



# Virtual Private LAN Service over MPLS on Cisco 12000 Series Router Line Cards

Part Number OL-8680-02 Rev. 02 April 20, 2007

## Feature History

Release	Modification
12.0(32)S	This feature was introduced on the Cisco 12000 series routers.
12.0(32)SY	This release adds support for the following features on the Cisco 12000 series routers: <ul style="list-style-type: none"><li>• Fast Reroute</li><li>• Support for edge facing Engine 5 line cards</li><li>• Support for 802.1ad (QinQ) on version 2 Engine 5 line cards</li></ul>
12.0(33)S	This release adds support for the following features on the Cisco 12000 series routers: <ul style="list-style-type: none"><li>• Support for Hierarchical-VPLS capability using Access Pseudo-Wire</li><li>• Support for the following new QoS features:<ul style="list-style-type: none"><li>– Access PseudoWire QoS</li><li>– “match vlan” functionality for VFI AC interfaces</li></ul></li><li>• Support for MAC table management enhancements</li><li>• Support for Layer 2 Access Control Lists on version 2 Engine 5 line cards</li></ul>

This feature module contains the following sections:

- [Virtual Private LAN Service Overview](#)
- [Supported Platforms](#)
- [Supported Standards, MIBs, and RFCs](#)
- [Prerequisites](#)
- [Configuration Tasks](#)
- [Monitoring VPLS](#)
- [Configuring and Verifying VPLS](#)

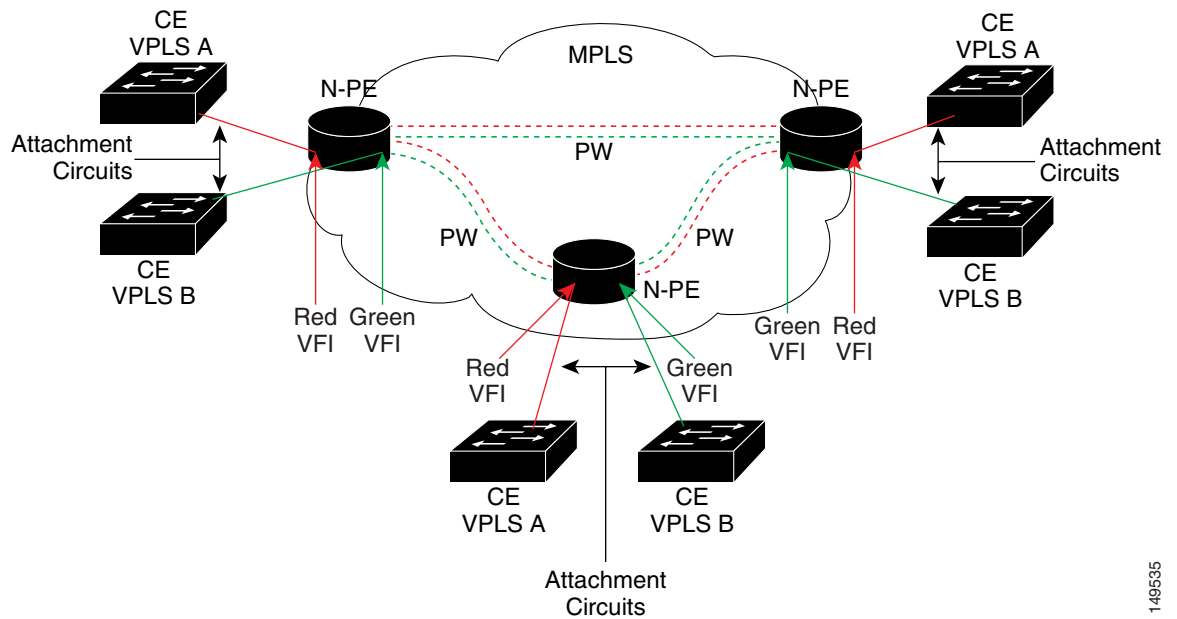
- [Command Reference](#)
- [Glossary](#)

## Virtual Private LAN Service Overview

Virtual Private LAN Service (VPLS) enables geographically separated Local Area Network (LAN) segments to be interconnected as a single bridged domain over an MPLS network. The full functionalities of the traditional LAN like MAC address learning, aging and switching are emulated across all the remotely connected LAN segments that are part of a single bridged domain. A service provider can offer VPLS service to multiple customers over the MPLS network by defining different bridged domains for different customers. Packets from one bridged domain are never carried over or delivered to another bridged domain, thus ensuring the “private” LAN service.

Figure 1 shows the logical components in a VPLS network.

