VPDN Configuration Guide, Cisco IOS XE Release 2

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

Last Updated: July 22, 2011

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

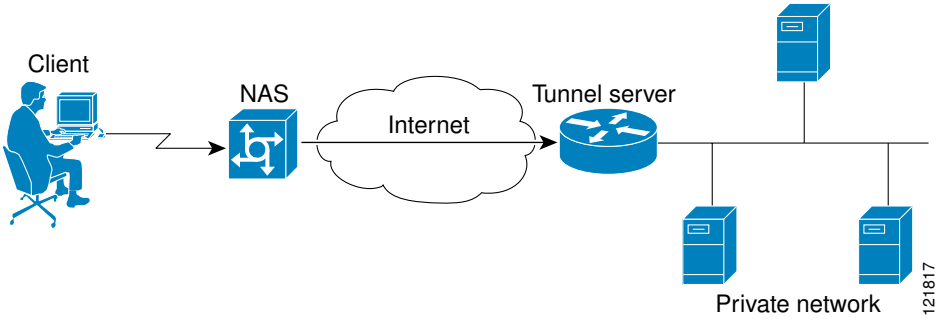
Instead of connecting directly to the remote private network, VPDN users connect to a nearby access server, which is often located at an Internet service provider (ISP) local point of presence (POP). Data is

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 in to, 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



A PPP client dials in to 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 calll* or *placing a calll*, 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 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 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

Generic Term	L2F Term	L2TP Term	PPTP Term
NAS	NAS	L2TP access concentrator (LAC)	PPTP access concentrator (PAC)
Tunnel server	Home gateway	L2TP network server (LNS)	PPTP network server (PNS)

Note 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

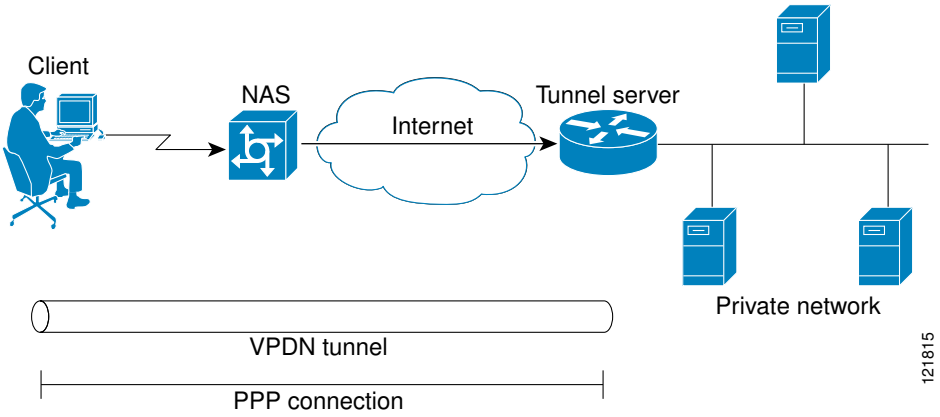
Client-initiated dial-in VPDN tunneling is also known as voluntary tunneling. In a client-initiated dial-in VPDN tunneling scenario, the client device initiates a Layer 2 tunnel to the tunnel server, and the NAS does not participate in tunnel negotiation or establishment. In this scenario, the NAS is 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



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

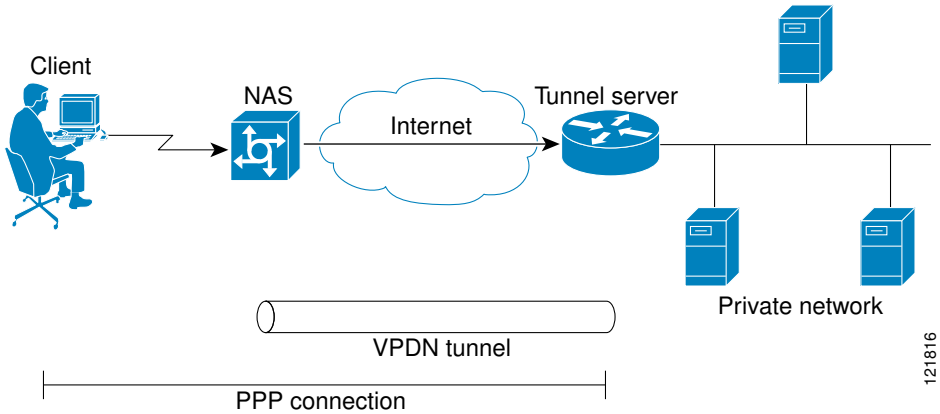
NAS-initiated dial-in VPDN tunneling is also known as compulsory tunneling. In a NAS-initiated dial-in VPDN tunneling scenario, the client dials in to the NAS through a medium that supports PPP. If the connection from the client to the ISP NAS is over a medium that is considered secure, such as digital 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



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, page 6
- Tunnel Switching VPDNs, page 6

VPDN Tunneling to an MMP Stack Group

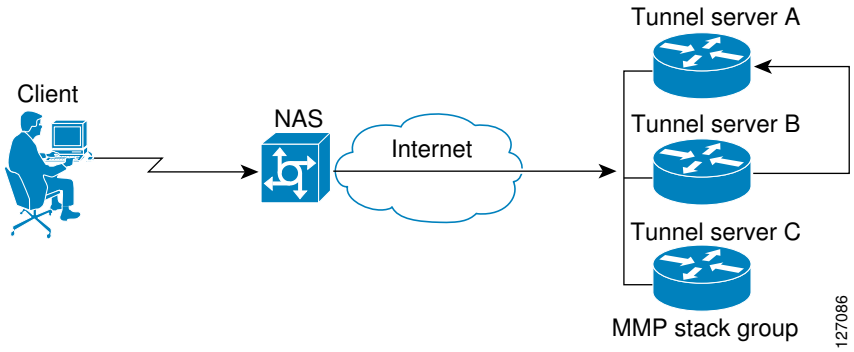
Multihop VPDN is required when the private network uses Mutlichassis Multilink PPP (MMP) with multiple tunnel servers in a stack group. Stack group configurations require the ability to establish Layer 2 tunnels between participating hardware devices. If the incoming data is delivered to the stack group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



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

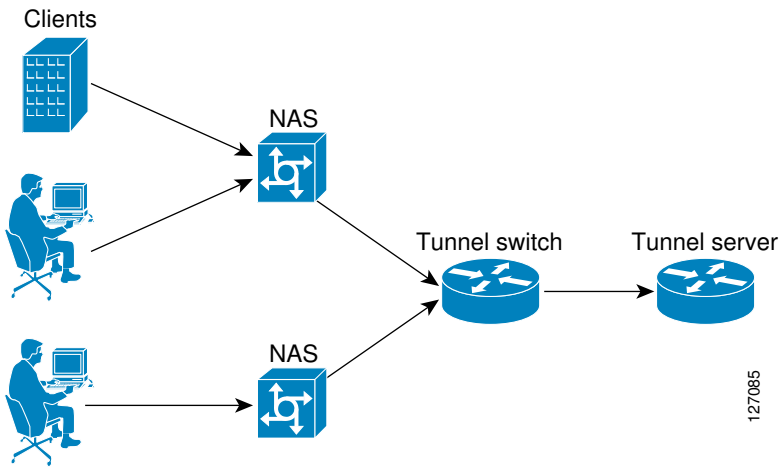
Multihop VPDN can be used to configure a router as a tunnel switch. A tunnel switch is a device that is configured as both a NAS and a tunnel server. A tunnel switch is able to receive packets from an incoming VPDN tunnel and send them out over an outgoing VPDN tunnel. Tunnel switch configurations can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



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, page 7
- L2TPv3, page 10

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.

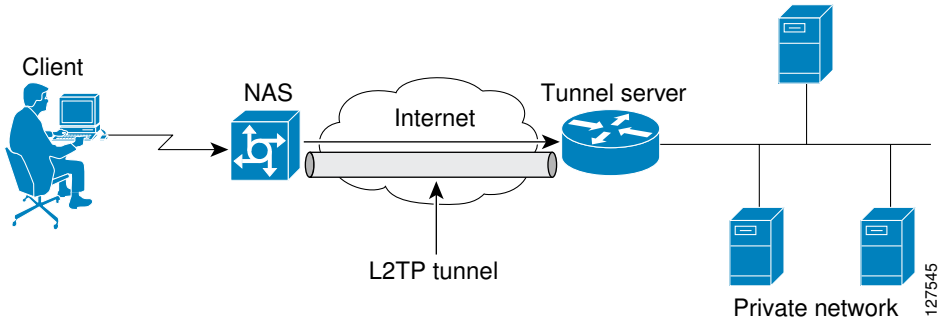
Table 2 L2F and L2TP Feature Comparison

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

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.

