L2VPN Advanced VPLS

The L2VPN Advanced VPLS feature introduces the following enhancements to Virtual Private LAN Services:

• Ability to load-balance traffic across multiple core interfaces using equal cost multipaths (ECMP)
• Support for redundant provide edge switches
• Command line interface enhancements to facilitate configuration of the L2VPN Advanced VPLS feature

The L2VPN Advanced VPLS feature uses Virtual Switch System (VSS) and Flow Aware Transport (FAT) pseudowires to achieve PE redundancy and load-balancing. The following sections explain the concepts and configuration tasks for this feature.

• Finding Feature Information, page 1
• Prerequisites for L2VPN Advanced VPLS, page 2
• Restrictions for L2VPN Advanced VPLS, page 2
• Information About L2VPN Advanced VPLS, page 3
• How to Configure L2VPN Advanced VPLS, page 3
• Configuration Examples for L2VPN Advanced VPLS, page 11
• Additional References for L2VPN Advanced VPLS, page 13
• Feature Information for L2VPN Advanced VPLS, page 14

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 at the end of this module.

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 L2VPN Advanced VPLS

• This feature requires that you understand how VPLS works. For information about VPLS, see “VPLS Overview” section in the Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide.

• Configuring the L2VPN Advanced VPLS feature works with MPLS Traffic Engineering tunnels with explicit paths and Generic Routing Encapsulation (GRE tunnels) with static routes to the tunnel destination. For information and configuration steps for MPLS traffic engineering and GRE tunnels, see the following documents:
  • MPLS Traffic Engineering and Enhancements
  • Implementing Tunnels

• This feature requires two Cisco 6500 series routers be configured as a virtual switch system.

• This feature requires nonstop forwarding and stateful switchover.

Restrictions for L2VPN Advanced VPLS

• The ping and traceroute commands that support the Any Transport over MPLS Virtual Circuit Connection Verification (VCCV) feature are not supported over FAT pseudowires.

• The VPLS Autodiscovery feature is not supported with the L2VPN Advanced VPLS feature.

• In Cisco IOS Release 12.2(33)SX14, the following types of configurations are supported:
  • MPLS core with configuration of PE routers through the neighbor command under transport vpls mode.
  • MPLS core with configuration of PE routers through MPLS traffic engineering tunnels using explicit paths.
  • IP core with configuration of PE routers through MPLS over GRE tunnels.

Other configuration methods, including using the route-via command, BGP autodiscovery, or explicit VLAN assignment to a PE egress port, are not supported.

• Load-balancing is not supported in the core routers when the core uses IP to transport packets.

• The maximum number of links per bundle is limited to eight.

• The maximum number of port channels is limited to 32.

• The maximum number of VPLS neighbors is limited to 60 minus the number of neighbors configured with the load-balanceflow command.

• In Cisco IOS Release 12.2(33)SX14, the L2VPN Advanced VPLS feature is supported on the Cisco Catalyst 6500 series switches with Supervisor 720-10GE engine.

• The L2VPN Advanced VPLS feature supports the following line cards and shared port adapters (SPAs):
  • 7600-SIP-400 (core facing)
Information About L2VPN Advanced VPLS

FAT Pseudowires and Their Role in Load-Balancing

FAT pseudowires are used to load-balance traffic in the core when equal cost multipaths are used. The MPLS labels add an additional label to the stack, called the flow label, which contains the flow information of a VC. For more information about FAT pseudowires, see PWE3 Internet-Draft *Flow Aware Transport of MPLS Pseudowires* (draft-bryant-filsfils-fat-pw).

Virtual Switch Systems

Two Cisco 6500 series switches can be connected to form one logical switch. One switch is designated as the master, while the other is the slave. The two switches are connected by a virtual switch link (VSL). The two switches are used for link redundancy, load-balancing, and failover.

For more information on virtual switch systems, see the "Configuring VSS" section in the *Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide*.

How to Configure L2VPN Advanced VPLS

Enabling Load-Balancing with ECMP and FAT Pseudowires

The following steps explain how to enable load-balancing at the provider edge (PE) device and on the core device.

To enable load-balancing on the edge device, issue the `load-balance flow` command. The load-balancing rules are configured through the `port-channel load-balance` command parameters.

To enable core load-balancing, issue the `flow-label enable` command on both PE devices. You must issue the `load-balance flow` command with the `flow-label enable` command.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `pseudowire-class name`
4. `encapsulation mpls`
5. `load-balance flow`
6. `flow-label enable`
7. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**  
  Device> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Device# configure terminal | |
| **Step 3** pseudowire-class name | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode. |
| **Example:**  
  Device(config)# pseudowire-class class1 | |
| **Step 4** encapsulation mpls | Specifies the MPLS tunneling encapsulation type. |
| **Example:**  
  Device(config-pw)# encapsulation mpls | |
| **Step 5** load-balance flow | Enables load-balancing on ECMPs. |
| **Example:**  
  Device(config-pw)# load-balance flow | |
| **Step 6** flow-label enable | Enables the imposition and disposition of flow labels for the pseudowire. |
| **Example:**  
  Device(config-pw)# flow-label enable | |
| **Step 7** end | Exits pseudowire class configuration mode and enters privileged EXEC mode. |
| **Example:**  
  Device(config-pw)# end | |
Enabling Port-Channel Load-Balancing

