Configuring Additional VPDN Features

This module documents concepts and tasks associated with configuring the following additional virtual private dialup network (VPDN) features:

- The following optional feature can be configured in isolation, or in combination with a dial-in VPDN deployment:
  - L2TP dial-out VPDNs
- The following optional features are used in combination with a VPDN deployment, and require that a VPDN deployment is first configured:
  - L2TP Security for the Protection of VPDN Tunnels
  - VPDN Template
  - VPDN Source IP Address
  - VRF-Aware VPDN Tunnels
  - MTU Tuning for L2TP VPDN Tunnels
  - QoS for VPDN Tunnels

All of the tasks documented in this module require that tasks documented elsewhere in the *Cisco IOS VPDN Configuration Guide* have first been completed.

Module History

This module was first published on October 31, 2005, and last updated on May 10, 2006.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the "Feature Information for Additional VPDN Features" section on page 278.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Information About Configuring Additional VPDN Features

This section contains information about the following additional VPDN features:

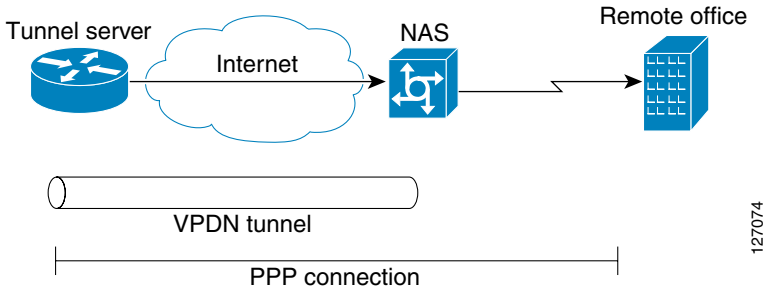
L2TP Dial-Out VPDNs

Dial-out VPDN configurations allow the tunnel server to tunnel outbound calls to the network access server (NAS). The NAS must establish a connection with the remote destination using a medium that supports PPP. Dial-out VPDNs allow a centralized network to efficiently and inexpensively establish virtual point-to-point connections with any number of remote offices.

Dial-out VPDNs are supported with only Layer 2 Tunnel Protocol (L2TP). Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnel.

Figure 23 shows a basic L2TP dial-out scenario.

Figure 23 Dial-Out VPDN Scenario



In an L2TP dial-out deployment, the tunnel server receives PPP packets from it's local network to send to a remote network or device. The tunnel server initiates establishment of an L2TP tunnel with the NAS, and the NAS terminates the tunnel. The NAS must then establish a connection to the client.

L2TP Security for the Protection of VPDN Tunnels

L2TP security provides enhanced security for tunneled PPP frames by allowing the robust security features of IP Security (IPSec) to protect the L2TP VPDN tunnel and the PPP sessions within the tunnel. Without L2TP security, only a one-time, optional mutual authentication is performed during tunnel setup, with no authentication of subsequent data packets or control messages.

The deployment of Microsoft Windows 2000 demands the integration of IPSec with L2TP because this is the default VPDN networking scenario. This integration of protocols is also used for LAN-to-LAN VPDN connections in Microsoft Windows 2000. L2TP security provides integration of IPSec with L2TP in a solution that is scalable to large networks with minimal configuration.

The enhanced protection provided by L2TP security increases the integrity and confidentiality of tunneled PPP sessions within a standardized, well-deployed Layer 2 tunneling solution. The security features of IPSec and Internet Key Exchange (IKE) include confidentiality, integrity checking, replay protection, authentication, and key management. Traditional routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Interior Gateway Routing Protocol (IGRP) will run transparently because a real PPP interface is associated with the secure tunnel. Additional benefits include built in keepalives and standardized interfaces for user authentication and accounting to authentication, authorization, and accounting (AAA) servers, interface statistics, standardized MIBs, and multiprotocol support.

VPDN Template

Beginning in Cisco IOS Release 12.2(8)T, a VPDN template can be configured with global default values that will supersede the system default values. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups.

Beginning in Cisco IOS Release 12.2(13)T and Cisco IOS Release 12.2(28)SB, multiple named VPDN templates can be configured in addition to a single global (unnamed) VPDN template. A VPDN group can be associated with only one VPDN template.

Values configured in the global VPDN template are applied to all VPDN groups by default. A VPDN group can be disassociated from the global VPDN template, or associated with a named VPDN template. Associating a VPDN group with a named VPDN template automatically disassociates it from the global VPDN template.

The default hierarchy for the application of VPDN parameters to a VPDN group is as follows:

- VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.
- VPDN parameters configured in the associated VPDN template are applied for any settings not specified in the individual VPDN group configuration.
- System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or the associated VPDN template.

Individual VPDN groups can be disassociated from the associated VPDN template if desired, allowing the system default settings to be used for any parameters not configured in that individual VPDN group.

VPDN Source IP Address

A tunnel endpoint can be configured with a source IP address that is different from the IP address used to open the VPDN tunnel. When a source IP address is configured on a tunnel endpoint, the router will generate VPDN packets labeled with the configured source IP address. A source IP address may need to be configured if the tunnel endpoints are managed by different companies and addressing requirements necessitate that a particular IP address be used.

The source IP address can be configured globally, or for an individual VPDN group. The VPDN group configuration will take precedence over the global configuration.

VRF-Aware VPDN Tunnels

Prior to Cisco IOS Release 12.2(15)T or Cisco IOS Release 12.2(28)SB, you had to specify IP addresses from the global routing table for the endpoints of a VPDN tunnel. VRF-aware VPDN tunnels provide support for VPDN tunnels that terminate on a virtual private network (VPN) routing and forwarding instance (VRF) by allowing you to use IP addresses from a VRF routing table.

VRF-aware VPDN tunnels enhance the support of VPDN tunnels by allowing VPDN tunnels to start outside a Multiprotocol Label Switching (MPLS) VPN and terminate within the MPLS VPN. For example, this feature allows you to use a VRF address from a customer VRF as the destination address.

You can use VRF-aware VPDN tunnels with multihop, dial-in, and dial-out VPDN tunneling scenarios. In a multihop scenario, this feature is sometimes referred to as VRF-aware VPDN multihop.

MTU Tuning for L2TP VPDN Tunnels

Fragmentation and reassembly of packets is done at the process level in Cisco IOS software. When a tunnel server is aggregating large numbers of sessions and traffic flows, process switching can dramatically reduce performance. For this reason, it is highly desirable to reduce or eliminate the need for packet fragmentation and reassembly in a VPDN deployment, and instead move the burden of any required packet reassembly to the client devices.

Packets are fragmented when they attempt to pass through an egress interface with a maximum transmission unit (MTU) that is smaller than the size of the packet. By default, the MTU of most interface is 1500 bytes. Because of this default MTU size, TCP segments are created with a default payload of 1460 bytes, allowing room for the 40 byte TCP/IP header. Because L2TP encapsulation adds 40 bytes of header information, tunneled packets will exceed the MTU of an interface if MTU tuning is not performed.

In order to reach its final destination, a packet may traverse multiple egress interfaces. The path MTU is defined as the smallest MTU of all of the interfaces that the packet must pass through.

A number of different methods are available to perform MTU tuning. Their end goal is to prevent fragmentation of packets after they have been encapsulated for tunneling. These methods take advantage of distinct mechanisms to accomplish this, as described in the following sections:

- MTU Tuning Using IP MTU Adjustments, page 227
- MTU Tuning Using Path MTU Discovery, page 227
- MTU Tuning Using TCP MSS Advertising, page 227
- MTU Tuning Using PPP MRU Advertising, page 228

MTU Tuning Using IP MTU Adjustments

The IP MTU configuration controls the maximum size of a packet allowed to be encapsulated by a Layer 2 protocol. The IP MTU of an interface can be manually lowered to compensate for the size of the L2TP header if the path MTU is known.

A router can also be configured to automatically adjust the IP MTU of an interface to compensate for the size of the L2TP header. The automatic adjustment corrects for the size of the L2TP header based on the MTU of the egress interface of that device. This configuration is effective only in preventing fragmentation when the MTU of that interface is the same as the path MTU.

MTU Tuning Using Path MTU Discovery

If the path MTU between the NAS and the tunnel server is unknown, or if it changes, path MTU discovery (PMTUD) can be used to perform MTU tuning. PMTUD, introduced in Cisco IOS Release 12.2(4)T, uses the Don't Fragment (DF) bit in the IP header to dynamically discover the smallest MTU among all the interfaces along a routing path.

The source host initially assumes that the path MTU is the known MTU of the first egress interface, and sends all packets on that path with the DF bit in the IP header set. If any of the packets are too large to be forwarded without fragmentation by the interface of a device along the path, that device will discard the packet and return an Internet Control Message Protocol (ICMP) Destination Unreachable message to the source host. The ICMP Destination Unreachable message includes code 4, which means "fragmentation needed and DF set," and indicates the IP MTU of the interface that was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission to allow it to fit through that interface.

Enabling PMTUD makes VPDN deployments vulnerable to Denial of Service (DoS) attacks that use crafted ICMP messages to set a connection's path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. For more information on throughput-reduction attacks against L2TP VPDN deployments, see the Security Advisory *Crafted ICMP Messages Can Cause Denial of Service*.

To protect against a throughput-reduction attack, a range of acceptable values for the path MTU can be specified. If the device receives an ICMP code 4 message that advertises a next-hop path MTU that falls outside the configured size range, the device will ignore the message.

PMTUD can be unreliable, and may fail when performed over the Internet because some routers or firewalls are configured to filter out all ICMP messages. When the source host does not receive an ICMP destination unreachable message from a device that is unable to forward a packet without fragmentation, it will not know to reduce the packet size. The source host will continue to retransmit the same large packet. Because the DF bit is set, these packets will be continually dropped because they exceed the path MTU, and the connection will stop responding.

MTU Tuning Using TCP MSS Advertising

Because PMTUD can be unreliable, an alternate method of performing MTU tuning was introduced in Cisco IOS 12.2(4)T. This method of MTU tuning takes advantage of TCP Maximum Segment Size (MSS) advertisements in the incoming and outgoing synchronize (SYN) packets sent by the end hosts.

The TCP MSS defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

If you configure a lower TCP MSS than the usual default of 1460, the size of TCP segments will be reduced to compensate for the information added by the L2TP header.

MTU Tuning Using PPP MRU Advertising

Another option for reducing fragmentation in an L2TP VPDN network requires that Maximum Receive Unit (MRU) negotiation is supported by the PPP client. One known client which supports MRU negotiations is the Windows XP PPP client. Unfortunately, other commonly deployed PPP clients do not adhere to the advertised PPP MRU as they should. Refer to the PPP client documentation to determine if your PPP client properly responds to the advertised PPP MRU.

