# Contents

# LDP commands

# LDP common commands

## backoff

Use **backoff** to set the LDP backoff initial delay time and maximum delay time.

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

### Syntax

**backoff initial** *initial-time* **maximum** *maximum-time*

**undo backoff**

### Default

The LDP backoff initial delay time is 15 seconds, and the maximum delay time is 120 seconds.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**initial** *initial-time*: Specifies the LDP backoff initial delay time in the range of 15 to 50331 seconds.

**maximum** *maximum-time*: Specifies the LDP backoff maximum delay time in the range of 120 to 50331 seconds.

### Usage guidelines

LDP peers continually negotiate with each other until a session is set up. If LDP peers use incompatible negotiation parameters (for example, different label advertisement modes), a large amount of negotiation traffic will enter the network. To suppress LDP session negotiation traffic, use this command to control the interval between negotiation attempts.

After LDP fails to establish a session to a peer LSR for the first time, LDP does not start another attempt until the initial delay timer expires. If the session setup fails again, LDP waits for two times the previous delay before the next attempt. This process continues until the maximum delay time is reached. After that, the maximum delay time always takes effect.

If you configure the initial delay time to be larger than the maximum delay time, the configuration does not take effect. LDP uses the maximum delay time as the initial delay time.

### Examples

# Configure LDP backoff for the public network, and set the initial delay time to 100 seconds and the maximum delay time to 300 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] backoff initial 100 maximum 300
```

# display mpls ldp discovery

Use **display mpls ldp discovery** to display LDP discovery information.

## Syntax

**display mpls ldp discovery** [ **vpn-instance** *vpn-instance-name* ] [ [ **interface** *interface-type interface-number* | **peer** *peer-lsr-id* ] [ **ipv6** ] | **targeted-peer** { *ipv4-address* | *ipv6-address* } ] [ **verbose** ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Displays LDP discovery information for the specified MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays LDP discovery information for the public network.

**interface** *interface-type interface-number*: Displays information about basic discovery that uses the specified interface to send Link Hellos. The *interface-type interface-number* argument represents the interface type and number.

**peer** *peer-lsr-id*: Displays information about both basic and extended discovery mechanisms that have discovered the specified LDP peer. The *peer-lsr-id* argument represents the LSR ID of the LDP peer.

**ipv6**: Displays LDP IPv6 basic and extended discovery information. If you do not specify this keyword, the command displays LDP IPv4 basic and extended discovery information.

**targeted-peer**: Displays information about extended discovery that has sent Targeted Hellos to the specified LDP peer.

*ipv4-address*: Specifies the IPv4 address of the LDP peer.

*ipv6-address*: Specifies the IPv6 address of the LDP peer.

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

## Usage guidelines

If you do not specify the **interface**, **peer**, **ipv6**, or **targeted-peer** keyword, this command displays all LDP IPv4 basic and extended discovery information.

## Examples

# Display brief LDP IPv4 discovery information for the public network.

```
<Sysname> display mpls ldp discovery
     Type: L - Link Hello, T - Targeted Hello
Discovery Source              Hello Sent/Rcvd       Peer LDP ID
(L) Vlan10                    83/80                 100.100.100.18:0
                                                    200.100.100.18:0
(T) 100.100.100.18            23/20                 100.100.100.18:0
```

**Table 1 Command output**

| Field | Description |
|---|---|
| Type | Type of LDP discovery:<br>• **L**—Basic discovery, which sends Link Hellos to discover peers.<br>• **T**—Extended discovery, which sends Targeted Hellos to discover peers. |
| Discovery Source | Discovery source.<br>• If the LDP discovery type is **L**, this field displays the interface that discovers the peer.<br>• If the LDP discovery type is **T**, this field displays the IPv4 address of the peer. |
| Hello Sent/Rcvd | Number of hellos sent to the peer/number of hellos received from the peer. |
| Peer LDP ID | LDP identifier of the LDP peer. |

# Display brief LDP IPv6 discovery information for the public network.

```
<Sysname> display mpls ldp discovery ipv6
Interface: Vlan10
  Hello Sent/Rcvd: 12/12
    Peer LDP ID: 100.100.100.18:0
    Peer LDP ID: 200.200.200.28:0
Targeted Hellos: 2001:0000:130F::09C0:876A:130B ->
                 2005:130F::09C0:876A:130B
  Hello Sent/Rcvd: 93/80
    Peer LDP ID: 100.100.100.180:0
```

**Table 2 Command output**

| Field | Description |
|---|---|
| Interface | Interface that discovers the LDP peer by using basic discovery. |
| Hello Sent/Rcvd | Number of hellos sent to the peer/number of hellos received from the peer. |
| Peer LDP ID | LDP identifier of the LDP peer. |
| Targeted Hellos | Extended LDP discovery information. The address before **->** is the local IP address. The address after **->** is the peer IP address. |

# Display detailed LDP IPv4 discovery information for the public network.

```
<Sysname> display mpls ldp discovery verbose
Link Hellos:
  Interface Vlan-interface10
    Hello Interval   : 5000 ms           Hello Sent/Rcvd  : 83/160
    Transport Address: 100.100.100.17
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 202.118.224.18     Transport Address: 100.100.100.18
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)
    Peer LDP ID      : 100.100.100.20:0
      Source Address : 202.118.224.20     Transport Address: 100.100.100.20
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)

Targeted Hellos:
  100.100.100.17 -> 100.100.100.18 (Active, Passive)
```

```
    Hello Interval   : 15000 ms           Hello Sent/Rcvd  : 23/20
    Transport Address: 100.100.100.17
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 100.100.100.18     Transport Address: 100.100.100.18
      Hello Hold Time: 45 sec (Local: 45 sec, Peer: 45 sec)
  100.100.100.17 -> 100.100.100.20 (Active, Passive)
    Hello Interval   : 15000 ms           Hello Sent/Rcvd  : 23/22
    Transport Address: 100.100.100.17
    Peer LDP ID      : 100.100.100.20:0
      Source Address : 100.100.100.20     Transport Address: 100.100.100.20
      Hello Hold Time: 45 sec (Local: 45 sec, Peer: 45 sec)
```

# Display detailed LDP IPv6 discovery information for the public network.

```
<Sysname> display mpls ldp discovery ipv6 verbose
Link Hellos:
  Interface Vlan-interface10
    Hello Interval   : 5000 ms            Hello Sent/Rcvd  : 83/160
    Transport Address: 2001::2
    Peer LDP ID      : 100.100.100.18:0
      Source Address : FE80:130F:20C0:29FF:FEED:9E60:876A:130B
      Transport Address: 2001::1
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)

Targeted Hellos:
  2001:0000:130F::09C0:876A:130B ->
        2005:130F::09C0:876A:130B(Active, Passive)
    Hello Interval   : 15000 ms           Hello Sent/Rcvd  : 23/22
    Transport Address: 2001:0000:130F::09C0:876A:130B
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 2005:130F::09C0:876A:130B
      Destination Address : 2001:0000:130F::09C0:876A:130B
      Transport Address   : 2005:130F::09C0:876A:130B
      Hello Hold Time: 45 sec (Local: 45 sec, Peer: 45 sec)
```

**Table 3 Command output**

| Field | Description |
|---|---|
| Link Hellos | Information about basic discovery that sends Link Hellos on interfaces.<br>In a non-point-to-point network, an interface might discover multiple peers. |
| Interface | Interface using basic discovery. |
| Hello Interval | Hello interval in milliseconds. |
| Hello Sent/Rcvd | Number of Hellos sent or received on the interface. |
| Transport Address | Local transport address. |
| Peer LDP ID | LDP identifier of the LDP peer. |
| Source Address | Source IP address of received Hello messages. |
| Destination Address | Destination IP address of received Hello messages. |

| Field | Description |
| --- | --- |
| Transport Address | Transport address in the received Hello messages—the transport address of the LDP peer. |
| Hello Hold Time | Hello hold time in seconds.<br>• **Local**—Local hello hold time.<br>• **Peer**—Peer hello hold time.<br>The negotiated hello hold time is the smaller value of the local and peer hold time values. |
| Targeted Hellos | Information about extended LDP discovery that sends Targeted Hellos to peers. |
| 100.100.100.17 -> 100.100.100.18 (Active, Passive) | • The address before **->** (100.100.100.17 in this example) is the local IP address.<br>• The address after **->** (100.100.100.18 in this example) is the peer IP address.<br>• **(Active)** indicates that the local LSR is the Targeted Hello sender.<br>• **(Passive)** indicates that the local LSR is the Targeted Hello receiver.<br>• **(Active, Passive)** indicates that the local LSR is both the Targeted Hello sender and receiver. |

# display mpls ldp fec

Use **display mpls ldp fec** to display LDP FEC-label mappings.

## Syntax

**display mpls ldp fec** [ **vpn-instance** *vpn-instance-name* ] [ *ipv4-address mask-length* | *ipv6-address prefix-length* | [ **ipv6** ] [ **summary** ] ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command displays FEC-label mappings for the specified VPN instance. If you do not specify a VPN instance, this command displays FEC-label mappings for the public network.

*ipv4-address mask-length*: Specifies an IPv4 FEC by an IPv4 address and a mask length in the range of 0 to 32.

*ipv6-address prefix-length*: Specifies an IPv6 FEC by an IPv6 address and a prefix length in the range of 0 to 128.

**ipv6**: Displays IPv6 FEC-label mappings.

**summary**: Displays summary information about all FEC-label mappings learned by LDP.

### Usage guidelines

If you specify only the **summary** keyword, this command displays summary information about all IPv4 FEC-label mappings.

If you specify only the **ipv6** keyword, this command displays detailed information about all IPv6 FEC-label mappings.

If you specify the **summary** and **ipv6** keywords, this command displays summary information about all IPv6 FEC-label mappings.

If you do not specify the *ipv4-address mask-length*, *ipv6-address prefix-length*, **ipv6**, and **summary** parameters, this command displays detailed information about all IPv4 FEC-label mappings.

### Examples

# Display detailed information about all IPv4 FEC-label mappings learned by LDP for the public network.

