Hewlett Packard Enterprise

HPE FlexFabric 5700 Switch Series

MCE Command Reference

Part number: 5200-4620
Software version: Release 243x
Document version: 6W100-20171124

Acknowledgments

Contents

MCE commands 1

address-family ipv4 (VPN instance view) 1
description (VPN instance view) 1
display ip vpn-instance 2
domain-id 3
ext-community-type 4
ip binding vpn-instance 4
ip vpn-instance (system view) 5
route-distinguisher (VPN instance view) 6
route-tag 6
routing-table limit 7
vpn-id 9
vpn-instance-capability simple 9
vpn-target (VPN instance view/IPv4 VPN view/IPv6 VPN view) 10

IPv6 MCE commands 12

address-family ipv6 (VPN instance view) 12
domain-id 12
vpn-instance-capability simple 13

Document conventions and icons 15

Conventions 15
Network topology icons 16

Support and other resources 17

Accessing Hewlett Packard Enterprise Support 17
Accessing updates 17
Websites 18
Customer self repair 18
Remote support 18
Documentation feedback 18

Index 20

MCE commands

address-family ipv4 (VPN instance view)

Use **address-family ipv4** in VPN instance view to enter IPv4 VPN view.

Use **undo address-family ipv4** to remove all configurations from IPv4 VPN view.

Syntax

address-family ipv4

undo address-family ipv4

Views

VPN instance view

Predefined user roles

network-admin

Usage guidelines

In IPv4 VPN view, you can configure IPv4 VPN parameters.

Examples

Enter IPv4 VPN view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] address-family ipv4
[Sysname-vpn-ipv4-vpn1]
```

Related commands

address-family ipv6 (VPN instance view)

description (VPN instance view)

Use **description** to configure a description for a VPN instance.

Use **undo description** to delete the description.

Syntax

description *text*

undo description

Default

No description is configured for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

Parameters

text: Specifies a description for the VPN instance, a case-sensitive string of 1 to 79 characters.

Examples

Configure a description of **This is vpn1** for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] description This is vpn1
```

display ip vpn-instance

Use **display ip vpn-instance** to display information about VPN instances.

Syntax

display ip vpn-instance [**instance-name** *vpn-instance-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-name *vpn-instance-name*: Displays information about the specified VPN instance. The *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays brief information about all VPN instances.

Examples

Display brief information about all VPN instances.

```
<Sysname> display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                    Create time
  abc                             1:1                   2011/05/18 10:48:17
```

Table 1 Command output

Field	Description
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance.
Create Time	Time when the VPN instance was created.

Display detailed information about VPN instance **vpn1**.

```
<Sysname> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and Index : vpn1, 2
  Route Distinguisher : 100:1
  VPN ID : 1:1
  Description : vpn1
  Interfaces : Vlan-interface2
  Address-family IPv4:
   Export VPN Targets :
       2:2
   Import VPN Targets :
       3:3
```

```
  Maximum Routes Limit : 5000
 Address-family IPv6:
  Export VPN Targets :
      2:2
  Import VPN Targets :
      3:3
  Maximum Routes Limit : 5000
```

domain-id

Use **domain-id** to configure an OSPF domain ID.

Use **undo domain-id** to restore the default.

Syntax

domain-id *domain-id* [**secondary**]

undo domain-id [*domain-id*]

Default

The OSPF domain ID is 0.

Views

OSPF view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an OSPF domain ID, in one of these formats:

- Integer, in the range of 0 to 4294967295. For example, 1.
- Dotted decimal notation. For example, 0.0.0.1.
- Dotted decimal notation:16-bit user-defined number in the range of 0 to 65535. For example, 0.0.0.1:512.

secondary: Specifies a secondary domain ID. If you do not specify this keyword, the command specifies a primary domain ID.

Usage guidelines

When you redistribute OSPF routes into BGP, BGP adds the primary domain ID to the redistributed BGP VPNv4 routes as a BGP extended community attribute. Then, BGP advertises the routes to the peer PE.