The following task explains how to enable port channel load-balancing, which sets the load-distribution method among the ports in the bundle. If the `port-channel load-balance` command is not configured, load-balancing occurs with default parameters.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `port-channel load-balance` *method*
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> port-channel load-balance <em>method</em></td>
<td>Specifies the load distribution method among the ports in a bundle.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# port-channel load-balance src-mac</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Explicitly Specifying the PE Routers As Part of Virtual Ethernet Interface Configuration

There are several ways to specify the route through which traffic should pass.
Explicitly specify the PE routers as part of the virtual Ethernet interface configuration

- Configure an MPLS Traffic Engineering tunnel
- Configure a GRE tunnel

The following task explains how to explicitly specify the PE routers as part of the virtual Ethernet interface configuration.

**Note**

This task includes steps for configuring the LAN port for Layer 2 Switching. For more information, see the "Configuring LAN Ports for Layer 2 Switching." task.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface virtual-ethernet num`
4. `transport vpls mesh`
5. `neighbor remote-router-id [pw-class pw-class-name]`
6. `exit`
7. `switchport`
8. `switchport mode trunk`
9. `switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]]`
10. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface virtual-ethernet num</td>
<td>Creates a virtual Ethernet interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface virtual-ethernet 1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> transport vpls mesh</td>
<td>Create a full mesh of pseudowires and enters VPLS transport mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# transport vpls mesh</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> neighbor remote-router-id [pw-class pw-class-name]</td>
<td>Specifies the PE routers to be used in the pseudowire.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if-transport)# neighbor 10.19.19.19 pw-class 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits VPLS transport configuration mode and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if-transport)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> switchport</td>
<td>Configures the port for Layer 2 switching.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> switchport mode trunk</td>
<td>Enables permanent trunking mode and negotiates to convert the link into a trunk link.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode trunk</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> switchport trunk allowed vlan {add</td>
<td>except</td>
<td>none</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport trunk allowed vlan except 10, 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring an MPLS Traffic Engineering Tunnel

There are several ways to specify the route through which traffic should pass.
Explicitly specify the PE devices as part of the virtual Ethernet interface configuration

- Configure an MPLS Traffic Engineering tunnel
- Configure a GRE tunnel

The following task explains how to configure an MPLS Traffic Engineering tunnel.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface tunnel number**
4. **ip unnumbered type number**
5. **tunnel destination ip-address**
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng autoroute announce**
8. **tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name} | identifier path-number} [lockdown]**
9. **exit**
10. **ip route ip-address tunnel num**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
   **Example:**
   Device> enable  
   - Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
   **Example:**
   Device# configure terminal |
| **Step 3** interface tunnel number | Configures an interface type and enters interface configuration mode.  
   **Example:**
   Device(config)# interface tunnel10 |
| **Step 4** ip unnumbered type number | Assigns an IP address to the tunnel interface.  
   **Example:**
   Device(config-if)# ip unnumbered loopback 0  
   - An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |
<p>| <strong>Step 5</strong> tunnel destination ip-address | Specifies the destination for a tunnel. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device(config-if)# tunnel destination 10.20.1.1</td>
<td>The <em>ip-address</em> keyword is the IP address of the host destination expressed in dotted decimal notation.</td>
</tr>
</tbody>
</table>

**Step 6**

**tunnel mode mpls traffic-eng**

**Example:** Device(config-if)# tunnel mode mpls traffic-eng

Configures the tunnel encapsulation mode to MPLS traffic engineering.

**Step 7**

**tunnel mpls traffic-eng autoroute announce**

**Example:** Device(config-if)# tunnel mpls traffic-eng autoroute announce

Configures the IGP to use the tunnel in its enhanced SPF calculation.

**Step 8**

**tunnel mpls traffic-eng path-option number**

`{dynamic | explicit {name path-name} | Identifier path-number} [lockdown]`

**Example:** Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit name TestPath

Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.

- A dynamic path is used if an explicit path is currently unavailable.

**Step 9**

**exit**

**Example:** Device(config-if)# exit

Exits interface configuration mode and returns to global configuration mode.

**Step 10**

**ip route ip-address tunnel num**

**Example:** Device(config)# ip route 10.19.19.19 255.255.255.255 tunnel10

Creates a static route.

---

**Configuring a GRE Tunnel**

There are several ways to specify the route through which traffic should pass.