PPP MRU allows a peer to advertise its maximum receive unit, which is derived from the MTU configuration on the virtual template interface. A device will not process a PPP frame with a payload larger than its advertised MRU. The Cisco PPP implementation uses the MTU of the interface as the advertised MRU value during PPP negotiations.

The MTU of a virtual template interface can be manually lowered to compensate for the size of the L2TP header. If the PPP peer listens to the MRU advertised during PPP negotiation, it will adjust its MTU (and indirectly its IP MTU) for that PPP link. This in turn will modify the TCP MSS that the peer advertises when opening up TCP connections.

Because the default MTU for an interface is 1500 bytes, the default MRU is 1500 bytes. Setting the MTU of an interface to 1460 changes the advertised MRU to 1460. This configuration would tell the peer to allow room for a 40-byte L2TP header.

One issue with lowering the MTU on the virtual-template interface is that the IP MTU is automatically lowered as well. It is not possible to configure an IP MTU greater than the MTU on a virtual template interface. This can be an issue if there is a mixture of peer devices that do and do not adjust their MTU based on the advertised MRU. The clients that are unable to listen to MRU advertisements and adjust accordingly will continue to send full-sized packets to the peer. Packets that are larger than the lowered IP MTU, yet smaller than the normal default IP MTU, will be forced to fragment. For example, an L2TP packet that is 1490 bytes would normally be transmitted without fragmentation. If the MTU has been lowered to 1460 bytes, this packet will be unnecessarily fragmented. In this situation, it would be optimal to advertise a lower MRU to those clients that are capable of listening and adjusting, yet still allow full-sized packets for those clients that are unable to adjust.

Clients that ignore the advertised MRU may experience the PMTUD problems described in the "MTU Tuning Using IP MTU Adjustments" section. PMTUD can be turned off by clearing the DF bit on the inner IP packet.

QoS for VPDN Tunnels

Quality of service (QoS) packet classification features provide the capability to partition network traffic into multiple priority levels or classes of service. Packet classifications provide the information required to coordinate QoS from end to end within and between networks. Packet classifications are used by other QoS features to assign the appropriate traffic handling policies, including congestion management, bandwidth allocation, and delay bounds for each traffic class.

For further information on QoS and traffic handling policies, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

Packets can be marked for end-to-end QoS using the type of service (ToS) byte in the IP header. The first three bits of the ToS byte are used for IP precedence settings. Four of the remaining five bits are used to set the ToS. The remaining bit of the ToS byte is unassigned.

In a VPDN deployment, IP packets may be classified by an external source such as the customer network or a downstream client. By default, a tunnel endpoint will set the ToS byte in the Layer 2 header to zero, specifying normal service. Depending on the VPDN deployment, you may choose to configure your VPDN network to do one of the following in regard to QoS classifications:

- Ignore existing QoS classifications by leaving the default configuration in place.
- Preserve existing QoS classifications by configuring the tunnel endpoint to copy the ToS byte from the IP header to the Layer 2 header.
- Configure QoS classifications specific to your VPDN network.

The following sections provide additional information on QoS options for VPDN deployments:

- QoS Classification Preservation, page 229
- IP Precedence for VPDN Tunnels, page 229
- ToS Classification for VPDN Tunnels, page 229

QoS Classification Preservation

When Layer 2 packets are created the ToS byte value is set to zero by default, indicating normal service. This setting ignores the values of the ToS byte of the encapsulated IP packets that are being tunneled. The tunnel server can be configured to copy the contents of the ToS field of the inner IP packets to the ToS byte of the Layer 2 header. Copying the ToS field from the IP header to the Layer 2 header preserves end-to-end QoS for tunneled packets.

IP Precedence for VPDN Tunnels

IP precedence settings mark the class of service (CoS) for a packet. The three precedence bits in the ToS field of the IP header can be used to define up to six classes of service. If you choose to manually configure a specific IP precedence value for Layer 2 packets, QoS will not be preserved end-to-end across the tunnel.

ToS Classification for VPDN Tunnels

The ToS bits mark the ToS classification for a packet. Each of the four bits controls a particular aspect of the ToS—reliability, throughput, delay, and cost. If you choose to manually configure a specific ToS value for Layer 2 packets, QoS will not be preserved end-to-end across the tunnel.

How to Configure Additional VPDN Features

This section contains the following configuration tasks, which may be configured in any order:

- Configuring a Dial-Out L2TP VPDN, page 230 (optional)
- Configuring L2TP Security for VPDN Tunnels, page 240 (optional)
- Verifying IPSec Protection of L2TP VPDN Tunnels, page 244 (optional)
- Creating a VPDN Template, page 247 (optional)
- Associating a VPDN Group with a VPDN Template, page 248
- Disassociating a VPDN Group from the VPDN Template, page 250 (optional)
- Configuring the VPDN Source IP Address, page 251 (optional)
- Configuring VRF-Aware VPDN Tunneling, page 253 (optional)
- Performing MTU Tuning for L2TP VPDNs, page 256 (optional)
- Configuring QoS Packet Classifications for VPDNs, page 264 (optional)

Configuring a Dial-Out L2TP VPDN

Configuring a dial-out VPDN enables a tunnel server to send outbound calls over a VPDN tunnel using L2TP as the tunneling protocol. Dial-out VPDN configuration allows a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnels.

The following sections contain additional information about L2TP dial-out configurations:

- L2TP Dial-Out Connection Establishment, page 230
- L2TP Dial-Out Load Balancing and Redundancy, page 232
- Prerequisites for Configuring a Dial-Out L2TP VPDN, page 232
- Restrictions for Configuring a Dial-Out L2TP VPDN, page 232

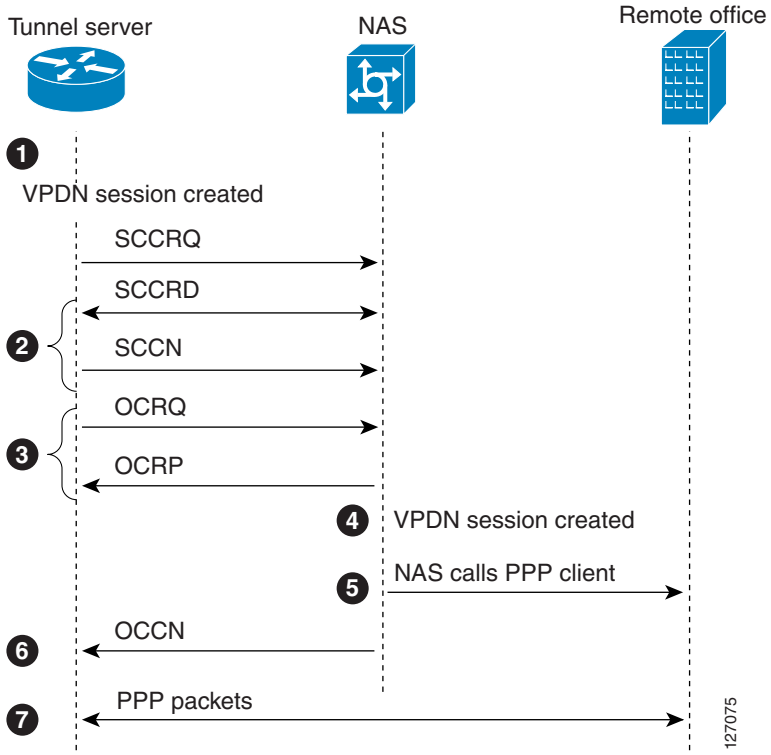
The following tasks must be completed to configure a dial-out L2TP VPDN:

- Configuring the Tunnel Server to Request Dial-Out, page 232 (required)
- Configuring the Dialer on the Tunnel Server, page 234 (required)
- Configuring the NAS to Accept Dial-Out, page 236 (required)
- Configuring the Dialer on the NAS, page 238 (required)

L2TP Dial-Out Connection Establishment

Figure 24 shows the steps involved in establishing a dial-out connection for a typical dial-out scenario.

Figure 24 L2TP Dial-Out Process



The following sequence of events occurs during session establishment, and is keyed to Figure 24:

1. The tunnel server receives PPP packets and forwards them to its dialer interface. The dialer interface can be either a dialer profile dialer pool or dial-on-demand routing (DDR) rotary group.

   The dialer issues a dial call request to the VPDN group, and the tunnel server creates a virtual access interface. If the dialer is a dialer profile, this interface becomes a member of the dial pool. If the dialer is DDR, the interface becomes a member of the rotary group.

   The VPDN group creates a VPDN session for this connection and sets it in the pending state.

2. The tunnel server and NAS establish an L2TP tunnel (unless a tunnel is already open) by exchanging Start Control Connection Request (SCCRQ) and Start Control Connection Reply (SCCRP) messages.

3. The tunnel server sends an Outgoing Call Request (OCRQ) packet to the NAS, which checks if it has a dial resource available.

   If the resource is available, the NAS responds to the tunnel server with an Outgoing Call Reply (OCRP) packet. If the resource is not available, the NAS responds with a Call Disconnect Notification (CDN) packet, and the session is terminated.

4. If the NAS has an available resource, it creates a VPDN session and sets it in the pending state.

5. The NAS then initiates a call to the PPP client. When the NAS call connects to the PPP client, the NAS binds the call interface to the appropriate VPDN session.

6. The NAS sends an Outgoing Call Connected (OCCN) packet to the tunnel server. The tunnel server binds the call to the appropriate VPDN session and then brings the virtual access interface up.

7. The dialer on the tunnel server and the PPP client can now exchange PPP packets. The NAS acts as a transparent packet forwarder.

If the dialer interface is a DDR and a virtual profile is configured, the PPP endpoint is the tunnel server virtual access interface, not the dialer. All Layer 3 routes point to this interface instead of to the dialer.

L2TP Dial-Out Load Balancing and Redundancy

In Cisco IOS software prior to Release 12.2(15)T or 12.2(28)SB, load balancing and redundancy for dial-out VPDNs could be configured only with L2TP large-scale dial-out (LSDO) using Stack Group Bidding Protocol (SGBP). This method of load balancing and redundancy requires that the primary NAS is up and running for dial-out to take place, because the IP address of only that NAS is configured on the tunnel server. When the primary NAS is down, no dial-out can take place. When the primary NAS is up, the NAS determines among itself and the secondary NASs which NAS has the least congestion, and then inform the tunnel server to use the selected NAS for dial-out. Because the tunnel server cannot contact any other NASs when the primary NAS is down, failover is not supported for dial-out calls by this mechanism. For more information about configuring LSDO, refer to the chapter "Configuring Large-Scale Dial-Out" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

The ability to configure a tunnel server with the IP addresses of multiple NASs was introduced in Cisco IOS Release 12.2(15)T and Cisco IOS Release 12.2(28)SB. Load balancing, redundancy, and failover can all be controlled by assigning each NAS the desired priority settings on the tunnel server. Load balancing occurs between NASs with identical priority settings. When NASs are assigned different priority settings, if the NAS with the highest priority goes down the tunnel server will fail over to a lower priority NAS.