**Figure 1** Logical VPLS Components



**Table 1** Acronym Definitions for Figure 1

CE	Customer edge device. Used to connect to the service provider network.
n-PE	Network-facing provider edge device. A gateway between the MPLS core and the customer domain.
VFI	Virtual Forwarding Instance (VFI). Each Virtual Forwarding Instance maintains its own MAC table. Provides the Ethernet bridge function within the n-PE.
PW	Pseudowire. An emulated point-to-point link between the endpoints.
LSP	Label Switch Path. The path the pseudowire takes in an MPLS network.

The service provider configures the customer's VPLS service by first provisioning the customer's attachment circuits and associating them to a VPLS instance specific to the customer. The attachment circuits can only be Ethernet in the current release. Within Ethernet as access medium, the attachment circuit's type could be untagged, tagged VLAN, QinQ (802.1ad) or Q in Any. The type of the attachment circuit could be different at different n-PEs for the same customer. Please refer to the "restrictions" section for exceptions to this.

After provisioning attachment circuits, neighbor relationship across the MPLS network for this specific instance is established through a set of manual commands identifying the end PEs. Once the neighbor association is done, a full mesh of pseudowires are established among the n-PEs and the service provider network will now start switching the packets within the bridged domain specific to this customer by looking at destination MAC addresses. All traffic with unknown, broadcast and multicast destination MAC addresses are flooded to all the connected CEs. n-PEs learn the source MAC addresses as the packets get flooded and then onwards the traffic gets unicasted to the CE for all the learnt MAC addresses.

Transparent LAN Service (TLS) and Ethernet Virtual Connection Service (EVCS) are available for service provider and enterprise use.

## VPLS Quality of Service

The Modular QoS CLI (MQC) is a platform independent interface for configuring QoS features on Cisco platforms.

The following three different VPLS specific match criteria are introduced in 12.0(32)S:

- Match destination-address mac vpls-unknown For unknown traffic
- Match destination-address mac vpls-known For known traffic
- Match destination-address mac multicast For multicast traffic

More details and configuration of the QoS feature can be found in "Any Transport over MPLS (AToM): Layer 2 QoS (Quality of Service)" at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s30/12s12qos.htm#wp1050921>

## VPLS Layer 2 Access Control Lists

Layer 2 Access Control Lists (ACLs) provide the ability to filter traffic on a VPLS enabled interface based on the source MAC address in the Layer 2 header of the packet. More details and configuration of this feature can be found in "Protocol-Independent MAC ACL Filtering on the Cisco 12000 Series Internet Router" at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s32/macaccl.htm>

## Transparent Layer 2 Protocol Tunneling and PDU Filtering

The Transparent Layer 2 Protocol Tunneling feature allows Layer 2 protocol data units (PDUs) to be tunneled across the core network without being interpreted and processed by intermediary network devices.

Layer 2 PDU filtering allows a service provider to specify which Layer 2 PDUs are to be dropped at an ingress interface on a provider edge (PE) router. Transparent Layer 2 Protocol Tunneling and PDU Filtering provide an enhanced feature set for service providers that transmit customer traffic from metro Ethernet VPNs across an MPLS core network.

These features are supported on VPLS enabled edge interfaces and are supported on VPLS attachment circuits.

Details and configuration of these features (L2PT/L2PDU filtering) can be found in “Transparent Layer 2 Protocol Tunneling and PDU Filtering” at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s28/12pt.htm>

## Pseudowire Tunnel Selection

The Pseudowire Tunnel Selection feature provides the capability to select core-facing routes and map them with VPLS Pseudowire overriding the default route selected by routing. The selected core-facing route could be a next hop or a traffic engineering tunnel.

Traffic engineering (TE) tunnels define LSPs destined to the peer PE router. The default TE tunnel configuration creates one TE tunnel with multiple choices of different paths with different priorities, including tunnel to IGP.

The preferred-path CLI also provides the option to specify whether the VCs should fallback to default route (the route LDP used for signaling) once the preferred path becomes unreachable. The fallback option is enabled by default unless it is explicitly disabled.

Pseudowire Tunnel Selection support is available on a per-neighbor basis. The Virtual Forwarding Instance (VFI) neighbor configuration uses the pseudowire-class as shown in the following example:

```
pseudowire-class tselect1
encapsulation mpls
preferred-path interface Tunnel1
!
pseudowire-class tselect2
encapsulation mpls
preferred-path peer 1.1.1.1
!
pseudowire-class tselect3
encapsulation mpls
preferred-path interface Tunnel2 disable-fallback
!
pseudowire-class tselect4
encapsulation mpls
preferred-path peer 1.1.1.2 disable-fallback
!
l2 vfi VPLS1 manual
vpn id 10
neighbor 8.8.8.1 pw-class tselect1
neighbor 8.8.8.2 pw-class tselect2
neighbor 8.8.8.3 pw-class tselect3
neighbor 8.8.8.4 pw-class tselect4
```

