



CHAPTER 9

Configuring Multihop

In a Virtual Private Dialup Network (VPDN) environment, sessions generated from a remote host are routed over an existing tunnel or a tunnel built to route a specific domain. Typically, sessions cannot traverse more than one L2TP tunnel before reaching the ISP or corporate network. However, by using the Multihop feature, you can configure the Cisco 10000 series router to terminate sessions arriving in L2TP tunnels from a LAC and then route the remote traffic through new L2TP tunnels to an LNS device in the ISP or corporate network.

The Multihop feature enables the Cisco 10000 series router to terminate sessions arriving in L2TP tunnels from a LAC and to forward the sessions through new L2TP tunnels to the router's peer L2TP Network Server (LNS). The packets arrive at the router with L2TP encapsulation and the router forwards the packets with a different L2TP encapsulation. The Cisco 10000 router maps the sessions to the new tunnels based on the session's domain or the tunnel in which the session arrived.

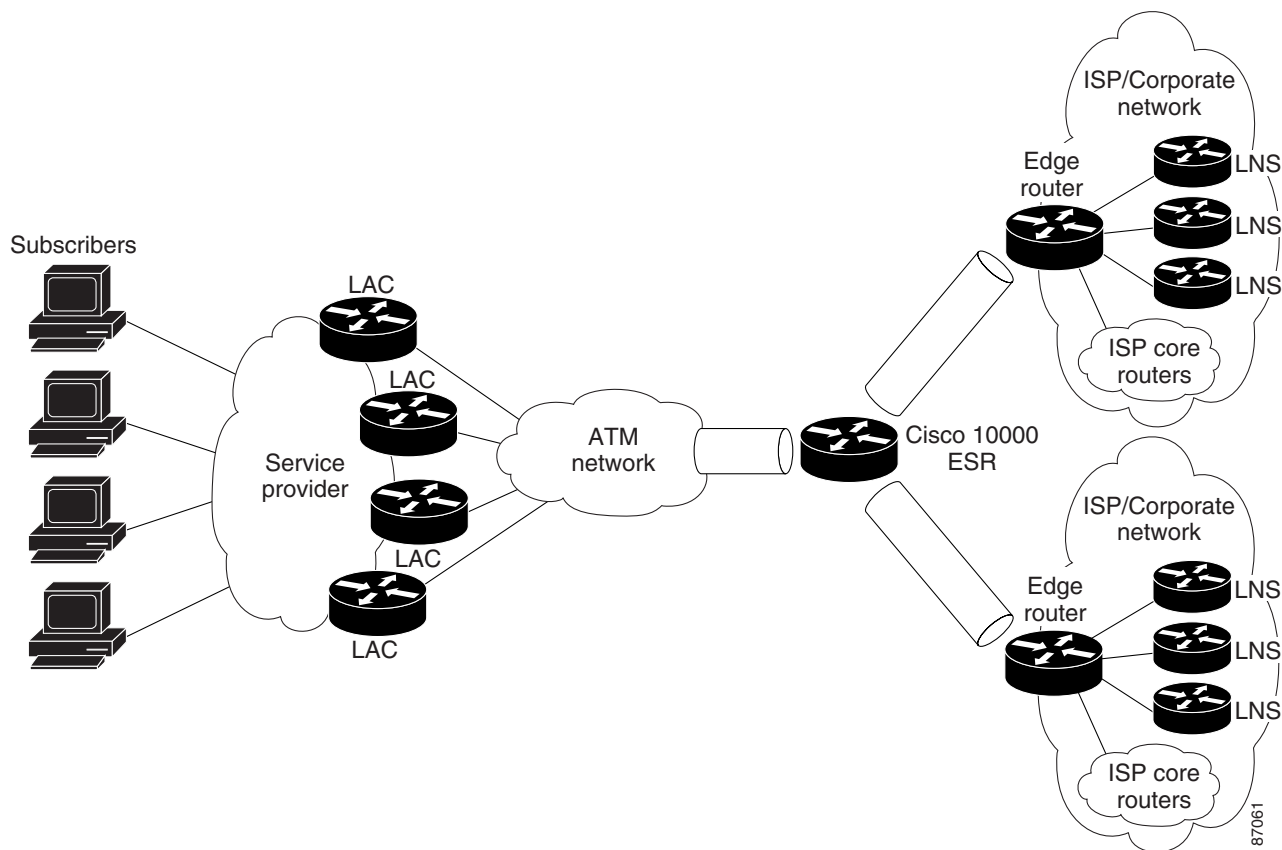
The Cisco 10000 router also supports the preservation of the IP type of service (TOS) field for tunneled IP packets. Each L2TP data packet and IP packet has a TOS field. When the router creates an L2TP data packet, the TOS field sets to zero (normal service), ignoring the TOS field of the encapsulated IP packet being tunneled. To preserve quality of service for tunneled packets, the Cisco 10000 router supports the configuration of accept-dialin and request-dialout VPDN groups using the **l2tp ip tos reflect** command. When the router creates an L2TP data packet at a virtual-access interface (VAI), instead of ignoring the IP packet TOS field, the router copies the field onto the L2TP data packet.