```
<Sysname> display mpls ldp fec
 FEC: 100.100.100.18/32
   Flags: 0x02
   In Label: 1531
   Label Advertisement Policy:
     FEC Prefix-list: Fec-prefix-list
     Peer Prefix-list: Peer-prefix-list
   Upstream Info:
     Peer: 100.100.100.18:0        State: Established (stale)
   Downstream Info:
     Peer: 100.100.100.18:0
       Out Label: 3                State: Established (stale)
       Next Hops: 202.118.224.18          Vlan10
                  100.19.100.18           Vlan20


 FEC: 200.100.100.18/32 (No route)
   Flags: 0x0
   In Label: 1532
   Upstream Info:
     Peer: 200.200.200.28:0        State: Established
   Downstream Info:
     Peer: 120.100.100.18:0
       Out Label: 3                State: Idle
```

# Display detailed information about all IPv6 FEC-label mappings learned by LDP for the public network.

```
<Sysname> display mpls ldp fec ipv6
 FEC: 2005:130F::09C0/128
   Flags: 0x02
   In Label: 1026
   Label Advertisement Policy:
     FEC Prefix-list: Fec-ipv6-prefix-list
     Peer Prefix-list: Peer-ipv6-prefix-list
   Upstream Info:
     Peer: 100.100.100.18:0        State: Established (stale)
   Downstream Info:
```

```
Peer: 100.100.100.18:0
  Out Label: 3                State: Established (stale)
  Next Hops:
  FE80:130F:20C0:29FF:FEED:9E60:876A:130B          Vlan10
```

**Table 4 Command output**

| Field | Description |
|---|---|
| FEC | Forwarding equivalence class identified by an IP prefix. |
| Flags | FEC flag. It represents different things by setting different bits to 1. If multiple bits are set to 1, the flag represents all the things that correspond to those bits. This field displays the sum of the flag values. For example, if the FEC flag has values 0x01 and 0x20, this field displays 0x21.<br>Possible value of the FEC flag:<br>• **0x0**—Initial value.<br>• **0x01**—Egress LSP.<br>• **0x02**—Ingress LSP.<br>• **0x04**—Waiting to add an outgoing label to RIB.<br>• **0x08**—Waiting to refresh LSPs in LSM.<br>• **0x10**—Ready to advertise labels.<br>• **0x20**—FEC-label mappings have been refreshed during a GR process.<br>• **0x40**—Delayed refreshing LSPs in LSM.<br>• **0x80**—Non-egress LSP waiting for the recovery during a GR process. |
| In Label | Incoming label assigned by the local LSR to the FEC. |
| Label Advertisement Policy | Label advertisement policy. |
| FEC Prefix-list | IP prefix list for filtering FEC prefixes. |
| Peer Prefix-list | IP prefix list for filtering LDP peers. |
| Upstream Info | Upstream peer to which the local LSR advertised the FEC-label mapping and current state of the LSP. |
| Peer | LDP ID of an upstream peer. |
| State | Current state of the LSP established with the upstream peer:<br>• **Established**—Active state.<br>• **Idle**—Initial state.<br>• **Release Awaited**—Waiting for a Release message.<br>• **Resource Awaited**—Waiting for a label for the FEC.<br>If the state is marked as **stale**, the FEC-label mapping is under a GR process. |
| Downstream Info | Downstream peer from which the local LSR received the FEC-label mapping, and current state of the LSP. |
| Peer | LDP ID of a downstream peer. |
| Out Label | Outgoing label assigned by the downstream LSR for the FEC. |
| State | Current state of the LSP established with the downstream peer:<br>• **Established**—Active state.<br>• **Idle**—Inactive state.<br>If the state is marked as **stale**, the FEC-label mapping is under a GR process. |
| Next Hops | Next hops and outgoing interfaces. |

# Display summary information about all IPv4 FEC-label mappings learned by LDP for the public network.

```
<Sysname> display mpls ldp fec summary
FECs         : 3
Implicit Null: 1
Explicit Null: 0
Non-Null     : 2
No Label     : 0
No Route     : 0
Sent         : 3
Received     : 3
```

# Display summary information about all IPv6 FEC-label mappings learned by LDP for the public network.

```
<Sysname> display mpls ldp fec ipv6 summary
FECs         : 4
Implicit Null: 0
Explicit Null: 0
Non-Null     : 4
No Label     : 0
No Route     : 0
Sent         : 3
Received     : 3
```

**Table 5 Command output**

| Field | Description |
|---|---|
| FECs | Number of FECs that LDP has discovered from the routing protocol or FEC-label mappings advertised by peers. |
| Implicit Null | Number of FECs that are bound to the implicit null label. |
| Explicit Null | Number of FECs that are bound to the explicit null label. |
| Non-Null | Number of FECs that are bound to non-null labels. |
| No Label | Number of FECs without a label. |
| No Route | Number of FECs without matching routes.<br>The reason why an FEC has no matching route might be one of the following:<br>• No matching route exists in the routing table.<br>• The matching route exists in the routing table, but it is not redistributed into LDP.<br>• (For IPv6) The **mpls ldp ipv6 enable** or **targeted-peer** *ipv6-address* command is not configured on the device. In this case, an FEC is considered to have no route even though the matching IPv6 route exists in the routing table and has been redistributed into LDP. |
| Sent | Number of label mappings sent and being sent. |
| Received | Number of label mappings accepted. |

# display mpls ldp interface

Use **display mpls ldp interface** to display LDP interface information.

## Syntax

**display mpls ldp interface** [ **vpn-instance** *vpn-instance-name* ] [ *interface-type interface-number* ] [ **ipv6** ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command displays LDP interface information for the specified VPN instance. If you do not specify a VPN instance, this command displays LDP interface information for the public network.

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all LDP interfaces.

**ipv6**: Displays information about interfaces enabled with IPv6 LDP. If you do not specify this keyword, the command displays information about interfaces enabled with IPv4 LDP.

## Examples

# Display information about all interfaces enabled with IPv4 LDP for the public network.

```
<Sysname> display mpls ldp interface
Interface                MPLS         LDP            Auto-config
Vlan10                   Enabled      Configured     -
Vlan20                   Enabled      Configured     -
```

# Display information about all interfaces enabled with IPv6 LDP for the public network.

```
<Sysname> display mpls ldp interface ipv6
Interface                MPLS         LDP            Auto-config
Vlan10                   Enabled      Not Configured  -
Vlan20                   Enabled      Not Configured  -
```

**Table 6 Command output**

| Field | Description |
|---|---|
| Interface | Interface enabled with LDP. |
| MPLS | Whether the interface is enabled with MPLS. |
| LDP | Whether the interface is configured with the **mpls ldp enable** command or the **mpls ldp ipv6 enable** command. |

| Field | Description |
| --- | --- |
| Auto-config | This field is not supported in the current software version.<br>LDP automatic configuration information:<br>• If LDP autoconfiguration is enabled, this field displays IGP process information, such as OSPF process ID and OSPF area ID.<br>• If LDP autoconfiguration is disabled, this field displays a hyphen (-). |

### Related commands

**mpls ldp**

**mpls ldp enable**

**mpls ldp ipv6 enable**

# display mpls ldp lsp

Use **display mpls ldp lsp** to display information about LSPs generated by LDP.

### Syntax

**display mpls ldp lsp** [ **vpn-instance** *vpn-instance-name* ] [ *ipv4-address mask-length* | *ipv6-address prefix-length* | **ipv6** ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command displays LDP LSP information for the specified VPN instance. If you do not specify a VPN instance, this command displays LDP LSP information for the public network.

*ipv4-address mask-length*: Specifies an IPv4 FEC by an IPv4 address and a mask length in the range of 0 to 32.

*ipv6-address prefix-length*: Specifies an IPv6 FEC by an IPv6 address and a mask length in the range of 0 to 128.

**ipv6**: Displays information about LDP LSPs for IPv6 FECs.

### Usage guidelines

If you do not specify the *ipv4-address mask-length* argument, the *ipv6-address prefix-length* argument, and the **ipv6** keyword, this command displays information about LDP LSPs for all IPv4 FECs.

### Examples

# Display LDP LSP information for IPv4 FECs on the public network.

```
<Sysname> display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup, N/A – unavailable
FECs: 4           Ingress: 1          Transit: 1      Egress: 3
```

```
FEC                 In/Out Label        Nexthop         OutInterface
1.1.1.1/32          -/3                 10.1.1.1        Vlan10
                    1151/3              10.1.1.1        Vlan10
                    -/1025(B)           30.1.1.1        Vlan20
                    1151/1025(B)        30.1.1.1        Vlan20
2.2.2.2/32          3/-
                    -/1151(L)
10.1.1.0/24         1149/-
                    -/1149(L)
192.168.1.0/24      1150/-
                    -/1150(L)
```

# Display LDP LSP information for IPv6 FECs on the public network.

```
<Sysname> display mpls ldp lsp ipv6
Status Flags: * - stale, L - liberal, B - backup, N/A – unavailable
FECs: 2             Ingress: 1          Transit: 1      Egress: 1

FEC: 2080::29FF:FEED:9E60:876A:130B/128
In/Out Label: -/3                                OutInterface : Vlan10
Nexthop     : FE80:12F:C0::130B
In/Out Label: 1151/3                             OutInterface : Vlan10
Nexthop     : FE80:12F:C0::130B
In/Out Label: -/1026(L)                          OutInterface : -
Nexthop     : -

FEC: 2001::1/128
In/Out Label: 3/-                               OutInterface : -
Nexthop     : -
```

**Table 7 Command output**

| Field | Description |
|---|---|
| Status Flags | LSP status:<br>• *****—Stale, indicating that the LSP is under a GR process.<br>• **L**—Liberal, indicating that the LSP is not activated because the peer that advertised the label is not the next hop of the route.<br>• **B**—Backup, indicating a backup LSP.<br>• **N/A**—Unavailable, indicating that the LSP is not the optimal LSP for traffic forwarding. |
| FECs | Total number of FECs. |
| Ingress | Number of LSPs that take the local device as the ingress node. |
| Transit | Number of LSPs that take the local device as a transit node. |
| Egress | Number of LSPs that take the local device as the egress node. |
| FEC | Forwarding equivalence class identified by an IP prefix. |
| In/Out Label | Incoming/outgoing label. |
| Nexthop | Next hop address for the FEC. |
| OutInterface | Outgoing interface for the FEC. |

### Related commands

**display mpls lsp**

# display mpls ldp parameter

Use **display mpls ldp parameter** to display LDP running parameters.

### Syntax

**display mpls ldp parameter** [ **vpn-instance** *vpn-instance-name* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command displays LDP running parameters for the specified VPN instance. If you do not specify a VPN instance, this command displays LDP running parameters for the public network.

### Usage guidelines

This command displays the following LDP running parameters:

- Global parameters, which are applicable to all LDP networks.
- Instance parameters, which are applicable to a specific LDP network.

### Examples

# Display LDP running parameters for the public network.

