

Contents

MPLS L2VPN commands	1
ac interface.....	1
address-family l2vpn	2
auto-discovery.....	3
backup-peer	4
ccc.....	5
connection.....	6
connection remote-site-id.....	7
control-word enable.....	8
description.....	9
display bgp l2vpn signaling	9
display l2vpn bgp	13
display l2vpn forwarding.....	15
display l2vpn ldp.....	19
display l2vpn pw.....	21
display l2vpn pw-class	24
display l2vpn service-instance	25
display l2vpn xconnect-group.....	27
encapsulation	29
l2vpn enable.....	30
l2vpn switchover.....	31
mtu	31
peer	32
peer signaling.....	34
policy vpn-target.....	35
pw-class (auto-discovery cross-connect group view).....	35
pw-class (system view)	36
pw-redundancy.....	37
pw-type.....	38
revertive	39
route-distinguisher.....	40
rr-filter.....	41
service-instance	42
shutdown (cross-connect group view).....	42
site.....	43
snmp-agent trap enable l2vpn.....	44
tunnel-policy (auto-discovery cross-connect view).....	45
vpn-target	46
xconnect-group	47

MPLS L2VPN commands

ac interface

Use **ac interface** to bind an Ethernet service instance to a cross-connect.

Use **undo ac interface** to remove the binding.

Syntax

```
ac interface interface-type interface-numberservice-instance  
instance-id [ access-mode { ethernet | vlan } ] [ track  
track-entry-number&<1-3> ]
```

```
undo ac interface interface-type interface-numberservice-instance  
instance-id
```

Default

No Ethernet service instance is bound to a cross-connect.

Views

Cross-connect view

Auto-discovery cross-connect view

Predefined user roles

network-admin

mdc-admin

Parameters

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

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

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

- **ethernet**: Specifies the Ethernet access mode.
- **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

After you execute this command, packets received from the Layer 3 interface or those matching the Ethernet service instance are forwarded to the bound PW or another AC.

The Ethernet service instance specified in this command must have a packet match criterion configured by the **encapsulation** command.

The access mode determines how the PE treats the VLAN tag in Ethernet frames received from the AC. It also determines how the PE forwards Ethernet frames to the AC.

- **VLAN access mode**—Ethernet frames received from the AC must carry a VLAN tag in the Ethernet header. The VLAN tag is called a P-tag assigned by the service provider. Ethernet frames sent to the AC must also carry the P-tag.

- **Ethernet access mode**—If Ethernet frames from the AC have a VLAN tag in the header, the VLAN tag is called a U-tag, and the PE ignores it. Ethernet frames sent to the AC do not carry the P-tag.

Examples

Configure Ethernet service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN tag of 200. Bind the Ethernet service instance to cross-connect **actopw** in cross-connect group **vpn1**.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] service-instance 200
[Sysname-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
[Sysname-Ten-GigabitEthernet1/0/1-srv200] quit
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection actopw
[Sysname-xcg-vpn1-actopw] ac interface ten-gigabitethernet 1/0/1 service-instance 200
```

Configure Ethernet service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets with an outer VLAN tag of 200. Bind the Ethernet service instance to the auto-discovery cross-connect in cross-connect group **vpwsbgp**.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] service-instance 200
[Sysname-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
[Sysname-Ten-GigabitEthernet1/0/1-srv200] quit
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] xconnect-group vpwsbgp
[Sysname-xcg-vpwsbgp] auto-discovery bgp
[Sysname-xcg-vpwsbgp-auto] site 1 range 10 default-offset 0
[Sysname-xcg-vpwsbgp-auto-1] connection remote-site-id 2
[Sysname-xcg-vpwsbgp-auto-1-2] ac interface ten-gigabitethernet 1/0/1 service-instance 200
```

Related commands

connection

display l2vpn service-instance

encapsulation

pw-type

address-family l2vpn

Use **address-family l2vpn** to create the BGP L2VPN address family and enter its view, or enter the view of the existing BGP L2VPN address family view.

Use **undo address-family l2vpn** to delete the BGP L2VPN address family and all settings from BGP L2VPN address family view.

Syntax

address-family l2vpn

undo address-family l2vpn

Default

No BGP L2VPN address family exists.

Views

BGP instance view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

To establish a BGP PW to a remote PE, you must execute the **peer enable** command in BGP L2VPN address family view to enable the remote PE.

Examples

```
# Create the BGP L2VPN address family and enter BGP L2VPN address family view.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn
[Sysname-bgp-default-l2vpn]
```

Related commands

peer enable (*Layer 3—IP Routing Command Reference*)

auto-discovery

Use **auto-discovery** to enable a cross-connect group to automatically discover neighbors and create PWs through BGP, and enter auto-discovery cross-connect group view.

Use **undo auto-discovery** to restore the default.

Syntax

```
auto-discovery bgp
undo auto-discovery
```

Default

A cross-connect group does not use BGP to automatically discover neighbors and create PWs.

Views

Cross-connect group view

Predefined user roles

network-admin

mdc-admin

Parameters

bgp: Enables the cross-connect group to automatically discover neighbors and create PWs through BGP.

Usage guidelines

In auto-discovery cross-connect group view, you can configure parameters such as the local site, remote site, and route target for BGP. The local PE can use BGP to discover remote PEs and create PWs.

Examples

```
# Enable cross-connect group bbb to automatically discover neighbors and create PWs through BGP, and enter auto-discovery cross-connect group view.
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto]
```

Related commands

```
display l2vpn pw
display l2vpn xconnect-group
```

backup-peer

Use **backup-peer** to configure a backup PW for a cross-connect and enter cross-connect backup PW view, or enter the view of an existing cross-connect backup PW.

Use **undo backup-peer** to restore the default.

Syntax

```
backup-peer ip-address pw-id pw-id [ in-label label-value out-label label-value ] [ pw-class class-name | tunnel-policy tunnel-policy-name ] *
undo backup-peer ip-address pw-id pw-id
```

Default

No backup PW exists for a cross-connect.

Views

Cross-connect PW view

Predefined user roles

```
network-admin
mdc-admin
```

Parameters

ip-address: Specifies the LSR ID of the peer PE on the backup PW.

pw-id *pw-id*: Specifies a PW ID for the backup PW, in the range of 1 to 4294967295.

in-label *label-value*: Specifies the incoming label for the backup PW. The value range is 16 to 1023.

out-label *label-value*: Specifies the outgoing label for the backup PW. The value range is 16 to 1048575.

pw-class *class-name*: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters. You can specify a PW class to configure the PW data encapsulation type and control word for the backup PW. If you do not specify a PW class, the PW data encapsulation type is determined by the link type of the interface. The control word feature is not supported for PW data encapsulation types that do not require using control word.

tunnel-policy *tunnel-policy-name*: Specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a tunnel policy, the default tunnel policy is used.

Usage guidelines

This command configures a backup PW to implement PW redundancy. The backup PW is used when the primary PW fails.

To configure a backup static PW, you must specify the **in-label** and **out-label**. To configure a backup LDP PW, you do not need to specify the **in-label** and **out-label**.

The peer LSR ID and PW ID for a backup PW must be different from those for an existing VPLS PW or cross-connect PW.

Backup PW and multi-segment PW are mutually exclusive with each other. If you have configured a multi-segment PW, you cannot configure a backup PW for the two PWs that form the multi-segment PW. If you have configured a backup PW for a PW, the PW cannot form a multi-segment PW. For information about configuring a multi-segment PW, see the **peer** command.

When you add a static PW, you must make sure that static PW uses a different incoming label than an existing static LSP or static CRLSP. If the incoming label is duplicated, you cannot make the static PW take effect by changing the incoming label of the static LSP or CRLSP. Instead, you must delete the static PW and then reconfigure the static PW with an unused incoming label.

Examples

Configure a primary PW and a backup PW for cross-connect **pw2pw** in cross-connect group **vpn2**. The primary PW is destined to 6.6.6.6 and has a PW ID of 100. The backup PW is destined to 7.7.7.7 and has a PW ID of 200.

```
<Sysname> system-view
[Sysname] xconnect-group vpn2
[Sysname-xcg-vpn2] connection pw2pw
[Sysname-xcg-vpn2-pw2pw] peer 6.6.6.6 pw-id 100 in-label 16 out-label 17
[Sysname-xcg-vpn2-pw2pw-6.6.6.6-100] backup-peer 7.7.7.7 pw-id 200 in-label 18 out-label 19
[Sysname-xcg-vpn2-pw2pw-6.6.6.6-100-backup]
```

Related commands

```
display l2vpn ldp
display l2vpn pw
peer
```

CCC

Use **ccc** to create a remote Circuit Cross Connect (CCC) connection.

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

Syntax

```
ccc in-label in-label-value out-label out-label-value { nexthop nexthop |
out-interface interface-type interface-number } [ pw-class class-name ]
undo ccc
```

Default

No remote CCC connections exist.