Note

Typically, the Cisco IOS software reflects the TOS field from the inner packet header to the outer packet header. However, the Cisco 10000 router propagates the TOS field from the ingress header to the egress header.

[Figure 9-1](#) shows an example of a multihop topology. On the access network side, the Cisco 10000 router connects to access provider LACs. On the provider network side, the router connects to LNS devices in other ISP or corporate provider networks. Multiple L2TP tunnels are carried over either multiple interfaces or a single interface. Typically, the connection between the router and the LAC or the router and the LNS is an ATM connection. However, this is not a requirement. You can use any interface that can carry L2TP tunneled traffic.

Figure 9-1 Multihop Topology Example

This chapter describes the Multihop feature in the following topics:

- [Feature History for Multihop](#), page 9-2
- [Restrictions for Multihop](#), page 9-3
- [Required Configuration Tasks for Multihop](#), page 9-3
- [Optional Configuration Tasks for Multihop](#), page 9-5
- [Configuration Examples for Multihop](#), page 9-8
- [Monitoring and Maintaining Multihop Configurations](#), page 9-9

Feature History for Multihop

Cisco IOS Release	Description	Required PRE
12.2(15)BX	This feature was introduced on the Cisco 10000 series router.	PRE2
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for Multihop

The Multihop feature has the following restrictions:

- The performance routing engine, part number ESR-PRE1 does not support the Multihop feature.
- Tunnel switching is based on a session's domain or tunnel in which the session arrived. The Cisco 10000 router does not support switching of individual sessions by using the CLI.
- The Cisco 10000 router does not support multichassis Multilink PPP (MLPPP).
- The Cisco 10000 router supports the Multihop feature for L2TP, but does not support the L2F protocol.
- You cannot apply per session features to switched sessions. For example, you cannot apply an ACL or a service policy to the sessions.

To preserve the IP TOS field of tunneled IP packets, the following restrictions apply:

- The Cisco 10000 router supports only the L2TP tunneling protocol.
- The tunneled link must carry IP to preserve the TOS field.
- The Cisco 10000 router does not support proxy PPP dialin.

Required Configuration Tasks for Multihop

To configure the Multihop feature on the Cisco 10000 router, perform the following configuration tasks:

- [Enabling VPDN and Multihop Functionality, page 9-3](#)
- [Terminating the Tunnel from the LAC, page 9-4](#)
- [Mapping the Ingress Tunnel Name to an LNS, page 9-4](#)

Enabling VPDN and Multihop Functionality

To enable VPDN and multihop functionality, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vpdn enable	Enables VPDN functionality.
Step 2	Router(config)# vpdn multihop	Enables VPDN multihop functionality.