Prerequisites for Configuring a Dial-Out L2TP VPDN

Before performing these tasks, you should configure the required tasks in the "Configuring AAA for VPDNs" module.

Restrictions for Configuring a Dial-Out L2TP VPDN

- L2TP is the only Layer 2 protocol that can be used to tunnel dial-out VPDNs.
- Large-scale dial-out, Bandwidth Allocation Protocol (BAP), and Dialer Watch are not supported with dial-out VPDNs.
- You must be running Cisco IOS Release 12.2(15)T, Cisco IOS Release 12.2(28)SB, or a later release to configure the tunnel server to contact multiple NASs, to perform dial-out load balancing, or to configure dial-out redundancy.
- When you configure the tunnel server to dial-out to multiple NASs, because each NAS is configured using the same VPDN group, all of the NASs must have the same tunnel configuration settings (the same L2TP tunnel password, for example).

Configuring the Tunnel Server to Request Dial-Out

The tunnel server must be configured to request the establishment of a VPDN tunnel with the NAS when it is directed to tunnel outbound PPP data. The VPDN group is linked to the dialer profile by the dialer pool number.

Perform this task to configure the tunnel server to request the establishment of a dial-out VPDN tunnel and to specify the dialer rotary group or dialer pool that may issue dial requests to the VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **description** *string*
5. **request-dialout**
6. **protocol l2tp**
7. **pool-member** *pool-number*
8. **exit**
9. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**request-dialout** **Example:** `Router(config-vpdn)# request-dialout`	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS and enters request dial-out VPDN subgroup configuration mode.
Step 6	**protocol l2tp** **Example:** `Router(config-vpdn-req-ou)# protocol l2tp`	Specifies L2TP as the Layer 2 protocol that the VPDN group will use.
Step 7	**pool-member** *pool-number* **Example:** `Router(config-vpdn-req-ou)# pool-member 1`	Assigns a request-dialout VPDN group to a dialer pool.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-vpdn-req-ou)# exit`	Exits request dial-out VPDN subgroup configuration mode.
Step 9	**initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*] **Example:** `Router(config-vpdn)# initiate-to ip 10.0.58.201 limit 5 priority 1`	Specifies the IP address that will be used for Layer 2 tunneling. • Beginning in Cisco IOS Release 12.2(15)T and Cisco IOS Release 12.2(28)SB, the following options are available for this command: – **limit**—Maximum number of connections that can be made to this IP address. – **priority**—Priority for this IP address (1 is the highest). **Note** Beginning in Cisco IOS Release 12.2(15)T and Cisco IOS Release 12.2(28)SB, multiple **initiate-to** commands can be entered to configure the tunnel server to contact multiple NASs. The tunnel server can also be configured to provide load balancing and redundancy for failover using the **initiate-to** command; see the examples in the "Configuring L2TP Dial-Out Load Balancing: Example" section.

What to Do Next

- You may perform the optional task "Configuring L2TP Control Packet Parameters for VPDN Tunnels" in the "VPDN Tunnel Management" module. Configuring the **l2tp tunnel** commands documented in this task is optional, and these commands should be configured only if it becomes necessary to change the default settings. See the "L2TP Dial-Out Failover Redundancy with Tunnel Timers: Example" section for an example of when and how to use the **l2tp tunnel** commands in a dial-out scenario.
- You must perform the task in the "Configuring the Dialer on the NAS" section.

Configuring the Dialer on the Tunnel Server

A request to tunnel outbound data from the tunnel server must be associated with a dialer profile.

Perform this task to configure the dialer profile on the tunnel server. A dialer profile must be configured for each dial-out destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dialer** *dialer-rotary-group-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **encapsulation ppp**

6. **dialer remote-name** *user-name*
7. **dialer-string** *dial-string*
8. **dialer vpdn**
9. **dialer pool** *number*
10. **dialer-group** *group-number*
11. **ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dialer** *dialer-rotary-group-number* **Example:** `Router(config)# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Sets PPP as the encapsulation method used by the interface.
Step 6	**dialer remote-name** *user-name* **Example:** `Router(config-if)# dialer remote-name router22`	Specifies the authentication name of the remote router on the destination subnetwork for a dialer interface.
Step 7	**dialer-string** *dial-string* **Example:** `Router(config-if)# dialer-string 5550100`	Specifies the string (telephone number) to be called for interfaces calling a single site.
Step 8	**dialer vpdn** **Example:** `Router(config-if)# dialer vpdn`	Enables a dialer profile or DDR dialer to use L2TP dial-out.

	Command or Action	Purpose
Step 9	**dialer pool** *number* **Example:** `Router(config-if)# dialer-pool 1`	Specifies, for a dialer interface, which dialing pool to use to connect to a specific destination subnetwork. **Note** The value used for the *number* argument must match the value configured for the **pool-member** *pool-number* command in the VPDN group configuration.
Step 10	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 1`	Controls access by configuring an interface to belong to a specific dialing group.
Step 11	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config-if)# ppp authentication chap`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

What to Do Next

You must perform the task in the "Configuring the NAS to Accept Dial-Out" section.

Configuring the NAS to Accept Dial-Out

The NAS must be configured to accept outbound tunnels from the tunnel server, and to initiate PPP calls to the destination client. Outbound calls will be placed using the dialer interface specified in the VPDN group configuration.

Perform this task to configure the NAS to accept tunneled dial-out connections from the tunnel server. If multiple NASs are configured on the tunnel server, perform this task on each NAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **description** *string*
5. **accept-dialout**
6. **protocol l2tp**
7. **dialer** *dialer-interface*
8. **exit**
9. **terminate-from hostname** *hostname*
10. **l2tp tunnel bearer capabilities** {**none** | **digital** | **analog** | **all**}
11. **l2tp tunnel framing capabilities** {**none** | **synchronous** | **asynchronous** | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**accept-dialout** **Example:** `Router(config-vpdn)# accept-dialout`	Creates an accept dial-out VPDN subgroup that configures a NAS to accept requests from a tunnel server to tunnel L2TP dial-out calls and enters accept dial-out VPDN subgroup configuration mode.
Step 6	**protocol l2tp** **Example:** `Router(config-vpdn-acc-ou)# protocol l2tp`	Specifies L2TP as the Layer 2 protocol that the VPDN group will use.
Step 7	**dialer** *dialer-interface* **Example:** `Router(config-vpdn-acc-ou)# dialer 2`	Specifies the dialer interface that an accept-dialout VPDN subgroup will use to dial out calls.
Step 8	**exit** **Example:** `Router(config-vpdn-acc-ou)# exit`	Exits accept dial-out VPDN subgroup configuration mode.
Step 9	**terminate-from hostname** *hostname* **Example:** `Router(config-vpdn)# terminate-from hostname tunnelserver32`	Specifies the hostname of the remote NAS or tunnel server that will be required when accepting a VPDN tunnel.

	Command or Action	Purpose
Step 10	**l2tp tunnel bearer capabilities** {**none** | **digital** | **analog** | **all**} **Example:** `Router(config-vpdn)# l2tp tunnel bearer capabilities digital`	(Optional) Sets the bearer-capability value used by the Cisco router. • When an accept dial-out VPDN subgroup is configured, the default value for this command is **all**. To ensure compatibility with some non-Cisco routers, you may be required to override the default bearer-capability value.
Step 11	**l2tp tunnel framing capabilities** {**none** | **synchronous** | **asynchronous** | **all**} **Example:** `Router(config-vpdn)# l2tp tunnel framing capabilities synchronous`	(Optional) Sets the framing-capability value used by the Cisco router. • When an accept dial-out VPDN subgroup is configured, the default value for this command is **all**. To ensure compatibility with some non-Cisco routers, you may be required to override the default framing-capability value.

What to Do Next

You must perform the task in the "Configuring the Dialer on the NAS" section.

Configuring the Dialer on the NAS

When the NAS receives outbound data from the tunnel server, it must initiate a PPP call to the destination client. The dialer used to initiate calls is specified in the VPDN group configuration, and must match the dialer rotary group number.

Perform this task to configure the dialer on the NAS for dial-out VPDN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dialer** *dialer-rotary-group-number*
4. **ip unnumbered** *interface-type interface-number*
5. **encapsulation ppp**
6. **dialer in-band**
7. **dialer aaa** [**suffix** *string*] [**password** *string*]
8. **dialer group** *group-number*
9. **ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dialer** *dialer-rotary-group-number* **Example:** `Router(config)# interface dialer 3`	Defines a dialer rotary group and enters interface configuration mode. **Note** The value configured for the *dialer-rotary-group-number* argument must match the value configured for the **dialer** *dialer-interface* command in the VPDN group configuration.
Step 4	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-if)# ip unnumbered serial 1`	Enables IP processing on a serial interface without assigning an explicit IP address to the interface.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Sets PPP as the encapsulation method used by the interface.
Step 6	**dialer in-band** **Example:** `Router(config-if)# dialer in-band`	Specifies that DDR is to be supported.
Step 7	**dialer aaa** [**suffix** *string*] [**password** *string*] **Example:** `Router(config-if)# dialer aaa`	Allows a dialer to access the AAA server for dialing information.
Step 8	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 3`	Controls access by configuring an interface to belong to a specific dialing group.
Step 9	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config-if)# ppp authentication chap`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring L2TP Security for VPDN Tunnels

L2TP security provides enhanced security for tunneled PPP frames between the NAS and the tunnel server, increasing the integrity and confidentiality of tunneled PPP sessions within a standardized, well-deployed Layer 2 tunneling solution. The security features of IPSec and IKE include confidentiality, integrity checking, replay protection, authentication, and key management. Additional benefits include built-in keepalives and standardized interfaces for user authentication and accounting to AAA servers, interface statistics, standardized MIBs, and multiprotocol support.

L2TP security can be configured for both NAS-initiated L2TP tunneling scenarios and client-initiated L2TP tunneling scenarios.

