiscoSecure NT, selecting RADIUS (Cisco) as the security protocol and identifying the access server by which authentication requests are transmitted
- Configures CiscoSecure NT to delete the domain name from incoming usernames so that the username matches the format CiscoSecure NT uses in 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**.

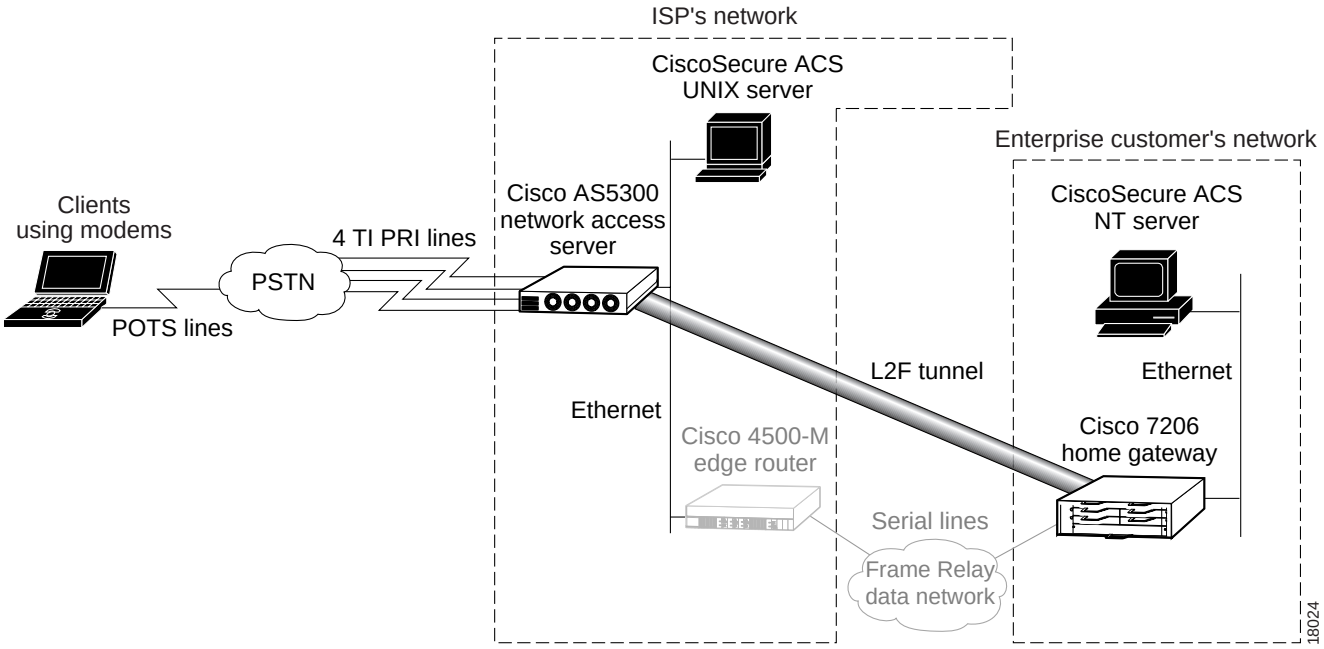
Use this display	To do this
	In the User Setup window, to create a user: • Type **jeremy** in the User box. • Click **Add/Edit**.
	In the User Setup screen, add the following supplementary user information: • Type **Jeremy Smith** in the Real Name box. • Type **Remote User** in the Description box. • 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:

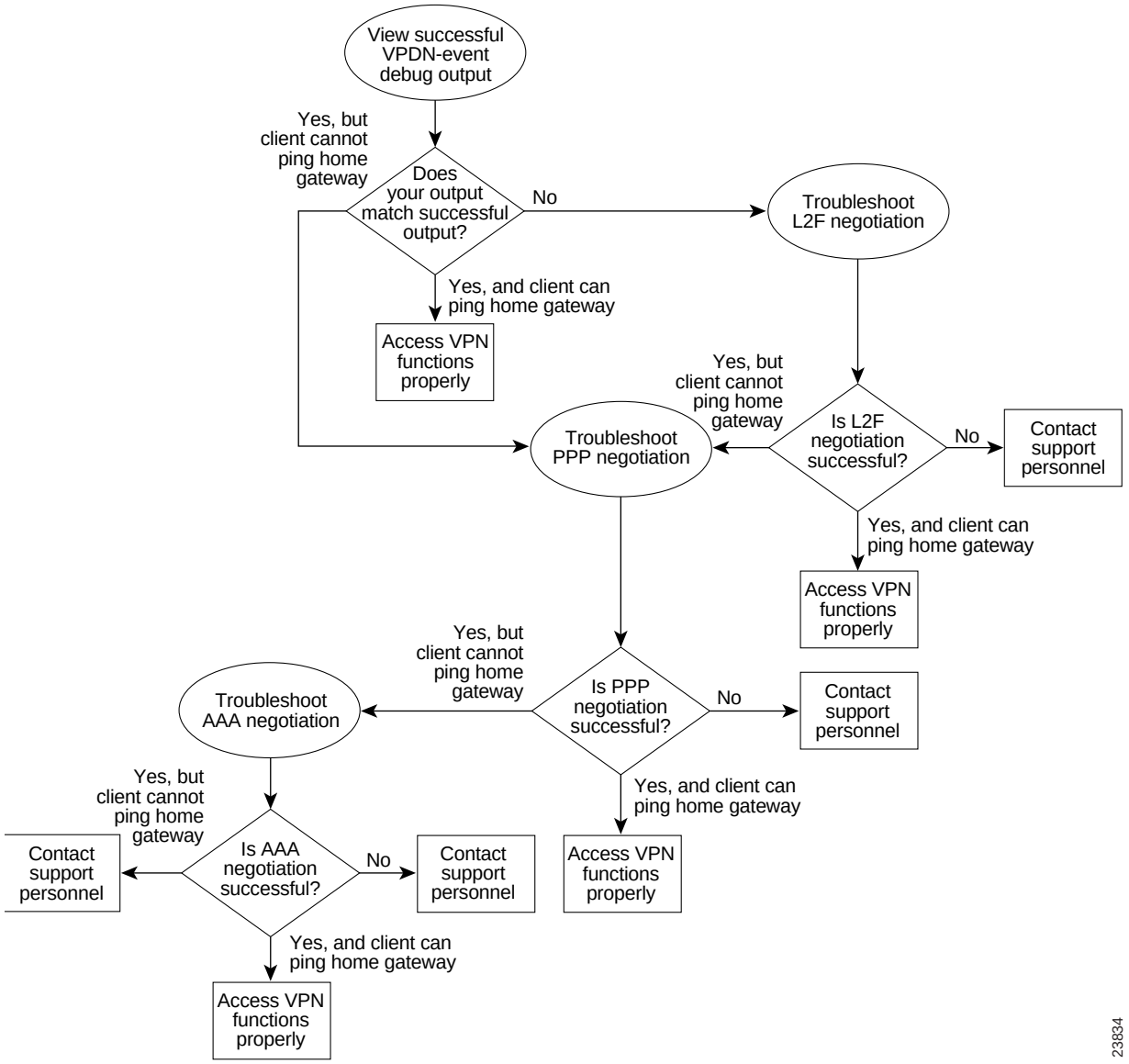
```
ENT_HGW# show vpdn

% 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.

L2F Debug Output for the L2F Case Study

This appendix contains comprehensive debug output from the configuration tasks in this case study. The output is a powerful tool that can help you understand the entire process of how an access VPN is established when a user dials in.

The most important lines of output in this appendix are shown in bold. Tables at the end of the output explain these bold lines.

This appendix is divided into the following sections:

- Debug Output from Configuring Basic Dial Access for the NAS
- Debug Output from Configuring Access VPN with Local AAA
- Debug Output from Configuring Access VPN with Remote AAA

Note 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.

Debug Output from Configuring Basic Dial Access for the NAS

The following debug output is produced when a client dials into the NAS via the public switched telephone network (PSTN) and is authenticated locally on the NAS.

For more information on how to configure basic dial access for the NAS, see "Configuring the NAS for Basic Dial Access."

Enable the following debug commands on the NAS:

- **debug isdn q931**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug modem csm**
- **debug ip peer**

From the client, dial the PRI telephone number assigned to the NAS' T1 trunks. The username is jeremy; the password is subaru. The user is locally authenticated by the NAS.

As the NAS receives the modem call from the client, the following debug command output appears on the NAS' terminal screen.