Terminating the Tunnel from the LAC

To terminate the tunnel from the LAC, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# username <i>remote-hostname</i> password <i>secret</i>	Configures the secret (password) for the remote LAC. The <i>secret</i> must match the <i>secret</i> configured on the LAC and can consist of any string of up to 11 ASCII characters.
Step 2	Router(config)# username <i>local-name</i> password <i>secret</i>	Configures the secret (password) for the local device. The <i>secret</i> must match the <i>secret</i> configured in step 1.
Step 3	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group.
Step 4	Router(config-vpdn)# accept-dialin	Accepts tunneled PPP connections from the LAC and creates an accept-dialin virtual private dialup network (VPDN) subgroup.
Step 5	Router(config-vpdn-acc-in)# protocol <i>l2tp</i>	Specifies the Layer 2 Tunnel Protocol (L2TP) that the VPDN subgroup will use.
Step 6	Router(config-vpdn-acc-in)# virtual-template <i>number</i>	Specifies the virtual template interface to use to clone the new virtual access interface.
Step 7	Router(config-vpdn-acc-in)# exit	Returns to VPDN group mode.
Step 8	Router(config-vpdn)# terminate-from <i>hostname</i> <i>remote-hostname</i>	Specifies the host name of the remote LAC that is required when accepting a VPDN tunnel. The <i>remote-hostname</i> must match the <i>remote-hostname</i> configured in Step 1.
Step 9	Router(config-vpdn)# local name <i>local-name</i>	Specifies the local host name that the tunnel will use to identify itself. The <i>local-name</i> must match the <i>local-name</i> configured in Step 2.

Mapping the Ingress Tunnel Name to an LNS

To map the ingress tunnel name to an LNS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# username <i>username</i> password <i>secret</i>	Configures the secret (password) for the LNS. The <i>username</i> must match the LNS hostname or tunnel ID. The <i>secret</i> must match the <i>secret</i> configured on the LNS.
Step 2	Router(config)# username <i>egress-tunnel-name</i> password <i>secret</i>	Configures the secret (password) for the tunnel. The <i>egress-tunnel-name</i> specifies the remote (LNS) host name of the tunnel. The <i>secret</i> must match the <i>secret</i> configured in Step 1.
Step 3	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group and enters VPDN configuration mode.
Step 4	Router(config-vpdn)# request-dialin	Enables the Cisco 10000 router to request L2TP tunnels to the LNS and enters VPDN request-dialin subgroup mode.
Step 5	Router(config-vpdn-req-in)# protocol <i>l2tp</i>	Specifies the Layer 2 Tunnel Protocol (L2TP) that the VPDN subgroup will use.

	Command	Purpose
Step 6	Router(config-vpdn-req-in)# multihop hostname <i>ingress-tunnel-name</i>	Initiates a tunnel based on the LAC's hostname or ingress tunnel ID.
Step 7	Router(config-vpdn-req-in)# exit	Returns to VPDN group mode.
Step 8	Router(config-vpdn)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	Specifies the IP address of the LNS that will be tunneled to. Optionally, you can configure the maximum number of connections that can be made to the IP address and the priority for the IP address (1 is the highest).
Step 9	Router(config-vpdn)# local name <i>egress-tunnel-name</i>	Specifies the local host name that the tunnel uses to identify itself. The <i>egress-tunnel-name</i> must match the <i>egress-tunnel-name</i> configured in Step 2.

Optional Configuration Tasks for Multihop

To configure the Multihop feature on the Cisco 10000 router, perform any of the following optional tasks:

- [Specifying VPDN Tunnel Authorization Searches by Ingress Tunnel Name, page 9-5](#)
- [Preserving the Type of Service Field of Encapsulated IP Packets, page 9-5](#)

Specifying VPDN Tunnel Authorization Searches by Ingress Tunnel Name

To specify that the provider's network access server is to perform VPDN tunnel authorization searches by using the ingress tunnel name, enter the following command in global configuration mode:

Command	Purpose
Router (config)# vpdn search-order multihop-hostname [<i>domain</i>]	Specifies a search by the configured ingress tunnel name. Optionally, you can specify to search by domain name only.

