



L2TP Tunnel Management Enhancements

This feature module describes enhancements to L2TP tunnel management. It includes information on the benefits of the enhancements, supported platforms, related documents, and configuration.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Configuration Tasks, page 2
- Configuration Examples, page 7
- Command Reference, page 9
- Glossary, page 13

Feature Overview

The L2TP tunnel management enhancements include the following features:

- Tunnel Sharing—Enables sessions authorized with different domains to share the same tunnel.
- Sessions per Tunnel Limiting—Enables the **initiate-to** command to limit the number of sessions per L2TP tunnel.

Benefits

Tunnel Reduction

Tunnel Sharing reduces the number of tunnels required from the L2TP access concentrator (LAC). When used with the L2TP Tunnel Switching feature, Tunnel Sharing also reduces the number of tunnels to an L2TP network server (LNS). While improving tunnel management, Tunnel Sharing helps to reduce the number of tunnel establishment messages that are sent after interface dropouts, reducing dropout recovery time.

Session Limiting Without Resource Pool Management

Prior to this release, the limit option of the **initiate-to** command was valid only when resource pool management (RPM) was enabled. The limit option also set the maximum number of sessions from the router to the specified IP address.

Sessions per Tunnel Limiting allows session limiting without RPM, and it limits the number of sessions per L2TP tunnel.

Sessions per PVC Limiting

Sessions per Tunnel Limiting enables you to limit the number of sessions ultimately carried by one ATM PVC.

Predictable Corporate Router Utilization

Because the Sessions per Tunnel Limiting feature enables you to specify the maximum number of VPDN sessions terminating at any L2TP network server (LNS), you can keep corporate router utilization at a more predictable level.

Related Documents

- *VPDN Group Reorganization* feature module
- *Layer 2 Tunnel Protocol* feature module
- *Cisco 6400 Software Configuration Guide and Command Reference*

Supported Platforms

The Sessions per Tunnel Limiting feature is supported on the Cisco 6400 UAC.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

No new or modified MIBs are supported by this feature.

RFCs

No new or modified RFCs are supported by this feature.


Configuration Tasks

The following sections describe two methods of implementing each L2TP tunnel management feature:

- Configuring Tunnel Sharing—Local Method
- Configuring Tunnel Sharing—RADIUS Service Profile
- Limiting the Number of Sessions per Tunnel—Local Method
- Limiting the Number of Sessions per Tunnel—RADIUS Service Profile

Configuring Tunnel Sharing—Local Method

To implement the tunnel sharing feature, complete the following steps on the NRP-LAC beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group.
Step 2	Router(config-vpdn)# request-dialin	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 3	Router(config-vpdn-req-in)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol.
Step 4	Router(config-vpdn-req-in)# multihop hostname <i>ingress-tunnel-name</i> or Router(config-vpdn-req-in)# domain <i>domain-name</i> or Router(config-vpdn-req-in)# dnis <i>dnis-number</i>	Initiates a tunnel based on the LAC's host name or ingress tunnel ID. Initiates a tunnel based on the client-supplied domain name. Initiates a tunnel based on the user's DNIS number.
		 Note Repeat Step 4 to enter all keys chosen for tunnel sharing.
Step 5	Router(config-vpdn-req-in)# exit	Returns to VPDN group mode.
Step 6	Router(config-vpdn)# initiate-to ip <i>ip-address</i> [priority <i>priority-number</i>]	Specifies the LNS IP address. Optionally specifies the priority of the IP address (1 is highest).
Step 7	Router(config-vpdn)# tunnel share	Enables tunnel sharing among the keys entered in Step 4.

Verifying Tunnel Sharing

Enter the **show running-config EXEC** command to check that you successfully enabled the tunnel sharing feature.

Configuring Tunnel Sharing—RADIUS Service Profile

To implement the tunnel sharing feature, enter the following Cisco-AVpair attributes in the RADIUS service profile.

VPDN Group

This attribute specifies the group to which the service belongs. All services with matching group names are considered members of the same VPDN group.

