H3C S5560X-EI Switch Series

VXLAN Command Reference

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 1118
Document version: 6W100-20180209

Preface

This command reference describes the VXLAN configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the S5560X-EI switch series.

Conventions

The following information 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 a minimum of 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.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

VXLAN commands

Basic VXLAN commands

ac statistics enable

Use **ac statistics enable** to enable packet statistics for Ethernet service instances of a VLAN.

Use **undo ac statistics enable** to disable packet statistics for Ethernet service instances of a VLAN.

Syntax

ac statistics enable

undo ac statistics enable

Default

The packet statistics feature is disabled for Ethernet service instances of a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables packet statistics for the Ethernet service instances automatically created for VLAN-based VXLAN assignment.

Before you enable this feature, you must use the **vxlan vlan-based** command to enable VLAN-based VXLAN assignment.

Examples

Map VLAN 10 to VXLAN 100, and enable packet statistics for Ethernet service instances of VLAN 10.

```
<Sysname> system-view
[Sysname] vxlan vlan-based
[Sysname] vlan 10
[Sysname-vlan10] vxlan vni 100
[Sysname-vlan10] ac statistics enable
```

Related commands

display l2vpn service-instance

reset l2vpn statistics ac

vxlan vlan-based

arp suppression enable

Use **arp suppression enable** to enable ARP flood suppression.

Use **undo arp suppression enable** to disable ARP flood suppression.

Syntax

arp suppression enable

undo arp suppression enable

Default

ARP flood suppression is disabled.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

ARP flood suppression reduces ARP request broadcasts by enabling the VTEP to reply to ARP requests on behalf of VMs.

This feature snoops ARP packets to populate the ARP flood suppression table with local and remote MAC addresses. If an ARP request has a matching entry, the VTEP replies to the request on behalf of the VM. If no match is found, the VTEP floods the request to both local and remote sites.

Examples

Enable ARP flood suppression for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] arp suppression enable
```

Related commands

display arp suppression vsi

reset arp suppression vsi

arp suppression ip-source-binding record

Use **arp suppression ip-source-binding record** to enable the device to generate dynamic IPv4SG bindings based on ARP flood suppression entries.

Use **undo arp suppression ip-source-binding record** to disable the device from generating dynamic IPv4SG bindings based on ARP flood suppression entries.

Syntax

arp suppression ip-source-binding record

undo arp suppression ip-source-binding record

Default

The device does not generate dynamic IPv4SG bindings based on ARP flood suppression entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you execute this command, the device notifies the IP source guard module of ARP flood suppression entries for it to generate dynamic IPv4SG bindings based on these entries.

For more information about IP source guard, see *Security Configuration Guide*.

Examples

Enable the device to generate dynamic IPv4SG bindings based on ARP flood suppression entries.

```
<Sysname> system-view
[Sysname] arp suppression ip-source-binding record
```

Related commands

arp suppression enable

reset arp suppression vsi

description

Use **description** to configure a description for a VSI.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A VSI does not have a description.

Views

VSI view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Examples

Configure a description for VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] description vsi for vpn1
```

Related commands

display l2vpn vsi

display arp suppression vsi

Use **display arp suppression vsi** to display ARP flood suppression entries.

Syntax

display arp suppression vsi [**name** *vsi-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays entries on the master device.

count: Displays the number of ARP flood suppression entries that match the command.

Examples

Display ARP flood suppression entries.

```
<Sysname> display arp suppression vsi
IP address      MAC address    Vsi Name                        Link ID    Aging
1.1.1.2         000f-e201-0101 vsi1                            0x70000    14
1.1.1.3         000f-e201-0202 vsi1                            0x80000    18
1.1.1.4         000f-e201-0203 vsi2                            0x90000    10
```

Display the number of ARP flood suppression entries.

```
<Sysname> display arp suppression vsi count
Total entries: 3
```

Table 1 Command output

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
Aging	Remaining lifetime (in minutes) of the ARP flood suppression entry. When the timer expires, the entry is deleted.

Related commands

arp suppression enable

reset arp suppression vsi

display ipv6 nd suppression vsi

Use **display ipv6 nd suppression vsi** to display ND flood suppression entries.

Syntax

display ipv6 nd suppression vsi [**name** *vsi-name*] [**slot** *slot-number*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays entries for all VSIs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays entries on the master device.

count: Displays the number of ND flood suppression entries that match the command.

Examples

Display ND flood suppression entries.

```
<Sysname> display ipv6 nd suppression vsi
IPv6 address    MAC address      VSI Name         Link ID      Aging (min)
1000::2         000f-e201-0101   vsi1             0x70000      5
1000::3         000f-e201-0202   vsi1             0x80000      5
1000::4         000f-e201-0203   vsi2             0x90000      5
```

Display the number of ND flood suppression entries.

```
<Sysname> display ipv6 nd suppression vsi count
Total entries: 3
```

Table 2 Command output

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
Aging (min)	Remaining lifetime (in minutes) of the ND flood suppression entry. When the timer expires, the entry is deleted.

Related commands

ipv6 nd suppression enable

reset ipv6 nd suppression vsi

display l2vpn mac-address

Use **display l2vpn mac-address** to display MAC address entries for VSIs.

Syntax

display l2vpn mac-address [**vsi** *vsi-name*] [**dynamic**] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays MAC address entries for all VSIs.

dynamic: Specifies dynamic MAC address entries learned in the data plane. If you do not specify this keyword, the command displays all MAC address entries, including:

- Dynamic remote- and local-MAC entries.
- Remote-MAC entries advertised through BGP EVPN.
- Manually added static remote-MAC entries.
- Remote-MAC entries issued through OpenFlow.
- Remote-MAC entries issued through OVSDB.

count: Displays the number of MAC address entries.

verbose: Displays detailed information about MAC address entries.

Usage guidelines

If you do not specify the **count** or **verbose** keyword, this command displays brief information about MAC address entries.

Examples

Display brief information about MAC address entries for all VSIs.

```
<Sysname> display l2vpn mac-address
MAC Address      State    VSI Name                        Link ID/Name  Aging
0000-0000-000b   Static   vpn1                            Tunnel10      NotAging
0000-0000-000c   Dynamic  vpn1                            Tunnel60      Aging
0000-0000-000d   Dynamic  vpn1                            Tunnel99      Aging
--- 3 mac address(es) found  ---
```

Display the total number of MAC address entries in all VSIs.

```
<Sysname> display l2vpn mac-address count
3 mac address(es) found
```

Table 3 Command output

Field	Description
State	Entry state: • **Dynamic**—Local- or remote-MAC entry dynamically learned in the data plane. • **Static**—Static remote-MAC entry. • **EVPN**—Remote-MAC entry advertised through BGP EVPN. • **OpenFlow**—Remote-MAC entry issued by a remote controller through OpenFlow. • **OVSDB**—Remote-MAC entry issued by a remote controller through OVSDB.
Link ID/Name	For a local MAC address, this field displays the name of the interface that hosts the Ethernet service instance for the MAC address. For a remote MAC address, this field displays the tunnel interface name.
Aging	Entry aging state: • **Aging**. • **NotAging**.

Display detailed information about MAC address entries for all VSIs.

```
<Sysname> display l2vpn mac-address verbose
MAC Address : 0000-0000-000b
VSI Name    : vpn1
VXLAN ID    : 123
Interface   : GE1/0/1
Link ID     : 1
State       : Dynamic
Aging       : Aging
```

Table 4 Command output

Field	Description
Interface	For a local MAC address, this field displays the name of the interface that hosts the Ethernet service instance for the MAC address. For a remote MAC address, this field displays the tunnel interface name.

