Configuring Additional VPDN Features

This module documents concepts and tasks associated with configuring additional virtual private dialup network (VPDN) features. These optional features are used in combination with a VPDN deployment, and require that a VPDN deployment is first configured:

- VPDN Template
- VPDN Source IP Address
- VRF-Aware VPDN Tunnels
- MTU Tuning for L2TP VPDN Tunnels
- QoS for VPDN Tunnels
- VPDN Group Selection

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Additional VPDN Features

VPDN Template

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.

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 might 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.

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

The VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP feature introduces support to make these RADIUS attributes VRF aware: attribute 22 (Framed-Route), a combination of attribute 8 (Framed-IP-Address) and attribute 9 (Framed-IP-Netmask), and the Cisco VSA route command. Thus, static IP routes can be applied to a particular VRF routing table rather than the global routing table.

VRF-Aware VPDN Tunnels

Prior to Cisco IOS XE Release 2.2, 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 (VRF) instance 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 and have overlapping IP addresses. For example, this feature allows you to use a VRF address from a customer VRF as the destination address.

Beginning with Cisco IOS XE Release 2.2, the VRF-Aware VPDN Tunnels feature adds support for L2TP on the LNS. The initiation and termination of tunnels in a VRF instance is supported on the Cisco ASR 1000 Series Aggregation Services Routers in both an LNS and Layer 2 Access Concentrator (LAC) environment.

You can use VRF-aware VPDN tunnels with multihop and dial-in 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 the 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 might 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 these sections:

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 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 "Additional References" section.

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 might 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. 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. To determine if your PPP client properly responds to the advertised PPP MRU, see the PPP client documentation.

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 might experience the PMTUD problems described in the MTU Tuning Using IP MTU Adjustments, on page 3. 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.

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 might 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 can 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.

These sections provide additional information on QoS options for VPDN deployments:

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.

VPDN Group Selection

The VPDN Group Selection feature allows configuration of multiple VPDN tunnels, between a LAC and LNS, with different VPDN group configurations.

The VPDN Group Selection feature introduces two new keys that allow an LNS to connect to multiple VPDN tunnels from the same LAC, and to bind to different VPDN groups that use a different VPDN template for customized configurations. These keys are:

- Destination IP address the L2TP Start-Control-Connection-Request (SCCRQ) was received on
- The virtual routing and forwarding (VRF) instance the SCCRQ was received on

The VPDN Group Selection feature allows the LAC to build VPDN tunnels to either different IP addresses or different VRFs.

Benefits of VPDN Group Selection

The VPDN Group Selection feature allows SPs to support multiple VPDN groups or tunnels between a LAC and LNS by using the new VPDN group selection keys destination IP address or VRF ID, in addition to the previously supported hostname selection key. The VPDN Group Selection feature enables SPs to provide customize configurations for each VPDN tunnel.

How to Configure Additional VPDN Features

Creating a VPDN Template

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

Note

- An L2TP 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, 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.

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.

Before you begin

- Create and enable the VPDN template. For details, see 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 l2tp`	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. • Associating a VPDN group with a named VPDN template disassociates it from the global VPDN template.

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.

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 l2tp`	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.

Configuring the VPDN Source IP Address

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

Configuring the Global VPDN Source IP Address

You can 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

	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 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.

Configuring the Source IP Address for a VPDN Group

You can 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

	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 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.

Configuring VRF-Aware VPDN Tunneling

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 these tasks to configure a VRF-aware VPDN tunnel:

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.

Before you begin

- 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.

Note 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.

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.

Before you begin

- 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.

- 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.

Note 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*
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.
Step 3	**Cisco-Avpair = vpdn:vpn-vrf=** *vrf-name* **Example:** or **Example:** **Cisco-Avpair = vpdn:vpn-id=** *vpn-id* **Example:** `Cisco-Avpair = vpdn:vpn-vrf=myvrf` **Example:** or	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.

	Command or Action	Purpose
	Example: `Cisco-Avpair = vpdn:vpn-id=A1:3F6C`	
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.

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. The most reliable method of MTU tuning is manually configuring the advertised TCP MSS.

Perform one of these tasks to perform MTU tuning:

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.

Before you begin

- 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:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
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.

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.

Before you begin

- A VPDN deployment must be configured.

Note

- Automatic adjustment of the IP MTU is disabled by default.
- 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.

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.

Caution 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. For more information on throughput-reduction attacks and for information on detecting a PMTUD attack on an L2TP VPDN deployment, see the "Additional References" section.

PMTUD might 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.

Before you begin

A VPDN deployment must be configured.

Note

- Cisco 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 software is to disable PMTUD.
- The software does not support the **vpdn pmtu** command to configure a range of acceptable values for the path MTU, which can help protect against a throughput-reduction attack.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **ip pmtu**
5. **exit**

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.

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.

Before you begin

A VPDN deployment must be configured.

SUMMARY STEPS

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

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.

Before you begin

A VPDN deployment must be configured.