```
ISP_NAS#
*Jan  1 21:22:16.410: TTY14: destroy timer type 1
*Jan  1 21:22:16.410: TTY14: destroy timer type 0
*Jan  1 21:22:16.410: tty14: Modem: IDLE->READY
*Jan  1 21:22:18.410: %LINK-3-UPDOWN: Interface Async14, changed state to up
*Jan  1 21:22:18.410: As14 PPP: Treating connection as a dedicated line
*Jan  1 21:22:18.410: As14 PPP: Phase is ESTABLISHING, Active Open
*Jan  1 21:22:18.410: As14 LCP: O CONFREQ [Closed] id 1 len 25
*Jan  1 21:22:18.410: As14 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  1 21:22:18.410: As14 LCP:    AuthProto CHAP (0x0305C22305)
*Jan  1 21:22:18.410: As14 LCP:    MagicNumber 0x151213B2 (0x0506151213B2)
*Jan  1 21:22:18.410: As14 LCP:    PFC (0x0702)
*Jan  1 21:22:18.410: As14 LCP:    ACFC (0x0802)
*Jan  1 21:22:18.542: As14 LCP: I CONFACK [REQsent] id 1 len 25
*Jan  1 21:22:18.542: As14 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  1 21:22:18.542: As14 LCP:    AuthProto CHAP (0x0305C22305)
*Jan  1 21:22:18.542: As14 LCP:    MagicNumber 0x151213B2 (0x0506151213B2)
*Jan  1 21:22:18.542: As14 LCP:    PFC (0x0702)
*Jan  1 21:22:18.542: As14 LCP:    ACFC (0x0802)
*Jan  1 21:22:19.262: As14 LCP: I CONFREQ [ACKrcvd] id 2 len 23
*Jan  1 21:22:19.262: As14 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  1 21:22:19.262: As14 LCP:    MagicNumber 0x001A9072 (0x0506001A9072)
*Jan  1 21:22:19.262: As14 LCP:    PFC (0x0702)
*Jan  1 21:22:19.262: As14 LCP:    ACFC (0x0802)
*Jan  1 21:22:19.262: As14 LCP:    Callback 6  (0x0D0306)
*Jan  1 21:22:19.262: As14 LCP: O CONFREJ [ACKrcvd] id 2 len 7
*Jan  1 21:22:19.262: As14 LCP:    Callback 6  (0x0D0306)
*Jan  1 21:22:19.374: As14 LCP: I CONFREQ [ACKrcvd] id 3 len 20
*Jan  1 21:22:19.374: As14 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  1 21:22:19.374: As14 LCP:    MagicNumber 0x001A9072 (0x0506001A9072)
*Jan  1 21:22:19.374: As14 LCP:    PFC (0x0702)
*Jan  1 21:22:19.374: As14 LCP:    ACFC (0x0802)
*Jan  1 21:22:19.374: As14 LCP: O CONFACK [ACKrcvd] id 3 len 20
*Jan  1 21:22:19.374: As14 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  1 21:22:19.374: As14 LCP:    MagicNumber 0x001A9072 (0x0506001A9072)
*Jan  1 21:22:19.374: As14 LCP:    PFC (0x0702)
*Jan  1 21:22:19.374: As14 LCP:    ACFC (0x0802)
*Jan  1 21:22:19.374: As14 LCP: State is Open
*Jan  1 21:22:19.374: As14 PPP: Phase is AUTHENTICATING, by this end
*Jan  1 21:22:19.374: As14 CHAP: O CHALLENGE id 1 len 28 from "ISP_NAS"
*Jan  1 21:22:19.518: As14 CHAP: I RESPONSE id 1 len 27 from "jeremy"
*Jan  1 21:22:19.518: As14 CHAP: O SUCCESS id 1 len 4
*Jan  1 21:22:19.518: As14 PPP: Phase is UP
*Jan  1 21:22:19.518: As14 IPCP: O CONFREQ [Closed] id 1 len 10
*Jan  1 21:22:19.518: As14 IPCP:    Address 172.22.66.23 (0x0306AC164217)
*Jan  1 21:22:19.630: As14 IPCP: I CONFREQ [REQsent] id 1 len 40
*Jan  1 21:22:19.630: As14 IPCP:    CompressType VJ 15 slots CompressSlotID (0x0
206002D0F01)
*Jan  1 21:22:19.630: As14 IPCP:    Address 0.0.0.0 (0x030600000000)
*Jan  1 21:22:19.630: As14 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Jan  1 21:22:19.630: As14 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jan  1 21:22:19.630: As14 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Jan  1 21:22:19.630: As14 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jan  1 21:22:19.630: As14 IPCP: Using pool 'dialin_pool'
*Jan  1 21:22:19.630: ip_get_pool: As14: using pool dialin_pool
*Jan  1 21:22:19.630: ip_get_pool: As14: returning address = 172.22.66.55
*Jan  1 21:22:19.630: As14 IPCP: Pool returned 172.22.66.55
*Jan  1 21:22:19.630: As14 IPCP: O CONFREJ [REQsent] id 1 len 22
*Jan  1 21:22:19.630: As14 IPCP:    CompressType VJ 15 slots CompressSlotID (0x0
206002D0F01)
*Jan  1 21:22:19.630: As14 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jan  1 21:22:19.630: As14 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jan  1 21:22:19.646: As14 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Jan  1 21:22:19.646: As14 CCP:    MS-PPC supported bits 0x00000001 (0x120600000
001)
```

```
*Jan  1 21:22:19.646: As14 CCP:    Stacker history 1 check mode EXTENDED (0x1105
000104)
*Jan  1 21:22:19.646: As14 LCP: O PROTREJ [Open] id 2 len 21 protocol CCP
*Jan  1 21:22:19.646: As14 LCP:  (0x80FD0101000F12060000000111050001)
*Jan  1 21:22:19.646: As14 LCP:  (0x04)
*Jan  1 21:22:19.646: As14 IPCP: I CONFACK [REQsent] id 1 len 10
*Jan  1 21:22:19.646: As14 IPCP:    Address 172.22.66.23 (0x0306AC164217)
*Jan  1 21:22:20.518: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async14, c
hanged state to up
*Jan  1 21:22:21.518: As14 IPCP: TIMEout: State ACKrcvd
*Jan  1 21:22:21.518: As14 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
*Jan  1 21:22:21.518: As14 IPCP:    Address 172.22.66.23 (0x0306AC164217)
*Jan  1 21:22:21.626: As14 IPCP: I CONFACK [REQsent] id 2 len 10
*Jan  1 21:22:21.626: As14 IPCP:    Address 172.22.66.23 (0x0306AC164217)
*Jan  1 21:22:22.634: As14 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
*Jan  1 21:22:22.634: As14 IPCP:    Address 0.0.0.0 (0x030600000000)
*Jan  1 21:22:22.634: As14 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Jan  1 21:22:22.634: As14 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jan  1 21:22:22.634: As14 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Jan  1 21:22:22.634: As14 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jan  1 21:22:22.634: As14 IPCP: O CONFREJ [ACKrcvd] id 2 len 16
*Jan  1 21:22:22.634: As14 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jan  1 21:22:22.634: As14 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jan  1 21:22:22.742: As14 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
*Jan  1 21:22:22.746: As14 IPCP:    Address 0.0.0.0 (0x030600000000)
*Jan  1 21:22:22.746: As14 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Jan  1 21:22:22.746: As14 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Jan  1 21:22:22.746: As14 IPCP: O CONFNAK [ACKrcvd] id 3 len 22
*Jan  1 21:22:22.746: As14 IPCP:    Address 172.22.66.55 (0x0306AC164237)
*Jan  1 21:22:22.746: As14 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
*Jan  1 21:22:22.746: As14 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
*Jan  1 21:22:22.854: As14 IPCP: I CONFREQ [ACKrcvd] id 4 len 22
*Jan  1 21:22:22.854: As14 IPCP:    Address 172.22.66.55 (0x0306AC164237)
*Jan  1 21:22:22.858: As14 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
*Jan  1 21:22:22.858: As14 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
*Jan  1 21:22:22.858: ip_get_pool: As14: validate address = 172.22.66.55
*Jan  1 21:22:22.858: ip_get_pool: As14: using pool dialin_pool
*Jan  1 21:22:22.858: ip_get_pool: As14: returning address = 172.22.66.55
*Jan  1 21:22:22.858: set_ip_peer_addr: As14: address = 172.22.66.55 (3) is redu
ndant
*Jan  1 21:22:22.858: As14 IPCP: O CONFACK [ACKrcvd] id 4 len 22
*Jan  1 21:22:22.858: As14 IPCP:    Address 172.22.66.55 (0x0306AC164237)
*Jan  1 21:22:22.858: As14 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
*Jan  1 21:22:22.858: As14 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
*Jan  1 21:22:22.858: As14 IPCP: State is Open
*Jan  1 21:22:22.858: As14 IPCP: Install route to 172.22.66.55
ISP_NAS#
```

Table 8 describes the debug output events in more detail.

Table 8 Time Stamps and Descriptions for Basic Dial Negotiation Events

Time Stamp	Description
21:22:16.410	A modem call comes in to the access server on TTY line 14.
21:22:18:410	Interface async 4 comes up. After PPP launches, TTY line 14 becomes async interface 14.
21:22:18:410	An incoming PPP frame is recognized. PPP is launched on TTY line 14.
21:22:19:262	Incoming config request (I CONFREQ). The remote test PC requests a set of options to be negotiated. The PC asks the Cisco AS5300 to support the callback option.
21:22:19:262	Outgoing config reject (O CONFREJ). The Cisco AS5300 rejects the callback option. The access server is not configured to support Microsoft Callback in this case study.

Time Stamp	Description
21:22:19:374	Incoming config request (I CONFREQ). The test PC requests a new set of options. Notice that Microsoft Callback is not requested.
21:22:19:374	Outgoing config acknowledgment (O CONFACK). The Cisco AS5300 accepts the new set of options.
21:22:19:374	LCP is now open (LCP: State is Open). Both sides have acknowledged (CONFACK) the other side's configuration request (CONFREQ).
21:22:19:374	After LCP negotiates, authentication starts. Authentication must take place before any network protocols, such as IP, are delivered. Both sides authenticate with the method negotiated during LCP. The Cisco AS5300 authenticates the client using CHAP. The client does not authenticate the access server.
21:22:19:374	Outgoing challenge sent from ISP_NAS.
21:22:19:518	Incoming CHAP response from the test PC, which shows the username jeremy.
21:22:19:518	An outgoing success message is sent from the NAS—authentication is successful.
21:22:19:518	PPP is up. The Cisco AS5300 PPP link is now open and available to negotiate any network protocols supported by both peers.
21:22:19:646	The client requests support for Microsoft Point-to-Point Compression (MPPC). The Cisco AS5300 rejects this request. The access server's integrated modems already support hardware compression, and the Cisco IOS is not configured to support software compression.
21:22:22:634	The primary and secondary DNS addresses are negotiated. At first, the client asks for 0.0.0.0. addresses. The access server sends out a CONFNAK and supplies the correct values, which include an IP address from the pool, the primary DNS address, and the backup DNS address.
21:22:22:854	The client sends an incoming request saying that the new values are accepted. Whenever the access server sends out a CONFNAK that includes values, the client still has to accept the new values.
21:22:22:858	An outgoing CONFACK is sent for IPCP. The state is open for IPCP. A route is negotiated and installed for the IPCP peer, which is assigned IP address 172.22.66.55.

Debug Output from Configuring Access VPN with Local AAA

The following debug output is produced by an access VPN that is using local AAA. The client dials in to the NAS, is forwarded to the home gateway using L2F, and the tunnel and username are authenticated using local AAA.

For more information on how to configure the access VPN for local AAA, see "Configuring the Access VPN to Work with Local AAA."

Enable the following debug commands on the NAS.

- **debug isdn q931**
- **debug modem csm**
- **debug ppp authentication**
- **debug ppp negotiation**
- **debug vpdn event**
- **debug vpdn l2x-events**

Enable the following debug commands on the home gateway:

- **debug vpdn events**
- **debug vpdn l2x-events**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug vtemplate**
- **debug ip peer**

Send an asynchronous PPP modem call in to the access server. As the call is forwarded to the home gateway, the following debug output appears on the NAS' terminal screen:

```
ISP_NAS#
*Jan  2 01:04:48.817: ISDN Se0:23: RX <-  SETUP pd = 8  callref = 0x0266
*Jan  2 01:04:48.817:         Bearer Capability i = 0x8090A2
*Jan  2 01:04:48.817:         Channel ID i = 0xA98381
*Jan  2 01:04:48.821:         Progress Ind i = 0x8283 - Origination address is n
on-ISDN
*Jan  2 01:04:48.821:         Calling Party Number i = '!', 0x83, '4089548042'
*Jan  2 01:04:48.821:         Called Party Number i = 0xC1, '5550945'
*Jan  2 01:04:48.821: ISDN Se0:23: TX ->  CALL_PROC pd = 8  callref = 0x8266
*Jan  2 01:04:48.821:         Channel ID i = 0xA98381
*Jan  2 01:04:48.821: ISDN Se0:23: TX ->  ALERTING pd = 8  callref = 0x8266
*Jan  2 01:04:48.821: EVENT_FROM_ISDN::dchan_idb=0x60E9DD98, call_id=0x2E, ces=0
x1
   bchan=0x0, event=0x1, cause=0x0

*Jan  2 01:04:48.821: VDEV_ALLOCATE: slot 1 and port 21 is allocated.