Field	Description
Link ID	Link ID that uniquely identifies an AC or a VXLAN tunnel on a VSI.
State	Entry state: • **Dynamic**—Local- or remote-MAC entry dynamically learned in the data plane. • **Static**—Static remote-MAC entry. • **EVPN**—Remote-MAC entry advertised through BGP EVPN. • **OpenFlow**—Remote-MAC entry issued by a remote controller through OpenFlow. • **OVSDB**—Remote-MAC entry issued by a remote controller through OVSDB.
Aging	Entry aging state: • **Aging**. • **NotAging**.

Related commands

`reset l2vpn mac-address`

display l2vpn service-instance

Use **`display l2vpn service-instance`** to display information about Ethernet service instances.

Syntax

`display l2vpn service-instance` [**`interface`** *`interface-type interface-number`* [**`service-instance`** *`instance-id`*]] [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`interface` *`interface-type interface-number`*: Specifies a Layer 2 Ethernet interface or Layer 2 aggregate interface by its interface type and number. If you do not specify an interface, this command displays Ethernet service instance information for all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

`service-instance` *`instance-id`*: Specifies an Ethernet service instance by its ID in the range of 1 to 4096. If you do not specify an Ethernet service instance, this command displays information about all Ethernet service instances on the specified Layer 2 Ethernet interface or Layer 2 aggregate interface.

`verbose`: Displays detailed information about Ethernet service instances. If you do not specify this keyword, the command displays brief information about Ethernet service instances.

Examples

Display brief information about all Ethernet service instances.

```
<Sysname> display l2vpn service-instance
Total number of service-instances: 4, 4 up, 0 down
Total number of ACs: 2, 2 up, 0 down

Interface               SrvID Owner                         LinkID State Type
```

```
GE1/0/1                  3      vsi12                          1       Up     VSI
GE1/0/1                  4      vsi13                          1       Up     VSI
```

Table 5 Command output

Field	Description
Total number of ACs	Total number of attachment circuits (ACs) and the number of ACs in each state (up or down).
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
SrvID	Ethernet service instance ID.
Owner	VSI name. This field is empty if an Ethernet service instance is not mapped to any VSI.
LinkID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state: • **Up**. • **Down**.
Type	L2VPN type of the Ethernet service instance: • **VSI**. • **VPWS**.

Display detailed information about all Ethernet service instances on GigabitEthernet 1/0/1.

```
<Sysname> display l2vpn service-instance interface gigabitethernet 1/0/1 verbose
Interface: GE1/0/1
  Service Instance: 1
    Type          : Manual
    Encapsulation : s-vid 16
    Bandwidth     : -
    VSI Name      : vsi10
    Link ID       : 1
    State         : Up
    Statistics    : Enabled
    Input Statistics:
      Octets   :0
      Packets  :0
    Output Statistics:
      Octets   :0
      Packets  :0
```

Table 6 Command output

Field	Description
Interface	Name of a Layer 2 Ethernet interface or Layer 2 aggregate interface.
Service Instance	Ethernet service instance ID.
Type	Type and traffic match mode of the Ethernet service instance: • **Dynamic (MAC-based)**—Dynamic Ethernet service instance in MAC-based traffic match mode. • **Manual**—Static Ethernet service instance in VLAN-based traffic match mode.
Encapsulation	Frame match criterion of the Ethernet service instance. If the Ethernet service instance does not contain a match criterion, the command does not display this field.

Field	Description
Bandwidth	This field is not supported in the current software version. Bandwidth limit in kbps. If no bandwidth limit is set for the Ethernet service instance, **Unlimited** is displayed.
Link ID	Ethernet service instance's link ID on the VSI.
State	Ethernet service instance state: • **Up**. • **Down**.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the Ethernet service instance. • **Disabled**—The packet statistics feature is disabled for the Ethernet service instance.
Input Statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets.
Output Statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets.

Related commands

service-instance

display l2vpn vsi

Use **display l2vpn vsi** to display information about VSIs.

Syntax

display l2vpn vsi [**name** *vsi-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays information about all VSIs.

verbose: Displays detailed information about VSIs. If you do not specify this keyword, the command displays brief information about VSIs.

Examples

Display brief information about all VSIs.

```
<Sysname> display l2vpn vsi
Total number of VSIs: 1, 1 up, 0 down, 0 admin down

VSI Name                        VSI Index       MTU    State
vpna                            0               1500   Up
```

Table 7 Command output

Field	Description
MTU	MTU on the VSI.
State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Admin down**—The VSI has been manually shut down by using the **shutdown** command.

Display detailed information about all VSIs.

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Enabled
  Input statistics:
    Octets   : 0
    Packets  : 0
    Errors   : 0
    Discards : 0
  Output statistics:
    Octets   : 0
    Packets  : 0
    Errors   : 0
    Discards : 0
  Gateway Interface       : VSI-interface 100
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type      Flood proxy
    Tunnel1              0x5000001  Up     Manual    Disabled
    Tunnel2              0x5000002  Up     Manual    Disabled
    MTunnel0             0x6002710  Up     Auto      Disabled
  ACs:
    AC                              Link ID    State    Type
    GE1/0/1 srv1000                 0          Up       Manual
```

Table 8 Command output

Field	Description
VSI Description	Description of the VSI. If the VSI does not have a description, the command does not display this field.
VSI State	VSI state: • **Up**—The VSI is up. • **Down**—The VSI is down. • **Administratively down**—The VSI has been manually shut down by using the **shutdown** command.
MTU	MTU on the VSI.
Bandwidth	This field is not supported in the current software version. Bandwidth limit in kbps. If no bandwidth limit is set for the VSI, **Unlimited** is displayed.
Broadcast Restrain	This field is not supported in the current software version. Broadcast restraint bandwidth (in kbps). If the broadcast restraint bandwidth is not set, **Unlimited** is displayed.
Multicast Restrain	This field is not supported in the current software version. Multicast restraint bandwidth (in kbps). If the multicast restraint bandwidth is not set, **Unlimited** is displayed.
Unknown Unicast Restrain	This field is not supported in the current software version. Unknown unicast restraint bandwidth (in kbps). If the unknown unicast restraint bandwidth is not set, **Unlimited** is displayed.
MAC Learning	State of the MAC learning feature.
MAC Table Limit	This field is not supported in the current software version. Maximum number of MAC address entries on the VSI.
MAC Learning rate	This field is not supported in the current software version. MAC address entry learning rate of the VSI.
Drop Unknown	This field is not supported in the current software version. Action on source MAC-unknown frames received after the maximum number of MAC entries is reached.
Flooding	State of the VSI's flooding feature: • **Enabled**—Flooding is enabled on the VSI. • **Disabled**—Flooding is disabled on the VSI.
Statistics	Packet statistics state: • **Enabled**—The packet statistics feature is enabled for the VSI. • **Disabled**—The packet statistics feature is disabled for the VSI.
Input statistics	Incoming traffic statistics: • **Octets**—Number of incoming bytes. • **Packets**—Number of incoming packets. • **Errors**—Number of error packets. • **Discards**—Number of discarded packets.
Output statistics	Outgoing traffic statistics: • **Octets**—Number of outgoing bytes. • **Packets**—Number of outgoing packets. • **Errors**—Number of error packets.

Field	Description
	• **Discards**—Number of discarded packets.
Gateway Interface	VSI interface name.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Down**—The tunnel interface is down.
Type	Tunnel assignment method: • **Auto**—The tunnel was automatically assigned to the VXLAN. For an EVPN network, VXLAN tunnels are automatically assigned to VXLANs. • **Manual**—The tunnel was manually assigned to the VXLAN.
Flood proxy	Flood proxy state. This field is not supported in the current software version.
ACs	ACs that are bound to the VSI.
Link ID	AC's link ID on the VSI.
State	AC state: • **Up**. • **Down**.
Type	Type and traffic match mode of the Ethernet service instance: • **Dynamic (MAC-based)**—Dynamic Ethernet service instance in MAC-based traffic match mode. • **Manual**—Static Ethernet service instance in VLAN-based traffic match mode.

display vxlan tunnel

Use **display vxlan tunnel** to display VXLAN tunnel information for VXLANs.

Syntax

display vxlan tunnel [**vxlan-id** *vxlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215. If you do not specify a VXLAN, this command displays VXLAN tunnel information for all VXLANs.

Examples

Display VXLAN tunnel information for all VXLANs.