The following sections contain additional information about L2TP security:

- L2TP Security with NAS-Initiated VPDN Tunnels, page 240
- L2TP Security with Client-Initiated VPDN Tunnels, page 241
- Prerequisites for L2TP Security, page 241

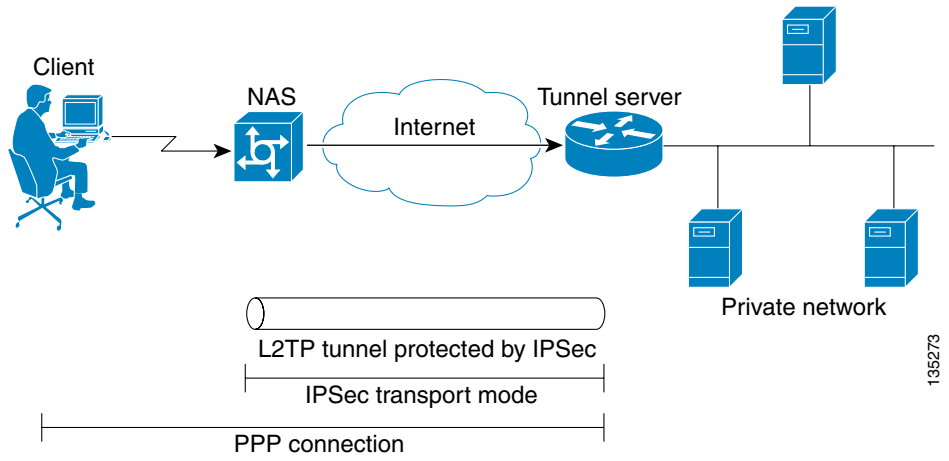
To configure L2TP security for VPDN tunnels, perform the following tasks:

- Configuring IPSec Protection of an L2TP Tunnel, page 242 (required)
- Creating the Security Profile, page 243 (required)

L2TP Security with NAS-Initiated VPDN Tunnels

L2TP security can be configured to protect VPDN tunnels between the NAS and the tunnel server in NAS-initiated VPDN deployments. A NAS-initiated tunneling scenario with L2TP security protection is depicted in Figure 25.

Figure 25 L2TP Security for a NAS-Initiated Tunneling Scenario

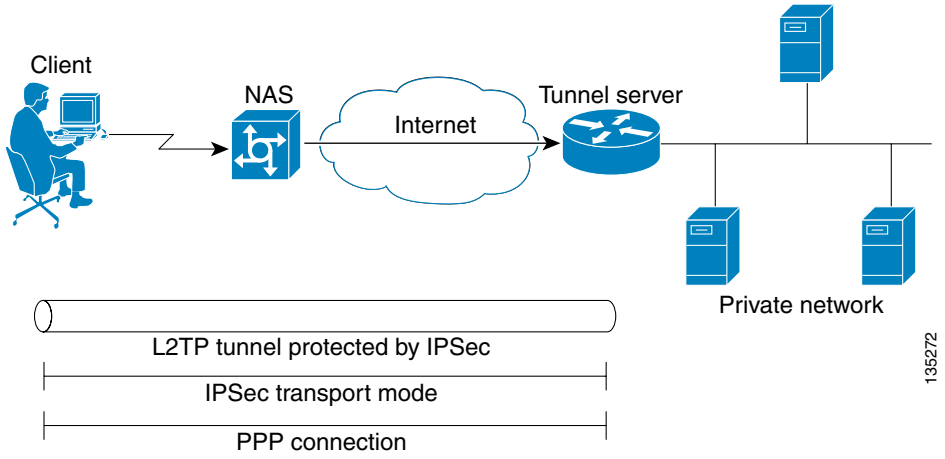


The client connects to the NAS through a medium that supports PPP, such as a dialup modem, digital subscriber line (DSL), ISDN, or a cable modem. If the connection from the client to the NAS is considered secure—such as a modem, ISDN, or a DSL connection—the client may choose not to provide additional security. The PPP session is securely tunneled from the NAS to the tunnel server without any required knowledge or interaction by the client. L2TP security protects the L2TP tunnel between the NAS and the tunnel server with IPSec.

L2TP Security with Client-Initiated VPDN Tunnels

L2TP security can be configured to protect VPDN tunnels between the client and the tunnel server in client-initiated VPDN deployments. A client-initiated tunneling scenario with L2TP security protection is depicted in Figure 26.

Figure 26 L2TP Security for a Client-Initiated Tunneling Scenario



The client initiates an L2TP tunnel to the tunnel server without the intermediate NAS participating in tunnel negotiation or establishment. The client must manage the software that initiates the tunnel. Microsoft Windows 2000 supports this VPDN scenario. In this scenario, extended services processor (ESP) with authentication must always be used. L2TP security protects the L2TP tunnel between the client and the tunnel server with IPSec.

Prerequisites for L2TP Security

- You must be running Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release to configure L2TP security for VPDN tunnels.
- You must perform the required tasks in the "Configuring AAA for VPDNs" module.
- The interface between the NAS and tunnel server must support IPSec. For more information on configuring IPSec, refer to the part "Implementing IPSec and IKE" in the *Cisco IOS Security Configuration Guide*, Release 12.4.

NAS-Initiated Tunnels

- For NAS-initiated tunneling scenarios, you must perform the required tasks in the "Configuring NAS-Initiated Dial-In VPDN Tunneling" module.

Client-Initiated Tunnels

- For client-initiated tunneling scenarios, you must perform the required tasks in the "Configuring Client-Initiated Dial-In VPDN Tunneling" module.
- The interface between the client and the NAS must support PPP. For more information on configuring PPP, refer to the "PPP Configuration" part of the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.
- The client software must support L2TP and IPSec. This is the default VPDN networking scenario in Microsoft Windows 2000.

Configuring IPSec Protection of an L2TP Tunnel

Perform this task to configure IPSec protection of an L2TP tunnel:

- For NAS-initiated L2TP tunnels, this task must be performed on both the NAS and the tunnel server.
- For client-initiated L2TP tunnels, this task must be performed on the tunnel server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **l2tp security crypto-profile** *profile-name* [**keep-sa**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**l2tp security crypto-profile** *profile-name* [**keep-sa**] **Example:** `Router(config-vpdn)# l2tp security crypto-profile l2tp keep-sa`	Enables the VPDN group to be protected by IPSec.

What to Do Next

You must perform the task in the "Creating the Security Profile" section.

Creating the Security Profile

A security profile must be configured to provide IPSec protection of L2TP tunnels. Perform this task to create the security profile:

- For NAS-initiated L2TP tunnels, this task must be performed on both the NAS and the tunnel server.
- For client-initiated L2TP tunnels, this task must be performed on the tunnel server.

Prerequisites

To create an IKE policy and a crypto profile configuration associated with the VPDN group, you must first configure phase 1 Internet Security Association and Key Management Protocol (ISAKMP) policy and an IPSec transform set. For information on configuring phase 1 ISAKMP policies and IPSec transform sets, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface** *type number*
7. **crypto-map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **Example:** `Router(config)# crypto map l2tpsec 10 ipsec-isakmp profile l2tp`	Enters crypto map configuration mode, creates or modifies a crypto map entry, or creates a crypto profile that provides a template for configuration of dynamically created crypto maps. **Note** The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

	Command or Action	Purpose
Step 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **Example:** `Router(config-crypto-map)# set transform-set esp-des-sha-transport`	Specifies which transform sets can be used with the crypto map entry.
Step 5	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 7	**crypto-map** *map-name* **Example:** `Router(config-if)# crypto map l2tpsec`	Applies a previously defined crypto map set to an interface.

What to Do Next

You may perform the optional task in the "Verifying IPSec Protection of L2TP VPDN Tunnels" section.

Verifying IPSec Protection of L2TP VPDN Tunnels

Perform the tasks in this section to verify that L2TP tunnels are protected by IPSec.

- Verifying Establishment of the Crypto Socket, page 244 (optional)
- Verifying the Crypto Map Configuration, page 245 (optional)
- Verifying Encryption and Decryption of L2TP Packets, page 246 (optional)

Verifying Establishment of the Crypto Socket

Perform this task on the NAS or the tunnel server to verify that the crypto socket is created and activated in response to VPDN tunneling events.

SUMMARY STEPS

1. **enable**
2. **debug crypto socket**
3. **debug vpdn l2x-events**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **debug crypto socket**

Enter this command to turn on debug messages for socket messages:

```
Router# debug crypto socket
```

Step 3 **debug vpdn l2x-events**

Enter this command to turn on debug messages for protocol-specific VPDN tunneling events. Examine the debug messages to verify that the socket is created and moved to the active state in response to L2TP tunnel events. The example shows debug output from successful crypto socket creation and activation:

```
Router# debug vpdn l2x-events

*Mar  1 00:56:46.959:CRYPTO_SS(L2X Security):Passive open, socket info:local
10.0.0.13/1701, remote 10.0.0.12/1701, prot 17, ifc Fa0/0
*Mar  1 00:56:47.291:L2TP:I SCCRQ from user02 tnl 5107
*Mar  1 00:56:47.295:L2X:Requested security for socket, UDP socket info:local
10.0.0.13(1701), remote 10.0.0.12(1701)
*Mar  1 00:56:47.295:Tnl 13582 L2TP:Got a challenge in SCCRQ, user02
*Mar  1 00:56:47.295:Tnl 13582 L2TP:New tunnel created for remote user02, address
10.0.0.12
*Mar  1 00:56:47.295:Tnl 13582 L2TP:O SCCRP  to user02 tnlid 5107
*Mar  1 00:56:47.295:Tnl 13582 L2TP:Control channel retransmit delay set to 1 seconds
*Mar  1 00:56:47.299:Tnl 13582 L2TP:Tunnel state change from idle to wait-ctl-reply
*Mar  1 00:56:47.299:CRYPTO_SS(L2X Security):Completed binding of application to socket
```

Verifying the Crypto Map Configuration

Perform this task to verify that the crypto map was dynamically created for the L2TP tunnel.

SUMMARY STEPS

1. **enable**
2. **show crypto map** [**interface** *interface* | **tag** *map-name*]

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show crypto map** [**interface** *interface* | **tag** *map-name*]

Enter this command to display information about a crypto map. Ensure that the proper interface is using the correct crypto map. The following example displays output for the crypto map with the name l2tpsec and shows that it is being used by the FastEthernet 0/0 interface:

```
Router# show crypto map tag l2tpsec

Crypto Map "l2tpsec" 10 ipsec-isakmp
        No matching address list set.
        Current peer:0.0.0.0
        Security association lifetime:4608000 kilobytes/3600 seconds
        PFS (Y/N):N
        Transform sets={ esp, }

Crypto Map "l2tpsec" 20 ipsec-isakmp
        Peer = 10.0.0.13
        Extended IP access list
            access-list  permit udp host 10.0.0.12 port = 1701 host 10.0.0.13 port = 1701
        Current peer:10.0.0.13
        Security association lifetime:4608000 kilobytes/3600 seconds
        PFS (Y/N):N
        Transform sets={ esp, }
!The output below shows that the interface FastEthernet0/0 is uing the crypto map named
!l2tpsec.
        Interfaces using crypto map l2tpsec:
                FastEthernet0/0
```

Verifying Encryption and Decryption of L2TP Packets

Perform this task to verify that L2TP packets are being encrypted and decrypted.

SUMMARY STEPS

1. **enable**
2. **show crypto engine connections active**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show crypto engine connections active**

Enter this command to display information about active crypto engine connections. The number of encryption and decryption events are displayed.

```
Router# show crypto engine connections active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0/0 10.0.0.13       set    HMAC_SHA+DES_56_CB        0        0
2000 FastEthernet0/0 10.0.0.13       set    HMAC_SHA+DES_56_CB        0       62
2001 FastEthernet0/0 10.0.0.13       set    HMAC_SHA+DES_56_CB       64        0
```

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Creating a VPDN Template

Beginning in Cisco IOS Release 12.2(8)T, a VPDN template can be configured with global default values that will supersede the system default values. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups.