Cisco-AVpair = "vpdn:vpdn-group=group-name"

Syntax Description

<i>group-name</i>	Group to which the service belongs.
-------------------	-------------------------------------

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:vpdn-group=group1"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:vpdn-group=group1"
```

Tunnel Share

This attribute indicates that the tunnel sharing feature is enabled for the service.

Cisco-AVpair = "vpdn:tunnel-share=yes"

Syntax Description

This attribute has no arguments or keywords.

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:tunnel-share=yes"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:tunnel-share=yes"
```

Verifying the RADIUS Service Profile

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Limiting the Number of Sessions per Tunnel—Local Method

To limit the number of sessions per tunnel without using a RADIUS server, complete the following steps on the NRP-LAC beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group.
Step 2	Router(config-vpdn)# request-dialin	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 3	Router(config-vpdn-req-in)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol.

	Command	Purpose
Step 4	Router(config- <i>vpdn-req-in</i>)# multihop <i>hostname</i> <i>ingress-tunnel-name</i>	Initiates a tunnel based on the LAC's host name or ingress tunnel ID.
	and/or	
	Router(config- <i>vpdn-req-in</i>)# domain <i>domain-name</i>	
	and/or	Initiates a tunnel based on the client-supplied domain name.
	Router(config- <i>vpdn-req-in</i>)# dnis <i>dnis-number</i>	Initiates a tunnel based on the user's DNIS number.
Step 5	Router(config- <i>vpdn-req-in</i>)# exit	Returns to VPDN group mode.
Step 6	Router(config- <i>vpdn</i>)# initiate-to ip <i>ip-address</i> limit <i>limit-number</i> [priority <i>priority-number</i>]	Specifies the LNS IP address and the maximum number of sessions per tunnel. Optionally specifies the priority of the IP address (1 is highest).

Verifying Sessions per Tunnel Limiting via the Local Method

- Step 1** Enter the **show running-config** EXEC command to check that you successfully configured the maximum number of sessions per tunnel.
- Step 2** Enter the **show vpdn tunnel** privileged EXEC command to verify that the number of displayed sessions does not exceed your configured limit.

```
Router# show vpdn tunnel
```

```
L2TP Tunnel Information (Total tunnels 50 sessions 2000)
```

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions
41234	7811	LNS1	est	10.1.1.1	1701	40
20022	2323	LNS1	est	10.1.1.1	1701	40
41234	7811	LNS2	est	10.1.2.2	1701	40
59765	3477	LNS2	est	10.1.3.3	1701	40
...						

Limiting the Number of Sessions per Tunnel—RADIUS Service Profile

To use a RADIUS server to limit the number of sessions per tunnel, enter the following Cisco-AVpair attributes in the RADIUS service profile.

VPDN IP Addresses

This attribute specifies the IP addresses of the LNSes to receive the L2TP connections.

Cisco-AVpair = "vpdn:ip-addresses=address1[<delimiter>address2][<delimiter>address3]..."

Syntax Description

<i>address</i>		IP address of the LNS.
<i><delimiter></i>	, (comma)	Selects load sharing among IP addresses.
	(space)	Selects load sharing among IP addresses.
	/ (slash)	Groups IP addresses on left side in higher priority than the right side.

In the following example, the LAC will send the first PPP session through a tunnel to 10.1.1.1, the second PPP session to 10.2.2.2, the third to 10.3.3.3. The fourth PPP session will be sent through the tunnel to 10.1.1.1, and so forth. If the LAC fails to establish a tunnel with any of the IP addresses in the first group, then the LAC will attempt to connect to those in the second group (10.4.4.4 and 10.5.5.5).

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

VPDN IP Address Limits

This attribute specifies the maximum number of sessions in each tunnel to the IP addresses listed with the **vpdn:ip-addresses** attribute.

Cisco-AVpair = "vpdn:ip-address-limits=limit1 [limit2] [limit3]..."