Views

Cross-connect view

Predefined user roles

network-admin

mdc-admin

Parameters

in-label *in-label-value*: Specifies an incoming label. The value range for the *in-label-value* argument is 16 to 1023.

out-label *out-label-value*: Specifies an outgoing label in the range of 16 to 1048575.

nexthop *nexthop*: Specifies the IP address of the next hop.

out-interface *interface-type interface-number*: Specifies the outgoing interface by its type and number.

pw-class *class-name*: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters. You can specify a PW class to configure the PW data encapsulation type and control word. If you do not specify a PW class, the PW data encapsulation type is determined by the interface type. The control word feature is not supported for PW data encapsulation types that do not require using control word.

Usage guidelines

A remote CCC connection is a static L2VPN connection that is manually created by specifying the incoming and outgoing labels on two PEs. A remote CCC connection does not need a public tunnel, but it requires configuring two static LSPs in opposite directions on each P device between the two PEs. CCC employs only one level of label to transfer packets. The static LSPs on the P devices transfer data only for the CCC connection.

This command must be configured on both the local and remote PEs to create a remote CCC connection. The outgoing label specified on a device must be the same as the incoming label specified on the next hop device.

After you create a remote CCC connection, you must execute the **ac interface** command to bind an Ethernet service instance. The PE can forward packets matching the Ethernet service instance to the remote CCC connection.

Use the **out-interface** keyword to specify the outgoing interface only on a point-to-point link. On other interfaces, for example, VLAN interfaces, you must use the **nexthop** keyword to specify the next hop IP address.

For the PEs to forward packets over a CCC connection, make sure the two PEs have the same CCC connection settings such as the encapsulation type and control word feature.

Examples

```
# Create a remote CCC connection that has incoming label 100, outgoing label 200, and next hop 10.1.1.1, and uses PW class pw1.
```

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] connection ccc1
[Sysname-xcg-bbb-ccc1] ccc in-label 100 out-label 200 nexthop 10.1.1.1 pw-class pw1
```

Related commands

ac interface

display l2vpn pw

connection

Use **connection** to create a cross-connect and enter its view, or enter the view of an existing cross-connect.

Use **undo connection** to remove a cross-connect.

Syntax

```
connection connection-name  
undo connection connection-name
```

Default

No cross-connects exist.

Views

Cross-connect group view

Predefined user roles

```
network-admin  
mdc-admin
```

Parameters

connection-name: Specifies the name of the cross-connect, a case-sensitive string of 1 to 20 characters, excluding hyphens.

Usage guidelines

A cross-connect is a point-to-point connection.

You can perform the following operations in cross-connect view:

- Execute the **ac interface** and **peer** commands to connect an AC to a PW, so the PE can forward packets between the AC and the PW.
- Execute the **peer** command twice to connect two PWs to form a multi-segment PW.
- Execute the **ac interface** and **ccc** commands to connect an AC to a remote CCC connection, so the PE can forward packets between the AC and the remote CCC connection.

Examples

```
# Create cross-connect ac2pw for cross-connect group vpn1 and enter cross-connect view.  
<Sysname> system-view  
[Sysname] xconnect-group vpn1  
[Sysname-xcg-vpn1] connection ac2pw  
[Sysname-xcg-vpn1-ac2pw]
```

connection remote-site-id

Use **connection remote-site-id** to create an auto-discovery cross-connect and enter its view, or enter the view of an existing auto-discovery cross-connect.

Use **undo connection remote-site-id** to remove the auto-discovery cross-connect.

Syntax

```
connection remote-site-id remote-site-id  
undo connection remote-site-id remote-site-id
```

Default

No auto-discovery cross-connects exist.

Views

Site view

Predefined user roles

network-admin
mdc-admin

Parameters

remote-site-id: Specifies a remote site by its ID in the range of 0 to 256.

Usage guidelines

This command creates an auto-discovery cross-connect that uses BGP to establish a PW from the local site to the specified remote site.

In auto-discovery cross-connect view, you can execute **ac interface** to bind an AC to the auto-discovery cross-connect. The PE can forward packets between the AC and the PW.

Examples

Create an auto-discovery cross-connect from site 1 to site 3 in site view, and enter auto-discovery cross-connect view.

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] site 1 range 10
[Sysname-xcg-bbb-auto-1] connection remote-site-id 3
[Sysname-xcg-bbb-auto-1-3]
```

control-word enable

Use **control-word enable** to enable the control word feature.

Use **undo control-word enable** to disable the control word feature.

Syntax

```
control-word enable
undo control-word enable
```

Default

The control word feature is disabled.

Views

PW class view

Predefined user roles

network-admin
mdc-admin

Usage guidelines

The control word field is between the MPLS label stack and the Layer 2 data. It carries control information for the Layer 2 frame, for example, the sequence number.

The control word feature has the following functions:

- Avoids fragment disorder. In multipath forwarding, fragments received might be disordered. You can configure the control word feature so the device reorders the fragments according to the sequence number carried in the control word field.
- Identifies the original payload length for packets that include padding.

When the PW data encapsulation type is Ethernet or VLAN, the control word field is optional. Packets transmitted on the PW carry the control word field only when control word is enabled on both PEs.

Examples

```
# Enable the control word feature for PW class pw100.
<Sysname> system-view
[Sysname] pw-class pw100
[Sysname-pw-pw100] control-word enable
```

Related commands

```
display l2vpn pw-class
```

description

Use **description** to configure a description for a cross-connect group.

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

Syntax

```
description text
undo description
```

Default

No description is configured for a cross-connect group.

Views

Cross-connect group view

Predefined user roles

```
network-admin
mdc-admin
```

Parameters

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

Examples

```
# Configure a description of vpws for vpn2 for cross-connect group vpn2.
<Sysname> system-view
[Sysname] xconnect-group vpn2
[Sysname-xcg-vpn2] description vpws for vpn2
```

Related commands

```
display l2vpn xconnect-group
```

display bgp l2vpn signaling

Use **display bgp l2vpn signaling** to display MPLS L2VPN label block information discovered by BGP.

Syntax

```
display bgp [ instance instance-name ] l2vpn signaling [ peer ip-address
{ advertised | received } | route-distinguisher route-distinguisher
[ site-id site-id [ label-offset label-offset [ advertise-info ] ] ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

instance *instance-name*: Displays MPLS L2VPN label block information in a BGP instance. The *instance-name* argument specifies the BGP instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays MPLS L2VPN label block information in the default BGP instance.

peer *ip-address*: Displays MPLS L2VPN label block information advertised to or received from a BGP peer. The *ip-address* argument specifies the peer IP address.

advertised: Displays MPLS L2VPN label block information advertised to the BGP peer.

received: Displays MPLS L2VPN label block information received from the BGP peer.

route-distinguisher *route-distinguisher*: Displays BGP MPLS L2VPN label block information for the route distinguisher (RD), which is a string of 3 to 21 characters. You can specify an RD in one of the following 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 be equal to or greater than 65536. For example, 65536:1.

site-id *site-id*: Displays BGP MPLS L2VPN label block information for a site. The *site-id* argument specifies the site ID. The site ID range is 0 to 65535.

label-offset *label-offset*: Displays information about the BGP MPLS L2VPN label block with an offset. The *label-offset* argument specifies the offset in the range of 0 to 65535.

advertise-info: Displays BGP MPLS L2VPN label block advertisement information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP MPLS L2VPN label blocks.

Examples

```
# Display brief information about all BGP MPLS L2VPN label blocks.
```

```
<Sysname> display bgp l2vpn signaling
```

```
BGP local router ID is 192.168.1.135
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

```
Total number of label blocks: 2
```

```
Route distinguisher: 2:2
```

```
Total number of label blocks: 2
```

```

      Site ID  LB offset  LB range  LB base  Nexthop
* > 1         0         10       1034    0.0.0.0
* >i 2         0         10       1162    192.3.3.3

```

Table 1 Command output

Field	Description
Status codes	Status codes: <ul style="list-style-type: none"> • * – valid—Valid route. • > – best—Best route. • d – damped—Dampened route. • h – history—History route. • s – suppressed—Suppressed route. • S – Stale—Stale route. • i – internal—Internal route. • e – external—External route.
Origin	Origin of the label block: <ul style="list-style-type: none"> • i – IGP—Originated in the AS. • e – EGP—Learned through EGP. • ? – incomplete—Unknown origin.
LB offset	Offset of the label block.
LB range	Size of the label block.
LB base	Initial value of the label block.