## Restrictions

In this release, the following limitations and restrictions apply:

- Only 2.5G and 10G IP Services Engine (ISE) line cards can be used for VPLS service on Cisco 12000 series routers.
- VPLS over IP and VPLS over L2TPv3 are not supported.
- 4-Port ISE Gigabit Ethernet line cards cannot have different Ethernet attachment circuits associated with the same VPLS instance. Only homogeneous interfaces and sub-interfaces are allowed.
- MPLS forwarding is not supported on non-ISE legacy line cards in a chassis configured as a VPLS provider edge router.
- Auto-discovery is not supported.
- The MPLS Fast Reroute feature is not supported in the core for VPLS connections on Engine 3 cards. The MPLS Fast Reroute feature is supported in the core for VPLS connections on Engine 5 cards.
- QinQ interfaces should not be configured as backup core facing interfaces when using the MPLS Fast Reroute feature
- The same 4-Port ISE Gigabit Ethernet line card cannot be used for both customer facing interfaces as well as core facing interfaces.
- VPLS over DPT core is not supported.
- VLAN ID is not supported as a match criteria for VPLS traffic.
- Only three Aggregate NetFlow schemes can be configured on the main interface when VPLS is configured.
- The QinQ and QinAny features are supported only on the version 2 SPAs for Engine 5.

## Related Documents

For information on configuring Cisco 12000 Series Routers, refer to the following documents:

- *Modular Quality of Service Command-Line Interface*
- *Stacked VLAN Processing*
- *Cisco IOS Quality of Service Solutions Command Reference*
- *Cisco 12000 Series Router Configuration Guide for Cisco IOS*
- *Any Transport over MPLS*
- *Any Transport over MPLS (AToM): Layer 2 QoS (Quality of Service)*
- *MPLS VPNs over IP Tunnels*

## Supported Platforms

VPLS is supported in Cisco IOS Release 12.0(32)SY on the following Integrated Services Engine (ISE) line cards and SPAs:

### Edge Cards

- Ethernet Line Cards
  - 4-port Gigabit Ethernet ISE Line Card (Minimum 512 Megabytes memory)

## Core Cards

- POS Line Cards
  - 4-port OC-12c POS MM (Minimum 512 Megabytes memory)
  - 1-port OC-48 (Minimum 512 Megabytes memory)
  - 16-port OC-3 (Minimum 512 Megabytes memory)
- Cisco 12000 SIP-600 SPAs
  - 1-port 10-Gigabit Ethernet SPA
  - 5-port Gigabit Ethernet SPA
  - 10-port Gigabit Ethernet SPA
  - 1-port OC-192c/STM-64 POS SPA
  - 2-port OC48-POS/RPR SPA
- Cisco 12000 SIP-401/501/601 SPAs
  - 8-port FastEthernet SPA
  - 8-port FastEthernet SPA Version 2 (12.0(32)SY)
  - 1-port 10-Gigabit Ethernet SPA
  - 1-port 10-Gigabit Ethernet SPA Version 2 (12.0(32)SY)
  - 2-port Gigabit Ethernet SPA
  - 2-port Gigabit Ethernet SPA hiVersion 2 (12.0(32)SY)
  - 5-port Gigabit Ethernet SPA
  - 5-port Gigabit Ethernet SPA Version 2 (12.0(32)SY)
  - 10-port Gigabit Ethernet SPA
  - 10-port Gigabit Ethernet SPA Version 2 (12.0(32)SY)
  - 1-port OC-192c/STM-64 POS SPA
  - 2-port OC48-POS/RPR SPA

## Supported Standards, MIBs, and RFCs

The Virtual Private LAN Service over MPLS on Cisco 12000 Series Router Line Cards feature supports the following standards, MIBs, and RFCs.

### Standards

Standards	Title
IEEE 802.1Q	—

## MIBs

MIBs	MIBs Link
PWE3-MIB VPDN-MIB IF-MIB No other 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 IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Prerequisites

Before you configure VPLS, ensure that the network is configured as follows:

- Configure IP routing in the core so that the PE routers can reach each other via IP.
- Configure MPLS and LDP in the core so that a label switched path (LSP) exists between the PE routers.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Make sure the PE routers can access the other router's loopback interface. Note that the loopback interface is not needed in all cases. For example, tunnel selection does not need a loopback interface when VPLS is directly mapped to a TE tunnel.

## Configuration Tasks

See the following sections for configuration tasks for the VPLS feature.

- [Provisioning a VPLS Service](#)
- [Verifying VPLS Configurations](#)

## Provisioning a VPLS Service

You must provision a VPLS service on all provider edge devices as follows:

1. First create a Layer 2 Virtual Forwarding Instance (VFI) on all provider edge devices.
2. Then, attach an Ethernet attachment circuit (untagged, tagged VLAN, QinQ (802.1ad) or Q in Any) to the VFI on the provider edge devices.