When the peer PE receives the routes, it compares the OSPF domain ID in the routes with the locally configured primary and secondary domain IDs. If the primary or secondary domain ID is the same as the received domain ID, and the received routes are intra-area routes, OSPF advertises these routes in Network Summary LSAs (Type 3). Otherwise, OSPF advertises these routes in AS External LSAs (Type 5) or NSSA External LSAs (Type 7).

If you do not specify any parameters, the **undo domain-id** command deletes all domain IDs.

Examples

Configure the OSPF domain ID as 234.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] domain-id 234
```

ext-community-type

Use **ext-community-type** to configure the type code of an OSPF extended community attribute.

Use **undo ext-community-type** to restore the default.

Syntax

ext-community-type { **domain-id** *type-code1* | **router-id** *type-code2* | **route-type** *type-code3* }

undo ext-community-type [**domain-id** | **router-id** | **route-type**]

Default

The type codes for domain ID, router ID, and route type are hex numbers 0005, 0107, and 0306, respectively.

Views

OSPF view

Predefined user roles

network-admin

Parameters

domain-id *type-code1*: Specifies the type code for domain ID. Valid values are hex numbers 0005, 0105, 0205, and 8005.

router-id *type-code2*: Specifies the type code for router ID. Valid values are hex numbers 0107 and 8001.

router-type *type-code3*: Specifies the type code for route type. Valid values are hex numbers 0306 and 8000.

Examples

Configure the type codes of domain ID, router ID, and route type as hex numbers 8005, 8001, and 8000, respectively, for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ext-community-type domain-id 8005
[Sysname-ospf-100] ext-community-type router-id 8001
[Sysname-ospf-100] ext-community-type route-type 8000
```

ip binding vpn-instance

Use **ip binding vpn-instance** to associate an interface with a VPN instance.

Use **undo ip binding vpn-instance** to remove the association.

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

Default

An interface is associated with no VPN instance and belongs to the public network.

Views

Interface view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Use the command on an MCE to associate the VPN instance with the interface connected to the site and the interface connected to the PE.

This command or its undo form clears the IP address and routing protocol configuration on the interface. After executing this command or its undo form, use the **display this** command to view the current configuration and reconfigure the IP address and routing protocol on the interface.

The specified VPN instance must have been created by using the **ip vpn-instance** command in system view.

To associate a new VPN instance with an interface, you must remove the previous association by using the **undo ip binding vpn-instance** command and then use the **ip binding vpn-instance** command to associate the new VPN instance with the interface.

Examples

Associate interface VLAN-interface 1 with VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1
```

Related commands

ip vpn-instance (system view)

ip vpn-instance (system view)

Use **ip vpn-instance** to create a VPN instance and enter VPN instance view.

Use **undo ip vpn-instance** to delete a VPN instance.

Syntax

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Default

No VPN instance is created.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies the name of the VPN instance, a case-sensitive string of 1 to 31 characters.

Examples

Create a VPN instance named **vpn1**.