Note

- 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. To determine if your PPP client properly responds to the advertised PPP MRU, see the PPP client documentation.
- 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 must 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 might 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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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.
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.

Configuring VPDN Group Selection

Configuring VPDN Group Selection Based on a Hostname

Use these steps to display the status of an LNS to determine if it is active.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **accept-dialin**

5. **protocol l2tp**
6. **terminate-from hostname** *hostname*
7. **exit**

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	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dialin VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**terminate-from hostname** *hostname* **Example:** `Router(config-vpdn-acc-in)# terminate-from hostname example`	Specify the hostname of the remote LAC or LNS that will be required when accepting a VPDN tunnel.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits VPDN accept dialin group configuration mode.

Configuring VPDN Group Selection Based on a Source IP Address

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **vpdn-group** *name*
4. **accept-dialin**
5. **protocol l2tp**
6. **source-ip** *ip-address*
7. **exit**

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	**accept-dialin** **Example:** `Router(config-vpdn)# accept dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dial-in VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**source-ip** *ip-address* **Example:** `Router(config-vpdn-acc-in)# source-ip 10.10.10.1`	Specifies a source IP addresses to which to map the destination IP addresses in subscriber traffic.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits a VPDN accept dialin group configuration mode.

Configuring VPDN Group Selection Based on VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **accept-dialin**
5. **protocol l2tp**
6. **vpn vrf** *vrf-name*
7. **exit**

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	**accept-dialin** **Example:** `Router(config-vpdn)# accept dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dial-in VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**vpn vrf** *vrf-name* **Example:** `Router(config-vpdn-acc-in)# vpn vrf myvrf`	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified Virtual Private Network (VPN) routing and VRF instance. • **vrf** *vrf-name* --Specifies the VRF instance by the VRF name.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config)# exit`	Exits accept dialin VPDN subgroup mode.

Displaying VPDN Group Selections

SUMMARY STEPS

1. **enable**
2. **show vpdn group-select**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn group-select** **Example:** `Router> show vpdn group-select`	Displays the information for the selected VPDN group.
Step 3	**exit** **Example:** `Router> exit`	Exits global configuration mode.

Configuring QoS Packet Classifications for VPDNs

Depending on the VPDN deployment, instead of using the default setting you can 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 this task if you choose to preserve end-to-end QoS:

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

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.

Before you begin

A VPDN deployment must be configured.

Note

- 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 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.

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.

Before you begin

A VPDN deployment must be configured.

Note 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 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.

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.

Before you begin

A VPDN deployment must be configured.

Note 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.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group 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.

Configuration Examples for Additional VPDN Features

Example Configuring a Global VPDN Template

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

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

Example Configuring a Named VPDN Template

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
```

Example Disassociating a VPDN Group from the VPDN Template

The following example disassociates the VPDN group named l2tp 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 l2tp
 no source vpdn-template
```

Example Configuring a Global VPDN Source IP Address

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
```

Example Configuring a Source IP Address for a VPDN Group

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
```

Example Configuring VRF-Aware VPDN Tunnels Locally

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
```

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

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"
```

Example Manually Configuring the IP MTU for VPDN Deployments

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
```

Example Enabling Automatic Adjustment of the IP MTU for VPDN Deployments

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
```

Example Manually Configuring the Advertised TCP MSS

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
```

Example Configuring MRU Advertising

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
```

Example Configuring Preservation of QoS Classifications in the ToS Byte

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

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

Example Manually Configuring the IP Precedence for VPDNs

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

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

Example Manually Configuring the ToS for VPDN Sessions

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

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

Configuration Examples for VPDN Group Selection

Example Configuring VPDN Group Selection Based on Hostname

The following example configuration shows a LAC-1 building a VPDN tunnel to an LNS, and the LNS would terminating the session on vpdn-group 1:

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
```

Example Configuring VPDN Group Selection Based on an IP Address

The following example configuration shows a LAC-1/LAC-2 building a VPDN tunnel to IP address 10.10.10.1, and the LNS terminating the session on vpdn-group 1. If an LAC-1/LAC-2 builds a VPDN tunnel to IP address 10.10.10.2, the LNS terminates the session on vpdn-group 2. Any source IP address match is optional.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
```

Example Configuring VPDN Group Selection Based on VRF

The following example configuration shows a LAC sending a SCCRQ on service-A, and the LNS terminating the tunnel on vpdn-group 1. When an LAC sends a SCCRQ on service-B, the LNS would terminate the tunnel on vpdn-group 2.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
```

Example Configuring VPDN Group Selection Based on a Hostname and IP Address

The following example configuration shows a LAC-1 building a VPDN tunnel to IP address 10.10.10.1, and the LNS terminating the session on vpdn-group 1. If LAC-1 builds a VPDN tunnel to IP address 10.10.10.2,

the LNS terminates the session on vpdn-group 2. If LAC-2 builds a VPDN tunnel to IP addresses 10.10.10.1 or 10.10.10.2, the LNS terminates the session on vpdn-group 3.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-2
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
```

