VPDN Configuration Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
# CONTENTS

## CHAPTER 1

Read Me First 1

## CHAPTER 2

VPDN Technology Overview 3
- Finding Feature Information 3
- Information About VPDNs 3
  - Overview of VPDN Technology 3
  - VPDN Terminology 5
    - VPDN Hardware Devices 5
    - VPDN Tunnels 6
    - VPDN Sessions 6
  - VPDN Architectures 6
    - Client-Initiated Dial-In VPDN Tunneling 6
    - NAS-Initiated Dial-In VPDN Tunneling 7
    - Multihop VPDN Tunneling 8
      - VPDN Tunneling to an MMP Stack Group 8
      - Tunnel Switching VPDNs 9
  - VPDN Tunneling Protocols 10
    - L2TP 10
    - L2TPv3 14
  - VPDN Group Configuration Modes 14
- Where to Go Next 14
- Additional References 15
- Feature Information for VPDN Technology Overview 16

## CHAPTER 3

Configuring AAA for VPDNs 19
- Finding Feature Information 19
- Prerequisites for Configuring AAA for VPDNs 19
- Information About AAA for VPDNs 20
Contents

VPDN Tunnel Authorization Search Order 20
  VPDN Tunnel Lookup Based on Domain Name 20
  VPDN Tunnel Lookup Based on DNIS Information 20
  VPDN Tunnel Lookup Based on Both Domain Name and DNIS Information 20
  VPDN Tunnel Lookup Based on the Multihop Hostname 21
Per-User VPDN AAA 21
  VPDN Authorization for Directed Request Users 21
  Domain Name Prefix and Suffix Stripping 21
VPDN Tunnel Authentication 22
  RADIUS Tunnel Accounting for L2TP VPDNs 22
  VPDN-Specific Remote RADIUS AAA Server Configurations 23
L2TP Forwarding of PPPoE Tagging Information 23
  DSL Sync-Rate VSAs 25
LNS Address Checking 26
  Benefits of LNS Address Checking 26
  LNS Address Checking Using a RADIUS Server 26
  Debugging Dropped Control Packets 27
Modified LNS Dead-Cache Handling 27
How to Configure AAA for VPDNs 27
  Enabling VPDN on the NAS and the Tunnel Server 27
  Configuring the VPDN Tunnel Authorization Search Order 28
Configuring per-User VPDN on the NAS 29
  Prerequisites 29
  Restrictions 29
  Configuring Global per-User VPDN 29
  Configuring per-User VPDN for a VPDN Group 30
Configuring AAA on the NAS and the Tunnel Server 32
Configuring Remote AAA for VPDNs 33
  Configuring the NAS for Remote AAA for Dial-In VPDNs 34
    What to Do Next 36
  Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels 36
    What to Do Next 38
Verifying and Troubleshooting Remote AAA Configurations 39
  Verifying that the VPDN Tunnel Is Up 39
  Verifying the Remote RADIUS AAA Server Configuration 39
Verifying the Remote TACACS+ AAA Server Configuration on the NAS
Verifying the Remote TACACS+ AAA Server Configuration on the Tunnel Server
Verifying L2TP Tunnel Establishment PPP Negotiations and Authentication with the Remote Client
Configuring Directed Request Authorization of VPDN Users
Configuring Directed Request Authorization of VPDN Users on the Tunnel Server
What to Do Next
Configuring Directed Request Authorization of VPDN Users on the NAS
What to Do Next
Configuring Domain Name Prefix and Suffix Stripping
What to Do Next
Configuring VPDN Tunnel Authentication
Prerequisites
Configuring VPDN Tunnel Authentication Using the Hostname
What to Do Next
Configuring VPDN Tunnel Authentication Using the Local Name
What to Do Next
Configuring VPDN Tunnel Authentication Using the L2TP Tunnel Password
What to Do Next
Disabling VPDN Tunnel Authentication for L2TP Tunnels
Configuring RADIUS Tunnel Accounting for L2TP VPDNs
Configuring Authentication of L2TP Tunnels at the Tunnel Terminator Remote RADIUS AAA Server
Configuring Tunnel Assignments on the NAS Remote RADIUS AAA Server
Configuring Secure Tunnel Authentication Names on the NAS Remote RADIUS AAA Server
Configuring L2TP Forwarding of PPPoE Tagging Information
Configuring L2TP Forwarding of the PPPoE Tagging Information
Overriding L2TP Forwarding of PPPoE Tag Information
Overriding nas-port VSA with circuit-id
Overriding calling-station-id VSA with remote-id
Removing L2TP Forwarding of PPPoE Tag Information
Displaying the Session Activity Log
Configuring L2TP Override Forwarding rx-speed and tx-speed Values Received from PPPoE
Prerequisites for Configuring a Multihop Tunnel Switch 125

Enabling Multihop VPDN on the Tunnel Switch 125

What to Do Next 126

Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels 126

What to Do Next 128

Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels 128

Configuration Examples for Multihop VPDN 130

Example Configuring Multihop VPDN Tunnel Switching 130

Where to Go Next 131

Additional References 132

Feature Information for Multihop VPDN 133

CHAPTER 6 Configuring Additional VPDN Features 135

Finding Feature Information 135

Information About Configuring Additional VPDN Features 136

VPDN Template 136

VPDN Source IP Address 136

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP 136

VRF-Aware VPDN Tunnels 137

MTU Tuning for L2TP VPDN Tunnels 137

MTU Tuning Using IP MTU Adjustments 137

MTU Tuning Using Path MTU Discovery 138

MTU Tuning Using TCP MSS Advertising 138

MTU Tuning Using PPP MRU Advertising 138

QoS for VPDN Tunnels 139

QoS Classification Preservation 140

IP Precedence for VPDN Tunnels 140

ToS Classification for VPDN Tunnels 140

VPDN Group Selection 140

Benefits of VPDN Group Selection 140

How to Configure Additional VPDN Features 141

Creating a VPDN Template 141

Associating a VPDN Group with a VPDN Template 142

Disassociating a VPDN Group from the VPDN Template 143

Configuring the VPDN Source IP Address 144
Configuring the Global VPDN Source IP Address 144
Configuring the Source IP Address for a VPDN Group 145
Configuring VRF-Aware VPDN Tunneling 146
   Configuring VRF-Aware VPDN Tunneling Locally 146
   Configuring VRF-Aware VPDN Tunneling on the Remote RADIUS AAA Server 147
Performing MTU Tuning for L2TP VPDNs 149
   Manually Configuring the IP MTU for VPDN Deployments 149
   Enabling Automatic Adjustment of the IP MTU for VPDN Deployments 150
   Enabling Path MTU Discovery for VPDNs 151
   Manually Configuring the Advertised TCP MSS 153
   Configuring MRU Advertising 154
Configuring VPDN Group Selection 156
   Configuring VPDN Group Selection Based on a Hostname 156
   Configuring VPDN Group Selection Based on a Source IP Address 158
   Configuring VPDN Group Selection Based on VRF 159
Displaying VPDN Group Selections 161
Configuring QoS Packet Classifications for VPDNs 161
   Configuring Preservation of QoS Classifications in the ToS Byte 162
   Manually Configuring the IP Precedence for VPDNs 163
   Manually Configuring the ToS for VPDN Sessions 164
Configuration Examples for Additional VPDN Features 165
   Example Configuring a Global VPDN Template 165
   Example Configuring a Named VPDN Template 165
   Example Disassociating a VPDN Group from the VPDN Template 166
   Example Configuring a Global VPDN Source IP Address 166
   Example Configuring a Source IP Address for a VPDN Group 166
   Example Configuring VRF-Aware VPDN Tunnels Locally 166
   Examples Configuring VRF-Aware VPDN Tunnels on the Remote RADIUS AAA Server 167
   Example Manually Configuring the IP MTU for VPDN Deployments 168
   Example Enabling Automatic Adjustment of the IP MTU for VPDN Deployments 168
   Example Manually Configuring the Advertised TCP MSS 168
   Example Configuring MRU Advertising 168
   Example Configuring Preservation of QoS Classifications in the ToS Byte 169
   Example Manually Configuring the IP Precedence for VPDNs 169
   Example Manually Configuring the ToS for VPDN Sessions 169
CHAPTER 7

VPDN Tunnel Management 177
Finding Feature Information 177
Prerequisites for VPDN Tunnel Management 177
Restrictions for VPDN Tunnel Management 178
Information About VPDN Tunnel Management 178
Termination of VPDN Tunnels 178
VPDN Session Limits 178
Control Packet Parameters for VPDN Tunnels 178
L2TP Congestion Avoidance 179
How L2TP Congestion Avoidance Works 179
VPDN Event Logging 180
How to Manage VPDN Tunnels 180
Manually Terminating VPDN Tunnels 180
Enabling Soft Shutdown of VPDN Tunnels 181
Verifying the Soft Shutdown of VPDN Tunnels 182
Limiting the Number of Allowed Simultaneous VPDN Sessions 184
Restrictions 184
Configuring Global VPDN Session Limits 184
Configuring VPDN Session Limits in a VPDN Template 185
CHAP TER 8

Configuring L2TP HA Session SSO ISSU on a LAC LNS 205

Finding Feature Information 205
Prerequisites for L2TP HA Session SSO ISSU on a LAC LNS 205
Restrictions for L2TP HA Session SSO ISSU on a LAC LNS 206
Information About L2TP HA Session SSO ISSU on a LAC LNS 206
  Stateful Switchover 206
  Checkpointing Data 207
  ISSU Software Superpackage and Rolling Upgrade Requirements 207
    Software Upgrades and Downgrades 207
    Adjusting Receive Window Size 208
How to Configure L2TP HA Session SSO ISSU on a LAC LNS 208
  Configuring SSO on a Route Processor 208
  Configuring Global L2TP HA SSO Mode 209
  Configuring VPDN Groups or VPDN Templates for L2TP HA SSO 210
  Controlling Packet Resynchronization for L2TP HA 212
  Verifying the Checkpoint Status of L2TP HA Sessions 214
  Verifying the Checkpoint Status of VPDN Sessions 215

Contents
Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Note

The Feature Information table in the technology configuration guide mentions when a feature was introduced. It might or might not mention when other platforms were supported for that feature. To determine if a particular feature is supported on your platform, look at the technology configuration guides posted on your product landing page. When a technology configuration guide is displayed on your product landing page, it indicates that the feature is supported on that platform.
VPDN Technology Overview

Virtual private dial-up networks (VPDNs) securely carry private data over a public network, allowing remote users to access a private network over a shared infrastructure such as the Internet. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network.

- Finding Feature Information, page 3
- Information About VPDNs, page 3
- Where to Go Next, page 14
- Additional References, page 15
- Feature Information for VPDN Technology Overview, page 16

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 at the end of this module.

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 VPDNs

Overview of VPDN Technology

VPDNs extend private network dial-in services to remote users. VPDNs use Layer 2 tunneling technologies to create virtual point-to-point connections between remote clients and a private network. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network.
Instead of connecting directly to the remote private network, VPDN users connect to a nearby access server, which is often located at an Internet service provider (ISP) local point of presence (POP). Data is securely forwarded from the access server to the private network over the Internet, providing a cost-effective method of communication between remote clients and the private network.

A benefit of VPDNs is the way they delegate responsibilities for the network. The customer can outsource responsibility for the information technology (IT) infrastructure to an ISP that maintains the modems that the remote users dial into, the access servers, and the internetworking expertise. The customer is then responsible only for authenticating users and maintaining the private network.

The figure below shows a basic VPDN network deployment.

**Figure 1: Basic VPDN Network Deployment**

A PPP client dials into an ISP access server, called the Network Access Server (NAS). The NAS determines whether it should forward that PPP session on to the router or access server that serves as the point of contact for the private network, the tunnel server. The tunnel server authenticates the user and initiates PPP negotiations. Once PPP setup is complete, all frames that are sent between the client and the tunnel server pass through the NAS.

VPDNs can use these tunneling protocols to tunnel link-level frames:

- Layer 2 Tunneling Protocol (L2TP)
- Layer 2 Tunneling Protocol Version 3 (L2TPv3)
- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)

Using one of these protocols, a tunnel is established between the NAS or client and the tunnel server, providing secure data transport over a shared infrastructure such as the Internet.

**Note**

VPDNs on the Cisco ASR 1000 Series Aggregation Services Routers can use only the Layer 2 Tunneling Protocol (L2TP) or the Layer 2 Tunneling Protocol Version 3 (L2TPv3) to tunnel link-level frames.
VPDN Terminology

VPDN Hardware Devices

Generally three devices are involved in VPDN tunneling. Two of these devices function as tunnel endpoints—one device initiates the VPDN tunnel, and the other device terminates the VPDN tunnel. Depending on the tunneling architecture, different types of devices can act as the local tunnel endpoint.

As new tunneling protocols have been developed for VPDNs, protocol-specific terminology has been created to describe some of the devices that participate in VPDN tunneling. However, these devices perform the same basic functions no matter what tunneling protocol is being used. For the sake of clarity we will use this generic terminology to refer to VPDN devices throughout this documentation:

- **Client**—The client device can be the PC of a dial-in user, or a router attached to a local network. In client-initiated VPDN tunneling scenarios, the client device acts as a tunnel endpoint.

- **NAS**—The network access server (NAS) is typically a device maintained by an ISP that provides VPDN services for its customers. The NAS is the local point of contact for the client device. Establishing a connection between the NAS and the client will referred to as receiving a call or placing a call, depending on whether a dial-in or dial-out scenario is being discussed. Depending on the tunneling architecture, the NAS functions as follows:

  - For NAS-initiated VPDN tunneling scenarios and dial-out VPDN tunneling scenarios, the NAS functions as a tunnel endpoint. The NAS initiates dial-in VPDN tunnels and terminates dial-out VPDN tunnels. The Cisco ASR 1000 Series Aggregation Services Routers support dial-in only.

  - For client-initiated VPDN tunneling scenarios, the NAS does not function as a tunnel endpoint; it simply provides Internet connectivity.

- **Tunnel server**—The tunnel server is typically maintained by the customer and is the contact point for the remote private network. The tunnel server terminates dial-in VPDN tunnels and initiates dial-out VPDN tunnels.

- **Tunnel switch**—A tunnel switch is a device configured to perform multihop VPDN tunneling. A tunnel switch acts as both a NAS and a tunnel server. The tunnel switch terminates incoming VPDN tunnels and initiates the outgoing VPDN tunnels that will carry data on to the next hop.

Although technically a tunnel switch is a tunnel endpoint for both the incoming tunnel and the outgoing tunnel, for the sake of simplicity the tunnel endpoints in a multihop deployment are considered to be the device that initiates the first tunnel and the device that terminates the final tunnel of the multihop path.

The table below lists the generic terms and the corresponding technology-specific terms that are sometimes used to describe the NAS and the tunnel server.
Table 1: VPDN Hardware Terminology

<table>
<thead>
<tr>
<th>Generic Term</th>
<th>L2F Term</th>
<th>L2TP Term</th>
<th>PPTP Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS</td>
<td>NAS</td>
<td>L2TP access concentrator (LAC)</td>
<td>PPTP access concentrator (PAC)</td>
</tr>
<tr>
<td>Tunnel server</td>
<td>Home gateway</td>
<td>L2TP network server (LNS)</td>
<td>PPTP network server (PNS)</td>
</tr>
</tbody>
</table>

The Cisco ASR 1000 Series Aggregation Services Routers support only L2TP.

**VPDN Tunnels**

A VPDN tunnel exists between the two tunnel endpoints. The tunnel consists of a control connection and zero or more Layer 2 sessions. The tunnel carries encapsulated PPP datagrams and control messages between the tunnel endpoints. Multiple VPDN sessions can use the same VPDN tunnel.

**VPDN Sessions**

A VPDN session is created between the tunnel endpoints when an end-to-end PPP connection is established between a client and the tunnel server. Datagrams related to the PPP connection are sent over the tunnel. There is a one-to-one relationship between an established session and the associated call. Multiple VPDN sessions can use the same VPDN tunnel.

**VPDN Architectures**

**Client-Initiated Dial-In VPDN Tunneling**

Client-initiated dial-in VPDN tunneling is also known as voluntary tunneling. In a client-initiated dial-in VPDN tunneling scenario, the client device initiates a Layer 2 tunnel to the tunnel server, and the NAS does not participate in tunnel negotiation or establishment. In this scenario, the NAS is not a tunnel endpoint; it simply provides Internet connectivity. The client device must be configured to initiate the tunnel.

The main advantage of client-initiated VPDN tunneling is that it secures the connection between the client and the ISP NAS. However, client-initiated VPDNs are not as scalable and are more complex than NAS-initiated VPDNs.

Client-initiated VPDN tunneling can use the L2TP protocol or the L2TPv3 protocol if the client device is a router. If the client device is a PC, only the PPTP protocol is supported.
The figure below shows a client-initiated VPDN tunneling scenario.

*Figure 2: Client-Initiated Dial-In VPDN Scenario*

For further information about client-initiated tunneling deployments, see the "Configuring Client-Initiated Dial-In VPDN Tunneling" module.

Before configuring a client-initiated dial-in VPDN tunneling deployment, you must complete the required tasks in the "Configuring AAA for VPDNs" module.

**NAS-Initiated Dial-In VPDN Tunneling**

NAS-initiated dial-in VPDN tunneling is also known as compulsory tunneling. In a NAS-initiated dial-in VPDN tunneling scenario, the client dials into the NAS through a medium that supports PPP. If the connection from the client to the ISP NAS is over a medium that is considered secure, such as digital subscriber line (DSL), ISDN, or the public switched telephone network (PSTN), the client can choose not to provide additional security. The PPP session is securely tunneled from the NAS to the tunnel server without any special knowledge or interaction required from the client.

NAS-initiated VPDN tunneling can be configured with the L2TP or L2F protocol.

**Note**

The Cisco ASR 1000 Series Aggregation Services Routers support only L2TP.
The figure below shows a NAS-initiated dial-in tunneling scenario.

*Figure 3: NAS-Initiated Dial-In VPDN Scenario*

For further information about NAS-initiated tunneling deployments, see the Configuring NAS-Initiated Dial-In VPDN Tunneling module.

Before configuring a NAS-initiated dial-in VPDN tunneling deployment, you must complete the required tasks in the Configuring AAA for VPDNs module.

**Multihop VPDN Tunneling**

Multihop VPDN is a specialized VPDN configuration that allows packets to pass through multiple tunnels. Ordinarily, packets are not allowed to pass through more than one tunnel. In a multihop tunneling deployment, the VPDN tunnel is terminated after each hop and a new tunnel is initiated to the next hop destination. A maximum of four hops is supported.

Multihop VPDN is required for the scenarios described in these sections:

**VPDN Tunneling to an MMP Stack Group**

Multihop VPDN is required when the private network uses Mutlichassis Multilink PPP (MMP) with multiple tunnel servers in a stack group. Stack group configurations require the ability to establish Layer 2 tunnels between participating hardware devices. If the incoming data is delivered to the stack group over a VPDN tunnel, multihop VPDN is required for the stack group to function.

Multihop VPDN tunneling with MMP can be configured using the L2TP or L2F protocol.

---

**Note**

The Cisco ASR 1000 Aggregation Services Routers support only L2TP.
The figure below shows a network scenario using a multihop VPDN with an MMP deployment.

**Figure 4: MMP Using Multihop VPDN**

For further information about configuring multihop VPDN for MMP deployments, see the Configuring Multihop VPDN module.

Before configuring a multihop VPDN for MMP deployment, you must configure MMP and you must complete the required tasks in the Configuring AAA for VPDNs module.

**Tunnel Switching VPDNs**

Multihop VPDN can be used to configure a router as a tunnel switch. A tunnel switch is a device that is configured as both a NAS and a tunnel server. A tunnel switch is able to receive packets from an incoming VPDN tunnel and send them out over an outgoing VPDN tunnel. Tunnel switch configurations can be used between ISPs to provide wholesale VPDN services.

Multihop tunnel switching can be configured using the L2TP, L2F, or PPTP protocol.

---

**Note**
The Cisco ASR 1000 Aggregation Services Routers support only L2TP.
The figure below shows a network scenario using a tunnel switching deployment.

**Figure 5: Tunnel Switching Using Multihop VPDN**

For further information about multihop tunnel switching deployments, see the Configuring Multihop VPDN module.

Before configuring a multihop tunnel switching deployment, you must complete the required tasks in the Configuring AAA for VPDNs module.

### VPDN Tunneling Protocols

VPDNs use Layer 2 protocols to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous High-Level Data Link Control (HDLC)). ISPs configure their NAS to receive calls from users and to forward the calls to the customer tunnel server.

Usually, the ISP maintains only information about the customer tunnel server. The customer maintains the users' IP addresses, routing, and other user database functions. Administration between the ISP and the tunnel server is reduced to IP connectivity.

This section contains information on L2TP and L2TPv3, which are the only protocols that can be used for VPDN tunneling on the Cisco ASR 1000 Series Routers.

**L2TP**

L2TP is an Internet Engineering Task Force (IETF) standard that combines the best features of the two older tunneling protocols: Cisco L2F and Microsoft PPTP.

L2TP offers the same full-range spectrum of features as L2F, but offers additional functionality. An L2TP-capable tunnel server will work with an existing L2F NAS and will concurrently support upgraded components running L2TP. Tunnel servers do not require reconfiguration each time an individual NAS is upgraded from L2F to L2TP. The table below compares L2F and L2TP feature components.
Table 2: L2F and L2TP Feature Comparison

<table>
<thead>
<tr>
<th>Function</th>
<th>L2F</th>
<th>L2TP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute-value (AV) pair hiding</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunnel server load sharing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunnel server stacking/multi-hop support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunnel server primary and secondary backup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Domain Name System (DNS) name support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Domain name flexibility</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Idle and absolute timeout</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multilink PPP support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multichassis Multilink PPP support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All security benefits of PPP, including multiple per-user authentication options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Challenge Handshake Authentication Protocol (CHAP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Microsoft CHAP (MS-CHAP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password Authentication Protocol (PAP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tunnel authentication mandatory</td>
<td>• All security benefits of PPP, including multiple per-user authentication options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CHAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MS-CHAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tunnel authentication optional</td>
</tr>
</tbody>
</table>

Traditional dialup networking services support only registered IP addresses, which limits the types of applications that are implemented over VPDNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses. This allows the existing access infrastructure--such as the Internet, modems, access servers, and ISDN terminal adapters (TAs)--to be used. It also allows customers to outsource
dial-out support, thus reducing overhead for hardware maintenance costs and 800 number fees, and allows them to concentrate corporate gateway resources.

The figure below shows the basic L2TP architecture in a typical dial-in environment.

*Figure 6: L2TP Architecture*

Using L2TP tunneling, an ISP or other access service can create a virtual tunnel to link remote sites or remote users with corporate home networks. The NAS located at the POP of the ISP exchanges PPP messages with remote users and communicates by way of L2TP requests and responses with the private network tunnel server to set up tunnels. L2TP passes protocol-level packets through the virtual tunnel between endpoints of a point-to-point connection. Frames from remote users are accepted by the ISP NAS, stripped of any linked framing or transparency bytes, encapsulated in L2TP, and forwarded over the appropriate tunnel. The private network tunnel server accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface.
The figure below depicts the events that occur during establishment of a NAS-initiated dial-in L2TP connection.

**Figure 7: L2TP Protocol Negotiation Events**

1. The remote user initiates a PPP connection to the ISP NAS using a medium that supports PPP such as the analog telephone system. The NAS accepts the connection, the PPP link is established, and Link Control Protocol (LCP) is negotiated.

2. After the end user and NAS negotiate LCP, the NAS partially authenticates the end user with CHAP or PAP. The username, domain name, or Dialed Number Information Service (DNIS) is used to determine whether the user is a VPDN client. If the user is not a VPDN client, authentication continues, and the client will access the Internet or other contacted service. If the username is a VPDN client, the mapping will name a specific endpoint (the tunnel server).

3. The tunnel endpoints, the NAS and the tunnel server, authenticate each other before any tunnel or session establishment is attempted. Alternatively, the tunnel server can accept tunnel creation without any tunnel authentication of the NAS. The NAS and the tunnel server exchange control messages to negotiate tunnel establishment.

4. Once the tunnel exists, an L2TP session is created for the end user. The NAS and the tunnel server exchange call messages to negotiate session establishment.

5. The NAS will propagate the negotiated LCP options and the partially authenticated CHAP or PAP information to the tunnel server. The tunnel server will funnel the negotiated options and authentication information directly to the virtual access interface, allowing authentication to be completed. If the options configured in the virtual template interface do not match the options negotiated with the NAS, the connection will fail and a disconnect notification will be sent to the NAS.
PPP packets are exchanged between the dial-in client and the remote tunnel server as if no intermediary device (the NAS) is involved.

Subsequent PPP incoming sessions (designated for the same tunnel server) do not repeat the L2TP tunnel negotiation because the L2TP tunnel is already open.

L2TPv3

L2TPv3 is an enhanced version of L2TP with the capability to tunnel any Layer 2 payload. L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 Virtual Private Networks (VPNs).

In VPDN deployments, L2TPv3 can be used to establish a client-initiated tunnel from a local router to the remote customer network over an emulated circuit known as a pseudowire. There is one pseudowire associated with each L2TPv3 session.

Rather than using a VPDN group configuration, L2TPv3 uses an L2TP class configuration that is associated with the pseudowire. L2TPv3 pseudowires can also be used to establish L2TP tunnels by configuring an L2TP class on the local device and an accept-dialin VPDN group on the customer network.

For detailed information about the L2TPv3 protocol, see the Additional References section.

VPDN Group Configuration Modes

Many VPDN configuration tasks are performed within a VPDN group. A VPDN group can be configured to function either as a NAS VPDN group or as a tunnel server VPDN group, but not as both. However, an individual router can be configured with both a NAS VPDN group and a tunnel server VPDN group.

You can configure a VPDN group as a specific type of VPDN group by issuing at least one of the commands listed in the table below:

<table>
<thead>
<tr>
<th>VPDN Group Type</th>
<th>Command</th>
<th>Command Mode</th>
<th>Command Mode Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel server</td>
<td>accept-dialin</td>
<td>VPDN accept-dialin configuration</td>
<td>Router(config-vpdn-acc-in)#</td>
</tr>
<tr>
<td>NAS</td>
<td>request-dialin</td>
<td>VPDN request-dialin configuration</td>
<td>Router(config-vpdn-req-in)#</td>
</tr>
</tbody>
</table>

Many of the commands required to properly configure VPDN tunneling are issued in one of the VPDN subgroup configuration modes shown in the table below. Removing the VPDN subgroup command configuration will remove all subordinate VPDN subgroup configuration commands as well.

Where to Go Next

Once you have identified the VPDN architecture that you want to configure and the tunneling protocol that you will use, you should perform the required tasks in the Configuring AAA for VPDNs module.
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>Technical support documentation for L2TP</td>
<td>Layer 2 Tunnel Protocol (L2TP)</td>
</tr>
<tr>
<td>Technical support documentation for VPDNs</td>
<td>Virtual Private Dial-Up Network (VPDN)</td>
</tr>
<tr>
<td>Information on L2TPv3</td>
<td>L2TPv3: Layer 2 Tunnel Protocol Version 3 module</td>
</tr>
</tbody>
</table>

## Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported, and support for existing</td>
<td>--</td>
</tr>
<tr>
<td>standards has not been modified.</td>
<td></td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>- CISCO-VPDN-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software</td>
</tr>
<tr>
<td>- CISCO-VPDN-MGMT-EXT-MIB</td>
<td>releases, and feature sets, use Cisco MIB Locator found at the following</td>
</tr>
<tr>
<td></td>
<td>URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol L2TP</td>
</tr>
<tr>
<td>RFC 3931</td>
<td>Layer Two Tunneling Protocol - Version 3 (L2TPv3)</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for VPDN Technology Overview

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 . An account on Cisco.com is not required.

Table 4: Feature Information for VPDN Technology Overview

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| L2TP Layer 2 Tunneling Protocol | Cisco IOS XE Release 2.1  
Cisco IOS XE Release 3.3S | This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. VPDNs use Layer 2 protocols to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous HDLC). L2TP is an IETF standard that combines the best features of the two older tunneling protocols: Cisco L2F and Microsoft PPTP. No commands were introduced or modified by this feature. |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Private Dial-up Network</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. VPDNs securely carry private data over a public network, allowing remote users to access a private network over a shared infrastructure such as the Internet. VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for point-to-point connections between remote users and a central network. No commands were introduced or modified by this feature.</td>
</tr>
</tbody>
</table>
Configuring AAA for VPDNs

This module describes how to configure authentication, authorization, and accounting (AAA) for virtual private dialup networks (VPDNs).

- Finding Feature Information, page 19
- Prerequisites for Configuring AAA for VPDNs, page 19
- Information About AAA for VPDNs, page 20
- How to Configure AAA for VPDNs, page 27
- Configuration Examples for AAA for VPDNs, page 82
- Where to Go Next, page 92
- Additional References, page 92
- Feature Information for AAA for VPDNs, page 94

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 at the end of this module.

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.

Prerequisites for Configuring AAA for VPDNs

- Before configuring AAA for VPDNs, you should understand the concepts in the VPDN Technology Overview module.
- You must identify the VPDN architecture you plan to implement.
- You must identify the tunneling protocol you will use.
If you plan to configure remote AAA, you should understand the concepts in the Authentication, Authorization, and Accounting (AAA) module and Security Server Protocols module.

If you plan to configure Layer 2 Tunneling Protocol (L2TP) Forwarding of Point-to-Point Protocol over Ethernet (PPPoE) Tagging Information, it is recommended that you be familiar with RFC 2516 and DSL Forum TR-101 before configuring this feature.

Information About AAA for VPDNs

VPDN Tunnel Authorization Search Order

When a call to a network access server (NAS) is to be tunneled to a tunnel server, the NAS must identify which tunnel server to forward the call to. The router can authorize users and select the outgoing tunnel based on the domain portion of the username, the Dialed Number Identification Service (DNIS) number, the multihop hostname, or any combination of these three parameters in a specified order. The default search order for VPDN tunnel authorization is to first search by DNIS, then by domain.

These sections contain information on VPDN tunnel lookup criteria:

VPDN Tunnel Lookup Based on Domain Name

When a NAS is configured to forward VPDN calls on the basis of the user domain name, the user must use a username of the form `username@domain`. The NAS then compares the user domain name to the domain names it is configured to search for. When the NAS finds a match, it forwards the user call to the proper tunnel server.

VPDN Tunnel Lookup Based on DNIS Information

When a NAS is configured to forward VPDN calls on the basis of the user DNIS information, the NAS identifies the user DNIS information, which is provided on ISDN lines, and then forwards the call to the proper tunnel server.

The ability to select a tunnel on the basis of DNIS information provides additional flexibility to network service providers that offer VPDN services and to the companies that use the services. Instead of using only the domain name for tunnel selection, the NAS can use dialed number information for tunnel selection.

With this feature, a company—which might have only one domain name—can provide multiple specific phone numbers for users to dial in to the NAS at the service provider point of presence (POP). The service provider can select the tunnel to the appropriate services or portion of the company network on the basis of the dialed number.

VPDN Tunnel Lookup Based on Both Domain Name and DNIS Information

When a service provider has multiple AAA servers configured, VPDN tunnel authorization searches based on domain name can be time consuming and might cause the client session to time out.

To provide more flexibility, service providers can configure the NAS to perform tunnel authorization searches by domain name only, by DNIS only, or by both in a specified order.
VPDN Tunnel Lookup Based on the Multihop Hostname

If a device will function as a multihop tunnel switch, tunnel authorization searches can be performed based on the multihop hostname. Configuring a multihop hostname on a tunnel switch allows authorization searches to be based on the identity of the peer device that initiated the tunnel. The multihop hostname can be the hostname of the remote peer that initiated the ingress tunnel, or the tunnel ID associated with the ingress tunnel.

A multihop tunnel switch can be configured to perform authorization searches by multihop hostname only, by domain name only, by DNIS only, or by any combination of these searches in a specified order.

Per-User VPDN AAA

If remote AAA is used for VPDN, the NAS that receives the call from a user forwards information about that user to its remote AAA server. With basic VPDN, the NAS sends the user domain name when performing authentication based on domain name or the telephone number the user dialed in from when performing authentication based on DNIS.

When per-user VPDN is configured, the entire structured username is sent to a RADIUS AAA server the first time the router contacts the AAA server. This enables the software to customize tunnel attributes for individual users that use a common domain name or DNIS.

Without VPDN per-user configuration, the software sends only the domain name or DNIS to determine VPDN tunnel attribute information. Then, if no VPDN tunnel attributes are returned, the software sends the entire username string.

VPDN Authorization for Directed Request Users

Directed requests allow users logging into a NAS to select a RADIUS server for authorization. With directed requests enabled, only the portion of the username before the “@” symbol is sent to the host specified after the “@” symbol. Using directed requests, authorization requests can be directed to any of the configured servers, and only the username is sent to the specified server.

Domain Name Prefix and Suffix Stripping

When a user connects to a NAS configured to use a remote server for AAA, the NAS forwards the username to the remote AAA server. Some RADIUS or TACACS+ servers require the username to be in a particular format, which might be different from the format of the full username. For example, the remote AAA server might require the username to be in the format user@domain.com, but the full username could be prefix/user@domain.com@suffix. Configuring domain name stripping allows the NAS to strip incompatible portions from the full username before forwarding the reformatted username to the remote AAA server.

The NAS can be configured to perform in these ways:

- Strip generic suffixes from the full username using the suffix delimiter character @. Any portion of the full username that follows the first delimiter that is parsed will be stripped.
- Use a different character or set of characters as the suffix delimiter.
- Strip both suffixes and prefixes from the full username. The NAS can also be configured to strip only specified suffixes instead of performing generic suffix stripping.
VPDN Tunnel Authentication

VPDN tunnel authentication enables routers to authenticate the other tunnel endpoint before establishing a VPDN tunnel. VPDN tunnel authentication is optional for L2TP tunnels.

For additional information on configuring VPDN tunnel authentication for client-initiated VPDN tunneling deployments, see the "Configuring VPDN Tunnel Authentication" section.

VPDN tunnel authentication can be performed in these ways:

- Using local AAA on both the NAS and the tunnel server
- Using a remote RADIUS AAA server on the NAS and local AAA on the tunnel server
- Using a remote TACACS+ AAA server on the NAS and local AAA on the tunnel server

For L2TP tunnels only, a remote RADIUS AAA server can be used to perform VPDN tunnel authentication on the VPDN tunnel terminator as follows:

- Using a remote RADIUS AAA server on the tunnel server for dial-in VPDNs
- Using a remote RADIUS AAA server on the NAS for dial-out VPDNs

For detailed information on configuring remote RADIUS or TACACS+ servers, see the "Additional References section."