*Jan  2 01:04:48.821: EVENT_FROM_ISDN:(002E): DEV_INCALL at slot 1 and port 21

*Jan  2 01:04:48.825: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 21
*Jan  2 01:04:48.825: Mica Modem(1/21): Configure(0x1 = 0x0)
*Jan  2 01:04:48.825: Mica Modem(1/21): Configure(0x23 = 0x0)
*Jan  2 01:04:48.825: Mica Modem(1/21): Call Setup
*Jan  2 01:04:48.913: Mica Modem(1/21): State Transition to Call Setup
*Jan  2 01:04:48.913: Mica Modem(1/21): Went offhook
*Jan  2 01:04:48.913: CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port
 21
*Jan  2 01:04:48.913: ISDN Se0:23: TX ->  CONNECT pd = 8  callref = 0x8266
*Jan  2 01:04:48.945: ISDN Se0:23: RX <-  CONNECT_ACK pd = 8  callref = 0x0266
*Jan  2 01:04:48.945: EVENT_FROM_ISDN::dchan_idb=0x60E9DD98, call_id=0x2E, ces=0
x1
   bchan=0x0, event=0x4, cause=0x0

*Jan  2 01:04:48.949: EVENT_FROM_ISDN:(002E): DEV_CONNECTED at slot 1 and port 2
1

*Jan  2 01:04:48.949: CSM_PROC_IC4_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at
 slot 1, port 21
*Jan  2 01:04:48.949: Mica Modem(1/21): Link Initiate
*Jan  2 01:04:50.049: Mica Modem(1/21): State Transition to Connect
*Jan  2 01:04:55.201: Mica Modem(1/21): State Transition to Link
*Jan  2 01:05:12.753: Mica Modem(1/21): State Transition to Trainup
*Jan  2 01:05:14.489: Mica Modem(1/21): State Transition to EC Negotiating
*Jan  2 01:05:15.149: Mica Modem(1/21): State Transition to Steady State
*Jan  2 01:05:17.969: %LINK-3-UPDOWN: Interface Async22, changed state to up
*Jan  2 01:05:17.969: As22 PPP: Treating connection as a dedicated line
*Jan  2 01:05:17.969: As22 PPP: Phase is ESTABLISHING, Active Open
*Jan  2 01:05:17.969: As22 LCP: O CONFREQ [Closed] id 1 len 39
*Jan  2 01:05:17.969: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
```

```
*Jan  2 01:05:17.969: As22 LCP:    AuthProto CHAP (0x0305C22305)
*Jan  2 01:05:17.969: As22 LCP:    MagicNumber 0x15DE3BBE (0x050615DE3BBE)
*Jan  2 01:05:17.969: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:17.969: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:17.969: As22 LCP:    MRRU 1524 (0x110405F4)
*Jan  2 01:05:17.969: As22 LCP:    EndpointDisc 1 Local (0x130A014953505F4E4153)

*Jan  2 01:05:18.101: As22 LCP: I CONFREJ [REQsent] id 1 len 18
*Jan  2 01:05:18.101: As22 LCP:    MRRU 1524 (0x110405F4)
*Jan  2 01:05:18.101: As22 LCP:    EndpointDisc 1 Local (0x130A014953505F4E4153)

*Jan  2 01:05:18.105: As22 LCP: O CONFREQ [REQsent] id 2 len 25
*Jan  2 01:05:18.105: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  2 01:05:18.105: As22 LCP:    AuthProto CHAP (0x0305C22305)
*Jan  2 01:05:18.105: As22 LCP:    MagicNumber 0x15DE3BBE (0x050615DE3BBE)
*Jan  2 01:05:18.105: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:18.105: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:18.213: As22 LCP: I CONFREQ [REQsent] id 2 len 23
*Jan  2 01:05:18.213: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  2 01:05:18.213: As22 LCP:    MagicNumber 0x00E6BDE9 (0x050600E6BDE9)
*Jan  2 01:05:18.213: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:18.213: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:18.217: As22 LCP:    Callback 6  (0x0D0306)
*Jan  2 01:05:18.217: As22 LCP: O CONFREJ [REQsent] id 2 len 7
*Jan  2 01:05:18.217: As22 LCP:    Callback 6  (0x0D0306)
*Jan  2 01:05:18.229: As22 LCP: I CONFACK [REQsent] id 2 len 25
*Jan  2 01:05:18.229: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  2 01:05:18.229: As22 LCP:    AuthProto CHAP (0x0305C22305)
*Jan  2 01:05:18.229: As22 LCP:    MagicNumber 0x15DE3BBE (0x050615DE3BBE)
*Jan  2 01:05:18.233: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:18.233: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:18.325: As22 LCP: I CONFREQ [ACKrcvd] id 3 len 20
*Jan  2 01:05:18.325: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  2 01:05:18.325: As22 LCP:    MagicNumber 0x00E6BDE9 (0x050600E6BDE9)
*Jan  2 01:05:18.325: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:18.325: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:18.325: As22 LCP: O CONFACK [ACKrcvd] id 3 len 20
*Jan  2 01:05:18.325: As22 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Jan  2 01:05:18.329: As22 LCP:    MagicNumber 0x00E6BDE9 (0x050600E6BDE9)
*Jan  2 01:05:18.329: As22 LCP:    PFC (0x0702)
*Jan  2 01:05:18.329: As22 LCP:    ACFC (0x0802)
*Jan  2 01:05:18.329: As22 LCP: State is Open
*Jan  2 01:05:18.329: As22 PPP: Phase is AUTHENTICATING, by this end
*Jan  2 01:05:18.329: As22 CHAP: O CHALLENGE id 1 len 28 from "ISP_NAS"
*Jan  2 01:05:18.469: As22 CHAP: I RESPONSE id 1 len 35 from "jeremy@hgw.com"
*Jan  2 01:05:18.469: VPDN: Got DNIS string 5550945
*Jan  2 01:05:18.469: As22 VPDN: Looking for tunnel -- hgw.com --
*Jan  2 01:05:18.473:  L2F: Tunnel state closed
*Jan  2 01:05:18.473: As22 VPDN: Get tunnel info for hgw.com with NAS ISP_NAS, I
P 172.22.66.25
*Jan  2 01:05:18.473: As22 VPDN: Forward to address 172.22.66.25
*Jan  2 01:05:18.473: As22 VPDN: Forwarding...
*Jan  2 01:05:18.473: As22 VPDN: Bind interface direction=1
*Jan  2 01:05:18.473:  L2F: MID  state closed
*Jan  2 01:05:18.473: L2F: Open UDP socket to 172.22.66.25
*Jan  2 01:05:18.473:  L2F: Tunnel state opening
*Jan  2 01:05:18.473: As22 L2F: MID jeremy@hgw.com state waiting_for_tunnel
*Jan  2 01:05:18.473: As22 VPDN: jeremy@hgw.com is forwarded
*Jan  2 01:05:18.477: L2F: L2F_CONF received
*Jan  2 01:05:18.477: L2F: Removing resend packet (L2F_CONF)
*Jan  2 01:05:18.477: ISP_NAS L2F: Tunnel state open
*Jan  2 01:05:18.481: L2F: L2F_OPEN received
*Jan  2 01:05:18.481: L2F: Removing resend packet (L2F_OPEN)
*Jan  2 01:05:18.481: L2F: Building nas2gw_mid0
*Jan  2 01:05:18.481: L2F: L2F_CLIENT_INFO: CLID/DNIS 4089548042/5550945
```

```
*Jan  2 01:05:18.481: L2F: L2F_CLIENT_INFO: NAS-Port Async22
*Jan  2 01:05:18.481: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
*Jan  2 01:05:18.481: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/0/0
*Jan  2 01:05:18.481: As22 L2F: MID jeremy@hgw.com state opening
*Jan  2 01:05:18.481: VPDN: Chap authentication succeeded for ISP_NAS
*Jan  2 01:05:18.569: L2F: L2F_OPEN received
*Jan  2 01:05:18.569: L2F: Got a MID management packet
*Jan  2 01:05:18.569: L2F: Removing resend packet (L2F_OPEN)
*Jan  2 01:05:18.569: As22 L2F: MID jeremy@hgw.com state open
*Jan  2 01:05:18.569: As22 L2F: MID synced NAS/HG Clid=8/8 Mid=1
*Jan  2 01:05:18.569: As22 PPP: Phase is FORWARDED
*Jan  2 01:05:19.473: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async22, c
hanged state to up
```

Table 9 describes the debug output events in more detail.

Table 9 Time Stamps and Descriptions of Access VPN Events on the NAS

Time Stamp	Description
01:04:48.817	The inbound call is received from the PRI TDM stream. The ISDN bearer capability reports that the call is an analog call (0x8090A2).
01:04:48.825 to 01:04:48.913	The access server routes the call to the onboard MICA modem at 1/21 and begins negotiation with the remote site.
01:04:48.913 to 01:05:17.969	Both sides successfully negotiate, and asynchronous interface 22 comes up. At this point, the NAS still does not know that the call is an access VPN call.
01:05:17.969	The first phase of PPP negotiation begins, which is link control protocol (LCP) negotiation. In this phase, the remote peers negotiate what type of authentication to use. The NAS demands that the client authenticate with CHAP.
01:05:18.213 to 01:05:18.329	The client asks the NAS to support call back. The NAS denies the request. The client now resends the same request without the rejected option.
01:05:18.329	The NAS sends the authentication CHAP challenge to the client.
01:05:18.469	The client responds with “jeremy@hgw.com.” The NAS saves the client’s response and later forwards it to the home gateway.
01:05:18.469	The NAS found a DNIS string. VPDN authorization is about to begin.
01:05:18.473	• Tunnel information is found for the domain name hgw.com, tunnel name ISP_NAS, and the tunnel IP endpoint 172.22.66.25. • A UDP socket interface is opened to the home gateway’s IP address. Because L2F is a UDP packet, a socket interface needs to be created. • Because no tunnel currently exists for jeremy@hgw.com, the message “waiting_for_tunnel” appears. After the tunnel is established, the message “jeremy@hgw.com is forwarded” appears. • The tunnel is authenticated and established between the NAS and home gateway. CHAP is the default tunnel authentication method.
01:05:18.473 to 01:05:18.569	The L2F protocol begins. A bidirectional authentication takes place between the NAS and the home gateway.
01:05:18.481	Cisco proprietary L2F client information is forwarded to the home gateway. This information is used by the home gateway for accounting purposes. L2F uses standard AV pairs to forward this information.
01:05:18.569	The PPP session is forwarded to the home gateway. Notice that IPCP negotiation does not occur on the NAS, but occurs on the home gateway. See the home gateway’s debug output.
01:05:19.473	The asynchronous line protocol is up, which enables network layer communication.

As the call is forwarded from the NAS to the home gateway, the following debug output appears on the home gateway's terminal screen.