## Steps for Provisioning a VPLS Service

Command	Purpose
<b>Creating a Layer 2 Virtual Forwarding Instance (VFI)</b>	
<b>Step 1</b> Router# <b>config t</b> Router(config)#	Enter configuration mode.
<b>Step 2</b> Router(config)# <b>l2 vfi</b> <name> <b>manual</b> Router(config-vfi)#	Creates a named Layer 2 Virtual Forwarding Instance (VFI) and enters the L2 VFI manual configuration mode.  For examples:  Router(config)# <b>l2 vfi Goldfinger manual</b> Router(config)# <b>l2 vfi Moonraker manual</b> Router(config)# <b>l2 vfi Goldeneye manual</b> Router(config)# <b>l2 vfi Thunderball manual</b>
<b>Step 3</b> Router(config-vfi)# <b>vpn id</b> <vpn id>	Configures a VPN ID for the VPLS domain. The emulated VCs bound to this L2 VFI use this VPN ID for signaling.
<b>Step 4</b> Router(config-vfi)# <b>neighbor</b> <remote router id> { <b>encapsulation</b> { <b>l2tpv3</b>   <b>mpls</b> }   <b>pw-class</b> <pw name> }	Specifies the remote peering router ID, which is the IP address of the router, and the tunnel encapsulation type (always set to mpls) or the pseudowire property for the emulated VC. Split horizon is enabled by default and should not be disabled in a fully meshed VPLS network to avoid looping.
<b>Step 5</b> Router(config-vfi)# <b>bridge-domain</b> <id>	Specifies the bridge domain ID number.
<b>Step 6</b> Router(config-vfi)# <b>exit</b> Router(config)#	Exits the L2 VFI manual configuration mode.
<b>Configuring the Interfaces for Ethernet Service</b>	
<b>Step 7</b> Router(config)# <b>interface</b> <b>GigabitEthernet</b> <slot/port>	Specifies the interface slot and port numbers.
<b>Step 8</b> Router(config-if)# <b>no ip</b> <b>directed-broadcast</b>	Blocks broadcast transmissions to the VPLS network.
<b>Step 9</b> Router(config-if)# <b>bridge-domain</b> <id>	Specifies the bridge domain ID number.
<b>Step 10</b> Router(config-if)# <b>no cdp enable</b>	Prevents Cisco Discovery Protocol (CDP) from being enabled.

## Verifying VPLS Configurations

You can verify the operation of the VPLS Ethernet Service by verifying each of the following components:

- State of the Virtual Forwarding Instance (VFI)
- State of the attachment circuit
- State of the pseudowire
- MAC address in the MAC table

	Command	Purpose
Step 1	<code>vpls-pe#show vfi &lt;name&gt;</code>	Verifies the state of the Virtual Forwarding Instance (VFI) on each provider edge router. For examples:  <pre>vpls-pe#show vfi Goldfinger vpls-pe#show vfi Moonraker vpls-pe#show vfi Goldeneye vpls-pe#show vfi Thunderball</pre>
Step 2	<code>vpls-pe#show xconnect interface GigabitEthernet &lt;slot/port&gt;</code>	Verifies the state of the attachment circuit on each provider edge router.
Step 3	<code>vpls-pe#show mpls l2transport vc &lt;vcNumber&gt; detail</code>	Displays information about Any Transport over MPLS (AToM) virtual circuits (VCs) that have been enabled to route Layer 2 packets on a router.
Step 4	<code>vpls-pe#show mac address-table bridge-domain &lt;id&gt;</code>	Verifies the MAC address in the MAC table for each provider edge router in the specified bridge domain.

## Monitoring VPLS

To monitor VFI information, use the following **show** commands:

Command	Purpose
<code>Router#show vfi</code>	Shows the state, type, emulation, and neighbors of all VFIs. For example:  <pre>Router#show vfi VFI name: Goldfinger, state: up, type: multipoint   Bridge-Domain 1 attachment circuits:     GigabitEthernet1/0   Neighbors connected via pseudowires:     7.7.7.7 6.6.6.6  VFI name: Moonraker, state: up, type: multipoint   Bridge-Domain 1 attachment circuits:     GigabitEthernet1/0   Neighbors connected via pseudowires:     7.7.7.7 6.6.6.6</pre>
<code>Router#show vfi &lt;name&gt;</code>	Shows the state, type, emulation, and neighbors of the specified VFI name. For Example:  <pre>Router#show vfi Goldfinger VFI name: Goldfinger, state: up, type: multipoint   Bridge-Domain 1 attachment circuits:     GigabitEthernet1/0   Neighbors connected via pseudowires:     7.7.7.7 6.6.6.6</pre>