RADIUS Tunnel Accounting for L2TP VPDNs

RADIUS tunnel accounting for VPDNs is supported by RFC 2867, which introduces six new RADIUS accounting types. Without RADIUS tunnel accounting support, VPDN with network accounting will not report all possible attributes to the accounting record file. RADIUS tunnel accounting support allows users to determine tunnel-link status changes. Because all possible attributes can be displayed, users can better verify accounting records with their Internet service providers (ISPs).

Enabling tunnel type accounting records allows the router to send tunnel and tunnel-link accounting records to the RADIUS server. The two types of accounting records allow the identification of VPDN tunneling events as described next.

Tunnel-Type Accounting Records

AAA sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server to identify these events:

- A VPDN tunnel is brought up or destroyed.
- A request to create a VPDN tunnel is rejected.

Tunnel-Link-Type Accounting Records

AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server to identify these events:

- A user session within a VPDN tunnel is brought up or brought down.
- A user session create request is rejected.
VPDN-Specific Remote RADIUS AAA Server Configurations

The RADIUS attributes are specific to VPDN configurations. For detailed information on configuring remote RADIUS or TACACS+ servers, see the Additional References section.

VPDN-specific RADIUS attributes provide this functionality:

- Tunnel assignments--The NAS AAA server can be configured to group users from different per-user or domain RADIUS profiles into the same active VPDN tunnel when the tunnel type and tunnel endpoint are identical.

- Authentication names for NAS-initiated tunnels--The NAS AAA server can be configured with authentication names other than the default names for the NAS and the NAS AAA server.

L2TP Forwarding of PPPoE Tagging Information

The L2TP Forwarding of PPPoE Tag Information feature allows you to transfer DSL line information from the L2TP access concentrator (LAC) to the L2TP network server (LNS). For example, the LAC transports the actual-rate-up and the actual-rate-down PPPoE tag information to the LNS, which learns about the actual PPPoE transfer speeds that are negotiated by the customer premise equipment (CPE) and the digital subscriber line access multiplexer (DSLAM). The DSLAM inserts the PPPoE tag values for the rate up and the rate down and signals this information during PPPoE establishment with the LAC, which in turn, sends this information to the LNS.

By using the L2TP Forwarding of PPPoE Tag Information feature, you can also override the nas-port-id or calling-station-id VSAs, or both, on the LNS with the Circuit-ID and Remote-ID VSA respectively.

When you configure the `dsl-line-info-forwarding` command in VPDN group or VPDN-template configuration mode, and when the LNS receives one of the specified AV pairs, the LNS sends a matching VSA to the RADIUS server as a AAA request. The associated AAA attributes are:

- AAA_CIRCUIT_ID (RADIUS attribute 87)
- AAA_REMOTE_ID (RADIUS attribute 31)
- DSL Sync Rate VSAs

Enter the `radius-server attribute 87 circuit-id` command to override the nas-port-id with the CIRCUIT_ID VSA. Enter the `radius-server attribute 31 remote-id` command to override the calling-station-id with the REMOTE_ID VSA.

In accordance with DSL Forum 2004-71, the DSL uses the Vendor Specific tag for line identification. The first 2 octets (TAG_TYPE) are PPPOE_TAG_VENDSPEC (0x0105). The next 2 octets (TAG_LENGTH) contain the total length including Sub-options, Sub-option-lengths, and Tag-values. The first four octets of the TAG_VALUE contain the vendor ID. The next octet contains sub-option for Agent Remote ID (0x02). Following octet contains total length of Sub-option-tag in bytes.

The maximum length for the Remote-ID tag is 63 bytes. The Remote-ID tag contains an operator administered string that uniquely identifies the subscriber on the associated DSL line. The Remote-ID tag can be a phone number, an email address, a billing account number, or any other string that can be used by Service Providers as a tracking mechanism.
If the discovery frame has the sub-option 0x01, it indicates the presence of the Circuit-ID tag. A single frame supports Circuit-ID, Remote-ID, or both. If Circuit-ID is present in the same frame, it sends to the RADIUS server through the Nas-Port-ID attribute.

The following examples show an access and accounting request sent to the RADIUS server with remote-ID tag and DSL-Sync-Rate tags:

```
01:24:52: RADIUS/ENCODE: Best Local IP-Address 10.0.73.20 for Radius-Server 128.107.164.254
01:24:52: RADIUS: authenticator 3B 49 F5 7D 8A 6F A4 D7 - 57 99 E6 60 A9 D0 C7 B9
01:24:52: RADIUS: Vendor, Cisco [26] 41
01:24:52: RADIUS: Cisco AVpair [1] 35 "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS: Vendor, Cisco [26] 39
01:24:52: RADIUS: Vendor, Cisco [26] 39
01:24:52: RADIUS: Vendor, Cisco [26] 39
01:24:52: RADIUS: Vendor, Cisco [26] 46
01:24:52: RADIUS: Vendor, Cisco [26] 36
01:24:52: RADIUS: Cisco AVpair [1] 33 "remote-id-tag=0090.bf06.c81c"
01:24:52: RADIUS: NAS-Port-Id [87] 25 "Ether1/0.1:ababababa"
01:24:52: RADIUS: Vendor, Cisco [26] 41
01:24:52: RADIUS: Cisco AVpair [1] 35 "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS: Vendor, Cisco [26] 41
01:24:55: RADIUS: Cisco AVpair [1] 30 "remote-id-tag=0090.bf06.c81c"
01:24:55: RADIUS: NAS-Port-Id [87] 25 "Ether1/0.1:ababababa"
01:24:55: RADIUS: Vendor, Cisco [26] 41
01:24:55: RADIUS: Cisco AVpair [1] 35 "client-mac-address=0090.bf06.c81c"
01:24:57: RADIUS: Received from id 1646/4 192.107.164.254:1646, Accounting-response, len 20
```

The LAC sends the indicated AV pairs, containing the DSL line information to the LNS, which sends them through AAA to the RADIUS server. The RADIUS server uses the DSL line identification when processing AAA requests.
If you plan to configure L2TP Forwarding of PPPoE Tagging Information, it is recommended that you be familiar with RFC 2516 and DSL Forum TR-101 before configuring this feature.

**DSL Sync-Rate VSAs**

The DSL uses PPPoE Vendor Specific tags for Sync-Rate tag information. DSL Sync-Rates are encoded as 32-bit binary values, describing the rate in kbps. The tag length is 4 bytes. The table below shows the mandatory DSL Sync-Rate tags and their associated RADIUS VSA.

**Table 5: Required DSL Sync-Rate Tags**

<table>
<thead>
<tr>
<th>DSL Line Information</th>
<th>RADIUS VSA</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL Line Actual-Data-Rate-Upstream AVP</td>
<td>AAA_AT_ACTUAL_RATE_UP</td>
<td>Actual data rate upstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Actual-Data-Rate-Downstream AVP</td>
<td>AAA_AT_ACTUAL_RATE_DOWN</td>
<td>Actual data rate downstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Minimum-Data-Rate-Upstream AVP</td>
<td>AAA_AT_MIN_RATE_UP</td>
<td>Minimum data rate upstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Minimum-Data-Rate-Downstream AVP</td>
<td>AAA_AT_MIN_RATE_DOWN</td>
<td>Minimum data rate downstream in kbps.</td>
</tr>
</tbody>
</table>

PADI/PADR frames might contain an optional DSL Sync-Rate tag. The table below shows DSL line information and their associated RADIUS VSA for the optional DSL Sync-Rate tags.

**Table 6: Optional DSL Sync-Rate Tags**

<table>
<thead>
<tr>
<th>DSL Line Information</th>
<th>RADIUS VSA</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL Line Attainable-Data-Rate-Upstream AVP</td>
<td>AAA_AT_ATTAINABLE_RATE_UP</td>
<td>Attainable data rate upstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Attainable-Data-Rate-Downstream AVP</td>
<td>AAA_AT_ATTAINABLE_RATE_DOWN</td>
<td>Attainable data rate downstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Maximum-Data-Rate-Upstream AVP</td>
<td>AAA_AT_MAX_RATE_UP</td>
<td>Maximum data rate upstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Maximum-Data-Rate-Downstream AVP</td>
<td>AAA_AT_MAX_RATE_DOWN</td>
<td>Maximum data rate downstream in kbps.</td>
</tr>
<tr>
<td>DSL Line Minimum-Data-Rate-Upstream -Low-Power AVP</td>
<td>AAA_AT_MIN_RATE_UP_LOW_POWER</td>
<td>Minimum data rate upstream in low power state in kbps.</td>
</tr>
<tr>
<td>DSL Line Minimum-Data-Rate-Downstream -Low-Power AVP</td>
<td>AAA_AT_MIN_RATE_DOWN_LOW_POWER</td>
<td>Minimum data rate downstream in low power state in kbps.</td>
</tr>
</tbody>
</table>
LNS Address Checking

Benefits of LNS Address Checking

The LNS Address Checking feature allows a LAC to check the IP address of the LNS sending traffic to it during the setup of an L2TP tunnel, thus providing a check for uplink and downlink traffic arriving from different interfaces.

The benefit of the LNS Address Checking feature is avoiding the loss of revenue from users sending back traffic through an alternate network.

LNS Address Checking Using a RADIUS Server

Use the Cisco attribute-value pair (AVP), downloaded from a RADIUS server during authentication, to enable IP address checking at the LAC.

The Cisco AVP is:

l2tp-security-ip-address-check=yes

The following RADIUS profile example shows the LNS address checking enabled:

```
example.com Password="example"
Service-Type=Outbound
Cisco-Avpair="vpdn:tunnel-id=tunnel"
Cisco-Avpair="vpdn:tunnel-type=l2tp"
Cisco-Avpair="ip-address=10.10.10.1"
Cisco-Avpair="vpdn:l2tp-tunnel-password=example"
Cisco-Avpair="vpdn:l2tp-security-ip-address-check=yes"
```
Debugging Dropped Control Packets

Use the LNS Address Checking feature to help troubleshoot dropped control packets. If you configure the `debug vpdn 12x-error` command, informational messages display for each control packet that is dropped in the following format:

```
Tnl <tunnel-ID>
   L2TP: Drop <L2TP-packet-name>
   from y.y.y.y (attempted) x.x.x.x
```

Modified LNS Dead-Cache Handling

The Modified LNS Dead-Cache Handling feature allows you to display and clear (restart) any Layer 2 Tunnel Protocol (L2TP) network server (LNS) entry in a dead-cache (DOWN) state. You can use this feature to generate a Simple Network Management Protocol (SNMP) or system message log (syslog) event when an LNS enters or exits a dead-cache state. Once an LNS exits the dead-cache state, the LNS is able to establish new sessions.

Prior to Cisco IOS XE Release 2.4, networks could not identify the status of a Load Sharing Group (LSG) on a LAC. As a result, it was not possible to know if an LNS is not responding (dead-cache state). An LNS in a dead-cache state causes an LSG to reject a call from an LAC.

Networks also have no method of logging, either though a syslog or SNMP event, when an LNS enters, or is cleared from a dead-cache state.

The Modified LNS Dead-Cache Handling feature allows you to view (identify) and clear (restart) one or more LNS entries in a dead-cache (DOWN) state, and generate either a syslog or SNMP event when an LNS exits or enters a dead-cache state. Once an LNS clears a dead-cache state, the LNS is active and available for new call-session establishments.

How to Configure AAA for VPDNs

Enabling VPDN on the NAS and the Tunnel Server

Before performing any VPDN configuration tasks, you must enable VPDN on the NAS and the tunnel server. If you are deploying a multihop VPDN tunnel switching architecture, VPDN must be enabled on the tunnel switch as well.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vpdn enable`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
Example:  
Router> enable |
| Step 2 | configure terminal | Enters global configuration mode.  
Example:  
Router# configure terminal |
| Step 3 | vpdn enable | Enables VPDN on the router.  
Example:  
Router(config)# vpdn enable |

Configuring the VPDN Tunnel Authorization Search Order

Perform this task on the NAS or the tunnel switch to configure the VPDN tunnel authorization search order if you prefer to use an order other than the default order. The default search order for VPDN tunnel authorization is to first search by DNIS, then by domain.

Before You Begin

You must perform the task in the "Enabling VPDN on the NAS and the Tunnel Server" section.

Note

Tunnel authorization searches based on the multihop hostname are supported only for multihop tunnel switching deployments.

SUMMARY STEPS

1. enable  
2. configure terminal  
3. vpdn search-order {dnis [domain] [multihop-hostname] | domain [dnis] [multihop-hostname] | multihop-hostname [dnis] [domain]}
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: enable</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure</td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td>Router# configure</td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>vpdn search-order</td>
<td>Specifies how the service provider NAS or tunnel switch is to</td>
</tr>
<tr>
<td>{dnis [domain]</td>
<td>perform VPDN tunnel authorization searches.</td>
</tr>
<tr>
<td>[multihop-hostname]</td>
<td></td>
</tr>
<tr>
<td>[domain [dnis]</td>
<td></td>
</tr>
<tr>
<td>[multihop-hostname]</td>
<td></td>
</tr>
<tr>
<td>[multihop-hostname [dnis]</td>
<td></td>
</tr>
<tr>
<td>[domain]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn</td>
<td></td>
</tr>
<tr>
<td>search-order</td>
<td></td>
</tr>
<tr>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>dnis</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  The **multihop-hostname** keyword is used only on a device configured as a tunnel switch.

**Configuring per-User VPDN on the NAS**

Per-user VPDN can be configured globally, or for individual VPDN groups. The VPDN group configuration will take precedence over the global configuration.

Perform one of these tasks on the NAS to configure per-user VPDN:

**Prerequisites**

The NAS remote RADIUS server must be configured for AAA. See the "Additional References" section.

**Restrictions**

- Per-user VPDN configuration supports only RADIUS as the AAA protocol.
- This task is compatible only with NAS-initiated dial-in VPDN scenarios.

**Configuring Global per-User VPDN**

Configuring per-user VPDN on a NAS causes the NAS to send the entire structured username of the user to a RADIUS AAA server the first time the NAS contacts the AAA server. Per-user VPDN can be configured
globally, or for individual VPDN groups. Configuring per-user VPDN globally will apply per-user VPDN to all request-dialin VPDN groups configured on the NAS.

Perform this task on the NAS to configure global per-user VPDN.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn authen-before-forward

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn authen-before-forward</td>
<td>Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in tunnels.</td>
</tr>
<tr>
<td>Example: Router(config)# vpdn authen-before-forward</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring per-User VPDN for a VPDN Group**

Configuring per-user VPDN on a NAS causes the NAS to send the entire structured username of the user to a RADIUS AAA server the first time the NAS contacts the AAA server. Per-user VPDN can be configured globally, or for individual VPDN groups. Configuring per-user VPDN at the VPDN group level will apply per-user VPDN only to calls associated with that specific VPDN group.

Perform this task on the NAS to configure per-user VPDN for a specific VPDN group.
SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. request-dialin
5. protocol l2tp
6. exit
7. authen-before-forward

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Example: | Router> enable | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| Step 3 | vpdn-group name | Creates a VPDN group and enters VPDN group configuration mode. |
| Example: | Router(config)# vpdn-group 1 | |
| Step 4 | request-dialin | Configures a NAS to request the establishment of an L2TP tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode. |
| Example: | Router(config-vpdn)# request-dialin | |
| Step 5 | protocol l2tp | Specifies the Layer 2 tunneling protocol that the VPDN group will use. |
| Example: | Router(config-vpdn-req-in)# protocol l2tp | |
| Step 6 | exit | Exits to VPDN group configuration mode. |
| Example: | Router(config-vpdn-req-in)# exit | |
Configuring AAA on the NAS and the Tunnel Server

For NAS-initiated dial-in VPDN tunneling and L2TP dial-out tunneling deployments, perform this task on the NAS and the tunnel server.

For client-initiated dial-in VPDN tunneling, perform this task on the tunnel server.

**Before You Begin**

- You must perform the task in the Enabling VPDN on the NAS and the Tunnel Server, on page 27.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login {default | list-name} method1 [method2...]
5. aaa authentication ppp {default | list-name} method1 [method2...]
6. aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]]
7. vpdn aaa attribute {nas-ip-address|vpdn-nas | vpdn-tunnel-client} | nas-port {physical-channel-id | vpdn-nas}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><code>Router(config)# aaa new-model</code></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td>`aaa authentication login {default</td>
<td>list-name} method1 [method2...]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td><code>Router(config)# aaa authentication login default local</code></td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.</td>
</tr>
<tr>
<td>`aaa authentication ppp {default</td>
<td>list-name} method1 [method2...]`</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.</td>
</tr>
<tr>
<td>This command must be configured with the <strong>if-needed</strong> option for the <code>method1</code> argument if you are configuring shell-based authentication for VPDNs. This configures PPP to bypass user authentication if the user has been authenticated at the login prompt.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.</td>
</tr>
<tr>
<td><code>Router(config)# aaa authentication ppp default radius</code></td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
<tr>
<td>`aaa authorization {network</td>
<td>exec</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
<tr>
<td><code>Router(config)# aaa authorization network default radius</code></td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Enables AAA attributes related to a VPDN that will be reported to the AAA server in accounting records.</td>
</tr>
<tr>
<td>`vpdn aaa attribute {nas-ip-address</td>
<td>vpdn-nas</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>(Optional) Enables AAA attributes related to a VPDN that will be reported to the AAA server in accounting records.</td>
</tr>
<tr>
<td>Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.</td>
<td>Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.</td>
</tr>
<tr>
<td><code>Router(config)# vpdn aaa attribute nas-ip-address vpdn-nas</code></td>
<td>Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.</td>
</tr>
</tbody>
</table>

**Configuring Remote AAA for VPDNs**

A remote RADIUS or TACACS+ AAA server can be used for tunnel authentication. For detailed information on configuring remote RADIUS or TACACS+ servers, see the "Additional References" section.

Remote AAA authentication can be configured on the NAS or the tunnel server in these ways:
Dial-In Configurations

• The NAS can be configured to use a remote AAA server.

• The tunnel server, functioning as the tunnel terminator, can be configured to use a remote AAA server for L2TP tunnels only.

Dial-Out Configurations

• The NAS, functioning as the tunnel terminator, can be configured to use a remote AAA server for L2TP tunnels only.

Perform one of these tasks to configure remote AAA for VPDNs:

Configuring the NAS for Remote AAA for Dial-In VPDNs

Perform this task to configure the NAS to use a remote RADIUS or TACACS+ server for tunnel authentication. This task applies only to dial-in VPDN configurations.

Before You Begin

SUMMARY STEPS

1. enable
2. configure terminal
3. Do one of the following:
   • radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname | ip-address}]
   • tacacs-server host {host-name | host-ip-address} [key string] [nat] [port [integer]] [single-connection] [timeout [integer]]
4. Do one of the following:
   • aaa group server radius group-name
   • aaa group server tacacs+ group-name
5. Do one of the following:
   • server ip-address [auth-port port-number] [acct-port port-number]
   • server ip-address

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2**

**configure terminal**

- **Example:**
  
  ```
  Router# configure terminal
  ```

- **Purpose:** Enters global configuration mode.

**Step 3**

- **Do one of the following:**
  - `radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname | ip-address}]`
  - `tacacs-server host {host-name | host-ip-address} [key string] [nat] [port integer] [single-connection] [timeout integer]`

- **Example:**
  
  ```
  Router(config)# radius-server host 10.1.1.1
  ```

- **Example:**
  
  ```
  Router(config)# tacacs-server host 10.2.2.2
  ```

**Step 4**

- **Do one of the following:**
  - `aaa group server radius group-name`
  - `aaa group server tacacs+ group-name`

- **Example:**
  
  ```
  Router(config)# aaa group server radius group1
  ```

- **Example:**
  
  ```
  Router(config)# aaa group server tacacs+ group7
  ```

**Step 5**

- **Do one of the following:**
  - `server ip-address [auth-port port-number] [acct-port port-number]`
  - `server ip-address`

- **Purpose:**
  - (Optional) Configures the IP address of the RADIUS server for the group server.
  - or
  - (Optional) Configures the IP address of the TACACS+ server for the group server.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646</td>
<td>Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-sg-radius)# server 10.2.2.2</td>
<td></td>
</tr>
</tbody>
</table>

### What to Do Next

You must perform the process in the Configuring VPDN Tunnel Authentication section.

### Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels

You can configure the device that terminates the L2TP VPDN tunnel to perform remote RADIUS AAA. Without this functionality, the tunnel terminator can only perform L2TP authentication locally. Local authentication requires that data about the corresponding tunnel endpoint be configured within a VPDN group. This mechanism does not scale well because the information stored in the VPDN groups on each device must be updated independently.

Remote RADIUS authentication allows users to store configurations on the RADIUS server, avoiding the need to store information locally. New information can be added to the RADIUS server as needed, and a group of tunnel terminators can access a common database on the RADIUS server.

Perform this task to configure remote RADIUS AAA for L2TP tunnels on the tunnel terminator. This task can be performed on the tunnel server for dial-in VPDN tunnels, or on the NAS for dial-out VPDN tunnels.

### Before You Begin

- The remote RADIUS AAA server must be configured. For more information on configuring remote RADIUS AAA servers, see the "Additional References" section.
- AAA must be enabled. To enable AAA, perform the task in the "Configuring AAA on the NAS and the Tunnel Server" section.
SUMMARY STEPS

1. enable
2. configure terminal
3. radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname | ip-address}]
4. aaa group server radius group-name
5. server ip-address [auth-port port-number] [acct-port port-number]
6. exit
7. vpdn tunnel authorization network {list-name | default}
8. vpdn tunnel authorization virtual-template vtemplate-number
9. vpdn tunnel authorization password password

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 radius-server host {hostname</td>
<td>ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa group server radius group-name</td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 5 server ip-address [auth-port port-number] [acct-port port-number]</td>
<td>Configures the IP address of the RADIUS server for the group server.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646</td>
<td><strong>Note</strong> Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>exit</code></td>
<td>Exits RADIUS server group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sg-radius)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> `vpdn tunnel authorization network {list-name</td>
<td>default}`</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn tunnel authorization network default</td>
<td>• If the <code>list-name</code> argument was specified in the <code>aaa authorization</code> command, you must use that list name.</td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>vpdn tunnel authorization virtual-template vtemplate-number</code></td>
<td>(Optional) Selects the default virtual template from which to clone virtual access interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn tunnel authorization virtual-template 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <code>vpdn tunnel authorization password password</code></td>
<td>(Optional) Configures a false password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn tunnel authorization password my-secret</td>
<td><strong>Note</strong> If this command is not enabled, the password will always be &quot;cisco.&quot;</td>
</tr>
</tbody>
</table>

**What to Do Next**

You must perform the task in the Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels.
Verifying and Troubleshooting Remote AAA Configurations

Verifying that the VPDN Tunnel Is Up

**SUMMARY STEPS**

1. `enable`
2. `show vpdn tunnel`

**DETAILED STEPS**

**Step 1**

`enable`

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

**Example:**

```
Router> enable
```

**Step 2**

`show vpdn tunnel`

Enter this command to display information about active VPDN tunnels. At least one tunnel and one session must be set up.

**Example:**

```
Router# show vpdn tunnel
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions VPDN Group
4571 61568 csidtw13 est 10.0.195.4 1701 1 ?
LocID RemID TunID Intf Username State Last Chg
4 11 4571 Vi4.1 csidtw9@cisco.com est 00:02:29
%No active PPPoE tunnels
```

Verifying the Remote RADIUS AAA Server Configuration

Perform this task to verify that the remote AAA authorization server is configured on the tunnel endpoint and that the tunnel endpoint can receive attributes 90 and 69 from the RADIUS server.

In this example the steps are performed on the tunnel server, which is performing remote RADIUS AAA as a tunnel terminator. These steps can also be performed on the NAS when remote RADIUS AAA is being performed on the NAS as a tunnel initiator for dial-in VPDNs or as a tunnel terminator for dial-out VPDNs.

**SUMMARY STEPS**

1. `enable`
2. `debug radius`
3. `show logging`
DETAILED STEPS

Step 1  
**enable**
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

**Example:**
```
Router> enable
```

Step 2  
**debug radius**
Enter this command on the tunnel server to display RADIUS debugging messages.

**Example:**
```
Router# debug radius
```

Step 3  
**show logging**
Enter this command on the tunnel server to display the contents of the standard system logging message buffer. Ensure that "access-accept" is in the output and that attributes 90 and 69 can be seen in the RADIUS reply, as shown in bold.

**Example:**
```
Router# show logging
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept
00:32:56: RADIUS: authenticator 73 2B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS: Tunnel-Type [64] 6 00:L2TP [3]
00:32:56: RADIUS: Tunnel-Medium-Type [65] 6 00:IPv4 [1]
00:32:56: RADIUS: Tunnel-Client-Auth-I [90]
   6 00:"csidtw13"
00:32:56: RADIUS: Tunnel-Password [69]
   8 *
00:32:56: RADIUS: Vendor, Cisco [26] 29
00:32:56: RADIUS: Cisco AVpair [1] 23 "vpdn:vpdn-vtemplate=1"
```

Verifying the Remote TACACS+ AAA Server Configuration on the NAS

Perform this task on the NAS to verify that the remote TACACS+ AAA server is properly configured.

**Before You Begin**

Enable these debug commands before performing this task:

- **debug aaa accounting** --Displays information on accountable events as they occur.
- **debug aaa authentication** --Displays information on AAA TACACS+ authentication.
- **debug aaa authorization** --Displays information on AAA TACACS+ authorization.
- **debug tacacs** --Displays information associated with TACACS+.
- **debug vpdn error** --Displays information about Layer 2 protocol-independent errors that occur.
• **debug vpdn events** -- Displays information about Layer 2 protocol-independent events that are part of normal tunnel establishment or shutdown.

• **debug vpdn l2x-errors** -- Displays information about Layer 2 protocol-specific errors that are part of normal PPP tunnel establishment or shutdown.

• **debug vpdn l2x-events** -- Displays information about Layer 2 protocol-specific events that are part of normal PPP tunnel establishment or shutdown.

• **debug vpdn l2x-packets** -- Displays information about Layer 2 protocol-specific

• **debug vtemplate** -- Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.

**SUMMARY STEPS**

1. **enable**
2. **show debugging**
3. Examine the debug output.

**DETAILED STEPS**

**Step 1**  
**enable**  
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

**Example:**

```
Router> enable
```

**Step 2**  
**show debugging**  
Enter this command to display information about the types of debugging that are enabled for your router.

**Example:**

```
Router# show debugging
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
```  

**Step 3**  
Examine the debug output.  
The following example shows complete debug output from the NAS for successful VPDN tunnel establishment using remote TACACS+ AAA authentication at the NAS:

**Example:**

```
Jan 30 12:17:09: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
```
Configuring AAA for VPDNs
Verifying and Troubleshooting Remote AAA Configurations

20:03:18: %LINK-3-UPDOWN: Interface Async1, changed state to up
Jan 30 12:17:09: As1 VPDN: Looking for tunnel -- rtp.cisco.com -Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x278B90) user='rtp.cisco.com'
ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447): Port='Async1' list='default'
service=NET
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) user='rtp.cisco.com'
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447) found list "default"
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) Method=TACACS+
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): user=rtp.cisco.com
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV protocol=vpdn
Jan 30 12:17:09: TAC+: (898425447): received author response status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR (898425447): Post authorization status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-id=rtp_tunnel
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.56
Jan 30 12:17:09: As1 VPDN: Get tunnel info for rtp.cisco.com with NAS
rtp_tunnel, IP 10.31.1.56
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x278B90) user='rtp.cisco.com' ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: As1 VPDN: Forward to address 10.31.1.56
Jan 30 12:17:09: As1 VPDN: Forwarding...
Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x22CDEC) user='user1@rtp.cisco.com'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1
Jan 30 12:17:09: As1 VPDN: Bind interface direction=1
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session FS enabled
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:09: As1 74/1 L2TP: Create session
Jan 30 12:17:09: Tnl 74 L2TP: SM State idle
Jan 30 12:17:09: Tnl 74 L2TP: O SCCRQ
Jan 30 12:17:09: Tnl 74 L2TP: Tunnel state change from idle to wait-ctl-reply
Jan 30 12:17:09: Tnl 74 L2TP: SM State wait-ctl-reply
Jan 30 12:17:09: As1 VPDN: user1@rtp.cisco.com is forwarded
Jan 30 12:17:10: Tnl 74 L2TP: I SCCRP from ABCDE
Jan 30 12:17:10: Tnl 74 L2TP: Got a challenge from remote peer, ABCDE
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x23232C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): found list default
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=1598999635
Jan 30 12:17:10: TAC+: ver=192 id=1598999635 received AUTHEN status = ERROR
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: TAC+: ver=192 id=3400389836 received AUTHEN status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x23232C) user='rtp_tunnel'
ruser='' port=''

VPDN Configuration Guide
42


Verifying the Remote TACACS+ AAA Server Configuration on the Tunnel Server

Perform this task on the tunnel server to verify that the remote TACACS+ AAA server is properly configured.

Before You Begin

Enable these debug commands before performing this task:

- **debug aaa authentication** --Displays information on AAA authentication.
- **debug aaa authorization** --Displays information on AAA authorization.
- **debug aaa accounting** --Displays information on accountable events as they occur. The information displayed by this command is independent of the accounting protocol used to transfer the accounting information to a server.
- **debug tacacs+** --Displays detailed debugging information associated with TACACS+.
• **debug vtemplate** -- Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends.

• **debug vpdn error** -- Displays errors that prevent a PPP tunnel from being established or errors that cause an established tunnel to be closed.

• **debug vpdn events** -- Displays messages about events that are part of normal PPP tunnel establishment or shutdown.

• **debug vpdn l2x-errors** -- Displays messages about events that are part of normal PPP tunnel establishment or shutdown.

• **debug vpdn l2x-events** -- Displays messages about events that are part of normal PPP tunnel establishment or shutdown for Layer 2.

**SUMMARY STEPS**

1. **enable**
2. **show debugging**
3. Examine the debug output.

**DETAILED STEPS**

**Step 1**  
**enable**  
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

**Example:**

Router> enable

**Step 2**  
**show debugging**  
Enter this command to display information about the types of debugging that are enabled for your router.

**Example:**

Router# show debugging  
General OS:  
AAA Authentication debugging is on  
AAA Authorization debugging is on  
AAA Accounting debugging is on  
VPN:  
L2X protocol events debugging is on  
L2X protocol errors debugging is on  
VPDN events debugging is on  
VPDN errors debugging is on  
VTEMPLATE:  
Virtual Template debugging is on

**Step 3**  
Examine the debug output.  
The following example shows complete debug output from the tunnel server for successful VPDN tunnel establishment using remote TACACS+ AAA authentication at the NAS:
Example:

Jan 30 12:17:09: L2TP: I SCCRQ from rtp_tunnel tnl 74
Jan 30 12:17:09: Tnl 56 L2TP: New tunnel created for remote
rtp_tunnel, address 10.31.1.144
Jan 30 12:17:09: Tnl 56 L2TP: Got a challenge in SCCRQ, rtp_tunnel
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x21F6D0) user='ABCDE'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): found list default
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = UNKNOWN
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): Method=TACACS+
Jan 30 12:17:09: TAC+: send AUTHEN/START packet ver=193 id=3194595626
Jan 30 12:17:09: TAC+: ver=192 id=3194595626 received AUTHEN status = ERROR
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x2281AC) user='ABCDE'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: TAC+: ver=192 id=3639011179 received AUTHEN status = PASS
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x2281AC) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = PASS
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): Method=TACACS+
Jan 30 12:17:09: TAC+: send AUTHEN/START packet ver=193 id=3194595626
Jan 30 12:17:09: TAC+: ver=192 id=3194595626 received AUTHEN status = ERROR
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x227F3C) user='ABCDE'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN (4117701992): status = UNKNOWN
Jan 30 12:17:09: AAA/AUTHEN/START (4117701992): Method=TACACS+
Jan 30 12:17:10: TAC+: ver=192 id=3639011179 received AUTHEN status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN (4117701992): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port='' rem_addr''
Verifying L2TP Tunnel Establishment PPP Negotiations and Authentication with the Remote Client

Perform this task to verify that the L2TP tunnel has been established and that the tunnel server can perform PPP negotiation and authentication with the remote client.

In this example the steps are performed on the tunnel server, which is performing remote AAA as a tunnel terminator. These steps can also be performed on the NAS when remote AAA is being performed on the NAS as a tunnel initiator for dial-in VPDNs or as a tunnel terminator for dial-out VPDNs.

SUMMARY STEPS

1. enable
2. debug ppp negotiation
3. debug ppp authentication
4. show logging

DETAILED STEPS

Step 1  enable
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example:

Router> enable

Step 2  debug ppp negotiation
Enter this command on the tunnel server to display PPP negotiation debugging messages.

Example:

Router# debug ppp negotiation

Step 3  debug ppp authentication
Enter this command on the tunnel server to display PPP authentication debugging messages.
Example:

```plaintext
Router# debug ppp authentication
```

**Step 4**

**show logging**

Enter this command on the tunnel server to display the contents of the standard system logging message buffer. Observe that the tunnel server receives a PPP Challenge Handshake Authentication Protocol (CHAP) challenge and then sends a PPP CHAP "SUCCESS" to the client.

Example:

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1 Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection to established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the tunnel server has received Link Control Protocol (LCP) IP Control Protocol (IPCP) packets, and that negotiation is successful.