```
ENT_HGW#
*Feb  4 14:14:40.413: L2F: L2F_CONF received
*Feb  4 14:14:40.413: L2F: Creating new tunnel for ISP_NAS
*Feb  4 14:14:40.413:  L2F: Tunnel state closed
*Feb  4 14:14:40.413: L2F: Got a tunnel named ISP_NAS, responding
*Feb  4 14:14:40.417: L2F: Open UDP socket to 172.22.66.23
*Feb  4 14:14:40.417: ISP_NAS L2F: Tunnel state opening
*Feb  4 14:14:40.417: L2F: L2F_OPEN received
*Feb  4 14:14:40.417: L2F: Removing resend packet (L2F_CONF)
*Feb  4 14:14:40.417: VPDN: Chap authentication succeeded for ISP_NAS
*Feb  4 14:14:40.417: ISP_NAS L2F: Tunnel state open
*Feb  4 14:14:40.421: L2F: L2F_OPEN received
*Feb  4 14:14:40.421: L2F: L2F_CLIENT_INFO: CLID/DNIS 4089548042/5550945
*Feb  4 14:14:40.421: L2F: L2F_CLIENT_INFO: NAS-Port Async21
*Feb  4 14:14:40.421: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
*Feb  4 14:14:40.421: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/0/0
*Feb  4 14:14:40.421: L2F: Got a MID management packet
*Feb  4 14:14:40.421:  L2F: MID  state closed
*Feb  4 14:14:40.421: L2F: Start create mid intf process for jeremy@hgw.com
*Feb  4 14:14:40.421: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
*Feb  4 14:14:40.421: Vi1 VTEMPLATE: Hardware address 0050.d193.e000
*Feb  4 14:14:40.421: Vi1 VPDN: Virtual interface created for jeremy@hgw.com
*Feb  4 14:14:40.421: Vi1 VPDN: Set to Async interface
*Feb  4 14:14:40.425: Vi1 PPP: Phase is DOWN, Setup
*Feb  4 14:14:40.425: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Feb  4 14:14:40.425: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vt
emplate
*Feb  4 14:14:40.425: Vi1 VTEMPLATE: ************* CLONE VACCESS1 **************
***
*Feb  4 14:14:40.425: Vi1 VTEMPLATE: Clone from Virtual-Template1
interface Virtual-Access1
default ip address
no ip address
encap ppp
ip unnumbered fastethernet 0/0
no ip directed-broadcast
ip unnumbered fastethernet 0/0
no ip directed-broadcast
ppp authentication chap
peer default ip address pool default
encapsulation ppp
ppp multilink
end

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 LCP: O CONFREQ [Closed] id 1 len 39
*Feb  4 14:14:40.505: Vi1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Feb  4 14:14:40.505: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
*Feb  4 14:14:40.505: Vi1 LCP:    MagicNumber 0x566F3EA8 (0x0506566F3EA8)
*Feb  4 14:14:40.505: Vi1 LCP:    PFC (0x0702)
*Feb  4 14:14:40.505: Vi1 LCP:    ACFC (0x0802)
*Feb  4 14:14:40.505: Vi1 LCP:    MRRU 1524 (0x110405F4)
*Feb  4 14:14:40.505: Vi1 LCP:    EndpointDisc 1 Local (0x130A01454E545F484757)
*Feb  4 14:14:40.505: Vi1 VPDN: Bind interface direction=2
*Feb  4 14:14:40.505: Vi1 PPP: Treating connection as a dedicated line
*Feb  4 14:14:40.505: Vi1 LCP: I FORCED CONFREQ len 21
*Feb  4 14:14:40.505: Vi1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
*Feb  4 14:14:40.505: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
*Feb  4 14:14:40.505: Vi1 LCP:    MagicNumber 0x15B7E4FD (0x050615B7E4FD)
*Feb  4 14:14:40.505: Vi1 LCP:    PFC (0x0702)
```

```
*Feb  4 14:14:40.505: Vi1 LCP:    ACFC (0x0802)
*Feb  4 14:14:40.505: Vi1 VPDN: PPP LCP accepted rcv CONFACK
*Feb  4 14:14:40.505: Vi1 VPDN: PPP LCP accepted sent CONFACK
*Feb  4 14:14:40.505: Vi1 PPP: Phase is AUTHENTICATING, by this end
*Feb  4 14:14:40.505: Vi1 CHAP: O CHALLENGE id 2 len 28 from "ENT_HGW"
*Feb  4 14:14:40.505: Vi1 L2F: Transfer NAS-Rate L2F/0/0 to LCP
*Feb  4 14:14:40.509: Vi1 CHAP: I RESPONSE id 1 len 35 from "jeremy@hgw.com"
*Feb  4 14:14:40.509: Vi1 L2F: Finish create mid intf for jeremy@hgw.com
*Feb  4 14:14:40.509: Vi1 L2F: MID jeremy@hgw.com state open
*Feb  4 14:14:40.509: Vi1 CHAP: O SUCCESS id 1 len 4
*Feb  4 14:14:40.509: Vi1 PPP: Phase is UP
*Feb  4 14:14:40.509: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Feb  4 14:14:40.509: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
*Feb  4 14:14:40.617: Vi1 IPCP: I CONFREQ [REQsent] id 1 len 40
*Feb  4 14:14:40.617: Vi1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x02
06002D0F01)
*Feb  4 14:14:40.617: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Feb  4 14:14:40.617: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Feb  4 14:14:40.617: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Feb  4 14:14:40.621: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Feb  4 14:14:40.621: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Feb  4 14:14:40.621: Vi1 IPCP: Using pool 'default'
*Feb  4 14:14:40.621: ip_get_pool: Vi1: using pool default
*Feb  4 14:14:40.621: ip_get_pool: Vi1: returning address = 172.30.2.1
*Feb  4 14:14:40.621: Vi1 IPCP: Pool returned 172.30.2.1
*Feb  4 14:14:40.621: Vi1 IPCP: O CONFREJ [REQsent] id 1 len 10
*Feb  4 14:14:40.621: Vi1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x02
06002D0F01)
*Feb  4 14:14:40.633: Vi1 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Feb  4 14:14:40.633: Vi1 CCP:    MS-PPC supported bits 0x00000001 (0x1206000000
01)
*Feb  4 14:14:40.633: Vi1 CCP:    Stacker history 1 check mode EXTENDED (0x11050
00104)
*Feb  4 14:14:40.633: Vi1 LCP: O PROTREJ [Open] id 2 len 21 protocol CCP
*Feb  4 14:14:40.633: Vi1 LCP:  (0x80FD0101000F12060000000111050001)
*Feb  4 14:14:40.633: Vi1 LCP:  (0x04)
*Feb  4 14:14:40.633: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Feb  4 14:14:40.637: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
1d02h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
*Feb  4 14:14:42.505: Vi1 LCP: TIMEout: State Open
*Feb  4 14:14:42.509: Vi1 IPCP: TIMEout: State ACKrcvd
*Feb  4 14:14:42.509: Vi1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
*Feb  4 14:14:42.509: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
*Feb  4 14:14:42.613: Vi1 IPCP: I CONFACK [REQsent] id 2 len 10
*Feb  4 14:14:42.617: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
*Feb  4 14:14:43.621: Vi1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
*Feb  4 14:14:43.621: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Feb  4 14:14:43.621: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Feb  4 14:14:43.621: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Feb  4 14:14:43.621: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Feb  4 14:14:43.621: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Feb  4 14:14:43.621: Vi1 IPCP: O CONFNAK [ACKrcvd] id 2 len 34
*Feb  4 14:14:43.621: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
*Feb  4 14:14:43.621: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
*Feb  4 14:14:43.621: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
*Feb  4 14:14:43.621: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
*Feb  4 14:14:43.621: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
*Feb  4 14:14:43.749: Vi1 IPCP: I CONFREQ [ACKrcvd] id 3 len 34
*Feb  4 14:14:43.749: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
*Feb  4 14:14:43.749: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
*Feb  4 14:14:43.749: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
*Feb  4 14:14:43.749: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
*Feb  4 14:14:43.749: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
*Feb  4 14:14:43.749: ip_get_pool: Vi1: validate address = 172.30.2.1
```