```
<Sysname> display mpls ldp parameter
 Global Parameters:
   Protocol Version    : V1         IGP Sync Delay on Restart : 90 sec
   Nonstop Routing     : Off        Nonstop Routing State     : Not Ready
   Graceful Restart    : Off        Forwarding State Hold Time: 360 sec
   Reconnect Time      : 120 sec    DSCP Value                : 48
 Instance Parameters:
   Instance ID         : 0
   LSR ID              : 0.0.0.0
   Loop Detection      : Off
   Hop Count Limit     : 32         Path Vector Limit              : 32
   Label Retention Mode: Liberal    Label Distribution Control Mode: Ordered
   IGP Sync Delay      : 0 sec
```

**Table 8 Command output**

| Field | Description |
|---|---|
| Global Parameters | LDP running parameters for all LDP-enabled networks. |
| Protocol Version | LDP protocol version. |

| Field | Description |
|---|---|
| IGP Sync Delay on Restart | Maximum delay time (in seconds) that LDP must wait before it notifies IGP of an LDP session-up event when there is an LDP restart. |
| Nonstop Routing | Whether the nonstop routing feature is enabled:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| Nonstop Routing State | LDP NSR state:<br>• **Ready**—NSR is enabled, and LDP session and LSP information has been synchronized to the standby process. If an active/standby switchover occurs, the LDP session stays in Operational state, and the forwarding is not interrupted.<br>• **Not Ready**—NSR is not enabled, or NSR is enabled but LDP session and LSP information synchronization to the standby process is not completed. If an active/standby switchover occurs, the LDP session might not be able to stay in Operational state, and the forwarding might be interrupted. |
| Graceful Restart | Whether the GR feature is enabled:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| Forwarding State Hold Time | MPLS Forwarding State Holding time in seconds. |
| Reconnect Time | Reconnect time in seconds. |
| DSCP Value | DSCP value for outgoing LDP packets. |
| Instance Parameters | LDP running parameters for a VPN instance or public network. |
| Instance ID | VPN instance ID. For the public network, this field displays **0**. |
| LSR ID | LSR ID of the local device. |
| Loop Detection | Whether loop detection is enabled:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| Hop Count Limit | Hop count limit specified for loop detection. |
| Path Vector Limit | Path Vector length limit specified for loop detection. |
| Label Retention Mode | The device supports only the Liberal mode. |
| Label Distribution Control Mode | Label distribution control mode: **Ordered** or **Independent**. |
| IGP Sync Delay | Delay time (in seconds) that LDP must wait before it notifies IGP of an LDP session-up event. |

# display mpls ldp peer

Use **display mpls ldp peer** to display LDP peer and session information.

## Syntax

**display mpls ldp peer** [ **vpn-instance** *vpn-instance-name* ] [ *peer-lsr-id* ] [ **verbose** ]

## Views

Any view

### Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command displays LDP peer and session information for the specified VPN instance. If you do not specify a VPN instance, this command displays LDP peer and session information for the public network.

**peer** *peer-lsr-id*: Specifies an LDP peer by its LSR ID. If you do not specify this option, the command displays all LDP peers and related session information.

**verbose**: Displays detailed LDP peer and session information. If you do not specify this keyword, the command displays brief LDP peer and session information.

### Examples

# Display brief information about all LDP peers and LDP sessions for the public network.

```
<Sysname> display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  39/39
```

**Table 9 Command output**

| Field | Description |
|---|---|
| Peer LDP ID | LDP identifier of the peer. |
| State | State of the LDP session between the local LSR and the peer:<br>• **Non Existent**—No TCP connection is established.<br>• **Initialized**—A TCP connection has been established.<br>• **OpenRecv**—LDP has received an acceptable initialization message.<br>• **OpenSent**—LDP has sent an initialization message.<br>• **Operational**—An LDP session has been established. |
| Role | Role of the local LSR in the session: **Active** or **Passive**.<br>In a session, the LSR with a higher IP address takes the Active role. The Active LSR initiates a TCP connection to the passive LSR. |
| GR | Whether GR is enabled on the peer:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| MD5 | Whether MD5 authentication is enabled for the LDP session on the local device:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| KA Sent/Rcvd | Number of keepalive messages sent/received. |

# Display detailed information about all LDP peers and LDP sessions for the public network.

```
<Sysname> display mpls ldp peer verbose
 Peer LDP ID      : 100.100.100.20:0
 Local LDP ID     : 100.100.100.17:0
 TCP Connection   : 100.100.100.20:47515 -> 100.100.100.17:646
```

```
Session State    : Operational        Session Role     : Passive
Session Up Time  : 0000:00:03 (DD:HH:MM)
Max PDU Length   : 4096 bytes (Local: 4096 bytes, Peer: 4096 bytes)
Keepalive Time     : 45 sec (Local: 45 sec, Peer: 45 sec)
Keepalive Interval : 15 sec
Msgs Sent/Rcvd   : 288/426
KA Sent/Rcvd     : 13/13
Label Adv Mode   : DU                 Graceful Restart : On
Reconnect Time   : 120 sec            Recovery Time    : 360 sec
Loop Detection   : On                 Path Vector Limit: 32
Discovery Sources:
  Targeted Hello 100.100.100.17 -> 100.100.100.20 (Active, Passive)
    Hello Hold Time: 45 sec           Hello Interval   : 15000 ms
  Targeted Hello 2005:130F::09C0:876A:130B ->
                 2001:0000:130F:0000:0000:09C0:876A:130B (Active, Passive)
    Hello Hold Time: 45 sec           Hello Interval   : 15000 ms
  Vlan-interface10
    Hello Hold Time: 15 sec           Hello Interval   : 5000 ms
  Vlan-interface10 (v6)
    Hello Hold Time: 15 sec           Hello Interval   : 5000 ms
Label Acceptance Policy :
  prefix-from-20
  prefix-from-30(v6)
Session Protection      : On
  State            : Ready            Duration         : 120 sec
Addresses received from peer:
  202.118.224.20   100.100.100.20   11.22.33.44      1.2.3.10
  1.2.3.4
  2005:130F::09C0:876A:130B
```

**Table 10 Command output**

| Field | Description |
|---|---|
| Peer LDP ID | LDP identifier of the peer. |
| Local LDP ID | LDP identifier of the local LSR. |
| TCP connection | TCP connection information for the session. It includes the IP addresses and port numbers used by both ends of the TCP connection, and whether MD5 authentication is enabled for the TCP connection. If MD5 authentication is enabled, this field displays **MD5 On**. If MD5 is not enabled, this field does not display MD5 information. |
| Session State | State of the LDP session:<br>• **Non Existent**—No TCP connection is established.<br>• **Initialized**—A TCP connection has been established.<br>• **OpenRecv**—LDP has received an acceptable initialization message.<br>• **OpenSent**—LDP has sent an initialization message.<br>• **Operational**—An LDP session has been established. |
| Session Role | Role the local LSR in the session: **Active** or **Passive**. |
| Session Up time | Duration of the session in Operational state. |

| Field | Description |
| --- | --- |
| Max PDU Length | Maximum PDU length negotiated, in bytes.<br>• **Local**—Maximum PDU length (in bytes) on the local LSR.<br>• **Peer**—Maximum PDU length (in bytes) on the peer. |
| Keepalive Time | Keepalive time negotiated, in seconds.<br>• **Local**—Locally configured Keepalive holding time in seconds.<br>• **Peer**—Keepalive holding time (in seconds) configured on the peer. |
| Keepalive Interval | Keepalive interval in seconds. |
| Msgs Sent/Rcvd | Total number of LDP messages sent and received. |
| KA Sent/Rcvd | Total number of Keepalive messages sent and received. |
| Label Adv Mode | Label advertisement mode negotiated. The device only supports the DU mode. |
| Graceful Restart | Whether GR is enabled on the peer:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| Reconnect Time | Reconnect time negotiated, in seconds. |
| Recovery Time | Recovery time (in seconds) carried in packets sent by the peer. |
| Loop Detection | Whether loop detection is enabled on the peer:<br>• **On**—Enabled.<br>• **Off**—Disabled. |
| Path Vector Limit | Maximum Path Vector length configured on the peer. |
| Discovery Sources | Discovery source of the LDP peer. |
| Targeted Hello | LDP peer discovered by the extended discovery mechanism.<br>• The address before **->** (100.100.100.17 in this example) is the local IP address.<br>• The address after **->** (100.100.100.20 in this example) is the peer IP address.<br>• **(Active)** indicates that the local LSR is the active end. It actively sends Targeted Hellos to its peer.<br>• **(Passive)** indicates that the local LSR is the passive end. It passively responds to the Targeted Hellos from its peer.<br>• **(Active, Passive)** indicates that the local LSR acts as both the active end and the passive end. |
| Vlan-interface10 | Interface running LDP basic discovery. The device discovers the LDP peer by sending Link Hellos out of the interface.<br>**(v6)** indicates that the LDP peer is discovered by sending IPv6 Link Hellos. |
| Hello Hold Time | Hello hold time negotiated, in seconds. |
| Hello Interval | Current Hello interval, in milliseconds. |
| Label Acceptance Policy | Label acceptance policy used to filter label mappings received from the peer.<br>**(v6)** indicates that the label acceptance policy uses IPv6 prefixes to filter label mappings. |
| Session Protection | Whether session protection is enabled:<br>• **On**—Enabled.<br>• **Off**—Disabled. |

| Field | Description |
| --- | --- |
| State | Session protection state:<br>• **Incomplete**—Session protection is not ready.<br>• **Ready**—Session protection is ready.<br>• **Protecting**—The session is under protection. |
| Duration | Local session protection duration, in seconds.<br>**Infinite** indicates that session protection takes effect permanently. |
| Holdup time remaining | Remaining time of the session hold timer, in seconds.<br>This field is displayed only when the session protection state is **Protecting**. A value of **Infinite** indicates that session protection takes effect permanently. |
| Addresses received from peer | IP addresses received from the peer. |

# display mpls ldp summary

Use **display mpls ldp summary** to display LDP summary information.

## Syntax

**display mpls ldp summary** [ **all** | **vpn-instance** *vpn-instance-name* ]

## Views

Any view

## Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

## Parameters

**all**: Displays LDP summary information for the public network and all VPN instances.

**vpn-instance** *vpn-instance-name*: Displays LDP summary information for the specified VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

## Usage guidelines

If you do not specify any parameters, this command displays LDP summary information for the public network.

## Examples

# Display LDP summary information for the public network.