Display detailed information about the BGP MPLS L2VPN label block that has RD 2:2, site ID 2, and offset 0.

```
<Sysname> display bgp l2vpn signaling route-distinguisher 2:2 site-id 2 label-offset 0
```

```

BGP local router ID: 192.168.1.135
Local AS number: 100

```

```

Route distinguisher: 2:2
Total number of label blocks: 1
Paths: 1 available, 1 best

```

```

From          : 192.3.3.3 (192.168.1.140)
Original nexthop: 192.3.3.3
Ext-Community  : <RT: 2:2>, <L2VPN info: MTU 1500, Encap type VLAN>
AS-path       : (null)
Origin        : igp
Attribute value : localpref 100, pref-val 0
Site ID       : 2
LB offset     : 0
LB base       : 1162
LB range      : 10
State        : valid, internal, best
CSV          : 0x010101BFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

FFFFFFFFFFFF

Table 2 Command output

Field	Description
Paths	Number of label block messages: <ul style="list-style-type: none"> • available—Number of available label block messages. • best—Number of best label block messages.
From	IP address of the peer from which the label block was received.
Original nexthop	Original next hop. If the label block was obtained from a BGP route update, this field displays the next hop address in that BGP route update.
Ext-Community	Extended community attribute: <ul style="list-style-type: none"> • RT—Route target. • L2VPN info—L2VPN information, including the MTU and encapsulation type.
AS-path	AS path attribute, which records all ASs that the label block passed to prevent routing loops.
Origin	Origin of the label block: <ul style="list-style-type: none"> • igp—Originated in the AS. • egp—Learned through EGP. • incomplete—Unknown origin.
Attribute value	Attribute of the label block: <ul style="list-style-type: none"> • MED—Multi-Exit Discriminator attribute. • localpref—Local preference value. • pref-val—Preferred value. • pre—Preference value.
LB offset	Offset of the label block.
LB base	Initial value of the label block.
LB range	Size of the label block.
State	State of the label block: <ul style="list-style-type: none"> • valid. • internal. • external. • local. • best.
CSV	Circuit status vector.

Display BGP advertisement information for the specified MPLS L2VPN label block.

```
<Sysname> display bgp l2vpn signaling route-distinguisher 2:2 site-id 1 label-offset 0
advertise-info
```

```
BGP local router ID: 192.168.1.135
Local AS number: 100
```

```
Route distinguisher: 2:2
Total number of label blocks: 1
Paths: 1 best
```

```

Site ID          : 1
LB offset       : 0
LB base        : 1034
LB range       : 10
CSV            : 0x010101EFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                FFFFFFFFFFFFFFFF
Advertised to peers (1 in total):
    192.3.3.3

```

Table 3 Command output

Field	Description
Paths	Number of label block messages: <ul style="list-style-type: none"> available—Number of available label block messages. best—Number of best label block messages.
LB offset	Offset of the label block.
LB base	Initial value of the label block.
LB range	Size of the label block.
CSV	Circuit status vector.
Advertised to peers (1 in total)	Peers to which the label block has been advertised.

display l2vpn bgp

Use `display l2vpn bgp` to display MPLS L2VPN label block information.

Syntax

```
display l2vpn bgp [ local | peer ip-address ] [ xconnect-group group-name ]
[ verbose ]
```

Views

Any view

Predefined user roles

```

network-admin
network-operator
mdc-admin
mdc-operator

```

Parameters

local: Displays local MPLS L2VPN label block information.

peer ip-address: Displays MPLS L2VPN label block information received from the remote peer.

xconnect-group group-name: Displays MPLS L2VPN label block information for a cross-connect group. The *group-name* argument specifies the cross-connect group name, a case-sensitive string of 1 to 31 characters. If you do not specify a cross-connect group, this command displays MPLS L2VPN label block information for all cross-connect groups.

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

Usage guidelines

If you specify a peer, this command displays both the label block received from the peer and the local label block that matches the received label block.

If you do not specify a peer or **local**, this command displays label blocks received from all peers and local label blocks that match the received ones. If no local label block matches the received ones, the command only displays the label blocks received from all peers.

A local label block matches a received label block if the following condition is met: local label block LO ≤ remote site ID ≤ local label block LO + local label block LR – 1.

Examples

```
# Display brief information about label blocks received from all peers.
```

```
<Sysname> display l2vpn bgp
Total number of BGP PWs: 1, 1 up, 0 down
```

```
Xconnect-group Name: vpnb, Site ID:1
Rmt Site   Offset  RD           Nexthop      In/Out Label  State
2          0        2:2         192.3.3.3    1036/1163     Up
```

Table 4 Command output

Field	Description
Rmt Site	ID of the remote site.
Offset	Offset of the label block.

```
# Display detailed information about label blocks received from all peers.
```

```
<Sysname> display l2vpn bgp verbose
Xconnect-group Name: vpnb, Site ID:1
Remote Site ID      : 2
Offset              : 0
RD                  : 2:2
PW State            : Up
Encapsulation       : VLAN
MTU                  : 1500
Nexthop             : 192.3.3.3
Local VC Label      : 1036
Remote VC Label     : 1163
Link ID             : 1
Local Label Block   : 1034/10/0
Remote Label Block  : 1162/10/0
Export Route Target : 2:2
```

Table 5 Command output

Field	Description
Local VC Label	Incoming label of the PW.
Remote VC Label	Outgoing label of the PW.
Link ID	Link ID of the PW.
Local Label Block	Local label block: label base/label range/Label-block offset.

Field	Description
Remote Label Block	Remote label block: label base/label range/Label-block offset.
Export Route Target	Route target of the remote label block.

Display brief information about all local label blocks.

```
<Sysname> display l2vpn bgp local
Xconnect-group Name: vbnb
Site   Offset  Range  Label Base   RD
1      0        10    1034        2:2
```

Display detailed information about all local label blocks.

```
<Sysname> display l2vpn bgp local verbose
Xconnect-group Name: vbnb
Site ID           : 1
Offset            : 0
RD                : 2:2
Range             : 10
Label Base        : 1034
Link ID           : 1
```

Table 6 Command output

Field	Description
Offset	Offset of the label block.
RD	RD of the label block. If no RD is configured, this field displays a hyphen (-).
Range	Range of the label block.
Label Base	Initial value of the label block.
Link ID	Link ID of the PW established using the label block. The link ID is fixed to 1 because an MPLS L2VPN cross-connect can establish only one BGP PW.

Related commands

`display l2vpn pw`

display l2vpn forwarding

Use `display l2vpn forwarding` to display cross-connect forwarding information.

Syntax

In standalone mode:

```
display l2vpn forwarding { ac | pw } [ xconnect-group group-name ] [ slot slot-number ] [ verbose ]
```

In IRF mode:

```
display l2vpn forwarding { ac | pw } [ xconnect-group group-name ] [ chassis chassis-number slot slot-number ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

ac: Displays AC forwarding information.

pw: Displays PW forwarding information.

xconnect-group *group-name*: Displays forwarding information for a cross-connect group. The *group-name* argument specifies the cross-connect group name, a case-sensitive string of 1 to 31 characters. If you do not specify a group, this command displays forwarding information for all cross-connect groups.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays cross-connect forwarding information on the active MPU. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays cross-connect forwarding information for the global active MPU. (In IRF mode.)

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

Examples

Display brief AC forwarding information for all cross-connect groups.

```
<Sysname> display l2vpn forwarding ac
Total number of cross-connections: 3
Total number of ACs: 3
```

AC	Xconnect-group Name	Link ID
XGE1/0/1 srv1	vpn1	0
XGE1/0/1 srv2	vpn2	1

Table 7 Command output

Field	Description
Total number of cross-connections	Total number of cross-connects, including cross-connects not bound to any ACs.
AC	AC type: Ethernet service instance on a Layer 2 interface.

Display detailed AC forwarding information for all cross-connect groups.

```
<Sysname> display l2vpn forwarding ac verbose
Xconnect-group Name: vpws1
Connection Name: actopw
Interface: XGE1/0/3 Service Instance: 1
Link ID      : 1
Access Mode  : VLAN
Encapsulation: s-vid 16
Bandwidth    : Unlimited
```

```

Connection Name: actopw2
Interface: XGE1/0/3 Service Instance: 4
  Link ID      : 1
  Access Mode  : VLAN
  Encapsulation: untagged
  Bandwidth    : Unlimited
Xconnect-group Name: vpws5
Connection Name: actopw
Interface: Vlan14
  Link ID      : 0
  Access Mode  : VLAN

```

Table 8 Command output

Field	Description
Xconnect-group Name	Cross-connect group name.
Connection Name	Cross-connect name.
Service Instance	The field is available only when the AC is an Ethernet service instance on a Layer 2 interface.
Access Mode	AC access mode: <ul style="list-style-type: none"> • VLAN. • Ethernet.
Encapsulation	Match criterion of the Ethernet service instance. This field is displayed only when the AC type is Ethernet service instance on a Layer 2 interface.
Bandwidth	This field is not supported in the current software version. Maximum bandwidth (in kbps) for traffic on the AC.

Display brief PW forwarding information for all cross-connect groups.

```

<Sysname> display l2vpn forwarding pw
Total number of cross-connections: 1
Total number of PWs: 2, 2 up, 0 blocked, 0 down

```

Xconnect-group Name	In/Out Label	NID	Link ID	State
vpn1	1279/1151	1025	0	Up
vpn1	1278/1151	1027	1	Up

Table 9 Command output

Field	Description
Total number of cross-connections	Total number of cross-connects, including those not bound to any PW.
NID	NHLFE ID for the public tunnel that carries the PW. If equal-cost tunnels are available, this field displays multiple NIDs. If no tunnel is available, this field displays None .
State	PW state: Up , Down , or Blocked . Blocked indicates that the PW is a backup PW.