# Configuring and Verifying VPLS

This section provides the following examples for configuring and verifying VPLS on provider edge routers:

- [Example of Configuring an Ethernet VPLS Network](#)
- [Example of Verifying a VPLS Configuration](#)

## Example of Configuring an Ethernet VPLS Network

### Provider Edge 1—PE1

```
Router#config t
Router(config)#12 vfi Goldfinger manual
Router(config-vfi)#vpn id 1
Router(config-vfi)#bridge-domain 1
Router(config-vfi)#neighbor 120.0.0.3 encapsulation mpls
Router(config-vfi)#neighbor 162.0.0.2 encapsulation mpls
Router(config-vfi)#exit
Router(config)#interface Loopback 0
Router(config-if)#ip address 20.0.0.1 255.255.255.255
Router(config-if)#exit
Router(config)#interface GigabitEthernet 2/1
Router(config-if)#bridge-domain 1
Router(config-if)#exit
Router(config)#interface GigabitEthernet 2/2
Router(config-if)#bridge-domain 1
Router(config-if)#exit
```

### Provider Edge 2—PE2

```
Router#config t
Router(config)#12 vfi Moonraker manual
Router(config-vfi)#vpn id 1
Router(config-vfi)#bridge-domain 1
Router(config-vfi)#neighbor 120.0.0.3 encapsulation mpls
Router(config-vfi)#neighbor 20.0.0.1 encapsulation mpls
Router(config-vfi)#exit
Router(config)#interface Loopback 0
Router(config-if)#ip address 162.0.0.2 255.255.255.255
Router(config-if)#exit
Router(config)#interface GigabitEthernet 2/1
Router(config-if)#bridge-domain 1
Router(config-if)#exit
```

### Provider Edge 3—PE3

```
Router#config t
Router(config)#12 vfi Goldeneye manual
Router(config-vfi)#vpn id 1
Router(config-vfi)#bridge-domain 6
Router(config-vfi)#neighbor 162.0.0.2 encapsulation mpls
Router(config-vfi)#neighbor 20.0.0.1 encapsulation mpls
Router(config-vfi)#exit
Router(config)#12 vfi Thunderball manual
Router(config-vfi)#vpn id 200
Router(config-vfi)#bridge-domain 1
Router(config-vfi)#neighbor 162.0.0.2 encapsulation mpls
Router(config-vfi)#neighbor 20.0.0.1 encapsulation mpls
Router(config-vfi)#exit
Router(config)#12 vfi Mercury manual
```



```

MPLS VC type is VFI, interworking type is Ethernet
Destination address: 6.6.6.6, VC ID: 1, VC status: up
  Preferred path: not configured
  Default path: active
  Next hop: 26.26.26.2
  Output interface: Gi5/1/0, imposed label stack {33}
Create time: 00:36:12, last status change time: 00:20:13
Signaling protocol: LDP, peer 6.6.6.6:0 up
  MPLS VC labels: local 31, remote 33
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 0, send 0
  byte totals:   receive 0, send 0
  packet drops: receive 0, seq error 0, send 0

Local interface: VFI VPLS_ETH_SERVICE VFI up
MPLS VC type is VFI, interworking type is Ethernet
Destination address: 7.7.7.7, VC ID: 1, VC status: up
  Preferred path: not configured
  Default path: active
  Next hop: point2point
  Output interface: PO2/2, imposed label stack {28 36}
Create time: 00:36:13, last status change time: 00:09:03
Signaling protocol: LDP, peer 7.7.7.7:0 up
  MPLS VC labels: local 30, remote 36
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 0, send 0
  byte totals:   receive 0, send 0
  packet drops: receive 0, seq error 0, send 0

vpls-pe1#

```

### Mac Address in the Mac Table

The following example verifies the MAC address in the MAC table on PE1.

```
vpls-pe1#show mac address-table bridge-domain 1001
```

```

Mac Address Table: 4 Bridge domain id: 1001
=====
aging time : 500 sec
max size : 5000
total number of addresses : 1
slots: 4, 5

```

Mac Address	Learned from	LC learned
0012.1212.1212	VC Label:2017	4

```
Total Mac Addresses displayed : 1
```

## Example of Configuring VPLS for an Ethernet Attachment Circuit

Create and apply an ethernet attachment circuit.

```
vpls-pe1#12 vfi vpls.1 manual
  vpn id 1
  bridge-domain 1
  neighbor 7.7.7.7 encapsulation mpls
  neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0
  no ip address
  no ip directed-broadcast
  bridge-domain 1
  duplex full
  negotiation auto
  no cdp enable
end
```