Preserving the Type of Service Field of Encapsulated IP Packets

To preserve the type of service (TOS) field of encapsulated IP packets, perform the following configuration tasks:

- [Configuring an Accept-Dialin VPDN Group to Preserve IP TOS, page 9-6](#)
- [Configuring a Request-Dialout VPDN Group to Preserve IP TOS, page 9-7](#)

Configuring an Accept-Dialin VPDN Group to Preserve IP TOS

To configure an accept-dialin VPDN group to preserve IP TOS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group and enters VPDN configuration mode.
Step 2	Router(config-vpdn)# accept-dialin	Accepts tunneled PPP connections from the LAC and creates an accept-dialin virtual private dialup network (VPDN) subgroup.
Step 3	Router(config-acc-in)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol (L2TP) that the VPDN subgroup will use. Note L2TP is the only protocol that supports dialout and IP TOS preservation.
Step 4	Router(config-vpdn-acc-in)# virtual-template <i>number</i>	Specifies the virtual template interface to use to clone the new virtual access interface.
Step 5	Router(config-vpdn-acc-in)# exit	Returns to VPDN group mode.
Step 6	Router(config-vpdn)# terminate-from <i>hostname</i> <i>remote-hostname</i>	Specifies the host name of the remote LAC that will be required when accepting a VPDN tunnel.
Step 7	Router(config-vpdn)# local name <i>local-name</i>	Specifies the local host name that the tunnel will use to identify itself.
Step 8	Router(config-vpdn)# ip tos reflect	Configures the VPDN group to preserve the TOS field of L2TP tunneled IP packets.

[Example 9-1](#) configures *vpdn-group 1* to accept tunneled PPP connections from the remote LAC named *myhost* and to preserve the TOS field of L2TP tunneled IP packets.

Example 9-1 Configuring an Accept-Dialin VPDN Group for IP TOS Preservation

```
vpdn-group 1
  accept-dialin
    protocol l2tp
    virtual-template 1
  terminate-from hostname myhost
  local name local-host1
  ip tos reflect
```

Configuring a Request-Dialout VPDN Group to Preserve IP TOS

To configure a request-dialout VPDN group to preserve IP TOS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group and enters VPDN configuration mode.
Step 2	Router(config-vpdn)# request-dialout	Enables the LNS to request L2TP tunnels for dialout calls.
Step 3	Router(config-vpdn-req-out)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol (L2TP) that the VPDN subgroup will use. Note L2TP is the only protocol that supports dialout and IP TOS preservation.
Step 4	Router(config-vpdn-req-out)# pool-member <i>pool-number</i> OR Router(config-vpdn-req-out)# rotary-group <i>group-number</i>	Specifies the dialer profile pool or dialer rotary group to use to dial out. Note You can only configure one dialer profile pool or one dialer rotary group. Attempting to configure a second dialer resource removes the first resource from the configuration.
Step 5	Router(config-vpdn-req-out)# exit	Returns to VPDN group mode.
Step 6	Router(config-vpdn)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	Specifies the IP address of the LNS that is dialed out. Optionally, you can configure the maximum number of connections that can be made to the IP address and the priority for the IP address (1 is the highest).
Step 7	Router(config-vpdn)# local name <i>local-name</i>	Specifies the local host name that the tunnel uses to identify itself.
Step 8	Router(config-vpdn)# ip tos reflect	Configures the VPDN group to preserve the TOS field of L2TP tunneled IP packets.

[Example 9-2](#) configures *vpdn-group 1* for L2TP dialout tunnel preservation of the IP TOS.

Example 9-2 Configuring a Request-Dialout VPDN Group for IP TOS Preservation

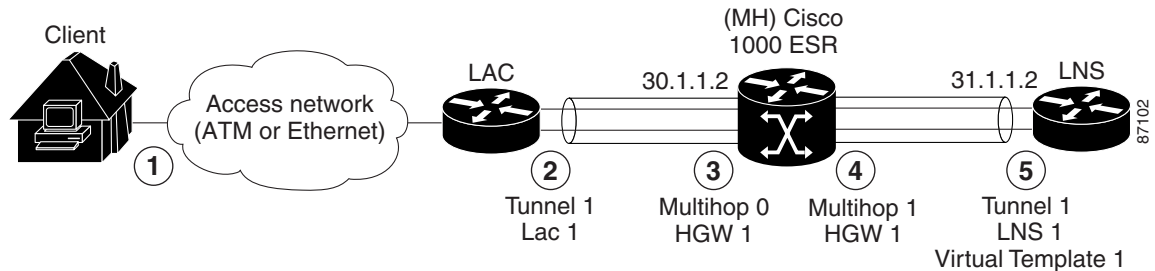
```
vpdn-group 1
  request-dialout
    protocol l2tp
    pool-member 1
  initiate-to ip 10.16.49.94
  ip tos reflect
```

Configuration Examples for Multihop

The example in this section is a multihop configuration in which the Cisco 10000 router is configured as the multihop system (MH). The example includes LAC and LNS configurations to complete the configuration. This configuration scenario supports a maximum of two hops between the LAC device and the destination LNS device.