```
<Sysname> display mpls ldp summary
VPN Instance Name    : Public
  Instance ID        : 0
  Instance State     : Active
  Interfaces         : 1 (1 active)
  Targeted Peers     : 0
  Targeted Peers(v6) : 0
  Adjacencies        : 1
```

```
Adjacencies(v6)    : 1
Peers              : 1
  Operational : 1 (0 GR)
  OpenSent    : 0
  OpenRecv    : 0
  Initialized : 0
  Non-Existent: 0
```

**Table 11 Command output**

| Field | Description |
|---|---|
| Instance ID | VPN instance identifier. A value of 0 represents the public network. |
| Instance State | LDP status in the VPN instance: **Active** or **Inactive**. |
| Interfaces | Number of interfaces enabled with LDP.<br>**active**: Number of interfaces running LDP. |
| Targeted Peers | Number of LDP IPv4 peers discovered by the LDP extended discovery mechanism, including the manually specified peers and the automatically established peers. |
| Targeted Peers(v6) | Number of LDP IPv6 peers discovered by the LDP extended discovery mechanism, including the manually specified peers and the automatically established peers. |
| Adjacencies | Number of IPv4 Hello adjacencies. |
| Adjacencies(v6) | Number of IPv6 Hello adjacencies. |
| Peers | Total number of peers. |
| Operational | Number of peers in Operational state.<br>GR: Number of GR-capable peers. |
| OpenSent | Number of peers in OpenSent state. |
| OpenRecv | Number of peers in OpenRecv state. |
| Initialized | Number of peers in Initialized state. |
| Non-Existent | Number of peers in Non-Existent state. |

# dscp

Use **dscp** to set a DSCP value for outgoing LDP packets.

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

## Syntax

**dscp** *dscp-value*

**undo dscp**

## Default

The DSCP value for outgoing LDP packets is 48.

## Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*dscp-value*: Specifies the DSCP value for outgoing LDP packets, in the range of 0 to 63.

### Usage guidelines

To control the transmission preference of outgoing LDP packets, set a DSCP value for outgoing LDP packets.

### Examples

# Set the DSCP value for outgoing LDP packets to 56.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] dscp 56
```

### Related commands

**display mpls ldp parameter**

## graceful-restart

Use **graceful-restart** to enable Graceful Restart (GR) for LDP.

Use **undo graceful-restart** to disable LDP GR.

### Syntax

**graceful-restart**

**undo graceful-restart**

### Default

LDP GR is disabled.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

LDP GR enables an LSR to retain MPLS forwarding entries during an LDP restart, ensuring continuous MPLS forwarding.

The configuration of this command takes effect only on new LDP sessions. To apply the configuration to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Enable GR for LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] graceful-restart
```

### Related commands

**display mpls ldp parameter**

**reset mpls ldp**

# graceful-restart timer

Use **graceful-restart timer** to set the MPLS Forwarding State Holding timer and the Reconnect timer for GR.

Use **undo graceful-restart timer** to restore the default.

### Syntax

**graceful-restart timer** { **forwarding-hold** *hold-time* | **reconnect** *reconnect-time* }

**undo graceful-restart timer** { **forwarding-hold** | **reconnect** }

### Default

The MPLS Forwarding State Holding timer is 180 seconds and the Reconnect timer is 120 seconds.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**forwarding-hold** *hold-time*: Specifies the MPLS Forwarding State Holding time in the range of 60 to 6000 seconds. This time specifies how long the local LSR retains its MPLS forwarding entries after the control plane of the local LSR restarts.

**reconnect** *reconnect-time*: Specifies the Reconnect time in the range of 60 to 300 seconds. This time specifies the period the local LSR expects the peer to wait for LDP session re-establishment after the peer detects an LDP session failure. The local LSR sends the Reconnect time to the peer.

### Usage guidelines

The MPLS Forwarding State Holding time must be greater than the Reconnect time.

The configuration of this command takes effect only on new LDP sessions. To apply the configuration to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Set the MPLS Forwarding State Holding time to 200 seconds, and the Reconnect time to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] graceful-restart timer forwarding-hold 200
[Sysname-ldp] graceful-restart timer reconnect 100
```

### Related commands

**display mpls ldp parameter**

**graceful-restart**

# label-distribution

Use **label-distribution** to configure the label distribution control mode.

Use **undo label-distribution** to restore the default.

### Syntax

**label-distribution** { **independent** | **ordered** }

**undo label-distribution**

### Default

The label distribution control mode is **ordered**.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**independent**: Specifies Independent label distribution mode. In this mode, an LSR can distribute label mappings to the upstream LSR at any time.

**ordered**: Specifies Ordered label distribution mode. In this mode, an LSR distributes a label mapping for an FEC to the upstream LSR only when one of the following events occurs:

- The LSR receives a label mapping for that FEC from the downstream LSR.
- The LSR is the egress node of that FEC.

### Usage guidelines

In Ordered mode, an LSR can determine that the downstream LSR has established an LSP when the LSR receives an FEC-label mapping from the downstream LSR.

The Independent mode enables faster LSP convergence because each LSR independently advertises labels without waiting for labels from downstream LSRs.

### Examples

# Set the Independent LDP label distribution mode for the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] label-distribution independent
```

### Related commands

**display mpls ldp parameter**

# loop-detect

Use **loop-detect** to enable loop detection.

Use **undo loop-detect** to disable loop detection.

### Syntax

**loop-detect**

**undo loop-detect**

### Default

Loop detection is disabled.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

The LDP loop detection feature enables LDP to detect loops during an LSP establishment. If LDP detects a loop, it terminates the LSP establishment. This feature is applicable to an MPLS network where most of the devices do not support the TTL mechanism, such as ATM switches.

LDP uses hop count (see "maxhops") and path vector (see "pv-limit") for loop detection.

To use this feature, you must enable it on all LSRs that the LSP passes through.

To avoid extra LDP overhead, do not use this feature if most of the devices in an MPLS network support the TTL mechanism. Using the TTL mechanism can prevent endless routing loops.

The configuration of this command takes effect only on new LDP sessions. To apply the configuration to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Enable LDP loop detection for the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] loop-detect
```

### Related commands

**display mpls ldp parameter**

**maxhops**

**pv-limit**

## lsr-id

Use **lsr-id** to configure an LDP LSR ID.

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

### Syntax

**lsr-id** *lsr-id*

**undo lsr-id**

### Default

No LDP LSR ID is configured. LDP uses the MPLS LSR ID configured by the **mpls lsr-id** command for both the public network and VPN instances.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*lsr-id*: Specifies an LDP LSR ID, in dotted decimal notation.

### Usage guidelines

If you configure an LDP LSR ID by using the **lsr-id** command in LDP view or LDP-VPN instance view, LDP uses the LDP LSR ID. If no LDP LSR ID is configured, LDP uses the LSR ID configured by the **mpls lsr-id** command.

LDP uses the same LSR ID for all sessions in the same VPN instance. After you configure a new LSR ID for a VPN instance, LDP does not use the new LSR ID unless the **reset mpls ldp** command is executed. The **reset mpls ldp** command re-establishes all LDP sessions in the VPN instance.

As a best practice, use the default LDP LSR ID configured by the **mpls lsr-id** command for the public network. If the **lsr-id** command is required to configure an LDP LSR ID for the public network, specify the IP address of a local loopback interface as the LDP LSR ID.

### Examples

# Configure the LDP LSR ID as 2.2.2.2 for the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] lsr-id 2.2.2.2
```

### Related commands

**display mpls ldp parameter**

**mpls lsr-id**

# maxhops

Use **maxhops** to set the maximum hop count for loop detection.

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

### Syntax

**maxhops** *hop-number*

**undo maxhops**

### Default

The maximum hop count for loop detection is 32.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*hop-number*: Specifies the maximum hop count for loop detection, in the range of 1 to 32.

### Usage guidelines

LDP adds a hop count in a label request or label mapping message. The hop count increments by 1 on each LSR. When the hop count reaches the maximum hop count configured by this command, LDP considers that a loop occurs and terminates LSP establishment.

Set a proper maximum hop count according to the number of LSRs in your network. For example, set a smaller maximum hop count in small networks to allow for fast loop detection. Set a higher maximum hop count in large networks to ensure that LSPs can be successfully established.

The configuration of this command takes effect only on new LDP sessions. To apply the configuration to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Set the maximum hop count to 25 for loop detection on the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] maxhops 25
```

### Related commands

**display mpls ldp parameter**

**loop-detect**

**pv-limit**

## md5-authentication

Use **md5-authentication** to enable LDP MD5 authentication.

Use **undo md5-authentication** to disable LDP MD5 authentication.

### Syntax

**md5-authentication** *peer-lsr-id* { **cipher** | **plain** } *string*

**undo md5-authentication** *peer-lsr-id*

### Default

LDP MD5 authentication is disabled.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*peer-lsr-id*: Specifies the LSR ID of a peer.

**cipher**: Specifies a key in encrypted form.

**plain**: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

*string*: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters.

### Usage guidelines

To improve security for LDP sessions, you can configure MD5 authentication for the underlying TCP connections to check the integrity of LDP messages.

For the local LSR and the peer LSR to establish a TCP connection, they must have the same key.