Example:

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 10.1.1.4
```

**Configuring Directed Request Authorization of VPDN Users**

Directed request authorization of VPDN users can be configured on the NAS or on the tunnel server. The directed request configuration is performed on the device that ultimately performs the authentication. Directed requests are most commonly configured on the tunnel server.

Perform one of these tasks to enable directed request authorization of VPDN users.

**Configuring Directed Request Authorization of VPDN Users on the Tunnel Server**

Perform this task on the tunnel server to configure directed request authorization of VPDN users when the tunnel server performs authentication.
Before You Begin

SUMMARY STEPS

1. enable
2. configure terminal
3. ip host \{name | t modem-telephone-number\} [tcp-port-number] address1 [address2...address8]
4. Do one of the following:
   - radius-server directed-request [restricted]
   - tacacs-server directed-request [restricted] [no-truncate]
5. vpdn authorize directed-request

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip host {name</td>
<td>t modem-telephone-number} [tcp-port-number] address1 [address2...address8]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ip host example.com 10.3.3.3</td>
<td>Note: The IP address specified with the ip host command must match the IP address you configured with the radius-server host or tacacs-server host command when performing the task in the Configuring Remote AAA for VPDNs, on page 33.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
<td>Allows users logging in to a NAS to select a RADIUS server for authentication.</td>
</tr>
<tr>
<td></td>
<td>• radius-server directed-request [restricted]</td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>• tacacs-server directed-request [restricted] [no-truncate]</td>
<td>Allows users logging in to a NAS to select a TACACS+ server for authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# radius-server directed-request</td>
<td></td>
</tr>
</tbody>
</table>
Enables VPDN authorization for directed request users.

Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpdn authorize directed-request</td>
<td>Enables VPDN authorization for directed request users.</td>
</tr>
</tbody>
</table>

What to Do Next

You must perform the process in the Configuring VPDN Tunnel Authentication section.

Configuring Directed Request Authorization of VPDN Users on the NAS

Perform this task on the NAS to configure directed request authorization of VPDN users when the NAS performs authentication.

Before You Begin

You must perform the task in the "Remote AAA for VPDNs" section.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip host {name | t modem-telephone-number} [tcp-port-number] address1 [address2...address8]
4. Do one of the following:
   - radius-server directed-request [restricted]
   - tacacs-server directed-request [restricted] [no-truncate]
5. vpdn authorize directed-request

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Configuring AAA for VPDNs

#### Configuring Domain Name Prefix and Suffix Stripping

A single set of stripping rules can be configured globally. An independent set of stripping rules can be configured for each virtual private network (VPN) routing and forwarding (VRF) instance.

Global stripping rules are applied to all usernames, and per-VRF rules are applied only to usernames associated with the specified VRF. If a per-VRF rule is configured, it will take precedence over the global rule for usernames associated with that VRF.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

Specifies or modifies the hostname for the network server.

- `ip host {name | t modem-telephone-number} [tcp-port-number] address1 [address2...address8]`

Example:

```
Router(config)# ip host example.com 10.3.3.3
```

**Note**

The IP address specified with the `ip host` command must match the IP address you configured with the `radius-server host` or `tacacs-server host` command when performing the task in the Configuring Remote AAA for VPDNs, on page 33.

**Step 4**

Do one of the following:

- `radius-server directed-request [restricted]`
- `tacacs-server directed-request [restricted] [no-truncate]`

Example:

```
Router(config)# radius-server directed-request
```

Example:

```
Router(config)# tacacs-server directed-request
```

**Step 5**

Enables VPDN authorization for directed request users.

- `vpdn authorize directed-request`

Example:

```
Router(config)# vpdn authorize directed-request
```

**What to Do Next**

You must perform the process in the Configuring VPDN Tunnel Authentication section.
Perform this task on the NAS to configure a set of global or per-VRF stripping rules.

Before You Begin

- AAA must be enabled on the NAS. See the "Configuring AAA on the NAS and the Tunnel Server" section.
- You must understand the usage guidelines for the `radius-server domain-stripping` command as described in the VPDN command reference.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. Do one of the following:
   - `radius-server domain-stripping [right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]`
   - `tacacs-server domain-stripping [right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]`
4. Do one of the following:
   - `radius-server domain-stripping strip-suffix suffix [vrf vrf-name]`
   - `tacacs-server domain-stripping strip-suffix suffix [vrf vrf-name]`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> Do one of the following:</td>
<td>(Optional) Configures a router to strip suffixes, or both suffixes and prefixes, from the username before forwarding the username to the RADIUS server. or (Optional) Configures a router to strip suffixes, or both suffixes and prefixes, from the username before forwarding the username to the TACACS+ server.</td>
</tr>
<tr>
<td>- <code>radius-server domain-stripping [right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]</code></td>
<td></td>
</tr>
<tr>
<td>- <code>tacacs-server domain-stripping [right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• tacacs-server domain-stripping [right-to-left] [prefix-delimiter character [character2...character7]] [delimiter character [character2...character7]] [vrf vrf-name]</td>
<td>Right-to-left -- Configures the router to parse the username for a delimiter from right to left, rather than in the default direction of left to right. The prefix or suffix will be stripped at the first valid delimiter character detected by the router. Changing the direction that the router parses the username will control the portion of the username that is stripped if multiple valid delimiters are present.</td>
</tr>
<tr>
<td>Example:</td>
<td>Only one parse direction can be configured per set of global or per-VRF rules. The router cannot be configured to parse for prefixes in one direction, and parse for suffixes in the other direction.</td>
</tr>
<tr>
<td>Router(config)# radius-server domain-stripping prefix-delimiter %$/$ delimiter @/</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enabling prefix stripping will automatically enable suffix stripping using the default suffix delimiter @, unless a different suffix delimiter is configured using the delimiter character keyword and argument.</td>
</tr>
<tr>
<td>Router(config)# tacacs-server domain-stripping prefix-delimiter %$/$ vrf myvrf</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4

Do one of the following:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• radius-server domain-stripping strip-suffix suffix [vrf vrf-name]</td>
<td>(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the RADIUS server.</td>
</tr>
<tr>
<td>• tacacs-server domain-stripping strip-suffix suffix [vrf vrf-name]</td>
<td>or</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the TACACS+ server.</td>
</tr>
<tr>
<td>Router(config)# radius-server</td>
<td>• strip-suffix suffix -- Enables per-suffix suffix stripping and specifies the string that must be matched for the suffix to be stripped.</td>
</tr>
<tr>
<td></td>
<td>Note Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters in .</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>domain-stripping strip-suffix cisco.com</code></td>
<td><strong>vrf</strong> <code>vrf-name</code> --Restricts the per-suffix stripping configuration to a VRF instance. The <code>vrf-name</code> argument specifies the name of a VRF.</td>
</tr>
</tbody>
</table>

**Note** You can configure a single ruleset to strip multiple specific suffixes by performing this step multiple times.

### What to Do Next

You must perform the process in the Configuring VPDN Tunnel Authentication section.

### Configuring VPDN Tunnel Authentication

VPDN tunnel authentication enables routers to authenticate the other tunnel endpoint before establishing a VPDN tunnel. VPDN tunnel authentication is optional but highly recommended for L2TP, L2TPv3, and PPTP tunnels.

By default, the router will use the hostname as the tunnel name in VPDN tunnel authentication. If a local name is configured under a VPDN group, the router will use the local name when negotiating authentication for tunnels belonging to that VPDN group.

For NAS-initiated VPDN deployments VPDN deployments, tunnel authentication requires that a single shared secret be configured on both the NAS and the tunnel server. For L2TP tunnels, the password can be configured using the hostname, the local name, or the L2TP tunnel password.

For client-initiated VPDN tunneling deployments, tunnel authentication requires that a single shared secret be configured on both the client and the tunnel server. The available authentication configuration options depend on the tunneling protocol being used.

For L2TPv3 client-initiated VPDN tunnels, the shared secret can be configured on the local peer router and the tunnel server in either of these ways:

- In an L2TP class configuration. Perform the task Configuring L2TP Control Channel Authentication Parameters in the Configuring Client-Initiated Dial-In VPDN Tunneling module instead of the process documented in this section.
  - Using the hostname of the router as described in the process documented in this section.

For L2TP client-initiated VPDN tunnels, the shared secret can be configured on the tunnel server using the hostname, the local name, or the L2TP tunnel password as described the process documented in this section. The shared secret can be configured on the local peer router in either of these ways:

- In an L2TP class configuration. Perform the task Configuring L2TP Control Channel Authentication Parameters in the Configuring Client-Initiated Dial-In VPDN Tunneling module instead of the process documented in this section.
  - Using the hostname of the router as described in the process documented in this section.
For PPTP client-initiated VPDN tunnels, authentication parameters can be configured by using the hostname or the local name as described in the process documented in this section.

To configure VPDN tunnel authentication, you must perform one of the following tasks on the NAS and the tunnel server as required. You need not choose the same method to configure the secret on the NAS and the tunnel server. However, the configured password must be the same on both devices.

VPDN tunnel authentication is optional for L2TP tunnels. Perform this task on the NAS and the tunnel server if you want to disable VPDN tunnel authentication:

**Prerequisites**

AAA must be enabled. See the Configuring AAA on the NAS and the Tunnel Server section.

**Configuring VPDN Tunnel Authentication Using the Hostname**

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the hostname.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **hostname name**
4. **username name password secret**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> hostname name</td>
<td>Specifies or modifies the hostname for the network server.</td>
</tr>
<tr>
<td>Example: Router(config)# hostname tunnelserver12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> username name password secret</td>
<td>Establishes a username-based authentication system.</td>
</tr>
</tbody>
</table>
Configuring AAA for VPDNs

Configuring VPDN Tunnel Authentication

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Router(config)# username nas4 password mysecret |
| • The specified username must be the name of the remote router. |
| • The secret password must be the same on both routers. |

What to Do Next

• Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.

Configuring VPDN Tunnel Authentication Using the Local Name

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the local name.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. local name host-name
5. exit
6. username name password secret

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Router> enable |
| Enables privileged EXEC mode. |
| • Enter your password if prompted. |
| Step 2 | configure terminal |
| Example: | 
Router# configure terminal |
<p>| Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>vpdn-group name</td>
<td>Enters VPDN group configuration mode and creates a VPDN group.</td>
</tr>
<tr>
<td><strong>Example:</strong>*</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group mygroup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>local name host-name</td>
<td>Specifies a local hostname that the tunnel will use to identify itself.</td>
</tr>
<tr>
<td><strong>Example:</strong>*</td>
<td></td>
</tr>
<tr>
<td>Router(config-vpdn)# local name tunnelserver2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>*</td>
<td></td>
</tr>
<tr>
<td>Router(config-vpdn)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>username name password secret</td>
<td>Establishes a username-based authentication system.</td>
</tr>
<tr>
<td><strong>Example:</strong>*</td>
<td></td>
</tr>
<tr>
<td>Router(config)# username nas? password mysecret</td>
<td></td>
</tr>
</tbody>
</table>

**What to Do Next**

- Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.

**Configuring VPDN Tunnel Authentication Using the L2TP Tunnel Password**

Perform this task on the NAS or tunnel server to configure VPDN tunnel authentication using the L2TP tunnel password. This task can be used only for VPDN tunnel authentication of L2TP tunnels.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vpdn-group name
4. l2tp tunnel password password
5. local name host-name
6. exit
7. username name password secret
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router&gt; enable</strong></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router# configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>vpdn-group name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# vpdn-group mygroup</strong></td>
</tr>
<tr>
<td></td>
<td>Enters VPDN group configuration mode and creates a VPDN group.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>l2tp tunnel password password</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-vpdn)# l2tp tunnel password mysecret</strong></td>
</tr>
<tr>
<td></td>
<td>Sets the password that the router will use to authenticate the tunnel.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>local name host-name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-vpdn)# local name tunnelserver2</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies a local hostname that the tunnel will use to</td>
</tr>
<tr>
<td></td>
<td>identify itself.</td>
</tr>
<tr>
<td></td>
<td>• You must perform this step if the remote router does not use the L2TP tunnel password.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-vpdn)# exit</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Exits VPDN group configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• You must perform this step only if the remote router does not</td>
</tr>
<tr>
<td></td>
<td>use the L2TP tunnel password method of VPDN tunnel authentication.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>username name password secret</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# username nas64 password mysecret</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Establishes a username-based authentication system.</td>
</tr>
<tr>
<td></td>
<td>• You need to perform this step only if the remote router does not</td>
</tr>
<tr>
<td></td>
<td>use the L2TP tunnel password method of VPDN tunnel authentication.</td>
</tr>
<tr>
<td></td>
<td>• The specified username must be the name of the remote router.</td>
</tr>
<tr>
<td></td>
<td>• The password must be the same on both routers.</td>
</tr>
</tbody>
</table>
What to Do Next

- Once you have configured a secret password on one tunnel endpoint, you must configure the same tunnel secret on the corresponding tunnel endpoint.

Disabling VPDN Tunnel Authentication for L2TP Tunnels

Perform this task to disable VPDN tunnel authentication for L2TP tunnels. You must perform this task on both the NAS and the tunnel server to disable VPDN tunnel authentication.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. no l2tp tunnel authentication

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vpdn-group name</td>
<td>Enters VPDN group configuration mode and creates a VPDN group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn-group mygroup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>no l2tp tunnel authentication</td>
<td>Disables L2TP tunnel authentication.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn)# no l2tp tunnel authentication</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS Tunnel Accounting for L2TP VPDNs

The new RADIUS tunnel accounting types are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

Perform this task to configure a NAS or tunnel server to send tunnel and tunnel-link accounting records to the remote RADIUS server.

Before You Begin

- You must perform the tasks in the Configuring AAA on the NAS and the Tunnel Server, on page 32.
- You must configure the router to use a remote RADIUS AAA server as described in the Configuring Remote AAA for VPDNs, on page 33.
- You must perform the tasks in the "Configuring VPDN Tunnel Authentication" section.

Note

RADIUS tunnel accounting is supported only for VPDNs using the L2TP protocol.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa accounting network default {list-name} {start-stop | stop-only | wait-start | none} group groupname
4. vpdn tunnel accounting network list-name
5. vpdn session accounting network list-name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa accounting network default {list-name} {start-stop</td>
</tr>
<tr>
<td></td>
<td>Enables network accounting.</td>
</tr>
<tr>
<td></td>
<td>• default --If the default network accounting method-list is configured and no additional accounting configurations are enabled on the</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Router(config)# aaa accounting network list1 start-stop group radius | interface, network accounting is enabled by default. If either the `vpdn session accounting network` command or the `vpdn tunnel accounting network` command is linked to the `default` method-list, all tunnel and tunnel-link accounting records are enabled for those sessions.  
  - `list-name` -- The `list-name` defined in the `aaa accounting` command must be the same as the `list-name` defined in the VPDN command; otherwise, accounting will not occur. |
| **Step 4**       |         |
| `vpdn tunnel accounting network list-name` | Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records.  
  - `list-name` -- The `list-name` must match the `list-name` defined in the `aaa accounting` command; otherwise, network accounting will not occur. |
| **Example:**     |         |
| Router(config)# vpdn tunnel accounting network list1 |         |
| **Step 5**       |         |
| `vpdn session accounting network list-name` | Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records.  
  - `list-name` -- The `list-name` must match the `list-name` defined in the `aaa accounting` command; otherwise, network accounting will not occur. |
| **Example:**     |         |
| Router(config)# vpdn session accounting network list1 |         |

**Configuring Authentication of L2TP Tunnels at the Tunnel Terminator Remote RADIUS AAA Server**

For L2TP tunnels, you can configure the device that terminates the VPDN tunnel to perform remote RADIUS AAA. A remote RADIUS AAA server can be used to perform VPDN tunnel authentication on the tunnel terminator as follows:

- Using a remote RADIUS AAA server on the tunnel server for dial-in VPDNs
- Using a remote RADIUS AAA server on the NAS for dial-out VPDNs

Perform this task on the remote RADIUS AAA server to configure the RADIUS server to authenticate VPDN tunnels at the device that terminates the tunnel.

**Before You Begin**

- The RADIUS server must be configured for AAA. For more information on configuring remote RADIUS AAA servers, see the "Additional References" section.
- The service type in the RADIUS user profile for the tunnel initiator should always be set to "Outbound."
This task applies only when the device that terminates the VPDN tunnel is performing remote RADIUS AAA. To configure the tunnel terminator to perform remote RADIUS AAA, perform the task in the "Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels" section.

**SUMMARY STEPS**

1. **service type** = *Outbound*
2. **tunnel-type** = *protocol*
3. **Cisco:Cisco-Avpair** = **vpdn:dout-dialer** = *NAS-dialer-number*
4. **Cisco:Cisco-Avpair** = **vpdn:vpdn-vtemplate** = *vtemplate-number*

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies the service type.</td>
</tr>
<tr>
<td>service type = <strong>Outbound</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>service type = Outbound</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the tunneling protocol.</td>
</tr>
<tr>
<td>tunnel-type = <strong>protocol</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>tunnel-type = l2tp</td>
<td><em>Note</em> L2TP is the only valid protocol for this task.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies which dialer to use on the NAS for dial-out configuration.</td>
</tr>
<tr>
<td><strong>Cisco:Cisco-Avpair</strong> = <strong>vpdn:dout-dialer</strong> = NAS-dialer-number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco:Cisco-Avpair = vpdn:dout-dialer = 2</td>
<td><em>Note</em> Perform this step only for dial-out configurations.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the virtual template number to use on the tunnel server for dial-in configuration.</td>
</tr>
<tr>
<td><strong>Cisco:Cisco-Avpair</strong> = <strong>vpdn:vpdn-vtemplate</strong> = vtemplate-number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate = 1</td>
<td><em>Note</em> Perform this step only for dial-in configurations.</td>
</tr>
<tr>
<td><em>Note</em> This configuration is optional if the vpdn tunnel authorization virtual-template command is used in the task in the Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels, on page 36.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Tunnel Assignments on the NAS Remote RADIUS AAA Server

Tunnel assignments allow the grouping of users from different per-user or domain RADIUS profiles into the same active tunnel. This functionality prevents the establishment of duplicate tunnels when the tunnel type, tunnel endpoints, and tunnel assignment ID are identical.

Perform this task on the NAS remote RADIUS AAA server for each user and domain that you want to group into the same tunnel.

**Before You Begin**
The RADIUS server must be configured for AAA.

**SUMMARY STEPS**

1. Do one of the following:

   - `user @ domain.com  Password = " secret "  Service-Type = Outbound`
   - `user.domain.com  Password = " secret "  Service-Type = Outbound`

2. `tunnel-type = protocol`

3. `tunnel-server-endpoint = ip-address`

4. `tunnel-assignment-id = name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies the user or domain, the tunnel password, and the service type.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td>- <code>user @ domain.com  Password = &quot; secret &quot;  Service-Type = Outbound</code></td>
<td></td>
</tr>
<tr>
<td>- <code>user.domain.com  Password = &quot; secret &quot;  Service-Type = Outbound</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:user@cisco.com">user@cisco.com</a> Password = &quot;cisco&quot; Service-Type = Outbound</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>user.cisco.com Password = &quot;cisco&quot; Service-Type = Outbound</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the tunneling protocol used.</td>
</tr>
<tr>
<td><code>tunnel-type = protocol</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>tunnel-type = l2tp</code></td>
<td></td>
</tr>
<tr>
<td>* The tunnel type must be identical for users to be grouped into the same tunnel.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>tunnel-server-endpoint = ip-address</strong></td>
</tr>
<tr>
<td></td>
<td>Specifies the IP address of the tunnel server that calls from</td>
</tr>
<tr>
<td></td>
<td>the specified user or domain are tunneled to.</td>
</tr>
<tr>
<td></td>
<td>• The tunnel server endpoint must be identical for users</td>
</tr>
<tr>
<td></td>
<td>to be grouped into the same tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>tunnel-server-endpoint = 10.1.1.1</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>tunnel-assignment-id = name</strong></td>
</tr>
<tr>
<td></td>
<td>Specifies the tunnel ID that calls from the specified user or</td>
</tr>
<tr>
<td></td>
<td>domain are assigned.</td>
</tr>
<tr>
<td></td>
<td>• The tunnel assignment ID must be identical for users</td>
</tr>
<tr>
<td></td>
<td>to be grouped into the same tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>tunnel-assignment-id = group1</strong></td>
</tr>
</tbody>
</table>

### Configuring Secure Tunnel Authentication Names on the NAS Remote RADIUS AAA Server

The NAS AAA server can be configured with authentication names other than the default names for the NAS and the NAS AAA server, providing a higher level of security during VPDN tunnel establishment.

RADIUS tunnel authentication name attributes allows you to specify a name other than the default name for the tunnel initiator and for the tunnel terminator. These authentication names are specified using RADIUS tunnel attributes 90 and 91.

Perform this task on the remote RADIUS AAA server. This task applies to NAS-initiated tunnels using either L2TP or L2F.

**Before You Begin**

- The RADIUS server must be configured for AAA.
- The NAS must be able to recognize RADIUS attributes 90 and 91.
- The RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91. Tagged attributes are defined in RFC 2868, *RADIUS Tunnel Authentication Attributes*.

**SUMMARY STEPS**

1. Do one of the following:
   - `user @ example.com Password = "secret" Service-Type = Outbound`
   - `user.example.com Password = "secret" Service-Type = Outbound`

2. `tunnel-client-auth-id = {1 | 2}: "NAS-name"`

3. `tunnel-server-auth-id = {1 | 2}: "tunnel-server-name"`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies the user or domain, the tunnel password, and the service type.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
</tbody>
</table>
| • *user* \@ *example.com*  
  **Password** = "*secret*"  
  **Service-Type** = Outbound | |
| • *user.*example.com*  
  **Password** = "*secret*"  
  **Service-Type** = Outbound | |
| Example: | user@cisco.com Password = "cisco" Service-Type = Outbound |
| Example: | user.cisco.com Password = "cisco" Service-Type = Outbound |

| **Step 2** | Specifies the name used by the NAS when it authenticates tunnel setup with the tunnel server. |
| *tunnel-client-auth-id* = \{:1 | :2\} : "NAS-name" | |
| Example: | tunnel-client-auth-id = :2:NAS36 |

| **Step 3** | Specifies the name used by the tunnel server when it authenticates tunnel setup with the NAS. |
| *tunnel-server-auth-id* = \{:1 | :2\} : "tunnel-server-name" | |
| Example: | tunnel-server-auth-id = :2:TS14 |

### Configuring L2TP Forwarding of PPPoE Tagging Information

#### Configuring L2TP Forwarding of the PPPoE Tagging Information

On the LAC, perform these steps to configure L2TP Forwarding of PPPoE Tagging Information to populate the circuit-id tag in the nas-port-id attribute and the remote-id tag in the calling-station-id attribute on the LNS.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vpdn-group name`
4. `dsl-line-info-forwarding`
5. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- [Example:](#) `Router> enable`  
  - Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
- [Example:](#) `Router# configure terminal` |
| **Step 3** vpdn-group `name` | Creates a VPDN group and enters VPDN group configuration mode.  
- [Example:](#) `Router(config)# vpdn-group pppoe-group` |
| **Step 4** `dsl-line-info-forwarding` | Enables the processing of the received PPPoE Vendor-Specific tag in the PADR packet, and sends a matching VSA to the AAA server in RADIUS access and accounting requests.  
- [Example:](#) `Router(config-vpdn)# dsl-line-info-forwarding` |
| **Step 5** `exit` | Exits VPDN group configuration mode.  
- [Example:](#) `Router(config-vpdn)# exit` |

### Overriding L2TP Forwarding of PPPoE Tag Information

You can configure the L2TP Forwarding of PPPoE Tagging Information feature to override the following VSA:
Overriding nas-port VSA with circuit-id

To override the population of the circuit-id tag in the nas-port-id attribute on the LNS, perform these steps on the LNS.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `radius-server attribute 87 circuit-id`
4. `exit`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>radius-server attribute 87 circuit-id</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# radius-server attribute 87 circuit-id</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# exit</code></td>
</tr>
</tbody>
</table>

Overriding calling-station-id VSA with remote-id

To override the calling-station-id VSA with the remote-id on the LNS, perform these steps:
SUMMARY STEPS

1. enable
2. configure terminal
3. radius-server attribute 31 remote-id
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router # configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 radius-server attribute 31 remote-id</td>
<td>Overrides the calling-station-id attribute with Remote-ID attribute in RADIUS access and accounting requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# radius-server attribute 31 remote-id</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Removing L2TP Forwarding of PPPoE Tag Information

Outgoing PADO and PADS packets will have the DSLAM-inserted Vendor-Specific Line-Id tag, and DSLAM must strip the Circuit-Id tag from the packets. If the DSLAM cannot strip the tag, the BRAS must remove it before sending out the packets. This task is accomplished through configuration of the vendor-tag remote-id strip command under BBA group configuration mode.
SUMMARY STEPS

1. enable
2. configure terminal
3. bba-group pppoe group-name
4. vendor-tag remote-id strip

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> bba-group pppoe group-name</td>
<td>Defines a PPPoE profile and enters BBA group configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# bba-group pppoe pppoe-group</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vendor-tag remote-id strip</td>
<td>Enables the BRAS to strip off incoming Vendor-Specific Remote-Id tags from outgoing PADO and PADS packets.</td>
</tr>
<tr>
<td>Example: Router(config-bba-group)# vendor-tag remote-id strip</td>
<td></td>
</tr>
</tbody>
</table>

Displaying the Session Activity Log

When the `radius-server attribute nas-port format d` global configuration command is added to the PPPoE Circuit-Id Tag Processing feature configuration on the BRAS (see the Examples Configuring the VPDN Tunnel Authorization Search Order, on page 82 for an example), the report from the `debug radius` privileged EXEC command will include information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

SUMMARY STEPS

1. Enable the `debug radius` command to display a report of session activity. In the example shown in this section:
Enable the **debug radius** command to display a report of session activity. In the example shown in this section:

- The acct_session_id is 79 or 4F in hexadecimal format.
- In the message *Acct-session-id pre-pended with Nas Port = 0/0/0/200*, the interface on which the PPPoE discovery frames arrived is FastEthernet0/0.0.200. The 0/0/0 is Cisco format for slot/subslot/port.
- The Acct-Session-Id vendor-specific attribute 44 contains the string 0/0/0/200_0000004F, which is a combination of the ingress interface and the session identifier.

**Note** Strings of interest in the **debug radius** output log are presented in bold text for purpose of example only.

**Example:**

```
Router# debug radius
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS/ENCODE(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS: authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS: User-Name [1] 7 "peer1"
02:10:49: RADIUS: NAS-Port-Type [61] 6 Ethernet
02:10:49: RADIUS: NAS-Port-Id [87] 22 "FastEthernet6/0.200:"
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32 02:10:49:
RADIUS: authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION Event PPP_LOCAL
02:10:49: [62]PPPoE 65/SB: Sent vtemplate request on base V12
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED Event VA_RESP
02:10:49: [62]PPPoE 65: V12.1 interface obtained
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attr
02:10:49: [62]PPPoE 65: AAA get dynamic attr
02:10:49: RADIUS/ENCODE(0000003F): Orig. component type = PPP
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1646/42, len 117
02:10:49: RADIUS: authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
02:10:49: RADIUS: Acct-Session-Id [44] 20 "0/0/0/200_0000004F"
02:10:49: RADIUS: User-Name [1] 7 "peer1"
02:10:49: RADIUS: Acct-Status-Type [40] 6 Start
02:10:49: RADIUS: NAS-Port-Type [61] 6 Ethernet
02:10:49: RADIUS: NAS-Port-Id [87] 22 "FastEthernet6/0.200:"
02:10:49: RADIUS: Acct-Delay-Time [41] 6 0
```
Configuring L2TP Override Forwarding rx-speed and tx-speed Values Received from PPPoE

By default, L2TP obtains the receive-speed (rx-speed) and transmit-speed (tx-speed) values from PPPoE and sends the values to LNS. To override L2TP forwarding of the rx-speed and tx-speed values received from PPPoE, the rx-speed and the tx-speed values should be configured in the RADIUS server, or by using the **l2tp rx-speed** and **l2tp tx-speed** commands in VPDN group configuration or VPDN template configuration mode. The speed values are configured in kbps.

**Configuring rx-speed and tx-speed Values When the RADIUS Server Is Not Used**

When the RADIUS server is not used, the rx-speed and the tx-speed values can be configured in VPDN group configuration or VPDN template configuration mode. The rx-speed and tx-speed values configured in VPDN group configuration mode are specific to the tunnel and are sent to all sessions under the tunnel.

Perform this task to configure rx-speed and tx-speed values in VPDN group configuration or VPDN template configuration mode when the RADIUS server is not used.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vpdn enable
4. Do one of the following:
   - vpdn-group name
   - vpdn-template name
5. l2tp rx-speed value
6. l2tp tx-speed value
7. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables VPDN on the router.</td>
</tr>
<tr>
<td><code>vpdn enable</code></td>
<td>Example: Router(config)# vpdn enable</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td><code>vpdn-group name</code></td>
<td>or</td>
</tr>
<tr>
<td><code>vpdn-template name</code></td>
<td>or</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters VPDN template configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn-group 1</td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn-template 1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Sends the rx-speed value to LNS.</td>
</tr>
<tr>
<td><code>l2tp rx-speed value</code></td>
<td>Example: Router(config-vpdn)# l2tp rx-speed 15000</td>
</tr>
<tr>
<td></td>
<td>• If the rx-speed value is not provided, L2TP receives the rx-speed value from PPPoE.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The command is the same irrespective of whether it is entered from VPDN group configuration or VPDN template configuration mode. These steps show how to enter the command from VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sends the tx-speed value to LNS.</td>
</tr>
<tr>
<td><code>l2tp tx-speed value</code></td>
<td>Example: Router(config-vpdn)# l2tp tx-speed 15000</td>
</tr>
<tr>
<td></td>
<td>• If the tx-speed value is not provided, L2TP receives the tx-speed value from PPPoE.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exits VPDN group configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Example: Router(config-vpdn)# end</td>
</tr>
</tbody>
</table>
Configuring rx-speed and tx-speed Values on the RADIUS Server

You can configure the rx-speed and tx-speed values on the RADIUS server by specifying the rx-speed and tx-speed values on the RADIUS server.

The values configured for rx-speed and tx-speed are session oriented. L2TP stores the rx-speed and tx-speed values for every session by using the `vpdn-authen-before-forward` command configured on LAC.

The steps for configuring the default rx-speed and tx-speed values on the RADIUS server are the same as configuring the rx-speed and tx-speed values when the RADIUS server is not used. For configuring rx-speed and tx-speed values on the RADIUS server, see the Configuring rx-speed and tx-speed Values When the RADIUS Server Is Not Used section.

Configuring rx-speed and tx-speed Values from ANCP on the RADIUS Server

ANCP sends the upstream and downstream values to L2TP. The upstream value is the rx-speed value and the downstream value is the tx-speed value.

Perform this task on the RADIUS server to configure rx-speed and tx-speed values from ANCP.

**Before You Begin**

- The quality of service (QoS) policy must be attached to PPPoE between the client and the LAC.
- The ANCP session and the ANCP neighbor session must be started.
- The average rate traffic shaping value must be configured for the default class by using the `shape average` command in policy-map class configuration mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vpdn enable`
4. Do one of the following:
   - `vpdn-group name`
   - `vpdn-template name`
5. `l2tp rx-speed ancp [value]`
6. `l2tp tx-speed ancp [value]`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn enable</td>
<td>Enables VPDN on the router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>• vpdn-group <em>name</em></td>
<td>Enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>• vpdn-template <em>name</em></td>
<td>or</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn-template 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> l2tp rx-speed ancp <em>value</em></td>
<td>Sends the rx-speed value to LNS if a value is not configured for ANCP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn)# l2tp rx-speed ancp 15000</td>
<td>• If the rx-speed value is not configured for ANCP and the rx-speed value is not provided in the command, L2TP sends the rx-speed value configured in VPDN group configuration or VPDN template configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• If the rx-speed value is not configured in VPDN group configuration or VPDN template configuration mode, L2TP sends the average rate traffic shaping value to LNS.</td>
</tr>
<tr>
<td></td>
<td>• For ATM interfaces, if the average rate traffic shaping value is not configured, L2TP sends the rx-speed value configured in VC-class configuration mode. If the rx-speed value is not configured in VC-class configuration mode, L2TP sends the rx-speed value obtained from PPPoE.</td>
</tr>
<tr>
<td></td>
<td>• For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the rx-speed value obtained from PPPoE.</td>
</tr>
<tr>
<td><strong>Step 6</strong> l2tp tx-speed ancp <em>value</em></td>
<td>Sends the tx-speed value to LNS if a value is not configured for ANCP.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example: &lt;br&gt;Router(config-vpdn)# l2tp tx-speed ancp 15000</td>
<td>• If the tx-speed value is not configured for ANCP and the tx-speed is not provided in the command, L2TP sends the tx-speed value configured in VPDN group configuration or VPDN template configuration mode.  &lt;br&gt;• If the tx-speed value is not configured in VPDN group configuration or VPDN template configuration mode, L2TP sends the average rate traffic shaping value to LNS.  &lt;br&gt;• For ATM interfaces, if the average rate traffic shaping value is not configured, L2TP sends the peak cell rate (PCR) value configured in VC-class configuration mode using the <code>vbr-nrt</code> command. If the tx-speed value is not configured in VC-class configuration mode, L2TP sends the tx-speed value obtained from PPPoE.  &lt;br&gt;• For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the tx-speed value obtained from PPPoE.</td>
</tr>
</tbody>
</table>
| Step 7 end | Exits VPDN group configuration mode and returns to privileged EXEC mode.  
Example: <br>Router(config-vpdn)# end |

**Configuring rx-speed and tx-speed Values from RAM-min on the RADIUS Server**

Perform this task on the RADIUS server to configure the rx-speed and tx-speed values from RAM-min.

**Before You Begin**

- The quality of service (QoS) policy must be attached to PPPoE between the client and the LAC.
- The average rate traffic shaping value must be configured for the default class using `shape average` command in policy-map class configuration mode.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vpdn enable`
4. Do one of the following:
   - `vpdn-group name`
   - `vpdn-template name`
5. `l2tp rx-speed ram-min [value]`
6. `l2tp tx-speed ram-min [value]`
7. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>vpdn enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td>- <code>vpdn-group name</code></td>
<td></td>
</tr>
<tr>
<td>- <code>vpdn-template name</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>l2tp rx-speed ram-min [value]</strong> Sends the rx-speed value to LNS if the average rate traffic shaping value is not configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# l2tp rx-speed ram-min 15000</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>l2tp tx-speed ram-min [value]</strong> Sends the tx-speed value to LNS if the average rate traffic shaping value is not configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# l2tp tx-speed ram-min 15000</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code> Exits VPDN group configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# end</code></td>
</tr>
</tbody>
</table>

### Configuring LNS Address Checking

To allow a LAC to check the IP address of the LNS sending traffic to it during the setup of an L2TP tunnel, thus providing a check for uplink and downlink traffic arriving from different interfaces, follow this procedure.
SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn enable
4. vpdn-group name
5. l2tp security ip address-check
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if</td>
<td></td>
</tr>
<tr>
<td>prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn enable</td>
<td>Enables virtual private dialup networking on the router and informs</td>
</tr>
<tr>
<td>Example:</td>
<td>the router to look for tunnel definitions in a local database or on a</td>
</tr>
<tr>
<td>Router(config)# vpdn enable</td>
<td>remote authorization server (home gateway), if one is present.</td>
</tr>
<tr>
<td><strong>Step 4</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group</td>
<td></td>
</tr>
<tr>
<td>example</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> l2tp security</td>
<td>Configures the LNS to compare the IP addresses contained in the</td>
</tr>
<tr>
<td>ip address-check</td>
<td>inbound and outbound message to ensure they are identical. If the</td>
</tr>
<tr>
<td>Example:</td>
<td>IP addresses to not match, the L2TP tunnel is not established.</td>
</tr>
<tr>
<td>Router(config-vpdn)#</td>
<td></td>
</tr>
<tr>
<td>l2tp security ip</td>
<td></td>
</tr>
<tr>
<td>address-check</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-vpdn)#</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Modified LNS Dead-Cache Handling

Identifying an LNS in a Dead-Cache State

With the Modified LNS Dead-Cache Handling feature, you can use the `show vpdn dead-cache` command to display the status of an LNS in an LSG on a LAC and determine if an LNS is not responding (dead-cache state). The `show vpdn dead-cache` command displays the IP address of the nonresponding LNS, and a time entry showing how long the LNS has been down.

This procedure shows how to use the `show vpdn dead-cache` command to display the status of an LNS to determine if it is in a dead-cache state. An LNS in a dead-cache state cannot establish new sessions or calls.

SUMMARY STEPS

1. `enable`
2. `show vpdn dead-cache {group name | all}`
3. `exit`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays the status of any LNS in a dead-cache state, including how long the entry has been in the dead-cache state.</td>
</tr>
<tr>
<td>`show vpdn dead-cache {group name</td>
<td>all}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show vpdn dead-cache all</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# exit</td>
</tr>
</tbody>
</table>

Clearing an LNS in a Dead-Cache State

With the Modified LNS Dead-Cache Handling feature, you can use the `clear vpdn dead-cache` command to clear an LNS entry in the dead-cache based on the IP address of the LNS, clear all LNS dead-cache states in a VPDN group, or clear all dead-cache LNS entries. If you clear an LNS based on its IP address, and the LNS is associated with more than one VPDN group, the LNS is cleared in all the associated VPDN groups.
This procedure shows how to clear an LNS in a dead-cache state. Once an entry clears from the dead-cache state, the entry is available for new session establishments and calls.

**Before You Begin**

Perform this procedure on the LAC.

**SUMMARY STEPS**

1. enable
2. clear vpdn dead-cache \{\textit{group name} | \textit{ip-address} \textit{ip-address} | all\}
3. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted.  
  **Example:**  
  Router> enable |

**Step 2** clear vpdn dead-cache \{\textit{group name} | \textit{ip-address} \textit{ip-address} | all\}  
  **Example:**  
  Router# clear vpdn dead-cache ip-address  
  10.10.10.1  
  Clears the designated LNS from the dead-cache state. |

**Step 3** exit  
  **Example:**  
  Router# exit  
  Exits privileged EXEC mode. |

**Generating an SNMP Event for a Dead-Cache Entry**

If you are a manager responsible for a large number of devices, and each device has a large number of objects, it is impractical for you to poll or request information from every object on every device. SNMP trap-directed notification alerts you without solicitation, by sending a message known as a trap of the event. After you receive the event, you can display it and can choose to take an appropriate action based on the event.

To generate an SNMP event when an LNS exits or enters the dead-cache state, follow this procedure.
SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server enable traps vpdn dead-cache
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 snmp-server enable traps vpdn dead-cache</td>
<td>Enables the generation of an SNMP event whenever an LNS enters or exits the dead-cache state.</td>
</tr>
<tr>
<td>Example: Router(config)# snmp-server enable traps vpdn dead-cache</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Generating a Syslog Event for a Dead-Cache Entry

To view a syslog event when an LNS is added, deleted, or cleared from a dead-cache state, configure the vpdn logging dead-cache command. You can use syslog events to help troubleshoot networks.

The table below summarizes the syslog messages generated by using the vpdn logging dead-cache command.

Table 7: VPDN Logging Dead-Cache Events

<table>
<thead>
<tr>
<th>Syslog Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry &lt;ip-address&gt; added</td>
<td>Added--An entry in the LSG table enters DOWN status, which marks it a dead-cache entry.</td>
</tr>
</tbody>
</table>
### Syslog Message

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted--An entry in the LSG table is removed from DOWN status, which deletes its dead-cache entry from the table.</td>
</tr>
<tr>
<td>Cleared--An entry in the LSG table is manually cleared.</td>
</tr>
</tbody>
</table>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn logging dead-cache**
4. **exit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong> in privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong> in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>vpdn logging dead-cache</strong> enables the generation of a syslog event when an LNS enters or exits the dead-cache state.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# vpdn logging dead-cache</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>exit</strong> in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>
Configuration Examples for AAA for VPDNs

Examples Configuring the VPDN Tunnel Authorization Search Order

The following configuration example enables VPDN and configures a tunnel authorization search order that will be used instead of the default search order of DNIS number, then domain.