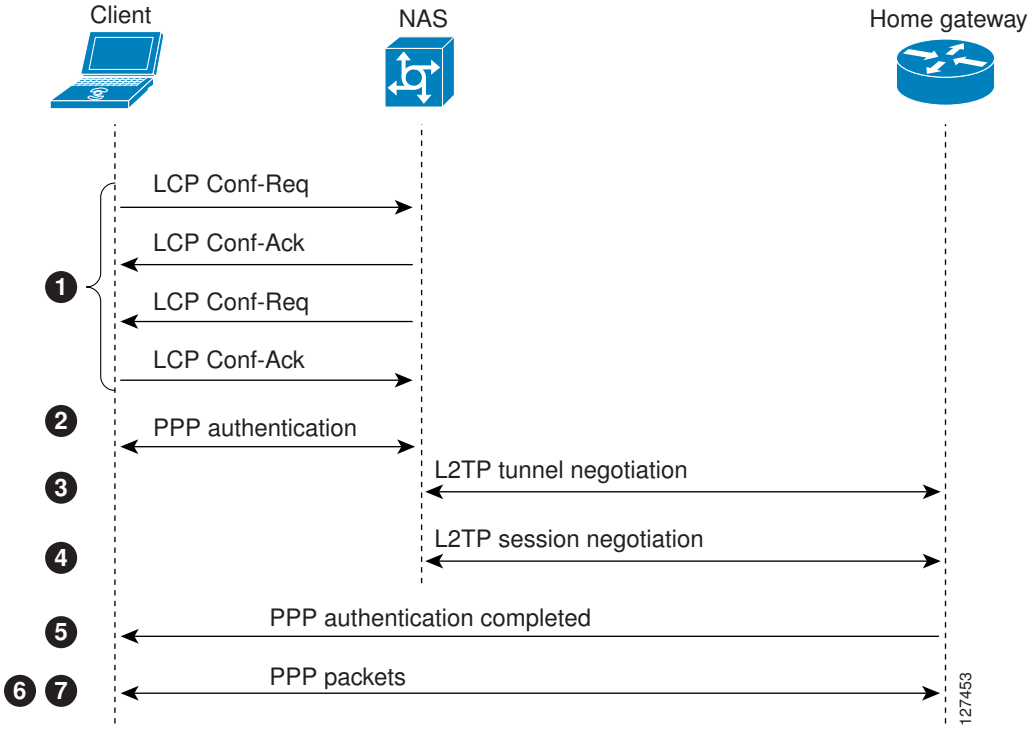
Figure 6



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



The following describes the sequence of events shown in the figure above and is keyed to the figure:

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.
6. 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 3 VPDN Subgroup Configuration Modes

VPDN Group Type	Command	Command Mode	Command Mode Prompt
tunnel server	**accept-dialin**	VPDN accept-dialin configuration	Router(config-vpdn-acc-in)#
NAS	**request-dialin**	VPDN request-dialin configuration	Router(config-vpdn-req-in)#

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

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

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer Two Tunneling Protocol L2TP*
RFC 3931	*Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4 Feature Information for VPDN Technology Overview

Feature Name	Releases	Feature Information
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.
Virtual Private Dial-up Network (VPDN)	Cisco IOS XE Release 2.1	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.

Configuring AAA for VPDNs

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 in to 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 example shows 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(00000011): Send Access-Request to 192.107.164.254:1645 id 1645/3, len 391
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:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:52: RADIUS:  Framed-Protocol     [7]   6   PPP                     [1]
01:24:52: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:52: RADIUS:  CHAP-Password       [3]   19  *
01:24:52: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                [15]
01:24:52: RADIUS:  Vendor, Cisco       [26]  46
01:24:52: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:52: RADIUS:  Vendor, Cisco       [26]  36
01:24:52: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:52: RADIUS:  NAS-Port            [5]   6   268435486
01:24:52: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
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:  Service-Type        [6]   6   Framed                  [2]
01:24:52: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS(00000011): Send Accounting-Request to 192.107.164.254:1646 id 1646/4,
len 495
01:24:55: RADIUS:  authenticator 22 6F B2 F3 88 B1 03 91 - 4A 70 53 BD 44 A6 A6 0F
01:24:55: RADIUS:  Acct-Session-Id     [44]  19  "1/0/0/30_00000008"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:55: RADIUS:  Vendor, Cisco       [26]  49
01:24:55: RADIUS:   Cisco AVpair       [1]   43  "minimum-data-rate-downstream-low-
power=32"
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "maximum-interleaving-delay-upstream=64"
01:24:55: RADIUS:  Framed-Protocol     [7]   6   PPP                     [1]
01:24:55: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:55: RADIUS:  Vendor, Cisco       [26]  32
01:24:55: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
01:24:55: RADIUS:  Acct-Authentic      [45]  6   RADIUS                  [1]
01:24:55: RADIUS:  Acct-Status-Type    [40]  6   Start                   [1]
01:24:55: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                [15]
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  36
01:24:55: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:55: RADIUS:  NAS-Port            [5]   6   268435486
01:24:55: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  41
01:24:55: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:55: RADIUS:  Service-Type        [6]   6   Framed                  [2]
01:24:55: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS:  Acct-Delay-Time     [41]  6   0
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, page 21

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

DSL Line Information	RADIUS VSA	Description
DSL Line Actual-Data-Rate-Upstream AVP	AAA_AT_ACTUAL_RATE_UP	Actual data rate upstream in kbps.
DSL Line Actual-Data-Rate-Downstream AVP	AAA_AT_ACTUAL_RATE_DOWN	Actual data rate downstream in kbps.
DSL Line Minimum-Data-Rate-Upstream AVP	AAA_AT_MIN_RATE_UP	Minimum data rate upstream in kbps.
DSL Line Minimum-Data-Rate-Downstream AVP	AAA_AT_MIN_RATE_DOWN	Minimum data rate downstream in kbps.

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

DSL Line Information	RADIUS VSA	Description
DSL Line Attainable-Data-Rate-Upstream AVP	AAA_AT_ATTAINABLE_RATE_UP	Attainable data rate upstream in kbps.
DSL Line Attainable-Data-Rate-Downstream AVP	AAA_AT_ATTAINABLE_RATE_DOWN	Attainable data rate downstream in kbps.
DSL Line Maximum-Data-Rate-Upstream AVP	AAA_AT_MAX_RATE_UP	Maximum data rate upstream in kbps.
DSL Line Maximum-Data-Rate-Downstream AVP	AAA_AT_MAX_RATE_DOWN	Maximum data rate downstream in kbps.
DSL Line Minimum-Data-Rate-Upstream -Low-Power AVP	AAA_AT_MIN_RATE_UP_LOW_POWER	Minimum data rate upstream in low power state in kbps.
DSL Line Minimum-Data-Rate-Downstream -Low-Power AVP	AAA_AT_MIN_RATE_DOWN_LOW_POWER	Minimum data rate downstream in low power state in kbps.
DSL Line Maximum-Interleaving-Delay-UpStream AVP	AAA_AT_MAX_INTER_DELAY_UP	Maximum interleaving delay upstream in ms.

DSL Line Information	RADIUS VSA	Description
DSL Line Maximum-Interleaving-Delay-DownStream AVP	AAA_AT_MAX_INTER_DELAY_DOWN	Maximum interleaving delay downstream in ms.
DSL Line Actual-Interleaving-Delay-Upstream AVP	AAA_AT_ACTUAL_INTER_DELAY_UP	Actual interleaving delay upstream in kbps.
DSL Line Actual-Interleaving-Delay-Downstream AVP	AAA_AT_ACTUAL_INTER_DELAY_DOWN	Actual interleaving delay downstream in kbps.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn search-order** {**dnis** [**domain**] [**multihop-hostname**] | **domain** [**dnis**] [**multihop-hostname**] | **multihop-hostname** [**dnis**] [**domain**]} **Example:** `Router(config)# vpdn search-order domain dnis`	Specifies how the service provider NAS or tunnel switch is to perform VPDN tunnel authorization searches. • At least one search parameter keyword must be specified. You can specify multiple search parameter keywords in any order to define the desired order in which searches will be performed. **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, page 25
- Restrictions, page 25
- Configuring Global per-User VPDN, page 25
- Configuring per-User VPDN for a VPDN Group, page 26

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn authen-before-forward** **Example:** `Router(config)# vpdn authen-before-forward`	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in tunnels.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**request-dialin** **Example:** `Router(config-vpdn)# 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.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 tunneling protocol that the VPDN group will use.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.
Step 7	**authen-before-forward** **Example:** `Router(config-vpdn)# authen-before-forward`	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP tunnels belonging to a VPDN group.

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.

- You must perform the task in the Enabling VPDN on the NAS and the Tunnel Server, page 23.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new model`	Enables the AAA access control model.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2*...] **Example:** `Router(config)# aaa authentication login default local`	Sets AAA authentication at login.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...] **Example:** `Router(config)# aaa authentication ppp default radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. **Note** This command must be configured with the **if-needed** option for the *method1*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.
Step 6	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2*...]] **Example:** `Router(config)# aaa authorization network default radius`	Sets parameters that restrict user access to a network.
Step 7	**vpdn aaa attribute** {**nas-ip-address**{**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}} **Example:** `Router(config)# vpdn aaa attribute nas-ip-address vpdn-nas`	(Optional) Enables AAA attributes related to a VPDN that will be reported to the AAA server in accounting records. **Note** Configure this command only on the tunnel server when remote AAA accounting will be enabled on the NAS.

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, page 30
- Configuring the Tunnel Terminator for Remote RADIUS AAA for L2TP Tunnels, page 32

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.

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

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

Step 3	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`
		Specifies a RADIUS server host.
		or
		Specifies a TACACS+ host.

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`
		(Optional) Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.
		or
		(Optional) Groups different TACACS+ server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
	• **server** *ip-address*
	
	Example:
	`Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`
	
	Example:
	`Router(config-sg-radius)# server 10.2.2.2`
		(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.
		Note Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.

• What to Do Next, page 32

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.

- 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 10.1.1.1`	Specifies a RADIUS server host.
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius group1`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters RADIUS server group configuration mode.

	Command or Action	Purpose
Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`	Configures the IP address of the RADIUS server for the group server. **Note** Perform this step multiple times to configure multiple RADIUS or TACACS+ servers as part of the server group.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits RADIUS server group configuration mode.
Step 7	**vpdn tunnel authorization network** {*list-name* | **default**} **Example:** `Router(config)# vpdn tunnel authorization network default`	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. • If the *list-name* argument was specified in the **aaa authorization** command, you must use that list name. • If the default keyword was specified in the **aaa authorization** command, you must use that keyword.
Step 8	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 3`	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 9	**vpdn tunnel authorization password** *password* **Example:** `Router(config)# vpdn tunnel authorization password my-secret`	(Optional) Configures a false password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname. **Note** If this command is not enabled, the password will always be "cisco."

• What to Do Next, page 34

What to Do Next

You must perform these tasks in these sections:

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

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
, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
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.