```
<Sysname> display vxlan tunnel
Total number of VXLANs: 1

VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name          Link ID    State  Type         Flood proxy
Tunnel1              0x5000001  Up     Manual       Disabled
Tunnel2              0x5000002  Up     Manual       Disabled
```

```
MTunnel0            0x6002710  Up     Auto         Disabled
```

Display VXLAN tunnel information for VXLAN **10**.

```
<Sysname> display vxlan tunnel vxlan-id 10
VXLAN ID: 10, VSI name: vpna, Total tunnels: 3 (3 up, 0 down, 0 defect, 0 blocked)
Tunnel name         Link ID    State  Type         Flood proxy
Tunnel1             0x5000001  Up     Manual       Disabled
Tunnel2             0x5000002  Up     Manual       Disabled
MTunnel0            0x6002710  Up     Auto         Disabled
```

Table 9 Command output

Field	Description
Link ID	Tunnel's link ID in the VXLAN.
State	Tunnel state: • **Up**—The tunnel is operating correctly. • **Down**—The tunnel interface is down.
Type	Tunnel assignment method: • **Auto**—The tunnel was automatically assigned to the VXLAN. For an EVPN network, VXLAN tunnels are automatically assigned to VXLANs. • **Manual**—The tunnel was manually assigned to the VXLAN.
Flood proxy	Flood proxy state. This field is not supported in the current software version.

Related commands

tunnel

vxlan

encapsulation

Use **encapsulation** to configure a frame match criterion for an Ethernet service instance.

Use **undo encapsulation** to restore the default.

Syntax

encapsulation s-vid *vlan-id* [**only-tagged**]

encapsulation untagged

undo encapsulation

Default

An Ethernet service instance does not contain a frame match criterion.

Views

Ethernet service instance view

Predefined user roles

network-admin

Parameters

s-vid: Matches frames that are tagged with the specified outer 802.1Q VLAN IDs.

vlan-id: Specifies an 802.1Q VLAN ID in the range of 1 to 4094.

only-tagged: Matches tagged frames. If the outer 802.1Q VLAN is not the PVID, the matching result does not differ, whether or not you specify the **only-tagged** keyword. If the outer 802.1Q VLAN is the PVID, the matching result depends on whether or not the **only-tagged** keyword is specified.

- To match only PVID-tagged frames, specify the **only-tagged** keyword.
- To match both untagged frames and PVID-tagged frames, do not specify the **only-tagged** keyword.

untagged: Matches any frames that do not have an 802.1Q VLAN tag.

Usage guidelines

An Ethernet service instance can contain only one match criterion. To change the match criterion, first execute the **undo encapsulation** command to remove the original criterion. When you remove the match criterion in an Ethernet service instance, the mapping between the service instance and the VSI is removed automatically.

Examples

Configure Ethernet service instance 1 on GigabitEthernet 1/0/1 to match frames that have an outer 802.1Q VLAN ID of 111.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1
[Sysname-GigabitEthernet1/0/1-srv1] encapsulation s-vid 111
```

Related commands

display l2vpn service-instance

flooding disable

Use **flooding disable** to disable flooding for a VSI.

Use **undo flooding disable** to enable flooding for a VSI.

Syntax

flooding disable { **all** | { **broadcast** | **unknown-multicast** | **unknown-unicast** } * }

undo flooding disable

Default

Flooding is enabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

Parameters

all: Specifies broadcast, unknown unicast, and unknown multicast traffic.

broadcast: Specifies broadcast traffic.

unknown-multicast: Specifies unknown multicast traffic.

unknown-unicast: Specifies unknown unicast traffic.

Usage guidelines

By default, the device floods broadcast, unknown unicast, and unknown multicast frames received from the local site to the following interfaces in the frame's VXLAN:

- All site-facing interfaces except for the incoming interface.
- All VXLAN tunnel interfaces.

To confine a kind of flood traffic to the site-facing interfaces, use this command to disable flooding for that kind of flood traffic on the VSI bound to the VXLAN. The VSI will not flood the corresponding frames to VXLAN tunnel interfaces.

Examples

Disable flooding of broadcast traffic for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] flooding disable broadcast
```

ipv6 nd suppression enable

Use **ipv6 nd suppression enable** to enable ND flood suppression.

Use **undo ipv6 nd suppression enable** to disable ND flood suppression.

Syntax

ipv6 nd suppression enable

undo ipv6 nd suppression enable

Default

ND flood suppression is disabled.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

ND flood suppression reduces ND request multicasts by enabling the VTEP to reply to ND requests on behalf of user terminals.

This feature snoops ND packets to populate the ND flood suppression table with local and remote MAC addresses. If an ND request has a matching entry, the VTEP replies to the request on behalf of the user terminal. If no match is found, the VTEP floods the request to both local and remote sites.

Examples

Enable ND flood suppression for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] ipv6 nd suppression enable
```

Related commands

display ipv6 nd suppression vsi

reset ipv6 nd suppression vsi

ipv6 nd suppression notify-ipsg

Use **ipv6 nd suppression notify-ipsg** to enable the device to generate dynamic IPv6SG bindings based on ND flood suppression entries.

Use **undo ipv6 nd suppression notify-ipsg** to disable the device from generating dynamic IPv6SG bindings based on ND flood suppression entries.

Syntax

ipv6 nd suppression notify-ipsg

undo ipv6 nd suppression notify-ipsg

Default

The device does not generate dynamic IPv6SG bindings based on ND flood suppression entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you execute this command, the device notifies the IP source guard module of ND flood suppression entries for it to generate dynamic IPv6SG bindings based on these entries.

For more information about IP source guard, see *Security Configuration Guide*.

Examples

Enable the device to generate dynamic IPv6SG bindings based on ND flood suppression entries.

```
<Sysname> system-view
[Sysname] ipv6 nd suppression notify-ipsg
```

Related commands

display ipv6 source binding (*Security Command Reference*)

ipv6 nd suppression enable

l2vpn enable

Use **l2vpn enable** to enable L2VPN.

Use **undo l2vpn enable** to disable L2VPN.

Syntax

l2vpn enable

undo l2vpn enable

Default

L2VPN is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must enable L2VPN before you can configure L2VPN settings.

Examples

Enable L2VPN.

```
<Sysname> system-view
[Sysname] l2vpn enable
```

mac-address static vsi

Use **mac-address static vsi** to add a static remote-MAC address entry for a VXLAN VSI.

Use **undo mac-address static vsi** to remove a static remote-MAC address entry for a VXLAN VSI.

Syntax

mac-address static *mac-address* **interface tunnel** *tunnel-number* **vsi** *vsi-name*

undo mac-address static [*mac-address*] **interface tunnel** *tunnel-number* **vsi** *vsi-name*

Default

VXLAN VSIs do not have static remote-MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format. Do not specify a multicast MAC address or an all-zeros MAC address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for **000f-00e2-0001**.

interface tunnel *tunnel-number*: Specifies a VXLAN tunnel interface by its tunnel interface number. The specified tunnel interface must already exist.

vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A remote MAC address is the MAC address of a VM in a remote site. Remote MAC entries include manually added MAC entries, dynamically learned MAC entries, and MAC entries advertised through BGP EVPN.

When you add a remote MAC address entry, make sure the VSI's VXLAN has been specified on the VXLAN tunnel.