Display detailed PW forwarding information for all cross-connect groups.

```

<Sysname> display l2vpn forwarding pw verbose

```

Xconnect-group Name: vpn1

Connection Name: ldp

Link ID: 0

PW Type : VLAN PW State : Up
In Label : 1279 Out Label: 1151
MTU : 1500
PW Attributes : Main
VCCV CC : Router-Alert
VCCV BFD : -
Tunnel Group ID : 0x60000000
Tunnel NHLFE IDs: 1025

Link ID: 1

PW Type : VLAN PW State : Up
In Label : 1278 Out Label: 1151
MTU : 1500
PW Attributes : Main
VCCV CC : Router-Alert
VCCV BFD : -
Tunnel Group ID : 0x160000001
Tunnel NHLFE IDs: 1027

Table 10 Command output

Field	Description
PW State	PW state: Up , Down , or Blocked . Blocked indicates that the PW is a backup PW.
PW Attributes	PW attribute: <ul style="list-style-type: none">• Main—The PW is the primary PW.• Backup—The PW is the backup PW.• Bypass—The PW is a bypass PW.
VCCV CC	VCCV CC type: Router-Alert —MPLS Router Alert Label. This field displays a hyphen (-) if no VCCV CC type is specified.
VCCV BFD	This field is not supported in the current software version. VCCV BFD type: <ul style="list-style-type: none">• Fault Detection with BFD. BFD packets use IP/UDP encapsulation (with IP/UDP headers).• Fault Detection with Raw-BFD. BFD packets use PW-ACH encapsulation (without IP/UDP headers). This field displays a hyphen (-) if BFD is not used to verify PW connectivity.
Tunnel Group ID	ID of the tunnel group for the PW.
Tunnel NHLFE IDs	NHLFE IDs of the public tunnels that carry the PW. If equal-cost tunnels are available, this field displays multiple tunnel NHLFE IDs. If no tunnel is available, this field displays None .

display l2vpn ldp

Use `display l2vpn ldp` to display LDP PW label information.

Syntax

```
display l2vpn ldp [ peer ip-address [ pw-id pw-id ] | xconnect-group  
group-name ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

peer ip-address: Displays LDP PW label information advertised by a peer PE. The *ip-address* argument specifies the LSR ID of the peer PE. If you do not specify a peer PE, this command displays LDP PW label information advertised by all peer PEs.

pw-id pw-id: Displays LDP PW label information for a PW. The *pw-id* argument specifies the PW ID in the range of 1 to 4294967295. If you specify **peer ip-address** without this option, the command displays all LDP PW label information advertised by the peer PE.

xconnect-group group-name: Displays LDP PW label information for a cross-connect group. The *group-name* argument specifies the cross-connect group name, a case-sensitive string of 1 to 31 characters. If you do not specify a cross-connect group, this command displays LDP PW label information for all cross-connect groups.

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

Examples

Display brief information about all LDP PW labels.

```
<Sysname> display l2vpn ldp
```

```
Total number of LDP PWs: 5, 4 up, 1 down
```

Peer	PW ID/VPLS ID	In/Out Label	State	Owner
192.3.3.3	1001	775125/775126	Up	vpws1
192.3.3.3	1001	775125/775126	Up	vpws1
192.3.3.3	1003	775117/775122	Up	vpws3
192.3.3.3	1004	775120/775120	Up	vpws4
192.4.4.4	1000	775116/unknown	Down	vpws5

Table 11 Command output

Field	Description
PW ID/VPLS ID	This field displays the PW ID for FEC 128, and displays the VPLS ID for FEC 129. Only VPLS supports FEC 129.
Owner	Cross-connect group of the PW.

Display detailed information about all LDP PW labels.

```

<Sysname> display l2vpn ldp verbose
Peer: 192.2.2.2          PW ID: 1000
  Xconnect-group: vpn1
  Connection      : ldp
  PW State       : Up
  PW Status Communication: Notification method
  PW Preferential Forwarding Status Bit: Process
  PW ID FEC (Local/Remote):
    PW Type      : VLAN/VLAN
    Group ID     : 0/0
    Label        : 151/279
    Control Word: Disabled/Disabled
    VCCV CC Type: -/-
    VCCV CV Type: -/-
    MTU          : 1500/1500
    PW Status    : PW forwarding/PW forwarding

```

Table 12 Command output

Field	Description
Xconnect-group	Cross-connect group of the PW.
Connection	Cross-connect of the PW.
PW Status Communication	PW state communicate: <ul style="list-style-type: none"> • Notification method—Uses notifications to communicate PW states. • Label withdraw method—Assigns a PW label to the PW when the AC is up and withdraws the PW label when the AC goes down.
PW Preferential Forwarding Status Bit	PW state processing mode: <ul style="list-style-type: none"> • Process—Process the received PW states. • Ignore—Ignore the received PW states.
VCCV CC Type	VCCV CC type: Router-Alert —MPLS Router Alert Label. This field displays a hyphen (-) if no VCCV CC type is specified. For information about VCCV, see <i>MPLS Configuration Guide</i> .
VCCV CV Type	VCCV CV type: LSP Ping —Uses MPLS LSP ping to verify PW connectivity. This field displays a hyphen (-) if VCCV is not performed on the PW.
PW Status	PW status: <ul style="list-style-type: none"> • PW forwarding—PW is ready for packet forwarding. • PW not forwarding—PW is not ready for packet forwarding. • AC receive fault—AC cannot receive packets. • AC transmit fault—AC cannot send packets. • PW receive fault—PW cannot receive packets. • PW transmit fault—PW cannot send packets. • PW standby—The PW is in standby state. • Unknown—Unknown protocol.

display l2vpn pw

Use `display l2vpn pw` to display L2VPN PW information.

Syntax

```
display l2vpn pw [ xconnect-group group-name ] [ protocol { bgp | ldp | static } ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

xconnect-group *group-name*: Displays L2VPN PW information for a cross-connect group. The *group-name* argument specifies the cross-connect group name, a case-sensitive string of 1 to 31 characters. If you do not specify a group, this command displays L2VPN PW information for all cross-connect groups.

protocol: Displays L2VPN PW information established by a protocol. If you do not specify a protocol, this command displays L2VPN PW information established by all protocols.

bgp: Displays BGP PW information.

ldp: Displays LDP PW information.

static: Displays static PW information, including remote CCC connections.

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

Usage guidelines

After you enable PW statistics, you can use the `display l2vpn pw verbose` command to display PW statistics.

Examples

Display brief information about all L2VPN PWs.

```
<Sysname> display l2vpn pw
Flags: M - main, B - backup, BY - bypass, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2
2 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate
```

```
Xconnect-group Name: ldp
Peer          PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID  State
192.3.3.3     500              500/500         LDP    M     0        Up
```

```
Xconnect-group Name: vpnb
Peer          PW ID/Rmt Site    In/Out Label    Proto  Flag  Link ID  State
192.3.3.3     2                1000/1021       BGP    M     1        Up
```

Table 13 Command output

Field	Description
Flags	PW flag.
PW ID/Rmt Site	This field displays the PW ID for a static or LDP PW, and displays the remote site ID for a BGP PW.
Proto	Protocol that established the PW: LDP , Static , or BGP .
Flag	PW attribute: <ul style="list-style-type: none"> • M—Primary PW. • B—Backup PW. • BY—Bypass PW.
Link ID	Link ID of the PW.
State	PW state: <ul style="list-style-type: none"> • Up—The PW is available. • Down—The PW is not available. • Blocked—The PW is a backup PW. • Idle—The incoming label of the PW is not available. • Dup—The incoming label of the static PW is used by a static LSP or a static CRLSP.

Display detailed information about all PWs.

```
<Sysname> display l2vpn pw verbose
```

```
Xconnect-group Name: ldp
```

```
Connection Name: ldp
```

```
Peer: 192.3.3.3          PW ID: 500
  Signaling Protocol   : LDP
  Link ID              : 0          PW State : Up
  In Label             : 1299      Out Label: 1299
  MTU                  : 1500
  PW Attributes        : Main
  VCCV CC              : -
  VCCV BFD             : -
  Tunnel Group ID     : 0x800000160000000
  Tunnel NHLFE IDs    : 1026
```

```
Xconnect-group Name: vpnb
```

```
Connection of auto-discovery: Site 1
```

```
Peer: 192.3.3.3          Remote Site: 2
  Signaling Protocol   : BGP
  Link ID              : 1          PW State : Up
  In Label             : 1036      Out Label: 1163
  MTU                  : 1500
  PW Attributes        : Main
  VCCV CC              : -
  VCCV BFD             : -
  Tunnel Group ID     : 0x800000160000000
  Tunnel NHLFE IDs    : 1026
```