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
```

```
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=''
rem_addr='' authen_type=CHAP service=PPP priv=1
```

```
Jan 30 12:17:10: Tnl 74 L2TP: Got a response 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 (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): found list default
Jan 30 12:17:10: AAA/AUTHEN (2964849625): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=2964849625
20:03:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
Jan 30 12:17:11: TAC+: ver=192 id=2964849625 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: TAC+: ver=192 id=1474818051 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN (2964849625): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel state change from wait-ctl-reply to
established
Jan 30 12:17:11: Tnl 74 L2TP: O SCCCN to ABCDE tnlid 56
Jan 30 12:17:11: Tnl 74 L2TP: SM State established
Jan 30 12:17:11: As1 74/1 L2TP: O ICRQ to ABCDE 56/0
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-for-tunnel
to wait-reply
Jan 30 12:17:11: Tnl 74 L2TP: Dropping old CM, Ns 0, expected 1
Jan 30 12:17:11: As1 74/1 L2TP: O ICCN to ABCDE 56/1
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-reply to
established
```

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.

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
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
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: free_user (0x21F6D0) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: Tnl 56 L2TP: O SCCRP to rtp_tunnel tnlid 74
Jan 30 12:17:09: Tnl 56 L2TP: Tunnel state change from idle to
wait-ctl-reply
Jan 30 12:17:10: Tnl 56 L2TP: O Resend SCCRP, flg TLF, ver 2, len 152,
tnl 74, cl 0, ns 0, nr 1
Jan 30 12:17:10: Tnl 56 L2TP: I SCCCN from rtp_tunnel tnl 74
Jan 30 12:17:10: Tnl 56 L2TP: Got a Challenge Response in SCCCN from rtp_tunnel
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x227F3C) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/STARTTranslating "rtp.cisco.com"
(4117701992): port='' list='default' action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): found list default
Jan 30 12:17:10: AAA/AUTHEN (4117701992): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=4117701992
Jan 30 12:17:11: TAC+: ver=192 id=4117701992 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: TAC+: ver=192 id=2827432721 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: 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: Tnl 56 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 56 L2TP: Tunnel state change from wait-ctl-reply
to established
Jan 30 12:17:11: Tnl 56 L2TP: SM State established
Jan 30 12:17:11: Tnl 56 L2TP: I ICRQ from rtp_tunnel tnl 74
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session FS enabled
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: New session created
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: O ICRP to rtp_tunnel 74/1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-for-tunnel
to wait-connect
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: I ICCN from rtp_tunnel tnl 74, cl 1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-connect
to established
Jan 30 12:17:11: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
Jan 30 12:17:11: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c
Jan 30 12:17:11: Vi1 VPDN: Virtual interface created for user1@rtp.cisco.com
Jan 30 12:17:11: Vi1 VPDN: Set to Async interface
Jan 30 12:17:11: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
Jan 30 12:17:11: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate
Jan 30 12:17:11: Vi1 VTEMPLATE: ************* CLONE VACCESS1 *****************
Jan 30 12:17:11: Vi1 VTEMPLATE: Clone from Virtual-Template1
```

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:

```
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, page 43
- Configuring Directed Request Authorization of VPDN Users on the NAS, page 45

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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip host** {*name* | **t** *modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] **Example:** `Router(config)# ip host example.com 10.3.3.3`	Specifies or modifies the hostname for the network server. **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, page 30.

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`
		Allows users logging in to a NAS to select a RADIUS server for authentication.
		or
		Allows users logging in to a NAS to select a TACACS+ server for authentication.

Step 5	**vpdn authorize directed-request** **Example:** `Router(config)# vpdn authorize directed-request`	Enables VPDN authorization for directed request users.

• What to Do Next, page 32

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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip host** {*name* | **t** *modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] **Example:** `Router(config)# ip host example.com 10.3.3.3`	Specifies or modifies the hostname for the network server. **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, page 30.

	Command or Action	Purpose

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`
		Allows users logging in to a NAS to select a RADIUS server for authentication.
		or
		Allows users logging in to a NAS to select a TACACS+ server for authentication.

Step 5	**vpdn authorize directed-request** **Example:** `Router(config)# vpdn authorize directed-request`	Enables VPDN authorization for directed request users.

- What to Do Next, page 32

What to Do Next

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

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.

Perform this task on the NAS to configure a set of global or per-VRF stripping rules.

- 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

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

Command or Action	Purpose

Step 3 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*]
 	
Example:
`Router(config)# radius-server domain-stripping prefix-delimiter #%&\\ delimiter @/`
 	
Example:
`Router(config)# tacacs-server domain-stripping prefix-delimiter %\$ vrf myvrf`
	(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.
	• **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.
	Note 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.
	• **prefix-delimiter** *character* [*character2...character7*]--Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\.
	Note 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.
	• **delimiter** *character* [*character2...character7*]--Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\.
	• **vrf** *vrf-name* --Restricts the stripping configuration to a VRF instance. The *vrf-name*argument specifies the name of a configured VRF.

	Command or Action	Purpose

Step 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*]
	
	Example:
	`Router(config)# radius-server domain-stripping strip-suffix cisco.com`
	
	Example:
	`Router(config)# tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf`
		(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the RADIUS server.
		or
		(Optional) Configures a router to strip a specific suffix from the username before forwarding the username to the TACACS+ server.
		• **strip-suffix** *suffix* --Enables per-suffix suffix stripping and specifies the string that must be matched for the suffix to be stripped.
		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 .
		• **vrf** *vrf-name* --Restricts the per-suffix stripping configuration to a VRF instance. The *vrf-name*argument specifies the name of a VRF.
		Note You can configure a single ruleset to strip multiple specific suffixes by performing this step multiple times.

• What to Do Next, page 32

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname tunnelserver12`	Specifies or modifies the hostname for the network server.
Step 4	**username** *name* **password** *secret* **Example:** `Router(config)# username nas4 password mysecret`	Establishes a username-based authentication system. • 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, page 51

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**local name** *host-name* **Example:** `Router(config-vpdn)# local name tunnelserver2`	Specifies a local hostname that the tunnel will use to identify itself.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.
Step 6	**username** *name* **password** *secret* **Example:** `Router(config)# username nas7 password mysecret`	Establishes a username-based authentication system. • 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, page 51

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**l2tp tunnel password** *password* **Example:** `Router(config-vpdn)# l2tp tunnel password mysecret`	Sets the password that the router will use to authenticate the tunnel.

	Command or Action	Purpose
Step 5	**local name** *host-name* **Example:** `Router(config-vpdn)# local name tunnelserver2`	(Optional) Specifies a local hostname that the tunnel will use to identify itself. • You must perform this step if the remote router does not use the L2TP tunnel password.
Step 6	**exit** **Example:** `Router(config-vpdn)# exit`	(Optional) Exits VPDN group configuration mode. • You must perform this step only if the remote router does not use the L2TP tunnel password method of VPDN tunnel authentication.
Step 7	**username** *name* **password** *secret* **Example:** `Router(config)# username nas64 password mysecret`	(Optional) Establishes a username-based authentication system. • You need to perform this step only if the remote router does not use the L2TP tunnel password method of VPDN tunnel authentication. • The specified username must be the name of the remote router. • The password must be the same on both routers.

- What to Do Next, page 51

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Enters VPDN group configuration mode and creates a VPDN group.
Step 4	**no l2tp tunnel authentication** **Example:** `Router(config-vpdn)# no l2tp tunnel authentication`	Disables L2TP tunnel authentication.

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.

- You must perform the tasks in the Configuring AAA on the NAS and the Tunnel Server, page 28.
- You must configure the router to use a remote RADIUS AAA server as described in the Configuring Remote AAA for VPDNs, page 30.
- 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa accounting network default** | *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname* **Example:** `Router(config)# aaa accounting network list1 start-stop group radius`	Enables network accounting. • **default** --If the default network accounting method-list is configured and no additional accounting configurations are enabled on the 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* **Example:** `Router(config)# vpdn tunnel accounting network list1`	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.

	Command or Action	Purpose
Step 5	**vpdn session accounting network** *list-name* **Example:** `Router(config)# vpdn session accounting network list1`	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.

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.

- 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."

Note 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

	Command or Action	Purpose
Step 1	**service type** = *Outbound* **Example:** `service type = Outbound`	Specifies the service type.
Step 2	**tunnel-type** = *protocol* **Example:** `tunnel-type = l2tp`	Specifies the tunneling protocol. **Note** L2TP is the only valid protocol for this task.
Step 3	**Cisco:Cisco-Avpair = vpdn:dout-dialer** = *NAS-dialer-number* **Example:** `Cisco:Cisco-Avpair = vpdn:dout-dialer = 2`	Specifies which dialer to use on the NAS for dial-out configuration. **Note** Perform this step only for dial-out configurations.
Step 4	**Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate** = *vtemplate-number* **Example:** `Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate = 1`	Specifies the virtual template number to use on the tunnel server for dial-in configuration. **Note** Perform this step only for dial-in configurations. **Note** 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, page 32.

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.

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

	Command or Action	Purpose

Step 1	Do one of the following:
	• *user @ domain.com* **Password = "** *secret* **" Service-Type = Outbound**
	• *user.domain.com* **Password = "** *secret* **" Service-Type = Outbound**
	
	Example:
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	
	Example:
	`user.cisco.com Password = "cisco" Service-Type = Outbound`
		Specifies the user or domain, the tunnel password, and the service type.

Step 2	**tunnel-type =** *protocol* **Example:** `tunnel-type = l2tp`	Specifies the tunneling protocol used. • The tunnel type must be identical for users to be grouped into the same tunnel.
Step 3	**tunnel-server-endpoint =** *ip-address* **Example:** `tunnel-server-endpoint = 10.1.1.1`	Specifies the IP address of the tunnel server that calls from the specified user or domain are tunneled to. • The tunnel server endpoint must be identical for users to be grouped into the same tunnel.
Step 4	**tunnel-assignment-id =** *name* **Example:** `tunnel-assignment-id = group1`	Specifies the tunnel ID that calls from the specified user or domain are assigned. • The tunnel assignment ID must be identical for users to be grouped into the same tunnel.

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.

- 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

	Command or Action	Purpose

Step 1	Do one of the following:
	• *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`
		Specifies the user or domain, the tunnel password, and the service type.

	Command or Action	Purpose
Step 2	**tunnel-client-auth-id** = {**:1** | **:2**}: " *NAS-name* " **Example:** `tunnel-client-auth-id = :2:NAS36`	Specifies the name used by the NAS when it authenticates tunnel setup with the tunnel server. • **:1** --Specifies L2F tunnels. • **:2** --Specifies L2TP tunnels.
Step 3	**tunnel-server-auth-id** = {**:1** | **:2**}: " *tunnel-server-name* " **Example:** `tunnel-server-auth-id = :2:TS14`	Specifies the name used by the tunnel server when it authenticates tunnel setup with the NAS. • **:1** --Specifies L2F tunnels. • **:2** --Specifies L2TP tunnels.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group pppoe-group`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**dsl-line-info-forwarding** **Example:** `Router(config-vpdn)# 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.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

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, page 62
- Overriding calling-station-id VSA with remote-id, page 63

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 87 circuit-id** **Example:** `Router(config)# radius-server attribute 87 circuit-id`	Overrides the NAS-Port-Id attribute with the Circuit-ID attribute in RADIUS access and accounting requests.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

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

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

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

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

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, page 79 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:

DETAILED STEPS

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 FastEthernet0/0.200. 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(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 Access-Request to 172.20.164.143:1645 id 1645/65, len 98
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:  Framed-Protocol     [7]   6 PPP                       [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                  [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
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:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                       [1]
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: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
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 attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
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 1 646/42, 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:  Framed-Protocol     [7]   6 PPP                       [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic      [45]  6 RADIUS                    [1]
02:10:49: RADIUS:  Acct-Status-Type    [40]  6 Start                     [1]
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                  [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time     [41]  6   0
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len 20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

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

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

	Command or Action	Purpose
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

Step 5	**l2tp rx-speed** *value* **Example:** `Router(config-vpdn)# l2tp rx-speed 15000`	Sends the rx-speed value to LNS. • If the rx-speed value is not provided, L2TP receives the rx-speed value from PPPoE. **Note** 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.
Step 6	**l2tp tx-speed** *value* **Example:** `Router(config-vpdn)# l2tp tx-speed 15000`	Sends the tx-speed value to LNS. • If the tx-speed value is not provided, L2TP receives the tx-speed value from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

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.

- 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

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

	Command or Action	Purpose
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

Step 5	**l2tp rx-speed ancp** [*value*] **Example:** `Router(config-vpdn)# l2tp rx-speed ancp 15000`	Sends the rx-speed value to LNS if a value is not configured for ANCP. • 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. • 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. • 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. • For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the rx-speed value obtained from PPPoE.

	Command or Action	Purpose
Step 6	**l2tp tx-speed ancp** [*value*] **Example:** `Router(config-vpdn)# l2tp tx-speed ancp 15000`	Sends the tx-speed value to LNS if a value is not configured for ANCP. • 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. • 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. • 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 **vbr-nrt** command. If the tx-speed value is not configured in VC-class configuration mode, L2TP sends the tx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured, L2TP sends the tx-speed value obtained from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

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.

- 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN on the router.

Step 4	Do one of the following:
	• **vpdn-group** *name*
	• **vpdn-template** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config)# vpdn-template 1`
		Enters VPDN group configuration mode.
		or
		Enters VPDN template configuration mode.

Step 5	**l2tp rx-speed ram-min** [*value*] **Example:** `Router(config-vpdn)# l2tp rx-speed ram-min 15000`	Sends the rx-speed value to LNS if the average rate traffic shaping value is not configured. • For ATM interfaces, if the average rate traffic shaping value is not configured and the rx-speed value is not provided in the command, 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. • For Ethernet interfaces, if the average rate traffic shaping value is not configured and the rx-speed value is not provided in the command, L2TP sends the rx-speed value obtained from PPPoE.

	Command or Action	Purpose
Step 6	**l2tp tx-speed ram-min** [*value*] **Example:** `Router(config-vpdn)# l2tp tx-speed ram-min 15000`	Sends the tx-speed value to LNS if the average rate traffic shaping value is not configured. • For ATM interfaces, if the average rate traffic shaping value is not configured and the tx-speed value is not provided in the command, L2TP sends the peak cell rate (PCR) value configured using the **vbr-nrt** command in VC-class configuration mode. If the tx-speed value is not configured in VC-class configuration mode, L2TP sends the tx-speed value obtained from PPPoE. • For Ethernet interfaces, if the average rate traffic shaping value is not configured and the tx-speed value is not provided in the command, L2TP sends the tx-speed value obtained from PPPoE.
Step 7	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN group configuration mode and returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database or on a remote authorization server (home gateway), if one is present.
Step 4	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group example`	Creates a VPDN group and enters VPDN group configuration mode.
Step 5	**l2tp security ip address-check** **Example:** `Router(config-vpdn)# l2tp security ip address-check`	Configures the LNS to compare the IP addresses contained in the inbound and outbound message to ensure they are identical. If the IP addresses to not match, the L2TP tunnel is not established.
Step 6	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn dead-cache** {**group** *name* | **all**} **Example:** `Router# show vpdn dead-cache all`	Displays the status of any LNS in a dead-cache state, including how long the entry has been in the dead-cache state.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

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.

Perform this procedure on the LAC.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear vpdn dead-cache** {**group** *name* | **ip-address** *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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps vpdn dead-cache** **Example:** `Router(config)# snmp-server enable traps vpdn dead-cache`	Enables the generation of an SNMP event whenever an LNS enters or exits the dead-cache state.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

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

Syslog Message	Description
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> added	Added--An entry in the LSG table enters DOWN status, which marks it a dead-cache entry.
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> deleted	Deleted--An entry in the LSG table is removed from DOWN status, which deletes its dead-cache entry from the table.
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> cleared	Cleared--An entry in the LSG table is manually cleared.

To generate a syslog event when an LNS enters or exits the dead-cache state, follow this procedure.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn logging dead-cache** **Example:** `Router(config)# vpdn logging dead-cache`	Enables the generation of a syslog event when an LNS enters or exits the dead-cache state.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

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
vpdn-group 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 mymethodlist group myvpdngroup
radius-server host 10.2.2.2 auth-port 1939 acct-port 1443
aaa group server radius myvpdngroup
 server 10.2.2.2 auth-port 1939 acct-port 1443
!
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 mymethodlist 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 mymethod 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.