- Explicitly specify the PE devices as part of the virtual Ethernet interface configuration
- Configure an MPLS Traffic Engineering tunnel
- Configure a GRE tunnel
The following task explains how to configure a GRE tunnel. For more information on GRE tunnels, see the Implementing Tunnels module.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. tunnel mode {gre ip | gre multipoint}
5. mpls ip
6. tunnel source {ip-address | interface-type interface-number}
7. tunnel destination {hostname | ip-address}
8. exit
9. ip route ip-address tunnel num

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>interface type number</td>
<td>Specifies the interface type and number and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To configure a tunnel, use tunnel for the type argument.</td>
</tr>
<tr>
<td>4</td>
<td>tunnel mode {gre ip</td>
<td>gre multipoint}</td>
</tr>
<tr>
<td>5</td>
<td>mpls ip</td>
<td>Enables MPLS on the tunnel.</td>
</tr>
<tr>
<td>6</td>
<td>tunnel source {ip-address</td>
<td>interface-type interface-number}</td>
</tr>
</tbody>
</table>
### Configuration Examples for L2VPN Advanced VPLS

The following sections show configuration examples for the three supported methods of configuring the L2VPN Advanced VPLS feature.

## Example: Configuring L2VPN Advanced VPLS—Explicitly Specifying Peer PE Devices

The following example shows how to create two VPLS domains under VLANs 10 and 20. Each VPLS domain includes two pseudowires to peer PE devices 10.2.2.2 and 10.3.3.3. Load-balancing is enabled through the `load-balance flow` and `flow-label enable` commands.

```plaintext
pseudowire-class cl1
encap mpls
```
Example: Configuring L2VPN Advanced VPLS—Using MPLS Traffic Engineering Tunnels

The following example shows the creation of two VPLS domains and uses MPLS Traffic Engineering tunnels to specify the explicit path.

```
pseudowire-class cl1
    encap mpls
    port-channel load-balance src-mac

interface Tunnel1
    ip unnumbered Loopback0
    tunnel mode mpls traffic-eng
    tunnel destination 192.168.1.1
    tunnel mpls traffic-eng autoroute announce
    tunnel mpls traffic-eng path-option 1 explicit name LSP1
    ip explicit-path name LSP1 enable
    next-address 192.168.2.2
    next-address loose 192.168.1.1

interface Tunnel2
    ip unnumbered Loopback0
    tunnel mode mpls traffic-eng
    tunnel destination 172.16.1.1
    tunnel mpls traffic-eng autoroute announce
    tunnel mpls traffic-eng path-option 1 explicit name LSP2
    ip explicit-path name LSP2 enable
    next-address 172.16.2.2
    next-address loose 172.16.1.1

interface virtual-ethernet 1
    transport vpls mesh
    neighbor 10.2.2.2 pw-class cl1
    neighbor 10.3.3.3 pw-class cl1
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 10,20
```

ip route 10.2.2.2 255.255.255.255 Tunnel1
ip route 10.3.3.3 255.255.255.255 Tunnel2
Example: Configuring L2VPN Advanced VPLS—Using MPLS over GRE Tunnels

The following example shows the creation of two VPLS domains under VLANs 10 and 20. Each VPLS domain includes two pseudowires to peer PEs 10.2.2.2 and 10.3.3.3. The pseudowires are MPLS over GRE tunnels because the core is IP.

```
pseudowire-class cl1
  encap mpls
  load-balance flow
  !
  port-channel load-balance src-mac
  !
  int tunnel 1
  
  tunnel mode gre ip
  mpls ip
  tunnel source 10.1.1.1
  tunnel destination 10.2.2.2
  !
  int tunnel 2
  
  tunnel mode gre ip
  mpls ip
  tunnel source 10.1.1.1
  tunnel destination 10.3.3.3
  !
  interface virtual-ethernet 1
  transport vpls mesh
  neighbor 10.2.2.2 pw-class cl1
  neighbor 10.3.3.3 pw-class cl1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10, 20
  ip route 10.2.2.2 255.255.255.255 Tunnel1
  ip route 10.3.3.3 255.255.255.255 Tunnel2
```

Additional References for L2VPN Advanced VPLS

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>MPLS commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>VPLS</td>
<td>Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide</td>
</tr>
<tr>
<td>MPLS Traffic Engineering tunnels</td>
<td>&quot;MPLS Traffic Engineering and Enhancements&quot;</td>
</tr>
<tr>
<td>GRE tunnels</td>
<td>&quot;Implementing Tunnels&quot;</td>
</tr>
<tr>
<td>Cisco 6500 LAN ports</td>
<td>&quot;Configuring LAN Ports for Layer 2 Switching&quot;</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-bryant-filsfils-fat-pw</td>
<td>Internet Draft: Flow Aware Transport of MPLS Pseudowires (FAT PWs)</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4762</td>
<td>Virtual Private LAN Services (VPLS) Using Label Distribution Protocol (LDP) Singling</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for L2VPN Advanced VPLS

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 L2VPN Advanced VPLS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2VPN Advanced VPLS</td>
<td>12.2(33)SX14</td>
<td>The L2VPN Advanced VPLS feature uses Virtual Switch System (VSS) and Flow Aware Transport (FAT) pseudowires to achieve PE redundancy and load-balancing.</td>
</tr>
<tr>
<td></td>
<td>15.1(1)SY</td>
<td>In 12.2(33)SX14, this feature was introduced on the Cisco 6500 series router.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>flow-label enable, interface virtual-ethernet, load-balance flow, neighbor (VPLS transport mode), show interface virtual-ethernet, and transport vpls mesh.</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following command was modified:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show mpls l2transport vc</td>
</tr>
</tbody>
</table>