Table 14 Command output

Field	Description
Xconnect-group Name	Cross-connect group name.
Connection Name	Cross-connect name, which is displayed for LDP and static PWs.
Peer	IP address of the peer PE of the PW.
Signaling Protocol	Protocol that established the PW: LDP , Static , or BGP .
PW State	<p>PW state:</p> <ul style="list-style-type: none"> • Up—The PW is available. • Down—The PW is not available. • Blocked—The PW is a backup PW. • Idle—The incoming label of the PW is not available. • Duplicate—The incoming label of the static PW is used by a static LSP or a static CRLSP.
Wait to Restore Time	<p>Wait time to switch traffic from the backup PW to the primary PW when the primary PW recovers, in seconds. If the switchover is disabled, this field displays Infinite.</p> <p>This field is available when both primary and backup PW exist, and is displayed only for the primary PW.</p>
Remaining Time	Remaining wait time for traffic switchover, in seconds.
PW Attributes	<p>PW attribute:</p> <ul style="list-style-type: none"> • Main—Primary PW. • Backup—Backup PW. • Bypass—Bypass PW.
VCCV CC	<p>VCCV CC type:</p> <p>Router-Alert—MPLS Router Alert Label.</p> <p>This field displays a hyphen (-) if no VCCV CC type is specified.</p>
VCCV BFD	<p>This field is not supported in the current software version.</p> <p>VCCV BFD type:</p> <ul style="list-style-type: none"> • Fault Detection with BFD. BFD packets use IP/UDP encapsulation (with IP/UDP headers). • Fault Detection with Raw-BFD. BFD packets use PW-ACH encapsulation (without IP/UDP headers). <p>This field displays a hyphen (-) if BFD is not used to verify PW connectivity.</p>
Tunnel Group ID	ID of the tunnel group for the PW.
Tunnel NHLFE IDs	<p>NHLFE IDs of the public tunnels that carry the PW.</p> <p>If equal-cost tunnels are available, this field displays multiple tunnel NHLFE IDs.</p> <p>If no tunnel is available, this field displays None.</p>
Connection of auto-discovery	The PW is a BGP PW.
Site	Local site ID.
Remote site	Remote site ID.

display l2vpn pw-class

Use `display l2vpn pw-class` to display PW class information.

Syntax

```
display l2vpn pw-class [ class-name ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

class-name: Displays information about the PW class specified by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a PW class, this command displays information about all PW classes.

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

Examples

```
# Display information about all PW classes.
```

```
<Sysname> display l2vpn pw-class  
Total number of PW classes: 2
```

PW Class Name	PW Type	Control Word	VCCV CC	VCCV BFD
pw1	Ethernet	Enabled	Router-Alert	-
pw2	VLAN	Disabled	Router-Alert	-

Table 15 Command output

Field	Description
VCCV CC	VCCV CC type: Router-Alert —MPLS Router Alert Label. This field displays a hyphen (-) if no VCCV CC type is specified.
VCCV BFD	This field is not supported in the current software version. VCCV BFD type: <ul style="list-style-type: none">• BFD—BFD packets use IP/UDP encapsulation (with IP/UDP headers).• Raw-BFD—BFD packets use PW-ACH encapsulation (without IP/UDP headers). This field displays a hyphen (-) if BFD is not used to verify PW connectivity.

```
# Display detailed information about all PW classes.
```

```
<Sysname> display l2vpn pw-class verbose  
PW Class Name : pw1  
PW Type      : Ethernet  
Control Word: Enabled  
VCCV CC     : Router-Alert
```

```
VCCV BFD      : -
Sequencing   : -
```

```
PW Class Name : pw2
PW Type       : VLAN
Control Word  : Disabled
VCCV CC      : Router-Alert
VCCV BFD     : -
Sequencing   : -
```

Table 16 Command output

Field	Description
PW Type	PW data encapsulation type: Ethernet or VLAN .
Control Word	Whether control word is enabled.
VCCV CC	VCCV CC type: Router-Alert —MPLS Router Alert Label. This field displays a hyphen (-) if no VCCV CC type is specified.
VCCV BFD	This field is not supported in the current software version. VCCV BFD type: <ul style="list-style-type: none"> • BFD—BFD packets use IP/UDP encapsulation (with IP/UDP headers). • Raw-BFD—BFD packets use PW-ACH encapsulation (without IP/UDP headers). This field displays a hyphen (-) if BFD is not used to verify PW connectivity.
Sequencing	This field is not supported in the current software version. Packet sequencing on the PW. The value is Both , which means sequencing is enabled for both incoming and outgoing packets on a PW. A hyphen (-) in this field indicates that packet sequencing is disabled on the PW.

Related commands

`pw-class`

display l2vpn service-instance

Use `display l2vpn service-instance` to display Ethernet service instance information.

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
mdc-admin
mdc-operator
```

Parameters

interface *interface-type interface-number*: Displays Ethernet service instance information for the specified Layer 2 Ethernet interface or Layer 2 aggregate interface. 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*: Displays information about the Ethernet service instance specified by its ID. The instance ID is in the range of 1 to 4096. If you specify **interface interface-type interface-number** without this option, the command displays information about all Ethernet service instances on the specified Layer 2 Ethernet interface or Layer 2 aggregate interface.

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

Examples

Display brief information about all Ethernet service instances.

```
<Sysname> display l2vpn service-instance
Total number of service-instances: 5, 5 up, 0 down
Total number of ACs: 2, 2 up, 0 down
```

Interface	SrvID	Owner	LinkID	State	Type
XGE1/0/1	1	vpws1	1	Up	VPWS
XGE1/0/1	2	vpws2	1	Up	VPWS

Table 17 Command output

Field	Description
SrvID	Ethernet service instance ID.
Owner	Name of the cross-connect group bound to the Ethernet service instance. This field is empty if no cross-connect group is bound.
Link ID	Link ID of the AC.
State	State of the service instance: UP or Down .
Type	L2VPN type. The value can only be VPWS for an MPLS L2VPN network.

Display detailed information about all Ethernet service instances on Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1.

```
<Sysname> display l2vpn service-instance interface ten-gigabitethernet 1/0/1 verbose
Interface: XGE1/0/1
  Service Instance: 1
    Type           : Manual
    Encapsulation  : s-vid 16
    Bandwidth      : -
    Xconnect-group: vpws1
    Connection     : actopw
    Link ID        : 1
    State          : Up
    Statistics     : Disabled
```

Table 18 Command output

Field	Description
Interface	Layer 2 Ethernet interface or Layer 2 aggregate interface.
Type	Ethernet service instance type. This field can only be Manual , which indicates that the Ethernet service instance is manually created.
Encapsulation	Packet match criterion of the Ethernet service instance. This field is not displayed if no packet match criterion is configured.
Bandwidth	This field is not supported in the current software version. Maximum bandwidth (in kbps) for traffic on the AC.
Xconnect-group	Name of the cross-connect group bound to the Ethernet service instance.
AD connection	Name of the auto-discovery cross-connect bound to the Ethernet service instance, identified by the local and remote site IDs.
Link ID	Link ID of the AC.
State	State of the Ethernet service instance: UP or Down .
Statistics	This field is not supported in the current software version. Packet statistics state: Disabled —Packet statistics is disabled for the Ethernet service instance.

Related commands

`service-instance`

display l2vpn xconnect-group

Use `display l2vpn xconnect-group` to display cross-connect group information.

Syntax

```
display l2vpn xconnect-group [ name group-name ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator
mdc-admin
mdc-operator

Parameters

name *group-name*: Displays information about a cross-connect group. The *group-name* argument specifies the cross-connect group name, a case-sensitive string of 1 to 31 characters. If you do not specify a group, this command displays information about all cross-connect groups.

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

Examples

```
# Display brief information about all cross-connect groups.
<Sysname> display l2vpn xconnect-group
```

Total number of cross-connections: 3, 0 up, 3 down, 0 admin down

Xconnect-group Name	Connection ID	MTU	State
abc	0	1500	Down
vpn1	2	1500	Down
vpn2	1	1500	Down

Table 19 Command output

Field	Description
Connection ID	Cross-connect ID.
State	Cross-connect group state: Up , Down , or Admin down . Admin down indicates that the cross-connect group has been shut down by using the shutdown command.

Display detailed information about all cross-connect groups.