```
radius-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, the username *user* 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
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
```

```
!
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 10.1.1.2 255.255.255.255 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
```

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
!
```

```
enable password example
!
no aaa new-model
!
vpdn enable
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 1 IP address>
 l2tp tunnel password 0 example
!
bba-group pppoe 1
 virtual-template 1
!
interface Virtual-Template 1
 no ip address
 ppp authentication pap
!
interface <interface>
 pppoe enable group 1
!
end
```

The following shows an example configuration for the LNS 1.

```
hostname LNS1
!
enable password example
!
aaa authentication ppp default local
!
vpdn enable
!
vpdn-group 1
!Default L2TP VPDN group
 accept-dialin
 protocol l2tp
 virtual-template 1
 l2tp tunnel password 0 example
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 2 IP address>
 l2tp tunnel password 0 example
!
interface Virtual-Template 1
 ip unnumbered <interface>
 ppp authentication pap
!
end
```

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

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
VPDN technology overview	VPDN Technology Overview module
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*
Information about configuring AAA	Authentication, Authorization, and Accounting (AAA) module
Layer 2 Tunnel Protocol	*Layer 2 Tunnel Protocol*
Information about configuring RADIUS and TACACS	Security Server Protocols module

Related Topic	Document Title
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

Standard	Title
DSL Forum 2004-72	--

MIBs

MIB	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Tunnel Authentication Attributes*

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8 Feature Information for AAA for VPDNs

Feature Name	Releases	Feature Information
Configurable Domain Name Prefix and Suffix Stripping for the RADIUS server	Cisco IOS XE Release 2.1	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: **radius-server domain-stripping**.
RADIUS Attribute 82: Tunnel Assignment ID	Cisco IOS XE Release 2.1	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.
RADIUS Tunnel Attribute Extensions	Cisco IOS XE Release 2.1	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.

Feature Name	Releases	Feature Information
RFC-2867 RADIUS Tunnel Accounting	Cisco IOS XE Release 2.1	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: **aaa accounting**, **vpdn session accounting network**, **vpdn tunnel accounting network**.
Tunnel Authentication via RADIUS on Tunnel Terminator	Cisco IOS XE Release 2.1	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: **vpdn tunnel authorization network**, **vpdn tunnel authorization password**, **vpdn tunnel authorization virtual-template**.
L2TP Forwarding of PPPoE Tagging Information	Cisco IOS XE Release 2.4	This feature was introduced on Cisco ASR 1000 Series Routers.
LNS Address Checking	Cisco IOS XE Release 2.4	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: **l2tp security ip address-check**.

