Assigning an ID Number to an MPLS VPN

You can identify Virtual Private Networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN.

- Finding Feature Information, on page 1
- Restrictions for MPLS VPN ID, on page 1
- Information About MPLS VPN ID, on page 2
- How to Configure an MPLS VPN ID, on page 3
- Configuration Examples for Assigning an ID Number to an MPLS VPN, on page 6
- Additional References, on page 6
- Feature Information for MPLS VPN ID, on page 7

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.

Restrictions for MPLS VPN ID

The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in the Multiprotocol Border Gateway Protocol (MP-BGP) VPNv4 routing updates.
Information About MPLS VPN ID

Introduction to MPLS VPN ID

You can identify Virtual Private Networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN. The VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with VPN ID numbers in the Multiprotocol Border Gateway Protocol (MP-BGP) VPNv4 routing updates.

Multiple VPNs can be configured in a device. A VPN is private and uses a private address space that might also be used by another VPN or by the Internet. The IP address used in a VPN is only significant to the VPN in which it exists. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the device. Alternately, you can use a VPN ID to identify a particular VPN in the device. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the devices in the service provider network that services that VPN.

Note

Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the device. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

Components of the MPLS VPN ID

Each MPLS VPN ID defined by RFC 2685 consists of the following elements:

- An Organizational Unique Identifier (OUI), a three-octet hex number: The IEEE Registration Authority assigns OUIs to any company that manufactures components under the ISO/IEC 8802 standard. The OUI is used to generate universal LAN MAC addresses and protocol identifiers for use in local and metropolitan area network applications. For example, an OUI for Cisco Systems is 00-03-6B (hex).

- A Virtual Private Network (VPN) index: a four-octet hex number, which identifies the VPN within the company.

Use the following `vpn id` command and specify the VPN ID:

```
vpn id oui:vpn-index
```

A colon separates the OUI from the VPN index.

Management Applications That Use MPLS VPN IDs

You can use several applications to manage Virtual Private Networks (VPNs) by MPLS VPN ID. Remote access applications, such as the Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP), can use the MPLS VPN ID feature to identify a VPN. RADIUS can use the MPLS VPN ID to assign dial-in users to the proper VPN, based on each user’s authentication information.
Dynamic Host Configuration Protocol

Using Dynamic Host Configuration Protocol (DHCP) network administrators can centrally manage and automate the assignment of IP addresses in an organization’s network. The DHCP application uses the MPLS VPN ID as follows:

1. A Virtual Private Network (VPN) DHCP client requests a connection to a provider edge (PE) device from a virtual routing and forwarding (VRF) interface.
2. The PE device determines the VPN ID associated with that interface.
3. The PE device sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to process the request.
5. The DHCP server sends a response back to the PE device, allowing the VPN DHCP client access to the VPN.

Remote Authentication Dial-In User Service

A RADIUS server (or daemon) provides authentication and accounting services to one or more client network access servers (NASs). RADIUS servers authenticate users and return all configuration information necessary for the client to deliver service to the users.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.

- The Access-Request packet contains the username, encrypted password, NAS IP address, MPLS VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- The RADIUS server returns an Access-Accept response if it finds the username and verifies the password. The response includes a list of attribute-value pairs that describe the parameters to be used for this session. If the user is not authenticated, an Access-Reject is sent by the RADIUS server and access is denied.

How to Configure an MPLS VPN ID

Specifying an MPLS VPN ID

Before you begin

Each virtual routing and forwarding (VRF) instance configured on a provider edge (PE) device can have an MPLS VPN ID configured. Configure all the PE devices that belong to the same Virtual Private Network (VPN) with the same VPN ID. Make sure the VPN ID is unique to the service provider network.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip vrf vrf-name
4. `vpn id oui:vpn-index`:

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip vrf vrf-name</code></td>
<td>Creates a VRF routing table and a Cisco Express Forwarding forwarding table and enters VRF configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip vrf vrf1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>vpn id oui:vpn-index</code></td>
<td>Assigns the VPN ID to the VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-vrf)# vpn id a1:3f6c</code></td>
<td></td>
</tr>
</tbody>
</table>

**Verifying the MPLS VPN ID Configuration**

**SUMMARY STEPS**

1. `enable`
2. `show ip vrf`
3. `show ip vrf id`
4. `show ip vrf detail`

**DETAILED STEPS**

**Step 1**

`enable`

Enables privileged EXEC mode.