MD5 authentication key settings take effect only on new LDP sessions. To apply the new settings to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Enable LDP MD5 authentication for peer 3.3.3.3 on the public network, and set a key of **pass** in plaintext form.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] md5-authentication 3.3.3.3 plain pass
```

### Related commands

**display mpls ldp peer**

## mpls ldp

Use **mpls ldp** to enable LDP globally for an LSR and enter LDP view.

Use **undo mpls ldp** to disable LDP globally for an LSR and delete all LDP-VPN instances.

### Syntax

**mpls ldp**

**undo mpls ldp**

### Default

LDP is globally disabled.

### Views

System view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

You must enable LDP globally for an LSR to run LDP.

The NSR ,and GR commands, the **session protection** command, and the **targeted-peer** command are available only in LDP view. All other commands available in LDP view are also available in LDP-VPN instance view.

Commands executed in LDP view take effect only on the public network. Commands executed in LDP-VPN instance view take effect only on the specified VPN instance. The NSR and GR commands are global commands and take effect on all VPN instances and the public network.

### Examples

# Enable LDP globally and enter LDP view.

```
<Sysname> System-view
[Sysname] mpls ldp
```

```
[Sysname-ldp]
```

### Related commands

**mpls ldp enable**

**vpn-instance**

# mpls ldp timer

Use **mpls ldp timer** to set the Hello hold time, Hello interval, Keepalive hold time, and Keepalive interval.

Use **undo mpls ldp timer** to restore the default.

### Syntax

**mpls ldp timer** { **hello-hold** *timeout* | **hello-interval** *interval* | **keepalive-hold** *timeout* | **keepalive-interval** *interval* }

**undo mpls ldp timer** { **hello-hold** | **hello-interval** | **keepalive-hold** | **keepalive-interval** }

### Default

- The Link Hello hold time is 15 seconds.
- The Link Hello interval is 5 seconds.
- The Targeted Hello hold time is 45 seconds.
- The Targeted Hello interval is 15 seconds.
- The Keepalive hold time is 45 seconds.
- The Keepalive interval is 15 seconds.

### Views

Interface view

LDP peer view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**hello-hold** *timeout*: Specifies the Hello hold time in the range of 1 to 65535 seconds. LDP keeps the hello adjacency during the Hello hold time. The negotiated Hello hold time takes the smaller value of the local Hello hold time and the peer Hello hold time. If LDP receives no Hello message from the peer before the Hello hold timer expires, LDP deletes the Hello adjacency with the peer. If you set the Hello hold time to 65535, LDP permanently keeps the Hello adjacency.

**hello-interval** *interval*: Specifies the Hello interval in the range of 1 to 65535 seconds. LDP sends Hello messages at this interval.

**keepalive-hold** *timeout*: Specifies the Keepalive hold time in the range of 15 to 65535 seconds. LDP keeps the LDP session to the peer during the Keepalive hold time. The negotiated Keepalive hold time takes the smaller value of the local Keepalive hold time and the peer Keepalive hold time. If LDP receives no LDP message from the peer before the Keepalive hold timer expires, LDP deletes the LDP session to the peer.

**keepalive-interval** *interval*: Specifies the Keepalive interval in the range of 1 to 65535 seconds. LDP sends Keepalive messages to the peer at this interval.

### Usage guidelines

In interface view, this command sets a Link Hello hold time and a Link Hello interval.

In LDP peer view, this command sets a Targeted Hello hold time and a Targeted Hello interval.

LDP automatically sends Targeted Hellos to the specified peer after one of the following features is configured:

- LDP session protection.
- LDP over MPLS TE.
- MPLS L2VPN LDP PW.
- VPLS LDP PW.

To modify the Targeted Hello/Keepalive hold time and interval, you must use the **targeted-peer** command to create the LDP peer, and then perform the modification in the LDP peer view.

If the local Hello hold time and local Keepalive hold time are different from those of a peer LSR, the negotiation is as follows:

- During LDP peer discovery, an LSR compares the local Hello hold time with the peer LSR's Hello hold time carried in Hellos. Then, the LSR uses the smaller one as the negotiated Hello hold time.
  - If the negotiated Hello hold time is larger than three times the local Hello interval, the LSR sends Hello messages at the local Hello interval.
  - If it is not larger than three times the local Hello interval, the LSR sends Hello messages at an interval 1/3 of the negotiated Hello hold time.
- During LDP session negotiation, an LSR compares the local Keepalive hold time with the Keepalive hold time of the peer LSR by exchanging Initialization messages. Then, the LSR uses the smaller one as the negotiated Keepalive hold time.
  - If the negotiated Keepalive hold time is larger than three times the local Keepalive interval, the LSR sends Keepalive messages at the local Keepalive interval.
  - If it is not larger than three times the local Keepalive interval, the LSR sends Keepalive messages at an interval 1/3 of the negotiated Keepalive hold time.

If the Hello hold time and the Keepalive hold time values are too large, LDP cannot quickly detect link failures. If the values are too small, LDP might mistakenly consider a normal link failed. As a best practice, use the default values.

Make sure all links between two LSRs have the same Keepalive hold time as the one configured in LDP peer view in either of the following situations:

- Multiple Link Hello adjacencies exist when the two LSRs are directly connected through multiple links.
- Both a Link Hello adjacency and a Targeted Hello adjacency exist between the two LSRs.

Keepalive hold time and keepalive interval settings take effect only on new LDP sessions. To apply the settings to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Set the Targeted Hello hold time to 1000 seconds, Targeted Hello interval to 50 seconds, Keepalive hold time to 1000 seconds, and Keepalive interval to 50 seconds for peer 3.3.3.3.

```
<Sysname> System-view
[Sysname] mpls ldp
[Sysname-ldp] targeted-peer 3.3.3.3
[Sysname-ldp-peer-3.3.3.3] mpls ldp timer hello-hold 1000
[Sysname-ldp-peer-3.3.3.3] mpls ldp timer hello-interval 50
[Sysname-ldp-peer-3.3.3.3] mpls ldp timer keepalive-hold 1000
```

```
[Sysname-ldp-peer-3.3.3.3] mpls ldp timer keepalive-interval 50
```

# On VLAN-interface 2, set the Link Hello hold time to 100 seconds, Link Hello interval to 20 seconds, Keepalive hold time to 50 seconds, and Keepalive interval to 10 seconds.

```
<Sysname> System-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] mpls ldp timer hello-hold 100
[Sysname-Vlan-interface2] mpls ldp timer hello-interval 20
[Sysname-Vlan-interface2] mpls ldp timer keepalive-hold 50
[Sysname-Vlan-interface2] mpls ldp timer keepalive-interval 10
```

### Related commands

**display mpls ldp discovery**

**display mpls ldp peer**

## non-stop-routing

Use **non-stop-routing** to enable LDP NSR.

Use **undo non-stop-routing** to disable LDP NSR.

### Syntax

**non-stop-routing**

**undo non-stop-routing**

### Default

LDP NSR is disabled.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Examples

# Enable LDP NSR.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] non-stop-routing
```

### Related commands

**display mpls ldp discovery**

**display mpls ldp fec**

**display mpls ldp peer**

**display mpls ldp summary**

## pv-limit

Use **pv-limit** to set the path vector limit.

Use **undo pv-limit** to restore the default.

### Syntax

**pv-limit** *pv-number*

**undo pv-limit**

### Default

The path vector limit is 32.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*pv-number*: Specifies the path vector limit in the range of 1 to 32.

### Usage guidelines

LDP adds LSR ID information in a label request or label mapping message. Each LSR checks whether its LSR ID is contained in the message.

- If it is not, the LSR adds its own LSR ID into the message.
- If it is, the LSR considers that a loop occurs and terminates LSP establishment.

In addition, when the number of LSR IDs in the message reaches the path vector limit, LDP also considers that a loop occurs and terminates LSP establishment.

The configuration of this command takes effect only on new LDP sessions. To apply the configuration to existing LDP sessions, you must reset the LDP sessions by using the **reset mpls ldp** command.

### Examples

# Set the path vector limit to 3 for LDP loop detection on the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] pv-limit 3
```

### Related commands

**display mpls ldp parameter**

**loop-detect**

**maxhops**

# reset mpls ldp

Use **reset mpls ldp** to reset LDP sessions.

### Syntax

**reset mpls ldp** [ **vpn-instance** *vpn-instance-name* ] [ **peer** *peer-id* ]

### Views

User view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. This command resets the LDP sessions in the specified VPN instance. If you do not specify a VPN instance, this command resets the LDP sessions in the public network.

**peer** *peer-id*: Specifies a peer by its LSR ID. If you do not specify a peer, this command resets all LDP sessions in the specified VPN instance or the public network.

### Usage guidelines

Resetting an LDP session deletes and re-establishes the session and all LSPs based on the session.

Changes to LDP session parameters take effect only on new LDP sessions. To apply the changes to an existing LDP session on a network, you must reset all LDP sessions on that network by executing this command without the **peer** keyword. If you specify the **peer** keyword, this command resets the LDP session to the specified peer without applying the parameter changes to the session.

### Examples

# Reset all LDP sessions in the public network.

```
<Sysname> reset mpls ldp
```

# Reset all LDP sessions in VPN instance **vpn1**.

```
<Sysname> reset mpls ldp vpn-instance vpn1
```

# snmp-agent trap enable ldp

Use **snmp-agent trap enable ldp** to enable SNMP notifications for LDP.

Use **undo snmp-agent trap enable ldp** to disable SNMP notifications for LDP.

### Syntax

**snmp-agent trap enable ldp**

**undo snmp-agent trap enable ldp**

### Default

SNMP notifications for LDP are enabled.

### Views

System view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

This command enables generating SNMP notifications for LDP upon LDP session changes, as defined in RFC 3815. For LDP 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.

### Examples

# Enable SNMP notifications for LDP.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ldp
```

## vpn-instance

Use **vpn-instance** to enable LDP for a VPN instance and enter LDP-VPN instance view, or enter the view of an existing LDP-VPN instance.

Use **undo vpn-instance** to delete the LDP-VPN instance.

### Syntax

**vpn-instance** *vpn-instance-name*

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

### Default

LDP is disabled for a VPN instance.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The VPN instance must have been created by the **ip vpn-instance** command in system view.