Feature Name	Releases	Feature Information
Modified LNS Dead-Cache Handling	Cisco IOS XE Release 2.4	This feature displays and clears (restarts) any LNS entry in a dead-cache (DOWN) state. The following commands were introduced by this feature: **clear vpdn dead-cache**, **show vpdn dead-cache**. The following commands were modified by this feature: **snmp-server enable traps**, **vpdn logging**.
Configurable Domain Name Prefix and Suffix Stripping for the TACACS+ server	Cisco IOS XE Release 2.5	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: **tacacs-server domain-stripping**.
ANCP values configuration support on LNS	Cisco IOS XE Release 3.2S	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: **l2tp rx-speed**, **l2tp tx-speed**.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

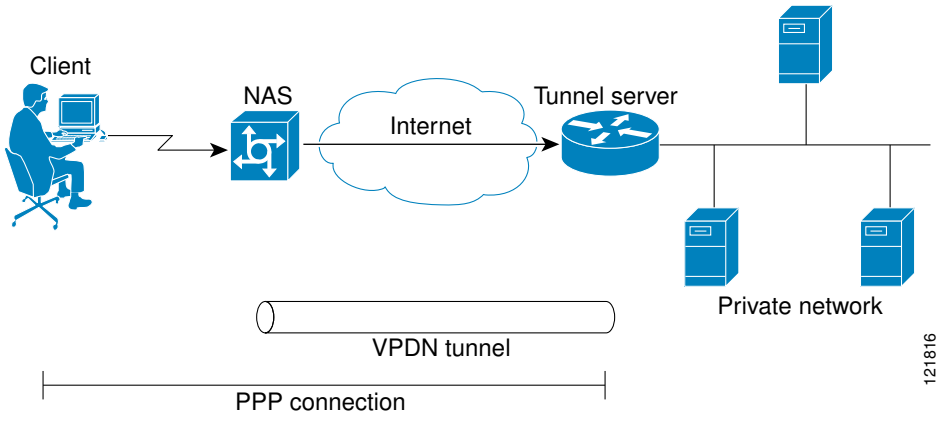
NAS-Initiated Dial-in VPDN Tunneling

NAS-initiated dial-in VPDN tunneling is also known as compulsory tunneling. In NAS-initiated dial-in VPDN tunneling, the client dials in to 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



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

Control Message	Result Code	Error Code
StopCCN, CDN	2: General error, see Error Code.	4: Insufficient resources to handle this operation now. 6: A generic vendor-specific error occurred.[1] 7: Try another. 9: Try another directed.
CDN	4: Temporary lack of resources.	--

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

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).

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	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.
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.

	Command or Action	Purpose
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, page 100

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.

	Command or Action	Purpose
Step 5	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures a tunnel server to accept requests from a NAS to establish an L2F or L2TP tunnel, creates an accept-dialin VPDN subgroup, and enters VPDN accept dial-in subgroup configuration mode.
Step 6	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 protocol that the VPDN group will use.
Step 7	**virtual-template** *number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 8	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits to VPDN group configuration mode.
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.
Step 10	**lcp renegotiation** {**always** | **on-mismatch**} **Example:** `Router(config-vpdn)# lcp renegotiation always`	(Optional) Allows the tunnel server to renegotiate the PPP Link Control Protocol (LCP) on dial-in calls using L2TP or L2F. • This command is useful for a tunnel server that tunnels to a non-Cisco NAS, where the NAS might negotiate a different set of LCP options than what the tunnel server expects.

	Command or Action	Purpose
Step 11	**force-local-chap** **Example:** `Router(config-vpdn)# force-local-chap`	(Optional) Forces the tunnel server to reauthenticate the client. • Enabling this command forces the tunnel server to reauthenticate the client in addition to the proxy authentication that occurs at the NAS. **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, page 103

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Enters interface configuration mode and creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 4	**ip unnumbered** *type number* **Example:** `Router(config-if)# ip unnumbered FastEthernet 0/0`	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.
Step 5	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config-if)# ppp authentication chap`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.
Step 6	**peer default ip address** {*ip-address*| **dhcp-pool** | **dhcp** | **pool** [*pool-name*]} **Example:** `Router(config-if)# peer default ip address pool mypool`	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.
Step 7	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.

Verifying a NAS-Initiated VPDN Configuration

- Verifying and Troubleshooting Tunnel Establishment Between the NAS and the Tunnel Server, page 105
- Verifying the Connection Between the Client and the NAS, page 106

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 ts1 tnl 8
20:19:17: L2X: Never heard of ts1
20:19:17: Tnl 7 L2TP: New tunnel created for remote ts1, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, ts1
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 ts1
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/Cl 7/1 L2TP: Session FS enabled
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/Cl 7/1 L2TP: New session created
20:19:17: Tnl/Cl 7/1 L2TP: O ICRP to ts1 8/1
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-connect to established
20:19:17: Vi1 VPDN: Virtual interface created for user1@cisco.com
20:19:17: Vi1 VPDN: Set to Async interface
20:19:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
20:19:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
20:19:18: Vi1 VPDN: Bind interface direction=2
20:19:18: Vi1 VPDN: PPP LCP accepting rcv CONFACK
20:19:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

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:

```
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
%LINK-3-UPDOWN: Interface Async1, changed state to up
%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-Template1
  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..., Vi2.9171 est    1d10h 9184
34090      31996      22         user@ci..., Vi2.1734 est    1d10h 1735
1217       42591      22         user@ci..., Vi2.9312 est    1d10h 9325
6737       22325      22         user@ci..., Vi2.1729 est    1d10h 1730
59420      17035      34         user@ci..., Vi2.9338 est    1d10h 9351
45069      60982      34         user@ci..., Vi2.1645 est    1d10h 1646
27825      44751      34         user@ci..., Vi2.1653 est    1d10h 1654
24600      7627       34         user@ci..., Vi2.9096 est    1d10h 9109
13018      65037      43         user@ci..., Vi2.8166 est    1d10h 8179
43090      34448      43         user@ci..., Vi2.8176 est    1d10h 8189
31798      41505      43         user@c..., Vi2.15752 est    1d10h 15765
56832      64322      43         user@c..., Vi2.15655 est    1d10h 15668
53944      25409      48         user@c..., Vi2.14115 est    1d10h 14128
16215      52915      48         user@c..., Vi2.14134 est    1d10h 14147
17332      14000      48         user@ci..., Vi2.6630 est    1d10h 6643
12466      54817      48         user@ci..., Vi2.6622 est    1d10h 6635
28290      37822      50         user@ci..., Vi2.5094 est    1d10h 15905
44839      30137      50         user@c..., Vi2.15875 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, page 105.

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, page 109
- Configuring Global L2TP Calling Station ID Suppression on the NAS, page 109
- Configuring L2TP Calling Station ID Suppression for a VPDN Group on the NAS, page 110
- Configuring L2TP Calling Station ID Suppression on the NAS Remote RADIUS Server, page 111

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn l2tp attribute clid mask-method** {**right** *mask-character characters* | **remove**} [**match** *match-string*] **Example:** `Router(config)# vpdn l2tp attribute clid mask-method right # 6 match %321`	Configures a NAS to suppress L2TP calling station IDs globally on the router. • **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. • **remove** --Removes the entire calling station ID. • **match** *match-string* --Removes or masks the calling station ID only when the username contains the specified *match-string*.

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.

- 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group L2TP`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**l2tp attribute clid mask-method** {**right** *mask-character characters*| **remove**} [**match** *match-string*] **Example:** `Router (config-vpdn)# l2tp attribute clid mask-method remove`	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template. • **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. • **remove** --Removes the entire calling station ID. • **match** *match-string* --Removes or masks the calling station ID only when the username contains the specified *match-string*.

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.

- 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*
5. **Cisco-Avpair = vpdn:l2tp-clid-mask-method=** {**right:** *character* **:** *characters* | **remove**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Cisco-Avpair = vpdn:l2tp-tunnel-password=** *secret* **Example:** `Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco`	Specifies the L2TP tunnel password in the RADIUS user profile.
Step 2	**Cisco-Avpair = vpdn:tunnel-type= l2tp** **Example:** `Cisco-Avpair = vpdn:tunnel-type=l2tp`	Specifies L2TP as the tunneling protocol in the RADIUS user profile.
Step 3	**Cisco-Avpair = vpdn:tunnel-id=** *name* **Example:** `Cisco-Avpair = vpdn:tunnel-id=test`	Specifies the tunnel ID in the RADIUS user profile.
Step 4	**Cisco-Avpair = vpdn:ip-address=** *address* **Example:** `Cisco-Avpair = vpdn:ip-address=172.16.9.9`	Specifies the NAS IP address in the RADIUS user profile.
Step 5	**Cisco-Avpair = vpdn:l2tp-clid-mask-method=** {**right:** *character* **:** *characters* | **remove**} **Example:** `Cisco-Avpair = vpdn:l2tp-clid-mask-method= right:#:5`	Specifies L2TP calling station ID suppression parameters in the RADIUS user profile. • **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:

```
! 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
!
 terminate-from hostname ISP-NAS
 local name ENT-TS
 force-local-chap
```