```
<Sysname> display l2vpn xconnect-group verbose
```

```
Xconnect-group Name: vpnb
Connection of auto-discovery: Site 1, Remote Site 2
Connection ID      : 0
State              : Up
MTU                : 1500
PW Redundancy     : Slave
BGP PWs:
  Peer             Remote Site   Link ID   State
  192.3.3.3       2                 1         Up
ACs:
  AC               Link ID   State   Type
  XGE1/0/4 srv1   0         Up      Manual
```

Table 20 Command output

Field	Description
Xconnect-group Name	Cross-connect group name.
Description	Description for the cross-connect group. If no description is configured, this field is not displayed.
Connection Name	Cross-connect name.
Connection of auto-discovery	Auto-discovery cross-connect.
Site	Local site ID.
Remote site	Remote site ID.
Connection ID	Cross-connect ID.
State	Cross-connect group state: Up , Down , or Admin down . Admin down indicates that the cross-connect group has been shut down by using the shutdown command.

Field	Description
PW Redundancy	PW redundancy mode: <ul style="list-style-type: none"> • Slave—Master/slave mode and the local PE operates as the slave node. • Master—Master/slave mode and the local PE operates as the master node.
State	PW state: Up , Down , Blocked , or Defect .
Type	Ethernet service instance type. This field can only be Manual , which indicates that the Ethernet service instance is manually created.
AC	AC type: <ul style="list-style-type: none"> • Layer 3 interface. • Ethernet service instance on a Layer 2 interface.

Related commands

`xconnect-group`

encapsulation

Use `encapsulation` to configure a packet match criterion for an Ethernet service instance.

Use `undo encapsulation` to restore the default.

Syntax

```
encapsulation s-vid vlan-id [ only-tagged ]
encapsulation { default | tagged | untagged }
undo encapsulation
```

Default

No packet match criterion is configured for an Ethernet service instance.

Views

Ethernet service instance view

Predefined user roles

network-admin

mdc-admin

Parameters

s-vid *vlan-id*: Matches packets with the specified outer VLAN ID.

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

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

vlan-id: Specifies a VLAN ID in the range of 1 to 4094.

default: Matches packets that do not match any other Ethernet service instances on the interface. On an interface, you can configure this criterion only in one Ethernet service instance. The Ethernet service instance matches all packets if it is the only instance on the interface.

tagged: Matches any packets that have a VLAN tag.

untagged: Matches any packets that do not have a VLAN tag.

Usage guidelines

You can configure the default packet match criterion in only one of the Ethernet service instances on an Ethernet interface. Packets that do not match any other Ethernet service instances match the Ethernet service instance configured with the default packet match criterion. If the Ethernet service instance configured with the default packet match criterion is the only instance on the interface, the Ethernet service instance matches all packets.

You cannot repeat the **encapsulation** command to modify the match criterion of an Ethernet service instance. To change the match criterion, first execute the **undo encapsulation** command to remove the original match criterion.

Examples

```
# Configure Ethernet service instance 1 on Ten-GigabitEthernet 1/0/1 to match packets that have an outer VLAN ID of 111.
```

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

Related commands

```
display l2vpn service-instance
```

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
mdc-admin
```

Usage guidelines

You must enable L2VPN before configuring other L2VPN settings.

Examples

```
# Enable L2VPN.
<Sysname> system-view
[Sysname] l2vpn enable
```

l2vpn switchover

Use **l2vpn switchover** to switch traffic from a PW to its backup or primary PW.

Syntax

```
l2vpn switchover peer ip-address pw-id pw-id
```

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

peer *ip-address*: Specifies the LSR ID of the peer PE.

pw-id *pw-id*: Specifies a PW by its ID in the range of 1 to 4294967295.

Usage guidelines

The specified LSR ID and PW ID uniquely identify a PW.

If a PW has a backup PW or primary PW, this command switches traffic from the PW to the backup or primary PW. If the PW does not have a backup or primary PW, this command does not perform the switchover.

Examples

```
# Switch traffic from PW 100 destined for 3.3.3.3 to its backup PW.
```

```
<Sysname> l2vpn switchover peer 3.3.3.3 pw-id 100
```

mtu

Use **mtu** to set an MTU for PWs established on a cross-connect or auto-discovery cross-connect.

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

Syntax

```
mtu size
```

```
undo mtu
```

Default

A PW has an MTU of 1500 bytes.

Views

Cross-connect view

Auto-discovery cross-connect group view

Predefined user roles

network-admin

mdc-admin

Parameters

size: Specifies an MTU value. The value range is 300 to 65535.

Usage guidelines

The specified MTU applies to all PWs established in the cross-connect view or the auto-discovery cross-connect group view.

The MTU specifies the maximum packet length, including the control word, PW label, and network layer packet.

For an LDP PW to come up, the PEs at the two ends of the PW must have the same MTU.

Examples

```
# Set the MTU to 1400 bytes for cross-connect ac2pw in cross-connect group vpn1.
```

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection ac2pw
[Sysname-xcg-vpn1-ac2pw] mtu 1400
```

```
# Set the MTU to 1400 bytes for the auto-discovery cross-connect in cross-connect group bbb.
```

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] mtu 1400
```

Related commands

```
display l2vpn xconnect-group
```

peer

Use **peer** to configure a PW for a cross-connect and enter cross-connect PW view, or enter the view of an existing cross-connect PW.

Use **undo peer** to delete a PW for a cross-connect.

Syntax

```
peer ip-address pw-id pw-id [ ignore-standby-state | in-label label-value out-label label-value ] [ pw-class class-name | tunnel-policy tunnel-policy-name ] *
```

```
undo peer ip-address pw-id pw-id
```

Default

No PWs exist for a cross-connect.

Views

Cross-connect view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies the LSR ID of the peer PE.

pw-id *pw-id*: Specifies a PW ID for the PW, in the range of 1 to 4294967295.

ignore-standby-state: Ignores the PW active/standby status bit received from the remote PE. This keyword is applicable only to LDP PWs.

in-label *label-value*: Specifies the incoming label of the PW. The value range is 16 to 1023.

out-label *label-value*: Specifies the outgoing label of the PW. The value range is 16 to 1048575.

pw-class *class-name*: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters. You can specify a PW class to configure the PW data encapsulation type and control word. If you do not specify a PW class, the PW data encapsulation type is determined by the interface type. The control word feature is not supported for PW data encapsulation types that do not require using control word.

tunnel-policy *tunnel-policy-name*: Specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a tunnel policy, the default tunnel policy is used.

Usage guidelines

A PE uses the PW Preferential Forwarding Status bit in LDP messages to advertise the local PWs' active/standby states. When the bit is set, it indicates that the local PW is in standby state. When the bit is cleared, it indicates that the local PW is in active state.

In master/slave mode of PW redundancy, the slave PE selects the forwarding PW among the set of redundant PWs based on the status bit received from the master PE. If you specify the **ignore-standby-state** keyword, the PE ignores the status bit received from the master PE and uses the primary PW to forward packets as long as the primary PW is up.

The PW ID for a PW must be the same on the PEs at the two ends of the PW.

On a PE, the LSR ID of the peer PE and the PW ID uniquely identify a PW. The peer LSR ID and PW ID combination of a PW must be unique among all VPLS PWs and cross-connect PWs.

To create a static PW, you must specify the incoming and outgoing labels. To enter the view of an existing static PW, you do not need to specify the incoming and outgoing labels.

If you do not specify the incoming and outgoing labels when you create a new PW, LDP is used to create the PW.

To create a multi-segment PW, execute the **peer** command twice to create two cross-connect PWs in the same cross-connect view. The two PWs form a multi-segment PW.

Multi-segment PW and backup PW are mutually exclusive with each other. If you have configured a multi-segment PW, you cannot configure a backup PW for the two PWs that form the multi-segment PW. If you have configured a backup PW for a PW, the PW cannot form a multi-segment PW. For information about configuring a backup PW, see the **backup-peer** command.

When you add a static PW, you must make sure that static PW uses a different incoming label than an existing static LSP or static CRLSP. If the incoming label is duplicated, you cannot make the static PW take effect by changing the incoming label of the static LSP or CRLSP. Instead, you must delete the static PW and then reconfigure the static PW with an unused incoming label.

Examples

Configure an LDP PW destined to 4.4.4.4 for cross-connect **pw2pw** in cross-connect group **vpn1** and enter cross-connect PW view. The PW ID is 200.

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection pw2pw
[Sysname-xcg-vpn1-pw2pw] peer 4.4.4.4 pw-id 200
[Sysname-xcg-vpn1-pw2pw-4.4.4.4-200]
```

Configure a static PW destined to 5.5.5.5 for cross-connect **pw2pw** in cross-connect group **vpn1** and enter cross-connect PW view. The static PW has an ID of 200, an incoming label of 100, and an outgoing label of 200.

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection pw2pw
```

```
[Sysname-xcg-vpn1-pw2pw] peer 5.5.5.5 pw-id 200 in-label 100 out-label 200
[Sysname-xcg-vpn1-pw2pw-5.5.5.5-200]
```

Related commands

```
display l2vpn ldp
display l2vpn pw
pw-class
tunnel-policy
```

peer signaling

Use **peer signaling** to enable BGP to exchange label block information with the specified peer or peer group.

Use **undo peer signaling** to disable BGP to exchange label block information with the specified peer or peer group.

Syntax

```
peer { group-name | ip-address [ mask-length ] } signaling [ non-standard ]
undo peer { group-name | ip-address [ mask-length ] } signaling
```

Default

BGP can exchange label block information with an L2VPN peer or peer group through RFC 4761 MP_REACH_NLRI.

Views

BGP L2VPN address family view

Predefined user roles

```
network-admin
mdc-admin
```

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The specified peer group must have been created.

ip-address: Specifies a peer by its IP address. The specified peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ip-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command enables BGP to exchange label block information with all dynamic peers in the subnet.

non-standard: Uses draft-kompella-ppvpn-l2vpn-03 MP_REACH_NLRI to exchange label block information. If you do not specify this keyword, RFC 4761 MP_REACH_NLRI is used to exchange label block information.

Usage guidelines

L2VPN uses MP-BGP to exchange label blocks when creating a BGP PW.