## Example of Configuring VPLS for a dot1Q Attachment Circuit

Create and apply a dot1Q attachment circuit.

```
vpls-pe1#12 vfi vpls.1 manual
vpn id 1
bridge-domain 1
neighbor 7.7.7.7 encapsulation mpls
neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0.1
encapsulation dot1Q 1 second-dot1q 11
no ip directed-broadcast
bridge-domain 1
no cdp enable
end
```

## Example of Configuring VPLS for a QinQ Attachment Circuit

Create and apply a QinQ attachment circuit.

```
vpls-pe1#12 vfi vpls.1 manual
vpn id 1
bridge-domain 1
neighbor 7.7.7.7 encapsulation mpls
neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0.1
encapsulation dot1Q 1 second-dot1q 11
no ip directed-broadcast
bridge-domain 1
no cdp enable
end
```

## Example of Configuring VPLS for a QinAny Attachment Circuit

Create and apply a QinAny attachment circuit.

```
vpls-pe1#12 vfi vpls.1 manual
vpn id 1
bridge-domain 1
neighbor 7.7.7.7 encapsulation mpls
neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0.1
encapsulation dot1Q 1 second-dot1q any
no ip directed-broadcast
bridge-domain 1
no cdp enable
end
```

## Example of Configuring a VPLS Ingress Policer

Create and apply a 2 rate 3 color policer policy to the ethernet attachment circuit.

```
vpls-pe1#policy-map vpls_police
  class class-default
    police cir percent 2 bc 256 ms pir percent 5 be 30 ms
      conform-action transmit
      exceed-action set-mpls-exp-imposition-transmit 7
      violate-action drop

vpls-pe1#12 vfi vpls.1 manual
  vpn id 1
  bridge-domain 1
  neighbor 7.7.7.7 encapsulation mpls
  neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0
  no ip address
  no ip directed-broadcast
  bridge-domain 1
  service-policy input vpls_police
  duplex full
  negotiation auto
  no cdp enable
end
```

## Example of Configuring a VPLS Egress Shaper

Create and apply an egress shaper policy to the ethernet attachment circuit.

```
vpls-pe1#policy-map vpls_shape_parent
  class class-default
    shape average percent 2
    service-policy vlan_shape_child

vpls-pe1#policy-map vpls_shape_child
  class class-default
    queue-limit 1000 packets
    shape average percent 1 1 ms 1 ms

vpls-pe1#12 vfi vpls.1 manual
  vpn id 1
  bridge-domain 1
  neighbor 7.7.7.7 encapsulation mpls
  neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0
  no ip address
  no ip directed-broadcast
  bridge-domain 1
  service-policy output vpls_shape_parent
  duplex full
  negotiation auto
  no cdp enable
end
```

## Example of Configuring a VPLS Ingress Exp Policy Setting

Create and apply an ingress exp policy to ethernet attachment circuit.

```
vpls-pe1#policy-map vpls_exp
  class class-default
    set mpls experimental imposition 3

vpls-pe1#12 vfi vpls.1 manual
  vpn id 1
  bridge-domain 1
  neighbor 7.7.7.7 encapsulation mpls
  neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0
  no ip address
  no ip directed-broadcast
  bridge-domain 1
  service-policy input vpls_exp
  duplex full
  negotiation auto
  no cdp enable
end
```

## Example of Configuring VPLS Ingress Match Criteria

Create and apply an ingress exp policy with different match criteria to ethernet attachment circuit.

```
vpls-pe1#class-map match-all vpls_multicast
  match destination-address mac multicast
vpls-pe1#class-map match-all vpls_known
  match destination-address mac vpls-known
vpls-pe1#class-map match-all vpls_unknown
  match destination-address mac vpls-unknown

vpls-pe1#policy-map vpls_exp
  class vpls_multicast
    set mpls experimental imposition 3

vpls-pe1#policy-map vpls_exp
  class vpls_known
    set mpls experimental imposition 3

vpls-pe1#policy-map vpls_exp
  class vpls_unknown
    set mpls experimental imposition 3

vpls-pe1#12 vfi vpls.1 manual
  vpn id 1
  bridge-domain 1
  neighbor 7.7.7.7 encapsulation mpls
  neighbor 6.6.6.6 encapsulation mpls

interface GigabitEthernet1/0
  no ip address
  no ip directed-broadcast
  bridge-domain 1
  service-policy input vpls_exp
  duplex full
  negotiation auto
```

```
no cdp enable
end
```

## Command Reference

This section documents new commands for VPLS. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

## mac-address-table aging-time

To configure the aging time for entries in the Layer 2 table, use the **mac-address-table aging-time** command in global configuration mode. To reset the seconds value to the default setting, use the **no** form of this command.