```
!
! 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$8qtb$MHcYeW2kn8VNYgz932eXl.
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
 domain cisco.com#184
!
 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 ppoe 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
 ppoe 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
```

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$8qtb$MHcYeW2kn8VNYgz932eXl.
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
aaa nas port extended
aaa session-id common
!
ip subnet-zero
ip cef
no ip domain lookup
!
vpdn enable
vpdn search-order domain
!
bba-group ppoe 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
!
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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VPDN commands	*Cisco IOS VPDN Command Reference*
VPDN technology overview	*VPDN Technology Overview*
Technical support documentation for L2TP	Layer 2 Tunnel Protocol (L2TP)
Technical support documentation for VPDNs	Virtual Private Dial-Up Network (VPDN)

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer Two Tunneling Protocol (L2TP)*

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

Feature Name	Software Releases	Feature Information
L2TP Calling Station ID Suppression	Cisco IOS XE Release 2.1	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: **l2tp attribute clid mask-method**, **vpdn l2tp attribute clid mask-method**.
L2TP Extended Failover	Cisco IOS XE Release 2.1	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.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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, page 123.

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, page 122

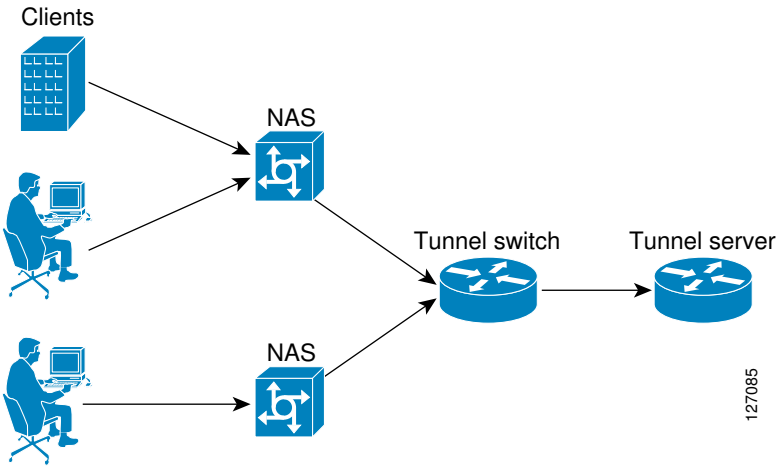
Tunnel Switching Using Multihop VPDN

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



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

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

- What to Do Next, page 124

What to Do Next

You must perform the task in the Configuring the Multihop Tunnel Switch to Terminate Incoming VPDN Tunnels, page 124.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and to enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	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.
Step 6	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 Tunneling Protocol that the VPDN group will use.
Step 7	**virtual-template** *number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	(Optional) Specifies which virtual template will be used to clone virtual access interfaces. This step is not required if the virtual access interface is not going to be cloned when a user connects.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits to VPDN group configuration mode.
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, page 126

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**description** *string* **Example:** `Router(config-vpdn)# description myvpdngroup`	(Optional) Adds a description to a VPDN group.
Step 5	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	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.
Step 6	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunneling Protocol that the VPDN group will use.

	Command or Action	Purpose

Step 7	Do one of the following:
	• **domain** *domain-name*
	• **dnis** {*dnis-number* | *dnis-group-name*}
	• **multihop-hostname** *ingress-tunnel-name*
	
	Example:
	`Router(config-vpdn-req-in)# domain company.com`
	
	Example:
	`Router(config-vpdn-req-in)# dnis 5687`
	
	Example:
	`Router(config-vpdn-req-in)# multihop-hostname nas1`
		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.
		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.

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 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.

Configuration Examples for Multihop VPDN

• Example Configuring Multihop VPDN Tunnel Switching, page 129

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

```
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch
vpdn-group 1
 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

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VPDN commands	*Cisco IOS VPDN Command Reference*
VPDN technology overview	*VPDN Technology Overview*
Broadband access aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer Two Tunneling Protocol (L2TP)*

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11 Feature Information for Multihop VPDN

Feature Name	Software Releases	Feature Configuration Information
Multihop VPDN	Cisco IOS XE Release 2.2	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.

Feature Name	Software Releases	Feature Configuration Information
Subscriber Service Switch	Cisco IOS XE Release 2.2.1	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: **multihop-hostname** and **vpdn search-order**.

Configuring Additional VPDN Features

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

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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, page 135
- MTU Tuning Using Path MTU Discovery, page 135
- MTU Tuning Using TCP MSS Advertising, page 136
- MTU Tuning Using PPP MRU Advertising, page 136

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, page 135. 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, page 138
- IP Precedence for VPDN Tunnels, page 138
- ToS Classification for VPDN Tunnels, page 138

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, page 138

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, page 139
- Associating a VPDN Group with a VPDN Template, page 140
- Disassociating a VPDN Group from the VPDN Template, page 141
- Configuring the VPDN Source IP Address, page 142

Creating a VPDN Template

Perform this task on the NAS or the tunnel server to create a VPDN template. If you remove a named VPDN template configuration, all VPDN groups that were associated with it will automatically be associated with the global VPDN template.

Note

- An L2TP tunnel must be established for the VPDN template settings to be used. Once a tunnel has been established, changes in the VPDN template settings will not have an effect on the tunnel until it is brought down and reestablished.
- Not all commands that are available for configuring a VPDN group can be used to configure a VPDN template. For a list of the commands that can be used in VPDN template configuration mode, use the **?** command in VPDN template configuration mode.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**vpdn-template** [*name*] **Example:** `Router(config)# vpdn-template l2tp`	Creates a VPDN template and enters VPDN template configuration mode.

Associating a VPDN Group with a VPDN Template

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

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

- Create and enable the VPDN template. For details, see the "Creating a VPDN Template" section.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**source vpdn-template** [*name*] **Example:** `Router(config-vpdn)# source vpdn-template l2tp`	Associates a VPDN group with a VPDN template. • VPDN groups are associated with the unnamed VPDN template by default. • If you have disassociated a VPDN group from the VPDN template using the **no source vpdn-template** command, you can reassociate it by issuing the **source vpdn-template** command. • Associating a VPDN group with a named VPDN template disassociates it from the global VPDN template.

Disassociating a VPDN Group from the VPDN Template

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**no source vpdn-template** [*name*] **Example:** `Router(config-vpdn)# no source vpdn-template l2tp`	Configures an individual VPDN group to use system default settings rather than the VPDN template settings for all unspecified parameters. • VPDN groups are associated with the unnamed VPDN template by default. Use the **no source vpdn-template** command to disassociate a VPDN group from its associated VPDN template. • If you have disassociated a VPDN group from the VPDN template using the **no source vpdn-template** command, you can reassociate it by issuing the **source vpdn-template** command.

Configuring the VPDN Source IP Address

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

- Configuring the Global VPDN Source IP Address, page 142
- Configuring the Source IP Address for a VPDN Group, page 143

Configuring the Global VPDN Source IP Address

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**vpdn source-ip** *ip-address* **Example:** `Router(config)# vpdn source-ip 10.1.1.1`	Globally specifies an IP address that is different from the physical IP address used to open a VPDN tunnel.

Configuring the Source IP Address for a VPDN Group

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**source-ip** *ip-address* **Example:** `Router(config-vpdn)# source-ip 10.1.1.1`	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.

Configuring VRF-Aware VPDN Tunneling

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

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

- Configuring VRF-Aware VPDN Tunneling Locally, page 144
- Configuring VRF-Aware VPDN Tunneling on the Remote RADIUS AAA Server, page 145

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.

- A multihop, dial-in, or dial-out L2TP VPDN tunneling deployment must be configured.
- The source IP address and the destination IP address configured in the L2TP VPDN group must exist in the specified VPN.
- Because VRFs use Cisco Express Forwarding, you must configure Cisco Express Forwarding before performing this task.

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

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

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

- A multihop, dial-in, or dial-out L2TP VPDN tunneling deployment must be configured.
- The source IP address and the destination IP address configured in the L2TP VPDN group must exist in the specified VPN.
- Because VRFs use Cisco Express Forwarding, you must configure Cisco Express Forwarding before performing this task.
- The NAS or tunnel switch must be configured for remote RADIUS AAA. Perform the tasks in the Configuring AAA on the NAS and the Tunnel Server and Configuring Remote AAA for VPDNs sections in the Configuring AAA for VPDNs module to configure the NAS for remote RADIUS AAA.

- The RADIUS server must be configured for AAA.

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose

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

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

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, page 148
- Enabling Automatic Adjustment of the IP MTU for VPDN Deployments, page 149

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.

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

SUMMARY STEPS

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

DETAILED STEPS

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

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.

- A VPDN deployment must be configured.

Note

- Automatic adjustment of the IP MTU is disabled by default.
- The IP MTU is automatically adjusted only if there is no IP MTU configured manually on the virtual template interface.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**ip mtu adjust** **Example:** `Router(config-vpdn)# ip mtu adjust`	Enables automatic adjustment of the IP MTU on a virtual access interface.

Enabling Path MTU Discovery for VPDNs

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

Caution When PMTUD is enabled, VPDN deployments are vulnerable to DoS attacks that use crafted ICMP messages to set a connection's path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. For more information on throughput-reduction attacks and for information on detecting a PMTUD attack on an L2TP VPDN deployment, see the "Additional References" section.

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

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

A VPDN deployment must be configured.

Note

- Cisco software releases remain vulnerable to throughput-reduction DoS attacks when PMTUD is enabled. The only way to protect against DoS attacks when running these versions of software is to disable PMTUD.
- The software does not support the **vpdn pmtu** command to configure a range of acceptable values for the path MTU, which can help protect against a throughput-reduction attack.

SUMMARY STEPS

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

DETAILED STEPS

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

Manually Configuring the Advertised TCP MSS

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

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

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

A VPDN deployment must be configured.

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring MRU Advertising

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

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

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

A VPDN deployment must be configured.

Note

- MRU negotiation must be supported on the PPP client. One known client that supports MRU negotiations is the Windows XP PPP client. Other commonly deployed PPP clients do not adhere to the advertised PPP MRU as they should. To determine if your PPP client properly responds to the advertised PPP MRU, see the PPP client documentation.
- Changing the MTU value for an interface with the **mtu** command can affect the value of the **ip mtu** command. The value specified with the **ip mtu** command must not be greater than the value specified with the **mtu** command. If you change the value for the **mtu** command and the new value would result in an **ip mtu** value that is higher than the new **mtu** value, the **ip mtu** value automatically changes to match the new value configured with the **mtu** command. Changing the value of the **ip mtu** commands has no effect on the value of the **mtu** command.
- If proxy Link Control Protocol (LCP) is running, LCP renegotiation must take place because the MRU option is set during LCP negotiations. To force LCP renegotiation, configure the **lcp renegotiation** command for the VPDN group.
- If the MTU is manually lowered for a tunnel server that communicates with a mixture of devices that do and do not listen to MRU advertising, those devices that do not listen might encounter the PMTUD issues discussed in the "Enabling Path MTU Discovery for VPDNs" section.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces and enters interface configuration mode.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1460`	Adjusts the maximum packet size or MTU size. **Note** Because Layer 2 headers are 40 bytes, the recommended value for the *bytes* argument is 1460.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.
Step 6	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	(Optional) Creates a VPDN group and enters VPDN group configuration mode.
Step 7	**lcp renegotiation** {**always** | **on-mismatch**} **Example:** `Router(config-vpdn)# lcp renegotiation always`	(Optional) Allows the tunnel server to renegotiate the PPP LCP on dial-in calls.