```
vpdn enable
vpdn search-order domain dnis
```

The following example enables VPDN and multihop, and configures a tunnel authorization search order of multihop hostname first, then domain, then DNIS number. This configuration is used only on a tunnel switch.

```
vpdn enable
vpdn multihop
vpdn search-order multihop-hostname domain dnis
```

Examples Configuring per-User VPDN on the NAS

The following example enables VPDN and configures global per-user VPDN on the NAS for all dial-in VPDN tunnels. The first time the NAS contacts the remote RADIUS AAA server, the entire structured username will be sent rather than just the domain name or DNIS number.

```
vpdn enable
vpdn authen-before-forward
```

The following example enables VPDN and configures per-user VPDN on the NAS for dial-in VPDN tunnels belonging to the VPDN group named cisco1. The first time the NAS contacts the remote RADIUS AAA server, the entire structured username will be sent rather than just the domain name or DNIS number.

```
vpdn enable
cisco1
request-dialin
protocol l2tp
exit
authen-before-forward
```

Examples Configuring AAA on the NAS and the Tunnel Server

The following example enables VPDN and local authentication and authorization on the NAS or the tunnel server:

```
vpdn enable
!
```

```
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authorization network default local
```

The following examples enables VPDN and configures the NAS and the tunnel server for dial-in VPDN tunnels when remote RADIUS AAA authentication occurs at the NAS:
NAS Configuration

```
vpdn enable
! aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

Tunnel Server Configuration

```
vpdn enable
! aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa untagged
```

The Basic TACACS+ Configuration Example document provides a basic configuration of TACACS+ for user dialup authentication to a NAS.

Examples Configuring Remote AAA for VPDNs on the L2TP Tunnel Terminator

The following example enables VPDN and configures the NAS and the tunnel server for dial-in VPDN tunnels with remote RADIUS AAA authentication occurring at the tunnel server. A sample RADIUS user profile for the remote RADIUS AAA server is also shown.

NAS Configuration

```
vpdn enable
! aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

Tunnel Server Configuration

```
vpdn enable
! aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

```
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 1
```

RADIUS User Profile

csidtw13  Password = "cisco"
   Service-Type = Outbound,
   Tunnel-Type = :0:L2TP,
   Tunnel-Medium-Type = :0:IP,
   Tunnel-Client-Auth-ID = :0:"csidtw13",
   Tunnel-Password = :0:"cisco"
   Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"

Examples Configuring Directed Request Authorization of VPDN Users

The following example enables VPDN and configures remote RADIUS AAA with VPDN authentication of directed request users on the tunnel server:

vpdn enable
!
   aaa new-model
   aaa authentication login default radius
   aaa authentication ppp default radius
   aaa authorization network default mymетодlist group myvpdngroup
   radius-server host 10.3.3.3 auth-port 1939 acct-port 1443
   aaa group server radius myvpdngroup
   server 10.3.3.3 auth-port 1939 acct-port 1443
!
   ip host example.com 10.3.3.3
   radius-server directed-request
   vpdn authorize directed-request

The following example enables VPDN and configures per-user VPDN, remote TACACS+ AAA, and VPDN authentication of directed request users on the NAS:

vpdn enable
vpdn-group 1
   request-dialin
   protocol l2tp
   domain example.com
   initiate-to 10.3.3.3
   local name local1
   authen-before-forward
!
   aaa new-model
   aaa authentication login default tacacs
   aaa authentication ppp default tacacs
   aaa authorization network default mymетодlist group mygroup
   radius-server host 10.4.4.4 auth-port 1201 acct-port 1450
   aaa group server tacacs mygroup
   server 10.3.3.3 auth-port 1201 acct-port 1450
!
   ip host example.com 10.3.3.3
   radius-server directed-request
   vpdn authorize directed-request

Examples Configuring Domain Name Prefix and Suffix Stripping

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username /user@cisco.com will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

radius-server domain-stripping right-to-left delimiter @\\$
The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username user will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username user@cisco.com will be forwarded to the RADIUS server.

```
tacacs-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com#cisco.com, the username user@cisco.com@cisco.net will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” will be forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username cisco/user@cisco.net will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

### Examples Configuring VPDN Tunnel Authentication

The following example configures VPDN tunnel authentication using the hostname on a NAS and the local name on the tunnel server. Note that the secret password configured for each device matches.

#### NAS Configuration

```
hostname NAS1
username tunnelserver1 password supersecret
```

#### Tunnel Server Configuration

```
vpdn-group 1
local name tunnelserver1
exit
username NAS1 password supersecret
```

The following example configures VPDN tunnel authentication using the local name on the NAS and the L2TP tunnel password on the tunnel server. Note that the secret password configured for each device matches.
NAS Configuration

vpdn-group 2
  local name NAS6
  username tunnelserver12 password verysecret

Tunnel Server Configuration

vpdn-group 4
  l2tp tunnel password verysecret
  local name tunnelserver12
  exit
  username NAS6 password verysecret

The following example configures VPDN tunnel authentication using the L2TP tunnel password on both the NAS and the tunnel server. Note that the secret password configured for each device matches.

NAS Configuration

vpdn-group l2tp
  l2tp tunnel password rathersecret

Tunnel Server Configuration

vpdn-group 46
  l2tp tunnel password rathersecret

Example Configuring RADIUS Tunnel Accounting on a NAS

The following example configures a NAS for remote AAA, configures a dial-in VPDN deployment, and enables the sending of tunnel and tunnel-link accounting records to the RADIUS server:

aaa new-model
  !
  aaa authentication ppp default group radius
  aaa authorization network default local
  aaa accounting network m1 start-stop group radius
  aaa accounting network m2 stop-only group radius
  aaa session-id common
  enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
  enable password secret
  !
  username ISP-LAC password 0 tunnelpass
  !
  resource-pool disable
  !
  ip subnet-zero
  ip cef
  no ip domain-lookup
  ip host myhost 172.16.1.129
  !
  vpdn enable
  vpdn tunnel accounting network m1
  vpdn session accounting network m1
  vpdn search-order domain dnis
  !
  vpdn-group 1
  request-dialin
  protocol l2tp
  domain cisco.com
  initiate-to ip 10.1.26.71
local name ISP-LAC
isdn switch-type primary-5ess
fax interface-type fax-mail
mta receive maximum-recipients 0
controller T1 7/4
framing esf
linecode b8zs
pri-group timeslots 1-24
interface GigabitEthernet0/0/0
ip address 10.1.27.74 255.255.255.0
no ip mroute-cache
duplex half
speed auto
no cdp enable
interface GigabitEthernet0/1/0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
interface Serial7/4:23
ip address 10.0.0.2 255.255.255.0
encapsulation ppp
dialer string 2000
dialer-group 1
isdn switch-type primary-5ess
ppp authentication chap
interface Group-Async0
no ip address
shutdown
group-range 1/00 3/107
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
! dialer-list 1 protocol ip permit
no cdp run
! radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync

Example Configuring RADIUS Tunnel Accounting on a Tunnel Server

The following example configures a tunnel server for remote AAA, configures a dial-in VPDN deployment, and enables the sending of tunnel and tunnel-link accounting records to the RADIUS server:

aaa new-model
! aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
! enable secret 5 $1$ftf.$wE6Q5Vv6hmQiwL9pizPCg1
! username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
  firmware location system:/ucode/mica_port_firmware
resource-pool disable
clock timezone est 2
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host myhost 172.16.1.129
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
terminate-from hostname ISP_NAS
  local name ENT_TS
isdn switch-type primary-5ess
fax interface-type modem
mta receive maximum-recipients 0
interface Loopback0
  ip address 10.0.0.101 255.255.255.0
interface Loopback1
  ip address 10.0.0.201 255.255.255.0
interface Ethernet0
  ip address 10.1.26.71 255.255.255.0
no ip mroute-cache
no cdp enable
interface Virtual-Template1
  ip unnumbered Loopback0
  peer default ip address pool vpdn-pool1
  ppp authentication chap
interface Virtual-Template2
  ip unnumbered Loopback1
  peer default ip address pool vpdn-pool2
  ppp authentication chap
interface FastEthernet0
  no ip address
  no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
ip local pool vpdn-pool1 10.0.0.2 10.0.0.200
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.1.1.12 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
no cdp run
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
Example Configuring Tunnel Assignments on the NAS RADIUS AAA Server

The following examples configure the RADIUS server to group sessions in a tunnel:

Per-User Configuration

```
user@cisco.com Password = "cisco" Service-Type = Outbound,
    tunnel-type = :1:L2TP,
    tunnel-server-endpoint = :1:"10.14.10.54",
    tunnel-assignment-Id = :1:"router"
client@cisco.com Password = "cisco" Service-Type = Outbound,
    tunnel-type = :1:L2TP,
    tunnel-server-endpoint = :1:"10.14.10.54",
    tunnel-assignment-Id = :1:"router"
```

Domain Configuration

```
eng.cisco.com Password = "cisco" Service-Type = Outbound,
    tunnel-type = :1:L2TP,
    tunnel-server-endpoint = :1:"10.14.10.54",
    tunnel-assignment-Id = :1:"router"
sales.cisco.com Password = "cisco" Service-Type = Outbound,
    tunnel-type = :1:L2TP,
    tunnel-server-endpoint = :1:"10.14.10.54",
    tunnel-assignment-Id = :1:"router"
```

Examples Configuring rx-speed and tx-speed Values

The following example shows how to configure average rate traffic shaping value for the default class in policy-map class configuration mode:

```
interface GigabitEthernet3/1/0.30880387
    encapsulation dot1Q 3088 second-dot1q 20
    ancp neighbor name ancp-neighbor id 0016.fa11.0488 client-ID "12.124.234.132/0.0.0.0 eth 3/4/1.32"
    pppoe enable group test2
    service-policy output speed:ether:22000:1200:06/0
        policy-map speed:ether:22000:1200:06/0
            class class-default
            shape average 10281000 !10,281 Mbps is so-called Rate Adaptive Mode (RAM) MIN value!
```

The following example shows how to configure rx-speed and tx-speed values for an ATM interface when the rx-speed and tx-speed values, including 0, 0, are not configured in the RADIUS server. The average rate traffic shaping value is configured for the Ethernet interface. If the average rate traffic shaping value for the default class in policy-map class configuration mode is not configured, the rx-speed and tx-speed values specified in the `l2tp rx-speed` and `l2tp tx-speed` commands are configured for the ATM interface.

```
Interface ATM 1/0/4.2
    vpdn-template 2
    l2tp rx-speed ram-min 8000
    l2tp tx-speed ram-min 8000
```

The following example shows how to configure rx-speed and tx-speed values for an Ethernet interface when the rx-speed and tx-speed values, including 0, 0, are not configured in the RADIUS server. The rx-speed and tx-speed values configured for ANCP is configured for the Ethernet interface. If the rx-speed and tx-speed
values are not configured for ANCP, the rx-speed and tx-speed values specified in the `l2tp rx-speed` and `l2tp tx-speed` commands are configured for the Ethernet interface.

```
Interface Ethernet 3/0/1.3
vpdn-template 1
l2tp rx-speed ancp 15000
l2tp tx-speed ancp 15000
```

### Example Configuring Secure Authentication Names

The following is an example of a RADIUS user profile that includes RADIUS tunneling attributes 90 and 91. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2F,
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2f-assignment-id",
Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
Tunnel-Preference = :1:1,
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Client-Endpoint = :2:"10.0.0.2",
Tunnel-Server-Endpoint = :2:"10.0.0.3",
Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :2:2
```

### Examples Configuring LNS Address Checking

The following shows an example configuration for the client router.

```
hostname Client
!
enable password example
!
no aaa new-model
!
vpdn enable
!
bba-group pppoe 1
    virtual-template 1
    
interface <interface toward LAC>
    pppoe enable group 1
!
interface Virtual-Template 1
    ip unnumbered <interface>
    ppp pap sent-username@example.com
!
end
```

The following shows an example configuration for the LAC.

```
hostname LAC
```
Examples Configuring Modified LNS Dead-Cache Handling

The following show an example configuration from the `show vpdn dead-cache all` command:

```
Router> enable
Router# show vpdn dead-cache all
vpdn-group ip address down time
exampleA 192.168.2.2 00:10:23
exampleB 192.168.4.2 00:10:16
exampleB 192.168.4.3 00:10:15
exampleB 192.168.4.4 00:10:12
```
The following shows an example configuration to clear an LNS, based on its IP address, from the dead-cache state:

```
Router# clear vpdn dead-cache ip-address 192.168.4.4
Router#
```

```
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.4 cleared
LAC# show vpdn dead-cache all
vpdn-group      ip address  down time
exampleA        192.168.2.2  00:10:28
exampleB        192.168.4.2  00:10:21
exampleB        192.168.4.3  00:10:20
```

The following shows an example configuration to clear an LNS group from the dead-cache state:

```
Router# clear vpdn dead-cache group exampleB
Router#
```

```
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.2 cleared
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.3 cleared
Router# show vpdn dead-cache all
vpdn-group      ip address  down time
exampleA        192.168.2.2  00:10:31
```

**Where to Go Next**

Depending on the type of VPDN deployment you are configuring, you should perform the tasks in one of these modules:

- To configure a NAS-initiated tunneling deployment, proceed to the Configuring NAS-Initiated Dial-In VPDN Tunneling module.
- To configure a multihop MMP or multihop tunnel switching VPDN deployment, proceed to the Configuring Multihop VPDN module.

### Additional References

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview module</td>
</tr>
<tr>
<td>VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>Information about configuring AAA</td>
<td>Authentication, Authorization, and Accounting (AAA) module</td>
</tr>
<tr>
<td>Layer 2 Tunnel Protocol</td>
<td>Layer 2 Tunnel Protocol</td>
</tr>
</tbody>
</table>
### Related Topic

| Information about configuring RADIUS and TACACS | Security Server Protocols module |
| Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples | *Cisco IOS Security Command Reference* |
| Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples | *Cisco IOS Dial Technologies Command Reference* |

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL Forum 2004-72</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-VPDN-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>CISCO-VPDN-MGMT-EXT-MIB</td>
<td></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2516</td>
<td><em>A Method for Transmitting PPP Over Ethernet (PPPoE)</em></td>
</tr>
<tr>
<td>RFC 2867</td>
<td><em>RADIUS Accounting Modifications for Tunnel Protocol Support</em></td>
</tr>
<tr>
<td>RFC 2868</td>
<td><em>RADIUS Tunnel Authentication Attributes</em></td>
</tr>
</tbody>
</table>
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.

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

## Feature Information for AAA for VPDNs

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 . An account on Cisco.com is not required.

### Table 8: Feature Information for AAA for VPDNs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Domain Name Prefix and Suffix Stripping for the RADIUS server</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature allows the NAS to be configured to strip prefixes, suffixes, or both from the full username. The reformatted username is then forwarded to the remote AAA server. The following command was introduced or modified by this feature: <code>radius-server domain-stripping</code>.</td>
</tr>
<tr>
<td>RADIUS Attribute 82: Tunnel Assignment ID</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature allows the L2TP NAS to group users from different per-user or domain RADIUS profiles into the same active tunnel if the tunnel endpoints, tunnel type, and Tunnel-Assignment-ID are identical. No commands were introduced or modified by this feature.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RADIUS Tunnel Attribute Extensions</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature introduces RADIUS attribute 90 and RADIUS attribute 91. Both attributes help support the provision of compulsory tunneling in VPDNs by allowing the user to specify authentication names for the NAS and the RADIUS server. No commands were introduced or modified by this feature.</td>
</tr>
<tr>
<td>RFC-2867 RADIUS Tunnel Accounting</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop). The following commands were introduced or modified by this feature: <code>aaa accounting</code>, <code>vpdn session accounting network</code>, <code>vpdn tunnel accounting network</code>.</td>
</tr>
<tr>
<td>Tunnel Authentication via RADIUS on Tunnel Terminator</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature allows the L2TP tunnel server to perform remote authentication and authorization with RADIUS on incoming L2TP NAS dial-in connection requests. This feature also allows the L2TP NAS to perform remote authentication and authorization with RADIUS on incoming L2TP tunnel server dial-out connection requests. The following commands were introduced by this feature: <code>vpdn tunnel authorization network</code>, <code>vpdn tunnel authorization password</code>, <code>vpdn tunnel authorization virtual-template</code>.</td>
</tr>
<tr>
<td>L2TP Forwarding of PPPoE Tagging Information</td>
<td>Cisco IOS XE Release 2.4</td>
<td>This feature was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LNS Address Checking</td>
<td>Cisco IOS XE Release 2.4</td>
<td>This feature allows an LAC, which is receiving data from a LNS, to check the IP address of the LNS prior to establishing an L2TP tunnel. The following command was introduced by this feature: <code>l2tp security ip address-check</code>.</td>
</tr>
<tr>
<td>Modified LNS Dead-Cache Handling</td>
<td>Cisco IOS XE Release 2.4</td>
<td>This feature displays and clears (restarts) any LNS entry in a dead-cache (DOWN) state. The following commands were introduced by this feature: <code>clear vpdn dead-cache</code>, <code>show vpdn dead-cache</code>. The following commands were modified by this feature: <code>snmp-server enable traps</code>, <code>vpdn logging</code>.</td>
</tr>
<tr>
<td>Configurable Domain Name Prefix and Suffix Stripping for the TACACS+ server</td>
<td>Cisco IOS XE Release 2.5</td>
<td>This feature allows the NAS to be configured to strip prefixes, suffixes, or both from the full username. The reformatted username is then forwarded to the remote AAA server. The following command was introduced or modified by this feature: <code>tacacs-server domain-stripping</code>.</td>
</tr>
<tr>
<td>ANCP values configuration support on LNS</td>
<td>Cisco IOS XE Release 3.2S</td>
<td>This feature allows L2TP to send the rx-speed and tx-speed values configured in VPDN group configuration or VPDN template configuration mode, or the rx-speed and the tx-speed values configured on the RADIUS server, to LNS. The following commands were introduced by this feature: <code>l2tp rx-speed</code>, <code>l2tp tx-speed</code>.</td>
</tr>
</tbody>
</table>
Configuring NAS-Initiated Dial-In VPDN Tunneling

Network access server (NAS)-initiated dial-in tunneling provides secure tunneling of a PPP session from a NAS to a tunnel server without any special knowledge or interaction required from the client.

- Finding Feature Information, page 97
- Prerequisites for Configuring NAS-Initiated Dial-In VPDN Tunneling, page 98
- Restrictions for Configuring NAS-Initiated Dial-In VPDN Tunneling, page 98
- Information About NAS-Initiated Dial-In VPDN Tunneling, page 98
- How to Configure NAS-Initiated Dial-In VPDN Tunneling, page 100
- Configuration Examples for NAS-Initiated Dial-In VPDN Tunneling, page 114
- Where to Go Next, page 119
- Additional References, page 119
- Feature Information for NAS-Initiated Dial-In VPDN Tunneling, page 120

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 at the end of this module.

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.
Prerequisites for Configuring NAS-Initiated Dial-In VPDN Tunneling

- Before performing the tasks documented in this module, you must perform the required tasks in the Configuring AAA for VPDNs module.
- The NAS should be configured to receive incoming calls from clients using ISDN, the Public Switched Telephone Network (PSTN), Digital Subscriber Line (DSL), or cable modem.

Restrictions for Configuring NAS-Initiated Dial-In VPDN Tunneling

- Layer 2 Forwarding (L2F) protocol is not supported on the Cisco ASR 1000 Series Aggregation Services Routers.

Information About NAS-Initiated Dial-In VPDN Tunneling

NAS-Initiated Dial-in VPDN Tunneling

NAS-initiated dial-in VPDN tunneling is also known as compulsory tunneling. In NAS-initiated dial-in VPDN tunneling, the client dials into the NAS through a medium that supports PPP. If the connection from the client to the Internet service provider (ISP) NAS is over a medium that is considered secure, such as DSL, ISDN, or the PSTN, the client might choose not to provide additional security. The PPP session is securely tunneled from the NAS to the tunnel server without any special knowledge or interaction required from the client. NAS-initiated dial-in VPDN tunnels can use either the Layer 2 Tunneling Protocol (L2TP) or the Layer 2 Forwarding (L2F) protocol.

Note

The Cisco ASR 1000 Series Aggregation Services Routers support only L2TP.
A NAS-initiated dial-in tunneling scenario is shown in the figure below.

**Figure 8: NAS-Initiated Dial-In VPDN Scenario**

### L2TP Calling Station ID Suppression

In a NAS-initiated dial-in L2TP tunneling scenario, when the NAS connects to a tunnel server it transfers numerous attribute-value (AV) pairs as part of the session setup process. One of these AV pairs is L2TP AV pair 22, the Calling Number ID. The Calling Number ID AV pair includes the calling station ID of the originator of the session, which can be the phone number of the originator, the Logical Line ID (LLID) used to make the connection on the LAC, or the MAC address of the PC connecting to the network. This information can be considered sensitive in cases where the NAS and tunnel server are being managed by different entities. Depending on the security requirements of the NAS or end users, it might be desirable for the NAS to suppress part or all of the calling station ID.

Parts of the calling station ID can be masked, or the calling station ID can be removed completely. Calling station ID suppression can be configured globally on the NAS, for individual VPDN groups on the NAS, or on the remote RADIUS server if one is configured.

### L2TP Failover

If a NAS fails to contact its peer during L2TP tunnel establishment, it can fail over to another configured tunnel server and attempt tunnel establishment with that device.

Failover can occur in these scenarios:

- If the router sends a Start Control Connection Request (SCCRQ) a number of times and receives no response from the peer
- If the router receives a Stop Control Connection Notification (StopCCN) from its peer
- If the router receives a Call Disconnect Notify (CDN) message from its peer

In both the StopCCN control message and the CDN control message, a Result Code AV pair is included, which indicates the reason for tunnel or session termination, respectively. This AV pair might also include an optional Error Code, which further describes the nature of the termination. The various Result Code and
Error Code values have been standardized in RFC 2661. Failover will occur if the combination of Result Code and Error Code values as defined in the table below is received from the peer.

Table 9: Defined Result and Error Codes from RFC 2661

<table>
<thead>
<tr>
<th>Control Message</th>
<th>Result Code</th>
<th>Error Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>StopCCN, CDN</td>
<td>2: General error, see Error Code.</td>
<td>4: Insufficient resources to handle this operation now.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6: A generic vendor-specific error occurred.⁴</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7: Try another.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9: Try another directed.</td>
</tr>
<tr>
<td>CDN</td>
<td>4: Temporary lack of resources.</td>
<td>--</td>
</tr>
</tbody>
</table>

¹ For failover, this error code would be accompanied by a vendor-specific error AVP in the error message—in this case containing the Cisco vendor code (SMI_CISCO_ENTERPRISE_CODE) and a Cisco error code (L2TP_VENDOR_ERROR_SLIMIT).

When one of the three scenarios occurs, the router marks the peer IP address as busy for 60 seconds by default. During that time no attempt is made to establish a session or tunnel with the peer. The router selects an alternate peer to contact if one is configured. If a tunnel already exists to the alternate peer, new sessions are brought up in the existing tunnel. Otherwise, the router begins negotiations to establish a tunnel to the alternate peer.

How to Configure NAS-Initiated Dial-In VPDN Tunneling

Configuring the NAS to Request Dial-In VPDN Tunnels

The NAS must be configured to request tunnel establishment with the remote tunnel server. Perform this task on the NAS to configure a VPDN request dial-in subgroup and the IP address of the tunnel server that will be the other endpoint of the VPDN tunnel.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vpdn-group name`
4. `description string`
5. `request-dialin`
6. `protocol l2tp`
7. Do one of the following:
   - `domain domain-name`
   - `dnis {dnis-number | dnis-group-name}`
8. `exit`
9. `initiate-to ip ip-address [limit limit-number] [priority priority-number]`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# vpdn-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> description string</td>
<td>(Optional) Adds a description to a VPDN group.</td>
</tr>
<tr>
<td>Example: Router(config-vpdn)# description myvpdngroup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> request-dialin</td>
<td>Configures a NAS to request the establishment of an L2F or L2TP tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-vpdn)# request-dialin</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring NAS-Initiated Dial-In VPDN Tunneling

### Command or Action | Purpose
--- | ---
**Step 6** | protocol l2tp
**Example:**
Router(config-vpdn-req-in)# protocol l2tp
| Specifies the Layer 2 protocol that the VPDN group will use.

**Step 7** | Do one of the following:
- domain domain-name
- dnis {dnis-number | dnis-group-name}
**Example:**
Router(config-vpdn-req-in)# domain example.com
**Example:**
Router(config-vpdn-req-in)# dnis 5687
| Requests that PPP calls from a specific domain name be tunneled. or Requests that PPP calls from a specific Dialed Number Identification Service (DNIS) number or DNIS group be tunneled.

**Step 8** | exit
**Example:**
Router(config-vpdn-req-in)# exit
| Exits to VPDN group configuration mode.

**Step 9** | initiate-to ip ip-address [limit limit-number] [priority priority-number]
**Example:**
Router(config-vpdn)# initiate-to ip 10.1.1.1 limit 12
| Specifies an IP address that will be used for Layer 2 tunneling.
- limit --Maximum number of connections that can be made to this IP address.
- priority --Priority for this IP address.

**Note** The priority keyword is typically not configured on a NAS. Information used for load balancing and failover is configured on a remote authentication, authorization, and accounting (AAA) server instead. See the Configuring AAA for VPDNs module.
- Multiple tunnel servers can be configured on the NAS by configuring multiple initiate-to commands.

### What to Do Next
You must perform the task in the Configuring the Tunnel Server to Accept Dial-In VPDN Tunnels section.
Configuring the Tunnel Server to Accept Dial-In VPDN Tunnels

The tunnel server must be configured to accept tunnel requests from the remote NAS. Perform this task on the tunnel server to create a VPDN accept dial-in subgroup and to configure the tunnel server to accept tunnels from the NAS that will be the other endpoint of the VPDN tunnel. To configure the tunnel server to accept tunnels from multiple NASs, you must perform this task for each NAS.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. description string
5. accept-dialin
6. protocol l2tp
7. virtual-template number
8. exit
9. terminate-from hostname host-name
10. lcp renegotiation {always | on-mismatch}
11. force-local-chap

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# vpdn-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> description string</td>
<td>(Optional) Adds a description to a VPDN group.</td>
</tr>
<tr>
<td>Example: Router(config-vpdn)# description myvpdngroup</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>5</td>
<td>accept-dialin</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>protocol l2tp</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>virtual-template number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>terminate-from hostname host-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>lcp renegotiation {always</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>force-local-chap</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|       |                  | Note: This command will function only if Challenge Handshake Authentication Protocol (CHAP) authentication is enabled for PPP using the `ppp authentication chap` command in the virtual template configured on the tunnel server.
What to Do Next

You must perform the task in the Configuring the Virtual Template on the Tunnel Server section.

Configuring the Virtual Template on the Tunnel Server

When a request to establish a tunnel is received by the tunnel server, the tunnel server must create a virtual access interface. The virtual access interface is cloned from a virtual template interface, used, and then freed when no longer needed. The virtual template interface is a logical entity that is not tied to any physical interface.

Perform this task on the tunnel server to configure a basic virtual template.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface virtual-template number
4. ip unnumbered type number
5. ppp authentication protocol1 [protocol2...] [if-needed] [list-name] [default] [callin] [one-time] [optional]
6. peer default ip address [ip-address] dhcp-pool | dhcp | pool [pool-name]}
7. encapsulation encapsulation-type

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface virtual-template number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface virtual-template 1</td>
</tr>
<tr>
<td></td>
<td>Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 4** ip unnumbered type number | Enables IP processing on a serial interface without assigning an explicit IP address to the interface.  
**Note** Configuring the ip address command within a virtual template is not recommended. Configuring a specific IP address in a virtual template can result in the establishment of erroneous routes and the loss of IP packets. |
| Example:  
Router(config-if)# ip unnumbered FastEthernet 0/0 |  |
| **Step 5** ppp authentication protocol1 [protocol2...] [if-needed] [list-name | Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.  
[default] [callin] [one-time] [optional] |  |
| Example:  
Router(config-if)# ppp authentication chap |  |
| **Step 6** peer default ip address {ip-address | Specifies an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface.  
dhcp | pool [pool-name]} |  |
| Example:  
Router(config-if)# peer default ip address pool mypool |  |
| **Step 7** encapsulation encapsulation-type | Sets the encapsulation method used by the interface. |
| Example:  
Router(config-if)# encapsulation ppp |  |

---

**Verifying a NAS-Initiated VPDN Configuration**

**Verifying and Troubleshooting Tunnel Establishment Between the NAS and the Tunnel Server**

Perform this task to verify that a tunnel between the NAS and the tunnel server has been established, and to troubleshoot problems with tunnel establishment.

**SUMMARY STEPS**

1. enable  
2. show vpdn tunnel all  
3. ping ip-address  
4. debug vpdn event  
5. debug vpdn errors
DETAILED STEPS

Step 1 enable
Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example:

Router> enable

Step 2 show vpdn tunnel all
Enter this command to display details about all active VPDN tunnels. This example shows an example of No active L2TP tunnels:

Example:

Router# show vpdn tunnel all
% No active L2TP tunnels

If no active tunnels have been established with the NAS, proceed with the following steps to troubleshoot the problem.

Step 3 ping ip-address
Enter this command to ping the NAS. The following output shows the result of a successful ping from the tunnel server to the NAS:

Example:

Router# ping 172.22.66.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.2.1, timeout is 2 seconds: 
!
!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/132/152 ms

If the tunnel server is unable to ping the NAS, there might be a problem with the routing path between the devices, or the NAS might not be functional.

Step 4 debug vpdn event
Enter this command to display the VPDN events that occur during tunnel establishment. The following output from the tunnel server shows normal VPDN tunnel establishment for an L2TP tunnel:

Example:

Router# debug vpdn event
20:19:17: L2TP: I SCCRQ from tsi tnl 8
20:19:17: L2X: Never heard of tsi
20:19:17: Tnl 7 L2TP: New tunnel created for remote tsi, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, tsi
20:19:17: Tnl 7 L2TP: Tunnel state change from idle to wait-ctl-reply
20:19:17: Tnl 7 L2TP: Got a Challenge Response in SCCCN from tsi
20:19:17: Tnl 7 L2TP: Tunnel Authentication success
20:19:17: Tnl 7 L2TP: Tunnel state change from wait-ctl-reply to established
20:19:17: Tnl 7 L2TP: SM State established
20:19:17: Tnl/C1 7/1 L2TP: Session FS enabled
20:19:17: Tnl/C1 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/C1 7/1 L2TP: New session created
20:19:17: Tnl/C1 7/1 L2TP: O ICRP to tsi 8/1
Step 5  **debug vpdn errors**

Enter this command to display error messages that are generated during tunnel establishment. The following output from the NAS shows an authentication failure during tunnel establishment.