```
<Sysname> system-view
```

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

Related commands

route-distinguisher

route-distinguisher (VPN instance view)

Use **route-distinguisher** to configure an RD for a VPN instance.

Use **undo route-distinguisher** to remove the RD of a VPN instance.

Syntax

route-distinguisher *route-distinguisher*

undo route-distinguisher

Default

No RD is specified for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

Parameters

route-distinguisher: Specifies an RD for the VPN instance, a string of 3 to 21 characters in one of these formats:

- *16-bit AS number*:*32-bit user-defined number*. For example, 101:3.
- *32-bit IP address*:*16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number*:*16-bit user-defined number*, where the minimum value of the AS number is 65536. For example, 65536:1.

Usage guidelines

RDs enable VPNs to use the same address space. An RD and an IPv4 prefix comprise a unique VPN IPv4 prefix. You can use RDs to identify different BGP VPN instances on an MCE.

To change the RD of a VPN instance, you must delete the RD with the **undo route-distinguisher** command, and then use the **route-distinguisher** command to configure a new RD.

Examples

Configure RD 22:1 for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

route-tag

Use **route-tag** to configure an external route tag for redistributed VPN routes.

Use **undo route-tag** to restore the default.

Syntax

route-tag *tag-value*

undo route-tag

Default

If BGP runs within an MPLS backbone, and the BGP AS number is not greater than 65535, the first two octets of the external route tag are 0xD000, and the last two octets are the local BGP AS number. For example, if the local BGP AS number is 100, the external route tag value is 3489661028 (100 + the decimal value of 0xD0000000). If the AS number is greater than 65535, the external route tag is 0.

Views

OSPF view

Predefined user roles

network-admin

Parameters

tag-value: Specifies an external route tag for redistributed VPN routes, in the range of 0 to 4294967295.

Usage guidelines

In a dual-homed CE scenario where OSPF runs between the CE and the connected PEs (PE-A and PE-B, for example), you can use external route tags to avoid routing loops.

When PE-A redistributes BGP routes received from the peer PE into OSPF, and advertises these routes in the Type 5 or 7 LSAs to the CE, PE-A adds the locally configured external route tag to Type 5 or 7 LSAs.

When PE-B receives the Type 5 or 7 LSAs advertised by the CE, it compares the external route tag in the LSAs with the locally configured tag. If they are the same, PE-B ignores the LSA in route calculation to avoid routing loops.

The commands used to configure the external route tag (in the descending order of tag priority) are as follows:

- **import-route**
- **route-tag**
- **default tag**

As a best practice, configure the same external route tag for MCEs in the same area.

An external route tag is not transferred in any BGP extended community attribute. It takes effect only on the MCEs that receive BGP routes and generate OSPF Type 5 or 7 LSAs.

You can configure the same external route tag for different OSPF processes.

Examples

In OSPF process 100, set the external route tag for redistributed VPN routes to 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] route-tag 100
```

Related commands

- **default** (*Layer 3—IP Routing Command Reference*)
- **import-route** (*Layer 3—IP Routing Command Reference*)

routing-table limit

Use **routing-table limit** to set the maximum number of active routes in a VPN instance.

Use **undo routing-table limit** to restore the default.

Syntax

routing-table limit *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

Default

The number of active routes in a VPN instance is not limited.

Views

VPN instance view, IPv4 VPN view, IPv6 VPN view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of active routes, in the range of 1 to 1024.

warn-threshold: Specifies a warning threshold in the range of 1 to 100 in percentage. When the percentage of the number of existing active routes to the maximum number of active routes exceeds the specified threshold, the system gives an alarm message but still allows new active routes. If active routes in the VPN instance reach the maximum, no more active routes are added.

simply-alert: Specifies that when active routes exceed the maximum number, the system still accepts active routes but generates a system log message.

Usage guidelines

A limit configured in VPN instance view applies to both the IPv4 VPN and the IPv6 VPN.

A limit configured in IPv4 VPN view or IPv6 VPN view applies to only the IPv4 VPN or the IPv6 VPN.

If you have specified limits in both IPv4 VPN view and VPN instance view, IPv4 VPN uses the limit specified in IPv4 VPN view.

If you have specified limits in both IPv6 VPN view and VPN instance view, IPv6 VPN uses the limit specified in IPv6 VPN view.

Examples

Specify that VPN instance **vpn1** supports up to 1000 active routes, and when active routes exceed the upper limit, can receive new active routes but generates a system log message.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

Specify that the IPv4 VPN **vpn2** supports up to 1000 active routes, and when active routes exceed the upper limit, can receive new active routes but generates a system log message.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn2
[Sysname-vpn-instance-vpn2] route-distinguisher 100:2
[Sysname-vpn-instance-vpn2] address-family ipv4
[Sysname-vpn-ipv4-vpn2] routing-table limit 1000 simply-alert
```

Specify that the IPv6 VPN **vpn3** supports up to 1000 active routes, and when active routes exceed the upper limit, can receive new active routes but generates a system log message.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] route-distinguisher 100:3
[Sysname-vpn-instance-vpn3] address-family ipv6
[Sysname-vpn-ipv4-vpn3] routing-table limit 1000 simply-alert
```

vpn-id

Use **vpn-id** to configure a VPN ID for a VPN instance.

Use **undo vpn-id** to remove the VPN ID of a VPN instance.

Syntax

vpn-id

undo vpn-id

Default

No VPN ID is configured for a VPN instance.