Configuring VPDN Group Selection

Configuring VPDN Group Selection Based on a Hostname

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dialin VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.

	Command or Action	Purpose
Step 6	**terminate-from hostname** *hostname* **Example:** `Router(config-vpdn-acc-in)# terminate-from hostname example`	Specify the hostname of the remote LAC or LNS that will be required when accepting a VPDN tunnel.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits VPDN accept dialin group configuration mode.

Configuring VPDN Group Selection Based on a Source IP Address

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dial-in VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**source-ip** *ip-address* **Example:** `Router(config-vpdn-acc-in)# source-ip 10.10.10.1`	Specifies a source IP addresses to which to map the destination IP addresses in subscriber traffic.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits a VPDN accept dialin group configuration mode.

Configuring VPDN Group Selection Based on VRF

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept dialin`	Creates a VPDN accept dialin group that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dialin calls, and enters accept dial-in VPDN subgroup configuration mode.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the tunneling protocol that a VPDN subgroup will use.
Step 6	**vpn vrf** *vrf-name* **Example:** `Router(config-vpdn-acc-in)# vpn vrf myvrf`	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified Virtual Private Network (VPN) routing and VRF instance. • **vrf** *vrf-name* --Specifies the VRF instance by the VRF name.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits accept dialin VPDN subgroup mode.

Displaying VPDN Group Selections

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring QoS Packet Classifications for VPDNs

Depending on the VPDN deployment, instead of using the default setting you can choose to configure your VPDN network to preserve QoS end to end by copying the contents of the ToS byte from the IP header to the Layer 2 header, or to manually configure custom packet classifications for the VPDN network.

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

Perform this task if you choose to preserve end-to-end QoS:

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

- Configuring Preservation of QoS Classifications in the ToS Byte, page 160
- Manually Configuring the IP Precedence for VPDNs, page 161
- Manually Configuring the ToS for VPDN Sessions, page 162

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.

A VPDN deployment must be configured.

Note

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**ip tos reflect** **Example:** `Router(config-vpdn)# ip tos reflect`	Configures a VPDN group to copy the ToS byte value of IP packet to the Layer 2 header.

Manually Configuring the IP Precedence for VPDNs

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

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

A VPDN deployment must be configured.

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**ip precedence** [*number* | *name*] **Example:** `Router(config-vpdn)# ip precedence 1`	Sets the precedence value in the VPDN Layer 2 encapsulation header.

Manually Configuring the ToS for VPDN Sessions

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

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

A VPDN deployment must be configured.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

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

Configuration Examples for Additional VPDN Features

Example Configuring a Global VPDN Template

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

```
vpdn-template
```

```
 local name host43
 ip tos reflect
```

Example Configuring a Named VPDN Template

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

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

Example Disassociating a VPDN Group from the VPDN Template

The following example disassociates the VPDN group named l2tp from the VPDN template. The system default settings will be used for all VPDN parameters that are not specified in the VPDN group configuration.

```
vpdn-group l2tp
 no source vpdn-template
```

Example Configuring a Global VPDN Source IP Address

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

```
vpdn source-ip 10.1.1.1
```

Example Configuring a Source IP Address for a VPDN Group

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

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

Example Configuring VRF-Aware VPDN Tunnels Locally

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

NAS

```
interface loopback 0
 ip address 172.16.45.6 255.255.255.255
!
vpdn enable
vpdn-group group1
 request-dialin
 protocol l2tp
 domain cisco.com
!
```

```
 initiate-to 10.10.104.9
 local name nas32
 source-ip 172.16.45.6
 l2tp tunnel password secret1
```

Multihop Tunnel Switch

```
ip vrf cisco-vrf
 vpn id A1:3F6C
!
interface loopback 0
 ip address 10.10.104.22 255.255.255.255
!
interface loopback 40
 ip vrf forwarding cisco-vrf
 ip address 172.16.40.241 255.255.255.255
!
vpdn enable
vpdn multihop
!
vpdn-group mhopin
 accept-dialin
 protocol l2tp
 virtual-template 4
!
 terminate-from hostname nas32
 source-ip 10.10.104.9
 l2tp tunnel password secret1
!
vpdn-group mhopout
 request-dialin
 protocol l2tp
 domain cisco.com
!
 vpn vrf cisco-vrf
 initiate-to ip 172.16.45.6
 source-ip 172.16.40.241
 local name multihop-tsw25
 l2tp tunnel password secret2
```

Tunnel Server

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

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

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

RADIUS User Profile--VRF Name

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

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

RADIUS User Profile--VRF ID

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

```
cisco.com Password = "secret"
      Service-Type = Outbound-User,
      cisco-avpair = "vpdn:tunnel-id=LAC",
      cisco-avpair = "vpdn:tunnel-type=l2tp",
      cisco-avpair = "vpdn:ip-addresses=10.0.0.1",
      cisco-avpair = "vpdn:source-ip=10.0.0.9",
      cisco-avpair = "vpdn:vpn-id=A1:3F6C"
      cisco-avpair = "vpdn:l2tp-tunnel-password=supersecret"
```

Example Manually Configuring the IP MTU for VPDN Deployments

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

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

Example Enabling Automatic Adjustment of the IP MTU for VPDN Deployments

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

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

Example Manually Configuring the Advertised TCP MSS

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

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

Example Configuring MRU Advertising

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

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

Example Configuring Preservation of QoS Classifications in the ToS Byte

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

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

Example Manually Configuring the IP Precedence for VPDNs

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

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

Example Manually Configuring the ToS for VPDN Sessions

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

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

Configuration Examples for VPDN Group Selection

Example Configuring VPDN Group Selection Based on Hostname

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

```
Router> enable
```

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

Example Configuring VPDN Group Selection Based on an IP Address

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

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

Example Configuring VPDN Group Selection Based on VRF

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

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

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

The following example configuration shows a LAC-1 building a VPDN tunnel to IP address 10.10.10.1, and the LNS terminating the session on vpdn-group 1. If LAC-1 builds a VPDN tunnel to IP address 10.10.10.2, the LNS terminates the session on vpdn-group 2. If LAC-2 builds a VPDN tunnel to IP addresses 10.10.10.1 or 10.10.10.2, the LNS terminates the session on vpdn-group 3.

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

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

Example Configuring VPDN Group Selection Based on Hostname and VRF

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

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

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

The following example configuration shows a LAC-1/LAC-2 sending an SCCRQ on vrf service-A to destination IP address 10.10.10.1, and the LNS terminating the VPDN tunnel on vpdn-group 1. If LAC-1/LAC-2 sends an SCCRQ on vrf service-A to destination IP address 10.10.10.2, the LNS terminates the VPDN tunnel on vpdn-group 2.

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

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

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

SCCRQ on vrf service-B to destination IP address 10.10.10.1, the LNS terminates the VPDN tunnel on vpdn-group 2.

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

Examples Displaying VPDN Group Selection

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

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

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group vgdefault
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 20
Router(config-vpdn-acc-in)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.2
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.3
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0
 example

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

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

- Examples Displaying VPDN Group-Select Summaries, page 171

Examples Displaying VPDN Group-Select Summaries

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

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

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

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

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

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

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

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

Where to Go Next

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VPDN technology overview	*VPDN Technology Overview*
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Information about QoS classification	Classification Overview module
QoS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Information on MTU tuning for L2TP tunneling deployments	MTU Tuning for L2TP
Information on IP packet fragmentation and PMTUD	IP Fragmentation and PMTUD
Information on throughput-reduction DoS attacks	Crafted ICMP Messages Can Cause Denial of Service

Standards

Standard	Title
None	--

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Additional VPDN Features

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

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

Table 12 Feature Information for Configuring Additional VPDN Features

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

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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, page 179

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, 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
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.

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, 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn softshut**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn softshut** **Example:** `Router(config)# vpdn softshut`	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

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 in to 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 in to the NAS using a second allowed username and password.
8. **show vpdn history failure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Establish a VPDN session by dialing in to the NAS using an allowed username and password.	
Step 2	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn session-limit** *sessions* **Example:** `Router(config)# vpdn session-limit 6`	Limits the number of simultaneous VPDN sessions globally on the router.

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.

- 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-template** [*name*] **Example:** `Router(config)# vpdn-template l2tp`	Creates a VPDN template and enters VPDN template configuration mode.
Step 4	**group session-limit** *sessions* **Example:** `Router(config-vpdn-templ)# group session-limit 6`	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group 1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**session-limit** *number* **Example:** `Router(config-vpdn)# session-limit 2`	Limits the number of sessions that are allowed through a specified VPDN group.

Verifying VPDN Session Limits

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

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

DETAILED STEPS

Step 1 **enable**

Enter this command to enable 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 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 in to the NAS using an allowed username and password.

Step 5 Attempt to establish a new VPDN session by dialing in to 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@scisco.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

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

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

	Command or Action	Purpose
Step 3	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group group1`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**l2tp tunnel hello** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel hello 90`	(Optional) Set the number of seconds between sending hello keepalive packets for an L2TP tunnel. • *seconds* --Time, in seconds, that the NAS and tunnel server will wait before sending the next L2TP tunnel keepalive packet. Valid values range from 0 to 1000. The default value is 60.
Step 5	**l2tp tunnel receive window** *packets* **Example:** `Router(config-vpdn)# l2tp tunnel receive window 500`	(Optional) Configures the number of packets allowed in the local receive window for an L2TP control channel. • *packets* --Number of packets allowed in the receive window. Valid values range from 1 to 5000. The default value varies by platform.
Step 6	**l2tp tunnel retransmit retries** *number* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit retries 8`	(Optional) Configures the number of retransmission attempts made for an L2TP control packet. • *number* --Number of retransmission attempts. Valid values range from 5 to 1000. The default value is 10.
Step 7	**l2tp tunnel retransmit timeout** {**min** | **max**} *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit timeout max 4`	(Optional) Configures the amount of time that the router will wait before resending an L2TP control packet. • **min** --Specifies the minimum time that the router will wait before resending a control packet. • **max** --Specifies the maximum time that the router will wait before resending a control packet. • *seconds* --Timeout length, in seconds, the router will wait before resending a control packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8.
Step 8	**l2tp tunnel timeout no-session** {*seconds* | **never**} **Example:** `Router(config-vpdn)# l2tp tunnel timeout no-session never`	(Optional) Configures the time a router waits after an L2TP tunnel becomes empty before tearing down the tunnel. • *seconds* --Time, in seconds, the router will wait before tearing down an empty L2TP tunnel. Valid values range from 0 to 86400. If the router is configured as a NAS, the default is 15 seconds. If the router is configured as a tunnel server, the default is 10. • **never** --Specifies that the router will never tear down an empty L2TP tunnel.