```
*Feb  4 14:14:43.749: ip_get_pool: Vi1: using pool default
*Feb  4 14:14:43.749: ip_get_pool: Vi1: returning address = 172.30.2.1
*Feb  4 14:14:43.749: set_ip_peer_addr: Vi1: address = 172.30.2.1 (3) is redunda
nt
*Feb  4 14:14:43.749: Vi1 IPCP: O CONFACK [ACKrcvd] id 3 len 34
*Feb  4 14:14:43.749: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
*Feb  4 14:14:43.749: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
*Feb  4 14:14:43.749: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
*Feb  4 14:14:43.753: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
*Feb  4 14:14:43.753: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
*Feb  4 14:14:43.753: Vi1 IPCP: State is Open
*Feb  4 14:14:43.753: Vi1 IPCP: Install route to 172.30.2.1
ENT_HGW#
```

Table 10 describes the debug output events in more detail.

Table 10 Time Stamps and Descriptions of Access VPN Events on the Home Gateway

Time Stamp	Description
14:14:40.413 to 14:14:40:417	The home gateway receives the request from the NAS to open an L2F tunnel. The home gateway authenticates the tunnel and opens it.
14:14:40:421	The NAS forwards the client's client information to the home gateway.
14:14:40:421 to 14:14:40:425	A virtual-access interface is cloned from virtual template 1, which is not a physical interface, but it is treated like a regular interface that uses the IP address of the Fast Ethernet 0/0 interface The debug output following "interface Virtual-Access1" lists every command that has been configured for virtual template 1. Enter the **clear vtemplate** command to reset the command history.
14:14:40.505	The NAS forces the information from the LCP negotiation with the client onto the virtual-access interface.
14:14:40:505 to 14:14:40:509	The home gateway sends a CHAP challenge to the client. The client responds and is authenticated by the home gateway.
14:14:40:621	The home gateway assigns the client the IP address 172.30.2.1 from the default pool.
14:14:40:637	The line protocol on interface Virtual-Access1 is changed to the up state.
14:14:43.621	The client requests IP addresses of DNS and WINS servers.
14:14:43.749 to 14:14:43.753	The home gateway receives a positive acknowledgment from the client confirming the IP addresses of the DNS and WNIS servers.
14:14:43:753	The home gateway installs the route to the client's IP address, 172.30.2.1

Debug Output from Configuring Access VPN with Remote AAA

The following debug output is produced by an access VPN using remote AAA. The client dials in to the NAS, is forwarded to the home gateway using L2F. The NAS authenticates the tunnel using CiscoSecure UNIX, and the home gateway authenticates the username using CiscoSecure NT.

For more information on how to configure the access VPN for remote AAA, see "Configuring the Access VPN to Work with Remote AAA."

Enable the following debug commands on the NAS:

- **debug isdn q931**
- **debug modem csm**
- **debug radius**
- **debug aaa authentication**
- **debug aaa authorization**
- **debug ppp authentication**
- **debug ppp negotiation**
- **debug vpdn event**
- **debug vpdn l2x-event**

Enable the following debug commands on the home gateway:

- **debug radius**
- **debug aaa authentication**
- **debug aaa authorization**
- **debug ppp negotiation**
- **debug ppp authentication**
- **debug vtemplate**
- **debug ip peer**
- **debug vpdn l2x-errors**
- **debug vpdn l2x-events**
- **debug vpdn events**

Launch an asynchronous PPP modem call in to the NAS. As the NAS receives the call and forwards it to the home gateway, the following debug output appears on the NAS:

```
ISP_NAS#
Jan  7 19:29:15.775: ISDN Se0:23: RX <-  SETUP pd = 8  callref = 0x0301
Jan  7 19:29:15.775:         Bearer Capability i = 0x9090A2
Jan  7 19:29:15.775:         Channel ID i = 0xA98381
Jan  7 19:29:15.775:         Calling Party Number i = 0x0083, '408'
Jan  7 19:29:15.775:         Called Party Number i = 0xC1, '5550945'
Jan  7 19:29:15.779: ISDN Se0:23: TX ->  CALL_PROC pd = 8  callref = 0x8301
Jan  7 19:29:15.779:         Channel ID i = 0xA98381
Jan  7 19:29:15.779: ISDN Se0:23: TX ->  ALERTING pd = 8  callref = 0x8301
Jan  7 19:29:15.779: EVENT_FROM_ISDN::dchan_idb=0x60E97CDC, call_id=0x53, ces=0x
1
   bchan=0x0, event=0x1, cause=0x0

Jan  7 19:29:15.779: VDEV_ALLOCATE: slot 1 and port 10 is allocated.
```

```
Jan  7 19:29:15.779: EVENT_FROM_ISDN:(0053): DEV_INCALL at slot 1 and port 10

Jan  7 19:29:15.779: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 10
Jan  7 19:29:15.779: Mica Modem(1/10): Configure(0x1 = 0x0)
Jan  7 19:29:15.779: Mica Modem(1/10): Configure(0x23 = 0x0)
Jan  7 19:29:15.779: Mica Modem(1/10): Call Setup
Jan  7 19:29:15.923: Mica Modem(1/10): State Transition to Call Setup
Jan  7 19:29:15.923: Mica Modem(1/10): Went offhook
Jan  7 19:29:15.923: CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port
10
Jan  7 19:29:15.923: ISDN Se0:23: TX ->  CONNECT pd = 8  callref = 0x8301
Jan  7 19:29:15.939: ISDN Se0:23: RX <-  CONNECT_ACK pd = 8  callref = 0x0301
Jan  7 19:29:15.943: EVENT_FROM_ISDN::dchan_idb=0x60E97CDC, call_id=0x53, ces=0x
1
   bchan=0x0, event=0x4, cause=0x0

Jan  7 19:29:15.943: EVENT_FROM_ISDN:(0053): DEV_CONNECTED at slot 1 and port 10

Jan  7 19:29:15.943: CSM_PROC_IC4_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at
slot 1, port 10
Jan  7 19:29:15.943: Mica Modem(1/10): Link Initiate
Jan  7 19:29:17.059: Mica Modem(1/10): State Transition to Connect
Jan  7 19:29:22.211: Mica Modem(1/10): State Transition to Link
Jan  7 19:29:33.715: Mica Modem(1/10): State Transition to Trainup
Jan  7 19:29:36.951: Mica Modem(1/10): State Transition to EC Negotiating
Jan  7 19:29:37.491: Mica Modem(1/10): State Transition to Steady State
Jan  7 19:29:40.339: %LINK-3-UPDOWN: Interface Async11, changed state to up
Jan  7 19:29:40.339: As11 PPP: Treating connection as a dedicated line
Jan  7 19:29:40.339: As11 PPP: Phase is ESTABLISHING, Active Open
Jan  7 19:29:40.339: As11 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
Jan  7 19:29:40.339: As11 LCP: O CONFREQ [Closed] id 3 len 25
Jan  7 19:29:40.339: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:40.339: As11 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:40.339: As11 LCP:    MagicNumber 0x33911E0F (0x050633911E0F)
Jan  7 19:29:40.339: As11 LCP:    PFC (0x0702)
Jan  7 19:29:40.339: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:40.443: As11 LCP: I CONFACK [REQsent] id 3 len 25
Jan  7 19:29:40.443: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:40.443: As11 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:40.443: As11 LCP:    MagicNumber 0x33911E0F (0x050633911E0F)
Jan  7 19:29:40.443: As11 LCP:    PFC (0x0702)
Jan  7 19:29:40.443: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:40.859: As11 LCP: I CONFREQ [ACKrcvd] id 2 len 23
Jan  7 19:29:40.859: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:40.859: As11 LCP:    MagicNumber 0x0002D813 (0x05060002D813)
Jan  7 19:29:40.859: As11 LCP:    PFC (0x0702)
Jan  7 19:29:40.859: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:40.859: As11 LCP:    Callback 6  (0x0D0306)
Jan  7 19:29:40.859: As11 LCP: O CONFREJ [ACKrcvd] id 2 len 7
Jan  7 19:29:40.859: As11 LCP:    Callback 6  (0x0D0306)
Jan  7 19:29:42.339: As11 LCP: TIMEout: State ACKrcvd
Jan  7 19:29:42.339: As11 LCP: O CONFREQ [ACKrcvd] id 4 len 25
Jan  7 19:29:42.339: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:42.339: As11 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:42.339: As11 LCP:    MagicNumber 0x33911E0F (0x050633911E0F)
Jan  7 19:29:42.339: As11 LCP:    PFC (0x0702)
Jan  7 19:29:42.339: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:42.439: As11 LCP: I CONFACK [REQsent] id 4 len 25
Jan  7 19:29:42.439: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:42.439: As11 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:42.439: As11 LCP:    MagicNumber 0x33911E0F (0x050633911E0F)
Jan  7 19:29:42.439: As11 LCP:    PFC (0x0702)
Jan  7 19:29:42.439: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:43.859: As11 LCP: I CONFREQ [ACKrcvd] id 3 len 23
Jan  7 19:29:43.859: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
```

```
Jan  7 19:29:43.859: As11 LCP:    MagicNumber 0x0002D813 (0x05060002D813)
Jan  7 19:29:43.863: As11 LCP:    PFC (0x0702)
Jan  7 19:29:43.863: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:43.863: As11 LCP:    Callback 6  (0x0D0306)
Jan  7 19:29:43.863: As11 LCP: O CONFREJ [ACKrcvd] id 3 len 7
Jan  7 19:29:43.863: As11 LCP:    Callback 6  (0x0D0306)
Jan  7 19:29:44.003: As11 LCP: I CONFREQ [ACKrcvd] id 4 len 20
Jan  7 19:29:44.003: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:44.003: As11 LCP:    MagicNumber 0x0002D813 (0x05060002D813)
Jan  7 19:29:44.003: As11 LCP:    PFC (0x0702)
Jan  7 19:29:44.003: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:44.007: As11 LCP: O CONFACK [ACKrcvd] id 4 len 20
Jan  7 19:29:44.007: As11 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:44.007: As11 LCP:    MagicNumber 0x0002D813 (0x05060002D813)
Jan  7 19:29:44.007: As11 LCP:    PFC (0x0702)
Jan  7 19:29:44.007: As11 LCP:    ACFC (0x0802)
Jan  7 19:29:44.007: As11 LCP: State is Open
Jan  7 19:29:44.007: As11 PPP: Phase is AUTHENTICATING, by this end
Jan  7 19:29:44.007: As11 CHAP: O CHALLENGE id 2 len 28 from "ISP_NAS"
Jan  7 19:29:44.115: As11 CHAP: I RESPONSE id 2 len 35 from "jeremy@hgw.com"
Jan  7 19:29:44.115: As11 PPP: Phase is FORWARDING
Jan  7 19:29:44.115: sVPDN: Got DNIS string As11
Jan  7 19:29:44.119: As11 VPDN: Looking for tunnel -- hgw.com --
Jan  7 19:29:44.119: AAA: parse name=Async11 idb type=10 tty=11
Jan  7 19:29:44.119: AAA: name=Async11 flags=0x11 type=4 shelf=0 slot=0 adapter=
0 port=11 channel=0
Jan  7 19:29:44.119: AAA: parse name=Serial0:0 idb type=12 tty=-1
Jan  7 19:29:44.119: AAA: name=Serial0:0 flags=0x51 type=1 shelf=0 slot=0 adapte
r=0 port=0 channel=0
Jan  7 19:29:44.119: AAA/AUTHEN: create_user (0x6118F250) user='hgw.com' ruser='
' port='Async11' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan  7 19:29:44.119: AAA/AUTHOR/VPDN (338468652): Port='Async11' list='default'
service=NET
Jan  7 19:29:44.119: AAA/AUTHOR/VPDN:  (338468652) send AV service=ppp
Jan  7 19:29:44.119: AAA/AUTHOR/VPDN:  (338468652) send AV protocol=vpdn
Jan  7 19:29:44.119: AAA/AUTHOR/VPDN (338468652) found list "default"
Jan  7 19:29:44.119: AAA/AUTHOR/VPDN:  (338468652) Method=RADIUS
Jan  7 19:29:44.119: RADIUS: authenticating to get author data
Jan  7 19:29:44.119: RADIUS: ustruct sharecount=2
Jan  7 19:29:44.119: RADIUS: Initial Transmit Async11 id 52 172.22.66.18:1645, A
ccess-Request, len 71
Jan  7 19:29:44.119:         Attribute 4 6 AC164217
Jan  7 19:29:44.119:         Attribute 5 6 0000000B
Jan  7 19:29:44.119:         Attribute 61 6 00000000
Jan  7 19:29:44.119:         Attribute 1 9 6867772E
Jan  7 19:29:44.119:         Attribute 2 18 99DFD8F8
Jan  7 19:29:44.119:         Attribute 6 6 00000005
Jan  7 19:29:44.123: RADIUS: Received from id 52 172.22.66.18:1645, Access-Accep
t, len 153
Jan  7 19:29:44.123:         Attribute 26 31 0000000901197670
Jan  7 19:29:44.123:         Attribute 26 32 00000009011A7670
Jan  7 19:29:44.123:         Attribute 26 31 0000000901197670
Jan  7 19:29:44.123:         Attribute 26 39 0000000901217670
Jan  7 19:29:44.123: RADIUS: saved authorization data for user 6118F250 at 61075
698
Jan  7 19:29:44.127: RADIUS: cisco AVPair "vpdn:gw-password=cisco"
Jan  7 19:29:44.127: RADIUS: cisco AVPair "vpdn:nas-password=cisco"
Jan  7 19:29:44.127: RADIUS: cisco AVPair "vpdn:tunnel-id=ISP_NAS"
Jan  7 19:29:44.127: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.66.25"
Jan  7 19:29:44.127: AAA/AUTHOR (338468652): Post authorization status = PASS_AD
D
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV service=ppp
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV gw-password=cisco
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV nas-password=cisco
```