### Usage guidelines

Enabling LDP for VPN instances is used for the Carrier's Carrier network that uses LDP between the Level 1 carrier and Level 2 carrier PEs. In such a network, you must enable LDP for each VPN instance on each Level 1 carrier PE.

The GR, NSR, and LDP-IGP synchronization commands, the **dscp** command, the **session protection** command, and the **targeted-peer** command are available only in LDP view. All other commands available in LDP view are available in LDP-VPN instance view.

Commands executed in LDP view take effect only on the public network. Commands executed in LDP-VPN instance view take effect only on the specified VPN instance. The **dscp** command, NSR commands, and GR commands are global commands and take effect on all VPN instances and the public network.

### Examples

# Enable LDP for VPN instance **vpn1** and enter LDP-VPN instance view.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] vpn-instance vpn1
[Sysname-ldp-vpn-instance-vpn1]
```

### Related commands

**ip vpn-instance**

**mpls ldp**

# IPv4 LDP commands

## accept-label

Use **accept-label** to configure a label acceptance policy.

Use **undo accept-label** to delete a label acceptance policy.

### Syntax

**accept-label peer** *peer-lsr-id* **prefix-list** *prefix-list-name*

**undo accept-label peer** *peer-lsr-id*

### Default

No label acceptance policy is configured. LDP accepts all IPv4 FEC-label mappings from all peers.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**peer** *peer-lsr-id*: Specifies an LDP peer by its LSR ID.

**prefix-list** *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters.

### Usage guidelines

This feature enables you to control the number of FEC-label mappings received from peers. LDP accepts only the FEC-label mappings whose IPv4 prefixes are permitted by the specified IPv4 prefix list from the specified peer.

To accept the previously denied label mappings from a peer, use the **undo accept-label** command or change the IPv4 prefix list for the peer. Then, execute the **reset mpls ldp** command to reset the LDP session to that peer to apply the new settings.

Using a label advertisement policy on an LSR or using a label acceptance policy on its upstream LSR can achieve the same purpose. As a best practice, use the label advertisement policy to reduce network load.

### Examples

# Configure a label acceptance policy to accept only the FEC-label mappings containing IPv4 prefixes 10.1.1.0/24 and 10.2.1.0/24 from LDP peer 1.1.1.9.

```
<Sysname> system-view
[Sysname] ip prefix-list prefix-from-RTA index 1 permit 10.1.1.0 24
[Sysname] ip prefix-list prefix-from-RTA index 2 permit 10.2.1.0 24
[Sysname] mpls ldp
[Sysname-ldp] accept-label peer 1.1.1.9 prefix-list prefix-from-RTA
```

### Related commands

**display mpls ldp peer verbose**

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

# advertise-label

Use **advertise-label** to configure a label advertisement policy.

Use **undo advertise-label** to delete a label advertisement policy.

## Syntax

**advertise-label prefix-list** *prefix-list-name* [ **peer** *peer-prefix-list-name* ]

**undo advertise-label prefix-list** *prefix-list-name*

## Default

No label advertisement policy is configured. The device advertises IPv4 FEC-label mappings permitted by the LSP generation policy to all peers.

## Views

LDP view

LDP-VPN instance view

## Predefined user roles

network-admin

mdc-admin

## Parameters

**prefix-list** *prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters. This prefix list filters advertised label mappings.

**peer** *peer-prefix-list-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters. This prefix list filters LDP peers. If you do not specify this option, the device advertises label mappings to all peers.

## Usage guidelines

Use a label advertisement policy to filter label mappings advertised to peers.

Configure multiple label advertisement policies by executing this command multiple times.

If a label mapping is permitted by an advertisement policy, LDP advertises the mapping by following these rules:

- If the policy has no peer IPv4 prefix list (**peer** *peer-prefix-list-name* not specified), LDP advertises the label mapping to all peers.
- If the policy has a peer IPv4 prefix list, LDP advertises the label mapping to the peers permitted by the peer IPv4 prefix list.

If a label mapping is permitted by multiple advertisement policies, LDP advertises the label mapping according to the first configured policy.

Using a label advertisement policy on an LSR or using a label acceptance policy on its upstream LSR can achieve the same purpose. As a best practice, use the label advertisement policy to reduce network load.

## Examples

# Configure two label advertisement policies. One policy advertises only the label mapping for subnet 10.1.1.0/24 to peer 3.3.3.9. The other policy advertises only the label mapping for subnet 10.2.1.0/24 to peer 4.4.4.9.

```
<Sysname> system-view
[Sysname] ip prefix-list prefix-to-C permit 10.1.1.0 24
[Sysname] ip prefix-list prefix-to-D permit 10.2.1.0 24
```

```
[Sysname] ip prefix-list peer-C permit 3.3.3.9 32
[Sysname] ip prefix-list peer-D permit 4.4.4.9 32
[Sysname] mpls ldp
[Sysname-ldp] advertise-label prefix-list prefix-to-C peer peer-C
[Sysname-ldp] advertise-label prefix-list prefix-to-D peer peer-D
```

### Related commands

**display mpls ldp fec**

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

**lsp-trigger**

# display mpls ldp igp sync

Use **display mpls ldp igp sync** to display LDP-IGP synchronization information.

### Syntax

**display mpls ldp igp sync** [ **interface** *interface-type interface-number* ]

### Views

Any view

### Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

### Parameters

**interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays LDP-IGP synchronization information for all interfaces.

### Examples

# Display LDP-IGP synchronization information for all interfaces.

```
<Sysname> display mpls ldp igp sync
Vlan-interface10:
  IGP protocols: OSPF
  Sync status: Ready
  Peers:
    10.1.1.2:0

Vlan-interface20:
  IGP protocols: OSPF, IS-IS
  Sync status: Delayed (24 sec remaining)
  Peers:
    20.1.1.2:0

Vlan-interface30:
  LDP-IGP synchronization is disabled on the interface
```

**Table 12 Command output**

| Field | Description |
|---|---|
| IGP protocols | IGP protocols that require LDP-IGP synchronization: OSPF and IS-IS. |
| Sync status | LDP-IGP synchronization state:<br>• **Ready**—LDP is converged and is available for IGP.<br>• **Delayed**—LDP is waiting to notify IGP of the convergence. *remaining* indicates the remaining time for the delay, in seconds.<br>• **Not ready**—LDP is not converged and is not available for IGP.<br>• **LDP not enabled**—LDP is not enabled on the interface. |
| Peers | LDP peer that completes LDP convergence on the interface. |

# igp sync delay

Use **igp sync delay** to set the delay for LDP to notify IGP of the LDP convergence completion.

Use **undo igp sync delay** to restore the default.

## Syntax

**igp sync delay** *time*

**undo igp sync delay**

## Default

LDP immediately notifies IGP of the LDP convergence completion.

## Views

LDP view

## Predefined user roles

network-admin

mdc-admin

## Parameters

*time*: Specifies the notification delay in the range of 5 to 300 seconds.

## Usage guidelines

LDP convergence on a link is completed when the following conditions exist:

- The local device establishes an LDP session to a minimum of one peer, and the LDP session is already in **Operational** state.
- The local device has distributed the label mappings to a minimum of one peer.

If LDP notifies IGP immediately after convergence, MPLS traffic forwarding might be interrupted in one of the following scenarios:

- LDP peers use the **Ordered** label distribution control mode. When LDP notifies IGP of the LDP convergence, the device has not received a label mapping from downstream.
- A large number of label mappings are distributed from downstream. When LDP notifies IGP of the LDP convergence completion, label advertisement is not completed.

In these scenarios, you must use the **igp sync delay** command to configure the notification delay. When LDP convergence on a link is completed, LDP waits a delay time before notifying IGP of the LDP convergence completion to reduce traffic interruption.

### Examples

# Set a 30-second delay for LDP to notify IGP of the LDP convergence.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] igp sync delay 30
```

### Related commands

**igp sync delay on-restart**

**mpls ldp igp sync disable**

**mpls ldp sync** (IS-IS view)

**mpls ldp sync** (OSPF view/OSPF area view)

# igp sync delay on-restart

Use **igp sync delay on-restart** to set the maximum delay for LDP to notify IGP of the LDP-IGP synchronization status after an LDP restart or an active/standby switchover occurs.

Use **undo igp sync delay on-restart** to restore the default.

### Syntax

**igp sync delay on-restart** *time*

**undo igp sync delay on-restart**

### Default

The maximum notification delay is 90 seconds.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*time*: Specifies the maximum notification delay in the range of 60 to 600 seconds.

### Usage guidelines

When an LDP restart or an active/standby switchover occurs, LDP takes time to converge. LDP notifies IGP of the LDP-IGP synchronization status as follows:

- If a notification delay is not configured, LDP immediately notifies IGP of the current synchronization states during convergence, and then updates the states after LDP convergence. This could impact IGP processing.
- If a notification delay is configured, LDP notifies IGP of the synchronization states in bulk when one of the following events occurs:
  - LDP recovers to the state before the restart or switchover.
  - The maximum delay timer expires.

### Examples

# Set a 300-second maximum delay for LDP to notify IGP of the LDP-IGP synchronization status after an LDP restart or active/standby switchover occurs.

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

```
[Sysname] mpls ldp
[Sysname-ldp] igp sync delay on-restart 300
```

### Related commands

**igp sync delay**

**mpls ldp igp sync disable**

**mpls ldp sync** (IS-IS view)

**mpls ldp sync** (OSPF view/OSPF area view)

# import bgp

Use **import bgp** to enable LDP to redistribute BGP IPv4 unicast routes.

Use **undo import bgp** to disable LDP from redistributing BGP IPv4 unicast routes.

### Syntax

**import bgp** [ *as-number* ]

**undo import bgp**

### Default

LDP does not redistribute BGP IPv4 unicast routes.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*as-number*: Redistributes BGP IPv4 unicast routes in the specified AS. An AS number is in the range of 1 to 4294967295. If you do not specify an AS number, this command enables LDP to redistribute all BGP IPv4 unicast routes.