Beginning in Cisco IOS Release 12.2(13)T and Cisco IOS Release 12.2(28)SB, multiple named VPDN templates can be configured in addition to a single global (unnamed) VPDN template. A VPDN group can be associated with only one VPDN template.

Values configured in the global VPDN template are applied to all VPDN groups by default. A VPDN group can be disassociated from the global VPDN template, or associated with a named VPDN template. Associating a VPDN group with a named VPDN template automatically disassociates it from the global VPDN template. If you remove a named VPDN template configuration, all VPDN groups that were associated with it will automatically be associated with the global VPDN template.

The hierarchy for the application of VPDN parameters to a VPDN group is as follows:

- VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.
- VPDN parameters configured in the associated VPDN template are applied for any settings not specified in the individual VPDN group configuration.
- System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or the associated VPDN template.

Perform this task on the NAS or the tunnel server to create a VPDN template.

Prerequisites

- You must be running Cisco IOS Release 12.2(8)T, Cisco IOS Release 12.2(28)SB, or a later release to configure a VPDN template.
- You must be running Cisco IOS Release 12.2(13)T, Cisco IOS Release 12.2(28)SB, or a later release to configure named VPDN templates.

Restrictions

- An L2TP or Layer 2 Forwarding Protocol (L2F) tunnel must be established for the VPDN template settings to be used. Once a tunnel has been established, changes in the VPDN template settings will not have an effect on the tunnel until it is brought down and reestablished.
- Not all commands that are available for configuring a VPDN group can be used to configure a VPDN template. For a list of the commands that can be used in VPDN template configuration mode see the **vpdn-template** command documentation in the *Cisco IOS VPDN Command Reference*, Release 12.4T or use the **?** command in VPDN template configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-template** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-template** [*name*] **Example:** `Router(config)# vpdn-template l2tp`	Creates a VPDN template and enters VPDN template configuration mode.

What to Do Next

- You may configure VPDN group parameters in the VPDN template. For a complete list of the commands available in VPDN template configuration mode, refer to the **vpdn-template** command documentation in the *Cisco IOS VPDN Command Reference*, Release 12.4T or use the **?** command in VPDN template configuration mode.
- You may perform the optional task in the "Associating a VPDN Group with a VPDN Template" section.
- You may perform the optional task in the "Disassociating a VPDN Group from the VPDN Template" section.
- You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Associating a VPDN Group with a VPDN Template

VPDN groups are associated with the global VPDN template by default. Individual VPDN groups can be associated with a named VPDN template instead. Associating a VPDN group with a named VPDN template disassociates the VPDN group from the global VPDN template.

Perform this task on the NAS or the tunnel server to associate a specific VPDN group with a named VPDN template, or to reassociate a VPDN group with the global VPDN template if it has been previously disassociated from the global VPDN template.

Prerequisites

- You must be running Cisco IOS Release 12.2(8)T, Cisco IOS Release 12.2(28)SB, or a later release.
- A VPDN template must be enabled. To enable a named VPDN template, perform the task in the "Creating a VPDN Template" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **source vpdn-template** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group l2f`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**source vpdn-template** [*name*] **Example:** `Router(config-vpdn)# source vpdn-template l2tp`	Associates a VPDN group with a VPDN template. • VPDN groups are associated with the unnamed VPDN template by default. • If you have disassociated a VPDN group from the VPDN template using the **no source vpdn-template** command, you can reassociate it by issuing the **source vpdn-template** command. • (Cisco IOS Release 12.2(13)T, Cisco IOS Release 12.2(28)SB, and later releases) Associating a VPDN group with a named VPDN template disassociates it from the global VPDN template.

What to Do Next

- You may perform the optional task in the "Disassociating a VPDN Group from the VPDN Template" section.
- You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Disassociating a VPDN Group from the VPDN Template

Individual VPDN groups can be disassociated from the VPDN template if desired, allowing the system default settings to be used for any parameters not configured in the individual VPDN group.

Perform this task on the NAS or the tunnel server to disassociate a specific VPDN group from any VPDN template.

Prerequisites

You must be running Cisco IOS Release 12.2(8)T, Cisco IOS Release 12.2(28)SB, or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **no source vpdn-template** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group l2f`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**no source vpdn-template** [*name*] **Example:** `Router(config-vpdn)# no source vpdn-template l2tp`	Configures an individual VPDN group to use system default settings rather than the VPDN template settings for all unspecified parameters. • VPDN groups are associated with the unnamed VPDN template by default. Use the **no source vpdn-template** command to disassociate a VPDN group from its associated VPDN template. • If you have disassociated a VPDN group from the VPDN template using the **no source vpdn-template** command, you can reassociate it by issuing the **source vpdn-template** command.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring the VPDN Source IP Address

A tunnel endpoint can be configured with a source IP address that is different from the IP address used to open the VPDN tunnel. When a source IP address is configured on a tunnel endpoint, the router will generate VPDN packets labeled with the configured source IP address. Setting a source IP address may be required if the tunnel endpoints are managed by different companies and addressing requirements necessitate that a particular IP address be used.

The source IP address can be configured globally, or for individual VPDN groups. The VPDN group configuration will take precedence over the global configuration.

Perform one of the following tasks to configure a source IP address on a NAS or a tunnel server:

- Configuring the Global VPDN Source IP Address, page 251 (optional)
- Configuring the Source IP Address for a VPDN Group, page 252 (optional)

Configuring the Global VPDN Source IP Address

You may configure a single global source IP address on a device. If a source IP address is configured for a VPDN group, the global source IP address will not be used for tunnels belonging to that VPDN group.

Perform this task on a tunnel endpoint to configure the global source IP address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn source-ip** *ip-address*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn source-ip** *ip-address* **Example:** `Router(config)# vpdn source-ip 10.1.1.1`	Globally specifies an IP address that is different from the physical IP address used to open a VPDN tunnel.

What to Do Next

- You may configure a different source IP address for an individual VPDN group by performing the task in the "Configuring the Source IP Address for a VPDN Group" section.
- You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring the Source IP Address for a VPDN Group

You may configure a source IP address for a specific VPDN group. If a source IP address is configured for a VPDN group, the global source IP address will not be used for tunnels belonging to that VPDN group.

Perform this task on a tunnel endpoint to configure a source IP address for a specific VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **source-ip** *ip-address*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**source-ip** *ip-address* **Example:** `Router(config-vpdn)# source-ip 10.1.1.1`	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.

What to Do Next

- You may configure additional VPDN groups with unique source IP addresses.
- You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring VRF-Aware VPDN Tunneling

Prior to Cisco IOS Release 12.2(15)T and Cisco IOS Release 12.2(28)SB, you had to specify IP addresses from the global routing table for the endpoints of a VPDN tunnel. VRF-aware VPDN tunnels support VPDN tunnels that terminate on a VRF by allowing you to use IP addresses from a VRF routing table.

VRF-aware VPDN tunneling enhances the support of L2TP VPDNs by allowing VPDN tunnels to start outside an MPLS VPN and terminate within the MPLS VPN. For example, this feature allows you to use a VRF address from a customer VRF as the destination address.

For more information on remote access to MPLS VPNs, refer to the "Overview of Dial Access to MPLS VPN Integration" chapter of the *Cisco Remote Access to MPLS VPN Solution Overview and Provisioning Guide*, Release 2.0.

You can use VRF-aware VPDN tunnels with multihop, dial-in, and dial-out L2TP VPDN tunneling scenarios. In a multihop scenario, this feature is sometimes referred to as VRF-aware VPDN multihop.

VRF-aware VPDN tunneling can be configured locally on a NAS, tunnel server, or multihop tunnel switch, or it can be configured in the remote RADIUS server profile. Configuring VRF-aware VPDN tunneling in the RADIUS server profile will propagate the configuration only to a NAS or multihop tunnel switch. To configure VRF-aware VPDN tunnels on a tunnel server, you must configure the tunnel server locally.

Perform one of the following tasks to configure a VRF-aware VPDN tunnel:

- Configuring VRF-Aware VPDN Tunneling Locally, page 253 (optional)
- Configuring VRF-Aware VPDN Tunneling on the Remote RADIUS AAA Server, page 254 (optional)

Configuring VRF-Aware VPDN Tunneling Locally

VRF-aware VPDN tunneling can be configured locally on a NAS, a tunnel server, or a multihop tunnel switch. Configuring VRF-aware VPDN tunneling on a device specifies that the tunnel endpoint IP addresses configured for that VPDN group belong to the specified VRF routing table rather than the global routing table.

Perform this task on the multihop tunnel switch, the NAS, or the tunnel server to configure a VPDN tunnel to belong to a VRF.

Prerequisites

- You must be running Cisco IOS Release 12.2(15)T, Cisco IOS Release 12.2(28)SB, or a later release.
- A multihop, dial-in, or dial-out L2TP VPDN tunneling deployment must be configured.
- The source IP address and the destination IP address configured in the L2TP VPDN group must exist in the specified VPN.
- Because VRFs use Cisco Express Forwarding, you must configure Cisco Express Forwarding before performing this task. For information on configuring Cisco Express Forwarding, refer to the "Configuring Cisco Express Forwarding" part of the *Cisco IOS IP Switching Configuration Guide*, Release 12.4.

Restrictions

L2TP is the only tunneling protocol supported for VRF-aware VPDN tunneling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **vpn** {**vrf** *vrf-name* | **id** *vpn-id*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**vpn** {**vrf** *vrf-name* | **id** *vpn-id*} **Example:** `Router(config-vpdn)# vpn vrf myvrf`	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified VRF instance. • **vrf** *vrf-name*—Specifies the VRF instance by the VRF name. • **id** *vpn-id*—Specifies the VRF instance by the VPN ID.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring VRF-Aware VPDN Tunneling on the Remote RADIUS AAA Server

VRF-aware VPDN tunneling can be configured in the remote RADIUS server profile. Configuring VRF-aware VPDN tunneling on a device specifies that the tunnel endpoint IP addresses configured for that VPDN group belong to the specified VRF routing table rather than the global routing table.

Configuring VRF-aware VPDN tunneling in the RADIUS server profile will propagate the configuration only to a NAS or multihop tunnel switch. To configure VRF-aware VPDN tunnels on a tunnel server, you must configure the tunnel server locally by performing the task in the "Configuring VRF-Aware VPDN Tunneling Locally" section.

Perform this task on the remote RADIUS server. The tunnel attributes configured in the RADIUS server profile will be propagated to the NAS or multihop tunnel switch.