**Example:**

```console
Router# debug vpdn errors
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to down
%LINK-5-CHANGED: Interface Async1, changed state to reset
%LINK-3-UPDOWN: Interface Async1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
VPDN tunnel management packet failed to authenticate
VPDN tunnel management packet failed to authenticate
```

If an authentication failure occurs, verify that both the NAS and the tunnel server are configured with the same secret password. You can also perform tasks to verify L2TP tunnel establishment, PPP negotiations, and authentication with the remote client as described in the Configuring AAA for VPDNs module.

---

**Verifying the Connection Between the Client and the NAS**

Perform this task to verify the connection between the dial-in client and the NAS.

**SUMMARY STEPS**

1. Dial in to the NAS from a client PC.
2. `enable`
3. `show caller user user`
4. `show interfaces virtual-access number`
5. `show vpdn session`

**DETAILED STEPS**

**Step 1**

Dial in to the NAS from a client PC.

Ensure that the client PC is able to connect to the NAS by establishing a dial-in connection. As the call comes into the NAS, a `%LINK-3-UPDOWN` message automatically appears on the NAS terminal screen. In the following example, the call comes into the NAS on asynchronous interface 14:
Example:

*Jan 1 21:22:18.410: %LINK-3-UPDOWN: Interface Async14, changed state to up

Note No debug commands are turned on to display this log message. This message should be displayed within 30 seconds after the client first sends the call.

If this message is not displayed by the NAS, there is a problem with the dial-in configuration.

Step 2 enable

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

Example:

Router> enable

Step 3 show caller user user

Enter this command on the tunnel server to verify that the client received an IP address. The following example shows that user3 is using IP address 10.0.0.1.

Example:

Router# show caller user user3@cisco.com
User: user3@cisco.com, line Vi2.502, service PPPoVPDN
Connected for 1d10h
Timeouts: Limit Remaining Timer Type
- - -
PPP: LCP Open, CHAP (<-), IPCP
IP: Local 10.0.0.1, remote 172.16.2.247
Counts: 2052 packets input, 32826 bytes
2053 packets output, 106742 bytes

If an incorrect IP address or no IP address is displayed, there is a problem with IP addresses assignment. Verify the configuration of the peer default ip address command in the virtual template on the tunnel server.

Step 4 show interfaces virtual-access number

Enter this command to verify that the interface is up, that LCP is open, and that no errors are reported. The following output shows a functional interface:

Example:

Router# show interfaces virtual-access 2.502
Virtual-Access2.502 is up, line protocol is up
Hardware is Virtual Access interface
Interface is unnumbered. Using address of Loopback1001 (60.0.0.1)
MTU 1454 bytes, BW 2000000 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 5/255
Encapsulation PPP, LCP Open
Open: IPCP
PPPoVPDN vaccess, cloned from Virtual-Template 1
Vaccess status 0x0
Protocol l2tp, tunnel id 30485, session id 55909
Keepalive set (60 sec)
2056 packets input, 32890 bytes
2057 packets output, 106950 bytes
Last clearing of "show interface" counters never

The virtual access interface is up and the line protocol is up, showing that virtual interface establishment was successful.

Step 5 show vpdn session
Enter this command on the tunnel server to verify that there are active VPDN sessions. This example shows output from a tunnel server with several active tunnels.

**Example:**

```
Router# show vpdn session
L2TP Session Information Total tunnels 4000 sessions 15960
LocID RemID TunID Username, Intf/ State Last Chg Uniq ID
Vcid, Circuit
43202 40336 22 user@ci..., V12.9171 est 1d10h 9184
34090 31996 22 user@ci..., V12.1734 est 1d10h 1735
1217 42591 22 user@ci..., V12.9312 est 1d10h 9325
6737 23225 22 user@ci..., V12.1729 est 1d10h 1730
59420 17035 34 user@ci..., V12.9338 est 1d10h 9351
45069 60982 34 user@ci..., V12.1645 est 1d10h 1646
27825 44751 34 user@ci..., V12.1653 est 1d10h 1654
24600 7627 34 user@ci..., V12.9096 est 1d10h 9109
13018 65037 43 user@ci..., V12.8166 est 1d10h 8179
43090 34448 43 user@ci..., V12.8176 est 1d10h 8189
31798 41505 43 user@ci..., V12.15752 est 1d10h 15765
56832 64322 43 user@ci..., V12.15655 est 1d10h 15668
53944 25409 48 user@ci..., V12.14115 est 1d10h 14128
16215 52915 48 user@ci..., V12.14134 est 1d10h 14147
17332 14000 48 user@ci..., V12.6630 est 1d10h 6643
12466 54817 48 user@ci..., V12.6622 est 1d10h 6635
28290 37822 50 user@ci..., V12.5094 est 1d10h 15905
48839 30137 50 user@ci..., V12.15875 est 1d10h 15888
```

If there is no session established for the client, perform the troubleshooting steps in the Verifying and Troubleshooting Tunnel Establishment Between the NAS and the Tunnel Server, on page 106.

### Configuring L2TP Calling Station ID Suppression

Calling station ID suppression can be configured globally on the NAS, for individual VPDN groups on the NAS, or on the remote RADIUS server if one is configured.

The order of precedence for L2TP calling station ID suppression configurations is as follows:

- A RADIUS server configuration will take precedence over any configuration on the NAS.
- A VPDN group configuration will take precedence over a global configuration for calls associated with that VPDN group.
- A global configuration will be applied if no other method is configured.

Perform one or more of the following tasks to configure L2TP calling station ID suppression:

#### Prerequisites for Configuring L2TP Calling Station ID Suppression

- You must configure the NAS and the tunnel server to use the L2TP protocol when performing the tasks in the Configuring the NAS to Request Dial-In VPDN Tunnels section and the Configuring the Tunnel Server to Accept Dial-In VPDN Tunnels section.

- You must configure the NAS to tunnel calls based on the domain name when performing the task in the Configuring the NAS to Request Dial-In VPDN Tunnels section.
• You must configure the VPDN search order to use the domain name when performing the task in the Configuring the VPDN Tunnel Authorization Search Order section of the Configuring AAA for VPDNs module.

### Configuring Global L2TP Calling Station ID Suppression on the NAS

The calling station ID information included in L2TP AV pair 22 can be removed or masked for every L2TP session established on the router if you configure L2TP calling station ID suppression globally. This configuration is compatible with either local or remote authorization.

Perform this task on the NAS to configure global L2TP calling station ID suppression.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `vpdn l2tp attribute clid mask-method {right mask-character characters | remove} [match match-string]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `vpdn l2tp attribute clid mask-method {right mask-character characters</td>
<td>remove} [match match-string]`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn l2tp attribute clid mask-method right # 6 match %321</td>
<td>• right <code>mask-character characters</code> -- Masks the calling station ID starting from the right end, using the specified <code>mask-character</code> to replace the defined number of <code>characters</code>. The <code>mask-character</code> must be a printable character.</td>
</tr>
<tr>
<td></td>
<td>• remove -- Removes the entire calling station ID.</td>
</tr>
<tr>
<td></td>
<td>• match <code>match-string</code> -- Removes or masks the calling station ID only when the username contains the specified <code>match-string</code>.</td>
</tr>
</tbody>
</table>
Configuring L2TP Calling Station ID Suppression for a VPDN Group on the NAS

The calling station ID information included in L2TP AV pair 22 can be removed or masked for calls associated with a specific VPDN group. This configuration is compatible with local authorization configurations.

Perform this task on the NAS to configure L2TP calling station ID suppression for calls associated with a particular VPDN group when using local authorization.

**Before You Begin**

- You must configure the NAS and the tunnel server for local authorization when performing the task in the Configuring AAA on the NAS and the Tunnel Server section of the Configuring AAA for VPDNs module.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vpdn-group name
4. l2tp attribute clid mask-method {right mask-character characters|remove} [match match-string]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# vpdn-group L2TP</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> l2tp attribute clid mask-method {right mask-character characters</td>
<td>remove} [match match-string]</td>
</tr>
<tr>
<td>Example: Router (config-vpdn)# l2tp attribute clid mask-method remove</td>
<td>- right mask-character characters -- Masks the calling station ID starting from the right end, using the specified mask-character to replace the defined number of characters. The mask-character must be a printable character.</td>
</tr>
<tr>
<td></td>
<td>- remove -- Removes the entire calling station ID.</td>
</tr>
</tbody>
</table>
### Configuring L2TP Calling Station ID Suppression on the NAS Remote RADIUS Server

L2TP calling station ID suppression can be configured directly on the NAS, or in the RADIUS user profile. Configuring L2TP calling station ID suppression in the RADIUS user profile allows the configuration to be propagated to multiple NASs without having to configure each one.

Perform this task on the RADIUS server to configure a user profile that will allow the RADIUS server to instruct NASs to remove or mask the L2TP calling station ID.

#### Before You Begin

- The NAS must be configured for remote RADIUS AAA. Perform the tasks for configuring AAA on the NAS and the tunnel server, and configuring remote AAA for VPDNs as described in the Configuring AAA for VPDNs module.
- The RADIUS server must be configured for AAA.

#### SUMMARY STEPS

1. Cisco-Avpair = vpdn:l2tp-tunnel-password= secret
2. Cisco-Avpair = vpdn:tunnel-type= l2tp
3. Cisco-Avpair = vpdn:tunnel-id= name
4. Cisco-Avpair = vpdn:ip-address= address

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:l2tp-tunnel-password= secret</td>
<td>Specifies the L2TP tunnel password in the RADIUS user profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:tunnel-type= l2tp</td>
<td>Specifies L2TP as the tunneling protocol in the RADIUS user profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:tunnel-type=l2tp</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** Cisco-Avpair = vpdn:tunnel-id= name | Specifies the tunnel ID in the RADIUS user profile.
**Example:**
Cisco-Avpair = vpdn:tunnel-id=test

**Step 4** Cisco-Avpair = vpdn:ip-address= address | Specifies the NAS IP address in the RADIUS user profile.
**Example:**
Cisco-Avpair = vpdn:ip-address=172.16.9.9

**Step 5** Cisco-Avpair = vpdn:l2tp-clid-mask-method= {right: character : characters | remove} | Specifies L2TP calling station ID suppression parameters in the RADIUS user profile.
**Example:**
Cisco-Avpair = vpdn:l2tp-clid-mask-method= right:#:5

- **right** -- Masks the calling station ID starting from the right side, using the specified mask-character to replace the defined number of characters.
- **remove** -- Removes the entire calling station ID.

---

## Configuration Examples for NAS-Initiated Dial-In VPDN Tunneling

### Example Configuring the NAS for Dial-In VPDNs

The following example configures a NAS named ISP-NAS to tunnel PPP calls to a tunnel server named ENT-TS using L2TP and local authentication and authorization:

```bash
! Enable AAA authentication and authorization with RADIUS as the default method
aaa new-model
aaa authentication ppp default radius
aaa authorization network default radius
!
! Configure the VPDN tunnel authentication password using the local name
username ISP-NAS password 7 tunnelme
username ENT-TS password 7 tunnelme
!
vpdn enable
!
! Configure VPN to first search on the client domain name and then on the DNIS
vpdn search-order domain dnis
!
! Allow a maximum of 10 simultaneous VPDN sessions
vpdn session-limit 10
!
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel server
vpdn-group 1
request-dialin
```
protocol l2tp
domain cisco.com
!
initiate-to ip 172.22.66.25
local name ISP-NAS
!
! Specifies the RADIUS server IP address, authorization port, and accounting port
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
!
! Specifies the authentication key to be used with the RADIUS server
radius-server key cisco
!

Example Configuring the Tunnel Server for Dial-in VPDNs

The following example show a tunnel server named ENT-TS configured to accept L2TP tunnels from a NAS named ISP-NAS using local authentication and authorization:

! Configure AAA to first use the local database and then contact the RADIUS server for
! PPP authentication
aaa new-model
aaa authentication ppp default local radius
!
! Configure AAA network authorization and accounting by using the RADIUS server
aaa authorization network default radius
aaa accounting network default start-stop radius
!
! Configure the VPDN tunnel authentication password using the local name
username ISP-NAS password 7 tunnelme
username ENT-TS password 7 tunnelme
!
vpdn enable
!
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
!
! Configure the virtual template
interface Virtual-Template1
gigabitethernet0/0/0
ppp authentication chap
peer default ip address pool default
encapsulation ppp
!
! Specifies the RADIUS server IP address, authorization port, and accounting port
radius-server host 172.22.66.13 auth-port 1645 acct-port 1646
!
! Specifies the authentication key to be used with the RADIUS server
radius-server key cisco
!

Example L2TP Calling Station ID Suppression with Local Authorization

The following example configures a NAS for PPP over Gigabit Ethernet over virtual LAN (PPPoEoVLAN). The NAS obtains a calling station ID from LLID NAS port preauthorization through RADIUS. The calling station ID will be removed from AV pair 22 for tunnels associated with the VPDN group named L2TP if the string #184 is included in the username.

hostname LAC
enable secret 5 $1$8qtb$MHcYeW2kn8VNYg932eX1.
enable password lab
!
aaa new-model
!
aaa group server radius LLID-Radius
   server 192.168.1.5 auth-port 1645 acct-port 1646
!
aaa group server radius LAC-Radius
   server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default local
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius
aaa nas port extended
aaa session-id common
!
ip subnet-zero
ip cef
no ip domain lookup
!
vpdn enable
vpdn search-order domain
!
vpdn-group L2TP
   request-dialin
   protocol l2tp
   domain cisco.com
!
   initiate-to ip 192.168.1.4
   local name test
   l2tp tunnel password 0 cisco
   l2tp attribute clid mask-method remove match #184
!
bba-group pppoe 2
   virtual-template 1
   nas-port format d 2/2/4
!
subscriber access pppoe pre-authorize nas-port-id LLID send username
!
interface Loopback0
   no ip address
!
interface Loopback1
   ip address 10.1.1.1 255.255.255.0
!
interface gigabitethernet0/0/0
   ip address 192.168.1.3 255.255.255.0
   no cdp enable
!
interface gigabitethernet0/0/0.20
   encapsulation dot1Q 1024
   no snmp trap link-status
   pppoe enable group 2
   pppoe max-sessions 200
   no cdp enable
!
interface gigabitethernet1/0/0
   ip address 10.1.1.10 255.255.255.0
   no cdp enable
!
interface Serial2/0/0
   no ip address
   shutdown
   serial restart-delay 0
!
interface Serial3/0/0
   no ip address
   shutdown
   serial restart-delay 0
Example L2TP Calling Station ID Suppression with RADIUS Authorization

The following example configures a NAS for PPPoEoVLAN. The NAS obtains a calling station ID from LLID NAS port preauthorization through RADIUS. The RADIUS user profile specifies that the calling station ID should be masked by replacing the rightmost six characters with the character X.

**NAS Configuration**

```
hostname LAC
!
enable secret 5 $1$8qtb$MHcYeW2kn8VNYgs932eX1.
enable password lab
!
aaa new-model
!
aaa group server radius LLID-Radius
  server 192.168.1.5 auth-port 1645 acct-port 1646
!
aaa group server radius LAC-Radius
  server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default group LAC-Radius
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius

ip subnet-zero
ip cef
no ip domain lookup
!
vpdn enable
vpdn search-order domain
!
no peer default ip address
!
ppp encryption pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 gigabitethernet0/0/0
ip route 10.0.0.0 255.0.0.0 gigabitethernet1/0/0
!
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
password lab
```
subscriber access pppoe pre-authorize nas-port-id LLID send username
interface Loopback0
  no ip address
interface Loopback1
  ip address 10.1.1.1 255.255.255.0
interface gigabitethernet0/0/0
  ip address 192.168.1.3 255.255.255.0
  no cdp enable
interface gigabitethernet0/0/0.20
  encapsulation dot1Q 1024
  no snmp trap link-status
  pppoe enable group 2
  pppoe max-sessions 200
  no cdp enable
interface gigabitethernet1/0/0
  ip address 10.1.1.10 255.255.255.0
  no cdp enable
interface Serial2/0/0
  no ip address
  shutdown
  serial restart-delay 0
interface Serial3/0/0
  no ip address
  shutdown
  serial restart-delay 0
interface Virtual-Template1
  ip unnumbered gigabitethernet1/0/0
  ip mroute-cache
  no peer default ip address
  ppp authentication pap
  ip classless
  ip route 0.0.0.0 0.0.0.0 gigabitethernet0/0/0
  ip route 10.0.0.0 255.0.0.0 gigabitethernet1/0/0
  no ip http server
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
control-plane
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password lab

RADIUS User Profile Configuration

Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco
Cisco-Avpair = vpdn:tunnel-type=l2tp
Cisco-Avpair = vpdn:tunnel-id=test
Cisco-Avpair = vpdn:ip-address=192.168.1.4
Cisco-Avpair = vpdn:l2tp-clid-mask-method=right:X:6
Where to Go Next

You can perform any of the relevant optional tasks in the Configuring Additional VPDN Features and in the VPDN Tunnel Management modules.

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview</td>
</tr>
<tr>
<td>Technical support documentation for L2TP</td>
<td>Layer 2 Tunnel Protocol (L2TP)</td>
</tr>
<tr>
<td>Technical support documentation for VPDNs</td>
<td>Virtual Private Dial-Up Network (VPDN)</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-VPDN-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-VPDN-MGMT-EXT-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for NAS-Initiated Dial-In VPDN Tunneling

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 . An account on Cisco.com is not required.

Table 10: Feature Information for NAS-Initiated Dial-In VPDN Tunneling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP Calling Station ID Suppression</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature allows the NAS to suppress part or all of the calling station ID from the NAS in the L2TP AV pair 22, the Calling Number ID. Calling station ID suppression can be configured globally on the router, for individual VPDN groups on the router, or on the remote RADIUS server if one is configured. The following commands were introduced by this feature: <code>l2tp attribute clid mask-method, vpdn l2tp attribute clid mask-method</code>.</td>
</tr>
</tbody>
</table>
### Feature Information for NAS-Initiated Dial-In VPDN Tunneling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP Extended Failover</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature extends L2TP failover to occur if, during tunnel establishment, a router receives a StopCCN message from its peer, or during session establishment a router receives a CDN message from its peer. In either case, the router selects an alternate peer to contact. No commands were introduced or modified by this feature.</td>
</tr>
</tbody>
</table>
Configuring Multihop VPDN

Multihop virtual private dialup networking (VPDN) is a specialized VPDN configuration that allows packets to pass through multiple tunnels. Ordinarily, packets are not allowed to pass through more than one tunnel. In a multihop deployment, the VPDN tunnel is terminated after each hop and a new tunnel is initiated to the next hop destination.

Multihop VPDN deployments can also be used to configure a device as a tunnel switch. A tunnel switch acts as both a network access server (NAS) and a tunnel server, able to receive packets from an incoming VPDN tunnel and send them out over an outgoing VPDN tunnel. Tunnel switch configurations can be used between Internet service providers (ISPs) to provide wholesale VPDN services.

- Finding Feature Information, page 123
- Prerequisites for Multihop VPDN, page 124
- Restrictions for Multihop VPDN, page 124
- Information About Multihop VPDN, page 124
- How to Configure Multihop VPDN, page 125
- Configuration Examples for Multihop VPDN, page 130
- Where to Go Next, page 131
- Additional References, page 132
- Feature Information for Multihop VPDN, page 133

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 at the end of this module.

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.
Prerequisites for Multihop VPDN

Before you configure multihop VPDN, a VPDN deployment must be configured. For more information about VPDN deployments that are compatible with multihop VPDN scenarios, see the Configuring a Multihop Tunnel Switch, on page 125.

Restrictions for Multihop VPDN

Only the Layer 2 Tunneling Protocol (L2TP) is supported on the Cisco ASR 1000 Series Aggregation Services Routers.

Information About Multihop VPDN

Tunnel Switching Using Multihop VPDN

Multihop VPDN can be used to configure a device as a tunnel switch. A tunnel switch acts as both a NAS and a tunnel server, receiving packets from an incoming VPDN tunnel and sending them out over an outgoing VPDN tunnel. Tunnel switch configurations can be used between ISPs to provide wholesale VPDN services. A VPDN tunnel switch on the Cisco ASR 1000 Series Aggregation Services Routers can forward L2TP sessions. L2F or Point-to-Point Tunneling Protocol (PPTP) are not supported.

In an L2TP tunnel switching deployment, the tunnel endpoints are considered the originating NAS and the terminating tunnel server. The tunnel switch is not considered a tunnel endpoint.

The figure below shows a network scenario using a basic L2TP tunnel switching deployment.

Figure 9: Tunnel Switching Using Multihop VPDN

The tunnel switch can be configured to terminate incoming VPDN tunnels from multiple devices, and to initiate outgoing VPDN tunnels to one or more tunnel servers.
The Subscriber Service Switch (SSS) framework is supported for VPDN tunnel switching. SSS supports additional Layer 2 protocols, including PPP over Ethernet (PPPoE) and generic routing encapsulation (GRE). Configuring SSS for VPDN tunnel switching is optional. SSS profiles increase the scalability of tunnel switching configurations, particularly in multiprotocol environments.

How to Configure Multihop VPDN

Configuring a Multihop Tunnel Switch

Multihop VPDN can be used to configure a device as a tunnel switch. A tunnel switch acts as both a NAS and a tunnel server, and must be configured with both a NAS VPDN group and a tunnel server VPDN group. Tunnel switching using the SSS infrastructure is supported. SSS allows L2TP, L2F, PPTP, PPPoE, PPPoA, GRE, and general packet radio service (GPRS) sessions to be switched over virtual links using a tunnel switch. SSS configurations are not required for tunnel switching data over L2TP, L2F, or PPTP tunnels, but SSS increases the scalability of tunnel switching deployments.

Note
On the Cisco ASR 1000 Series Aggregation Services Router, a multihop VPDN tunnel switch can be configured to forward L2TP tunnels only.

Perform these tasks to configure a device as a multihop VPDN tunnel switch:

**Prerequisites for Configuring a Multihop Tunnel Switch**

- The tunnel endpoints must be configured for VPDN tunneling as described in the Configuring NAS-Initiated Dial-In VPDN Tunneling module.
- If you want to perform VPDN tunnel authorization searches based on the multihop hostname, you must configure the search to use the multihop hostname as described in the Configuring AAA for VPDNs module.

**Enabling Multihop VPDN on the Tunnel Switch**

In tunnel switching deployments, packets must traverse multiple tunnels. Multihop VPDN must be enabled on the tunnel switch for the deployment to function.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vpdn multihop`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | **enable** | Enables privileged EXEC mode.  
| Example:          |          |  
| Router> enable    |          | • Enter your password if prompted.  
| **Step 2**        | **configure terminal** | Enters global configuration mode.  
| Example:          |          |  
| Router# configure terminal | |  
| **Step 3**        | **vpdn multihop** | Enables VPDN multihop.  
| Example:          |          |  
| Router(config)# vpdn multihop | |  

**What to Do Next**  
You must perform the task in the Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels, on page 126.

**Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels**  
A tunnel switch must be configured as a tunnel server, allowing it to terminate incoming VPDN tunnels. You can configure a tunnel switch to terminate tunnels from multiple devices.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. vpdn-group name  
4. description string  
5. accept-dialin  
6. protocol l2tp  
7. virtual-template number  
8. exit  
9. terminate-from hostname host-name
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# vpdn-group 1</td>
</tr>
<tr>
<td>Step 4 description string</td>
<td>(Optional) Adds a description to a VPDN group.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# description myvpdngroup</td>
</tr>
<tr>
<td>Step 5 accept-dialin</td>
<td>Configures a tunnel switch to accept requests from a NAS to establish a tunnel, creates an accept-dialin VPDN subgroup, and enters VPDN accept dial-in subgroup configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# accept-dialin</td>
</tr>
<tr>
<td>Step 6 protocol l2tp</td>
<td>Specifies the Layer 2 Tunneling Protocol that the VPDN group will use.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn-acc-in)# protocol l2tp</td>
</tr>
<tr>
<td>Step 7 virtual-template number</td>
<td>(Optional) Specifies which virtual template will be used to clone virtual access interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn-acc-in)# virtual-template 1</td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Exits to VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn-acc-in)# exit</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 9**

| terminate-from hostname host-name |

*Example:*

Router(config-vpdn)# terminate-from hostname NAS12

-Specifies the hostname of the remote NAS that will be required when accepting a VPDN tunnel.

---

### What to Do Next

You must perform the task in the Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels section.

### Configuring the Multihop Tunnel Switch to Initiate Outgoing VPDN Tunnels

A tunnel switch must be configured as a NAS, allowing it to initiate outgoing VPDN tunnels. You can configure a tunnel switch to initiate tunnels to multiple devices.

### SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. description string
5. request-dialin
6. protocol l2tp
7. Do one of the following:
   - domain domain-name
   - dnis {dnis-number | dnis-group-name}
   - multihop-hostname ingress-tunnel-name
8. exit
9. initiate-to ip ip-address [limit limit-number] [priority priority-number]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>vpdn-group name</code></td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# vpdn-group 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>description string</code></td>
<td>(Optional) Adds a description to a VPDN group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-vpdn)# description myvpdngroup</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>request-dialin</code></td>
<td>Configures a tunnel switch to request the establishment of a tunnel to a tunnel server, creates a request-dialin VPDN subgroup, and enters VPDN request dial-in subgroup configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-vpdn)# request-dialin</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>protocol l2tp</code></td>
<td>Specifies the Layer 2 Tunneling Protocol that the VPDN group will use.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-vpdn-req-in)# protocol l2tp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>Do one of the following:</td>
<td>Requests that PPP calls from a specific domain name be tunneled. or Requests that PPP calls from a specific DNIS number or DNIS group be tunneled. or Enables the tunnel switch to initiate a tunnel based on the NAS host name or the ingress tunnel ID.</td>
</tr>
<tr>
<td>• <code>domain domain-name</code></td>
<td></td>
</tr>
<tr>
<td>• `dnis {dnis-number</td>
<td>dnis-group-name}`</td>
</tr>
<tr>
<td>• <code>multihop-hostname ingress-tunnel-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-vpdn-req-in)# domain company.com</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** If you use the `multihop-hostname` command to configure your tunnel switch, you must configure `vpdn search-order` command with the `multihop-hostname` keyword. For more information on configuring the VPDN tunnel authorization search order, see the Configuring AAA for VPDNs module.
### Configuration Examples for Multihop VPDN

#### Example Configuring Multihop VPDN Tunnel Switching

The following example configures a NAS, tunnel switch, and tunnel server to establish a multihop VPDN tunnel using L2TP:

**NAS Configuration**

```plaintext
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch

 vpdn-group 1
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Router(config-vpdn-req-in)# dnis 5687</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn-req-in)# multihop-hostname nas1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits to VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn-req-in)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> initiate-to ip ip-address [limit limit-number] [priority priority-number]</td>
<td>Specifies an IP address that will be used for Layer 2 tunneling.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn)# initiate-to ip 10.1.1.1 limit 12</td>
<td>- limit --Maximum number of connections that can be made to this IP address.</td>
</tr>
<tr>
<td></td>
<td>- priority --Priority for this IP address.</td>
</tr>
</tbody>
</table>

**Note**

The `priority` keyword is typically not configured on a tunnel switch. Information used for load balancing and failover is configured on a remote authentication, authorization, and accounting (AAA) server instead. For more information about configuring load balancing and failover priorities using a remote AAA server, see the Configuring AAA for VPDNs module.

- Multiple tunnel servers can be configured on the tunnel switch by configuring multiple `initiate-to` commands.
request-dialin
  protocol l2tp
  domain cisco.com
!
initiate-to ip 172.22.66.25
local name ISP-NAS

Tunnel Switch Configuration

!Enable VPDN
vpdn enable
!
!Enable multihop
vpdn multihop
!
! Configure the tunnel switch to use the multihop hostname in the authentication search.
vpdn search-order multihop-hostname domain dnis
!
! Configure the tunnel switch to accept dial-in sessions from the NAS
vpdn-group tunnelin
  accept-dialin
  protocol l2tp
  virtual-template 1
!
  terminate-from hostname ISP-NAS
  local name ISP-Sw
!
! Configure the tunnel switch to initiate VPDN dial-in sessions to the tunnel server
vpdn-group tunnelout
  request-dialin
  protocol l2tp
  multihop-hostname ISP-NAS
!
  initiate-to ip 10.2.2.2
  local name ISP-Sw

Tunnel Server Configuration

! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
!
  terminate-from hostname ISP-Sw
  local name ENT-TS

Where to Go Next

You can perform any of the relevant optional tasks in the Configuring Additional VPDN Features and in the VPDN Tunnel Management modules.
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview</td>
</tr>
<tr>
<td>Broadband access aggregation and DSL commands</td>
<td>Cisco IOS Broadband Access Aggregation and DSL Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
</tbody>
</table>
### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

### Feature Information for Multihop VPDN

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 . An account on Cisco.com is not required.

**Table 11: Feature Information for Multihop VPDN**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multihop VPDN</td>
<td>Cisco IOS XE Release 2.2</td>
<td>This feature was introduced on Cisco ASR 1000 Series Routers. Multihop VPDN is a specialized VPDN configuration that allows packets to pass through multiple tunnels. Ordinarily, packets are not allowed to pass through more than one tunnel. In a multihop deployment, the VPDN tunnel is terminated after each hop and a new tunnel is initiated to the next hop destination. No commands were introduced or modified by this feature.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Software Releases</td>
<td>Feature Configuration Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subscriber Service Switch</td>
<td>Cisco IOS XE Release 2.2.1</td>
<td>This feature provides flexibility on where and how many subscribers are connected to available services and how those services are defined. The primary focus of SSS is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy will manage tunneling of PPP in a policy-based bridging fashion. The following VPDN commands were introduced or modified by this feature: <strong>multihop-hostname</strong> and <strong>vpdn search-order</strong>.</td>
</tr>
</tbody>
</table>
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, page 135
- Information About Configuring Additional VPDN Features, page 136
- How to Configure Additional VPDN Features, page 141
- Configuration Examples for Additional VPDN Features, page 165
- Where to Go Next, page 173
- Additional References, page 173
- Feature Information for Additional VPDN Features, page 175

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 at the end of this module.
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 137. 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>vpdn-template [name]</td>
<td>Creates a VPDN template and enters VPDN template configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-template l2tp</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Associates a VPDN group with a VPDN template.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>vpdn-group name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>VPDN groups are associated with the unnamed VPDN template by default.</td>
</tr>
<tr>
<td>Router(config)# vpdn-group l2tp</td>
<td>If you have disassociated a VPDN group from the VPDN template using the</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>source vpdn-template [name]</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>no source vpdn-template command, you can reassociate it by issuing the</td>
</tr>
<tr>
<td>Router(config-vpdn)# source vpdn-template l2tp</td>
<td>source vpdn-template command.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>vpdn-group name</code></td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# vpdn-group l2tp</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
PurposeCommand or Action

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3 vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group 1</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

| Step 4 | source-ip  | ip-address

**Example:**

```
Router(config-vpdn)# source-ip 10.1.1.1
```

**Purpose**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn-group mygroup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vpn {vrf vrf-name</td>
<td>id vpn-id}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn)# vpn vrf myvrf</td>
<td>• vrf vrf-name --Specifies the VRF instance by the VRF name.</td>
</tr>
<tr>
<td></td>
<td>• id vpn-id --Specifies the VRF instance by the VPN ID.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Cisco-Avpair = vpdn:tunnel-id= name</td>
<td>Specifies the tunnel ID in the RADIUS user profile.</td>
</tr>
<tr>
<td>Example: Cisco-Avpair = vpdn:tunnel-id=test</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** Cisco-Avpair = vpdn:tunnel-type= l2tp | Specifies L2TP as the tunneling protocol in the RADIUS user profile. |
| Example: Cisco-Avpair = vpdn:tunnel-type=l2tp | |

| **Step 3** Cisco-Avpair = vpdn:vpn-vrf= vrf-name | Specifies the VRF instance that the VPDN tunnel should be associated with using the VRF name in the RADIUS user profile. |
| Example: or Cisco-Avpair = vpdn:vpn-id= vpn-id | or Specifies the VRF instance that the VPDN tunnel should be associated with using the VPN ID in the RADIUS user profile. |
| Example: | |
### Step 4: Configuring Additional VPDN Features

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:vpn-vrf=myvrf</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Cisco-Avpair = vpdn:vpn-id=A1:3F6C</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| Example:                    | Router# configure terminal |

| **Step 3** interface virtual-template number | Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode. |
| Example:                              | Router(config)# interface virtual-template 1 |

| **Step 4** ip mtu bytes | Sets the MTU size of IP packets sent on an interface. |
| Example:                 | Router(config-if)# ip mtu 1460 |

**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

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

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. 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.

---

**Caution**

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.

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>vpdn-group <em>name</em></td>
<td></td>
</tr>
<tr>
<td>Example: Router(config)# vpdn-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the discovery of a path MTU for Layer 2 traffic.</td>
</tr>
<tr>
<td>ip pmtu</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config-vpdn)# ip pmtu</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits VPDN group configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example: Router(config-vpdn)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| configure terminal| Router# configure terminal |

| **Step 3**        | Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode. |
| interface virtual-template number | |
| **Example:**      | Router(config)# interface virtual-template 1 |

| **Step 4**        | Adjusts the MSS value of TCP SYN packets going through a router. |
| ip tcp adjust-mss bytes | |
| **Example:**      | Router(config-if)# ip tcp adjust-mss 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>interface virtual-template <strong>number</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface virtual-template 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mtu <strong>bytes</strong></td>
<td>Adjusts the maximum packet size or MTU size.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# mtu 1460</td>
<td>Note Because Layer 2 headers are 40 bytes, the recommended value for the <strong>bytes</strong> argument is 1460.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>(Optional) Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vpdn-group <strong>name</strong></td>
<td>(Optional) Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# vpdn-group 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>lcp renegotiation **{always</td>
<td>on-mismatch}**</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# lcp renegotiation always</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:**  
Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode.  
**Example:**  
Router# configure terminal | |
| **Step 3** vpdn-group name | Creates a VPDN group and enters VPDN group configuration mode.  
**Example:**  
Router(config)# vpdn-group 1 | |
| **Step 4** 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.  
**Example:**  
Router(config-vpdn)# accept-dialin | |
| **Step 5** protocol l2tp | Specifies the tunneling protocol that a VPDN subgroup will use.  
**Example:**  
Router(config-vpdn-acc-in)# protocol l2tp | |
| **Step 6** terminate-from hostname hostname | Specify the hostname of the remote LAC or LNS that will be required when accepting a VPDN tunnel.  
**Example:**  
Router(config-vpdn-acc-in)# terminate-from hostname example | |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits VPDN accept dial-in group configuration mode.</td>
</tr>
</tbody>
</table>

### Example:

Router(config-vpdn-acc-in)# exit

---

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>vpdn-group name</code></td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group 1</td>
<td></td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>vpdn-group name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn-group 1</td>
</tr>
<tr>
<td>Step 4</td>
<td>accept-dialin</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn)# accept dialin</td>
</tr>
<tr>
<td>Step 5</td>
<td>protocol l2tp</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn-acc-in)# protocol l2tp</td>
</tr>
<tr>
<td>Step 6</td>
<td>vpn vrf vrf-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn-acc-in)# vpn vrf myvrf</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>
Displaying VPDN Group Selections

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>show vpdn group-select</td>
<td>Displays the information for the selected VPDN group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; show vpdn group-select</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; exit</td>
<td></td>
</tr>
</tbody>
</table>

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:
Perfom 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group 1</td>
<td></td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>vpdn-group <em>name</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config)# vpdn-group 1</td>
</tr>
</tbody>
</table>

**Create a VPDN group and enters VPDN group configuration mode.**

**Step 4**

<table>
<thead>
<tr>
<th>ip precedence [number</th>
<th>name]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# ip precedence 1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
## Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip tos {tos-bit-value</td>
<td>max-reliability</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-vpdn)# ip tos 9</td>
<td></td>
</tr>
</tbody>
</table>

## 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
```
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:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```plaintext
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.

```plaintext
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-vpn)# 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-vpn)# 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-group 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)# exit

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-B
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
```
Examples Displaying VPDN Group Selection

