



Large-Scale Dial-Out (LSDO) VRF Aware

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the LSDO VRF Aware feature in Cisco IOS Release 12.2(8)T and includes the following sections:

- [Feature Overview, page 1191](#)
- [Supported Platforms, page 1193](#)
- [Supported Standards, MIBs, and RFCs, page 1193](#)
- [Prerequisites, page 1194](#)
- [Configuration Tasks, page 1194](#)
- [Configuration Examples, page 1195](#)
- [Command Reference, page 1196](#)
- [Glossary, page 1196](#)

Feature Overview

Currently, the Cisco large-scale dial-out (LSDO) feature is not supported in a Multiprotocol Label Switching (MPLS) virtual private network (VPN), which means it does not support tunneling protocols and cannot take advantage of cost benefits inherent in an MPLS VPN. (See the sections “[Benefits](#)” and the “[Related Documents](#)” for more details on the benefits of MPLS VPN.) Beginning with Cisco IOS Release 12.2(8)T, large-scale dial-out will support the Layer 2 Tunnel Protocol (L2TP) in an MPLS VPN.

The basic operation of large-scale dial-out relies on per-user static routes stored in an authentication, authorization, and accounting (AAA) server, and redistributed static and redistributed connected routes to put better routes pointing to the same remote network or host on the alternate network access server (NAS).



A static route is manually configured on a NAS. If the static route that pointed to the next hop of the NAS has a name, that name with the -out suffix attached becomes the profile name.

When a packet arrives on a dialer interface where a static map is not configured, the dial string is retrieved from the AAA server. The query made to the AAA server is based on the destination IP address of the packet received.

When using L2TP VPN large-scale dial-out, overlapping IP addresses are often present in virtual routing and forwarding instances (VRFs), so that a unique key is needed to retrieve the correct route from the AAA server. With VPDN as a dial-out resource, a virtual access interface is created for maintaining each PPP session. Software prior to Cisco IOS Release 12.2(8)T did not update the VRF information on the virtual access interface; rather, this information was cloned from the dialer interface.

In the Cisco IOS Release 12.2(8)T software, the VRF table identifier is retrieved from the incoming packet and is mapped to the VRF name. This VRF name and the destination IP address are combined to make the unique key needed to retrieve the dial string and other user profile information from the AAA server. When response from the AAA server is received and the virtual access interface is created, the virtual access interface is updated with VRF information that was retrieved from the incoming packet. As with profile names on dialer interfaces, the IP address and VRF name combination with the -out suffix attached becomes the profile name for large-scale dial-out in MPLS VPN using L2TP.

**Note**

Another way to build a unique key is to use the name of the IP route. In this situation, the key is made from the IP route name and VRF name combination with the -out suffix attached. Refer to the technical note listed in the [“Related Documents”](#) section for more information.

Benefits

Layer 2 Tunneling Technologies Trim Costs by Forwarding Calls over the Internet

Access VPNs use Layer 2 tunneling technologies to create a virtual point-to-point connection between users and the customer network. These tunneling technologies provide the same direct connectivity as the expensive Public Switched Telephone Network (PSTN) by using the Internet. Instead of connecting directly to the network by using the PSTN, access VPN users need only use the PSTN to connect to the Internet service provider (ISP) local point of presence (POP). The ISP then uses the Internet to forward users from the POP to the customer network. Forwarding a user call over the Internet provides cost savings for the customer.

The MPLS VPN Model Simplifies Network Routing Configuration

The MPLS VPN model simplifies network routing by allowing VPN services to be supported in service provider networks. An MPLS VPN user can generally employ the backbone of the service provider as the default route in communicating with all of the other VPN sites.

The customer outsources the responsibility for the information technology (IT) infrastructure to an ISP that maintains the pool of modems the remote users dial in to, the access servers, and the internetworking expertise. The customer is responsible only for authenticating its users and maintaining its network.

L2TP Large-Scale Dial-Out Benefits from MPLS VPN Environment

The unique key created from the VRF name and the destination IP address allows retrieval of the dial string and other user profile information from a AAA server using L2TP in an MPLS VPN environment.

Restrictions

Cisco IOS Release 12.2(8)T supports *only* L2TP large-scale dial-out, and this feature makes it possible to retrieve *only* the dialer string that large-scale dial-out needs to construct the dynamic dialer map. This feature cannot create virtual access interfaces in the large-scale dial-out environment.

Related Documents

Additional information about configuring networks that can take advantage of this feature can be found in the following Cisco IOS documentation:

- [Cisco IOS Dial Technologies Command Reference](#), Release 12.2.
- [Cisco IOS Dial Technologies Configuration Guide](#), Release 12.2. Refer to the chapter “Configuring Large-Scale Dial-Out” in the part “Dial Access Specialized Features,” and the chapter “Configuring Virtual Private Networks” in the part “Virtual Templates, Profiles, and Networks.”
- [Cisco IOS Switching Services Command Reference](#), Release 12.2.
- [Cisco IOS Switching Services Configuration Guide](#), Release 12.2. Refer to the chapter “Multiprotocol Label Switching Overview” in the part “Multiprotocol Label Switching.”

Supported Platforms

Use Cisco’s Feature Navigator tool to determine which platforms support the Asynchronous Line Monitoring feature.

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Prerequisites

No new Cisco IOS commands are introduced with the Asynchronous Line Monitoring feature feature. Before configuring this feature, read through the chapters listed in the “[Related Documents](#)” section, to be sure you know how to configure VPDNs, dialer interfaces, and MPLS, then use the examples in the section “[Configuration Examples](#)” to help you determine the configuration you need for your network.

Configuration Tasks

No new configuration tasks are required for configuring the Asynchronous Line Monitoring feature feature. See the sections “[Prerequisites](#)” and “[Related Documents](#)” for more information.

Monitoring and Maintaining Asynchronous Line Monitoring feature

**Note**

Effective with Cisco Release 12.4(11)T, the **L2F protocol** was removed in Cisco IOS software.

To monitor and maintain Asynchronous Line Monitoring feature feature, use the following EXEC commands:

Command	Purpose
Router# show dialer	Displays general diagnostic information for interfaces configured for DDR.
Router# show ip protocols vrf	Displays the routing protocol information associated with a VRF.
Router# show ip route vrf	Displays the IP routing table associated with a VPN routing and VRF forwarding instance.
Router# show ip vrf	Displays the set of defined VRF instances and associated interfaces.
Router# show vpdn	Displays information about active L2F protocol tunnel and L2F message identifiers in a VPDN.
Router# show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.

Command	Purpose
Router# <code>show vpdn group</code>	Displays a summary of the relationships among VPDN groups and customer or VPDN profiles, and summarizes the configuration of a VPDN group including domain or DNIS, loadsharing information, and current session information.
Router# <code>show vpdn history failure</code>	Displays the content of the failure history table.
Router# <code>show vpdn multilink</code>	Displays the multilink sessions authorized for all VPDN groups.
Router# <code>show vpdn session</code>	Displays information about active L2TP or L2F sessions in a VPDN.
Router# <code>show vpdn tunnel</code>	Displays information about active L2TP or L2F tunnels in a VPDN.

Configuration Examples

This section contains partial sample configurations of the Asynchronous Line Monitoring feature. (Additional examples can be found in the technical note listed in the [“Related Documents”](#) section.)

In the following examples, VRF VPN_A has two hosts with the IP address 1.1.1.1 and 2.2.2.2 and, similarly, VRF VPN_B has two hosts with IP address 1.1.1.1 and 2.2.2.2. The AAA server is configured with a list containing “10.10.10.10-VPN_A-out” and “10.10.10.10-VPN_B-out” as keys to search on.



Note

The network addresses used in the following configuration are examples only and will not work if tried in an actual network configuration.

LNS Configuration

This partial example configures L2TP dial-out tunnels to an L2TP access concentrator (LAC) from an L2TP network server (LNS):

```
request-dialout
  protocol l2tp
  rotary-group 1
! LAC IP address:
  initiate-to ip 172.16.0.2
  local name PE2_LNS
  l2tp tunnel password 7 13!9@61&
```

Dialer Configuration

This partial example configures the dialer interface:

```
interface Dialer 1
! Global IP address:
  ip address 10.10.10.10
  encapsulation ppp
  dialer in-band
  dialer aaa
  dialer vpdn
  dialer-group 1
  ppp authentication chap
```

Routing Configuration

This partial example configures the VRF static routes:

```
ip route vrf VPN_A 1.1.1.1 255.255.255.255 Dialer1
ip route vrf VPN_A 2.2.2.2 255.255.255.255 Dialer1
```

```
ip route vrf VPN_B 1.1.1.1 255.255.255.255 Dialer1
ip route vrf VPN_B 2.2.2.2 255.255.255.255 Dialer1
```

Command Reference

This feature uses no new or modified commands. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Glossary

L2TP—Layer 2 Tunnel Protocol. A tunneling protocol that permits separating the remote access network function—terminating the PSTN circuit, for example—from the local network access operations such as authenticating and authorizing the remote user.

L2TP access concentrator—See LAC.

L2TP network server—See LNS.

LAC—L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol. The connection from the LAC to the remote system is either local or a PPP link.

Layer 2 Tunnel Protocol—See L2TP.

LNS—L2TP network server. A device that terminates an L2TP tunnel. It receives the remote user PPP connection over an L2TP tunnel. The LNS authenticates and authorizes the remote user and then forwards packets between the remote user and the data network.

MPLS—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on pre-established IP routing information.

Multiprotocol Label Switching—See MPLS.

NAS—network access server. A device that provides local network access to users across a remote access network such as the PSTN. For example, a NAS may provide access to a user dialing in from the PSTN to the data network, that is, it terminates the PSTN circuit, terminates the remote user PPP session, authenticates and authorizes the remote user, and finally forwards packets between the remote user and the data network.

network access server—See NAS.

virtual private dialup network—See VPDN.

virtual routing and forwarding instance—See VRF.

VPDN—virtual private dialup network. A type of access VPN that uses PPP to interface with the subscriber. VPDN enables the service provider to configure VPNs across an IP access network that connects to the VRFs on a PE. VPDN uses the Layer 2 Tunnel Protocol (L2TP) to extend or "tunnel" a PPP session across the IP access network.

VRF—virtual routing and forwarding instance. Identifies a separate VPN within a particular MPLS VPN network domain.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.

© 2007-2008 Cisco Systems, Inc. All rights reserved.