Views

VPN instance view

Predefined user roles

network-admin

Parameters

vpn-id: Specifies a VPN ID for the VPN instance, in the form of OUI:Index. Both OUI and Index are hex numbers. The OUI is in the range of 0 to FFFFFF, and the index is in the range of 0 to FFFFFFFF.

Usage guidelines

The VPN ID uniquely identifies the VPN instance. Different VPN instances must have different VPN IDs.

The VPN ID cannot be 0:0.

Examples

Configure VPN ID 20:1 for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] vpn-id 20:1
```

Related commands

display ip vpn-instance

vpn-instance-capability simple

Use **vpn-instance-capability simple** to disable routing loop detection for an OSPF VRF process.

Use **undo vpn-instance-capability** to restore the default.

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

Default

Routing loop detection is enabled for an OSPF VRF process.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

For the MCE to receive OSPF routes from the PE, you must disable routing loop detection for an OSPF VRF process on the MCE.

This command is applicable only to an OSPF VRF process.

Examples

Disable routing loop detection for OSPF VRF process 100.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpna
[Sysname-ospf-100] vpn-instance-capability simple
```

vpn-target (VPN instance view/IPv4 VPN view/IPv6 VPN view)

Use **vpn-target** to configure route targets for a VPN instance.

Use **undo vpn-target** to remove the specified or all route targets of a VPN instance.

Syntax

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

Default

No route targets are configured for a VPN instance.

Views

VPN instance view, IPv4 VPN view, IPv6 VPN view

Predefined user roles

network-admin

Parameters

vpn-target&<1-8>: Specifies a space-separated list of up to eight route targets.

A route target is a string of 3 to 21 characters in one of these formats:

- *16-bit AS number*:*32-bit user-defined number*. For example, 101:3.
- *32-bit IP address*:*16-bit user-defined number*. For example, 192.168.122.15:1.
- *32-bit AS number*:*16-bit user-defined number*, where the AS number must not be less than 65536. For example, 65536:1.

both: Uses the specified route targets as both import targets and export targets. The **both** keyword is also used when you do not specify any of the following keywords: **both**, **export-extcommunity**, and **import-extcommunity**.

export-extcommunity: Uses the specified route targets as export targets.

import-extcommunity: Uses the specified route targets as import targets.

all: Removes all route targets.

Usage guidelines

MPLS L3VPN uses route targets to control the advertisement of VPN routing information. A PE adds the configured export targets into the route target attribute of routes advertised to a peer. The peer

uses the local import targets to match the route targets of received routes. If a match is found, the peer adds the routes to the routing table of the VPN instance.

Route targets configured in VPN instance view are applicable to both the IPv4 VPN and the IPv6 VPN.

Route targets configured in IPv4 VPN view or IPv6 VPN view are applicable to only the IPv4 VPN or IPv6 VPN.

Route targets configured in IPv4 VPN view or IPv6 VPN view take precedence over those configured in VPN instance view. If you configure route targets in both IPv4 VPN view (or IPv6 VPN view) and VPN instance view, the IPv4 VPN or IPv6 VPN uses the route targets configured in IPv4 VPN view or IPv6 VPN view.

Examples

Configure route targets for VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
```

Configure route targets for the IPv4 VPN **vpn2**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn2
[Sysname-vpn-instance-vpn2] address-family ipv4
[Sysname-vpn-ipv4-vpn2] vpn-target 3:3 export-extcommunity
[Sysname-vpn-ipv4-vpn2] vpn-target 4:4 import-extcommunity
[Sysname-vpn-ipv4-vpn2] vpn-target 5:5 both
```

Configure route targets for the IPv6 VPN **vpn3**.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn3
[Sysname-vpn-instance-vpn3] address-family ipv6
[Sysname-vpn-ipv6-vpn3] vpn-target 3:3 export-extcommunity
[Sysname-vpn-ipv6-vpn3] vpn-target 4:4 import-extcommunity
[Sysname-vpn-ipv6-vpn3] vpn-target 5:5 both
```

IPv6 MCE commands

For information about the commands available for both MCE and IPv6 MCE, see "MCE commands."

address-family ipv6 (VPN instance view)

Use **address-family ipv6** to enter IPv6 VPN view.

Use **undo address-family ipv6** to remove all configurations from IPv6 VPN view.

Syntax

address-family ipv6

undo address-family ipv6

Views

VPN instance view

Predefined user roles

network-admin

Usage guidelines

In IPv6 VPN view, you can configure IPv6 VPN parameters.

Examples

Enter IPv6 VPN view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] address-family ipv6
[Sysname-vpn-ipv6-vpn1]
```

Related commands

address-family ipv4 (VPN instance view)

domain-id

Use **domain-id** to configure an OSPFv3 domain ID.

