



VRF-Aware VPDN Tunnels

Last Updated: April, 2007

The VRF-Aware VPDN Tunnels feature provides support for VPDN tunnels that terminate on a VPN routing and forwarding (VRF) instance by allowing you to use a VRF address from a VRF routing table as the destination address. Previously, you had to specify a global IP address for the destination address for a virtual private dial-up network (VPDN) tunnel.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for VRF-Aware VPDN Tunnels](#)” section on page 12.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for VRF-Aware VPDN Tunnels, page 2](#)
- [Restrictions for VRF-Aware VPDN Tunnels, page 2](#)
- [Information About VRF-Aware VPDN Tunnels, page 2](#)
- [How to Configure VRF-Aware VPDN Tunnels, page 4](#)
- [Configuration Examples for VRF-AWARE VPDN Tunnels, page 7](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)
- [Feature Information for VRF-Aware VPDN Tunnels, page 12](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 13](#)



Americas Headquarters:

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

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for VRF-Aware VPDN Tunnels

Cisco 7000 Series Router Prerequisite

Because VRF instances use Cisco Express Forwarding (CEF), you must configure CEF before configuring the VRF-Aware VPDN Tunnels feature.

**Note**

CEF is on by default on the Cisco 10000 series router and it cannot be turned off. If you attempt to enable CEF, an error message appears.

Restrictions for VRF-Aware VPDN Tunnels

Cisco 7000 Series Router Restriction

- The VRF-Aware VPDN Tunnels feature can only be used with Layer 2 Tunnel Protocol (L2TP).

Cisco 10000 Series Router Restrictions

- The VRF-Aware VPDN Tunnels feature can only be used with Layer 2 Tunnel Protocol (L2TP) on the L2TP access concentrator (LAC). The reason is that the Cisco 10000 series router can only initiate tunnels in a VRF instance; it cannot terminate tunnels that arrive in a VRF instance. Therefore, this feature does not apply to the Cisco 10000 series router when the router is acting as the L2TP network server (LNS) because, as the LNS, the Cisco 10000 series router cannot terminate tunnels that arrive in a VRF instance.
- For multihop configuration in Cisco IOS Release 12.3(7)XI7 and later releases, the ingress tunnel also needs to arrive in the global routing table, but the tunnel can be switched out into a VRF instance towards the final LNS destination.

Information About VRF-Aware VPDN Tunnels

To configure the VRF-Aware VPDN Tunnels feature, you need to understand the following concepts:

- [How VRF-Aware VPDN Tunnels Work, page 3](#)
- [PPP Sessions That Are Forwarded over the VPDN Tunnel, page 3](#)
- [Benefits of Using the VRF-Aware VPDN Tunnels Feature, page 4](#)

**Note**

The Cisco 10000 series router supports the VRF-Aware VPDN Tunnels with the Layer 2 Tunnel Protocol (L2TP) on the L2TP access concentrator (LAC). As the LAC, the router supports the termination of tunnels in a virtual private network (VPN) routing and forwarding (VRF) instance. The Cisco 10000 series router supports the VRF-Aware VPDN Tunnels feature on the PRE2 and PRE3.

How VRF-Aware VPDN Tunnels Work

Before Cisco IOS Release 12.2(15)T, you had to specify a global IP address from a global VRF instance for the destination and sources addresses of a VPDN tunnel. The VRF-Aware VPDN Tunnels feature enhances the support of VPDN tunnels by allowing VPDN tunnels to start outside the Multiprotocol Label Switching (MPLS) VPN and terminate within the MPLS VPN. For example, this feature allows you to use a VRF address from a customer VRF instance as the destination address.

You can use the VRF-Aware VPDN Tunnels feature for dial-in and dial-out. In addition to configuring this feature on the multihop node, you can configure this feature on the L2TP access concentrator (LAC).

**Note**

You can configure VRF-aware VPDN tunnels only on the LAC and the multihop node. The Cisco 10000 series router requires tunnels to *arrive* in the global routing table, not in a VRF instance. However tunnels may start (using the LAC) or re-originate (using multihop) in a VRF instance.