Do not configure static remote-MAC entries for tunnels that are automatically established by using EVPN.

- EVPN re-establishes tunnels if the transport-facing interface goes down and then comes up. If you have configured static remote-MAC entries, the entries are deleted when the tunnels are re-established.
- EVPN re-establishes tunnels if you perform configuration rollback. If the tunnel IDs change during tunnel re-establishment, configuration rollback fails, and static remote-MAC entries on the tunnels cannot be restored.

The **undo mac-address static vsi** *vsi-name* command removes all static remote-MAC address entries for a VSI.

Examples

Add MAC address **000f-e201-0101** to VSI **vsi1**. Specify Tunnel-interface 1 as the outgoing interface.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface tunnel 1 vsi vsi1
```

Related commands

vxlan tunnel mac-learning disable

mac-based ac

Use **mac-based ac** to enable MAC-based traffic match mode for dynamic Ethernet service instances on an interface.

Use **undo mac-based ac** to disable MAC-based traffic match mode for dynamic Ethernet service instances on an interface.

Syntax

mac-based ac

undo mac-based ac

Default

MAC-based traffic match mode is disabled for dynamic Ethernet service instances.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X or MAC authentication feature can use the authorization VSI, the guest VSI, the Auth-Fail VSI, and the critical VSI to control the access of users to network resources. When assigning a user to a VSI, 802.1X or MAC authentication sends the VXLAN feature the VSI information and the user's access information, including access interface, VLAN, and MAC address. Then the VXLAN feature creates a dynamic Ethernet service instance for the user and maps it to the VSI.

A dynamic Ethernet service instance matches frames by VLAN ID and source MAC address. To use MAC-based traffic matching for dynamic Ethernet service instances, you must enable MAC authentication or 802.1X authentication that uses MAC-based access control.

This command takes effect only on dynamic Ethernet service instances. Static Ethernet service instances created by using the **service-instance** command match traffic only by the VLAN IDs specified by using the **encapsulation** command.

You cannot change the traffic match mode when dynamic Ethernet service instances already exist on an interface.

Examples

Enable MAC-based traffic match mode for dynamic Ethernet service instances on GigabitEthernet 1/0/1.

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-based ac
```

Related commands

display l2vpn service-instance

reserved vxlan

Use **reserved vxlan** to specify a reserved VXLAN.

Use **undo reserved vxlan** to restore the default.

Syntax

reserved vxlan *vxlan-id*

undo reserved vxlan

Default

No VXLAN has been reserved.

Views

System view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

You can specify only one reserved VXLAN on the VTEP. The reserved VXLAN cannot be the VXLAN created on any VSI.

Examples

Specify VXLAN 10000 as the reserved VXLAN.

```
<Sysname> system-view
[Sysname] reserved vxlan 10000
```

reset arp suppression vsi

Use **reset arp suppression vsi** to clear ARP flood suppression entries on VSIs.

Syntax

reset arp suppression vsi [**name** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears ARP flood suppression entries on all VSIs.

Examples

Clear ARP flood suppression entries on all VSIs.

```
<Sysname> reset arp suppression vsi
This command will delete all entries. Continue? [Y/N]:y
```

Related commands

arp suppression enable

display arp suppression vsi

reset ipv6 nd suppression vsi

Use **reset ipv6 nd suppression vsi** to clear ND flood suppression entries on VSIs.

Syntax

reset ipv6 nd suppression vsi [**name** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears ND flood suppression entries on all VSIs.

Examples

Clear ND flood suppression entries on all VSIs.

```
<Sysname> reset ipv6 nd suppression vsi
This command will delete all entries. Continue? [Y/N]:y
```

Related commands

display ipv6 nd suppression vsi

ipv6 nd suppression enable

reset l2vpn mac-address

Use **reset l2vpn mac-address** to clear dynamic MAC address entries on VSIs.

Syntax

reset l2vpn mac-address [**vsi** *vsi-name*]

Views

User view

Predefined user roles

network-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command clears all dynamic MAC address entries on all VSIs.

Usage guidelines

Use this command when the number of dynamic MAC address entries reaches the limit or the device learns incorrect MAC addresses.

Examples

Clear the dynamic MAC address entries on VSI **vpn1**.

```
<Sysname> reset l2vpn mac-address vsi vpn1
```

Related commands

display l2vpn mac-address vsi

reset l2vpn statistics ac

Use **reset l2vpn statistics ac** to clear packet statistics on ACs.

Syntax

reset l2vpn statistics ac [**interface** *interface-type interface-number* [**service-instance** *instance-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

service-instance *instance-id*: Specifies an Ethernet service instance ID in the range of 1 to 4096.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics on all ACs.

Examples

Clear packet statistics for Ethernet service instance 1 on GigabitEthernet 1/0/1.

```
<Sysname> reset l2vpn statistics ac interface gigabitethernet 1/0/1 service-instance 1
```

Related commands

ac statistics enable

display l2vpn interface

display l2vpn service-instance verbose

statistics enable (Ethernet service instance view)

service-instance

Use **service-instance** to create an Ethernet service instance and enter its view, or enter the view of an existing Ethernet service instance.

Use **undo service-instance** to delete an Ethernet service instance.

Syntax

service-instance *instance-id*

undo service-instance *instance-id*

Default

No Ethernet service instances exist.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an Ethernet service instance ID in the range of 1 to 4096.

Examples

On Layer 2 Ethernet interface GigabitEthernet 1/0/1, create Ethernet service instance 1 and enter Ethernet service instance view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1
[Sysname-GigabitEthernet1/0/1-srv1]
```

Related commands

display l2vpn service-instance

shutdown

Use **shutdown** to shut down a VSI.

Use **undo shutdown** to bring up a VSI.

Syntax

shutdown

undo shutdown

Default

VSIs are up.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

Use this command to temporarily disable a VSI to provide Layer 2 switching services. The shutdown action does not change settings on the VSI. You can continue to configure the VSI. After you bring up the VSI again, the VSI provides services based on the latest settings.

Examples

Shut down VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
```

```
[Sysname-vsi-vpn1] shutdown
```

Related commands

display l2vpn vsi

statistics enable (Ethernet service instance view)

Use **statistics enable** to enable packet statistics for an Ethernet service instance.

Use **undo statistics enable** to disable packet statistics for an Ethernet service instance.

Syntax

statistics enable

undo statistics enable

Default

The packet statistics feature is disabled for an Ethernet service instance.

Views

Ethernet service instance view

Predefined user roles

network-admin

Usage guidelines

For this command to take effect, you must configure a frame match criterion for the Ethernet service instance and map it to a VSI. If you modify the frame match criterion or VSI mapping, packet statistics of the instance is cleared.

Examples

Enable packet statistics for Ethernet service instance 200 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 200
[Sysname-GigabitEthernet1/0/1-srv200] statistics enable
```

Related command

display l2vpn service-instance verbose

reset l2vpn statistics ac

statistics enable (VSI view)

Use **statistics enable** to enable packet statistics for a VSI.

Use **undo statistics enable** to disable packet statistics for a VSI.

Syntax

statistics enable

undo statistics enable

Default

The packet statistics feature is disabled for a VSI.

Views

VSI view

Predefined user roles

network-admin

Examples

Enable packet statistics for VSI **vsi1**.

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] statistics enable
```

Related commands

display l2vpn vsi verbose

reset l2vpn statistics vsi

tunnel

Use **tunnel** to assign VXLAN tunnels to a VXLAN.

Use **undo tunnel** to remove VXLAN tunnels from a VXLAN.

Syntax

tunnel { *tunnel-number* [**backup-tunnel** *tunnel-number*] | **all** }

undo tunnel { *tunnel-number* | **all** }

Default

A VXLAN does not contain VXLAN tunnels.