Prerequisites

- You must be running Cisco IOS Release 12.2(15)T, Cisco IOS Release 12.2(28)SB, or a later release.
- A multihop, dial-in, or dial-out L2TP VPDN tunneling deployment must be configured.
- The source IP address and the destination IP address configured in the L2TP VPDN group must exist in the specified VPN.
- Because VRFs use Cisco Express Forwarding, you must configure Cisco Express Forwarding before performing this task. For information on configuring Cisco Express Forwarding, refer to the "Configuring Cisco Express Forwarding" part of the *Cisco IOS IP Switching Configuration Guide*, Release 12.4.
- The NAS or tunnel switch must be configured for remote RADIUS AAA. Perform the tasks in the "Configuring AAA on the NAS and the Tunnel Server" and "Configuring Remote AAA for VPDNs" sections in the "Configuring AAA for VPDNs" module to configure the NAS for remote RADIUS AAA.
- The RADIUS server must be configured for AAA. For information on configuring remote RADIUS servers, refer to the *Cisco IOS Security Configuration Guide*, Release 12.4.

Restrictions

L2TP is the only tunneling protocol supported for VRF-aware VPDN tunneling.

SUMMARY STEPS

1. **Cisco-Avpair = vpdn:tunnel-id=***name*
2. **Cisco-Avpair = vpdn:tunnel-type=l2tp**
3. **Cisco-Avpair = vpdn:vpn-vrf=***vrf-name*
   or
   Cisco-Avpair = vpdn:vpn-id=*vpn-id*
4. **Cisco-Avpair = vpdn:l2tp-tunnel-password=***secret*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Cisco-Avpair = vpdn:tunnel-id=***name* **Example:** `Cisco-Avpair = vpdn:tunnel-id=test`	Specifies the tunnel ID in the RADIUS user profile.
Step 2	**Cisco-Avpair = vpdn:tunnel-type=l2tp** **Example:** `Cisco-Avpair = vpdn:tunnel-type=l2tp`	Specifies L2TP as the tunneling protocol in the RADIUS user profile.

	Command or Action	Purpose

Step 3	**Cisco-Avpair = vpdn:vpn-vrf=***vrf-name*
	
	or
	
	Cisco-Avpair = vpdn:vpn-id=*vpn-id*
	
	Example:
	`Cisco-Avpair = vpdn:vpn-vrf=myvrf`
	
	or
	
	`Cisco-Avpair = vpdn:vpn-id=A1:3F6C`
		Specifies the VRF instance that the VPDN tunnel should be associated with using the VRF name in the RADIUS user profile.
		
		or
		
		Specifies the VRF instance that the VPDN tunnel should be associated with using the VPN ID in the RADIUS user profile.

Step 4	**Cisco-Avpair = vpdn:l2tp-tunnel-password=***secret* **Example:** `Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco`	Specifies the L2TP tunnel password in the RADIUS user profile.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Performing MTU Tuning for L2TP VPDNs

MTU tuning reduces or prevents packet fragmentation and reassembly of L2TP packets in a VPDN deployment. Because the tunnel server is typically the device that aggregates large numbers of sessions and traffic flows in a VPDN deployment, the performance impact of the process switching required for packet fragmentation and reassembly is most dramatic, and least desirable, on this device.

A number of different methods are available to perform MTU tuning. The goal is to prevent fragmentation of packets after they have been encapsulated for tunneling. In Cisco IOS Release 12.2(4)T and later releases, the most reliable method of MTU tuning is manually configuring the advertised TCP MSS.

Perform one of the following tasks to perform MTU tuning:

- Manually Configuring the IP MTU for VPDN Deployments, page 256 (optional)
- Enabling Automatic Adjustment of the IP MTU for VPDN Deployments, page 257 (optional)
- Enabling Path MTU Discovery for VPDNs, page 259 (optional)
- Manually Configuring the Advertised TCP MSS, page 261 (optional)
- Configuring MRU Advertising, page 262 (optional)

Manually Configuring the IP MTU for VPDN Deployments

One method for reducing the amount of fragmentation of tunneled packets is to manually configure the IP MTU to the largest IP packet size that will not exceed the path MTU between the NAS and the tunnel server once the full Layer 2 header is added to the packet.

Perform this task on the tunnel server to lower the IP MTU manually.

Prerequisites

- An L2TP VPDN deployment must be configured.
- The path MTU between the NAS and the tunnel server should be known.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip mtu** *bytes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
Step 4	**ip mtu** *bytes* **Example:** `Router(config-if)# ip mtu 1460`	Sets the MTU size of IP packets sent on an interface. **Note** Because Layer 2 headers are 40 bytes, the recommended value for the *bytes* argument is 1460.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Enabling Automatic Adjustment of the IP MTU for VPDN Deployments

A tunnel server can be configured to automatically adjust the IP MTU of an interface to compensate for the size of the Layer 2 header. The automatic adjustment corrects for the size of the Layer 2 header based on the MTU of the egress interface of that device. This configuration is effective in preventing fragmentation only when the MTU of that interface is the same as that of the path MTU.

Perform this task on the tunnel server to enable automatic adjustment of the IP MTU.

Prerequisites

- A VPDN deployment must be configured.
- You must be running Cisco IOS Release 12.2(3), Cisco IOS Release 12.2(4)T, or a later release to control automatic adjustment of the IP MTU.

Restrictions

- Automatic adjustment of the IP MTU was introduced in Cisco IOS Release 12.1(5)T, and is enabled by default. No mechanism is available to disable it in releases prior to Cisco IOS Release 12.2(3) and 12.2(4)T.
- The **ip mtu adjust** command was introduced in Cisco IOS Release 12.2(3) and 12.2(4)T. The **no** form of this command can be used to disable automatic adjustment of the IP MTU.
- In Cisco IOS Release 12.2(6) and 12.2(8)T, the default was changed so that automatic adjustment of the IP MTU is disabled.
- The IP MTU is automatically adjusted only if there is no IP MTU configured manually on the virtual template interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip mtu adjust**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**ip mtu adjust** **Example:** `Router(config-vpdn)# ip mtu adjust`	Enables automatic adjustment of the IP MTU on a virtual access interface.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Enabling Path MTU Discovery for VPDNs

If the path MTU between the NAS and the tunnel server is variable or unknown, PMTUD can be enabled for VPDNs. PMTUD uses the DF bit in the IP header to dynamically discover the smallest MTU among all the interfaces along a routing path.

When PMTUD is enabled, VPDN deployments are vulnerable to DoS attacks that use crafted ICMP messages to set a connection's path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack.

To protect against a throughput-reduction attack, configure a range of acceptable values for the path MTU. If the device receives an ICMP message that advertises a next-hop path MTU that falls outside the configured size range, the device will ignore the message.

For more information on throughput-reduction attacks and for information on detecting a PMTUD attack on an L2TP VPDN deployment, see the Cisco Security Advisory *Crafted ICMP Messages Can Cause Denial of Service*.

PMTUD may fail when performed over the Internet, because some routers or firewalls are configured to filter out all ICMP messages. When the source host does not receive an ICMP Destination Unreachable message from a device that is unable to forward a packet without fragmentation, it will not know to reduce the packet size. The source host will continue to retransmit the same large packet. Because the DF bit is set, these packets will be continually dropped because they exceed the path MTU, and the connection will stop responding entirely.

Perform this task on the tunnel server to enable PMTUD and to protect the L2TP VPDN deployment against throughput-reduction DoS attacks.

Prerequisites

- A VPDN deployment must be configured.
- You must be running Cisco IOS Release 12.2(4)T or a later release.
- You must be running Cisco IOS Release 12.2(11)T or a later release on the Cisco 1760 modular access router, the Cisco AS5300 series universal gateways, the Cisco AS5400 series universal gateways, and the Cisco AS5800 series universal gateways.
- To protect against a DoS throughput-reduction attack, you must be running a version of Cisco IOS software that supports the **vpdn pmtu** command. The following maintenance releases of Cisco IOS software support the **vpdn pmtu** command:
  - Cisco IOS Release 12.3(25) and later releases
  - Cisco IOS Release 12.3(14)T and later releases
  - Cisco IOS Release 12.2(28)SB and later releases

  For a complete list of Cisco IOS software rebuild releases that support the **vpdn pmtu** command, refer to the Cisco Security Advisory *Crafted ICMP Messages Can Cause Denial of Service*.

Note Some Cisco IOS software releases remain vulnerable to throughput-reduction DoS attacks when PMTUD is enabled. The only way to protect against DoS attacks when running these versions of the Cisco IOS software is to disable PMTUD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip pmtu**
5. **exit**
6. **vpdn pmtu maximum** *bytes*
7. **vpdn pmtu minimum** *bytes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**ip pmtu** **Example:** `Router(config-vpdn)# ip pmtu`	Enables the discovery of a path MTU for Layer 2 traffic.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

	Command or Action	Purpose
Step 6	**vpdn pmtu maximum** *bytes* **Example:** `Router(config)# vpdn pmtu maximum 1460`	Manually configures the maximum allowed path MTU size, in bytes, for an L2TP VPDN.
Step 7	**vpdn pmtu minimum** *bytes* **Example:** `Router(config)# vpdn pmtu minimum 576`	Manually configures the minimum allowed path MTU size, in bytes, for an L2TP VPDN.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Manually Configuring the Advertised TCP MSS

Manually configuring a lower value for the advertised TCP MSS reduces the size of IP packets created by TCP at the transport layer, reducing or eliminating the amount of packet fragmentation that will occur in a VPDN deployment.

The default advertised TCP MSS is 1460, which allows room for the 40-byte TCP/IP header. To prevent packet fragmentation over a tunnel, additionally reduce the TCP MSS to provide space for the Layer 2 encapsulation header.

Perform this task on the tunnel server to manually lower the TCP MSS.

Prerequisites

- A VPDN deployment must be configured.
- You must be running Cisco IOS Release 12.2(4)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip tcp adjust-mss** *max-segment-size*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
Step 4	**ip tcp adjust-mss** *max-segment-size* **Example:** `Router(config-if)# ip tcp adjust-mss 1420`	Adjusts the MSS value of TCP SYN packets going through a router. **Note** Because Layer 2 headers are 40 bytes, the recommended value for the *bytes* argument is 1420.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring MRU Advertising

You can manually configure a lower MTU on the virtual template interface to compensate for the size of the Layer 2 header. The MTU of the interface is advertised to PPP peers as the MRU. If the peer is running a PPP client that is capable of listening to this advertisement, it can adjust its MTU (and indirectly its IP MTU) for that PPP link. This in turn modifies the TCP MSS that the peer advertises when opening up TCP connections.

Because the default MTU for an interface is 1500 bytes, the default MRU is 1500 bytes. Setting the MTU of an interface to 1460 changes the advertised MRU to 1460. This configuration would tell the peer to allow room for a 40-byte Layer 2 header.

Perform this task on the tunnel server to manually lower the MTU of the virtual template interface.

Prerequisites

- A VPDN deployment must be configured.
- You must be running Cisco IOS Release 12.2(4)T or a later release.