### Usage guidelines

**IMPORTANT:**

Use this command only if necessary. Execution of this command will increase the number of routes redistributed to LDP. A large number of redistributed routes will use a large amount of labels and memory.

By default, LDP automatically redistributes IPv4 IGP routes, including the BGP IPv4 unicast routes that have been redistributed into IGP. Then, LDP assigns labels to the IGP routes and labeled BGP routes if these routes are permitted by an LSP generation policy. LDP does not automatically redistribute BGP IPv4 unicast routes if the routes are not redistributed into the IGP.

For example, on a carrier's carrier network where IGP is not configured between a PE of a Level 1 carrier and a CE of a Level 2 carrier, LDP cannot redistribute BGP IPv4 unicast routes to assign labels to them. For this network to operate correctly, you can enable LDP to redistribute BGP IPv4 unicast routes. If the routes are permitted by an LSP generation policy, LDP assigns labels to them to establish LSPs. For more information about carrier's carrier, see *MPLS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

### Examples

# Enable LDP to redistribute BGP IPv4 unicast routes in AS 100 on the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] import bgp 100
```

### Related commands

**lsp-trigger**

# lsp-trigger

Use **lsp-trigger** to configure an LSP generation policy for IPv4 FECs.

Use **undo lsp-trigger** to restore the default.

### Syntax

**lsp-trigger** { **all** | **prefix-list** *prefix-list-name* }

**undo lsp-trigger**

### Default

LDP only uses redistributed IPv4 host routes with a 32-bit mask to generate LSPs.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**all**: Enables LDP to use all redistributed routes to generate LSPs.

**prefix-list** *prefix-name*: Specifies an IPv4 prefix list by its name, a case-sensitive string of 1 to 63 characters. LDP uses only the redistributed routes permitted by the IPv4 prefix list to generate LSPs.

### Usage guidelines

LDP assigns labels to the routes that have been redistributed into LDP to generate LSPs. An LSP generation policy specifies the routes that LDP uses to generate LSPs.

The default LSP generation policy depends on the label distribution control mode.

- In Ordered mode, LDP can only use the following routes to generate LSPs:
  - Loopback interface address routes with a 32-bit mask.
  - The routes with a 32-bit mask that match the FECs of label mappings received from downstream LSRs.
- In Independent mode, LDP can use all routes with a 32-bit mask to generate LSPs.

After you configure an LSP generation policy, LDP uses all redistributed routes or those permitted by the IPv4 prefix list to generate LSPs, regardless of the label distribution control mode.

As a best practice, use the default LSP generation policy.

### Examples

# Configure an LSP generation policy that enables LDP to use only redistributed routes 10.10.1.0/24 and 10.20.1.0/24 to establish LSPs for the public network.

```
<Sysname> system-view
[Sysname] ip prefix-list egress-fec-list index 1 permit 10.10.1.0 24
[Sysname] ip prefix-list egress-fec-list index 2 permit 10.20.1.0 24
[Sysname] mpls ldp
[Sysname-ldp] lsp-trigger prefix-list egress-fec-list
```

### Related commands

**`import bgp`**

**`ip prefix-list`** (*Layer 3—IP Services Command Reference*)

# mpls ldp enable

Use **`mpls ldp enable`** to enable IPv4 LDP on an interface.

Use **`undo mpls ldp enable`** to disable IPv4 LDP on an interface.

### Syntax

**`mpls ldp enable`**

**`undo mpls ldp enable`**

### Default

IPv4 LDP is disabled on an interface.

### Views

Interface view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

An up interface enabled with IPv4 LDP and MPLS sends IPv4 Link Hellos for neighbor discovery.

On an LDP over MPLS TE network, an up MPLS TE tunnel interface enabled with LDP sends Targeted Hellos to the tunnel destination. The interface establishes a session to the tunnel peer to set up an LDP LSP over the MPLS TE tunnel.

Before you enable IPv4 LDP on an interface, use the **`mpls ldp`** command in system view to enable LDP globally. If the interface is bound to a VPN instance, you must also use the **`vpn-instance`** command to enable LDP for the VPN instance.

Disabling LDP on an interface terminates all LDP sessions on the interface, and removes all LSPs established through the sessions.

An interface can be enabled with both IPv4 LDP and IPv6 LDP.

### Examples

# Enable IPv4 LDP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] quit
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] mpls ldp enable
```

**Related commands**

**display mpls ldp interface**

**mpls enable**

**mpls ldp**

**mpls ldp ipv6 enable**

# mpls ldp igp sync disable

Use **mpls ldp igp sync disable** to disable LDP-IGP synchronization on an interface.

Use **undo mpls ldp igp sync disable** to enable LDP-IGP synchronization on an interface.

**Syntax**

**mpls ldp igp sync disable**

**undo mpls ldp igp sync disable**

**Default**

LDP-IGP synchronization is enabled on an interface.

**Views**

Interface view

**Predefined user roles**

network-admin

mdc-admin

**Usage guidelines**

After you enable LDP-IGP synchronization for an OSPF area or an IS-IS process, LDP-IGP synchronization is enabled on the OSPF or IS-IS process interfaces by default. To disable LDP-IGP synchronization on an interface, execute the **mpls ldp igp sync disable** command on that interface.

**Examples**

# Disable LDP-IGP synchronization on VLAN-interface 2.

```
<Sysname> System-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] mpls ldp igp sync disable
```

**Related commands**

**mpls ldp sync** (IS-IS view)

**mpls ldp sync** (OSPF view/OSPF area view)

# mpls ldp sync (IS-IS view)

Use **mpls ldp sync** to enable LDP-ISIS synchronization.

Use **undo mpls ldp sync** to disable LDP-ISIS synchronization.

**Syntax**

**mpls ldp sync** [ **level-1** | **level-2** ]

**undo mpls ldp sync** [ **level-1** | **level-2** ]

### Default

LDP-ISIS synchronization is disabled.

### Views

IS-IS view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**level-1**: Specifies Level-1 of the IS-IS process.

**level-2**: Specifies Level-2 of the IS-IS process.

### Usage guidelines

LDP establishes LSPs based on the IGP optimal route. If LDP is not synchronized with IGP, MPLS traffic forwarding might be interrupted. The LDP-IGP synchronization feature is used to solve the synchronization problem.

After LDP-IGP synchronization is enabled, IGP advertises the actual cost of a link only when LDP convergence on the link is completed. Before LDP is converged, IGP advertises the maximum cost of the link. As a result, the link is visible on the IGP topology, but IGP does not select the link as the optimal route when other links are available. In this way, the device can avoid discarding MPLS packets due to lack of LDP LSP on the optimal route.

LDP-IGP synchronization is not supported for an IS-IS process that belongs to a VPN instance.

If you do not specify any keywords, this command enables LDP-ISIS synchronization for both Level-1 and Level-2.

If you execute this command multiple times, the most recent configuration takes effect. For example, if you execute the **mpls ldp sync level-1** command after you execute the **mpls ldp sync** command, LDP-ISIS synchronization is enabled for Level-1 but disabled for Level-2.

### Examples

# Enable LDP-ISIS synchronization for Level-2 of IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] mpls ldp sync level-2
```

### Related commands

**display mpls ldp igp sync**

**igp sync delay**

**igp sync delay on-restart**

**mpls ldp igp sync disable**

# mpls ldp sync (OSPF view/OSPF area view)

Use **mpls ldp sync** to enable LDP-OSPF synchronization.

Use **undo mpls ldp sync** to disable LDP-OSPF synchronization.

### Syntax

**mpls ldp sync**

**undo mpls ldp sync**

### Default

LDP-OSPF synchronization is disabled.

### Views

OSPF view

OSPF area view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

LDP establishes LSPs based on the IGP optimal route. If LDP is not synchronized with IGP, MPLS traffic forwarding might be interrupted. The LDP-IGP synchronization feature is used to solve the synchronization problem.

After LDP-IGP synchronization is enabled, IGP advertises the actual cost of a link only when LDP convergence on the link is completed. Before LDP is converged, IGP advertises the maximum cost of the link. As a result, the link is visible on the IGP topology, but IGP does not select the link as the optimal route when other links are available. In this way, the device can avoid discarding MPLS packets due to lack of LDP LSP on the optimal route.

LDP-IGP synchronization is not supported for an OSPF process and its OSPF areas if the OSPF process belongs to a VPN instance.

To enable LDP-OSPF synchronization for an OSPF area, use this command in OSPF area view. To enable LDP-OSPF synchronization for all areas of an OSPF process, use this command in OSPF view.

### Examples

# Enable LDP-OSPF synchronization for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] mpls ldp sync
```

### Related commands

**display mpls ldp igp sync**

**igp sync delay**

**igp sync delay on-restart**

**mpls ldp igp sync disable**

# mpls ldp transport-address

Use **mpls ldp transport-address** to specify the LDP IPv4 transport address.

Use **undo mpls ldp transport-address** to remove the configuration.

### Syntax

In interface view:

**mpls ldp transport-address** { *ipv4-address* | **interface** }

**undo mpls ldp transport-address** { *ipv4-address* | **interface** }

In LDP peer view:

**mpls ldp transport-address** *ipv4-address*

**undo mpls ldp transport-address**

### Default

In interface view, if the interface belongs to the public network, the LDP IPv4 transport address is the local LSR ID. If the interface belongs to a VPN, the LDP IPv4 transport address is the primary IP address of the interface.

In LDP peer view, the LDP IPv4 transport address is the local LSR ID.

### Views

Interface view

LDP peer view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*ipv4-address*: Specifies the LDP IPv4 transport address.

**interface**: Uses the IPv4 address of the current interface as the LDP IPv4 transport address.

### Usage guidelines

Before two LSRs establish an IPv4 LDP session, they must establish a TCP connection by using the LDP IPv4 transport address.

As a best practice, use the default LDP IPv4 transport address.

If two LSRs have multiple links in between and you want to establish an IPv4 LDP session on each link, make sure all the links use the same IPv4 transport address.

### Examples

# Specify the LDP transport address carried in Targeted Hellos sent to peer 3.3.3.3 as 2.2.2.2.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] targeted-peer 3.3.3.3
[Sysname-ldp-peer-3.3.3.3] mpls ldp transport-address 2.2.2.2
```

# On VLAN-interface 2, specify the transport address carried in Link Hellos as the IP address of the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] mpls ldp transport-address interface
```

### Related commands

**display mpls ldp discovery**

**targeted-peer**

# session protection

Use **session protection** to enable session protection.