**Example:**

Device> enable
Device#
Step 2  show ip vrf

Displays information about the virtual routing and forwarding (VRF) tables on the provider edge (PE) device. This example displays three VRF tables called vpn1, vpn2, and vpn5.

Example:

```
Device# show ip vrf

Name  Default RD  Interfaces
vpn1  100:1       FastEthernet1/1/1
        FastEthernet1/0/0
vpn2  <not set>            
vpn5  500:1       Loopback2
```

Step 3  show ip vrf id

Ensures that the PE device contains the MPLS VPN ID you specified. The following example shows that only VRF tables vpn1 and vpn2 have VPN IDs assigned. The VRF table called vpn5 is not displayed, because it does not have a VPN ID.

Example:

```
Device# show ip vrf id

VPN Id  Name  RD
2:3     vpn2  <not set>
A1:3F6C vpn1  100:1
```

Step 4  show ip vrf detail

Displays all the VRFs on a PE device. This command displays all the MPLS VPN IDs that are configured on the device, their associated VRF names, and VRF route distinguishers (RDs). If a VRF table in the PE device has not been assigned an MPLS VPN ID, that VRF entry is not included in the output.

Example:

```
Device# show ip vrf detail

VRF vpn1; default RD 100:1; default VPNID A1:3F6C
Interfaces:
    FastEthernet1/1/1   FastEthernet1/0/1
Connected addresses are not in global routing table
Export VPN route-target communities
    RT:100:1
Import VPN route-target communities
    RT:100:1
No import route-map
No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
No interfaces
Connected addresses are not in global routing table
No Export VPN route-target communities
No Import VPN route-target communities
No import route-map
No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
Interfaces:
```

Verifying the MPLS VPN ID Configuration
Configuration Examples for Assigning an ID Number to an MPLS VPN

Example: Specifying an MPLS VPN ID

The following example specifies the MPLS VPN ID assigned to the virtual routing and forwarding (VRF) table called vpn1:

```
Device# configure terminal
Device(config)# ip vrf vpn1
Device(config-vrf)# vpn id a1:3f6c
```

Example: Verifying the MPLS VPN ID Configuration

The following is sample output of the `show ip vrf detail` command, one of the commands that can be used to verify the MPLS VPN ID configuration. Use this command to see all the virtual routing and forwarding (VRF) instances on a provider edge (PE) device. This command displays all the MPLS VPN IDs that are configured on the device, their associated VRF names, and VRF route distinguishers (RDs). If a VRF table in the PE device has not been assigned a VPN ID, that VRF entry is not included in the output.

```
Device# show ip vrf detail
VRF vpn1; default RD 100:1; default VPNID A1:3F6C
    Interfaces:
        FastEthernet1/1/1    FastEthernet1/0/1
    Connected addresses are not in global routing table
    Export VPN route-target communities
        RT:100:1
    Import VPN route-target communities
        RT:100:1
    No import route-map
    No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
    No interfaces
    Connected addresses are not in global routing table
    No Export VPN route-target communities
    No Import VPN route-target communities
    No import route-map
    No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
    Interfaces:
```

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco Master Command List, All Releases</td>
</tr>
</tbody>
</table>
Feature Information for MPLS VPN ID

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
</table>
| MPLS VPN ID  | 12.0(17)ST, 12.2(8)T, 12.2(11)S, 12.2(17b)SXA, 12.2(27)SBB, Cisco IOS XE Release 2.1 | You can identify VPNs by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN.
In Cisco IOS Release 12.0(17)ST, this feature was introduced.
In Cisco IOS Releases 12.2(8)T, 12.2(11)S, 12.2(17b)SXA, and 12.2(27)SBB, this feature was integrated.
In Cisco IOS XE Release 2.1, this feature was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
No commands were introduced or modified. |