Restrictions

- MRU negotiation must be supported on the PPP client. One known client that supports MRU negotiations is the Windows XP PPP client. Other commonly deployed PPP clients do not adhere to the advertised PPP MRU as they should. Refer to the PPP client documentation to determine if your PPP client properly responds to the advertised PPP MRU.

- Changing the MTU value for an interface with the **mtu** command can affect the value of the **ip mtu** command. The value specified with the **ip mtu** command may not be greater than the value specified with the **mtu** command. If you change the value for the **mtu** command and the new value would result in an **ip mtu** value that is higher than the new **mtu** value, the **ip mtu** value automatically changes to match the new value configured with the **mtu** command. Changing the value of the **ip mtu** commands has no effect on the value of the **mtu** command.
- If proxy Link Control Protocol (LCP) is running, LCP renegotiation must take place because the MRU option is set during LCP negotiations. To force LCP renegotiation, configure the **lcp renegotiation** command for the VPDN group.
- If the MTU is manually lowered for a tunnel server that communicates with a mixture of devices that do and do not listen to MRU advertising, those devices that do not listen may encounter the PMTUD issues discussed in the "Enabling Path MTU Discovery for VPDNs" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **mtu** *bytes*
5. **exit**
6. **vpdn-group** *name*
7. **lcp renegotiation** {**always** | **on-mismatch**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1460`	Adjusts the maximum packet size or MTU size. **Note** Because Layer 2 headers are 40 bytes, the recommended value for the *bytes* argument is 1460.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.

	Command or Action	Purpose
Step 6	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	(Optional) Creates a VPDN group and enters VPDN group configuration mode.
Step 7	**lcp renegotiation** {**always** | **on-mismatch**} **Example:** `Router(config-vpdn)# lcp renegotiation always`	(Optional) Allows the tunnel server to renegotiate the PPP LCP on dial-in calls.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuring QoS Packet Classifications for VPDNs

QoS packet classification provides the capability to partition network traffic into multiple priority levels or classes of service. Packet classifications provide the information required to coordinate QoS from end to end within and between networks.

In a VPDN deployment, IP packets may be classified by an external source such as the customer network or a downstream client. By default, a tunnel endpoint will set the ToS byte in the Layer 2 header to zero, specifying normal service. Depending on the VPDN deployment, instead of using the default setting you may choose to configure your VPDN network to preserve QoS end to end by copying the contents of the ToS byte from the IP header to the Layer 2 header, or to manually configure custom packet classifications for the VPDN network.

QoS configurations are generally required only on the tunnel server, the device that must manage and prioritize large volumes of outbound traffic.

Perform the following task if you choose to preserve end-to-end QoS:

- Configuring Preservation of QoS Classifications in the ToS Byte, page 264 (optional)

Perform either or both of these tasks to manually configure custom packet classifications for your VPDN deployment:

- Manually Configuring the IP Precedence for VPDNs, page 266 (optional)
- Manually Configuring the ToS for VPDN Sessions, page 267 (optional)

Configuring Preservation of QoS Classifications in the ToS Byte

When Layer 2 packets are created the ToS byte value is set to zero by default, indicating normal service. This setting ignores the values of the ToS byte of the encapsulated IP packets that are being tunneled. The tunnel server can be configured to copy the contents of the ToS field of the inner IP packets to the ToS byte of the Layer 2 header. Copying the ToS field from the IP header to the Layer 2 header preserves end-to-end QoS for tunneled packets.

Perform this task to configure a tunnel server to copy the ToS byte from the IP packet to the Layer 2 header.

Prerequisites

A VPDN deployment must be configured.

Restrictions

- The tunneled link must carry IP packets for the ToS field to be preserved.
- Proxy PPP dial-in is not supported.
- The tunneled link must carry IP for the ToS field to be preserved. The encapsulated payload of Multilink PPP (MLP) connections is not IP, therefore this task has no effect when MLP is tunneled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip tos reflect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group or associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.
Step 4	**ip tos reflect** **Example:** `Router(config-vpdn)# ip tos reflect`	Configures a VPDN group to copy the ToS byte value of IP packet to the Layer 2 header.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Manually Configuring the IP Precedence for VPDNs

IP precedence bits of the ToS byte can be manually configured to set a CoS for Layer 2 packets. If you choose to manually configure a specific IP precedence value for Layer 2 packets, QoS will not be preserved end to end across the tunnel.

Perform this task on the tunnel server to manually configure a CoS for Layer 2 packets.

Prerequisites

A VPDN deployment must be configured.

Restrictions

Manual configuration of an IP precedence value will override the configuration of the **ip tos reflect** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip precedence** [*number* | *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group or associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.
Step 4	**ip precedence** [*number* | *name*] **Example:** `Router(config-vpdn)# ip precedence 1`	Sets the precedence value in the VPDN Layer 2 encapsulation header.

What to Do Next

- You may perform the optional task in the "Manually Configuring the ToS for VPDN Sessions" section.
- You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Manually Configuring the ToS for VPDN Sessions

The ToS bits can be manually configured to mark the ToS of a packet. If you choose to manually configure a specific ToS value for Layer 2 packets, QoS will not be preserved end-to-end across the tunnel.

Perform this task on the tunnel server to manually configure a CoS for Layer 2 packets.

Prerequisites

A VPDN deployment must be configured.

Restrictions

Manual configuration of a ToS value will override the configuration of the **ip tos reflect** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip tos** {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group or associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.
Step 4	**ip tos** {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} **Example:** `Router(config-vpdn)# ip tos 9`	Sets the ToS bits in the VPDN Layer 2 encapsulation header.

What to Do Next

You may perform any of the relevant optional tasks in this module or the "VPDN Tunnel Management" module.

Configuration Examples for Additional VPDN Features

This section contains the following configuration examples:

Configuring a Basic Dial-Out VPDN: Examples

The following example enables VPDN, configures a tunnel server to request dial-out VPDN tunnels for outbound PPP calls, and configures the dialer interface to place outbound calls using the VPDN tunnel:

```
vpdn enable
vpdn-group out
 request-dialout
 protocol l2tp
 pool-member 1
!
 initiate-to ip 10.10.10.1
 local name tunnelserver32
!
interface dialer 1
 ip address 10.1.1.1 255.255.0
 encapsulation ppp
 dialer remote-name router22
 dialer string 5550100
 dialer vpdn
 dialer pool 1
 dialer-group 1
 ppp authentication chap
```

The following example enables VPDN, configures a NAS to accept dial-out VPDN tunnel requests, and configures a dialer interface on the NAS to place outbound calls to the PPP client:

```
vpdn enable
vpdn-group 1
 accept-dialout
 protocol l2tp
 dialer 3
!
 terminate-from hostname tunnelserver32
!
interface dialer 3
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer in-band
 dialer aaa
 dialer-group 3
 ppp authentication chap
```

Configuring L2TP Dial-Out Load Balancing: Example

The following example configures a preexisting dial-out VPDN group on a tunnel server to load balance calls across multiple NASs. Calls will be load balanced between the NASs because the same priority value has been assigned to each NAS with the **initiate-to** command:

```
vpdn-group 1
 initiate-to ip 10.0.58.201 priority 10
 initiate-to ip 10.0.58.205 priority 10
 initiate-to ip 10.0.58.207 priority 10
 initiate-to ip 10.0.58.209 priority 10
```

Configuring L2TP Dial-Out Failover Redundancy: Example

The following example configures a preexisting dial-out VPDN group on a tunnel server for failover between multiple NASs. If the NAS with the highest priority goes down, the tunnel server will fail over to a NAS with a lower priority. The highest priority value you can assign is 1.

```
vpdn-group 1
 initiate-to ip 10.0.58.201 priority 1
 initiate-to ip 10.0.58.205 priority 10
 initiate-to ip 10.0.58.209 priority 15
```

L2TP Dial-Out Failover Redundancy with Tunnel Timers: Example

The following example configures a preexisting dial-out VPDN group on a tunnel server for failover using custom L2TP tunnel timers. The tunnel server is configured to retry to connect to a NAS five times, with a minimum wait of 10 seconds between attempts. If the tunnel server is not able to connect to the highest priority NAS after the specified number of retries, failover to the next highest priority NAS will occur. The tunnel server will not attempt to recontact the highest priority NAS until 420 seconds have passed.

```
vpdn-group 1
 initiate-to ip 10.0.58.201 priority 1
 initiate-to ip 10.0.58.207 priority 50
 initiate-to ip 10.0.58.205 priority 100
 l2tp tunnel retransmit initial retries 5
 l2tp tunnel retransmit initial timeout min 10
 l2tp tunnel busy timeout 420
```

Configuring IPSec Protection of a NAS-Initiated L2TP Tunnel: Example

The following example configures IPSec protection of L2TP tunnels on the NAS and the tunnel server for a NAS-initiated tunneling scenario:

NAS Configuration

```
! Passwords for the L2TP tunnel authentication
username NAS password 0 cisco
username TS1 password 0 cisco
!
! VPDN configuration to tunnel users with the domain cisco.com to the LNS. This
! configuration has l2tp tunnel authentication enabled.
!
vpdn enable
vpdn-group 1
 request-dialin
 protocol l2tp
 domain cisco.com
!
 initiate-to ip 10.0.0.13
 local name NAS
 l2tp security crypto-profile l2tp keep-sa
 l2tp tunnel password cisco
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key cisco address 10.0.0.13
!
```

```
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
! Crypto profile configuration which is bound to the vpdn-group shown above
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set esp-des-sha-transport
!
interface FastEthernet0/0
 ip address 10.0.0.12 255.255.255.0
 crypto map l2tpsec
```

Tunnel Server Configuration

```
! PPP client username and password needed for CHAP authentication
username userSerial10@cisco.com password 0 cisco
!
! Passwords for the L2TP tunnel authentication
username NAS password 0 cisco
username TS1 password 0 cisco
!
! Using address pool to assign client an IP address
ip address-pool local
!
! VPDN configuration
vpdn enable
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
!
 terminate-from hostname NAS
 lcp renegotiation on-mismatch
 l2tp security crypto-profile l2tp keep-sa
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.0.0.12
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set esp-des-sha-transport
!
interface FastEthernet0/0
 ip address 10.0.0.13 255.255.255.0
 speed 10
 half-duplex
 crypto map l2tpsec
```

Configuring IPSec Protection of a Client-Initiated L2TP Tunnel: Example

The following example configures IPSec protection of L2TP tunnels on the tunnel server for a client-initiated tunneling scenario:

```
! PPP client username and password needed for CHAP authentication
username userSerial10@cisco.com password 0 cisco
! Passwords for the L2TP tunnel authentication.
username NAS password 0 cisco
username TS1 password 0 cisco
!
```

```
! Using address pool to assign client an IP address
ip address-pool local
!
! VPDN configuration
vpdn enable
vpdn-group dial-in
 accept-dialin
 protocol l2tp
 virtual-template 1
!
 l2tp security crypto-profile l2tp
 no l2tp tunnel authentication
ip pmtu
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set esp-des-sha-transport
 set security-association lifetime seconds 120
!
interface FastEthernet0/0
 ip address 10.0.0.13 255.255.255.0
 speed 10
 half-duplex
 crypto map l2tpsec
```