Views

VXLAN view

Predefined user roles

network-admin

Parameters

*tunnel-numb*er: Specifies a tunnel interface number. The value range for this argument is 0 to 511. The tunnel must be a VXLAN tunnel.

backup-tunnel *tunnel-number*: Specifies a backup tunnel by its tunnel interface number. The value range for the *tunnel-number* argument is 0 to 511. The tunnel must be a VXLAN tunnel.

all: Specifies all VXLAN tunnels.

Usage guidelines

This command assigns a VXLAN tunnel to a VXLAN to provide Layer 2 connectivity for the VXLAN between two sites. In unicast mode, the system floods unknown unicast, multicast, and broadcast traffic to each tunnel in the VXLAN.

You can assign multiple VXLAN tunnels to a VXLAN, and configure a VXLAN tunnel to trunk multiple VXLANs.

To assign a pair of primary and backup VXLAN tunnels to the VXLAN, specify the **backup-tunnel** *tunnel-number* option. When the primary VXLAN tunnel is operating correctly, the backup VXLAN tunnel does not forward traffic. When the primary VXLAN tunnel goes down, traffic is switched to the backup VXLAN tunnel.

If the **tunnel all** command is used for a VXLAN, you cannot remove the VXLAN tunnels one by one. You can only use the **undo tunnel all** command to remove all the VXLAN tunnels.

Examples

Assign VXLAN tunnels 1 and 2 to VXLAN 10000.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] vxlan 10000
[Sysname-vsi-vpna-vxlan-10000] tunnel 1
[Sysname-vsi-vpna-vxlan-10000] tunnel 2
```

Related commands

display vxlan tunnel

tunnel bfd enable

Use **tunnel bfd enable** to enable BFD on a VXLAN tunnel interface.

Use **undo tunnel bfd enable** to disable BFD on a VXLAN tunnel interface.

Syntax

tunnel bfd enable destination-mac *mac-address*

undo tunnel bfd enable

Default

BFD is disabled on a VXLAN tunnel interface.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

Parameters

destination-mac *mac-address*: Specifies a destination MAC address in H-H-H format for BFD control packets. The MAC address can be a remote VTEP address or a multicast address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for **000f-00e2-0001**.

Usage guidelines

Enable BFD on both ends of a VXLAN tunnel for quick link connectivity detection. The VTEPs periodically send BFD single-hop control packets to each other through the VXLAN tunnel. A VTEP sets the tunnel state to Defect if it has not received control packets from the remote end for 5 seconds. In this situation, the tunnel interface state is still Up. The tunnel state will change from Defect to Up if the VTEP can receive BFD control packets again.

For BFD sessions to come up, you must reserve a VXLAN by using the **reserved vxlan** command.

Examples

Enable BFD on VXLAN tunnel interface Tunnel 9, and specify 1-1-1 as the destination MAC address for BFD control packets.

```
<Sysname> system-view
[Sysname] interface tunnel 9 mode vxlan
[Sysname-Tunnel9] tunnel bfd enable destination-mac 1-1-1
```

tunnel global source-address

Use **tunnel global source-address** to specify a global source address for VXLAN tunnels.

Use **undo tunnel global source-address** to restore the default.

Syntax

tunnel global source-address *ip-address*

undo tunnel global source-address

Default

No global source address is specified for VXLAN tunnels.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address.

Usage guidelines

IMPORTANT:

For correct VXLAN deployment and VTEP management, do not manually specify tunnel-specific source addresses for VXLAN tunnels if OVSDB is used.

A VXLAN tunnel uses the global source address if you do not specify a source interface or source address for the tunnel.

The global source address takes effect only on VXLAN tunnels.

Examples

Specify 1.1.1.1 as the global source address for VXLAN tunnels.

```
<Sysname> system-view
[Sysname] tunnel global source-address 1.1.1.1
```

vsi

Use **vsi** to create a VSI and enter its view, or enter the view of an existing VSI.

Use **undo vsi** to delete a VSI.

Syntax

vsi *vsi-name*

undo vsi *vsi-name*

Default

No VSIs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vsi-name: Specifies a VSI name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A VSI acts as a virtual switch to provide Layer 2 switching services for a VXLAN on a VTEP. A VSI has all functions of a physical Ethernet switch, including source MAC address learning, MAC address aging, and flooding.

A VSI can provide services only for one VXLAN.

Examples

Create VSI **vxlan10** and enter VSI view.

```
<Sysname> system-view
[Sysname] vsi vxlan10
[Sysname-vsi-vxlan10]
```

Related commands

display l2vpn vsi

vxlan

Use **vxlan** to create a VXLAN and enter its view, or enter the view of an existing VXLAN.

Use **undo vxlan** to restore the default.

Syntax

vxlan *vxlan-id*

undo vxlan

Default

No VXLANs exist.

Views

VSI view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

You can create only one VXLAN for a VSI. The VXLAN ID for each VSI must be unique.

Examples

Create VXLAN 10000 for VSI **vpna** and enter VXLAN view.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] vxlan 10000
[Sysname-vsi-vpna-vxlan-10000]
```

Related commands

vsi

vxlan ip-forwarding

Use **vxlan ip-forwarding** to enable Layer 3 forwarding for all VXLANs.

Use **undo vxlan ip-forwarding** to enable Layer 2 forwarding for all VXLANs.

Syntax

vxlan ip-forwarding

undo vxlan ip-forwarding

Default

Layer 3 forwarding is enabled for all VXLANs.

Views.

System view

Predefined user roles

network-admin

Usage guidelines

If the device is a VTEP, enable Layer 2 forwarding for VXLANs. If the device is a VXLAN IP gateway, enable Layer 3 forwarding for VXLANs.

In Layer 3 forwarding mode, the VTEP uses the ARP table (IPv4 network) or ND table (IPv6 network) to forward traffic for VXLANs. In Layer 2 forwarding mode, the VTEP uses the MAC address table to forward traffic for VXLANs.

You must delete all VSIs, VSI interfaces, and VXLAN tunnel interfaces before you can change the forwarding mode.

Examples

Enable Layer 3 forwarding for all VXLANs.

```
<Sysname>system-view
[Sysname] vxlan ip-forwarding
```

vxlan local-mac report

Use **vxlan local-mac report** to enable local-MAC logging.

Use **undo vxlan local-mac report** to disable local-MAC logging.

Syntax

vxlan local-mac report

undo vxlan local-mac report

Default

Local-MAC logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When the local-MAC logging feature is enabled, the VXLAN module immediately sends a log message with its local MAC addresses to the information center. When a local MAC address is added or removed, a log message is also sent to the information center to notify the local-MAC change.

With the information center, you can set log message filtering and output rules, including output destinations. For more information about configuring the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable local-MAC logging.

```
<Sysname> system-view
[Sysname] vxlan local-mac report
```

vxlan tunnel mac-learning disable

Use **vxlan tunnel mac-learning disable** to disable remote-MAC address learning.

Use **undo vxlan tunnel mac-learning disable** to enable remote-MAC address learning.

Syntax

vxlan tunnel mac-learning disable

undo vxlan tunnel mac-learning disable

Default

Remote-MAC address learning is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When network attacks occur, use this command to prevent the device from learning incorrect remote MAC addresses in the data plane.

Examples

Disable remote-MAC address learning.

```
<Sysname> system-view
[Sysname] vxlan tunnel mac-learning disable
```

vxlan udp-port

Use **vxlan udp-port** to set the destination UDP port number for VXLAN packets.

Use **undo vxlan udp-port** to restore the default.

Syntax

vxlan udp-port *port-number*

undo vxlan udp-port

Default

The destination UDP port number is 4789 for VXLAN packets.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535. As a best practice, specify a port number in the range of 1024 to 65535 to avoid conflict with well-known ports.

Usage guidelines

You must configure the same destination UDP port number on all VTEPs in a VXLAN.