The VPDN Group Selection feature allows you to display VPDN group information based on 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 12tp
Router(config-vpdn-acc-in)# virtual-template 20
Router(config-vpdn-acc-in)# local name lns
Router(config-vpdn)# 12tp 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 12tp
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)# 12tp 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 12tp
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)# 12tp 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 12tp
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)# 12tp 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 12tp
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)# 12tp 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 12tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts1
```
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
vgl          10.1.1.2  l2tp  accept-dialin
vgl          10.1.1.3  l2tp  accept-dialin
vgl          0.0.0.0  l2tp  accept-dialin
vgl          10.1.1.2  l2tp  accept-dialin
vgl          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
vgl          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
vgldefault  l2tp
vgldefault  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 10.1.0.1, 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
vgl          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**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview</td>
</tr>
</tbody>
</table>
### Related Topic

| 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 |
| 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

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1191</td>
<td>Path MTU Discovery</td>
</tr>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
<tr>
<td>RFC 2923</td>
<td>TCP Problems with Path MTU Discovery</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

### 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 . An account on Cisco.com is not required.

#### Table 12: Feature Information for Configuring Additional VPDN Features

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPDN Default Group Template</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Software Releases</td>
<td>Feature Configuration Information</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VPDN Group Selection</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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: <code>show vpdn group-select</code> and <code>show vpdn group-select keys</code>.</td>
</tr>
<tr>
<td>VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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.</td>
</tr>
<tr>
<td>VRF-Aware VPDN Tunnels</td>
<td>Cisco IOS XE Release 2.2</td>
<td>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: <code>vpn</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 7

VPDN Tunnel Management

This module contains information about managing virtual private dialup network (VPDN) tunnels and monitoring VPDN events. The tasks documented in this module should be performed only after configuring and deploying a VPDN.

- Finding Feature Information, page 177
- Prerequisites for VPDN Tunnel Management, page 177
- Restrictions for VPDN Tunnel Management, page 178
- Information About VPDN Tunnel Management, page 178
- How to Manage VPDN Tunnels, page 180
- Configuration Examples for VPDN Tunnel Management, page 196
- Additional References, page 200
- Feature Information for VPDN Tunnel Management, page 201

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 at the end of this module.

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.

Prerequisites for VPDN Tunnel Management

Before you can perform the tasks in this module, you must configure a VPDN deployment. For an overview of VPDN deployments, see the VPDN Technology Overview module.
Restrictions for VPDN Tunnel Management

VPDN tunnels using the Layer 2 Forwarding (L2F) protocol or Point-to-Point Tunnel Protocol (PPTP) are not supported.

Information About VPDN Tunnel Management

Termination of VPDN Tunnels

VPDN tunnels can be terminated manually or through a soft shutdown. Manual termination of a VPDN tunnel results in the immediate shutdown of the specified VPDN tunnel and all sessions within that tunnel, resulting in a sudden disruption of VPDN services. Enabling soft shutdown on a router prevents the establishment of new VPDN sessions in all VPDN tunnels that terminate on that router, but does not affect existing sessions. Opting to terminate a VPDN tunnel by enabling soft shutdown prevents the disruption of established sessions that occurs when a VPDN tunnel is manually terminated.

VPDN Session Limits

The number of simultaneous VPDN sessions that can be established on a router can be manually configured, providing network administrators more control over the network. VPDN session limits can increase performance and reduce latency for routers that are otherwise forced to operate at high capacity.

The maximum number of VPDN sessions can be configured globally, at the level of a VPDN group, or for all VPDN groups associated with a particular VPDN template.

The hierarchy for the application of VPDN session limits is as follows:

• Globally configured session limits take precedence over session limits configured for a VPDN group or in a VPDN template. The total number of sessions on a router cannot exceed a configured global session limit.

• Session limits configured for a VPDN template are enforced for all VPDN groups associated with that VPDN template. The total number of sessions for all of the associated VPDN groups cannot exceed the configured VPDN template session limit.

• Session limits configured for a VPDN group are enforced for that VPDN group.

Control Packet Parameters for VPDN Tunnels

Certain control packet timers, retry counters, and the advertised control packet receive window size can be configured for Layer 2 Transport Protocol (L2TP) or Layer 2 Forwarding (L2F) VPDN tunnels. Adjustments to these parameters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.
L2TP Congestion Avoidance

L2TP congestion avoidance provides packet flow control and congestion avoidance by throttling L2TP control messages as described in RFC 2661. Throttling L2TP control message packets prevents input buffer overflows on the peer tunnel endpoint, which can result in dropped sessions.

Before the introduction of L2TP congestion avoidance, the window size used to send packets between the network access server (NAS) and the tunnel server was set to the value advertised by the peer endpoint and was never changed. Configuring L2TP congestion avoidance allows the L2TP packet window to be dynamically resized using a sliding window mechanism. The window size grows larger when packets are delivered successfully, and is reduced when dropped packets must be retransmitted.

L2TP congestion avoidance is useful in networks with a relatively high rate of calls being placed by either tunnel endpoint. L2TP congestion avoidance is also useful on highly scalable platforms that support many simultaneous sessions.

How L2TP Congestion Avoidance Works

TCP/IP and RFC 2661 define two algorithms--slow start and congestion avoidance--used to throttle control message traffic between a NAS and a tunnel server. Slow start and congestion avoidance are two independent algorithms that work together to control congestion. Slow start and congestion avoidance require that two variables, a slow start threshold (SSTHRESH) size and a congestion window (CWND) size, be maintained by the sending device for each connection.

The congestion window defines the number of packets that can be transmitted before the sender must wait for an acknowledgment from its peer. The size of the congestion window expands and contracts, but can never exceed the size of the peer device’s advertised receive window.

The slow start threshold defines the point at which the sending device switches operation from slow start mode to congestion avoidance mode. When the congestion window size is smaller than the slow start threshold, the device operates in slow start mode. When the congestion window size equals the slow start threshold, the device switches to congestion avoidance mode.

When a new connection is established, the sending device initially operates in slow start mode. The congestion window size is initialized to one packet, and the slow start threshold is set to the receive window size advertised by the peer tunnel endpoint (the receiving side).

The sending device begins by transmitting one packet and waiting for it to be acknowledged. When the acknowledgment is received, the congestion window size is incremented from one to two, and two packets can be sent. When those two packets are each acknowledged, the congestion window is increased to four. The congestion window doubles for each complete round trip, resulting in an exponential increase in size.

When the congestion window size reaches the slow start threshold value, the sending device switches over to operate in congestion avoidance mode. Congestion avoidance mode slows down the rate at which the congestion window size grows. In congestion avoidance mode, for every acknowledgment received the congestion window increases at the rate of 1 divided by the congestion window size. This results in linear, rather than exponential, growth of the congestion window size.

At some point, the capacity of the peer device will be exceeded and packets will be dropped. This indicates to the sending device that the congestion window has grown too large. When a retransmission event is detected, the slow start threshold value is reset to half of the current congestion window size, the congestion window size is reset to one, and the device switches operation to slow start mode (if it was not already operating in that mode).
VPDN Event Logging

There are two types of VPDN event logging available, VPDN failure event logging and generic VPDN event logging. The logging of VPDN failure events is enabled by default. Generic VPDN event logging is disabled by default, and must be explicitly enabled before generic event messages can be viewed.

How to Manage VPDN Tunnels

Manually Terminating VPDN Tunnels

Manual termination of a VPDN tunnel results in the immediate shutdown of the specified VPDN tunnel and all sessions within that tunnel, resulting in a sudden disruption of VPDN services. Before manually terminating a VPDN tunnel, consider performing the task in the Enabling Soft Shutdown of VPDN Tunnels, on page 181 instead.

A manually terminated VPDN tunnel can be restarted immediately when a user logs in. Manually terminating and restarting a VPDN tunnel while VPDN event logging is enabled can provide useful troubleshooting information about VPDN session establishment.

Perform this task to manually shut down a specific VPDN tunnel, resulting in the termination of the tunnel and all sessions in that tunnel. You can perform this task on these devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

Note

- For client-initiated L2TP tunnels, you can perform this task only on the tunnel server.
- Tunnels using the L2F protocol and PPTP are not supported.

SUMMARY STEPS

1. enable
2. clear vpdn tunnel l2tp {all | hostname remote-name [local-name] | id local-id | ip local-ip-address | ip remote-ip-address}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
## Enabling Soft Shutdown of VPDN Tunnels

Enabling soft shutdown of VPDN tunnels on a router prevents the establishment of new VPDN sessions in all VPDN tunnels that terminate on that router, but does not affect existing sessions. Opting to terminate a VPDN tunnel by enabling soft shutdown prevents the disruption of established sessions that occurs when a VPDN tunnel is manually terminated. Enabling soft shutdown on a router or access server will affect all of the tunnels terminating on that device. There is no way to enable soft shutdown for a specific tunnel. If you want to shut down a specific tunnel on a device without affecting any other tunnels, see the Manually Terminating VPDN Tunnels, on page 180 instead.

When soft shutdown is performed on a NAS, the potential session will be authorized before it is refused. This authorization ensures that accurate accounting records can be kept.

When soft shutdown is performed on a tunnel server, the reason for the session refusal will be returned to the NAS. This information is recorded in the VPDN history failure table.

### Note

Enabling soft shutdown of VPDN tunnels does not affect the establishment of Multichassis Multilink PPP (MMP) tunnels.

Perform this task to prevent new sessions from being established in any VPDN tunnel terminating on the router without disturbing service for existing sessions. You can perform this task on these devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

### Note

- For client-initiated L2TP tunnels, you can perform this task only on the tunnel server.
- Enabling soft shutdown of VPDN tunnels will not prevent new MMP sessions from being established.

### Command or Action | Purpose
--- | ---
Step 2 | clear vpdn tunnel l2tp \{all | hostname remote-name [local-name] | id local-id | ip local-ip-address | ip remote-ip-address\}
Example: | Router# clear vpdn tunnel l2tp all

Shuts down a specified tunnel and all sessions within the tunnel.
SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn softshut

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn softshut</td>
<td>Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn softshut</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Soft Shutdown of VPDN Tunnels

Perform this task to ensure that soft shutdown is working properly.

SUMMARY STEPS

1. Establish a VPDN session by dialing into the NAS using an allowed username and password.
2. enable
3. configure terminal
4. vpdn softshut
5. exit
6. show vpdn
7. Attempt to establish a new VPDN session by dialing into the NAS using a second allowed username and password.
8. show vpdn history failure
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Establish a VPDN session by dialing in to the NAS using an allowed username and password.</td>
</tr>
</tbody>
</table>
| **Step 2** | enable  
Example:  
Router> enable  
- Enter your password if prompted. |
| **Step 3** | configure terminal  
Example:  
Router# configure terminal |
| **Step 4** | vpdn softshut  
Example:  
Router(config)# vpdn softshut  
Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions. You can issue this command on either the NAS or the tunnel server. |
| **Step 5** | exit  
Example:  
Router(config)# exit  
Exits to privileged EXEC mode. |
| **Step 6** | show vpdn  
Example:  
Router# show vpdn  
Displays information about active L2TP or L2F tunnels and message identifiers in a VPDN. Issue this command to verify that the original session is active: |
| **Step 7** | Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.  
If soft shutdown has been enabled, a system logging (syslog) message appears on the console of the soft shutdown router. |
| **Step 8** | show vpdn history failure  
Example:  
Router# show vpdn history failure  
Displays the content of the history failure table. |
Limiting the Number of Allowed Simultaneous VPDN Sessions

The number of simultaneous VPDN sessions that can be established on a router can be manually configured, providing network administrators more control over the network. VPDN session limits can increase performance and reduce latency for routers that are otherwise forced to operate at high capacity.

The maximum number of VPDN sessions can be configured globally, at the level of a VPDN group, or for all VPDN groups associated with a particular VPDN template.

The hierarchy for the application of VPDN session limits is as follows:

- Globally configured session limits take precedence over session limits configured for a VPDN group or in a VPDN template. The total number of sessions on a router cannot exceed a configured global session limit.
- Session limits configured for a VPDN template are enforced for all VPDN groups associated with that VPDN template. The total number of sessions for all of the associated VPDN groups cannot exceed the configured VPDN template session limit.
- Session limits configured for a VPDN group are enforced for that VPDN group.

For an example of the interactions of global, template-level, and group-level VPDN session limits, see the "Examples Configuring VPDN Session Limits" section.

Perform any or all of the following optional tasks to configure VPDN session limits:

You can perform these tasks on the NAS or the tunnel server.

Restrictions

For client-initiated L2TP tunnels, you can perform these tasks only on the tunnel server.

Configuring Global VPDN Session Limits

Perform this task to limit the total number of VPDN sessions allowed on the router.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn session-limit sessions

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 2**

configure terminal

**Example:**

Router# configure terminal

**Step 3**

vpdn session-limit sessions

**Example:**

Router(config)# vpdn session-limit 6

---

### Configuring VPDN Session Limits in a VPDN Template

Perform this task to configure a session limit in a VPDN template. The session limit is applied across all VPDN groups associated with the VPDN template.

**Before You Begin**

- A VPDN template must be configured. See the "Creating a VPDN Template" section in the "Configuring Additional VPDN Features" module.

- If you configure a named VPDN template, you must associate the desired VPDN groups with the VPDN template. See the "Associating a VPDN Group with a VPDN Template" section in the "Configuring Additional VPDN Features" module.

### SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-template [name]
4. group session-limit sessions

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Session Limits for a VPDN Group

Perform this task to limit the number of VPDN sessions at the VPDN group level.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group *name*
4. session-limit *number*

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td>vpdn-group <em>name</em></td>
</tr>
<tr>
<td>4</td>
<td>session-limit <em>number</em></td>
</tr>
</tbody>
</table>

### Verifying VPDN Session Limits

Perform this task to ensure that VPDN sessions are being limited properly.

> Note<br>If you use a Telnet session to connect to the NAS, enable the `terminal monitor` command, which ensures that your EXEC session is receiving the logging and debug output from the NAS.

#### SUMMARY STEPS

1. enable<br>2. configure terminal<br>3. vpdn session-limit *sessions*<br>4. Establish a VPDN session by dialing in to the NAS using an allowed username and password.<br>5. Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.<br>6. exit<br>7. show vpdn history failure

#### DETAILED STEPS

**Step 1** enable<br>Enter this command to enable privileged EXEC mode. Enter your password if prompted:

Example: <br>`Router> enable`

**Step 2** configure terminal<br>Enters global configuration mode.
Example:

Router# configure terminal

Step 3  **vpdn session-limit sessions**
Limits the number of simultaneous VPDN sessions on the router to the number specified with the **sessions** argument.
Issue this command on either the NAS or the tunnel server.

Example:

Router(config)# vpdn session-limit 1

Step 4  Establish a VPDN session by dialing into the NAS using an allowed username and password.

Step 5  Attempt to establish a new VPDN session by dialing into the NAS using a second allowed username and password.
If VPDN session limits have been configured properly, this session will be refused and a syslog message similar to the following should appear on the console of the router:

Example:

00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW tunnelserver1 has exceeded configured local session-limit and rejected user user2@cisco.com

Step 6  exit
Exits to privileged EXEC mode.

Step 7  show vpdn history failure
Shows the content of the history failure table.

Example:

Router# show vpdn history failure
User:user2@cisco.com
NAS:NAS1, IP address = 172.25.52.8, CLID = 2
Gateway:tunnelserver1, IP address = 172.25.52.7, CLID = 13
Log time:00:04:21, Error repeat count:1
Failure type:Exceeded configured VPDN maximum session limit.
!This output shows that the configured session limit is being properly applied.
Failure reason:

### Configuring L2TP Control Packet Parameters for VPDN Tunnels

Control packet timers, retry counters, and the advertised control packet receive window size can be configured for L2TP VPDN tunnels. Adjustments to these parameters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.

Perform this task to configure control packet parameters if your VPDN configuration uses L2TP tunnels. The configuration of each parameter is optional. If a parameter is not manually configured, the default value will be used.

You can perform this task on these devices:
• The tunnel server
• The NAS when it is functioning as a tunnel endpoint

Before You Begin
Load balancing must be enabled for the configuration of the `l2tp tunnel retransmit initial timeout` command or the `l2tp tunnel retransmit initial retries` command to have any effect.

---

Note
For client-initiated L2TP tunnels, you can perform this task only on the tunnel server.

SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn-group name
4. l2tp tunnel hello seconds
5. l2tp tunnel receive window packets
6. l2tp tunnel retransmit retries number
7. l2tp tunnel retransmit timeout \{min | max\} seconds
8. l2tp tunnel timeout no-session \{seconds | never\}
9. l2tp tunnel timeout setup seconds
10. l2tp tunnel zlb delay seconds
11. l2tp tunnel retransmit initial timeout \{min | max\} seconds
12. l2tp tunnel retransmit initial retries number
13. l2tp tunnel busy timeout seconds

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enters your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>3</td>
<td><code>vpdn-group name</code></td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# vpdn-group group1</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>l2tp tunnel hello seconds</code></td>
<td>(Optional) Set the number of seconds between sending hello keepalive packets for an L2TP tunnel.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-vpdn)# l2tp tunnel hello 90</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>l2tp tunnel receive window packets</code></td>
<td>(Optional) Configures the number of packets allowed in the local receive window for an L2TP control channel.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-vpdn)# l2tp tunnel receive window 500</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>l2tp tunnel retransmit retries number</code></td>
<td>(Optional) Configures the number of retransmission attempts made for an L2TP control packet.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-vpdn)# l2tp tunnel retransmit retries 8</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>`l2tp tunnel retransmit timeout {min</td>
<td>max} seconds`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-vpdn)# l2tp tunnel retransmit timeout max 4</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>`l2tp tunnel timeout no-session {seconds</td>
<td>never}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-vpdn)# l2tp tunnel timeout no-session never</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>l2tp tunnel timeout setup</strong> <em>seconds</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures the amount of time that the router will wait for a confirmation message after sending out the initial L2TP control packet before considering a peer busy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>seconds</em> --Time, in seconds, the router will wait for a confirmation message. Valid values range from 60 to 6000. The default value is 10.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>l2tp tunnel zlb delay</strong> <em>seconds</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures the delay time before a zero length bit (ZLB) control message must be acknowledged.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>seconds</em> --Maximum number of seconds the router will delay before acknowledging ZLB control messages. Valid values range from 1 to 5. The default value is 3.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 11** | **l2tp tunnel retransmit initial timeout** *
| Example: | (Optional) Sets the amount of time, in seconds, that the router will wait before resending an initial packet out to establish a tunnel. |
| | • *min* --Specifies the minimum time that the router will wait before resending an initial packet. |
| | • *max* --Specifies the maximum time that the router will wait before resending an initial packet. |
| | • *seconds* --Timeout length, in seconds, the router will wait before resending an initial packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8. |
| **Step 12** | **l2tp tunnel retransmit initial retries** *
| Example: | (Optional) Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy. |
| | • *number* --Number of retransmission attempts. Valid values range from 1 to 1000. The default value is 2. |
| **Step 13** | **l2tp tunnel busy timeout** *seconds*  |
| Example: | (Optional) Configures the amount of time, in seconds, that the router will wait before attempting to recontact a router that was previously busy. |
| | • *seconds* --Time, in seconds, the router will wait before checking for router availability. Valid values range from 60 to 6000. The default value is 300. |
Configuring L2TP Congestion Avoidance

Perform this task to configure L2TP congestion avoidance on a tunnel endpoint, allowing dynamic throttling of the L2TP control packet window size.

You can perform this task on these devices:

• The tunnel server
• The NAS when it is functioning as a tunnel endpoint

This task need be performed only on the sending device.

Note

• This task is compatible only with VPDN deployments that use the L2TP tunneling protocol.
• For client-initiated L2TP tunnels, you can perform this task only on the tunnel server.
• The congestion window size cannot exceed the size of the advertised receive window set by the `l2tp tunnel receive-window` command on the peer device. To configure the advertised receive window on the remote peer device, see the Configuring L2TP Control Packet Parameters for VPDN Tunnels, on page 188.
• L2TP congestion avoidance is enabled (or disabled) only for those tunnels that are established after the configuration has been applied. Tunnels that already exist when the `l2tp congestion-control` command is issued are not affected by the command.

SUMMARY STEPS

1. enable
2. configure terminal
3. l2tp congestion-control
4. exit
5. show vpdn tunnel l2tp all
6. debug vpdn l2x-events

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> l2tp congestion-control</td>
<td>Enables L2TP congestion avoidance.</td>
</tr>
<tr>
<td>Example: Router(config)# l2tp congestion-control</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show vpdn tunnel l2tp all</td>
<td>Displays information about all active L2TP VPDN tunnels.</td>
</tr>
<tr>
<td>Example: Router# show vpdn tunnel l2tp all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> debug vpdn l2x-events</td>
<td>Displays troubleshooting information for protocol-specific VPDN tunneling events.</td>
</tr>
<tr>
<td>Example: Router(config)# debug vpdn l2x-events</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring VPDN Failure Event Logging

Logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a history failure table, which keeps records of failure events. The table defaults to a maximum of 20 entries, but the size of the table can be configured to retain up to 50 entries.

Failure entries are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept. When the total number of entries in the table reaches the configured maximum table size, the oldest record is deleted and a new entry is added.

The logging of VPDN failure events to the VPDN history failure table is enabled by default. You need enable VPDN failure event logging only if it has been previously disabled. Perform this task to enable VPDN failure event logging, to configure the maximum number of entries the history failure table can hold, and to display and clear the contents of the VPDN history failure table.
### SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn history failure
4. vpdn history failure table-size entries
5. exit
6. show vpdn history failure
7. clear vpdn history failure

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>vpdn history failure</td>
<td>(Optional) Enables logging of VPDN failure events to the history failure table.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn history failure</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>VPDN history failure logging is enabled by default. You need issue the vpdn history failure command only if you have previously disabled VPDN history failure logging using the no vpdn history failure command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>vpdn history failure table-size entries</td>
<td>(Optional) Sets the history failure table size.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# vpdn history failure table-size 50</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>The VPDN history failure table size can be configured only when VPDN failure event logging is enabled using the vpdn history failure command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>show vpdn history failure</td>
<td>(Optional) Displays the contents of the history failure table.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show vpdn history failure</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling Generic VPDN Event Logging

Generic VPDN events are a mixture of error, warning, notification, and information reports logged by the syslog facility. When VPDN event logging is enabled locally or at a remote tunnel endpoint, VPDN event messages are printed to the console as the events occur. VPDN event messages can also be reported to a remote authentication, authorization, and accounting (AAA) server in a AAA vendor-specific attribute (VSA), allowing the correlation of VPDN call success rates with accounting records.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vpdn logging [accounting | local | remote | tunnel-drop | user]`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`vpdn logging [accounting</td>
<td>local</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# vpdn logging remote</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The reporting of VPDN event log messages to a AAA server can be enabled independently of all other generic VPDN event logging configurations.
Configuration Examples for VPDN Tunnel Management

Examples Manually Terminating VPDN Tunnels

The following example manually terminates all L2TP tunnels that terminate on the router:

```
Router# clear vpdn tunnel l2tp all
```

Example Enabling Soft Shutdown of VPDN Tunnels

The following example enables soft shutdown of all VPDN tunnels that terminate on the device that the command is issued on:

```
Router# configure terminal
Router(config)# vpdn softshut
!
The following syslog message will appear on the device whenever an attempt is made to
establish a new VPDN session after soft shutdown is enabled.

00:11:17:%VPDN-6-SOFTSHUT:L2TP HGW tunnelserver1 has turned on softshut and rejected user
user2@cisco.com
```

Examples Configuring VPDN Session Limits

The following example configures a VPDN group named customer7 with a group-level session limit of 25. No more than 25 sessions can be associated with this VPDN group.

```
Router(config)# vpdn-group customer7
Router(config-vpdn)# session-limit 25
```

A VPDN template named customer4 is then created, and a session limit of 8 is configured at the VPDN template level. Two VPDN groups are associated with the VPDN template, each with a VPDN group-level session limit of 5.

```
Router(config)# vpdn-template customer4
Router(config-vpdn-templ)# group session-limit 8
!
Router(config)# vpdn-group customer4_l2tp
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
!
Router(config)# vpdn-group customer4_l2f
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
```

With this configuration, if the VPDN group named customer4_l2tp has 5 active sessions, the VPDN group named customer4_l2f can establish only 3 sessions. The VPDN group named customer7 can still have up to 25 active sessions.
If a global limit of 16 VPDN sessions is also configured, the global limit takes precedence over the configured VPDN group and VPDN template session limits:

```
Router# configure terminal
Router(config)# vpdn session-limit 16
```

The three VPDN groups will be able to establish a total of 16 sessions between them. For example, if the VPDN group named customer4_l2tp has the maximum allowable number of active sessions (5 sessions), and the VPDN group named customer4_l2f has 2 active sessions, the VPDN group named customer7 can establish only up to 9 sessions.

### Example Verifying Session Limits for a VPDN Group

The following example creates the VPDN group named l2tp and restricts it to three sessions. The configured session limit is displayed when the `show vpdn group` command is issued.

```
Router# configure terminal
Router(config)# vpdn-group l2tp
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)# exit
Router(config-vpdn)# terminate-from hostname host1
Router(config-vpdn)# session-limit 3
Router(config-vpdn)# end
Router# show vpdn group l2tp
```

```
Tunnel (L2TP)
---
dnis:cg1
dnis:cg2
dnis:jan
cisco.com
Endpoint Session Limit Priority Active Sessions Status Reserved Sessions
-------- ------------- -------- --------------- ------ ---------------------
172.21.9.67 3 1 0 OK -

Total * 0 0
```

### Example Configuring L2TP Control Packet Timers and Retry Counters for VPDN Tunnels

The following example configures custom values for all of the available L2TP control packet parameters for the VPDN group named l2tp:

```
Router# configure terminal
Router(config)# vpdn-group l2tp
```

```
Router(config-vpdn)# 12tp tunnel hello 90
Router(config-vpdn)# 12tp tunnel receive window 500
Router(config-vpdn)# 12tp tunnel retransmit retries 8
Router(config-vpdn)# 12tp tunnel retransmit timeout min 2
Router(config-vpdn)# 12tp tunnel timeout no-session 500
Router(config-vpdn)# 12tp tunnel timeout setup 25
Router(config-vpdn)# 12tp tunnel zlb delay 4
Router(config-vpdn)# 12tp tunnel retransmit initial timeout min 2
Router(config-vpdn)# 12tp tunnel retransmit initial retries 5
Router(config-vpdn)# 12tp tunnel busy timeout 90
```
Example Configuring Verifying and Debugging L2TP Congestion Avoidance

The following example configures a basic dial-in L2TP VPDN tunnel, sets the receive window size to 500 on the tunnel server (the receiving device), and enables L2TP congestion avoidance on the NAS (the sending device):

**Tunnel Server Configuration**

```console
Router(config)# vpn enable
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
Router(config-vpdn)# terminate from hostname NAS1
Router(config-vpdn)# l2tp tunnel receive-window 500
```

**NAS Configuration**

```console
Router(config)# vpn enable
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
Router(config-vpdn)# initiate-to ip 172.22.66.25
Router(config-vpdn)# local name NAS1
Router(config)# l2tp congestion-control
```

The following example shows L2TP tunnel activity, including the information that L2TP congestion control is enabled. Note that the slow start threshold is set to the same size as the remote receive window size. The Remote RWS value advertised by the remote peer is shown in the Remote RWS field. When the actual RWS value differs from the advertised value, the actual RWS value will be displayed as In Use Remote RWS <value>.

```console
Router# show vpdn tunnel l2tp all
L2TP Tunnel Information Total tunnels 1 sessions 1
Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
  Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
  Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 1024 (default), Remote RWS 256
  In Use Remote RWS 15
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 256
    Mode of operation is Slow Start
    Tunnel PMTU checking disabled
    Retransmission time 1, max 2 seconds
    Unsent queue size 0, max 0
```
Resend queue size 0, max 1
Total retransmits 0, ZLB ACKs sent 2
Current no session queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
Control message authentication is disabled

The following partial output from the `debug vpdn l2x-events` command shows that congestion occurred. The congestion window size and the slow start threshold have been reset due to a packet retransmission event.

```
Router# debug vpdn l2x-events
!
* Jul 15 19:02:57.963: Tnl 47100 L2TP: Congestion Control event received is retransmission
* Jul 15 19:02:57.963: Tnl 47100 L2TP: Congestion Window size, Cwnd 1
* Jul 15 19:02:57.963: Tnl 47100 L2TP: Slow Start threshold, Ssthresh 2
* Jul 15 19:02:57.963: Tnl 47100 L2TP: Remote Window size, 500
* Jul 15 19:02:57.963: Tnl 47100 L2TP: Control channel retransmit delay set to 4 seconds
* Jul 15 19:03:01.607: Tnl 47100 L2TP: Update ns/nr, peer ns/nr 2/5, our ns/nr 5/2
!
```

The following partial output from the `debug vpdn l2x-events` command shows that traffic has been restarted with L2TP congestion avoidance operating in slow start mode.

```
Router# debug vpdn l2x-events
!
* Jul 15 14:45:16.123: Tnl 30597 L2TP: Control channel retransmit delay set to 2 seconds
* Jul 15 14:45:16.123: Tnl 30597 L2TP: Tunnel state change from idle to wait-ctl-reply
* Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Control event received is positive acknowledgement
* Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Window size, Cwnd 2
* Jul 15 14:45:16.131: Tnl 30597 L2TP: Slow Start threshold, Ssthresh 500
* Jul 15 14:45:16.131: Tnl 30597 L2TP: Remote Window size, 500
* Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Ctrl Mode is Slow Start
!
```

**Example Configuring VPDN Failure Event Logging**

The following example first disables and then reenables VPDN failure event logging, and sets the maximum number of entries in the VPDN history failure table to 50. The contents of the history failure table are displayed and then cleared.