Configuring a Global VPDN Template: Example

The following example configures two VPDN parameters in the unnamed global VPDN template:

```
vpdn-template
 local name host43
 ip tos reflect
```

Configuring a Named VPDN Template: Example

The following example configures two VPDN parameters in a VPDN template named l2tp. The named VPDN template is associated with the VPDN group named l2tp_tunnels.

```
vpdn-template l2tp
 l2tp tunnel busy timeout 65
 l2tp tunnel password tunnel4me
!
vpdn-group l2tp_tunnels
 source vpdn-template l2tp_tunnels
```

Disassociating a VPDN Group from the VPDN Template: Example

The following example disassociates the VPDN group named l2f from the VPDN template. The system default settings will be used for all VPDN parameters that are not specified in the VPDN group configuration.

```
vpdn-group l2f
 no source vpdn-template
```

Configuring a Global VPDN Source IP Address: Example

The following example configures a global source IP address. This source IP address will be used for all tunnels established on the router unless a specific source IP address is configured for a VPDN group.

```
vpdn source-ip 10.1.1.1
```

Configuring a Source IP Address for a VPDN Group: Example

The following example configures a source IP address for tunnels associated with the VPDN group named tunneling. This source IP address will override any configured global source IP address for tunnels associated with this VPDN group.

```
vpdn-group tunneling
 source-ip 10.1.1.2
```

Configuring VRF-Aware VPDN Tunnels Locally: Example

The following example configures a multihop tunnel switch to connect a NAS to a remote tunnel server within a VRF:

NAS

```
interface loopback 0
 ip address 172.16.45.6 255.255.255.255
!
vpdn enable
vpdn-group group1
 request-dialin
 protocol l2tp
 domain cisco.com
!
 initiate-to 10.10.104.9
 local name nas32
 source-ip 172.16.45.6
 l2tp tunnel password secret1
```

Multihop Tunnel Switch

```
ip vrf cisco-vrf
 vpn id A1:3F6C
!
interface loopback 0
 ip address 10.10.104.22 255.255.255.255
!
interface loopback 40
 ip vrf forwarding cisco-vrf
 ip address 172.16.40.241 255.255.255.255
!
vpdn enable
vpdn multihop
!
vpdn-group mhopin
 accept-dialin
 protocol l2tp
 virtual-template 4
!
```

```
 terminate-from hostname nas32
 source-ip 10.10.104.9
 l2tp tunnel password secret1
!
vpdn-group mhopout
 request-dialin
 protocol l2tp
 domain cisco.com
!
 vpn vrf cisco-vrf
 initiate-to ip 172.16.45.6
 source-ip 172.16.40.241
 local name multihop-tsw25
 l2tp tunnel password secret2
```

Tunnel Server

```
interface loopback 0
 ip address 172.16.45.6 255.255.255.255
!
vpdn enable
vpdn-group cisco
 accept-dialin
 protocol l2tp
 virtual-template 1
!
 terminate-from hostname multihop-tsw25
 source-ip 172.16.45.6
 local name ts-12
 l2tp tunnel password secret2
```

Configuring VRF-Aware VPDN Tunnels on the Remote RADIUS AAA Server: Examples

The following examples configure VRF-aware VPDN tunnels for a service provider network. The AAA RADIUS server user profile defines VPDN tunnel attributes, which can propagate to multiple NASs or tunnel switches.

RADIUS User Profile—VRF Name

The following example specifies that the source and destination IP addresses belong to the VPN named vpn-first:

```
cisco.com Password = "secret"
      Service-Type = Outbound-User,
      cisco-avpair = "vpdn:tunnel-id=LAC",
      cisco-avpair = "vpdn:tunnel-type=l2tp",
      cisco-avpair = "vpdn:ip-addresses=10.0.0.1",
      cisco-avpair = "vpdn:source-ip=10.0.0.9",
      cisco-avpair = "vpdn:vpn-vrf=vpn-first"
      cisco-avpair = "vpdn:l2tp-tunnel-password=supersecret"
```

RADIUS User Profile—VRF ID

The following example specifies that the source and destination IP addresses belong to the VPN with the ID A1:3F6C:

```
cisco.com Password = "secret"
      Service-Type = Outbound-User,
      cisco-avpair = "vpdn:tunnel-id=LAC",
      cisco-avpair = "vpdn:tunnel-type=l2tp",
```

```
cisco-avpair = "vpdn:ip-addresses=10.0.0.1",
cisco-avpair = "vpdn:source-ip=10.0.0.9",
cisco-avpair = "vpdn:vpn-id=A1:3F6C"
cisco-avpair = "vpdn:l2tp-tunnel-password=supersecret"
```

Manually Configuring the IP MTU for VPDN Deployments: Example

The following example manually configures an IP MTU of 1460 bytes for all tunnels that use the virtual-template named 1:

```
interface virtual-template 1
 ip mtu 1460
```

Enabling Automatic Adjustment of the IP MTU for VPDN Deployments: Example

The following example configures tunnels associated with the VPDN group named tunneler to automatically adjust the IP MTU based on the MTU of the egress interface of the device:

```
vpdn-group tunneler
 ip mtu adjust
```

Enabling Path MTU Discovery for VPDNs: Example

The following example enables PMTUD for the VPDN group named tunnelme and configures the device to accept path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
vpdn-group tunnelme
ip pmtu
!
vpdn pmtu maximum 1460
vpdn pmtu minimum 576
```

Manually Configuring the Advertised TCP MSS: Example

The following example manually configures a TCP MSS of 1420 bytes for all tunnels that use the virtual template named 2:

```
interface virtual-template 2
 ip tcp adjust-mss 1420
```

Configuring MRU Advertising: Example

The following example manually configures an MTU of 1460 bytes for all tunnels that use the virtual template named 3. The VPDN group named mytunnels is configured to perform LCP renegotiation because it uses proxy LCP.

```
interface virtual-template 3
 mtu 1460
!
vpdn-group mytunnels
 lcp renegotiation always
```

Configuring Preservation of QoS Classifications in the ToS Byte: Example

The following example configures preservation of the IP ToS field for an existing VPDN group named out1:

```
vpdn-group out1
 ip tos reflect
```

Manually Configuring the IP Precedence for VPDNs: Example

The following example manually configures an IP precedence value for an existing VPDN group named out2:

```
vpdn-group out2
 ip precedence priority
```

Manually Configuring the ToS for VPDN Sessions: Example

The following example manually configures a ToS classification for an existing VPDN group named out3:

```
vpdn-group out3
 ip tos 9
```

Where to Go Next

You may perform any of the relevant optional tasks in the "VPDN Tunnel Management" module.

Additional References

The following sections provide references related to additional L2TP VPDN features.

Related Documents

Related Topic	Document Title
VPDN technology overview	"VPDN Technology Overview"
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*, Release 12.4T
Information about PPP configurations	"PPP Configuration" part of the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*, Release 12.4T
Information about IP application configurations	*Cisco IOS IP Application Services Configuration Guide*, Release 12.4

Related Topic	Document Title
IP application commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*, Release 12.4
Information about MPLS VPNs	"Overview of Dial Access to MPLS VPN Integration" chapter of the *Cisco Remote Access to MPLS VPN Solution Overview and Provisioning Guide*, Release 2.0
Information about IPSec transform sets, crypto maps, and ISAKMP policies	"Implementing IPSec and IKE" part of the *Cisco IOS Security Configuration Guide*, Release 12.4
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*, Release 12.4T
Information about QoS configurations	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
QoS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4T
Information on MTU tuning for L2TP tunneling deployments	*MTU Tuning for L2TP*
Information on IP packet fragmentation and PMTUD	*IP Fragmentation and PMTUD*
Information on throughput-reduction DoS attacks	*Crafted ICMP Messages Can Cause Denial of Service*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1191	*Path MTU Discovery*
RFC 2341	*Cisco Layer Two Forwarding (Protocol) "L2F"*
RFC 2637	*Point-to-Point Tunneling Protocol (PPTP)*
RFC 2661	*Layer Two Tunneling Protocol "L2TP"*

RFCs	Title
RFC 2923	*TCP Problems with Path MTU Discovery*
RFC 3193	*Securing L2TP using IPsec*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Additional VPDN Features

Table 10 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the "VPDN Features Roadmap."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 10 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 10 Feature Information for Configuring Additional VPDN Features

Feature Name	Software Releases	Feature Configuration Information
L2TP Dial-Out Load Balancing and Redundancy	12.2(15)T 12.2(28)SB	This feature enables a tunnel server to dial out to multiple NASs. When the NAS with the highest priority goes down, it is possible for the tunnel server to fail over to another lower priority NAS. The tunnel server can also load balance sessions between multiple NASs that have the same priority settings. The following sections provide information about this feature: • L2TP Dial-Out Load Balancing and Redundancy, page 232 • Configuring the Tunnel Server to Request Dial-Out, page 232 The following command was modified by this feature: **initiate-to**.
L2TP Security	12.2(4)T 12.2(28)SB	This feature allows the security features of IP Security (IPSec) to protect the L2TP tunnel and the PPP sessions within the tunnel. In addition, the L2TP Security feature provides built-in keepalives and standardized interfaces for user authentication and accounting to authentication, authorization, and accounting (AAA) servers. The following sections provide information about this feature: • L2TP Security for the Protection of VPDN Tunnels, page 225 • Configuring L2TP Security for VPDN Tunnels, page 240 • Verifying IPSec Protection of L2TP VPDN Tunnels, page 244 The following commands were introduced or modified by this feature: **crypto map** (global IPSec), **ip pmtu**, **l2tp security crypto-profile**.

Table 10 Feature Information for Configuring Additional VPDN Features

Feature Name	Software Releases	Feature Configuration Information
VPDN Default Group Template	12.2(8)T 12.2(28)SB	This feature introduces the ability to configure global default values for VPDN group parameters in a VPDN template. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups. The following sections provide information about this feature: • VPDN Template, page 225 • Creating a VPDN Template, page 247 The following commands were introduced by this feature: **source vpdn-template**, **vpdn-template**.
VRF-Aware VPDN Tunnels	12.2(15)T 12.2(28)SB	This feature enhances the support of VPDN tunnels by allowing VPDN tunnels to start outside an MPLS VPN and terminate within the MPLS VPN. The following sections provide information about this feature: • VRF-Aware VPDN Tunnels, page 226 • Configuring VRF-Aware VPDN Tunneling, page 253 The following command was introduced by this feature: **vpn**.

This module first published October 31, 2005. Last updated May 10, 2006.