Example Configuring VPDN Group Selection Based on Hostname and VRF

The following example configuration shows a LAC-1 sending an SCCRQ on vrf service-A with any destination IP address, and the LNS terminating the VPDN tunnel on vpdn-group 1. If LAC-1 sends an SCCRQ on vrf service-B with any destination IP address, the LNS terminates the VPDN tunnel on vpdn-group 2. If LAC-2 sends an SCCRQ on vrf service-B with any destination IP address, the LNS terminates the VPDN tunnel on vpdn-group 3.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-2
Router(config-vpdn-acc-in)# exit
```

Example Configuring VPDN Group Selection Based on an IP Address and VRF

The following example configuration shows a LAC-1/LAC-2 sending an SCCRQ on vrf service-A to destination IP address 10.10.10.1, and the LNS terminating the VPDN tunnel on vpdn-group 1. If LAC-1/LAC-2 sends

an SCCRQ on vrf service-A to destination IP address 10.10.10.2, the LNS terminates the VPDN tunnel on vpdn-group 2.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
Router(config-vpdn-acc-in)# exit
```

Example Configuring VPDN Group Selection Based on Hostname VRF and IP Address

The following example configuration shows a LAC-1 sending an SCCRQ on vrf service-A to destination IP address 10.10.10.1, and the LNS terminating the VPDN tunnel on vpdn-group 1. If LAC-1 sends an SCCRQ on vrf service-B to destination IP address 10.10.10.1, the LNS terminates the VPDN tunnel on vpdn-group 2.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
```

Examples Displaying VPDN Group Selection

The VPDN Group Selection feature allows you to display VPDN group information based in a source IP address, a hostname, or VFR.

For examples purposes, the following configuration will be used for the display examples.

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group vgdefault
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 20
```

```
Router(config-vpdn-acc-in)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.2
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.3
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0
 example

Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in) # protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts1
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts1-ip2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts1
Router(config-vpdn)# source-ip 10.1.1.2
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# end
```

Examples Displaying VPDN Group-Select Summaries

The following example shows VPDN group-select information for the example configuration.

```
Router# show vpdn group-select summary
VPDN Group     Vrf    Remote Name     Source-IP     Protocol     Direction
vg-ip2            10.1.1.2     l2tp     accept-dialin
vg-ip3            10.1.1.3     l2tp     accept-dialin
vg-lts        lts     0.0.0.0     l2tp     accept-dialin
vg-lts1        lts1    0.0.0.0     l2tp     accept-dialin
vg-lts1-ip2     vfr101   lts1     10.1.1.2     l2tp     accept-dialin
vgdefault            0.0.0.0     l2tp     accept-dialin
```

The following is sample output from the **show vpdn group-select keys** command for a host with the name lac-1 and an IP address of 10.0.0.1:

```
Router# show vpdn group-select keys vrf vrf-blue hostname lac-1 source-ip 10.0.0.1
VPDN Group       Vrf        Hostname   Source Ip
vg1              vrf-blue   lac-1      10.0.0.1
```

The following shows an example output for the **show vpdn group-select default** command for the example configuration:

```
Router# show vpdn group-select default
Default VPDN Group       Protocol
vgdefault       l2tp
None       pptp
```

The following is sample output from the **show vpdn group-select keys**command for a host with the name lac-5 and an IP address of 10.1.1.0, and VRF name vrf-red:

```
Router# show vpdn group-select keys vrf vrf-red hostname lac-5 source-ip 10.1.1.0
VPDN Group    Vrf        Hostname    Source Ip
Vg2           vrf-red    lac-5         10.1.1.0
```

Where to Go Next

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
VPDN technology overview	*VPDN Technology Overview*
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Information about QoS classification	Classification Overview module
QoS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Information on MTU tuning for L2TP tunneling deployments	MTU Tuning for L2TP

Related Topic	Document Title
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

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 1191	*Path MTU Discovery*
RFC 2661	*Layer Two Tunneling Protocol (L2TP)*
RFC 2923	*TCP Problems with Path MTU Discovery*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Additional VPDN Features

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Additional VPDN Features

Feature Name	Software Releases	Feature Configuration Information
VPDN Default Group Template	Cisco IOS XE Release 2.1	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 commands were introduced by this feature: **source vpdn-template** and **vpdn-template**.
VPDN Group Selection	Cisco IOS XE Release 2.1	This feature configures customized, multiple VPDN tunnels with different VPDN group configurations between a LAC and an LNS. The following command were introduced by this feature: **show vpdn group-select**and **show vpdn group-select keys.**
VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP	Cisco IOS XE Release 2.1	This feature introduces support to make the following RADIUS attributes VRF aware: attribute 22 (Framed-Route), a combination of attribute 8 (Framed-IP-Address) and attribute 9 (Framed-IP-Netmask), and the Cisco VSA route command. Thus, static IP routes can be applied to a particular VRF routing table rather than the global routing table.
VRF-Aware VPDN Tunnels	Cisco IOS XE Release 2.2	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 command was introduced by this feature: **vpn**.