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.