### Cisco 12000 Series Routers

**mac-address-table aging-time** *seconds* [**bridge-domain** *id*]

**no mac-address-table aging-time** *seconds* [**bridge-domain** *id*]

### Syntax Description

<i>seconds</i>	Aging time; valid values are 0, and from 10 to 1,000,000 seconds.
<b>bridge-domain</b> <i>id</i>	(Optional) Specifies the bridge-domain to apply the changed aging time; valid values are from 2 to 1001.

### Defaults

300 seconds

### Command Modes

Global configuration

### Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 family switches.
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S on Cisco 12000 series routers.
12.1(1)E	This command was implemented on Catalyst 6000 family switches.
12.2(2)XT	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

### Usage Guidelines

#### Cisco 12000 Series Routers

The aging time entry will take the specified value. Valid entries are from 10 to 1,000,000 seconds.

This command cannot be disabled.

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

### Examples

#### Cisco 12000 Series Routers

The following example shows the aging time being configured:

```
Router(config)# mac-address-table aging-time 300
```

The following example shows the aging time being disabled:

```
Router(config)# mac-address-table aging-time 0
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show mac-address-table aging-time</b>	Displays the MAC address aging time.

---

## mac-address-table limit

To enable MAC limiting, use the **mac-address-table limit** command. Use the **no** form of this command to disable MAC limiting.

```
mac-address-table limit [maximum num] [action {warning | limit | shutdown}]
[notification {syslog | trap | both}]
```

```
mac-address-table limit [{vlan vlan} | {interface type mod/port}] [maximum num] [action
{warning | limit | shutdown}] [flood]
```

```
no mac-address-table limit [vlan vlan] [maximum | action]
```

### Syntax Description

<b>maximum num</b>	(Optional) Specifies the maximum number of MAC entries per VLAN per EARL allowed; valid values are from 5 to 32000 MAC-address entries.
<b>action</b>	(Optional) Specifies the type of action to be taken when the action is violated.
<b>warning</b>	Specifies that the one syslog message will be sent and no further action will be taken when the action is violated.
<b>limit</b>	Specifies that the one syslog message will be sent and/or a corresponding trap will be generated with the MAC limit when the action is violated.
<b>shutdown</b>	Specifies that the one syslog message will be sent and/or the VLAN is moved to the blocked state when the action is violated.
<b>notification</b>	(Optional) Specifies the type of notification to be sent when the action is violated.
<b>syslog</b>	Sends a syslog message when the action is violated.
<b>trap</b>	Sends trap notifications when the action is violated.
<b>both</b>	Sends syslog and trap notifications when the action is violated.
<b>vlan vlan</b>	(Optional) Enables MAC limiting on a per-VLAN basis.
<b>interface type mod/port</b>	(Optional) Enables MAC limiting on a per-port basis.
<b>flood</b>	(Optional) Enables unknown unicast flooding on a VLAN.

### Defaults

The defaults are as follows:

- **maximum num** is **500** MAC address entries.
- **action** is **warning**.
- **notification** is **syslog**.

### Command Modes

Global configuration

Command History	Release	Modification
	12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
	12.2(18)SXD1	This command was changed to include the <b>vlan</b> <i>vlan</i> keyword and argument to support per VLAN MAC limiting.
	12.2(18)SXE	This command was changed to include the <b>interface</b> <i>type mod/port</i> keyword and arguments to support per-port MAC limiting.

### Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Use this syntax for enabling MAC limiting globally:

```
mac-address-table limit [maximum num] [action { warning | limit | shutdown }]
[notification { syslog | trap | both }]
```

Use this syntax for enabling per-VLAN MAC limiting:

```
mac-address-table limit [vlan vlan] [maximum num] [action { warning | limit | shutdown }]
[flood]
```

Use this syntax for enabling per-port MAC limiting:

```
mac-address-table limit [interface type mod/port] [maximum num] [action { warning | limit |
shutdown }] [flood]
```

If you enable per-VLAN MAC limiting, the per-VLAN MAC limiting supersedes the **mac-address-table limit** command that globally enables MAC limiting.

The maximum number of MAC entries is based per VLAN and per EARL.

If you do not specify a maximum, an action, or a notification, the default settings are used.

If you enable per-VLAN MAC limiting, MAC limiting is enabled on the VLAN specified only.

The **flood** keyword is supported on VLAN interfaces only.

The **flood** action occurs only if the **limit** action is configured and is violated.

In the **shutdown** state, the VLAN remains in the blocked state until you reenables it through the CLI.

### Examples

This example shows how to enable the MAC limit globally:

```
Router(config)# mac-address-table limit
Router(config)#
```

This example shows how to enable per-VLAN MAC limiting:

```
Router(config)# mac-address-table limit vlan 501 maximum 50 action shutdown
Router(config)#
```

## clear mac-address-table

To remove a specified address (or set of addresses) from the MAC address table, use the **clear mac-address-table** command in privileged EXEC mode.

### Cisco 12000 Series Routers

```
clear mac-address-table [dynamic | secure | static] [address mac-address] [interface type
slot/port]
```

Syntax Description		
<b>bridge-domain</b> <i>id</i>	(Optional)	Clears all addresses for a specified bridge-domain.
<b>address</b>	(Optional)	Clears only a specified address.
<i>mac-address</i>	(Optional)	Target MAC address.
<b>interface</b>		Clears all addresses for an interface.
<i>type</i>	(Optional)	Interface type: ethernet, fastethernet, fddi, atm, or port channel.
<i>slot</i>	(Optional)	The module interface number. Valid entries equal the number of ports on the chassis.
<i>port</i>	(Optional)	Port interface number ranges based on type of Ethernet switch network module used: 0 to 15 for NM-16ESW 0 to 35 for NM-36ESW 0 to 1 for GigabitEthernet

### Defaults

#### Cisco 12000 Series Routers

All MAC addresses on the router being configured are cleared.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S on Cisco 12000 series routers.
12.2(2)XT	This command was introduced on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**Usage Guidelines****Cisco 12000 Series Routers**

If the **clear mac-address-table** command is invoked with no options, all MAC addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, all addresses on the specified interface are removed.

If a targeted address is not present in the MAC forwarding table, the following error message appears:

```
MAC address not found
```

**Examples****Cisco 12000 Series Routers**

The following example shows how to clear all dynamic addresses in the MAC forwarding table:

```
Router# clear mac-address-table dynamic
```

The following example shows how to clear the static address 0040.C80A.2F07 on Ethernet port 1:

```
Router# clear mac-address-table static address 0040.C80A.2F07 interface ether 0/1
```

**Related Commands****Cisco 12000 Series Routers**

Command	Description
<b>mac-address-table (aging-time)</b>	Configures the length of time the switch keeps dynamic MAC addresses in memory before discarding.
<b>show (mac-address-table)</b>	Displays addresses in the MAC address table for a switched port or module.

## l2 vfi <name> manual

To create a Layer 2 Virtual Forwarding Instance (VFI), use the **l2 vfi <name> manual** command in L2 VFI manual configuration mode.

**l2 vfi <name> manual**

Syntax Description		
<i>name</i>	Variable that specifies the name of the Layer 2 Virtual Forwarding Instance (VFI) being created.	
<b>manual</b>	Keyword that specifies that the VFI is being created manually as opposed to being created automatically by VPLS.	

**Defaults** No default behavior or values.

**Command Default** **l2 vfi <name> manual**

**Command Modes** L2 VFI manual configuration mode

Router(config-vfi)#

Command History	Release	Modification
	12.0(32)SY	This command was introduced.

**Usage Guidelines** You must create a Layer 2 Virtual Forwarding Instance (VFI) for each provider edge router in the VPLS network.

**Examples** The following example shows how to create a Layer 2 Virtual Forwarding Instance (VFI) for Ethernet service labeled as “Goldfinger”.

```
Router#config t
Router(config)#l2 vfi Goldfinger manual
Router(config-vfi)#vpn id 1
Router(config-vfi)#bridge-domain 1
Router(config-vfi)#neighbor 120.0.0.3 encapsulation mpls
Router(config-vfi)#neighbor 162.0.0.2 encapsulation mpls
Router(config-vfi)#exit
Router(config-vfi)#
```

Related Commands	Command	Description
	Router# <b>show vfi</b>	Shows the state, type, emulation, and neighbors of all VFIs.
	Router# <b>show vfi &lt;name&gt;</b>	Shows the state, type, emulation, and neighbors of the VFI with the specified name.

# Glossary

ACL	Access Control List
BPDU	Bridge Protocol Data Unit
CE	Customer Edge
CDP	Cisco Discovery Protocol
EVCS	Ethernet Virtual Connection Service
L2PT	Layer 2 Protocol Tunnelling
MAC	Media Access Control
MPLS	Multi Protocol Label Switching
PE	Provider Edge
QoS	Quality of Service
Split Horizon	A packet forwarding technique that prevents packets received from an emulated VC from being forwarded to another emulated VC. This technique is important for creating loop-free paths in a full-meshed network.
STP	Spanning-Tree Protocol
TLS	Transparent LAN Service
VC	Virtual Connection
VFI	Virtual Forwarding Instance
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	A Virtual Private Network (VPN) routing/forwarding instance.
VTP	Virtual Terminal Protocol

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

©2006 Cisco Systems, Inc. All rights reserved.