The VRF-Aware VPDN Tunnels feature is sometimes referred to as VRF-Aware VPDN Multihop. Unlike a LAC/LNS deployment where the LAC initiates a tunnel that is terminated by an LNS, multihop allows an intermediate node to switch a tunnel. This means that the tunnel is terminated and forwarded to its final LNS destination. The VRF awareness of the feature allows the tunnel to be switched out into a VRF instance. Therefore, the final destination LNS is found in a VRF instance, instead of the global routing table. For example, wholesale providers can switch the tunnel received from the first-level Internet service provider (ISP) to their customers and the LNS is found using an MPLS cloud of the wholesale provider's ISP.

**Note**

Because the Cisco 10000 series router is a PFX-based platform, all tunnel switching is done without route processor (RP) involvement. However, tunnel establishment is done by the RP.

PPP Sessions That Are Forwarded over the VPDN Tunnel

When the VRF-Aware VPDN Tunnels feature has been configured on an LNS that has VPN knowledge and acts as a PE, the PPP sessions that are being forwarded over the VPDN tunnel to the LNS do not necessarily need to belong to the VPN routing table to which the VPDN tunnel belongs. The PPP peer at the other end negotiating IP will eventually be placed in a certain routing table, depending on the VRF instance specified when the **ip vrf forwarding** command has been entered for authentication. If no VRF command is received during the authorization and authentication of the forwarded PPP session, the host route for the PPP session will be inserted into the global routing table.

**Note**

If the Cisco 10000 series router is acting as the LNS (which is terminating the tunnel that arrives in a VRF instance), the VRF-Aware VPDN Tunnels feature cannot be applied because the Cisco 10000 series router requires tunnels to *arrive* in the global routing table. The router supports VRF-aware VPDN tunnels only on the LAC.

For more information on remote access to MPLS VPN and how to insert your PPP session in a certain VPN, refer to the “Overview of Dial Access to MPLS VPN Integration” chapter of the *Cisco Remote Access to MPLS VPN Integration 2.0 Overview and Provisioning Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/ramp2/ovprov/ra_op_02.htm

Benefits of Using the VRF-Aware VPDN Tunnels Feature

The ability to use VRF addresses for destination and source addresses matches current network design. For instance, Internet service providers (ISPs) support VRF and have one VRF routing table per customer. The VRF-Aware VPDN Tunnels features allows for the creation of VPDN tunnels that use the customer VRF address as the tunnel endpoint.

How to Configure VRF-Aware VPDN Tunnels

You can configure VRF-aware VPDN tunnels either in a local VPDN group or by updating the RADIUS server profile definitions for VPDN tunnel attributes. This section contains the following tasks:

- [Configuring VRF-Aware VPDN Tunnels Locally, page 4](#)
- [Configuring VRF-Aware VPDN Tunnels by Updating the RADIUS Server Profile Definitions for the VPDN Tunnel Attributes, page 6](#)
- [Verifying VRF-Aware VPDN Tunnels, page 6](#)

Configuring VRF-Aware VPDN Tunnels Locally

To configure VRF-Aware VPDN Tunnels locally, perform these steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **request-dialin**
5. **protocol** [*l2f* | *l2tp* | *pptp*]
6. **domain** *domain-name*
7. **exit**
8. **vpn** { **vrf** *vrf-name* | **id** *vpn-id* }
9. **source-ip** *ip-address*
10. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]
11. **exit**



Note

For Cisco IOS Release 12.2(31)SB5 and later releases, when configuring VRF-aware VPDN tunnels on the Cisco 10000 series router, different tunnels can have overlapping IP addresses across VRF instances.

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 vpdngroup1	Selects the VPDN group to configure and enters VPDN group configuration mode. <i>name</i>—The name of the VPDN group to be configured.
Step 4	request-dialin Example: Router(config-vpdn)# request-dialin	Enters VPDN request-dialin configuration mode and enables the router to accept dial-in requests.
Step 5	protocol [l2f l2tp pptp] Example: Router(config-vpdn-req-in)# protocol l2tp	Specifies which tunneling protocol will be used. l2f—Layer 2 Forwarding (L2F) tunnels. l2tp—Layer 2 Transport Protocol (L2TP). pptp—Point-to-Point Tunneling Protocol. Note Only L2TP is supported for this feature.
Step 6	domain domain-name Example: Router(config-vpdn-req-in)# domain V1.40.com	Specifies the domain name of users that are to be forwarded to a tunnel server using a VPDN. And initiates a tunnel based on the LAC-supplied domain name. <i>domain-name</i>—Case-sensitive name of the domain that will be tunneled.
Step 7	exit Example: Router(config-vpdn-req-in)# exit	Returns to VPDN group configuration mode.
Step 8	vpn {vrf vrf-name id vpn-id} Example: Router(config-vpdn)# vpn vrf vrf-first	Specifies that the source and destination IP addresses of a given VPDN group belong to the specified VRF. Note Before you can issue the vpn command, the VRF instance information must be previously created using the ip vrf command.
Step 9	source-ip ip-address Example: Router(config-vpdn)# source-ip 172.0.0.21	Specifies the source IP address to be used for the tunnel. The source address should exist in the VPN that is specified in Step 8. Note The L2TP source and destination IP addresses must reside in the same VPN network.

	Command or Action	Purpose
Step 10	initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>] Example: Router(config-vpdn)# initiate-to ip 172.0.0.3	Specifies the destination IP address that will be tunneled to. The destination IP address should exist in the VPN that has been specified in Step 8. Note In order to select a source IP that belongs to the MPLS VPN, configure at least one IP address on the router that belongs to the VPN, or else you will not have IP connectivity.
Step 11	exit Example: Router(config-vpdn)# exit	Exits VPDN group configuration mode. Enter exit again to exit from global configuration mode and return to privileged EXEC mode.

Troubleshooting Tips

For information on troubleshooting, refer to the *Layer 2 Tunnel Protocol Technology Brief* document at the following URL:

http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm

Configuring VRF-Aware VPDN Tunnels by Updating the RADIUS Server Profile Definitions for the VPDN Tunnel Attributes

You can configure the VRF-Aware VPDN Tunnels feature by updating the VPDN tunnel attributes within the RADIUS server profile.



Note

For the Cisco 10000 series router, remotely configured VPDN groups can be used when you are configuring the LAC and not the LNS. When you terminate sessions, you can retrieve a VPDN group configuration from the RADIUS server.

You can specify the VPDN group either by its VPN ID or by the name of the associated VRF as follows:

cisco-avpair "vpdn:vpn-id=<vpn-id>"

cisco-avpair "vpdn:vpn-vrf=<vrf-name>"

For an example of an updated RADIUS record, see the [“AAA RADIUS: Examples”](#) section on page 9.

Verifying VRF-Aware VPDN Tunnels

To verify the configuration of the VRF-Aware VPDN Tunnels feature, use the following commands:

SUMMARY STEPS

1. **enable**
2. **show ip route vrf** *vrf-name*
3. **show vpdn session**
4. **show vpdn tunnel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	show ip route vrf <i>vrf-name</i> Example: Router# show ip route vrf vrf-first	Displays the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance.
Step 3	show vpdn session Example: Router# show vpdn session	Displays information about active L2TP or L2F sessions in a VPDN.
Step 4	show vpdn tunnel Example: Router# show vpdn tunnel	Displays information about active L2TP or L2F tunnels in a VPDN.

Configuration Examples for VRF-AWARE VPDN Tunnels

This section provides the following configuration examples to show how the VRF-Aware VPDN Tunnels feature might be configured:

- [Locally Configuring and Verifying VRF-Aware VPDN Tunnels: Example, page 7](#)
- [AAA RADIUS: Examples, page 9](#)

Locally Configuring and Verifying VRF-Aware VPDN Tunnels: Example

The following two sets of platform-specific examples show the VRF-Aware VPDN Tunnels feature configured on a multihop PE router that connects a LAC to a remote customer edge (CE) router and LNS.

Cisco 7000 Series Router Examples

LAC Configuration

```
interface loopback 0
 ip address 172.1.45.6 255.255.255.255
!
vpdn enable
vpdn group V1.40
 request-dialin
  protocol l2tp
  domain V1.40.com
 initiate-to 10.10.104.9
 local name lac-V1.40
 source-ip 172.1.45.6
 l2tp tunnel password west
```

Multihop PE Configuration

```
ip vrf v1.40.com
 vpn id 22:4444
interface loopback 0
 ip address 10.10.104.22 255.255.255.255
interface loopback 40
 ip vrf forwarding V1.40.com
 ip address 172.1.40.241 255.255.255.255
!
vpdn enable
vpdn multihop
vpdn group V1.40
 accept-dialin
  protocol l2tp
  virtual-template 4
 terminate-from hostname lac-V1.40
 source-ip 10.10.104.9
 l2tp tunnel password west
vpdn group V1.40_2
 request-dialin
  protocol l2tp
  domain V1.40.com
 vpn vrf V1.40.com
 initiate-to ip 172.1.45.6
 source-ip 172.1.40.241
 local name multihop-V1.40
 l2tp tunnel password test
```

Remote CE or LNS Configuration

```
interface loopback 0
 ip address 172.1.45.6 255.255.255.255
vpdn enable
vpdn group V1.40_2
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname multihop-V1.40
 source-ip 172.1.45.6
 local name remote-LNS-V1.40
 l2tp tunnel password test
```

When the **show vpdn tunnel** command is entered, the output shows the tunnel information as follows:

```
Router# show vpdn tunnel
```

```
l2tp Tunnel Information Totals tunnels 2 sessions
LocID   RemID   Remote Name   State   Remote Address  Port   Sessions   VPDN Group
9390    3222    lac-V1.40     est     10.10.104.10    1701   1           V1.40
53273   52035   remote-LNS-V1.40 est     172.1.45.6      1701   1           V1.40_2
```

AAA RADIUS: Examples

The following examples show the VRF-Aware VPDN Tunnels feature being configured for a service provider network. The AAA RADIUS server has a user profile that defines VPDN tunnel attributes. By either defining the VRF name or the VPN ID, you can specify that the source and destination IP addresses belong to the VPN.

RADIUS Users File with VRF Name Defined

For the following example, the VRF name “vpn-first” has been defined to specify the source and destination IP addresses that belong to the VPN.

```
west.com Password = "west"
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=labtunnel"
```

RADIUS Users File with VRF ID Defined

For the following example, the VPN ID “A1:3F6C” has been defined to specify the source and destination IP addresses that belong to the VPN.

```
west.com Password = "west"
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=labtunnel"
```

Additional References

The following sections provide references related to the VRF-Aware VPDN Tunnels feature.

Related Documents

Related Topic	Document Title
Dial commands	<i>Cisco IOS Dial Technologies Command Reference, Release 12.2.</i>
L2TP tunneling	<i>Layer 2 Tunnel Protocol</i>

Related Topic	Document Title
MPLS VPNs	<i>Cisco Remote Access to MPLS VPN Integration 2.0 Overview and Provisioning Guide.</i>
VPDN	<i>Cisco IOS Dial Technologies Configuration Guide, Release 12.2;</i> see the part “Virtual Templates, Profiles, and Networks.

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
None	—

Technical Assistance

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

Command Reference

This section documents the following new command:

- **vpn**

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn { **vrf** *vrf-name* | **id** *vpn-id* }

no vpn

Syntax Description	vrf <i>vrf-name</i>	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
	id <i>vpn-id</i>	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default VPDN groups are not associated with a VRF.

Command Modes VPDN group configuration
VPDN template configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.

Usage Guidelines Use the **vpn** command to configure the Cisco IOS software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
```

```

request-dialin
protocol l2tp
!
vpn vrf vrf-second
source-ip 172.16.1.9
initiate-to ip 172.16.1.1

```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```

vpdn-group group2
 request-dialin
 protocol l2tp
!
vpn id 11:2222
source-ip 172.16.1.9
initiate-to ip 172.16.1.1

```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

Feature Information for VRF-Aware VPDN Tunnels

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for VRF-Aware VPDN Tunnels**

Feature Name	Releases	Feature Information
VRF-Aware VPDN Tunnels	12.2(15)T 12.3(7)XI7 12.2(28)SB 12.2(31)SB2	This feature provides support for VPDN tunnels that terminate on VPN routing and forwarding (VRF) instance by allowing you to use a VRF address from a VRF routing table as the destination address. In Cisco IOS Release 12.2(15)T, this feature was introduced on the Cisco 7200 series and Cisco 7400 series routers. In Cisco IOS Release 12.3(7)XI7, this feature was implemented on the Cisco 10000 series router for the LAC. The domain <i>domain-name</i> configuration step was added. In Cisco IOS Release 12.2(28)SB, this feature was integrated into the Release 12.2SB software. In Cisco IOS Release 12.2(31)SB2, this feature was implemented on the PRE3 for the Cisco 10000 series router. The following commands were introduced or modified by this feature: vpn.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.