If you modify the destination UDP port number, only VXLAN tunnels established after the modification use the new port number for sending VXLAN packets. For the new port number to take effect on VXLAN tunnels created before the modification, you must disconnect and re-establish the tunnels.

Examples

Set the destination UDP port number to 6666 for VXLAN packets.

```
<Sysname> system-view
[Sysname] vxlan udp-port 6666
```

vxlan vlan-based

Use **vxlan vlan-based** to enable VLAN-based VXLAN assignment.

Use **undo vxlan vlan-based** to disable VLAN-based VXLAN assignment.

Syntax

vxlan vlan-based

undo vxlan vlan-based

Default

VLAN-based VXLAN assignment is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You can assign customer traffic to a VXLAN by using one of the following methods:

- **Ethernet service instance-to-VSI mapping**—This method uses the frame match criterion of an Ethernet service instance to match a list of VLANs on a site-facing Layer 2 interface. The VTEP assigns customer traffic to a VXLAN by mapping the Ethernet service instance to a VSI.
- **VLAN-based VXLAN assignment**—This method maps a VLAN to a VXLAN. When a VLAN is mapped to a VXLAN and VLAN-based VXLAN assignment is enabled, the device automatically performs the following operations:
  a. Creates an Ethernet service instance that uses the VLAN ID as its instance ID on each interface in the VLAN. The matching outer VLAN ID of the Ethernet service instances is the VLAN ID.
  b. Maps the Ethernet service instances to the VSI of the VXLAN.

Do not configure both Ethernet service instance-to-VSI mapping and VLAN-based VXLAN assignment.

Examples

Enable VLAN-based VXLAN assignment.

```
<Sysname> system-view
[Sysname] vxlan vlan-based
```

vxlan vni

Use **vxlan vni** to map a VLAN to a VXLAN.

Use **undo vxlan vni** to remove the VXLAN mapping for a VLAN.

Syntax

vxlan vni *vxlan-id*

undo vxlan vni

Default

A VLAN is not mapped to a VXLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

vxlan-id: Specifies a VXLAN ID in the range of 0 to 16777215.

Usage guidelines

Before you map VLANs to VXLANs, enable VLAN-based VXLAN assignment by using the **vxlan vlan-based** command.

You cannot map VLAN 1 to any VXLAN. Do not map a VLAN to the L3 VXLAN ID of EVPN.

If you map a VLAN to a nonexistent VXLAN, the configuration takes effect after the VXLAN is created.

Examples

Map VLAN 10 to VXLAN 100.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] vxlan vni 100
```

Related commands

vxlan vlan-based

xconnect vsi

Use **xconnect vsi** to map an AC to a VSI.

Use **undo xconnect vsi** to restore the default.

Syntax

xconnect vsi *vsi-name* [**access-mode vlan**] [**track** *track-entry-number*&<1-3>]

undo xconnect vsi

Default

An AC is not mapped to any VSI.

Views

Ethernet service instance view

Predefined user roles

network-admin

Parameters

vsi-name: Specifies the VSI name, a case-sensitive string of 1 to 31 characters.

access-mode: Specifies an access mode. The default access mode is VLAN.

vlan: Specifies the VLAN access mode.

track *track-entry-number*&<1-3>: Specifies a space-separated list of up to three track entry numbers in the range of 1 to 1024. The AC is up only if a minimum of one associated track entry is in positive state.

Usage guidelines

To monitor the status of an AC, associate it with track entries.

To use this command for an Ethernet service instance, you must first use the **encapsulation** command to add a traffic match criterion to the service instance.

For traffic that matches the Ethernet service instance, the system uses the VSI's MAC address table to make a forwarding decision.

The device supports the VLAN access mode. In this mode, Ethernet frames received from or sent to the local site must contain 802.1Q VLAN tags.

- For an Ethernet frame received from the local site, the VTEP removes all its 802.1Q VLAN tags before forwarding the frame.
- For an Ethernet frame destined for the local site, the VTEP adds 802.1Q VLAN tags to the frame before forwarding the frame.

In VLAN access mode, VXLAN packets sent between VXLAN sites do not contain 802.1Q VLAN tags. VXLAN can provide Layer 2 connectivity for different 802.1Q VLANs between sites. You can use different 802.1Q VLANs to provide the same service in different sites.

Examples

On GigabitEthernet 1/0/1, configure Ethernet service instance 200 to match frames with an outer 802.1Q VLAN tag of 200, and map the instance to VSI **vpn1**.

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 200
[Sysname-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
[Sysname-GigabitEthernet1/0/1-srv200] xconnect vsi vpn1
```

Related commands

display l2vpn service-instance

encapsulation

vsi

VXLAN IP gateway commands

arp distributed-gateway dynamic-entry synchronize

Use **arp distributed-gateway dynamic-entry synchronize** to enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Use **undo arp distributed-gateway dynamic-entry synchronize** to disable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

Syntax

arp distributed-gateway dynamic-entry synchronize

undo arp distributed-gateway dynamic-entry synchronize

Default

Dynamic ARP entry synchronization is disabled for distributed VXLAN IP gateways.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When local proxy ARP is enabled on distributed VXLAN IP gateways, each gateway learns ARP information independently. A gateway does not forward ARP packets destined for its local VSI interfaces to other gateways. For distributed VXLAN IP gateways to have the same ARP entries, you must enable dynamic ARP entry synchronization.

A controller or the EVPN feature can also synchronize ARP entries among distributed VXLAN IP gateways. When you use a controller or the EVPN feature, do not enable dynamic ARP entry synchronization.

Examples

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
<Sysname> system-view
[Sysname] arp distributed-gateway dynamic-entry synchronize
```

Related commands

distributed-gateway local

local-proxy-arp enable (*Layer 3—IP Services Command Reference*)

arp send-rate

Use **arp send-rate** to set an ARP packet sending rate limit for a VSI interface.

Use **undo arp send-rate** to remove the ARP packet sending rate limit for a VSI interface.

Syntax

arp send-rate *pps*

undo arp send-rate

Default

The ARP packet sending rate is not limited for a VSI interface.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

pps: Specifies a rate limit in the range of 1 to 500 pps.

Usage guidelines

VMs have limited capacity to process packets. To prevent packet processing from degrading VM performance, limit the ARP packet sending rate of the VSI interface for VMs. The VTEP will drop excess ARP packets if the rate limit is exceeded.

Examples

Set the ARP packet sending rate limit to 50 pps for VSI-interface 1.

```
<Sysname> system
[Sysname] interface vsi-interface 1
[Sysname-Vsi-interface1] arp send-rate 50
```

default

Use **default** to restore the default settings for a VSI interface.

Syntax

default

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions.

To resolve this problem:

1. Use the **display this** command in interface view to identify these commands.
2. Use their **undo** forms or follow the command reference to restore their default settings.
3. If the restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VSI-interface 100.

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

```
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Use **description** to configure the description of a VSI interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of a VSI interface is *interface-name* plus **Interface** (for example, **Vsi-interface100 Interface**).

Views

VSI interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **gateway for VXLAN 10** for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] description gateway for VXLAN 10
```

display interface vsi-interface

Use **display interface vsi-interface** to display information about VSI interfaces.

Syntax

display interface [**vsi-interface** [*vsi-interface-id*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi-interface [*vsi-interface-id*]: Specifies VSI interfaces. If you specify a VSI interface, this command displays information about the specified interface. If you specify only the **vsi-interface** keyword, this command displays information about all VSI interfaces. If you do not specify the **vsi-interface** [*vsi-interface-id*] option, this command displays

information about all interfaces. Make sure the specified VSI interfaces have been created on the device.

brief: Display brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays interfaces that are physically down as well as the down reason. If you do not specify this keyword, the command does not filter output by physical interface state.

Examples

Display information about VSI-interface 100.