```
Router# configure terminal
Router(config)# no vpdn history failure
Router(config)# vpdn history failure
Router(config)# vpdn history failure table-size 50
Router(config)# end
Router# show vpdn history failure
!
Table size: 50
Number of entries in table: 1
User: user@cisco.com, MID = 1
NAS: isp, IP address = 172.21.9.25, CLID = 1
Gateway: hp-gw, IP address = 172.21.9.15, CLID = 1
Log time: 13:08:02, Error repeat count: 1
Failure type: The remote server closed this session
Failure reason: Administrative intervention
!
Router# clear vpdn history failure
```
Examples Configuring Generic VPDN Event Logging

The following example enables VPDN logging locally:

Router# configure terminal
Router(config)# vpdn logging local

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of both VPDN user and VPDN tunnel-drop events to the remote router:

Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# vpdn logging remote
Router(config)# vpdn logging user
Router(config)# vpdn logging tunnel-drop

The following example disables the logging of VPDN events at the remote tunnel endpoint, and enables the logging of VPDN event log messages to the AAA server:

Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# no vpdn logging remote
Router(config)# vpdn logging accounting

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview module</td>
</tr>
<tr>
<td>VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>Technical support documentation for VPDNs</td>
<td>Virtual Private Dial-up Network (VPDN)</td>
</tr>
<tr>
<td>Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Dial Technologies Command Reference</td>
</tr>
<tr>
<td>Concepts and tasks associated with configuring additional VPDN features</td>
<td>Configuring Additional VPDN Features module</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP; slow start and congestion avoidance algorithms</td>
<td><em>TCP/IP Illustrated, Volume 1</em></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-VPDN-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-VPDN-MGMT-EXT-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2661</td>
<td><em>Layer Two Tunneling Protocol (L2TP)</em></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for VPDN Tunnel Management

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 . An account on Cisco.com is not required.
### Table 13: Feature Information for VPDN Tunnel Management

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP Congestion Avoidance</td>
<td>Cisco IOS XE Release 2.3</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It provides packet flow control and congestion avoidance by throttling Layer 2 Transport Protocol (L2TP) control messages as described in RFC 2661. The following commands were introduced or modified by this feature: <code>debug vpdn</code>, <code>l2tp congestion-control</code>.</td>
</tr>
<tr>
<td>Session Limit per VRF</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It allows you to apply session limits on all VPDN groups associated with a common VPDN template. You can limit the number of VPDN sessions that terminate in a single VPN routing and forwarding (VRF) instance. The following commands were introduced or modified by this feature: <code>group session-limit</code>, <code>source vpdn-template</code>, and <code>vpdn-template</code>.</td>
</tr>
<tr>
<td>Timer and Retry Enhancements for L2TP</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It allows the user to configure certain adjustable timers and counters for L2TP. The following commands were introduced by this feature: <code>l2tp tunnel busy timeout</code>, <code>l2tp tunnel retransmit initial retries</code>, and <code>l2tp tunnel retransmit initial timeout</code>.</td>
</tr>
</tbody>
</table>
### Feature Information for VPDN Tunnel Management

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPDN Group Session Limiting</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. It allows the user to configure a limit on the number L2TP VPDN sessions allowed for each VPDN group. The following command was introduced by this feature: <code>session-limit</code> (VPDN).</td>
</tr>
</tbody>
</table>
CHAPTER 8

Configuring L2TP HA Session SSO ISSU on a LAC LNS

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic stateful switchover/In Service Software Upgrade (SSO/ISSU) mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

- Finding Feature Information, page 205
- Prerequisites for L2TP HA Session SSO ISSU on a LAC LNS, page 205
- Restrictions for L2TP HA Session SSO ISSU on a LAC LNS, page 206
- Information About L2TP HA Session SSO ISSU on a LAC LNS, page 206
- How to Configure L2TP HA Session SSO ISSU on a LAC LNS, page 208
- Configuration Examples for L2TP HA Session SSO ISSU on a LAC LNS, page 217
- Additional References, page 219
- Feature Information for L2TP HA Session SSO ISSU on a LAC LNS, page 220

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 at the end of this module.

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.

Prerequisites for L2TP HA Session SSO ISSU on a LAC LNS

- Configure a VPDN deployment. For an overview of VPDN deployments, see the VPDN Technology Overview module.
• This implementation does not require the peer L2TP node to be HA or redundancy aware. It does not require the peer L2TP node to implement L2TP failover RFC.
• Ensure that the peer L2TP node is L2TP RFC compliant.

Restrictions for L2TP HA Session SSO ISSU on a LAC LNS

• Cisco IOS XE Release 2.2 provides support for the L2TP HA Session SSO/ISSU on a LAC/LNS feature on Cisco ASR 1000 Series Routers only.
• Cisco IOS XE Release 2.4 provides support for VPDN Multihop nodes for VPDN tunnels and sessions. VPDN tunnels and sessions are preserved after a Route Processor (RP) failover in a dual RP ASR set up.
• L2TP HA Session SSO/ISSU on a LAC/LNS does not support HA/SSO on the following software features, and sessions with these will be lost following an RP failover:
  • L2TP Dialout
  • L2TP Active Discovery Relay for PPPoE
  • Multilink PPP on LNS

Information About L2TP HA Session SSO ISSU on a LAC LNS

Stateful Switchover

Development of the stateful switchover (SSO) feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

In specific Cisco networking devices that support dual RPs, stateful switchover takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor and designating the other RP as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

SSO is particularly useful at the network edge. Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with dual RPs that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.
If a new L2TP session request is received on a tunnel that is in the resync phase after switchover, it is rejected. A new Cisco vendor-specific disconnect cause code (611) provides the reason for this session disconnect. The `show vpdn history failure` command displays the Failure Type field as *Tunnel in HA resync*.

### Checkpointing Data

SSO is always checkpointing or saving and resynchronizing client-specific state data that transfers to a peer client on a remote RP for HA switchover and on the local RP for ION restart. Once a valid checkpointing session is established, the checkpointed state data is established without error.

### ISSU Software Superpackage and Rolling Upgrade Requirements

This section describes the affects on L2TP when performing an ISSU superpackage or subpackage software upgrade or downgrade on a Cisco ASR 1000 Series Router. During the ISSU operation of software upgrades and downgrades, there can be control traffic interruption in some scenarios of ISSU, causing the L2TP resynchronization operation (with L2TP silent switchover) to fail, resulting in a loss of an L2TP tunnel or session.

In general, there is no effect on the data traffic while performing an ISSU superpackage or subpackage software upgrade or downgrade. Data traffic interruptions are contained within a managed and expected operating set. For example, when you upgrade the software for a given spa, the software upgrade only affects the data traffic serviced by that spa; the remaining network continues to operate normally.

### Software Upgrades and Downgrades

When you are configuring a superpackage software upgrade or downgrade, L2TP sessions and tunnels might be lost. To help mitigate any potential loss of L2TP tunnels or sessions, use a rolling-upgrade method to help minimize any L2TP tunnel or session outages.

**Note**

You can help minimize any tunnel or session outage as seen by the IP layer, by either configuring a backup interface for IP routing or an Ether-channel interface towards the L2TP peer.

For the Cisco ASR 1000 Series Routers, it is important to realize that ISSU-compatibility depends on the software sub-package being upgraded and the hardware configuration. Consolidated packages are ISSU-compatible in dual RP configurations only and have other limitations. The SPA and SIP software sub-packages must be upgraded on a per-SPA or per-SIP basis.

If you are upgrading a software package on the Cisco ASR 1000 Series Router that requires a reload of the standby Route Processor (RP), you must manually initiate a upgrade of the standby FP, SPA and SIP software with the same version of software provisioned on the new active RP following the switchover, to prevent any reload when the standby RP takes over as the new active RP.
Adjusting Receive Window Size

When configuring L2TP HA Session SSO/ISSU on a LAC/LNS, Cisco IOS software internally adjusts the L2TP receive window size to a smaller value. This adjusted receive-window value displays when using the `show vpdn tunnel detail` command. If required, use the `l2tp tunnel resync` command to increase the size of the L2TP receive window.

How to Configure L2TP HA Session SSO ISSU on a LAC LNS

You can configure L2TP HA globally using the `l2tp sso enable` command. You can also configure L2TP HA sessions for a specific VPDN group by using the `sso enable` command in VPDN group configuration mode. Both global and VPDN group L2TP HA sessions are enabled, by default. You must configure both the `l2tp sso enable` command and the `sso enable` command for VPDN groups for protocol L2TP to execute L2TP HA session functionality.

Global and VPDN group-specific L2TP HA sessions are hidden from the output of the `show running-config` command, because they are enabled by default. If you use the `no l2tp sso enable` command, the HA commands will display as NVGEN and appear in the output of the `show running-config` command.

After an SSO switchover, L2TP HA sessions determines the sequence numbers used by L2TP peers. Determining sequence numbers can be time consuming if peers send a large number of unacknowledged messages. You can use the `l2tp tunnel resync` command to control the number of unacknowledged messages sent by a peer. Increasing the value of the number of packets can improve the session setup rate for L2TP HA tunnels with a large number of sessions.

Configuring SSO on a Route Processor

Cisco series Internet routers operate in SSO mode by default after reloading the same version of SSO-aware images on the device.

Before you can use SSO, use must enable SSO on an RP. This task explains how to use the `redundancy` command to enable SSO on an RP. This task ensures that all redundancy session data, following a SSO, is used to re-create and reestablishes existing sessions to their peer connections.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. redundancy
4. mode sso
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Global L2TP HA SSO Mode

Cisco series Internet routers operate in L2TP HA SSO mode by default after reloading the same version of SSO-aware images on the device. No configuration is necessary to enable L2TP HA SSO sessions.

This procedure shows how to use the `l2tp sso enable` command to enable or disable HA globally. The `l2tp sso enable` command is enabled by default.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `l2tp sso enable`
4. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>l2tp sso enable</td>
<td>Enables L2TP HA SSO.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# l2tp sso enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring VPDN Groups or VPDN Templates for L2TP HA SSO

Perform this task when configuring a VPDN group or a VPDN template for L2TP HA SSO. This configuration example provides recommended scaling parameters to use when the number of VPDN tunnels in use is high, such as 8000 tunnels, with each tunnel supporting only a few VPDN sessions (two or less).

Conversely, if the number of VPDN tunnels is low and the number of VPDN sessions per VPDN tunnel is high, use the `l2tp tunnel resync` command to increase the resynchronization value. For example, if the number of VPDN session per VPDN tunnel are in the hundreds, use the `l2tp tunnel resync` command to increase the resynchronization value to a matching value in the hundreds.

Beginning with Cisco IOS XE Release 2.3, you can set the retransmit retries and timeout values to default values.

For HA functionality for a VPDN group, both the `l2tp sso enable` and `sso enable` commands must be enabled (default). If either command is disabled, no HA functionality is available for the VPDN group.
SUMMARY STEPS

1. enable
2. configure terminal
3. l2tp sso enable
4. vpdn enable
5. vpdn-group name
6. sso enable
7. l2tp tunnel resync packets
8. l2tp tunnel retransmit retries number
9. l2tp tunnel retransmit timeout min seconds
10. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> l2tp sso enable</td>
<td>Enables L2TP SSO mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# l2tp sso enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vpdn enable</td>
<td>Enters VPDN configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# vpdn enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-vpdn)# vpdn-group example</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><em>sso enable</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# sso enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables L2TP SSO for the VPDN group.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><em>l2tp tunnel resync packets</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# l2tp tunnel resync 4</code></td>
</tr>
<tr>
<td></td>
<td>Configures the number of packets after an SSO, an L2TP HA tunnel sends before waiting for an acknowledgement.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><em>l2tp tunnel retransmit retries number</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# l2tp tunnel retransmit retries 30</code></td>
</tr>
<tr>
<td></td>
<td>Configures the number of retransmission attempts made for an L2TP control packet.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><em>l2tp tunnel retransmit timeout min seconds</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# l2tp tunnel retransmit timeout min 8</code></td>
</tr>
<tr>
<td></td>
<td>Configures the amount of time that the router waits before resending an L2TP control packet.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><em>exit</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-vpdn)# exit</code></td>
</tr>
<tr>
<td></td>
<td>Exits VPDN group configuration mode.</td>
</tr>
</tbody>
</table>

**Controlling Packet Resynchronization for L2TP HA**

After a SSO switchover, L2TP HA determines the sequence numbers used by L2TP peers. Determining sequence numbers can be time consuming, if peers send a large number of unacknowledged messages. You can use the `l2tp tunnel resync` command to control the number of unacknowledged messages sent by a peer. Increasing the value of the number of packets can improve the session setup rate for L2TP HA tunnels with a large number of sessions.

You can use the `show l2tp redundancy` command to display the time taken to resynchronize with the peer L2TP node.

This procedure shows how to use the `l2tp tunnel resync` command, in VPDN-group configuration mode, to control the number of packets a L2TP HA tunnel sends before waiting for an acknowledgement.
### SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn enable
4. vpdn-group name
5. l2tp tunnel resync packets
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
<td><code>Router&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>* Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> vpdn enable</td>
<td>Enters VPDN configuration mode.</td>
<td><code>Router(config)# vpdn enable</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> vpdn-group name</td>
<td>Creates a VPDN group and enters VPDN group configuration mode.</td>
<td><code>Router(config-vpdn)# vpdn-group example</code></td>
</tr>
<tr>
<td><strong>Step 5</strong> l2tp tunnel resync packets</td>
<td>Specifies the number of packets to be processed after an SSO before an acknowledgment message is sent.</td>
<td><code>Router(config-vpdn)# l2tp tunnel resync 250</code></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
<td><code>Router(config-vpdn)# end</code></td>
</tr>
</tbody>
</table>
Verifying the Checkpoint Status of L2TP HA Sessions

The `show l2tp redundancy` command provides information regarding the global state of the L2TP or specific L2TP sessions, with regard to their checkpointing status. You can display detailed information on:

- L2TP HA protocol state:
  - Standby readiness
  - Received message counter
  - Number of tunnels and sessions, compared to the number of HA-enabled tunnels and sessions
  - Number of tunnels that successfully resynchronized with the peer L2TP node after the last switchover, and the number that failed to resynchronize.

- L2TP control channel (tunnel) redundancy information:
  - Tunnel state
  - Local ID
  - Remote ID
  - Remote name
  - Class or group name
  - Number of sessions using this tunnel

- L2TP Session redundancy information:
  - Local session ID
  - Remote session ID
  - Tunnel ID
  - Status of assignment of logical tunnel and logical session handles

The L2TP HA protocol state information for tunnels configured for HA (HA-enabled) and HA tunnels established successfully (HA-established) should match on the active and standby RP, unless there is a failure.

The output of the `show l2tp redundancy` command on the standby RP does not display total counter values or values for L2TP resynchronized tunnels. Total counter values would include non-HA protected tunnels and sessions, and these are not present on the standby RP.

To display global L2TP or specific L2TP sessions having checkpoint status, follow this procedure.

**SUMMARY STEPS**

1. `enable`
2. `show l2tp redundancy` `[all | [detail] [id  local-tunnel-ID [local-session-ID]]]`
3. `exit`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>show l2tp redundancy [all] [detail] [id local-tunnel-ID [local-session-ID]]</code></td>
<td>Display the status of L2TP session with redundancy data.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show l2tp redundancy all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the Checkpoint Status of VPDN Sessions

#### SUMMARY STEPS

1. enable
2. `show vpdn redundancy [all] [detail] [id local-tunnel-ID [local-session-ID]]`
3. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>show vpdn redundancy [all] [detail] [id local-tunnel-ID [local-session-ID]]</code></td>
<td>Displays the status of VPDN session with checkpointed data.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show vpdn redundancy all</td>
<td></td>
</tr>
</tbody>
</table>
Table 12: Command or Action, Purpose

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Troubleshooting L2TP or VPDN Redundancy Sessions**

There is extensive troubleshooting for L2TP or VPDN redundancy sessions. For example, if the standby RP does not initialize, the **show l2tp redundancy** command displays a warning message and will display no tunnel or session information.

```
Router# show l2tp redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up: TRUE
  Recv'd Message Count: 0
No HA CC of Session data to display until Standby RP is up.
```

You can use the **debug l2tp redundancy** or **debug vpdn redundancy** commands to display debug information relating to L2TP- or VPDN-checkpointing events or errors. Debug information includes:

- **cf**—L2TP redundancy checkpointing-facility events (cf-events)
- **detail**—L2TP redundancy details
- **error**—L2TP redundancy errors
- **event**—L2TP redundancy events
- **fsm**—L2TP redundancy fsm-events
- **resync**—L2TP redundancy resynchronizations
- **rf**—L2TP redundancy-facility events (rf-events)

To debug an L2TP or VPDN session having redundancy event errors, follow this procedure.

**SUMMARY STEPS**

1.  **enable**
2.  **debug {l2tp | vpdn} redundancy {cf | detail | error | event | fsm | resync | rf}**
3.  **exit**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router> enable | |
| **Step 2** | debug {l2tp | vpdn} redundancy {cf | detail | error | event | fsm | resync | rf} | Displays debug information for VPDN session with redundancy data. |
| **Example:** | Router# debug vpdn redundancy cf | |
| **Step 3** | exit | Exits privileged EXEC mode. |
| **Example:** | Router# exit | |

---

**Configuring L2TP HA SSO ISSU on a RADIUS Server**

You can configure L2TP HA SSO/ISSU on a RADIUS server, using the following RADIUS attribute-value (AV) pair:

```
cisco:cisco-avpair="vpdn:l2tp-silent-switchover=1"
```

You can configure the L2TP HA SSO/ISSU resynchroneous parameter on a RADIUS server, using the following RADIUS AV pair:

```
cisco:cisco-avpair="vpdn:l2tp-tunnel-resync-packet=<num>"
```

---

**Configuration Examples for L2TP HA Session SSO ISSU on a LAC LNS**

**Example Configuring SSO on a Route Processor**

This example shows how to configure SSO on a route processor:

```
Router# configure terminal
Router(config)# redundancy
Router (config-red)# mode sso
Router (config-red)# end
```
**Example Configuring L2TP High Availability**

This example shows how to configure L2TP SSO:

```
Router# configure terminal
Router(config)# l2tp sso enable
Router (config-red)# end
```

**Examples Displaying L2TP Checkpoint Status**

**Example Displaying L2TP Redundancy Information**

The following example shows an L2TP redundancy information request:

```
Router# show l2tp redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up: TRUE
  Recv'd Message Count: 189
L2TP Tunnels: 2/2/2/0 (total/HA-enabled/HA-est/resync)
L2TP Sessions: 20/20/20 (total/HA-enabled/HA-est)
L2TP Resynced Tunnels: 2/0 (success/fail)
Resync duration 0.63 secs (complete)
```

**Example Displaying L2TP Redundancy Detail Information**

The following example shows an L2TP redundancy detail information request:

```
Router# show l2tp redundancy detail id 44233 2
Local session ID : 2
Remote session ID : 2
Local CC ID : 44233
Local UDP port : 1701
Remote UDP port : 1701
Waiting for VPDN application : No
Waiting for L2TP protocol : No
```

**Example Displaying All L2TP Redundancy Information**

The following example shows an L2TP redundancy all-information request:

```
Router# show l2tp redundancy all
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up: TRUE
  Recv'd Message Count: 0
L2TP Active Tunnels: 1/1/0 (total/HA-enabled/resync)
L2TP Active Sessions: 1/1 (total/HA-enabled)
L2TP Resynced Tunnels: 1/0 (success/fail)
L2TP HA CC Check Point Status:
  State LocID RemID Remote Name Class/Group Num. Sessions
  est 33003 26355 LAC-1 1 1
L2TP HA Session Status:
```
Example Displaying L2TP Redundancy ID Information

The following example shows how to limit the information displayed by providing a tunnel ID:

Router# show l2tp redundancy id 33003
L2TP HA Session Status:
LocID RemID TunID Waiting for Waiting for
VPDN app? L2TP proto?
2 2 33003 No No

Example Displaying L2TP Redundancy Detail ID Information

The following example shows how to limit the information displayed by providing a session ID:

Router# show l2tp redundancy detail id 33003 3
Local session ID : 3
Remote session ID : 3
Local CC ID : 33003
Local UDP port : 1701
Remote UDP port : 1701
Waiting for VPDN application : No
Waiting for L2TP protocol : No

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>Layer 2 Tunnel Protocol</td>
<td>Layer 2 Tunnel Protocol Technology Brief</td>
</tr>
<tr>
<td>Stateful switchover and high availability</td>
<td>Configuring Stateful Switchover module</td>
</tr>
<tr>
<td>VPDN technology overview</td>
<td>VPDN Technology Overview module</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2661</td>
<td>Layer 2 Tunneling Protocol (L2TP)</td>
</tr>
<tr>
<td>RFC 4591</td>
<td>Fail Over for Layer 2 Tunneling Protocol (L2TP)</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for L2TP HA Session SSO ISSU on a LAC LNS

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 . An account on Cisco.com is not required.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP HA Session SSO/ISSU on a LAC/LNS</td>
<td>Cisco IOS XE Release 2.2, Cisco IOS XE Release 2.3, Cisco IOS XE Release 2.4</td>
<td>Provides a generic SSO/ISSU mechanism for Layer 2 Tunneling Protocol (L2TP) on a LAC and a LNS. This feature was introduced on the Cisco ASR 1000 Series Routers. The following commands were introduced by this feature: <code>debug l2tp redundancy</code>, <code>debug vpdn redundancy</code>, <code>l2tp sso enable</code>, <code>l2tp tunnel resync</code>, <code>show l2tp redundancy</code>, <code>show vpdn redundancy</code>, <code>sso enable</code>. In 2.3, support was added for scaling parameters for VPDN groups and templates. In 2.4, support was added for support for Multihop VPDN for VPDN tunnels and sessions.</td>
</tr>
</tbody>
</table>
L2TP Disconnect Cause Information

The L2TP Disconnect Cause Information feature adds support for additional Layer 2 Tunnel Protocol (L2TP) disconnect error codes using attribute-value (AV) pair 46 as specified by RFC 3145. Prior to the introduction of this feature, L2TP hosts could not exchange PPP disconnect error codes.

- Finding Feature Information, page 223
- Restrictions for L2TP Disconnect Cause Information, page 223
- Information About L2TP Disconnect Cause Information, page 224
- Additional References, page 226
- Feature Information for L2TP Disconnect Cause Information, page 227

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 at the end of this module.

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.

Restrictions for L2TP Disconnect Cause Information

- This feature implements only error codes that are compliant with RFC 3145.
- If a router receives AV pair 46 with a nonsupported disconnect code it is mapped to code 0, indicating that no information is available.
Information About L2TP Disconnect Cause Information

How L2TP Disconnect Cause Information Works

L2TP disconnect cause codes allow the devices functioning as L2TP hosts to exchange PPP-related disconnect cause information. Normally L2TP operation is isolated from details of the PPP session that is being encapsulated. AV pair 46 PPP Disconnect Cause Code is used to exchange PPP-related disconnect cause information between L2TP hosts. The information can be translated to the appropriate authentication, authorization, and accounting (AAA) code and relayed to the remote RADIUS AAA server.

Benefits of L2TP Disconnect Cause Information

When L2TP service fails or session establishment is unsuccessful, PPP-specific disconnect information provides valuable information that can be used for troubleshooting or accounting purposes. The lack of this information is a problem particularly when the L2TP hosts are not owned or managed by the same entities. The L2TP Disconnect Cause Information feature enables service providers to determine the specific failure reason, facilitating analysis and error correction.

L2TP Disconnect Cause Information Codes

The table below lists the supported L2TP disconnect cause codes from RFC 3145 and a brief description of the codes.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Errors</td>
<td>No information available.</td>
</tr>
<tr>
<td>0</td>
<td>Administrative disconnect.</td>
</tr>
<tr>
<td>3</td>
<td>Normal disconnection, Link Control Protocol (LCP) Terminate-Request sent. Valid direction values are:</td>
</tr>
<tr>
<td></td>
<td>• 1--LCP Terminate-Request sent by the peer device.</td>
</tr>
<tr>
<td></td>
<td>• 2--LCP Terminate-Request sent by the local device.</td>
</tr>
</tbody>
</table>

Note: If a router receives AV pair 46 with a nonsupported disconnect code, possibly from another vendor or a newer version of Cisco software, it is mapped to this code.
### LCP Errors

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Finite State Machine (FSM) timeout error.</td>
</tr>
<tr>
<td>6</td>
<td>No recognizable LCP packets were received.</td>
</tr>
<tr>
<td>8</td>
<td>LCP link failure: Echo Request timeout.</td>
</tr>
<tr>
<td>9</td>
<td>The peer has an unexpected endpoint-discriminator for an existing Multilink PPP (MLP) bundle.</td>
</tr>
</tbody>
</table>
| 12   | Compulsory call-back required by a PPP peer was refused by the peer. Valid direction values are:  
- 1--Required by the local device; refused by the peer device.  
- 2--Required by the peer device; refused by the local device. |

### Authentication Errors

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>FSM timeout error.</td>
</tr>
</tbody>
</table>
| 16   | PPP authentication failed due to a bad hostname, password, or secret. Valid direction values are:  
- 1--Authentication of the peer’s identity by the local system failed.  
- 2--Authentication of the local identity by the peer system failed. |

### Network Control Protocol (NCP) Errors

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>FSM timeout error.</td>
</tr>
<tr>
<td>18</td>
<td>No NCPs available (all disabled or rejected) or no NCPs went to Opened state. The Control Protocol Number can be zero only if neither peer has enabled NCPs.</td>
</tr>
</tbody>
</table>
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Information about configuring L2TP VPDN tunnels</td>
<td>VPDN Tunnel Management module</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3145</td>
<td>L2TP Disconnect Cause Information</td>
</tr>
</tbody>
</table>
Feature Information for L2TP Disconnect Cause Information

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 . An account on Cisco.com is not required.

Table 16: Feature Information for the L2TP Disconnect Cause Information Feature

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP Disconnect Cause Information</td>
<td>Cisco IOS XE Release 2.1</td>
<td>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The L2TP Disconnect Cause Information feature adds support for additional Layer 2 Tunnel Protocol (L2TP) disconnect error codes using attribute-value (AV) pair 46 as specified by RFC 3145. Prior to the introduction of this feature, L2TP hosts could not exchange PPP disconnect error codes. No commands were introduced or modified by this feature.</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuring the Managed IPv6 Layer 2 Tunnel Protocol Network Server

This document describes how to enable the Managed IPv6 Layer 2 Tunnel Protocol Network Server feature.

- Finding Feature Information, page 229
- Prerequisites for Configuring the Managed IPv6 LNS, page 229
- Information About Configuring the Managed IPv6 LNS, page 230
- How to Configure the Managed LNS, page 232
- Configuration Examples for the Managed IPv6 Layer 2 Tunnel Protocol Network Server, page 250
- Additional References, page 256
- Feature Information for Configuring Managed IPv6 Layer 2 Tunnel Protocol Network Server, page 257

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 at the end of this module.

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.

Prerequisites for Configuring the Managed IPv6 LNS

For the router to function as an LNS, you must enable Authentication, Authorization, and Accounting (AAA) on the Layer 2 Tunnel Protocol Network Server (LNS) and the Layer 2 Access Concentrator (LAC), by entering the aaa-new-model global configuration command. For more information, see the “Authentication, Authorization, and Accounting” chapter in the Cisco IOS XE Security: Securing User Services Configuration Guide.
Information About Configuring the Managed IPv6 LNS

L2TP Network Server

The router can function as an LNS. The LNS is a peer to the LAC and sits on one side of an L2TP tunnel. The LNS routes packets to and from the LAC and a destination network. When the router functions as an LNS, you can configure the router to terminate the PPP sessions and route the client IP packets onto the ISP or corporate network toward their final destination (see the figure below). The router can use the Managed IPv6 LNS feature to terminate L2TP sessions from the LAC and place each session into the appropriate IPv6 VRF instance based on the VRF applied to the virtual template interface or alternatively, based on the VRF received for the user through AAA. The router then routes each session within the VRF to the destination network.

Figure 10: Terminating and Forwarding Sessions from the LAC

Tunnel Accounting

The tunnel accounting feature enhances AAA accounting by adding the ability to include tunnel-related statistics in the RADIUS information. Before you can collect tunnel usage information, you must configure the following attributes on the RADIUS server:

- Acct-Tunnel-Connection—Specifies the identifier assigned to the tunnel session. This attribute and the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes provide a way to uniquely identify a tunnel session for auditing purposes.

- Acct-Tunnel-Packets-Lost—Specifies the number of packets lost on a given link.

The table below describes the values for the Acct-Status-Type attribute that support tunnel accounting on the RADIUS server.
Table 17: Acct-Status-Type Values for RADIUS Tunnel Accounting

<table>
<thead>
<tr>
<th>Acct-Status-Type Values</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-Link-Reject</td>
<td>14</td>
<td>Marks the rejection of the establishment of a new link in an existing tunnel.</td>
</tr>
<tr>
<td>Tunnel-Link-Start</td>
<td>12</td>
<td>Marks the creation of a tunnel link within an L2TP tunnel that carries multiple links.</td>
</tr>
<tr>
<td>Tunnel-Link-Stop</td>
<td>13</td>
<td>Marks the destruction of a tunnel link within an L2TP tunnel that carries multiple links.</td>
</tr>
<tr>
<td>Tunnel-Reject</td>
<td>11</td>
<td>Marks the rejection of the establishment of a tunnel with another device.</td>
</tr>
<tr>
<td>Tunnel-Start</td>
<td>9</td>
<td>Marks the establishment of a tunnel with another device.</td>
</tr>
<tr>
<td>Tunnel-Stop</td>
<td>10</td>
<td>Marks the destruction of a tunnel to or from another device.</td>
</tr>
</tbody>
</table>

For more information about the RADIUS tunnel accounting attributes or the Acct-Status-Type values that support RADIUS tunnel accounting, see RFC 2867, RADIUS Accounting Modifications for Tunnel Protocol Support.

For information about RADIUS accounting attributes supported on the Cisco ASR 1000 Series Aggregation Services Routers, see the "RADIUS Attributes" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.

For more information on configuring RADIUS, see your RADIUS user documentation.
# How to Configure the Managed LNS

## Configuring a VRF on the LNS

### SUMMARY STEPS

1. `enable`  
2. `configure terminal`  
3. `vrf definition vrf-name`  
4. `rd route-distinguisher`  
5. `address-family {ipv4|ipv6}`  
6. `route-target {import|export|both} route-target-ext-community`  
7. `exit-address-family`  
8. `address-family {ipv4|ipv6}`  
9. `route-target {import|export|both} route-target-ext-community`  
10. `end`  
11. `show ipv6 route vrf vrf-name`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enters privileged EXEC mode.  
**Example:**  
Router> enable |
| **Step 2** | configure terminal | Enters global configuration mode.  
**Example:**  
Router# configure terminal |
| **Step 3** | vrf definition vrf-name | Configures a VRF routing table and enters VRF configuration mode.  
**Example:**  
Router(config)# vrf definition vrf1  
- The `vrf-name` argument is the name of the VRF |
| **Step 4** | rd route-distinguisher | Creates routing and forwarding tables for a VRF.  
**Example:**  
Router(config-vrf)# rd 100:1  
- The `route-distinguisher` argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 16-bit autonomous system number (ASN): your 32-bit number For example, 101:3.</td>
<td></td>
</tr>
<tr>
<td>• 32-bit IP address: your 16-bit number For example, 192.168.122.15:1.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5** address-family \{ipv4|ipv6\}

Example:

```
Router(config-vrf) address-family ipv6
```

Enters VRF address family configuration mode to specify an address family for a VRF.

- The `ipv4` keyword specifies an IPv4 address family for a VRF.
- The `ipv6` keyword specifies an IPv6 address family for a VRF.

**Step 6** route-target \{import|export|both\}

Example:

```
Router(config-vrf-af) route-target both 100:2
```

Creates a route-target extended community for a VRF.

- The `import` keyword imports routing information from the target VPN extended community.
- The `export` keyword exports routing information to the target VPN extended community.
- The `both` keyword imports both import and export routing information to the target VPN extended community.
- The `route-target-ext-community` argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.

**Step 7** exit-address-family

Example:

```
Router(config-vrf-af)# exit-address-family
```

Exits VRF address family configuration mode and enters VRF configuration mode.

**Step 8** address-family \{ipv4|ipv6\}

Example:

```
Router(config-vrf) address-family ipv6
```

Enters VRF address family configuration mode to specify an address family for a VRF.

- The `ipv4` keyword specifies an IPv4 address family for a VRF.
- The `ipv6` keyword specifies an IPv6 address family for a VRF.

**Step 9** route-target \{import|export|both\}

Example:

```
Router(config-vrf-af)# route-target both 100:3
```

Creates a route-target extended community for a VRF.

- The `import` keyword specifies to import routing information from the target VPN extended community.
- The `export` keyword specifies to export routing information to the target VPN extended community.
- The `both` keyword specifies to import both import and export routing information to the target VPN extended community.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The <code>route-target-ext-community</code> argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.</td>
<td></td>
</tr>
<tr>
<td>• Enter the <code>route-target</code> command one time for each target community.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 10

**end**

**Example:**

```
Router(config-vrf-af)# end
```

Exits VRF address family configuration mode and returns to privileged EXEC mode.

**Step 11**

**show ipv6 route vrf vrf-name**

**Example:**