```
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV tunnel-id=ISP_NAS
Jan  7 19:29:44.127: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.66.25
Jan  7 19:29:44.127: As11 VPDN: Get tunnel info for hgw.com with NAS ISP_NAS, IP
 172.22.66.25
Jan  7 19:29:44.127: AAA/AUTHEN: free_user (0x6118F250) user='hgw.com' ruser=''
port='Async11' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan  7 19:29:44.127:  L2F: Tunnel state closed
Jan  7 19:29:44.127: As11 VPDN: Forward to address 172.22.66.25
Jan  7 19:29:44.127: As11 VPDN: Forwarding...
Jan  7 19:29:44.127: AAA: parse name=Async11 idb type=10 tty=11
Jan  7 19:29:44.127: AAA: name=Async11 flags=0x11 type=4 shelf=0 slot=0 adapter=
0 port=11 channel=0
Jan  7 19:29:44.127: AAA: parse name=Serial0:0 idb type=12 tty=-1
Jan  7 19:29:44.127: AAA: name=Serial0:0 flags=0x51 type=1 shelf=0 slot=0 adapte
r=0 port=0 channel=0
Jan  7 19:29:44.127: AAA/AUTHEN: create_user (0x612B7E1C) user='jeremy@hgw.com'
ruser='' port='Async11' rem_addr='408/5550945' authen_type=CHAP service=PPP priv
=1
Jan  7 19:29:44.127: As11 VPDN: Bind interface direction=1
Jan  7 19:29:44.127:  L2F: MID  state closed
Jan  7 19:29:44.127: L2F: Open UDP socket to 172.22.66.25
Jan  7 19:29:44.131:  L2F: Tunnel state opening
Jan  7 19:29:44.131: As11 L2F: MID jeremy@hgw.com state waiting_for_tunnel
Jan  7 19:29:44.131: As11 VPDN: jeremy@hgw.com is forwarded
Jan  7 19:29:44.135: L2F: L2F_CONF received
Jan  7 19:29:44.135: L2F: Removing resend packet (L2F_CONF)
Jan  7 19:29:44.135: ENT_HGW L2F: Tunnel state open
Jan  7 19:29:44.135: L2F: L2F_OPEN received
Jan  7 19:29:44.139: L2F: Removing resend packet (L2F_OPEN)
Jan  7 19:29:44.139: L2F: Building nas2gw_mid0
Jan  7 19:29:44.139: L2F: L2F_CLIENT_INFO: CLID/DNIS 408/5550945
Jan  7 19:29:44.139: L2F: L2F_CLIENT_INFO: NAS-Port Async11
Jan  7 19:29:44.139: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
Jan  7 19:29:44.139: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/28800/50000
Jan  7 19:29:44.139: As11 L2F: MID jeremy@hgw.com state opening
Jan  7 19:29:44.139: RADIUS: ustruct sharecount=3
Jan  7 19:29:44.139: RADIUS: Initial Transmit Async11 id 53 172.22.66.18:1646, A
ccounting-Request, len 108
Jan  7 19:29:44.139:         Attribute 4 6 AC164217
Jan  7 19:29:44.139:         Attribute 5 6 0000000B
Jan  7 19:29:44.139:         Attribute 61 6 00000000
Jan  7 19:29:44.139:         Attribute 1 16 6A657265
Jan  7 19:29:44.139:         Attribute 30 9 35373130
Jan  7 19:29:44.139:         Attribute 31 5 34303828
Jan  7 19:29:44.139:         Attribute 40 6 00000001
Jan  7 19:29:44.139:         Attribute 45 6 00000002
Jan  7 19:29:44.139:         Attribute 6 6 00000002
Jan  7 19:29:44.139:         Attribute 44 10 30303030
Jan  7 19:29:44.139:         Attribute 7 6 00000001
Jan  7 19:29:44.139:         Attribute 41 6 00000000
Jan  7 19:29:44.227: L2F: L2F_OPEN received
Jan  7 19:29:44.227: L2F: Got a MID management packet
Jan  7 19:29:44.227: L2F: Removing resend packet (L2F_OPEN)
Jan  7 19:29:44.227: As11 L2F: MID jeremy@hgw.com state open
Jan  7 19:29:44.227: As11 L2F: MID synced NAS/HG Clid=64/34 Mid=1
Jan  7 19:29:44.227: As11 PPP: Phase is FORWARDED
Jan  7 19:29:44.795: RADIUS: Received from id 53 172.22.66.18:1646, Accounting-r
esponse, len 20
Jan  7 19:29:45.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async11, ch
anged state to up
```

Table 11 describes the debug output events in more detail.

Table 11 Time Stamps and Descriptions of Access VPN Events on the NAS

Time Stamp	Description
19:29:44:007 to 19:29:44:115	LCP negotiation is finished. The NAS sends a CHAP challenge to the client. The client sends a CHAP response with the username jeremy@hgw.com.
19:29:44:119	The NAS is searching for tunnel information.
19:29:44:119	The AAA subsystem inside the Cisco IOS software displays the call-path information. The current call uses TTY line 11, asynchronous interface 11, and serial B-channel 0:0.
19:29:44:119	The local authorization module is accessed. The running configuration wants authorization for PPP and VPN services, and a AAA list called default. The default authorization method is RADIUS.
19:29:44:119	The RADIUS module inside the Cisco IOS software transmits authentication and authorization attributes to the remote RADIUS server. The server is located at IP address 172.22.66.18. RADIUS authentication on UNIX platforms listens to port 1645. All authentication packets go out this port. The NAS requests RADIUS attributes to be negotiated by the AAA server.
19:29:44:123	The remote RADIUS server performs its authentication and authorization for hgw.com. The NAS receives vendor specific AV pairs from the AAA server.
19:29:44:127	The RADIUS module transfers the attribute information to the local AAA subsystem. The post authorization status is equal to pass. The domain name hgw.com has been authenticated (see the free_user field).
19:29:44:127	The NAS attempts to forward the L2F tunnel to the home gateway at IP address 172.22.66.25. The home gateway authenticates the tunnel. A UDP socket is opened from the NAS to 172.22.66.25. The first IP connection is made between the NAS and the home gateway.
19:29:44:139	An accounting packet is sent to the AAA RADIUS server at IP address 172.22.66.18. RADIUS accounting listens on port 1646 on UNIX platforms. All accounting packets go out this port.
19:29:45:131	The line protocol on asynchronous interface 11 is up, which means the L2F tunnel is established between the NAS and the home gateway.

The following debug output appears on the home gateway's terminal screen.

```
ENT_HGW#
Jan  7 19:29:44.132: L2F: L2F_CONF received
Jan  7 19:29:44.132: L2F: Creating new tunnel for ISP_NAS
Jan  7 19:29:44.132:  L2F: Tunnel state closed
Jan  7 19:29:44.132: L2F: Got a tunnel named ISP_NAS, responding
Jan  7 19:29:44.132: AAA: parse name=<no string> idb type=-1 tty=-1
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: free_user (0x612D550C) user='ENT_HGW' ruser=''
port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.132: AAA: parse name=<no string> idb type=-1 tty=-1
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 19:29:44.132: AAA/AUTHEN: free_user (0x612D550C) user='ISP_NAS' ruser=''
port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.132: L2F: Open UDP socket to 172.22.66.23
Jan  7 19:29:44.132: ISP_NAS L2F: Tunnel state opening
Jan  7 19:29:44.136: L2F: L2F_OPEN received
Jan  7 19:29:44.136: L2F: Removing resend packet (L2F_CONF)
Jan  7 19:29:44.136: AAA: parse name=<no string> idb type=-1 tty=-1
Jan  7 19:29:44.136: AAA/AUTHEN: create_user (0x612D550C) user='ISP_NAS' ruser='
' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.136: AAA/AUTHEN/START (1465065509): port='' list='default' actio
n=LOGIN service=PPP
Jan  7 19:29:44.136: AAA/AUTHEN/START (1465065509): found list default
Jan  7 19:29:44.136: AAA/AUTHEN/START (1465065509): Method=LOCAL
Jan  7 19:29:44.136: AAA/AUTHEN (1465065509): status = PASS
Jan  7 19:29:44.136: VPDN: Chap authentication succeeded for ISP_NAS
Jan  7 19:29:44.136: AAA/AUTHEN: free_user (0x612D550C) user='ISP_NAS' ruser=''
port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan  7 19:29:44.136: ISP_NAS L2F: Tunnel state open
Jan  7 19:29:44.140: L2F: L2F_OPEN received
Jan  7 19:29:44.140: L2F: L2F_CLIENT_INFO: CLID/DNIS 408/5550945
Jan  7 19:29:44.140: L2F: L2F_CLIENT_INFO: NAS-Port Async11
Jan  7 19:29:44.140: L2F: L2F_CLIENT_INFO: Client-Bandwidth-Kbps 115
Jan  7 19:29:44.140: L2F: L2F_CLIENT_INFO: NAS-Rate L2F/28800/50000
Jan  7 19:29:44.140: L2F: Got a MID management packet
Jan  7 19:29:44.140:  L2F: MID  state closed
Jan  7 19:29:44.140: L2F: Start create mid intf process for jeremy@hgw.com
Jan  7 19:29:44.140: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
Jan  7 19:29:44.140: Vi1 VTEMPLATE: Hardware address 0050.d193.e000
Jan  7 19:29:44.140: Vi1 VPDN: Virtual interface created for jeremy@hgw.com
Jan  7 19:29:44.140: Vi1 VPDN: Set to Async interface
Jan  7 19:29:44.140: Vi1 PPP: Phase is DOWN, Setup
Jan  7 19:29:44.140: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
Jan  7 19:29:44.140: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vte
mplate
Jan  7 19:29:44.140: Vi1 VTEMPLATE: ************ CLONE VACCESS1 ***************
**
Jan  7 19:29:44.144: Vi1 VTEMPLATE: Clone from Virtual-Template1
interface Virtual-Access1
default ip address
no ip address
encap ppp
ip unnumbered fastethernet 0/0
no ip directed-broadcast
ip unnumbered fastethernet 0/0
no ip directed-broadcast
ppp authentication chap
peer default ip address pool default
encapsulation ppp
ppp multilink
end