Syntax Description

<i>limit</i>	Maximum number of sessions per tunnel to the corresponding IP address.
--------------	--

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:ip-address-limits=10 20 30 40 50 "
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:ip-address-limits=10 20 30 40 50 "
```



Note

You must enter a space between the final *limit* entry and the end quotes.

Verifying the RADIUS Service Profile

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Configuration Examples

This section provides the following configuration examples:

- Local Method of Tunnel Sharing
- RADIUS Service Profiles with Tunnel Sharing
- Local Method of Sessions per Tunnel Limiting
- RADIUS Service Profile Including Sessions per Tunnel Limiting

Local Method of Tunnel Sharing

In the following example, all sessions that are locally authorized through VPDN group 1 are sent through the same tunnel to 10.1.1.1.

```
!  
vpdn-group 1  
  request-dialin  
  protocol l2tp  
  domain net1.com  
  domain net2.com  
  initiate-to ip 10.1.1.1  
  tunnel share  
!
```

RADIUS Service Profiles with Tunnel Sharing

In the following example, both the net1.com and net2.com services are members of the “group1” VPDN group. With tunnel sharing enabled in both service profiles, the sessions for net1.com and net2.com will be combined and sent through the same tunnels.

```

user = net1.com{
  profile_id = 45
  profile_cycle = 18
  member = me
  radius=Cisco {
    check_items= {
      2=cisco
    }
    reply_attributes= {
      9,1="vpdn:tunnel-id=LAC-1"
      9,1="vpdn:l2tp-tunnel_password=MySecret"
      9,1="vpdn:tunnel-type=l2tp"
      9,1="vpdn:ip-addresses=10.10.10.10"
      → 9,1="vpdn:vpdn-group=group1"
      → 9,1="vpdn:tunnel-share=yes"
      6=5
    }
  }
}

user = net2.com{
  profile_id = 45
  profile_cycle = 18
  member = me
  radius=Cisco {
    check_items= {
      2=cisco
    }
    reply_attributes= {
      9,1="vpdn:tunnel-id=LAC-1"
      9,1="vpdn:l2tp-tunnel_password=MySecret"
      9,1="vpdn:tunnel-type=l2tp"
      9,1="vpdn:ip-addresses=10.10.10.10"
      → 9,1="vpdn:vpdn-group=group1"
      → 9,1="vpdn:tunnel-share=yes"
      6=5
    }
  }
}

```

Local Method of Sessions per Tunnel Limiting

In the following example, the LAC initiates up to three tunnels. Each tunnel is limited to 40 sessions.

```

!
vpdn-group 1
  request-dialin
  protocol l2tp
  domain net.com
  initiate-to ip 10.1.1.1 limit 40
  initiate-to ip 10.2.2.2 limit 40
  initiate-to ip 10.2.2.2 limit 40
!

```

RADIUS Service Profile Including Sessions per Tunnel Limiting

The following example shows a tunnel service authorization RADIUS service profile, along with the session limiting entry. IP addresses 10.1.1.1 and 10.2.2.2 are assigned priority 1, while IP addresses 10.3.3.3 and 10.4.4.4 are assigned priority 2. Tunnels to 10.1.1.1 are limited to 100 sessions, tunnels to 10.2.2.2 are limited to 200 sessions, tunnels to 10.3.3.3 are limited to 300 sessions, and tunnels to 10.4.4.4 are limited to 400 sessions.