Use **undo session protection** to disable session protection.

### Syntax

**session protection** [ **duration** t*ime* ] [ **peer** *peer-prefix-list-name* ]

**undo session protection**

### Default

Session protection is disabled.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**duration** *time*: Specifies the session protection duration time in the range of 30 to 2147483 seconds. If you do not specify the duration, session protection always takes effect.

**peer** *peer-prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. Sessions to the peers whose LSR IDs are permitted by the specified IP prefix list are protected. If you do not specify this option, all sessions established by the Basic Discovery mechanism are protected.

### Usage guidelines

If two LDP peers have both a direct link and an indirect link in between, you can configure this feature to protect their LDP session when the direct link fails.

LDP establishes both a Link Hello adjacency over the direct link and a Targeted Hello adjacency over the indirect link with the peer. When the direct link fails, LDP deletes the Link Hello adjacency but still maintains the Targeted Hello adjacency. In this way, the LDP session between the two peers is kept available, and the FEC-label mappings based on this session are not deleted. When the direct link recovers, the LDP peers do not need to re-establish the LDP session or re-learn the FEC-label mappings.

When you enable the session protection feature, you can specify the session protection duration. If the Link Hello adjacency does not recover within the duration, LDP deletes the Targeted Hello adjacency and the LDP session. If you do not specify the session protection duration, the two peers always maintain the LDP session over the Targeted Hello adjacency.

### Examples

# Enable protection for the session to peer 3.3.3.3, and set the session protection duration to 120 seconds.

```
<Sysname> system-view
[Sysname] ip prefix-list protected-peer-list index 1 permit 3.3.3.3 32
[Sysname] mpls ldp
[Sysname-ldp] session protection duration 120 peer protected-peer-list
```

### Related commands

**display mpls ldp peer**

## targeted-peer

Use **targeted-peer** to create a targeted IPv4 LDP peer and enter its view, or enter the view of an existing targeted IPv4 LDP peer. The device can send unsolicited IPv4 Targeted Hellos to the peer and can respond to IPv4 Targeted Hellos received from the peer.

Use **undo targeted-peer** to cancel the configuration.

### Syntax

**targeted-peer** *ipv4-address*

**undo targeted-peer** *ipv4-address*

### Default

No targeted LDP peers exist. The device does not send IPv4 Targeted Hellos to any peers, or respond to IPv4 Targeted Hellos received from any peers.

### Views

LDP view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*ipv4-address*: Specifies the peer IPv4 address.

### Usage guidelines

If you do not specify the LDP transport address, LDP sends the local LSR ID to the peer specified by this command in IPv4 Targeted Hellos.

To ensure a successful IPv4 Targeted Hello adjacency, make sure the following requirements are met:

- The peer IPv4 address configured on the local LSR is the same as the IPv4 transport address configured in LDP peer view on the peer.
- A route exists between the local IPv4 transport address and the peer IPv4 address.

LDP automatically sends Targeted Hellos to the specified peer after one of the following features is configured:

- LDP session protection.
- LDP over MPLS TE.
- MPLS L2VPN LDP PW.
- VPLS LDP PW.

To modify the Targeted Hello/Keepalive hold time and interval, you must use this command to create the LDP peer, and then perform the modification in the LDP peer view.

### Examples

# Configure the device to send IPv4 Targeted Hellos to peer 3.3.3.3, and enter LDP peer view.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] targeted-peer 3.3.3.3
[Sysname-ldp-peer-3.3.3.3]
```

### Related commands

**display mpls ldp discovery**

**display mpls ldp peer**

# IPv6 LDP commands

## ipv6 accept-label

Use **ipv6 accept-label** to configure a label acceptance policy.

Use **undo ipv6 accept-label** to delete a label acceptance policy.

### Syntax

**ipv6 accept-label peer** *peer-lsr-id* **prefix-list** *prefix-list-name*

**undo ipv6 accept-label peer** *peer-lsr-id*

### Default

No label acceptance policy is configured. LDP accepts all IPv6 FEC-label mappings from all peers.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**peer** *peer-lsr-id*: Specifies an LDP peer by its LSR ID.

**prefix-list** *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

### Usage guidelines

This feature enables you to control the number of FEC-label mappings received from peers. LDP accepts only the FEC-label mappings whose IPv6 prefixes are permitted by the specified IPv6 prefix list from the specified peer.

To accept the previously denied label mappings from a peer, use the **undo ipv6 accept-label** command or change the IPv6 prefix list for the peer. Then, execute the **reset mpls ldp** command to reset the LDP session to that peer to apply the new settings.

Using a label advertisement policy on an LSR or using a label acceptance policy on its upstream LSR can achieve the same purpose. As a best practice, use the label advertisement policy to reduce network load.

### Examples

# Configure a label acceptance policy to accept only the FEC-label mappings containing IPv6 prefix 2001:D00::/32 and a prefix length greater than or equal to 32 bits from LDP peer 1.1.1.9.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list prefix-from-RTA permit 2001:D00:: 32 less-equal 128
[Sysname] mpls ldp
[Sysname-ldp] ipv6 accept-label peer 1.1.1.9 prefix-list prefix-from-RTA
```

### Related commands

**display mpls ldp peer verbose**

**ipv6 prefix-list** (*Layer 3—IP Routing Command Reference*)

# ipv6 advertise-label

Use **ipv6 advertise-label** to configure a label advertisement policy.

Use **undo ipv6 advertise-label** to delete a label advertisement policy.

## Syntax

**ipv6 advertise-label prefix-list** *prefix-list-name* [ **peer** *peer-prefix-list-name* ]

**undo ipv6 advertise-label prefix-list** *prefix-list-name*

## Default

No label advertisement policy is configured. The device advertises IPv6 FEC-label mappings permitted by the LSP generation policy to all peers.

## Views

LDP view

LDP-VPN instance view

## Predefined user roles

network-admin

mdc-admin

## Parameters

**prefix-list** *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. This prefix list filters advertised label mappings.

**peer** *peer-prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. This prefix list filters LDP peers. If you do not specify this option, the device advertises label mappings to all peers.

## Usage guidelines

Use a label advertisement policy to filter label mappings advertised to peers.

Configure multiple label advertisement policies by executing this command multiple times.

If a label mapping is permitted by an advertisement policy, LDP advertises the mapping by following these rules:

- If the policy has no peer IPv6 prefix list (**peer** *peer-prefix-list-name* not specified), LDP advertises the label mapping to all peers.
- If the policy has a peer IPv6 prefix list, LDP advertises the label mapping to the peers permitted by the peer IPv6 prefix list.

If a label mapping is permitted by multiple advertisement policies, LDP advertises the label mapping according to the first configured policy.

Using a label advertisement policy on an LSR or using a label acceptance policy on its upstream LSR can achieve the same purpose. As a best practice, use the label advertisement policy to reduce network load.

## Examples

# Configure two label advertisement policies. One policy advertises only the label mapping for subnet 2001::1/64 to peer 3.3.3.9. The other policy advertises only the label mapping for subnet 3001::1/64 to peer 4.4.4.9.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list prefix-to-C permit 2001::1 64
[Sysname] ipv6 prefix-list prefix-to-D permit 3001::1 64
```

```
[Sysname] ip prefix-list peer-C permit 3.3.3.9 32
[Sysname] ip prefix-list peer-D permit 4.4.4.9 32
[Sysname] mpls ldp
[Sysname-ldp] ipv6 advertise-label prefix-list prefix-to-C peer peer-C
[Sysname-ldp] ipv6 advertise-label prefix-list prefix-to-D peer peer-D
```

### Related commands

**display mpls ldp fec**

**ipv6 prefix-list** (*Layer 3—IP Routing Command Reference*)

**ipv6 lsp-trigger**

# ipv6 import bgp

Use **ipv6 import bgp** to enable LDP to redistribute BGP IPv6 unicast routes.

Use **undo ipv6 import bgp** to disable LDP from redistributing BGP IPv6 unicast routes.

### Syntax

**ipv6 import bgp** [ *as-number* ]

**undo ipv6 import bgp**

### Default

LDP does not redistribute BGP IPv6 unicast routes.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

*as-number*: Redistributes BGP IPv6 unicast routes in the specified AS. An AS number is in the range of 1 to 4294967295. If you do not specify an AS number, this command enables LDP to redistribute all BGP IPv6 unicast routes.

### Usage guidelines

**IMPORTANT:**

Use this command only if necessary. Execution of this command will increase the number of routes redistributed to LDP. A large number of redistributed routes use a large amount of labels and memory.

By default, LDP automatically redistributes IPv6 IGP routes, including the BGP IPv6 unicast routes that have been redistributed into IGP. Then, LDP assigns labels to the IGP routes and labeled BGP routes if these routes are permitted by an LSP generation policy. LDP does not automatically redistribute BGP IPv6 unicast routes if the routes are not redistributed into the IGP.

For example, on a carrier's carrier network where IGP is not configured between a PE of a Level 1 carrier and a CE of a Level 2 carrier, LDP cannot redistribute BGP IPv6 unicast routes to assign labels to them. For this network to operate correctly, enable LDP to redistribute BGP IPv6 unicast routes. If the routes are permitted by an LSP generation policy, LDP assigns labels to them to establish LSPs. For more information about carrier's carrier, see *MPLS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

### Examples

# Enable LDP to redistribute BGP IPv6 unicast routes in AS 100 on the public network.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] ipv6 import bgp 100
```

### Related commands

**ipv6 lsp-trigger**

# ipv6 lsp-trigger

Use **ipv6 lsp-trigger** to configure an LSP generation policy for IPv6 FECs.

Use **undo ipv6 lsp-trigger** to restore the default.

### Syntax

**ipv6 lsp-trigger** { **all** | **prefix-list** *prefix-list-name* }

**undo ipv6 lsp-trigger**

### Default

LDP only uses redistributed IPv6 host routes with a 128-bit prefix to generate LSPs.

### Views

LDP view

LDP-VPN instance view

### