Remote Access MPLS VPNs

The Remote Access MPLS VPNs feature allows the service provider to offer a scalable end-to-end Virtual Private Network (VPN) service to remote users. This feature integrates the Multiprotocol Label Switching (MPLS)-enabled backbone with broadband access capabilities.

Finding Feature Information

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

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

Prerequisites for Remote Access MPLS VPNs

- Your network must be running the following Cisco services before you configure Virtual Private Network (VPN) operation:
  - Multiprotocol Label Switching (MPLS) in the service provider backbone devices
  - Tag Distribution Protocol (TDP) or the Label Distribution Protocol (LDP)
  - Border Gateway Protocol (BGP) in all devices providing a VPN service
  - Cisco Express Forwarding switching in each MPLS-enabled device

- The provider edge (PE) devices that belong to the same VPN must be configured with the same VPN ID. The VPN ID must be unique to the service provider network.

Restrictions for Remote Access MPLS VPNs

- The Virtual Private Network (VPN) ID is not used to control the distribution of routing information or to associate IP addresses.

Information About Remote Access MPLS VPNs

Introduction to Remote Access MPLS VPNs

Multiprotocol Label Switching (MPLS)-based Virtual Private Networks (VPNs) allow service providers to deploy a scalable and cost-effective VPN service that provides a stable and secure path through the network. An enterprise connects to geographically dispersed sites in the Internet service provider's (ISPs) network through use of an MPLS backbone. Sites are interconnected to create an MPLS VPN.

The Remote Access MPLS VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. The Remote Access MPLS VPNs feature integrates the MPLS-enabled backbone with broadband access capabilities. By integrating access VPNs with MPLS VPNs, a service provider can:

- Enable remote users and offices to seamlessly access their corporate networks
- Offer equal access to a set of different ISPs or retail service providers
- Integrate their broadband access networks with the MPLS-enabled backbone
- Provide end-to-end VPN service to enterprise customers with remote access (RA) users and offices
- Separate network access and connectivity functions from ISP functions

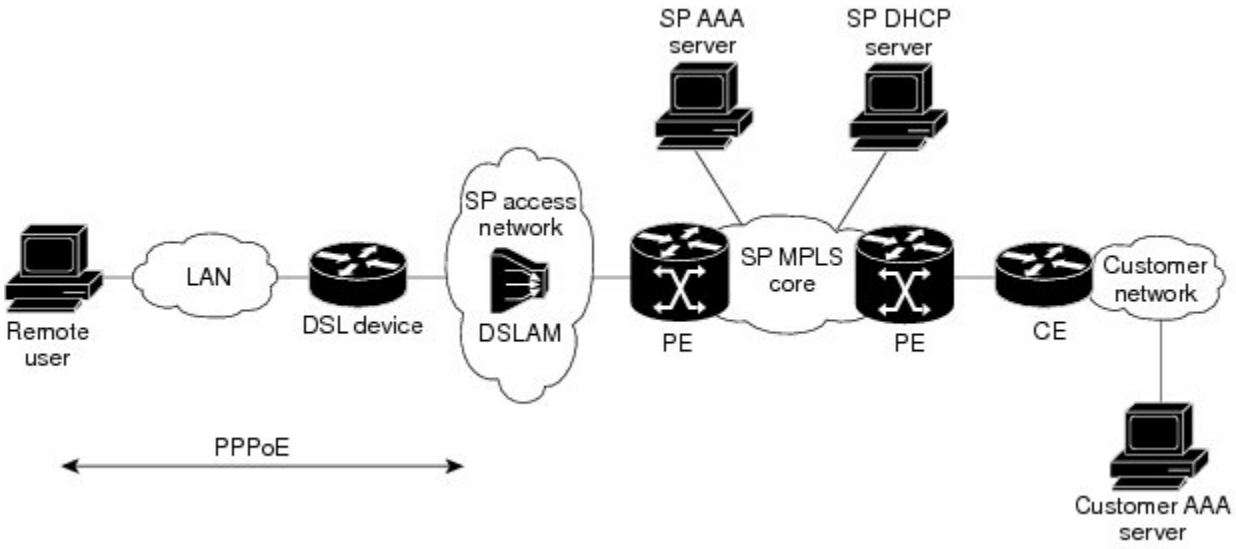
MPLS VPN Architecture

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) architecture enables the service provider to build the MPLS VPN network one time and add VPNs for new customers as needed, including them in the already established network. The elements that comprise the MPLS VPN are:

- Customer edge (CE) devices--The devices to which subscribers in a customer's network connect. The CE device connects to a service provider's edge device (PE device). The CE device initiates the remote access session to the PE device.
- Provider edge (PE) devices--The devices located at the edge of the service provider's MPLS core network. The PE device connects to one or more CE devices and has full knowledge of the routes to the VPNs associated with those CE devices. The PE device does not have knowledge of the routes to VPNs whose associated CE devices are not connected to it.
- Provider (P) devices--The service provider devices that comprise the provider's core network. The P devices do not assign VPN information and they do not have any knowledge of CE devices. Instead, the main focus of the P device is on label switching.

The figure below shows an example of MPLS VPN network architecture.

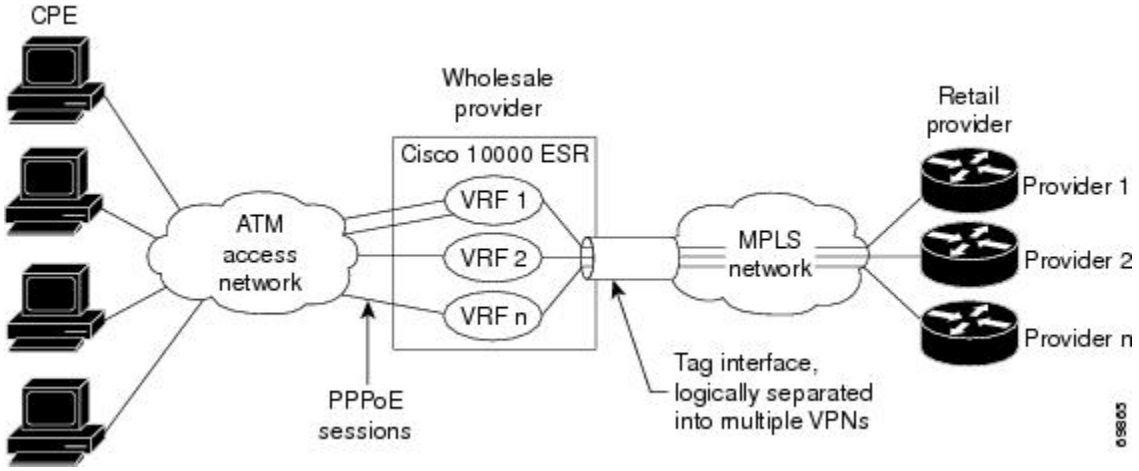
Figure 1: MPLS VPN Network Example



PPP over Ethernet to MPLS VPN

The figure below shows the topology of integrated PPP over Ethernet (PPPoE) access to an Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

Figure 2: PPPoE Access to MPLS VPN Topology



In the figure above, the service provider operates an MPLS VPN that interconnects all customer sites. The service provider's core network is an MPLS backbone with VPN service capability. The service provider provides all remote access operations to its customer. The network-side interfaces are tagged interfaces, logically separated into multiple VPNs.

Remote access is provided using a PPPoE connection. In this model, when a remote user attempts to establish a connection with a corporate network, a PPPoE session is initiated and is terminated on the service provider's

virtual home gateway (VHG) or provider edge (PE) device. All remote hosts connected to a particular customer edge (CE) device must be part of the VPN to which the CE device is connected.

The PPPoE to MPLS VPN architecture is a flexible architecture with the following characteristics:

- A remote host can create multiple concurrent PPPoE sessions, each to a different VPN.
- If multiple remote hosts exist behind the same CE device, each remote host can log in to a different VPN.
- Any remote host can log in to any VPN at any time because each VHG or PE device has the virtual routing and forwarding (VRF) instances for all possible VPNs preinstantiated on it. This configuration requires that the VRF be applied through the RADIUS server, which can cause scalability issues.

The following events occur as the VHG or PE device processes the incoming PPPoE session:

1. A PPPoE session is initiated over the broadband access network.
2. The VHG/PE device accepts and terminates the PPPoE session.
3. The VHG/PE device obtains virtual access interface (VAI) configuration information:
   - The VHG/PE obtains a virtual template interface configuration information, which typically includes VRF mapping for sessions.
   - The VHG/PE sends a separate request to either the customer's or service provider's RADIUS server for the VPN to authenticate the remote user.
   - The VPN's VRF instance is instantiated on the VHG or PE. The VPN's VRF contains a routing table and other information associated with a specific VPN.

Typically, the customer RADIUS server is located within the customer VPN. To ensure that transactions between the VHG/PE device and the customer RADIUS server occur over routes within the customer VPN, the VHG/PE device is assigned at least one IP address that is valid within the VPN.

1. The VHG/PE device forwards accounting records to the service provider's proxy RADIUS server, which in turn logs the accounting records and forwards them to the appropriate customer RADIUS server.
2. The VHG/PE obtains an IP address for the CPE. The address is allocated from one of the following:
   - Local address pool
   - Service provider's RADIUS server, which either specifies the address pool or directly provides the address
   - Service provider's DHCP server
3. The CPE is now connected to the customer VPN. Packets can flow to and from the remote user.

How to Configure Remote Access MPLS VPNs

Configuring the MPLS Core Network

The Multiprotocol Label Switching (MPLS) core network is configured by enabling label switching of IP packets on interfaces, configuring virtual routing and forwarding (VRF) instances, associating VRFs and configuring Multiprotocol Border Gateway Protocol (BGP) provider edge (PE)-to-PE routing sessions.

Configuring PPPoE

Configuring a Virtual Template Interface

To create and configure a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered ethernet** *number*
5. **ppp authentication chap**
6. **ppp ipcp address required**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**ip unnumbered ethernet** *number* **Example:** `Device(config-if)# ip unnumbered ethernet 1`	Enables IP without assigning a specific IP address on the LAN.
Step 5	**ppp authentication chap** **Example:** `Device(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 6	**ppp ipcp address required** **Example:** `Device(config-if)# ppp ipcp address required`	(Required for legacy dialup and DSL networks.) Prevents a PPP session from being configured with 0.0.0.0 remote ip address.

Configuring PPPoE in a Broadband Aggregation Group

To configure a broadband aggregation (BBA) group for PPP over Ethernet (PPPoE) and to link it to the appropriate virtual template interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {**name** | **global**}
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions max limit** *global-pppoe-session-limit*
7. **exit**
8. **interface gigabitethernet** *slot/subslot/port.* [*subinterface*]
9. **encapsulation dot1q** *vlan-id*
10. **pppoe enable** [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {**name**	**global**} **Example:** `Device(config)# bba-group pppoe bba1`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA configuration mode • The name argument identifies the BBA group. You can have multiple BBA groups. • The global keyword is the default BBA group used when a BBA group name is not specified.
Step 4	**virtual-template** *template-number* **Example:** `Device(config-bba)# virtual-template 20`	Specifies the virtual template interface to use to clone virtual access interfaces (VAIs).
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Device(config-bba)# sessions per-mac limit 32000`	(Optional) Specifies the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.

	Command or Action	Purpose
Step 6	**sessions max limit** *global-pppoe-session-limit* **Example:** `Device(config-bba)# sessions max limit 32000`	(Optional) Specifies the maximum number of PPPoE sessions that will be permitted on a device and sets the PPPoE session-count threshold
Step 7	**exit** **Example:** `Device(config-bba)# exit`	Returns to global configuration mode.
Step 8	**interface gigabitethernet** *slot/subslot/port.* [*subinterface*] **Example:** `Device(config)# interface gigabitethernet 2/0/0.2`	Specifies the interface to which you want to attach the BBA group.
Step 9	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-subif)# encapsulation dot1q 2`	Creates an 802.1q sub-interface and specifies the VLAN id.
Step 10	**pppoe enable** [**group** *group-name*] **Example:** `Device(config-subif)# pppoe enable group bba1`	Attaches the BBA group to the VLAN.

Configuring and Associating Virtual Private Networks

A Virtual Private Network (VPN) service can be added to your Multiprotocol Label Switching (MPLS) configuration by configuring VPNs and associating the VPNs with a virtual template interface.