```
<Sysname> display interface vsi-interface 100
Vsi-interface100
Current state: UP
Line protocol state: UP
Description: Vsi-interface100 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet address: 10.1.1.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0011-2200-0102
IPv6 packet frame type: Ethernet II, hardware address: 0011-2200-0102
Physical: Unknown, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 10 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the interface: • **UP**—The data link layer protocol is up. • **UP(spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. • **DOWN**—The data link layer protocol is down.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address.

Field	Description
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address.
IPv6 packet frame type	IPv6 packet framing format.
Physical	Physical type of the interface, which is fixed at **Unknown**.
baudrate	Interface baudrate in kbps.
Last clearing of counters	Last time when the interface statistics are cleared. The current software version does not support clearing interface statistics. This field always displays **Never.**
Last 300 seconds input rate	Average input rate for the last 300 seconds.
Last 300 seconds output rate	Average output rate for the last 300 seconds.
Input: 0 packets, 0 bytes, 0 drops	Incoming traffic statistics on the interface: • Number of incoming packets. • Number of incoming bytes. • Number of dropped incoming packets.
Output: 0 packets, 0 bytes, 0 drops	Outgoing traffic statistics on the interface: • Number of outgoing packets. • Number of outgoing bytes. • Number of dropped outgoing packets.

Display brief information about all VSI interfaces.

```
<Sysname> display interface vsi-interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               DOWN DOWN     --
```

Display brief information and complete description for VSI-interface 100.

```
<Sysname> display interface vsi-interface 100 brief description
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi100               UP   UP       1.1.1.1         VSI-interface100
```

Displays interfaces that are physically down and the down reason.

```
<Sysname> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link   Cause
Vsi100               DOWN   Administratively
Vsi200               DOWN   Administratively
```

Table 11 Command output

Field	Description
Interface	Abbreviated interface name.

Field	Description
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **UP (s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. • **DOWN**—The data link layer protocol of the interface is down.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Not connected**—The interface is not mapped to any VSI, or the mapped VSI does not have any AC or VXLAN tunnel.

Related commands

reset counters interface vsi-interface

distributed-gateway local

Use **distributed-gateway local** to specify a VSI interface as a distributed gateway to provide services for the local site.

Use **undo distributed-gateway local** to restore the default.

Syntax

distributed-gateway local

undo distributed-gateway local

Default

A VSI interface is not a distributed gateway.

Views

VSI interface view

Predefined user roles

network-admin

Usage guidelines

If a VXLAN uses distributed gateway services, you must assign the same IP address to the VXLAN's VSI interfaces on different VTEPs. To avoid IP address conflicts, you must specify the VSI interface on each VTEP as a distributed gateway.

Examples

Specify VSI-interface 100 as a distributed gateway.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] distributed-gateway local
```

gateway vsi-interface

Use **gateway vsi-interface** to specify a gateway interface for a VSI.

Use **undo gateway vsi-interface** to restore the default.

Syntax

gateway vsi-interface *vsi-interface-id*

undo gateway vsi-interface

Default

No gateway interface is specified for a VSI.

Views

VSI view

Predefined user roles

network-admin

Parameters

vsi-interface-id: Specifies a VSI interface by its number. The VSI interface must already exist.

Usage guidelines

When you delete a VSI interface by using the **undo interface vsi-interface** command, the gateway interface setting of the VSI interface is also deleted.

A VSI can have only one gateway interface.

Examples

Specify VSI-interface 100 as the gateway interface for VSI **vpna**.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] gateway vsi-interface 100
```

Related commands

interface vsi-interface

interface vsi-interface

Use **interface vsi-interface** to create a VSI interface and enter its view, or enter the view of an existing VSI interface.

Use **undo interface vsi-interface** to delete a VSI interface.

Syntax

interface vsi-interface *vsi-interface-id*

undo interface vsi-interface *vsi-interface-id*

Default

No VSI interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

vsi-interface-id: Specifies a VSI interface number. The value range for this argument is 0 to 16777215.

Usage guidelines

When you delete a VSI interface by using the **undo interface vsi-interface** command, the gateway interface setting of the VSI interface is also deleted.

Examples

Create VSI-interface 100 and enter VSI interface view.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100]
```

Related commands

gateway vsi-interface

ipv6 nd distributed-gateway dynamic-entry synchronize

Use **ipv6 nd distributed-gateway dynamic-entry synchronize** to enable dynamic ND entry synchronization for distributed VXLAN IP gateways.

Use **undo ipv6 nd distributed-gateway dynamic-entry synchronize** to disable dynamic ND entry synchronization for distributed VXLAN IP gateways.

Syntax

ipv6 nd distributed-gateway dynamic-entry synchronize

undo ipv6 nd distributed-gateway dynamic-entry synchronize

Default

Dynamic ND entry synchronization is disabled for distributed VXLAN IP gateways.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When local ND proxy is enabled on distributed VXLAN IP gateways, each gateway learns ND information independently. A gateway does not forward ND packets destined for its local VSI

interfaces to other gateways. For distributed VXLAN IP gateways to have the same ND entries, you must enable dynamic ND entry synchronization.

A controller or the EVPN feature can also synchronize ND entries among distributed VXLAN IP gateways. When you use a controller or the EVPN feature, do not enable dynamic ND entry synchronization.

Examples

Enable dynamic ND entry synchronization for distributed VXLAN IP gateways.

```
<Sysname> system-view
[Sysname] ipv6 nd distributed-gateway dynamic-entry synchronize
```

Related commands

distributed-gateway local

local-proxy-nd enable (*Layer 3—IP Services Command Reference*)

mac-address

Use **mac-address** to assign a MAC address to a VSI interface.

Use **undo mac-address** to restore the default.

Syntax

mac-address *mac-address*

undo mac-address

Default

The MAC address of VSI interfaces is the bridge MAC address + 26.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in H-H-H format.

Examples

Assign MAC address 0001-0001-0001 to VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] mac-address 1-1-1
```

mtu

Use **mtu** to set the MTU for a VSI interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The default MTU of a VSI interface is 1444 bytes.

Views

VSI interface view

Predefined user roles

network-admin

Parameters

size: Specifies an MTU value in the range of 46 to 1500 bytes.

Examples

Set the MTU to 1430 bytes for VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] mtu 1430
```

shutdown

Use **shutdown** to shut down a VSI interface.

Use **undo shutdown** to bring up a VSI interface.

Syntax

shutdown

undo shutdown

Default

A VSI interface is up.

Views

VSI interface view

Predefined user roles

network-admin

Examples

Shut down VSI-interface 100.

```
<Sysname> system-view
[Sysname] interface vsi-interface 100
[Sysname-Vsi-interface100] shutdown
```

vxlan tunnel arp-learning disable

Use **vxlan tunnel arp-learning disable** to disable remote ARP learning for VXLANs.

Use **undo vxlan tunnel arp-learning disable** to enable remote ARP learning for VXLANs.

Syntax

vxlan tunnel arp-learning disable

undo vxlan tunnel arp-learning disable

Default

Remote ARP learning is enabled for VXLANs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device learns ARP information of remote VMs from packets received on VXLAN tunnel interfaces. To save resources on VTEPs in an SDN transport network, you can temporarily disable remote ARP learning when the controller and VTEPs are synchronizing entries. After the entry synchronization is completed, use the **undo vxlan tunnel arp-learning disable** command to enable remote ARP learning.

As a best practice, disable remote ARP learning for VXLANs only when the controller and VTEPs are synchronizing entries.

Examples

Disable remote ARP learning for VXLANs.