Use **undo domain-id** to restore the default.

Syntax

domain-id { *domain-id* [**secondary**] | **null** }

undo domain-id [*domain-id* | **null**]

Default

The OSPFv3 domain ID is 0.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an OSPFv3 domain ID, in one of the following formats:

- Integer, in the range of 0 to 4294967295. For example, 1.
- Dotted decimal notation. For example, 0.0.0.1.
- Dotted decimal notation:16-bit user-defined number in the range of 0 to 65535. For example, 0.0.0.1:512.

secondary: Specifies a secondary domain ID. If you do not specify this keyword, the command specifies a primary domain ID.

null: Carries no domain ID in the community attribute.

Usage guidelines

When you redistribute OSPFv3 routes into BGP, BGP adds the primary domain ID to the redistributed BGP VPNv6 routes as a BGP extended community attribute. Then, BGP advertises the routes to the peer PE.

When the peer PE receives the routes, it compares the OSPFv3 domain ID in the routes with the locally configured primary and secondary domain IDs. If the primary or secondary domain ID is the same as the received domain ID, and the received routes are intra-area or inter-area routes, OSPFv3 advertises these routes in Inter-Area-Prefix LSAs (Type 3 LSAs). Otherwise, OSPFv3 advertises these routes in AS External LSAs (Type 5 LSAs) or NSSA External LSAs (Type 7 LSAs).

A null domain ID and a domain ID of 0 are considered the same in domain ID comparison.

You cannot configure a secondary domain ID when the primary domain ID is configured as 0.

With no parameters specified, the **undo domain-id** command deletes all domain IDs.

This command takes effect only for an OSPFv3 VRF process that is not configured with the **vpn-instance-capability simple** command.

Examples

Configure the primary domain ID for OSPFv3 VRF process 100 as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 100 vpn-instance vpn1
[Sysname-ospfv3-100] domain-id 1.1.1.1
```

Related commands

display ospfv3 (*Layer 3—IP Routing Command Reference*)

vpn-instance-capability simple

Use **vpn-instance-capability simple** to disable routing loop detection for an OSPFv3 VRF process.

Use **undo vpn-instance-capability** to restore the default.

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

Default

Routing loop detection is enabled for an OSPFv3 VRF process.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

For the MCE to receive OSPFv3 routes from the PE, you must disable routing loop detection for an OSPFv3 VRF process on the MCE.

This command is applicable only to an OSPFv3 VRF process.

Examples

Disable routing loop detection for OSPFv3 VRF process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100 vpn-instance vpn1
[Sysname-ospfv3-100] vpn-instance-capability simple
```

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
    http://www.hpe.com/support/e-updates
  - Software Depot website:
    http://www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
  http://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	http://www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	http://www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	http://www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	http://www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	http://www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	http://www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	http://www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	http://ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	http://www.hpe.com/assistance
Subscription Service/Support Alerts	http://www.hpe.com/support/e-updates
Software Depot	http://www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	http://www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	http://www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

http://www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation

Feedback (mailto:docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

A C D E I R V W

A

address-family ipv4 (VPN instance view),1
address-family ipv6 (VPN instance view),12

C

Customer self repair,18

D

description (VPN instance view),1
display ip vpn-instance,2
Documentation feedback,18
domain-id,3
domain-id,12

E

ext-community-type,4

I

ip binding vpn-instance,4
ip vpn-instance (system view),5

R

Remote support,18
route-distinguisher (VPN instance view),6
route-tag,6
routing-table limit,7

V

vpn-id,9
vpn-instance-capability simple,9
vpn-instance-capability simple,13
vpn-target (VPN instance view/IPv4 VPN view/IPv6 VPN view),10

W

Websites,18