Configuration Examples for Remote Access MPLS VPNs

Example: Configuring Remote Access MPLS VPNs with One VRF for PPPoE Sessions

The following example shows how to configure the Remote Access MPLS VPNs feature with one virtual routing and forwarding (VRF) instance for PPP over Ethernet (PPPoE) sessions:

```
!
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication enable default none
```

```
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default local
aaa session-id common
enable password cisco
!
username pppoe password 0 pppoe
username common password 0 common
!
!Creates the common VRF.
ip vrf common
rd 100:1000
route-target export 100:1000
route-target import 100:1000
!
!Specifies the BBA group to be used to establish PPPoE sessions and specifies the maximum
!number of PPPoE sessions to be established over a vlan.
bba-group pppoe
virtual-template 1
sessions per-mac limit 32000
!
no virtual-template snmp
!
!Configures the small buffer.
buffers small permanent 15000
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
ip address 10.16.3.1 255.255.255.255
ip ospf network point-to-point
!
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP
!unnumber interfaces to.
interface Loopback1
ip vrf forwarding vpn1
ip address 10.24.1.1 255.255.255.255
!
interface Loopback2
ip vrf forwarding vpn2
ip address 10.8.1.2 255.255.255.255
!
interface gigaethernet 0/0/0
load-interval 30
negotiation auto
no cdp enable
interface gigaethernet 0/0/0.9
encapsulation dot1q 9
pppoe enable
no cdp enable
!
!Enables label switching of IP packets on the interface.
interface GigabitEthernet1/0/0
ip address 10.1.10.1 255.255.0.0
no ip redirects
load-interval 30
negotiation auto
tag-switching ip
!
!Defines the virtual template and associates the common VRF with it.
interface Virtual-Template1
ip vrf forwarding common
ip unnumbered Loopback1
peer default ip address pool common
```

```
ppp authentication chap
!
!Configures OSPF to advertise the networks.
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 10.16.3.1 0.0.0.0 area 0
network 10.1.0.0 0.0.255.255 area 0
!
router rip
version 2
!
!Enters address family configuration mode to configure the VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
version 2
network 10.0.0.0
no auto-summary
exit-address-family
!
!Configures BGP to advertise the networks for the VPN.
router bgp 100
no synchronization
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 172.16.1.4 remote-as 100
neighbor 172.16.1.4 activate
!
!Enters address family configuration mode to configure the common VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
no auto-summary
no synchronization
aggregate-address 10.10.0.0 255.255.0.0 summary-only
exit-address-family
!
address-family vpnv4
neighbor 172.16.1.4 activate
neighbor 172.16.1.4 send-community both
exit-address-family
!
!Specifies the IP local pool to use for the VRF address assignment.
ip local pool common 10.10.1.1 10.10.126.0
ip classless
!Enters routing information in the routing table for the VRF.
ip route 10.0.0.0 255.0.0.0 FastEthernet0/0/0 10.9.0.1
ip route vrf common 10.22.0.0 255.255.0.0 Null0
ip route vrf common 10.30.0.0 255.255.0.0 2.1.1.1 3
ip route vrf common 10.32.0.0 255.255.0.0 2.2.151.1 2
ip route vrf common 10.33.0.0 255.255.0.0 2.3.101.1 2
no ip http server
ip pim bidir-enable
!
no cdp run
!
!Specifies the RADIUS host and configures RADIUS accounting. radius-server retransmit is
!on by default and cannot be removed.
radius-server host 10.19.100.150 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key test
radius-server authorization permit missing Service-Type
radius-server vsa send authentication
call admission limit 90
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco Master Command List, All Releases
MPLS and MPLS applications commands	Cisco IOS Multiprotocol Label Switching Command Reference
Basic MPLS VPNs	"MPLS Virtual Private Networks" module

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 Remote Access MPLS VPNs

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

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

Table 1: Feature Information for Remote Access MPLS VPNs

Feature Name	Releases	Feature Information
Remote Access MPLS VPNs	Cisco IOS XE Release 2.1	The Remote Access MPLS VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. This feature integrates the MPLS-enabled backbone with broadband access capabilities. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

CE—customer edge.

PPPoE—Point-to-Point Protocol over Ethernet.

PE —provider edge.