To enable BGP to exchange label blocks with the specified peers through RFC 4761 MP_REACH_NLRI, you can also use the **peer enable** command in BGP L2VPN address family view. To disable the capability, use the **undo peer signaling** command.

Examples

```
# Enable BGP to exchange label block information with the peer 3.3.3.9 through
draft-kompella-ppvpn-l2vpn-03 MP_REACH_NLRI.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn
[Sysname-bgp-default-l2vpn] peer 3.3.3.9 signaling non-standard
```

Related commands

```
display bgp l2vpn signaling
```

policy vpn-target

Use **policy vpn-target** to enable route target-based filtering of incoming BGP L2VPN information.

Use **undo policy vpn-target** to disable route target-based filtering of incoming BGP L2VPN information.

Syntax

```
policy vpn-target
undo policy vpn-target
```

Default

Route target-based filtering of incoming BGP L2VPN information is enabled.

Views

BGP L2VPN address family view

Predefined user roles

```
network-admin
mdc-admin
```

Usage guidelines

If route target-based filtering is enabled, L2VPN accepts only the incoming BGP L2VPN information whose export route target attribute matches the local import route target attribute. If route target-based filtering is disabled, L2VPN accepts all incoming BGP L2VPN information.

To establish a BGP PW between two MP-IBGP peers that use a route reflector, you must disable route target-based filtering of incoming BGP L2VPN information on the route reflector.

Examples

```
# Disable route target-based filtering of incoming BGP L2VPN information.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn
[Sysname-bgp-default-l2vpn] undo policy vpn-target
```

pw-class (auto-discovery cross-connect group view)

Use **pw-class** to specify a PW class for an auto-discovery cross-connect group.

Use **undo pw-class** to restore the default.

Syntax

```
pw-class class-name
undo pw-class
```

Default

No PW class is specified.

Views

Auto-discovery cross-connect group view

Predefined user roles

network-admin

mdc-admin

Parameters

class-name: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters.

Usage guidelines

The specified PW class will be used to establish all PWs in the auto-discovery cross-connect group.

Examples

Specify a PW class named **pw100** for auto-discovery cross-connect group **bbb**.

```
<Sysname> system-view
[Sysname] pw-class pw100
[Sysname-pw-pw100] quit
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] pw-class pw100
```

Related commands

control-word enable

display l2vpn pw-class

pw-class

pw-type

pw-class (system view)

Use **pw-class** to create a PW class and enter its view, or enter the view of an existing PW class.

Use **undo pw-class** to delete a PW class.

Syntax

```
pw-class class-name
```

```
undo pw-class class-name
```

Default

No PW classes exist.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

class-name: Specifies a name for the PW class, a case-sensitive string of 1 to 19 characters.

Usage guidelines

In PW class view, you can configure PW attributes such as the PW data encapsulation type and whether to enable control word. You can configure PWs to use the same PW class to simplify PW attribute configuration.

Examples

```
# Create a PW class named pw100 and enter PW view.  
<Sysname> system-view  
[Sysname] pw-class pw100  
[Sysname-pw-pw100]
```

Related commands

```
control-word enable  
display l2vpn pw-class  
pw-type
```

pw-redundancy

Use **pw-redundancy** to specify the master/slave PW redundancy mode and configure the local PE as the master node.

Use **undo pw-redundancy** to restore the default.

Syntax

```
pw-redundancy master  
undo pw-redundancy
```

Default

The PW redundancy mode is master/slave and the local PE operates as the slave node.

Views

Cross-connect view

Predefined user roles

```
network-admin  
mdc-admin
```

Parameters

master: Uses the master/slave PW redundancy mode and configures the local PE as the master node.

Usage guidelines

This command is applicable only to LDP PWs.

For LDP PWs, PEs use LDP to negotiate the active/standby states of the PWs. In master/slave mode, one endpoint PE of a PW operates as the master node and the other endpoint PE operates as the slave node. The master PE determines the active/standby state of the PW and uses LDP to advertise the PW state to the slave PE. The slave PE uses the same PW state as the master PE based on the information received from the master PE. In this way, the master and slave PEs for the set of redundant PWs can use the same active PW to forward user traffic.

The slave PE does not need to send the PW states to the master PE and the master PE ignores the PW states sent by the slave PE.

Do not configure this command on the local PE if the remote PE does not support the master/slave PW redundancy mode.

Examples

Configure the master/slave PW redundancy mode for cross-connect **pw2pw** of cross-connect group **vpn1** and configure the local PE as the master node.

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection pw2pw
[Sysname-xcg-vpn1-pw2pw] pw-redundancy master
```

Related commands

```
backup-peer
display l2vpn ldp
display l2vpn pw
peer
```

pw-type

Use **pw-type** to specify a PW data encapsulation type for a PW class.

Use **undo pw-type** to restore the default.

Syntax

```
pw-type { ethernet | vlan }
undo pw-type
```

Default

The PW data encapsulation type is VLAN.

Views

PW class view

Predefined user roles

```
network-admin
mdc-admin
```

Parameters

ethernet: Specifies the PW data encapsulation type as Ethernet.

vlan: Specifies the PW data encapsulation type as VLAN.

Usage guidelines

This command takes effect only when the AC type is Ethernet.

When the PW data encapsulation type is Ethernet, P-tag is not transferred on a PW.

- For a packet from a CE:
 - If the packet contains a P-tag, the PE removes the P-tag, and adds a PW label and an outer tag into the packet before forwarding it.
 - If the packet contains no P-tag, the PE directly adds a PW label and an outer tag into the packet before forwarding it.

- For a packet to a CE:
 - If the access mode is configured as VLAN by using the **ac interface** command, the PE adds a P-tag into the packet before sending it to the CE.
 - If the access mode is configured as Ethernet by using the **ac interface** command, the PE directly sends the packet to the CE.

You cannot rewrite or remove existing tags.

When the PW data encapsulation type is VLAN, packets transmitted over a PW must carry a P-tag.

- For a packet from a CE:
 - If the peer PE does not require the ingress to rewrite the P-tag, the PE keeps the P-tag unchanged for the packet, and then encapsulates the packet. If the packet contains no P-tag, the PE adds a null label (the label value is 0) into the packet, and then encapsulates the packet.
 - If the peer PE requires the ingress to rewrite the P-tag, the PE changes the P-tag to the expected VLAN tag (the tag value might be 0), and then adds a PW label and an outer tag into the packet. If the packet contains no P-tag, the PE adds a VLAN tag expected by the peer PE (the tag value might be 0), and then adds a PW label and an outer tag into the packet.
- For a packet to a CE:
 - If the access mode is configured as VLAN by using the **ac interface** command, the PE rewrites or retains the P-tag before forwarding the packet.
 - If the access mode is configured as Ethernet by using the **ac interface** command, the PE removes the P-tag before forwarding the packet.

Examples

Configure the PW data encapsulation type as Ethernet.

```
<Sysname> system-view
[Sysname] pw-class pw100
[Sysname-pw-pw100] pw-type ethernet
```

Related commands

```
ac-interface
display l2vpn pw-class
```

revertive

Use **revertive** to specify the switchover mode and set the switchover wait time.

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

Syntax

```
revertive { wtr wtr-time | never }
undo revertive { wtr | never }
```

Default

The switchover mode is revertive and the switchover wait time is 0 seconds. When the primary PW recovers, traffic is immediately switched from the backup PW to the primary PW.

Views

Cross-connect view

Predefined user roles

network-admin

mdc-admin

Parameters

wtr *wtr-time*: Specifies the switchover mode as revertive and specifies the wait time in the range of 0 to 3600 seconds. When the primary PW recovers, the PE waits for the specified time before switching traffic from the backup PW to the primary PW.

never: Specifies the switchover mode as non-revertive. After the primary PW recovers, traffic is not switched from the backup PW to the primary PW.

Examples

```
# Specify the revertive mode and set the switchover wait time to 120 seconds for cross-connect ac2pw in cross-connect group vpn1.
```

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1] connection ac2pw
[Sysname-xcg-vpn1-ac2pw] revertive wtr 120
```

Related commands

```
display l2vpn pw
```

route-distinguisher

Use **route-distinguisher** to configure a route distinguisher (RD) for a BGP cross-connect group.

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

Syntax

```
route-distinguisher route-distinguisher
undo route-distinguisher
```

Default

No RD is configured for a BGP cross-connect group.

Views

Auto-discovery cross-connect group view

Predefined user roles

network-admin
mdc-admin

Parameters

route-distinguisher: Specifies an RD, a string of 3 to 21 characters. An RD can be in one of the following 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 be equal to or greater than 65536. For example, 65536:1.

Usage guidelines

MPLS L2VPN uses RDs to differentiate the sites with the same site ID but in different VPNs.

BGP adds the configured RD before the site ID. The RD and the site ID uniquely identify a VPN site.

You cannot configure the same RD for different BGP cross-connect groups.

To modify an RD, execute the **undo route-distinguisher** command to remove the RD, and then execute the **route-distinguisher** command.

Examples

Configure the RD **22:2** for BGP cross-connect group **bbb**.