```
user = net.com{
  profile_id = 45
  profile_cycle = 18
  member = me
  radius=Cisco {
    check_items= {
      2=cisco
    }
    reply_attributes= {
      9,1="vpdn:tunnel-id=LAC-1"
      9,1="vpdn:l2tp-tunnel_password=MySecret"
      9,1="vpdn:tunnel-type=l2tp"
      → 9,1="vpdn:ip-addresses=10.1.1.1 10.2.2.2/10.3.3.3 10.4.4.4"
      → 9,1="vpdn:ip-address-limits=100 200 300 400 "
      6=5
    }
  }
}
```

Command Reference

This section documents the modified command that configures the Sessions per Tunnel Limiting feature.

- **initiate-to**
- **tunnel share**

initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** VPDN group command. To remove an IP address from the VPDN group, use the **no** form of this command.

initiate-to ip *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

no initiate-to [**ip** *ip-address*]

Syntax Description

ip <i>ip-address</i>	IP address of the router that will be tunneled to.
limit <i>limit-number</i>	Maximum number of sessions in each tunnel to the IP address.
priority <i>priority-number</i>	Priority for the IP address (1 is the highest).

Defaults

Disabled.
Unlimited number of sessions per tunnel.

Command Modes

VPDN Group Mode

Command History

Release	Modification
12.0(5) T	This command was introduced.
12.1(1) DC1	This command was modified for the Cisco 6400 NRP. The command option “ limit <i>limit-number</i> ” was extended for use without RPM, and its syntax description was modified. Sessions are now limited per tunnel instead of limited per IP address.

Usage Guidelines

Before you can use this command, you must enable one of the two request VPDN subgroups by using either the **request dialin** or **request dialout** command.

A LAC configured to request dial-in can be configured with multiple **initiate-to** commands to tunnel to more than one IP address.

An LNS configured to request dialout can only be configured with a single **initiate-to** command. If you enter a second **initiate-to** command, it will replace the original **initiate-to** command.

At least one **initiate-to** command must be configured for the VPDN group initiator services (**request-dialin** and **request-dialout**) to function.

Examples

The following example configures VPDN group 1 to request up to three L2TP tunnels to the LNS. This group can tunnel a maximum of 40 sessions per tunnel.

```
!  
vpdn-group 1  
  request-dialin  
  protocol l2tp  
  domain net.com  
  initiate-to ip 10.1.1.1 limit 40  
  initiate-to ip 10.2.2.2 limit 40  
  initiate-to ip 10.2.2.2 limit 40  
!
```

Related Commands

Command	Description
request-dialin	Enables a router to request L2TP tunnels for dial-in.
request-dialout	Enables a router to request L2TP tunnels for dialout calls.

tunnel share

To enable tunnel sharing for a VPDN group, use the **tunnel share** VPDN group command. To disable tunnel sharing, use the **no** form of this command.

tunnel share

no tunnel share

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes VPDN group

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.

Examples

In the following example, all sessions that are locally authorized through VPDN group 1 are sent through the same tunnel to 10.1.1.1.

```

!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain net1.com
  domain net2.com
  initiate-to ip 10.1.1.1
→ tunnel share
!
```

Related Commands

Command	Description
vpdn-group	Selects the VPDN group.
request-dialin	Enables a router to request L2TP tunnels for dial-in.
initiate-to	Specifies the IP address that calls are tunneled to.

Glossary

B-ISDN—Broadband ISDN. ITU-T communication standards designed to handle high-bandwidth applications such as video. B-ISDN currently uses ATM technology over SONET-based transmission circuits to provide data rates from 155 to 622 Mbps and beyond.

Broadband ISDN—See B-ISDN.

Dialed Number Identification Service—See DNIS.

DNIS—Dialed Number Identification Service. The called party number. Typically, this is a number used by call centers or a central office where different numbers are each assigned to a specific service.

Layer 2 Tunnel Protocol—See L2TP.

L2TP—Layer 2 Tunnel Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

L2TP Access Concentrator—See LAC.

LAC—L2TP Access Concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS requires tunneling with the L2TP protocol as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

L2TP network server—See LNS.

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

permanent virtual circuit—See PVC.

permanent virtual connection—See PVC.

PVC—Permanent virtual circuit or connection. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

RADIUS—Remote Access Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

Remote Access Dial-In User Service—See RADIUS.

tunnel—A virtual pipe between the LAC and LNS that can carry multiple L2TP sessions.

Virtual Private Dialup Networking—See VPDN.

VPDN—Virtual Private Dialup Networking. A system that permits the physical dialup connection to appear to be connected directly to a home network while actually residing elsewhere on the network. A virtual pipe is connected between the physical dialup connections and the termination point at the home network.