```
<Sysname> system
[Sysname] vxlan tunnel arp-learning disable
```

vxlan tunnel nd-learning disable

Use **vxlan tunnel nd-learning disable** to disable remote ND learning for VXLANs.

Use **undo vxlan tunnel nd-learning disable** to enable remote ND learning for VXLANs.

Syntax

vxlan tunnel nd-learning disable

undo vxlan tunnel nd-learning disable

Default

Remote ND learning is enabled for VXLANs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device learns ND information of remote VMs from packets received on VXLAN tunnel interfaces. To save resources on VTEPs in an SDN transport network, you can temporarily disable remote ND learning when the controller and VTEPs are synchronizing entries. After the entry synchronization is completed, use the **undo vxlan tunnel nd-learning disable** command to enable remote ND learning.

As a best practice, disable remote ND learning for VXLANs only when the controller and VTEPs are synchronizing entries.

Examples

Disable remote ND learning for VXLANs.

```
<Sysname> system
```

```
[Sysname] vxlan tunnel nd-learning disable
```

OVSDB commands

ovsdb server bootstrap ca-certificate

Use **ovsdb server bootstrap ca-certificate** to specify a CA certificate file for establishing OVSDB SSL connections.

Use **undo ovsdb server bootstrap ca-certificate** to restore the default.

Syntax

ovsdb server bootstrap ca-certificate *ca-filename*

undo ovsdb server bootstrap ca-certificate

Default

SSL uses the CA certificate file in the PKI domain.

Views

System view

Predefined user roles

network-admin

Parameters

ca-filename: Specifies the CA certificate file name, a case-insensitive string. The file name cannot contain the **slot** string.

Usage guidelines

For the specified certificate to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

If the specified CA certificate file does not exist, the device obtains a self-signed certificate from the controller. The obtained file uses the name specified for the *ca-filename* argument.

Examples

Specify CA certificate file **ca-new** for establishing OVSDB SSL connections.

```
<Sysname> system-view
[Sysname] ovsdb server bootstrap ca-certificate ca-new
```

Related commands

ovsdb server enable

ovsdb server pki domain

ovsdb server pssl

ovsdb server ssl

ovsdb server enable

Use **ovsdb server enable** to enable the OVSDB server.

Use **undo ovsdb server enable** to disable the OVSDB server.

Syntax

ovsdb server enable

undo ovsdb server enable

Default

The OVSDB server is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To obtain configuration data from controllers, you must enable the OVSDB server.

Before you enable the OVSDB server, you must establish an OVSDB SSL or TCP connection with a minimum of one controller.

Examples

Enable the OVSDB server.

```
<Sysname> system-view
[Sysname] ovsdb server enable
```

ovsdb server pki domain

Use **ovsdb server pki domain** to specify a PKI domain for establishing OVSDB SSL connections.

Use **undo ovsdb bootstrap server pki domain** to restore the default.

Syntax

ovsdb server pki domain *domain-name*

undo ovsdb server pki domain

Default

No PKI domain is specified for establishing OVSDB SSL connections.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain name, a case-sensitive string of 1 to 31 characters. The PKI domain must already exist and contain a complete certificate and key.

Usage guidelines

To communicate with controllers through SSL, you must specify a PKI domain.

For the specified PKI domain to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

For more information about PKI domains, see PKI in *Security Configuration Guide*.

Examples

Specify PKI domain **ovsdb_test** for establishing OVSDB SSL connections.

```
<Sysname> system-view
[Sysname] ovsdb server pki domain ovsdb_test
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pssl

ovsdb server ssl

ovsdb server pssl

Use **ovsdb server pssl** to enable the device to listen for OVSDB SSL connection requests.

Use **undo ovsdb server pssl** to restore the default.

Syntax

ovsdb server pssl [**port** *port-number*]

undo ovsdb server pssl

Default

The device does not listen for OVSDB SSL connection requests.

Views

System view

Predefined user roles

network-admin

Parameters

port *port-number*: Specifies a port to listen for OVSDB SSL connection requests. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port, the device uses the port number 6640.

Usage guidelines

Before you use this command, you must specify a PKI domain for SSL.

You can specify only one port to listen for OVSDB SSL connection requests. If you execute this command multiple times, the most recent configuration takes effect.

For the specified port setting to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Enable the device to listen for OVSDB SSL connection requests on port 6640.

```
<Sysname> system-view
[Sysname] ovsdb server pssl
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pki domain

ovsdb server ssl

ovsdb server ptcp

Use **ovsdb server ptcp** to enable the device to listen for OVSDB TCP connection requests.

Use **undo ovsdb server ptcp** to restore the default.

Syntax

ovsdb server ptcp [**port** *port-number*]

undo ovsdb server ptcp

Default

The device does not listen for OVSDB TCP connection requests.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port to listen for OVSDB TCP connection requests. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port, the device uses the port number 6640.

Usage guidelines

You can specify only one port to listen for OVSDB TCP connection requests. If you execute this command multiple times, the most recent configuration takes effect.

For the specified port setting to take effect, you must execute the **ovsdb server enable** command to enable the OVSDB server. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Enable the device to listen for OVSDB TCP connection requests on port 6640.

```
<Sysname> system-view
[Sysname] ovsdb server ptcp
```

Related commands

ovsdb server enable

ovsdb server tcp

ovsdb server ssl

Use **ovsdb server ssl** to set up an active OVSDB SSL connection to a controller.

Use **undo ovsdb server ssl** to remove an OVSDB SSL connection from a controller.

Syntax

ovsdb server ssl ip *ip-address* **port** *port-number*

undo ovsdb server ssl ip *ip-address* **port** *port-number*

Default

The device does not have active OVSDB SSL connections to a controller.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the destination IP address for the SSL connection.

port *port-number*: Specifies the destination port for the SSL connection. The value range for the *port-number* argument is 1 to 65535.

Usage guidelines

Before you use this command, you must specify a PKI domain for SSL.

The device can have a maximum of eight active SSL connections.

To establish the connection, you must execute the **ovsdb server enable** command. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Set up an active SSL connection to port 6632 at 192.168.12.2.

```
<Sysname> system-view
[Sysname] ovsdb server ssl ip 192.168.12.2 port 6632
```

Related commands

ovsdb server bootstrap ca-certificate

ovsdb server enable

ovsdb server pki domain

ovsdb server pssl

ovsdb server tcp

Use **ovsdb server tcp** to set up an active OVSDB TCP connection to a controller.

Use **undo ovsdb server tcp** to remove an OVSDB TCP connection.

Syntax

ovsdb server tcp ip *ip-address* **port** *port-number*

undo ovsdb server tcp ip *ip-address* **port** *port-number*

Default

The device does not have active OVSDB TCP connections.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the destination IP address for the TCP connection.

port *port-number*: Specifies the destination port for the TCP connection. The value range for the *port-number* argument is 1 to 65535.

Usage guidelines

The device can have a maximum of eight active OVSDB TCP connections.

To establish the connection, you must execute the **ovsdb server enable** command. You must disable and then re-enable the OVSDB server if it has been enabled.

Examples

Set up an active OVSDB TCP connection to port 6632 at 192.168.12.2.

```
<Sysname> system-view
[Sysname] ovsdb server tcp ip 192.168.12.2 port 6632
```

Related commands

ovsdb server enable

ovsdb server ptcp

vtep access port

Use **vtep access port** to specify a site-facing interface as a VTEP access port.

Use **undo vtep access port** to restore the default.

Syntax

vtep access port

undo vtep access port

Default

An interface is not a VTEP access port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

For controllers to manage a site-facing interface, you must specify the interface as a VTEP access port.

Examples

Specify GigabitEthernet 1/0/1 as a VTEP access port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vtep access port
```

vtep enable

Use **vtep enable** to enable the OVSDB VTEP service.

Use **undo vtep enable** to disable the OVSDB VTEP service.

Syntax

vtep enable

undo vtep enable

Default

The OVSDB VTEP service is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the OVSDB VTEP service.

```
<Sysname> system-view
[Sysname] vtep enable
```

Index