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] route-distinguisher 22:2
```

rr-filter

Use **rr-filter** to create a route reflector (RR) reflection policy.

Use **undo rr-filter** to restore the default.

Syntax

```
rr-filter ext-comm-list-number
undo rr-filter
```

Default

An RR does not filter reflected L2VPN information.

Views

BGP L2VPN address family view

Predefined user roles

network-admin
mdc-admin

Parameters

ext-comm-list-number: Specifies an extended community list number in the range of 1 to 199.

Usage guidelines

After this command is executed, only the L2VPN information that is permitted by the specified extended community list is reflected.

By configuring different RR reflection policies on RRs in a cluster, you can implement load balancing among the RRs.

For more information about extended community lists, see *Layer 3—IP Routing Configuration Guide*.

Examples

Configure the RR to reflect only the BGP L2VPN information that is permitted by extended community list 10.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn
[Sysname-bgp-default-l2vpn] rr-filter 10
```

Related commands

ip extcommunity-list (*Layer 3—IP Routing Command Reference*)

service-instance

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

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

Syntax

```
service-instance instance-id  
undo service-instance instance-id
```

Default

No Ethernet service instances exist.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin
mdc-admin

Parameters

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

Examples

```
# Create Ethernet service instance 1 on Layer 2 Ethernet interface Ten-GigabitEthernet 1/0/1, and  
enter Ethernet service instance 1 view.  
<Sysname> system-view  
[Sysname] interface ten-gigabitethernet 1/0/1  
[Sysname-Ten-GigabitEthernet1/0/1] service-instance 1  
[Sysname-Ten-GigabitEthernet1/0/1-srv1]
```

Related commands

```
display l2vpn service-instance
```

shutdown (cross-connect group view)

Use **shutdown** to disable a cross-connect group.

Use **undo shutdown** to enable a cross-connect group.

Syntax

```
shutdown  
undo shutdown
```

Default

A cross-connect group is enabled.

Views

Cross-connect group view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

After you disable a cross-connect group, all cross-connects in the group cannot provide L2VPN services.

Use the **shutdown** command when you want to temporarily disable L2VPN. When a cross-connect group is disabled, you can still configure the cross-connect group. After the configuration, use the **undo shutdown** command to enable the cross-connect group. The cross-connect group will provide L2VPN services using the new settings.

Examples

```
# Disable cross-connect group vpn2.
```

```
<Sysname> system-view  
[Sysname] xconnect-group vpn2  
[Sysname-xcg-vpn2] shutdown
```

Related commands

```
display l2vpn xconnect-group
```

site

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

Use **undo site** to delete a local site.

Syntax

```
site site-id [ range range-value ] [ default-offset default-offset ]  
undo site site-id
```

Default

No sites exist.

Views

Auto-discovery cross-connect group view

Predefined user roles

```
network-admin  
mdc-admin
```

Parameters

site-id: Specifies a local site ID in the range of 0 to 256.

range *range-value*: Specifies the maximum number of sites in a VPN, in the range of 2 to 257. The default value is 10.

default-offset *default-offset*: Specifies the start site ID, 0 or 1. The default value is 0.

Usage guidelines

The **range** *range-value* and **default-offset** *default-offset* options determine the label block of the site.

- If you execute the **site** command with the *range-value* of *range1*, a label block with LR of *range1* and LO of *default-offset* is assigned to the site.

- If you execute another **site** command with *range-value* of *range2* (*range2* is larger than *range1*), a second label block with LR of *range2* to *range1* and LO being *range1* + *default-offset* is assigned to the site.

For example, if you execute the following commands, three label blocks LB1/0/10, LB2/10/12, and LB3/22/14 are assigned to site 1. LB1, LB2, and LB3 are automatically selected.

```
site 1 range 10 default-offset 0
site 1 range 22
site 1 range 36
```

You can create multiple local sites for a cross-connect group.

You can use the **site** command to increase the range value for an existing site. You cannot decrease the range value for an existing site with the **site** command. To decrease the range value, execute the **undo site** command to delete the site and then execute the **site** command.

Select a large range value to reduce future modifications for VPN expansion.

You cannot modify the *default-offset* for a site with the **site** command. To modify it, execute the **undo site** command to delete the site and then execute the **site** command.

Examples

Create site 1, configure the VPN to contain a maximum of 30 sites, set the start site ID to 0 for cross-connect group **bbb**, and enter site view.

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] site 1 range 30 default-offset 0
[Sysname-xcg-bbb-auto-1]
```

Related commands

```
display l2vpn pw
display l2vpn xconnect-group
```

snmp-agent trap enable l2vpn

Use **snmp-agent trap enable l2vpn** to enable SNMP notifications for L2VPN PW.

Use **undo snmp-agent trap enable l2vpn** to disable SNMP notifications for L2VPN PW.

Syntax

```
snmp-agent trap enable l2vpn [ pw-delete | pw-switch | pw-up-down ] *
undo snmp-agent trap enable l2vpn [ pw-delete | pw-switch | pw-up-down ] *
```

Default

SNMP notifications for L2VPN PW are disabled.

Views

System view

Predefined user roles

```
network-admin
mdc-admin
```

Parameters

pw-delete: Enables PW deletion notifications.

pw-switch: Enables PW primary/backup switchover notifications.

pw-up-down: Enables PW up-down notifications.

Usage guidelines

This feature enables L2VPN to generate SNMP notifications when PW deletions, PW status changes, or PW switchovers occur. For L2VPN event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

If you do not specify a notification type, this command enables all types of notifications for L2VPN PW.

Examples

```
# Enable PW up-down notifications.
<Sysname> system-view
[Sysname] snmp-agent trap enable l2vpn pw-up-down
```

Related commands

display snmp-agent trap-list (*Network Management and Monitoring Command Reference*)

tunnel-policy (auto-discovery cross-connect view)

Use **tunnel-policy** to specify a tunnel policy for an auto-discovery cross-connect.

Use **undo tunnel-policy** to restore the default.

Syntax

```
tunnel-policy tunnel-policy-name
undo tunnel-policy
```

Default

No tunnel policy is specified.

Views

Auto-discovery cross-connect view

Predefined user roles

network-admin
mdc-admin

Parameters

tunnel-policy-name: Specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters.

Usage guidelines

The PWs on the auto-discovery cross-connect use the specified tunnel policy to select public tunnels.

If you do not specify a tunnel policy or specify a nonexistent tunnel policy, the default tunnel policy applies. The default tunnel policy selects only one public tunnel for a PW in this order: LSP tunnel, CRLSP tunnel.

Examples

```
# Specify tunnel policy policy1 for the auto-discovery cross-connect in cross-connect group bbb.
<Sysname> system-view
```

```
[Sysname] tunnel-policy policy1
[Sysname-tunnel-policy-policy1] quit
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] site 2 range 10 default-offset 0
[Sysname-xcg-bbb-auto-2] connection remote-site-id 3
[Sysname-xcg-bbb-auto-2-3] tunnel-policy policy1
```

Related commands

tunnel-policy (system view)

vpn-target

Use **vpn-target** to configure route targets for a cross-connect group.

Use **undo vpn-target** to remove the specified or all route targets for a cross-connect group.

Syntax

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

Default

No route targets are configured for a cross-connect group.

Views

Auto-discovery cross-connect group view

Predefined user roles

network-admin
mdc-admin

Parameters

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

A route target is a string of 3 to 21 characters in one of the following 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 be equal to or greater than 65536. For example, 65536:1.

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

A local PE sets the route targets as export targets in BGP update messages when it advertises L2VPN information through the update messages to a remote peer. The peer uses its import targets to match the received export targets. If a match is found, the peer accepts the L2VPN information.

If you repeat this command, all the configured route targets take effect.

Examples

Configure import route targets as 10:1 100:1 1000:1 and export route targets as 20:1 200:1 2000:1 for BGP cross-connect group **bbb**.

```
<Sysname> system-view
[Sysname] xconnect-group bbb
[Sysname-xcg-bbb] auto-discovery bgp
[Sysname-xcg-bbb-auto] vpn-target 10:1 100:1 1000:1 import-extcommunity
[Sysname-xcg-bbb-auto] vpn-target 20:1 200:1 2000:1 export-extcommunity
```

xconnect-group

Use **xconnect-group** to create a cross-connect group and enter its view, or enter the view of an existing cross-connect group.

Use **undo xconnect-group** to delete a cross-connect group.

Syntax

```
xconnect-group group-name
undo xconnect-group group-name
```

Default

No cross-connect groups exist.

Views

System view

Predefined user roles

network-admin
mdc-admin

Parameters

group-name: Specifies a name for the cross-connect group, a case-sensitive string of 1 to 31 characters excluding hyphens.

Usage guidelines

L2VPN can create multiple LDP, BGP, and static PWs for a cross-connect group.

Examples

Create a cross-connect group named **vpn1** and enter cross-connect group view.

```
<Sysname> system-view
[Sysname] xconnect-group vpn1
[Sysname-xcg-vpn1]
```

Related commands

```
display l2vpn xconnect-group
```