Figure 9-2 shows the example multihop configuration, described in more detail in the list that follows.

Figure 9-2 Multihop Configuration Example



The remote client dials in to the LAC. The LAC negotiates link control protocol (LCP) and preauthenticates the user.

5. The LAC configuration sets up a vpdn-group named *tunnel1*. This vpdn-group initiates a tunnel to IP address 30.1.1.2 to request dialin connection for any packets associated with the *cisco.com* domain. The local name of tunnel1 is *LAC1*. This is the name by which tunnel1 identifies itself to the receiving end of the L2TP tunnel.
6. The Cisco 10000 router acts as the multihop system (MH). On the LAC side, the MH configuration requires users to log in to the system. The MH configuration creates a vpdn-group named *multihop0*, which identifies the L2TP tunnel terminating from the LAC. The multihop0 tunnel only accepts dialin connections from the LAC and identifies itself by using the local name *Home Gateway 1* (*HGW1*).
7. On the LNS side, the MH configuration creates a vpdn-group named *multihop1*, which initiates an L2TP tunnel to the LNS at IP address 31.1.1.2. The multihop1 vpdn-group requests dialin connections to the LNS based on the LAC's hostname. Using the **multihop hostname LAC1** command creates the association between the LAC and the LNS devices. Like multihop0, multihop1 shares the same HGW1 local name.
8. The LNS configuration sets up a vpdn-group named *tunnel1*, which accepts dialin connections from the MH system. The tunnel1 vpdn-group terminates the L2TP tunnel from the MH system (identified by the HGW1 local name) and uses the local name *LNS1* to identify itself. The LNS configuration creates a virtual template interface named *Virtual-Template1*, which it associates with tunnel1. *Virtual-Template1* uses PAP authentication and assigns the IP address by using the local IP address pool named *pool-1*.

LAC Configuration

```
!
vpdn enable
!
vpdn-group tunnel1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 30.1.1.2 priority 1
```

```

local name LAC1
l2tp tunnel password 7 060A0E23
l2tp tunnel receive-window 100
l2tp tunnel retransmit timeout min 2
!

```

Multihop Configuration

```

username user@cisco.com password 0 lab
!
vpdn enable
vpdn multihop
vpdn search-order multihop-hostname domain dnis
!
vpdn-group multihop0
accept-dialin
protocol l2tp
terminate-from hostname LAC1
local name HGW1
l2tp tunnel password 7 09404F0B
!
vpdn-group multihop1
request-dialin
protocol l2tp
multihop hostname LAC1
initiate-to ip 31.1.1.2 priority 1
local name HGW1
l2tp tunnel password 7 0507070D
!

```

LNS Configuration

```

vpdn enable
!
vpdn-group tunnel1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname HGW1
local name LNS1
l2tp tunnel password 7 04570A04
l2tp tunnel receive-window 100
l2tp tunnel retransmit timeout min 2
!
interface Virtual-Template1
ip unnumbered GigabitEthernet2/0/0
no keepalive
peer default ip address pool pool-1
ppp mtu adaptive
ppp authentication pap callin
!
ip local pool pool-1 4.2.0.0 4.2.255.255

```

Monitoring and Maintaining Multihop Configurations

To monitor and maintain multihop configurations and VPDN groups, enter the following commands in privileged EXEC mode:

Command	Purpose
Router# show running-config	Displays the current router configuration. Use the output of this command to ensure that the configuration: • Enables VPDN and multihop functionality • Terminates tunnels from the LAC • Maps the ingress tunnel name to the LNS • Performs VPDN tunnel authorization searches by ingress tunnel name • (Optional) Configures an accept-dialin and request-dialout VPDN group to preserve the TOS field of L2TP tunneled IP packets
Router# show vpdn	Displays information about active L2TP tunnels and sessions.
Router# show vpdn session [all [interface tunnel username] packets sequence state timers window]	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
Router# show vpdn tunnel [all [id local-name remote-name] packets state summary transport]	Displays VPDN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status.
Router# show interface virtual-access number	Displays information about the virtual access interface, LCP, protocol states, and interface statistics. The following information indicates a normal working status for the virtual access interface (# indicates the number of the VAI): <pre>Virtual-Access# is up, line protocol is up</pre>
Router# clear vpdn tunnel [l2tp [remote-name local-name]]	Shuts down a specific tunnel and all the sessions within the tunnel.
Router# debug vpdn event [protocol flow-control]	Displays VPDN errors and basic events within the L2TP protocol. Also displays errors associated with flow control. Note Flow control is only possible if you use L2TP and you configure the remote peer receive window with a value greater than zero.
Router# debug vpdn error	Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.
Router# debug vpdn packet [control data] [detail]	Displays protocol-specific packet header information, such as sequence numbers, flags, and length.
Router# debug vpdn l2x-events	Displays L2TP events that are part of tunnel establishment or shutdown.
Router# debug vpdn l2x-errors	Displays L2TP protocol errors that prevent tunnel establishment or normal operation.
Router# debug vpdn l2x-packets	Displays the dialog between the LAC and LNS for tunnel or session creation.
Router# debug vpdn l2x-data	Checks L2TP data transfer.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

[Example 9-3](#) shows the information that displays when you use the **show vpdn** command. All tunnel and session information displays for all active sessions and tunnels when you use the **show vpdn** command without any keywords or arguments.

Example 9-3 show vpdn Command

```
Router# show vpdn
L2TP Tunnel and Session Information Total tunnels 2 sessions 22
LocID RemID Remote Name   State Remote Address  Port  Sessions VPDN Group
1206019602tunnel5est45.1.5.170111tunnel5

LocIDRemIDTunIDIntfUsernameStateLast Chg
3  312060SSSCircuitu@n5est2d19h
2  212060SSSCircuitu@n5est2d19h
4  412060SSSCircuitu@n5est2d19h
5  512060SSSCircuitu@n5est2d19h
6  612060SSSCircuitu@n5est2d19h
7  712060SSSCircuitu@n5est2d19h
8  812060SSSCircuitu@n5est2d19h
9  912060SSSCircuitu@n5est2d19h
10 1012060SSSCircuitu@n5est2d19h
11 1112060SSSCircuitu@n5est2d19h
12 1212060SSSCircuitu@n5est2d19h

LocID RemID Remote Name   State Remote Address  Port  Sessions VPDN Group
103352883tunnel6est45.1.6.5170111tunnel6

LocIDRemIDTunIDIntfUsernameStateLast Chg
14 1410335SSSCircuitu@n6est2d19h
15 1510335SSSCircuitu@n6est2d19h
16 1610335SSSCircuitu@n6est2d19h
17 1710335SSSCircuitu@n6est2d19h
18 1810335SSSCircuitu@n6est2d19h
19 1910335SSSCircuitu@n6est2d19h
20 2010335SSSCircuitu@n6est2d19h
21 2110335SSSCircuitu@n6est2d19h
22 2210335SSSCircuitu@n6est2d19h
23 2310335SSSCircuitu@n6est2d19h
13 1310335SSSCircuitu@n6est2d19h

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

[Example 9-4](#) uses the **show interface virtual-access** command to display information about virtual access interface 3. In this example, the following information indicates a normal working status:

```
Virtual-Access3 is up, line protocol is up
```

Example 9-4 show interface virtual access Command

```
Router# show interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 128 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open, multilink Open
  Open: IPCP
  Last input 00:02:30, output never, output hang never
  Last clearing of "show interface" counters 1d19h
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 21/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    55930 packets input, 3347967 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
    105261 packets output, 9607052 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```