	Command or Action	Purpose
Step 9	**l2tp tunnel timeout setup** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel timeout setup 25`	(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. • *seconds* --Time, in seconds, the router will wait for a confirmation message. Valid values range from 60 to 6000. The default value is 10.
Step 10	**l2tp tunnel zlb delay** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel zlb delay 2`	(Optional) Configures the delay time before a zero length bit (ZLB) control message must be acknowledged. • *seconds* --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.
Step 11	**l2tp tunnel retransmit initial timeout** {**min** | **max**} *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit initial timeout min 2`	(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. **Note** Load balancing must be configured for the retry counter configured with the **l2tp tunnel retransmit initial timeout** command to take effect.
Step 12	**l2tp tunnel retransmit initial retries** *number* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit initial retries 5`	(Optional--Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release) 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. **Note** Load balancing must be configured for the retry counter configured with the **l2tp tunnel retransmit initial retries** command to take effect.
Step 13	**l2tp tunnel busy timeout** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel busy timeout 90`	(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, 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

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

	Command or Action	Purpose
Step 3	**l2tp congestion-control** **Example:** `Router(config)# l2tp congestion-control`	Enables L2TP congestion avoidance.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 5	**show vpdn tunnel l2tp all** **Example:** `Router# show vpdn tunnel l2tp all`	Displays information about all active L2TP VPDN tunnels.
Step 6	**debug vpdn l2x-events** **Example:** `Router(config)# debug vpdn l2x-events`	Displays troubleshooting information for protocol-specific VPDN tunneling events.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn history failure** **Example:** `Router(config)# vpdn history failure`	(Optional) Enables logging of VPDN failure events to the history failure table. **Note** 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.
Step 4	**vpdn history failure table-size** *entries* **Example:** `Router(config)# vpdn history failure table-size 50`	(Optional) Sets the history failure table size. **Note** The VPDN history failure table size can be configured only when VPDN failure event logging is enabled using the **vpdn history failure** command.
Step 5	**exit** **Example:** `Router# exit`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show vpdn history failure** **Example:** `Router# show vpdn history failure`	(Optional) Displays the contents of the history failure table.
Step 7	**clear vpdn history failure** **Example:** `Router# clear vpdn history failure`	(Optional) Clears the contents of the history failure 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

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

	Command or Action	Purpose
Step 3	**vpdn logging** [**accounting** | **local** | **remote** | **tunnel-drop** | **user**] **Example:** `Router(config)# vpdn logging remote`	(Optional) Enables the logging of generic VPDN events. • You can configure as many types of generic VPDN event logging as you want by issuing multiple instances of the **vpdn logging** command. **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 issue 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)# l2tp tunnel hello 90
Router(config-vpdn)# l2tp tunnel receive window 500
Router(config-vpdn)# l2tp tunnel retransmit retries 8
Router(config-vpdn)# l2tp tunnel retransmit timeout min 2
Router(config-vpdn)# l2tp tunnel timeout no-session 500
Router(config-vpdn)# l2tp tunnel timeout setup 25
Router(config-vpdn)# l2tp tunnel zlb delay 4
Router(config-vpdn)# l2tp tunnel retransmit initial timeout min 2
Router(config-vpdn)# l2tp tunnel retransmit initial retries 5
Router(config-vpdn)# l2tp 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

```
Router(config)# vpdn 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

```
Router(config)# vpdn 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>*.

```
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 queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 0, ZLB ACKs sent 2
  Current nosession 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

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
VPDN technology overview	VPDN Technology Overview module
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS VPDN Command Reference*
Technical support documentation for VPDNs	Virtual Private Dial-up Network (VPDN)
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*
Concepts and tasks associated with configuring additional VPDN features	Configuring Additional VPDN Features module

Standards

Standard	Title
TCP/IP; slow start and congestion avoidance algorithms	*TCP/IP Illustrated, Volume 1*

MIBs

MIB	MIBs Link
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer Two Tunneling Protocol (L2TP)*

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13 Feature Information for VPDN Tunnel Management

Feature Name	Releases	Feature Information
L2TP Congestion Avoidance	Cisco IOS XE Release 2.3	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: **debug vpdn**, **l2tp congestion-control**.

Feature Name	Releases	Feature Information
Session Limit per VRF	Cisco IOS XE Release 2.1	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: **group session-limit**, **source vpdn-template,** and **vpdn-template**.
Timer and Retry Enhancements for L2TP	Cisco IOS XE Release 2.1	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: **l2tp tunnel busy timeout**, **l2tp tunnel retransmit initial retries**, and **l2tp tunnel retransmit initial timeout**.
VPDN Group Session Limiting	Cisco IOS XE Release 2.1	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: **session-limit** (VPDN).

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

Note 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, page 207
- Adjusting Receive Window Size, page 207

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**mode sso** **Example:** `Router(config-red)# mode sso`	Specifies the mode of redundancy.
Step 5	**end** **Example:** `Router(config-red)# end`	Returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2tp sso enable** **Example:** `Router(config)# l2tp sso enable`	Enables L2TP HA SSO.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2tp sso enable** **Example:** `Router(config)# l2tp sso enable`	Enables L2TP SSO mode.
Step 4	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enters VPDN configuration mode.
Step 5	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group example`	Creates a VPDN group and enters VPDN group configuration mode.

	Command or Action	Purpose
Step 6	**sso enable** **Example:** `Router(config-vpdn)# sso enable`	Enables L2TP SSO for the VPDN group.
Step 7	**l2tp tunnel resync** *packets* **Example:** `Router(config-vpdn)# l2tp tunnel resync 4`	Configures the number of packets after an SSO, an L2TP HA tunnel sends before waiting for an acknowledgement.
Step 8	**l2tp tunnel retransmit retries** *number* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit retries 30`	Configures the number of retransmission attempts made for an L2TP control packet.
Step 9	**l2tp tunnel retransmit timeout min** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit timeout min 8`	Configures the amount of time that the router waits before resending an L2TP control packet.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enters VPDN configuration mode.
Step 4	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group example`	Creates a VPDN group and enters VPDN group configuration mode.
Step 5	**l2tp tunnel resync** *packets* **Example:** `Router(config-vpdn)# l2tp tunnel resync 250`	Specifies the number of packets to be processed after an SSO before an acknowledgment message is sent. This example specifies that 250 packets will process before an acknowledgment message is sent.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-vpdn)# end`	Returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show l2tp redundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]] **Example:** `Router# show l2tp redundancy all`	Display the status of L2TP session with redundancy data.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn redundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]] **Example:** `Router# show vpdn redundancy all`	Displays the status of VPDN session with checkpointed data.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug** {**l2tp** | **vpdn**} **redundancy** {**cf** | **detail** | **error** | **event** | **fsm** | **resync** | **rf**} **Example:** `Router# debug vpdn redundancy cf`	Displays debug information for VPDN session with redundancy data.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

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 resynchronous 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:
LocID      RemID      TunID     Waiting for    Waiting for
                                 VPDN app?     L2TP proto?
28017      10         33003        No             No
```

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VPDN commands	*Cisco IOS VPDN Command Reference*
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief
Stateful switchover and high availability	Configuring Stateful Switchover module
ISSU on Cisco ASR 1000 Series Routers	http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/issu.html
VPDN technology overview	VPDN Technology Overview module

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 2661	*Layer 2 Tunneling Protocol (L2TP)*
RFC 4591	Fail Over for Layer 2 Tunneling Protocol (L2TP)

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14 Feature Information for L2TP HA Session SSO/ISSU on a LAC/LNS

Feature Name	Releases	Feature Information
L2TP HA Session SSO/ISSU on a LAC/LNS	Cisco IOS XE Release 2.2 Cisco IOS XE Release 2.3 Cisco IOS XE Release 2.4	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: **debug l2tp redundancy**, **debug vpdn redundancy**, **l2tp sso enable**, **l2tp tunnel resync**, **show l2tp redundancy**, **show vpdn redundancy**, **sso enable**. 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.

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 15 L2TP Disconnect Cause Codes

Code	Description
Global Errors	
0	No information available. **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.
1	Administrative disconnect.
3	Normal disconnection, Link Control Protocol (LCP) Terminate-Request sent. Valid direction values are: • 1--LCP Terminate-Request sent by the peer device. • 2--LCP Terminate-Request sent by the local device.
LCP Errors	
5	Finite State Machine (FSM) timeout error.
6	No recognizable LCP packets were received.
8	LCP link failure: Echo Request timeout.
9	The peer has an unexpected endpoint-discriminator for an existing Multilink PPP (MLP) bundle.

Code	Description
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	
13	FSM timeout error.
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	
17	FSM timeout error.
18	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.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Information about configuring L2TP VPDN tunnels	VPDN Tunnel Management module
VPDN commands	*Cisco IOS VPDN Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3145	L2TP Disconnect Cause Information

Technical Assistance

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

Feature Information for 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 16 Feature Information for the L2TP Disconnect Cause Information Feature

Feature Name	Releases	Feature Information
L2TP Disconnect Cause Information	Cisco IOS XE Release 2.1	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.