```
Router# show ipv6 route vrf vrf1
```

Displays the IPv6 routing table associated with a VRF.

### Configuring a Virtual Template Interface

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface virtual-template number`
4. `vrf forwarding name`
5. `ppp authentication chap`
6. `end`
7. `show interfaces virtual-access number [configuration]`
8. `debug ppp chap`
9. `debug ppp negotiation`
10. `debug ppp negotiation chap`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`
| **Example:**
<p>| <code>Router&gt; enable</code> |
| Enters privileged EXEC mode. |</p>
<table>
<thead>
<tr>
<th>Step 2</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>interface virtual-template number</code></td>
<td>Creates a virtual template interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# interface virtual-template 1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>vrf forwarding name</code></td>
<td>(Optional) Maps the virtual template interface to a VRF routing table.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# vrf forwarding vpn-1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>If the VRF assignment is received via the RADIUS server, then this step is not required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ppp authentication chap</code></td>
<td>Enables CHAP authentication on the virtual template interface, which is applied to virtual access interfaces (VAI).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# ppp authentication chap</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show interfaces virtual-access number [configuration]</code></td>
<td>Displays status, traffic data, and configuration information about the VAI you specify.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# show interfaces virtual-access number [configuration]</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>debug ppp chap</code></td>
<td>Displays authentication protocol messages for Challenge Authentication Protocol (CHAP) packet exchanges.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# debug ppp chap</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>This command is useful when a CHAP authentication failure occurs due to a configuration mismatch between devices. Verifying and correcting any username and password mismatch resolves the problem.</td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 9</th>
<th>debug ppp negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug ppp negotiation</td>
</tr>
</tbody>
</table>

#### Command or Action

<table>
<thead>
<tr>
<th>Step 10</th>
<th>debug ppp negotiation chap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug ppp negotiation chap</td>
</tr>
</tbody>
</table>

### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 9</th>
<th>debug ppp negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug ppp negotiation</td>
</tr>
</tbody>
</table>

#### Command or Action

<table>
<thead>
<tr>
<th>Step 10</th>
<th>debug ppp negotiation chap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# debug ppp negotiation chap</td>
</tr>
</tbody>
</table>

### Assigning a VRF via the RADIUS Server

#### SUMMARY STEPS

1. enable
2. configure terminal
3. aaa authorization configuration method-name group group-name
4. ipv6 dhcp pool pool-name
5. prefix-delegation aaa [method-list method-list]
6. dns-server ipv6-address
7. exit
8. interface virtual-template number
9. ipv6 nd prefix framed-ipv6-prefix
10. ipv6 dhcp server pool-name rapid-commit
11. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Downloads configuration information from the AAA server using RADIUS.</td>
</tr>
<tr>
<td><code>aaa authorization configuration method-name</code>&lt;br&gt;<code>group group-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa authorization configuration&lt;br&gt;DHCPv6-PD group DHCPv6-PD-RADIUS</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.</td>
</tr>
<tr>
<td><code>ipv6 dhcp pool pool-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ipv6 dhcp pool DHCPv6-PD</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies that prefixes are to be acquired from AAA servers.</td>
</tr>
<tr>
<td><code>prefix-delegation aaa [method-list method-list]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcpv6)# prefix-delegation aaa&lt;br&gt;method-list DHCPv6-PD</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the Domain Name System (DNS) IPv6 servers available to a DHCP for IPv6 client.</td>
</tr>
<tr>
<td><code>dns-server ipv6-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcpv6)# dns-server&lt;br&gt;2001:0DB8:3000:3000::42</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exits DHCP for IPv6 pool configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcpv6)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Creates a virtual template interface that can be configured and applied dynamically in creating VAls, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface virtual-template number</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface virtual-template 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue.</td>
</tr>
<tr>
<td><code>ipv6 nd prefix framed-ipv6-prefix</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ipv6 nd prefix&lt;br&gt;framed-ipv6-prefix</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the LNS to Initiate and Receive L2TP Traffic

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vpdn enable`
4. `vpdn-group group-name`
5. `accept-dialin`
6. `protocol 12tp`
7. `virtual-template template-number`
8. `exit`
9. `terminate-from hostname hostname`
10. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>vpdn enable</td>
<td>Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway) if one is present.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn enable</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>vpdn-group group-name</td>
<td>Defines a local group name for which you can assign other VPDN variables.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# vpdn-group group1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>accept-dialin</td>
<td>Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn)# accept-dialin</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>protocol 12tp</td>
<td>Specifies the Layer 2 Tunnel Protocol.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn-acc-in)# protocol 12tp</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>virtual-template template-number</td>
<td>Specifies the virtual template to be used to clone VAIs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn-acc-in)# virtual-template 1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Returns to VPDN group configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn-acc-in)# exit</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>terminate-from hostname hostname</td>
<td>Specifies the hostname of the remote LAC that is required when accepting a VPDN tunnel.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn)# terminate-from hostname lac1-vpn1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>end</td>
<td>Exits VPDN configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-vpdn)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Limiting the Number of Sessions per Tunnel

### SUMMARY STEPS

1. `enable`  
2. `configure terminal`  
3. `vpdn-group group-name`  
4. `accept-dialin`  
5. `protocol 12tp`  
6. `virtual-template template-number`  
7. `exit`  
8. `terminate-from hostname host-name`  
9. `session-limit limit-number`  
10. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>vpdn-group group-name</td>
<td>Defines a local group name for which you can assign other VPDN variables.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# vpdn-group group1</td>
<td>• Enters VPDN group configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>accept-dialin</td>
<td>Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-vpdn)# accept-dialin</td>
<td>• Enters accept dial-in VPDN subgroup configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>protocol 12tp</td>
<td>Specifies the Layer 2 Tunnel Protocol.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-vpdn-acc-in)# protocol 12tp</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>specifies the virtual template to be used to clone VAIs.</td>
<td></td>
</tr>
<tr>
<td>virtual-template template-number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn-acc-in)# virtual-template 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>returns to VPDN group configuration mode.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn-acc-in)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>specifies the hostname of the remote LAC that is required when accepting a VPDN tunnel.</td>
<td></td>
</tr>
<tr>
<td>terminate-from hostname host-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# terminate-from hostname test_LAC</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>specifies the maximum number of sessions per tunnel.</td>
<td></td>
</tr>
<tr>
<td>session-limit limit-number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# session-limit 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>exits VPDN configuration mode and returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-vpdn)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS Attribute Accept or Reject Lists

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa authentication ppp default group group-name
4. aaa authorization network group group group-name
5. aaa group server radius group-name
6. server-private ip-address [acct-port port-number] [timeout seconds] [retransmit retries] [keystring]
7. authorization [accept|reject] list-name
8. exit
9. radius-server attribute list listname
10. attribute value1 [value2 [value3...]]
11. end
12. show accounting

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authentication ppp default group group-name</td>
<td>Specifies one or more AAA authentication methods for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# aaa authentication ppp default group radius_authen1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>aaa authorization network group group group-name</td>
<td>Sets the parameters that restrict network access to the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# aaa authorization network group group radius_authen1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>aaa group server radius group-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# aaa group server radius VPDN-Group</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods and enters server group RADIUS configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>server-private ip-address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-sg-radius)# server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <em>ip-address</em> argument specifies the IP address of the private RADIUS server host.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) The <em>port-number</em> argument specifies the UDP destination port for accounting requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) The <em>seconds</em> argument specifies the timeout value (1 to 1000).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) The <em>retries</em> argument specifies the number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <em>string</em> argument specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**authorization [accept</td>
<td>reject] list-name**</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-sg-radius)# authorization accept vpn1-autho-list</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <em>accept</em> keyword indicates that all attributes will be rejected except the attributes specified in the <em>listname</em> argument.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <em>reject</em> keyword indicates that all attributes will be accepted except for the attributes specified in the <em>listname</em> argument and all standard attributes.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>exit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-sg-radius)# exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exits server group RADIUS configuration mode and enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>radius-server attribute list listname</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# radius-server attribute list vpn1-autho-list</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defines the list name given to the set of attributes defined using the <em>attribute</em> command and enters RADIUS attribute list configuration mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Define the <em>listname</em> argument to be the same as you defined it in step 7.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>attribute value1 [value2 [value3...]]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adds attributes to the configured accept or reject list.</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Example: Router(config-radius-attrl)# attribute 26,200 | • You can use this command multiple times to add attributes to an accept or reject list.

**Step 11**

end | Exits RADIUS attribute list configuration mode and returns to privileged EXEC mode.

**Example:**

Router(config-radius-attrl)# end

**Step 12**

show accounting | Displays accounting records for users currently logged in.

**Example:**

Router# show accounting

- Displays active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

---

### Configuring AAA Accounting Using Named Method Lists

**Note**

System accounting does not use named method lists. For system accounting you can define only the default method list. For more information, see the “Configuring Accounting” chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.

---

### SUMMARY STEPS

1. enable
2. configure terminal
3. aaa accounting network list-name start-stop group radius
4. line [aux | console | vty] [line-number]
5. accounting {arap|commands|level|connection|exec|resource} [default | list-name]
6. end
7. debug aaa accounting
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;aaa accounting network list-name start-stop group radius</td>
<td>Creates an accounting method list and enables accounting.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# aaa accounting network methodlist start-stop group radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;line [aux</td>
<td>console</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;accounting {arap</td>
<td>commands</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-line)# accounting commands 15 list1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;end</td>
<td>Exits line configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-line)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong>&lt;br&gt;debug aaa accounting</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router# debug aaa accounting</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS Tunnel Authentication Method Lists on the LNS

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa authorization network list-name method1 [method2...]
4. vpdn tunnel authorization network list-name method1 [method2...]
5. vpdn tunnel authorization virtual-template vtemplate-number
6. vpdn tunnel authorization password dummy-password
7. debug aaa authorization

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authorization network list-name method1 [method2...]</td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# aaa authorization network mymethodlist group VPDN-Group</td>
<td></td>
</tr>
</tbody>
</table>

- The list-name argument is a character string used to name the list of authentication methods tried when a user logs in.
- group radius: Uses the list of all RADIUS servers for authentication.
- group group-name: Uses a subset of RADIUS servers for authentication as defined by the aaa group server radius command.
- if-authenticated: Succeeds if user has been successfully authenticated.
- local: Uses the local username database for authentication.
- none: Uses no authentication.

**Note** The method list is only for VPDN tunnel authorization and termination, not for domain and Digital Number Identification Service (DNIS) authorization. Therefore, the method list applies only on the tunnel terminator device - the LAC for dialout sessions and the LNS for dialin sessions.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 4    | vpdn tunnel authorization network lmethod-list-name method1 [method2...] | Specifies the AAA method list to use for VPDN remote tunnel hostname-based authorization.  
   • If you do not specify a method list (including a default method list) by using the `vpdn tunnel authorization network` command, local authorization occurs by using the local VPDN group configuration. |
|      | Example:         |         |
|      | Router(config)# vpdn tunnel authorization network mymethodlist |         |
| 5    | vpdn tunnel authorization virtual-template vtemplate-number | Specifies the default virtual template interface used to clone a VAI.  
   • If you do not specify a virtual template interface in the local VPDN group configuration or in a remote RADIUS configuration, then the default virtual template interface is used. |
|      | Example:         |         |
|      | Router(config)# vpdn tunnel authorization virtual-template 10 |         |
| 6    | vpdn tunnel authorization password dummy-password | Specifies the password to use for the RADIUS authorization request to retrieve the tunnel configuration based on the remote tunnel hostname. |
|      | Example:         |         |
|      | Router(config)# vpdn tunnel authorization password mypassword |         |
| 7    | debug aaa authorization | Displays information on AAA authorization. |
|      | Example:         |         |
|      | Router# debug aaa authorization |         |

### Configuring the LNS for RADIUS Tunnel Authentication

Perform the following tasks to configure LNS for RADIUS Tunnel Authentication:

- **Note**
  Cisco ASR 1000 Series Aggregation Services Routers supports L2TP tunnel authorization. However, RADIUS does not provide attributes for such parameter values as L2TP tunnel timeouts, L2TP tunnel hello intervals, and L2TP tunnel receive window size. When the Cisco ASR 1000 Series Aggregation Services Router does not receive a RADIUS attribute for a parameter, the router uses the default value.

### Configuring RADIUS Tunnel Authentication Method Lists on the LNS

To configure method lists on the LNS for RADIUS tunnel authentication, perform the following task.
## SUMMARY STEPS

1. enable  
2. configure terminal  
3. aaa authorization network list-name method1 [method2...]  
4. vpdn tunnel authorization network method-list-name  
5. vpdn tunnel authorization virtual-template vtemplate-number  
6. vpdn tunnel authorization password dummy-password  
7. end  
8. debug aaa authorization

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa authorization network list-name method1 [method2...]</td>
<td>Sets parameters that restrict user access to a network</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# aaa authorization network mymethodlist group VPDN-Group</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The method list is only for VPDN tunnel authorization and termination, not for domain and Digital Number Identification Service (DNIS) authorization. Therefore, the method list applies only on the tunnel terminator device—the LAC for dialout sessions and the LNS for dialin sessions.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The list-name argument is a character string used to name the list of authentication methods tried when a user logs in.</td>
<td></td>
</tr>
<tr>
<td>• groupradius—Uses the list of all RADIUS servers for authentication.</td>
<td></td>
</tr>
<tr>
<td>• groupgroup-name—Uses a subset of RADIUS servers for authentication as defined by the aaagroupserverradius command.</td>
<td></td>
</tr>
<tr>
<td>• if-authenticated—Succeeds if user has been successfully authenticated.</td>
<td></td>
</tr>
<tr>
<td>• local—Uses the local username database for authentication.</td>
<td></td>
</tr>
<tr>
<td>• none—Uses no authentication.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 4** vpdn tunnel authorization network method-list-name | Specifies the AAA method list to use for VPDN remote tunnel hostname-based authorization.  
  - If you do not specify a method list (including a default method list) by using the `vpdntunnelauthorizationnetwork` command, local authorization occurs by using the local VPDN group configuration. |
| Example: Router(config)# vpdn tunnel authorization network mymethodlist | |
| **Step 5** vpdn tunnel authorization virtual-template vtemplate-number | Specifies the default virtual template interface used to clone a VAI.  
  - If you do not specify a virtual template interface in the local VPDN group configuration or in a remote RADIUS configuration, then the default virtual template interface is used. |
| Example: Router(config)# vpdn tunnel authorization virtual-template 10 | **Note** The `vpdntunnelauthorizationvirtual-template` command is applicable only on the LNS. |
| **Step 6** vpdn tunnel authorization password dummy-password | Specifies the password to use for the RADIUS authorization request to retrieve the tunnel configuration based on the remote tunnel hostname.  
  - By default, the password is cisco, but you can configure a different password. |
| Example: Router(config)# vpdn tunnel authorization password mypassword | **Note** The `vpdntunnelauthorizationpassword` command is applicable on both the LAC and LNS. |
| **Step 7** end | Exits global configuration mode and returns to privileged EXEC mode. |
| Example: Router(config)# end | |
| **Step 8** debug aaa authorization | Displays information on AAA authorization. |
| Example: Router# debug aaa authorization | |
Configuring AAA Authentication Methods

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
5. aaa authentication
6. Apply the authentication method lists to an interface, a line, or a set of lines as required. For more information about authentication method lists, see the "Configuring Authentication" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.
7. end

DETAILED STEPS

Step 1 enable
Step 2 configure terminal
Step 3 aaa new-model
Enter this command in global configuration mode to enable AAA.
Step 4 Configure RADIUS security protocol parameters. For more information about RADIUS, see the "Configuring RADIUS" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.
Step 5 aaa authentication
Enter this command to define the authentication method lists.
Step 6 Apply the authentication method lists to an interface, a line, or a set of lines as required. For more information about authentication method lists, see the "Configuring Authentication" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.
Step 7 end

Configuration Examples for the Managed IPv6 Layer 2 Tunnel Protocol Network Server

Example Managed IPv6 LNS Configuration

The following example shows how to configure Managed IPv6 LNS features on the router. In this example, the router terminates the tunnel from the LAC and associates the VRFs with the interfaces and the virtual
template interfaces. This configuration also shows how to configure RADIUS attribute screening and AAA accounting for the VRFs.

! vrf definition Mgmt-intf
! address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!

vrf definition user_vrf1
rd 1:1
route-target export 1:1
route-target import 1:1
!
address-family ipv6
exit-address-family
!
logging buffered 10000000
enable password lab
!

aaa new-model
!

aaa group server radius radius_authen1
server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1
ip radius source-interface Loopback20000
!

aaa authentication login default none
aaa authentication ppp default group radius_authen1
aaa authorization network default group radius_authen1
aaa authorization configuration DHCPv6-PD group radius_authen1
!

aaa session-id common
aaa policy interface-config allow-subinterface
ppp hold-queue 80000
! clock timezone EST -5 0
ip source-route
no ip gratuitous-arps
!

! no ip domain lookup
ip host mcp-matrix 10.0.0.2
ip host mcp-sun-2 10.0.0.2
!
ipv6 unicast-routing
ipv6 dhcp binding track ppp
ipv6 dhcp pool ipv6_dhcp_pool1
prefix-delegation aaa method-list DHCPv6-PD
!
!

! multilink bundle-name authenticated
vpdn enable
!

vpdn-group VPDN_LNS1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname test_LAC1
source-ip 10.0.0.2
local name test_LNS1
l2tp tunnel password 0 tunnel1
l2tp tunnel receive-window 100
l2tp tunnel timeout no-session 30
l2tp tunnel retransmit retries 7
l2tp tunnel retransmit timeout min 2
no virtual-template snmp

username asifp1@test1 password 0 hello1
redundancy
notification-timer 30000
mode none

ip tftp source-interface GigabitEthernet 0

interface Loopback1
no ip address
interface Loopback20000
ip address 209.165.202.131 255.255.255.224
interface GigabitEthernet1/1/0
mac-address 8888.8888.8888
no ip address
load-interval 30
negotiation auto
hold-queue 4096 in
hold-queue 4096 out
interface GigabitEthernet1/1/0.1
encapsulation dot1Q 3
ip address 209.165.202.132 255.255.255.224
interface GigabitEthernet1/1/1
mac-address 4444.4444.4444
no ip address
load-interval 30
no negotiation auto
hold-queue 4096 in
hold-queue 4096 out
interface GigabitEthernet1/1/1.1
vrf forwarding user_vrf1
encapsulation dot1Q 2
ipv6 address 12::1/72
interface GigabitEthernet1/1/2
no ip address
negotiation auto
!
interface GigabitEthernet1/1/3
no ip address
negotiation auto
!
interface GigabitEthernet1/1/4
no ip address
negotiation auto
!
interface GigabitEthernet1/1/5
no ip address
negotiation auto
!
interface GigabitEthernet1/1/6
no ip address
negotiation auto
!
interface GigabitEthernet1/1/7
description Connected to RADIUS
ip address 209.165.201.1 255.255.255.224
negotiation auto
!
interface GigabitEthernet1/3/0
no ip address
media-type sfp
negotiation auto
!
interface GigabitEthernet1/3/1
no ip address
media-type sfp
negotiation auto
!
interface GigabitEthernet 0
vrf forwarding Mgmt-intf
ip address 209.165.201.1 255.255.255.224
negotiation auto
!
interface Virtual-Template 1
no ip address
no logging event link-status
ipv6 dhcp server ipv6_dhcp_pool1 rapid-commit
keepalive 30
ppp mtu adaptive
ppp authentication pap
!
ip default-gateway 10.1.0.5
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 209.165.201.1 255.255.255.254 172.16.1.1
ip route vrf Mgmt-intf 209.165.201.29 255.255.255.224 172.16.0.1
!
ip radius source-interface GigabitEthernet1/1/7
logging esm config
cdp run
ipv6 route vrf user_vrf1 ::/0 12::2
!
ipv6 neighbor 12::2 GigabitEthernet1/1.1 2222.2222.2222
!
!
control-plane
!
call admission limit 90
!
!
alias exec call show caller summ
alias exec caller show caller summ
alias exec palt show plat
Example LNS Tunnel Accounting Configuration

The following example shows how to configure the LNS to send tunnel accounting records to the RADIUS server:

```
aaa new-model
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnellpass
username user1@example.com password 0 lab
username user2@example.com password 0 lab
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
  firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname ISP_LAC
  local name ENT_LNS
  !
  isdn switch-type primary-5ess
  !
  fax interface-type modem
  mta receive maximum-recipients 0
  !
  interface Loopback 0
  ip address 172.16.0.101 255.255.255.0
  !
  interface Loopback 1
  ip address 192.168.0.101 255.255.255.0
  !
  interface Ethernet 0
  ip address 10.1.26.71 255.255.255.0
  no ip mrout-cache
```
no cdp enable
!
interface virtual-template 1
ip unnumbered Loopback 0
peer default ip address pool vpdn-pool1
ppp authentication chap
!
interface virtual-template 2
ip unnumbered Loopback1
peer default ip address pool vpdn-pool2
ppp authentication chap
!
interface fastethernet 0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip local pool vpdn-pool1 172.16.5.1 172.16.128.100
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 192.168.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
end

For additional accounting examples, see the "Configuring Accounting" chapter in the Cisco IOS XE Security: Secure Services Configuration Guide.

---

Example Verifying the User Profile on the RADIUS Server

The following is an example user profile on the RADIUS server. The Cisco ASR 1000 Series Aggregation Services Routers retrieves the information in the user profile from the RADIUS server.

Radius Profile "user1"
Auth-Type = Local, User-Password = "pwd"
User-Service-Type = Framed-User
Framed-Protocol = PPP
cisco-avpair = "lcp:interface-config-vrf forwarding VRF01"
cisco-avpair = "lcp:interface-config-ipv6 unnumbered loopback1"
Framed-IPv6-Prefix = "2001:DB8:4567:1234::/64"
Delegated-IPv6-Prefix = "2001:DB8:AAAA::/48"
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS XE MPLS commands</td>
<td>Cisco IOS MPLS Command Reference</td>
</tr>
<tr>
<td>Authentication, authorization and accounting</td>
<td>Authentication, Authorization, and Accounting (AAA)</td>
</tr>
<tr>
<td>Configuring RADIUS</td>
<td>Configuring RADIUS</td>
</tr>
<tr>
<td>Configuring accounting</td>
<td>Configuring Accounting</td>
</tr>
<tr>
<td>RADIUS attributes</td>
<td>&quot;RADIUS Attributes Overview and RADIUS IETF Attributes&quot; module in the Cisco IOS XE Security Configuration Guide: Securing User Services</td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported, and support for existing standards has not been modified.</td>
<td>—</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported, and support for existing MIBs has not been modified.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2867</td>
<td>RADIUS Accounting Modifications for Tunnel Protocol Support</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for Configuring Managed IPv6 Layer 2 Tunnel Protocol Network Server

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 . An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Information for Managed IPv6 Layer 2 Tunnel Protocol Network Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Name</td>
</tr>
<tr>
<td>Managed IPv6 Layer 2 Tunnel Protocol Network Server</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managed IPv6 Layer 2 Tunnel Protocol Network Server - VRF-Lite only</td>
</tr>
<tr>
<td>Managed IPv6 Layer 2 Tunnel Protocol Network Server - MPLS VPN</td>
</tr>
</tbody>
</table>
ISDN/Dialer Access-Link Support for Broadband Aggregation

The ISDN/Dialer Access-Link Support for Broadband Aggregation feature provides client connectivity to a network through PPP connections by using an ISDN PRI Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) session over IPv4.

This module describes how to configure the ISDN and dialer access-link support for broadband aggregation.

- Finding Feature Information, page 259
- Prerequisites for ISDN/Dialer Access-Link Support for Broadband Aggregation, page 260
- Restrictions for ISDN/Dialer Access-Link Support for Broadband Aggregation, page 260
- Information About ISDN/Dialer Access-Link Support for Broadband Aggregation, page 260
- How to Configure ISDN/Dialer Access-Link Support for Broadband Aggregation, page 261
- Verifying ISDN/Dialer Access-Link Support for Broadband Aggregation, page 270
- Configuration Examples for ISDN/Dialer Access-Link Support for Broadband Aggregation, page 271
- Additional References, page 272
- Feature Information for ISDN/Dialer Access-Link Support for Broadband Aggregation, page 273

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 at the end of this module.

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.
Prerequisites for ISDN/Dialer Access-Link Support for Broadband Aggregation

- You must configure a Layer 2 Tunneling Protocol (L2TP) network server (LNS) and enable IPv4 before configuring ISDN support for broadband.
- Ensure that the ISDN/Dialer Access-Link Support for Broadband Aggregation feature installs correctly by enabling the activation of the `adventerprise` license upon the next reload.

```
enable
configure terminal
license boot level adventerprise
end
```

Restrictions for ISDN/Dialer Access-Link Support for Broadband Aggregation

- Only IPv4 PPP sessions inside Layer 2 Tunneling Protocol (L2TP) version 2 tunnels are supported.
- ISDN termination is not supported on the dialer interface or on the d-channel interface. To achieve PPP termination and aggregation (PTA), the router will need to act as a L2TP Access Concentrator (LAC) and forward incoming ISDN calls to a L2TP Network Server (LNS).

Information About ISDN/Dialer Access-Link Support for Broadband Aggregation

Deployment Model for ISDN/Dialer Access-Link Support for Broadband Aggregation

The ISDN/Dialer Access-Link Support for Broadband Aggregation feature provides support for ISDN and dialer PRI access link to broadband PPP IPv4 sessions at the Layer 2 Tunneling Protocol (L2TP) network server (LNS). These sessions are carried over PPP by the L2TP access concentrator (LAC) using ISDN over IPv4. The sessions are sent from the LAC to the LNS through L2TP tunnels. The LNS terminates the PPP sessions and assigns a network layer address to the client. The client data in the IPv4 packet is then routed to the ISP or a corporate network and forwarded to the final destination. The LNS also performs authentication,
authorization, and accounting (AAA) actions on the PPP sessions. The figure below describes the deployment model.

*Figure 11: Topology Diagram*

```
CPE          LAC           LNS
PRI          L2TP tunnel   
PPP session
```

**How to Configure ISDN/Dialer Access-Link Support for Broadband Aggregation**

*Note* Before you can configure the ISDN switch type on an interface, you must configure a global ISDN switch type by using the `isdn switch-type` global configuration command. Because global commands are processed before interface-level commands, the command parser does not accept the `isdn switch-type` command on an interface unless a switch type is first added globally.

**Configuring an L2TP Access Concentrator**

Perform this task to configure a virtual private dial-up network (VPDN), a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC), and an ISDN switch type.
SUMMARY STEPS

1. enable
2. configure terminal
3. vpdn enable
4. vpdn search-order domain dnis
5. vpdn-group group-name
6. request-dialin
7. protocol l2tp
8. domain domain-name
9. exit
10. initiate-to ip ip-address
11. local name host-name
12. l2tp tunnel password password
13. exit
14. isdn switch-type switch-type
15. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>vpdn enable</td>
<td>Enables VPDN on a device.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# vpdn enable</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>vpdn search-order domain dnis</td>
<td>Specifies how a network access server (NAS) or a tunnel switch performs VPDN tunnel authorization searches.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# vpdn search-order domain dnis</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>vpdn-group group-name</td>
<td>Creates and associates a VPDN group with a customer or a VPDN profile and enters VPDN group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# vpdn-group group1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 6 request-dialin</td>
<td>Creates a request-dialin VPDN subgroup that indicates the dialing direction and initiates the tunnel; enters VPDN request-dialin group configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn)# request-dialin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7 protocol l2tp</td>
<td>Specifies that L2TP is the tunneling protocol used by the VPDN subgroup.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn-req-in)# protocol l2tp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8 domain domain-name</td>
<td>Specifies the domain name of users that are to be forwarded to a tunnel server using VPDN.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn-req-in)# domain xyz.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 9 exit</td>
<td>Returns to VPDN group configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn-req-in)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10 initiate-to ip ip-address</td>
<td>Specifies an IP address that is used for Layer 2 tunneling.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn)# initiate-to ip 192.0.2.55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 11 local name host-name</td>
<td>Specifies a local hostname that the tunnel uses to identify itself.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn)# local name host1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 12 l2tp tunnel password password</td>
<td>Sets a password that the device uses to authenticate the Layer 2 Tunneling Protocol (L2TP) tunnel.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn)# l2tp tunnel password password1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 13 exit</td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-vpdn)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 14 isdn switch-type switch-type</td>
<td>Selects a service provider switch type that accommodates PRI.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# isdn switch-type primary-4ess</td>
<td>• In this example, the ISDN switch type is primary-4ess.</td>
<td></td>
</tr>
<tr>
<td>Step 15 end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a PRI Group

Perform this task to specify an ISDN switch type and to configure a PRI group.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `isdn switch-type switch-type`
4. `controller {T1 | E1} slot/port`
5. `framing esf`
6. `linecode {ami | b8zs | hdb3}`
7. `cablelength long db-gain-value db-loss-value`
8. `pri-group timeslots timeslot-range`
9. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>isdn switch-type switch-type</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# isdn switch-type primary-ni</td>
</tr>
<tr>
<td></td>
<td>Selects a service provider switch type that accommodates PRI.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>controller {T1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# controller T1 0/1</td>
</tr>
<tr>
<td></td>
<td>Enters controller configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>framing esf</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-controller)# framing esf</td>
</tr>
<tr>
<td></td>
<td>Selects the extended super frame (esf) type for the T1 data line.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>linecode {ami | b8zs | hdb3}</td>
<td>Selects the line code type for T1 or E1 lines.</td>
</tr>
<tr>
<td></td>
<td>• Alternate Mark Inversion (AMI) is the default for T1 lines.</td>
</tr>
<tr>
<td></td>
<td>• Bipolar With 8-Bit Substitution (B8ZS) is valid only for the T1 controller.</td>
</tr>
<tr>
<td></td>
<td>• High-Density Bipolar 3 (hdb3) is the default for E1 lines.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-controller)# linecode b8zs</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>cablelength long (db)-gain-value (db)-loss-value</td>
<td>Increases the pulse of a signal at the receiver and decreases the pulse from the transmitter by using pulse equalization and line build-out for a T1 cable.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-controller)# cablelength long gain36 0db</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>pri-group timeslots timeslot-range</td>
<td>Configures the PRI group for the T1 or E1 controller to carry voice traffic.</td>
</tr>
<tr>
<td></td>
<td>• Use a hyphen to indicate a range. Groups of time slot ranges separated by commas (for example: 1-4,8-23) are also accepted.</td>
</tr>
<tr>
<td></td>
<td>• You can configure the PRI group to include all available time slots, or you can configure a select group of time slots for the PRI group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-controller)# pri-group timeslots 1-2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-controller)# end</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring a Dialer for an ISDN PRI Interface

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface serial controller-number:time-slot`
4. `no ip address`
5. `dialer rotary-group interface-number`
6. `dialer-group group-number`
7. `exit`
8. `isdn switch-type switch-type`
9. `isdn timer timer milliseconds`
10. `isdn skipsend-idverify`
11. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| | **Example:**  
  Device> enable | |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| | **Example:**  
  Device# configure terminal | |
| Step 3 | `interface serial controller-number:time-slot` | Specifies a serial interface created on a channelized E1 or channelized T1 controller and enters interface configuration mode. |
| | **Example:**  
  Device(config)# interface serial 0/1/7:23 | |
| Step 4 | `no ip address` | Removes an existing IP address or disables IP processing. |
| | **Example:**  
  Device(config-if)# no ip address | |
| Step 5 | `dialer rotary-group interface-number` | Includes a specified interface in a dialer rotary group. |
| | **Example:**  
  Device(config-if)# dialer rotary-group 100 | |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>dialer-group group-number</code></td>
<td>Controls access by configuring an interface to belong to a specific dialing group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# dialer-group group1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>isdn switch-type switch-type</code></td>
<td>Selects a service provider switch type that accommodates PRI.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# isdn switch-type primary-4ess</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td><code>isdn timer timer milliseconds</code></td>
<td>Identifies and configures an ISDN timer and changes the value of the timer for network, call connect, and disconnect waiting periods.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# isdn timer T321 30000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td><code>isdn skipsend-idverify</code></td>
<td>Stops user-side PRI interfaces from sending ID verification information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# isdn skipsend-idverify</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Dialer Interface by Enabling PPP Authentication

SUMMARY STEPS

1. enable
2. configure terminal
3. interface dialer dialer-rotary-group-number
4. no ip address
5. encapsulation encapsulation-type
6. dialer in-band
7. dialer idle-timeout seconds
8. dialer-group group-number
9. no peer default ip address
10. ppp authentication protocol1 [protocol2...] [if-needed | list-name | default | callin | one-time | optional]
11. exit
12. dialer-list dialer-group protocol protocol-name {permit | deny | list access-list-number | access-group}
13. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface dialer dialer-rotary-group-number</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config)# interface dialer 100</td>
</tr>
<tr>
<td></td>
<td>Defines a dialer rotary group and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>no ip address</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config-if)# no ip address</td>
</tr>
<tr>
<td></td>
<td>Removes an existing IP address or disables IP processing.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>encapsulation encapsulation-type</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config-if)# encapsulation ppp</td>
</tr>
<tr>
<td></td>
<td>Sets the encapsulation method used by the interface.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>dialer in-band</strong>&lt;br&gt;Example:&lt;br&gt;Device(config-if)# dialer in-band</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>dialer idle-timeout seconds</strong>&lt;br&gt;Example:&lt;br&gt;Device(config-if)# dialer idle-timeout 5000</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>dialer-group group-number</strong>&lt;br&gt;Example:&lt;br&gt;Device(config-if)# dialer-group group1</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>no peer default ip address</strong>&lt;br&gt;Example:&lt;br&gt;Device(config-if)# no peer default ip address</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>**ppp authentication protocol1 [protocol2...][if-needed</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>exit</strong>&lt;br&gt;Example:&lt;br&gt;Device(config-if)# exit</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>**dialer-list dialer-group protocol protocol-name {permit</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>end</strong>&lt;br&gt;Example:&lt;br&gt;Device(config)# end</td>
</tr>
</tbody>
</table>
Verifying ISDN/Dialer Access-Link Support for Broadband Aggregation

SUMMARY STEPS

1. enable
2. show ppp all
3. show vpdn

DETAILED STEPS

Step 1 enable
Enables privileged EXEC mode.

Example:

Device> enable

Step 2 show ppp all
Displays the PPP session information.

Example:

Device# show ppp all

<table>
<thead>
<tr>
<th>Interface/ID</th>
<th>OPEN+</th>
<th>Nego*</th>
<th>Fail-</th>
<th>Stage</th>
<th>Peer Address</th>
<th>Peer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Se0/1/0:0</td>
<td>LCP+</td>
<td>CHAP*</td>
<td>Fwded</td>
<td>10.1.1.1</td>
<td><a href="mailto:example@example.com">example@example.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Step 3 show vpdn
Displays basic information about all active virtual private dial-up network (VPDN) tunnels.

Example:

Device# show vpdn

<table>
<thead>
<tr>
<th>L2TP Tunnel and Session Information</th>
<th>Total tunnels 1</th>
<th>sessions 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocTunID</td>
<td>RemTunID</td>
<td>Remote Name</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>46988</td>
<td>29813</td>
<td>o2-ins</td>
</tr>
<tr>
<td>LocID</td>
<td>RemID</td>
<td>TunID</td>
</tr>
<tr>
<td>2300</td>
<td>46414</td>
<td>46988</td>
</tr>
</tbody>
</table>
Troubleshooting Tips

Use the following commands to troubleshoot the ISDN/dialer access-link support for broadband aggregation:

- **debug dialer**—Displays debugging information about the packets received on a dialer interface.
- **debug isdn q931**—Displays information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network.
- **debug ppp authentication**—Displays authentication protocol messages, including Challenge Handshake Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
- **debug ppp negotiation**—Displays information on traffic and exchanges of PPP packets sent during PPP startup, when PPP options are negotiated.

Configuration Examples for ISDN/Dialer Access-Link Support for Broadband Aggregation

Example: Configuring an L2TP Access Concentrator

The following example shows how to configure the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC):

```
Device(config)# vpdn enable
Device(config)# vpdn search-order domain dnis
Device(config)# vpdn-group group1
Device(config-vpdn)# request-dialin
Device(config-vpdn-req-in)# protocol l2tp
Device(config-vpdn-req-in)# domain xyz.com
Device(config-vpdn-req-in)# exit
Device(config-vpdn)# initiate-to ip 192.0.2.55
Device(config-vpdn)# local name host1
Device(config-vpdn)# l2tp tunnel password password1
Device(config-vpdn)# exit
Device(config)# isdn switch-type primary-4ess
```

Example: Configuring a PRI Group

The following example shows how to specify the ISDN PRI on the T1 controller for slot 0, port 1, and configures time slots 1 to 2:

```
Device(config)# isdn switch-type primary-ni
Device(config)# controller T1 0/1
Device(config-controller)# framing esf
Device(config-controller)# linecode b8zs
Device(config-controller)# cablelength long gain36 0db
Device(config-controller)# pri-group timeslots 1-2
```
Example: Configuring a Dialer for an ISDN PRI Interface

The following example shows how to specify the dialer profile configuration for an ISDN PRI interface:

```
Device(config)# interface serial 0/1/7:23
Device(config-if)# no ip address
Device(config-if)# dialer rotary-group 100
Device(config-if)# dialer-group group1
Device(config-if)# exit
Device(config)# isdn switch-type primary-4ess
Device(config)# isdn timer T321 30000
Device(config)# isdn skipsend-idverify
```

Example: Configuring a Dialer Interface by Enabling PPP Authentication

```
Device(config)# interface dialer 100
Device(config-if)# no ip address
Device(config-if)# encapsulation ppp
Device(config-if)# dialer in-band
Device(config-if)# dialer idle-timeout 5000
Device(config-if)# dialer-group group1
Device(config-if)# no peer default ip address
Device(config-if)# ppp authentication chap callin
Device(config-if)# exit
Device(config)# dialer-list dialergroup1 protocol ip permit
```

Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Broadband and DSL commands</td>
<td>Cisco IOS Broadband Access Aggregation and DSL Command Reference</td>
</tr>
<tr>
<td>Dial commands</td>
<td>Cisco IOS Dial Technologies Command Reference</td>
</tr>
<tr>
<td>VPDN commands</td>
<td>Cisco IOS VPDN Command Reference</td>
</tr>
<tr>
<td>Broadband and DSL configuration</td>
<td>Broadband Access Aggregation and DSL Configuration Guide</td>
</tr>
<tr>
<td>Technical support documentation for L2TP</td>
<td>Layer 2 Tunnel Protocol (L2TP)</td>
</tr>
<tr>
<td>Technical support documentation for PPP</td>
<td>Point-to-Point Protocol (PPP)</td>
</tr>
</tbody>
</table>
### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1661</td>
<td>Point-to-Point Protocol (PPP)</td>
</tr>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

### Feature Information for ISDN/Dialer Access-Link Support for Broadband Aggregation

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 . An account on Cisco.com is not required.

#### Table 19: Feature Information for ISDN/Dialer Access-Link Support for Broadband Aggregation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN/Dialer Access-Link Support for Broadband Aggregation</td>
<td>Cisco IOS XE Release 3.8S</td>
<td>The ISDN/Dialer Access-Link Support for Broadband Aggregation feature provides client connectivity to a network through PPP by using an ISDN PRI LAC session over IPv4.</td>
</tr>
</tbody>
</table>
Feature Information for ISDN/Dialer Access-Link Support for Broadband Aggregation