6w5d: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan  7 19:29:44.224: Vi1 PPP: Treating connection as a dedicated line
Jan  7 19:29:44.224: Vi1 PPP: Phase is ESTABLISHING, Active Open
Jan  7 19:29:44.224: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
Jan  7 19:29:44.224: Vi1 LCP: O CONFREQ [Closed] id 1 len 39
Jan  7 19:29:44.224: Vi1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:44.224: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:44.224: Vi1 LCP:    MagicNumber 0x47ADAD67 (0x050647ADAD67)
Jan  7 19:29:44.224: Vi1 LCP:    PFC (0x0702)
Jan  7 19:29:44.224: Vi1 LCP:    ACFC (0x0802)
Jan  7 19:29:44.224: Vi1 LCP:    MRRU 1524 (0x110405F4)
Jan  7 19:29:44.224: Vi1 LCP:    EndpointDisc 1 Local (0x130A01454E545F484757)
Jan  7 19:29:44.224: Vi1 VPDN: Bind interface direction=2
```

```
Jan  7 19:29:44.224: Vi1 PPP: Treating connection as a dedicated line
Jan  7 19:29:44.224: Vi1 LCP: I FORCED CONFREQ len 21
Jan  7 19:29:44.224: Vi1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Jan  7 19:29:44.224: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
Jan  7 19:29:44.224: Vi1 LCP:    MagicNumber 0x33911E0F (0x050633911E0F)
Jan  7 19:29:44.224: Vi1 LCP:    PFC (0x0702)
Jan  7 19:29:44.224: Vi1 LCP:    ACFC (0x0802)
Jan  7 19:29:44.224: Vi1 VPDN: PPP LCP accepted rcv CONFACK
Jan  7 19:29:44.224: Vi1 VPDN: PPP LCP accepted sent CONFACK
Jan  7 19:29:44.224: Vi1 PPP: Phase is AUTHENTICATING, by this end
Jan  7 19:29:44.224: Vi1 CHAP: O CHALLENGE id 3 len 28 from "ENT_HGW"
Jan  7 19:29:44.224: Vi1 L2F: Transfer NAS-Rate L2F/28800/50000 to LCP
Jan  7 19:29:44.228: Vi1 CHAP: I RESPONSE id 2 len 35 from "jeremy@hgw.com"
Jan  7 19:29:44.228: Vi1 L2F: Finish create mid intf for jeremy@hgw.com
Jan  7 19:29:44.228: Vi1 L2F: MID jeremy@hgw.com state open
Jan  7 19:29:44.228: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
Jan  7 19:29:44.228: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=1 channel=0
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 19:29:44.228: RADIUS: ustruct sharecount=1
Jan  7 19:29:44.228: RADIUS: Initial Transmit Virtual-Access1 id 119 172.22.66.1
3:1645, Access-Request, len 99
Jan  7 19:29:44.228:         Attribute 4 6 AC164219
Jan  7 19:29:44.228:         Attribute 5 6 00000001
Jan  7 19:29:44.228:         Attribute 61 6 00000005
Jan  7 19:29:44.228:         Attribute 1 16 6A657265
Jan  7 19:29:44.228:         Attribute 30 9 35373130
Jan  7 19:29:44.228:         Attribute 31 5 34303803
Jan  7 19:29:44.228:         Attribute 3 19 02A4F6DD
Jan  7 19:29:44.228:         Attribute 6 6 00000002
Jan  7 19:29:44.228:         Attribute 7 6 00000001
Jan  7 19:29:44.692: RADIUS: Received from id 119 172.22.66.13:1645, Access-Acce
pt, len 38
Jan  7 19:29:44.692:         Attribute 6 6 00000002
Jan  7 19:29:44.692:         Attribute 7 6 00000001
Jan  7 19:29:44.692:         Attribute 8 6 FFFFFFFE
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' lis
t='' 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_R
EPL
Jan  7 19:29:44.692: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
Jan  7 19:29:44.692: Vi1 CHAP: O SUCCESS id 2 len 4
Jan  7 19:29:44.692: Vi1 PPP: Phase is UP
Jan  7 19:29:44.696: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
Jan  7 19:29:44.696: AAA/AUTHOR/FSM Vi1 (2925705703): Port='Virtual-Access1' lis
t='' service=NET
Jan  7 19:29:44.696: AAA/AUTHOR/FSM: Vi1 (2925705703) user='jeremy@hgw.com'
Jan  7 19:29:44.696: AAA/AUTHOR/FSM: Vi1 (2925705703) send AV service=ppp
Jan  7 19:29:44.696: AAA/AUTHOR/FSM: Vi1 (2925705703) send AV protocol=ip
Jan  7 19:29:44.696: AAA/AUTHOR/FSM (2925705703) found list "default"
```

```
Jan  7 19:29:44.696: AAA/AUTHOR/FSM: Vi1 (2925705703) Method=RADIUS
Jan  7 19:29:44.696: RADIUS: Using NAS default peer
Jan  7 19:29:44.696: RADIUS: Authorize IP address 0.0.0.0
Jan  7 19:29:44.696: AAA/AUTHOR (2925705703): Post authorization status = PASS_R
EPL
Jan  7 19:29:44.696: Vi1 AAA/AUTHOR/FSM: We can start IPCP
Jan  7 19:29:44.696: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
Jan  7 19:29:44.696: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
Jan  7 19:29:44.696: RADIUS: ustruct sharecount=2
Jan  7 19:29:44.696: RADIUS: Initial Transmit Virtual-Access1 id 120 172.22.66.1
3:1646, Accounting-Request, len 108
Jan  7 19:29:44.696:         Attribute 4 6 AC164219
Jan  7 19:29:44.696:         Attribute 5 6 00000001
Jan  7 19:29:44.696:         Attribute 61 6 00000005
Jan  7 19:29:44.696:         Attribute 1 16 6A657265
Jan  7 19:29:44.696:         Attribute 30 9 35373130
Jan  7 19:29:44.696:         Attribute 31 5 34303828
Jan  7 19:29:44.696:         Attribute 40 6 00000001
Jan  7 19:29:44.696:         Attribute 45 6 00000001
Jan  7 19:29:44.696:         Attribute 6 6 00000002
Jan  7 19:29:44.700:         Attribute 44 10 30303030
Jan  7 19:29:44.700:         Attribute 7 6 00000001
Jan  7 19:29:44.700:         Attribute 41 6 00000000
Jan  7 19:29:44.740: RADIUS: Received from id 120 172.22.66.13:1646, Accounting-
response, len 20
Jan  7 19:29:44.804: Vi1 IPCP: I CONFREQ [REQsent] id 1 len 40
Jan  7 19:29:44.804: Vi1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x020
6002D0F01)
Jan  7 19:29:44.804: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
Jan  7 19:29:44.804: Vi1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Jan  7 19:29:44.804: Vi1 IPCP:    PrimaryWINS 171.68.235.228 (0x8206AB44EBE4)
Jan  7 19:29:44.804: Vi1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Jan  7 19:29:44.808: Vi1 IPCP:    SecondaryWINS 171.68.235.229 (0x8406AB44EBE5)
Jan  7 19:29:44.808: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we want 0
.0.0.0
Jan  7 19:29:44.808: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
Jan  7 19:29:44.808: Vi1 AAA/AUTHOR/IPCP: Processing AV addr=0.0.0.0
Jan  7 19:29:44.808: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
Jan  7 19:29:44.808: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we want 0.
0.0.0
Jan  7 19:29:44.808: Vi1 IPCP: Using pool 'default'
Jan  7 19:29:44.808: ip_get_pool: Vi1: using pool default
Jan  7 19:29:44.808: ip_get_pool: Vi1: returning address = 172.30.2.1
Jan  7 19:29:44.808: Vi1 IPCP: Pool returned 172.30.2.1
Jan  7 19:29:44.808: Vi1 IPCP: O CONFREJ [REQsent] id 1 len 10
Jan  7 19:29:44.808: Vi1 IPCP:    CompressType VJ 15 slots CompressSlotID (0x020
6002D0F01)
Jan  7 19:29:44.808: Vi1 CCP: I CONFREQ [Not negotiated] id 1 len 15
Jan  7 19:29:44.808: Vi1 CCP:    MS-PPC supported bits 0x00000001 (0x12060000000
1)
Jan  7 19:29:44.808: Vi1 CCP:    Stacker history 1 check mode EXTENDED (0x110500
0104)
Jan  7 19:29:44.808: Vi1 LCP: O PROTREJ [Open] id 2 len 21 protocol CCP
Jan  7 19:29:44.808: Vi1 LCP:  (0x80FD0101000F12060000000111050001)
Jan  7 19:29:44.808: Vi1 LCP:  (0x04)
Jan  7 19:29:44.808: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
Jan  7 19:29:44.808: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
6w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed s
tate to up
Jan  7 19:29:46.224: Vi1 LCP: TIMEout: State Open
Jan  7 19:29:46.696: Vi1 IPCP: TIMEout: State ACKrcvd
Jan  7 19:29:46.696: Vi1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
Jan  7 19:29:46.696: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
Jan  7 19:29:46.784: Vi1 IPCP: I CONFACK [REQsent] id 2 len 10
Jan  7 19:29:46.784: Vi1 IPCP:    Address 172.22.66.25 (0x0306AC164219)
```

```
Jan  7 19:29:47.792: Vi1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
Jan  7 19:29:47.792: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
Jan  7 19:29:47.792: Vi1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Jan  7 19:29:47.792: Vi1 IPCP:    PrimaryWINS 171.68.235.228 (0x8206AB44EBE4)
Jan  7 19:29:47.792: Vi1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Jan  7 19:29:47.792: Vi1 IPCP:    SecondaryWINS 171.68.235.229 (0x8406AB44EBE5)
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we want 1
72.30.2.1
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Processing AV addr=0.0.0.0
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
Jan  7 19:29:47.792: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we want 17
2.30.2.1
Jan  7 19:29:47.792: Vi1 IPCP: O CONFNAK [ACKrcvd] id 2 len 34
Jan  7 19:29:47.792: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
Jan  7 19:29:47.792: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
Jan  7 19:29:47.792: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
Jan  7 19:29:47.792: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
Jan  7 19:29:47.792: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
Jan  7 19:29:47.952: Vi1 IPCP: I CONFREQ [ACKrcvd] id 3 len 34
Jan  7 19:29:47.952: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
Jan  7 19:29:47.952: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
Jan  7 19:29:47.952: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
Jan  7 19:29:47.952: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
Jan  7 19:29:47.952: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
Jan  7 19:29:47.952: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 172.30.2.1, we wan
t 172.30.2.1
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP Vi1 (1744344778): Port='Virtual-Access1' li
st='' service=NET
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP: Vi1 (1744344778) user='jeremy@hgw.com'
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP: Vi1 (1744344778) send AV service=ppp
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP: Vi1 (1744344778) send AV protocol=ip
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP: Vi1 (1744344778) send AV addr*172.30.2.1
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP (1744344778) found list "default"
Jan  7 19:29:47.952: AAA/AUTHOR/IPCP: Vi1 (1744344778) Method=RADIUS
Jan  7 19:29:47.952: RADIUS: Using NAS default peer
Jan  7 19:29:47.952: RADIUS: Authorize IP address 172.30.2.1
Jan  7 19:29:47.952: AAA/AUTHOR (1744344778): Post authorization status = PASS_R
EPL
Jan  7 19:29:47.952: set_ip_peer_addr: Vi1: address = 172.30.2.1 (4) is redundan
t
Jan  7 19:29:47.952: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
Jan  7 19:29:47.952: Vi1 AAA/AUTHOR/IPCP: Processing AV addr=172.30.2.1
Jan  7 19:29:47.952: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
Jan  7 19:29:47.952: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 172.30.2.1, we want
 172.30.2.1
Jan  7 19:29:47.952: Vi1 IPCP: O CONFACK [ACKrcvd] id 3 len 34
Jan  7 19:29:47.956: Vi1 IPCP:    Address 172.30.2.1 (0x0306AC1E0201)
Jan  7 19:29:47.956: Vi1 IPCP:    PrimaryDNS 172.23.1.10 (0x8106AC17010A)
Jan  7 19:29:47.956: Vi1 IPCP:    PrimaryWINS 172.23.1.11 (0x8206AC17010B)
Jan  7 19:29:47.956: Vi1 IPCP:    SecondaryDNS 172.23.2.10 (0x8306AC17020A)
Jan  7 19:29:47.956: Vi1 IPCP:    SecondaryWINS 172.23.2.11 (0x8406AC17020B)
Jan  7 19:29:47.956: Vi1 IPCP: State is Open
Jan  7 19:29:47.956: Vi1 IPCP: Install route to 172.30.2.1
ENT_HGW#
```

Table 12 describes the debug output events in more detail.

Table 12 Time Stamps and Descriptions of Access VPN Events on the Home Gateway

Time Stamp	Description
19:27:36.066 to 19:27:36.074	The home gateway receives a request from the NAS to open an L2F tunnel. The home gateway authenticates the tunnel and opens it.
19:27:36.070	The home gateway receives a SENDAUTH packet from the NAS, which wants to authenticate the home gateway.
19:27:36.074	The NAS authenticates the home gateway and sends an L2F_OPEN packet to open the tunnel.
19:27:36.074	The home gateway authenticates the tunnel by using local AAA.
19:27:36.074 to 19:27:36.078	The L2F tunnel is opened.
19.27.36.078	The NAS forwards the client information to the home gateway.
19:27:36.078 to 19:27:36.082	A virtual-access interface is cloned from virtual template 1, which is not a physical interface, but is treated like a regular interface that uses the IP address of the Fast Ethernet 0/0 interface. The debug output following “interface Virtual-Access1” lists every command that has been configured for virtual template 1. Enter the **clear vtemplate** command to reset the command history.
19:27:36.162	The NAS forces the information from the LCP negotiation with the client onto the virtual-access interface.
19:27:36.162	The home gateway sends a CHAP challenge to the client, who responds and is authenticated by the home gateway.
19:27:36.282	The home gateway assigns the client the IP address 172.30.2.1 from the default pool.
19:27:36.294	The line protocol on interface Virtual-Access1 changes to the up state.
19:27:39.282	The client requests IP addresses of DNS and WINS servers.
19:27:39.414	The home gateway receives a positive acknowledgment from the client confirming the IP addresses of the DNS and WNIS servers.
19:27:39.414	The home gateway installs the route to the client’s IP address, 172.30.2.1.

Glossary

attribute-value pair (AV pair)—A generic pair of values passed from a AAA server to a AAA client. For example, in the AV pair user = bill, “user” is the attribute and “bill” is the value.

calling line identification (CLID)—A unique number that informs the called party of the phone number of the calling party.

challenge handshake authentication protocol (CHAP)—A PPP cryptographic challenge/response authentication protocol in which the cleartext password is not passed over the line. CHAP allows the secure exchange of a shared secret between the two endpoints of a connection.

client—The hardware and software that the user uses to establish the PPP session. Because all clients discussed in these case studies are remote clients, the term “client” refers to any “remote client.”

cloning—Creating and configuring a virtual access interface by applying a specific virtual template interface. The template is the source of the generic user and router-dependent information. The result of cloning is a virtual access interface configured with all the commands in the template.

control messages—Exchange messages between the NAS and home gateway pairs, operating in-band within the tunnel protocol. Control messages govern the aspects of the tunnel and sessions within the tunnel.

Dialed Number identification Service (DNIS)—The called party number used by call centers or a central office where different numbers are assigned to a specific service.

home gateway—The device, maintained by the enterprise customer, where a tunnel terminates. A home gateway is analogous to the L2TP network server.

Integrated Services Digital Network (ISDN)—Communication protocols offered by telephone companies that permit telephone networks to carry date, voice, and other source traffic.

Layer 2 Forwarding (L2F)—A Layer 2 tunneling protocol that establishes a secure tunnel across a public infrastructure (such as the Internet) that connects an ISP POP to a enterprise home gateway. This tunnel creates a virtual point-to-point connection between the user and the enterprise customer’s network. L2F is the most established and stable Layer 2 tunneling protocol.

Layer 2 Tunnel Protocol (L2TP)—A Layer 2 tunneling protocol that is an extension of the PPP protocol used for virtual private networks (VPNs). L2TP merges the best features of two existing tunneling protocols: Microsoft’s PPTP and Cisco’s L2F. L2TP is the emerging IETF standard, currently being drafted by participants from Ascend, Cisco Systems, Copper Mountain Networks, IBM, Microsoft, and 3Com.

Link Control Protocol (**LCP)**—A protocol that establishes, configures, and tests data link connections used by the PPP.

L2TP access concentrator (LAC)—In L2TP technology, a device that the client directly connects to and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server (NAS).

L2TP network server (LNS)—In L2TP technology, a termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS may have a single LAN or WAN interface—yet it can terminate calls arriving at any of the LAC's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

Message Digest 5 (MD5)—An algorithm used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Multiplex Identifier (MID)—The number associated with a specific user's L2TP/L2F session.

Multilink PPP Protocol (MLP)—A protocol that splits and recombines packets to a single end system across a logical pipe (also called a bundle) formed by multiple links. Multilink PPP provides bandwidth on demand and reduces transmission latency across WAN links.

Network Access Server (NAS)—A device providing temporary, on-demand network access to users. The access is typically point-to-point using PSTN or ISDN lines. In Cisco's implementation for L2TP, the NAS serves as a LAC for incoming calls and serves as a LNS for outgoing calls. A NAS is analogous to an L2TP access server (LAC).

Network Control protocol (NCP)—A PPP protocol for negotiating OSI Layer 3 (the network layer) parameters.

Password Authentication Protocol (PAP)—A simple PPP authentication mechanism where a cleartext username and password are transmitted to prove identity. PAP is not as secure as CHAP because the password is passed in cleartext.

point-of-presence (POP)—The access point to a service provider's network. The device that the user dials in to.

Point-to-Point Protocol (PPP)—A protocol that encapsulates network layer protocol information over point-to-point links. The RFC for PPP is RFC 1661.

Point-to-Point Tunneling Protocol (PPTP)—A Microsoft proprietary tunneling protocol that was combined with L2F to create L2TP.

public switched telephone network (PSTN)—Telephone networks and services in place worldwide.

remote client—See client.

remote user—See user.

session—A single tunneled PPP call.

tunnel—A virtual pipe between the ISP and home gateway that can carry multiple PPP sessions.

tunnel ID—A two-octet value that denotes a tunnel between an ISP and a home gateway.

user—Instigator of a PPP session. Because all users discussed in these case studies are remote users, the term "user" refers to any "remote user."

virtual access interface—A unique virtual interface that is created dynamically and exists temporarily. Virtual access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks. Virtual access interfaces are cloned from virtual template interfaces. In access VPNs, the home gateway clones a virtual access interface for VPN users.

virtual template—A template that is used to create a logical interface configured with generic configuration information for a specific purpose or common configuration. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed. In access VPNs, the virtual template is configured on the home gateway and used to clone virtual access interfaces for VPN users.

virtual private dialup networking (VPDN)—See virtual private network.

virtual private network (VPN)—A system that permits networks to extend beyond a physical home networks while giving the appearance and functonality of being directly connected to a home network. VPNs use L2TP and L2F to extend the Layer 2 and higher parts of the network connection from the ISP to the home gateway. The specific term “VPDN” is being replaced by the more general term “VPN.”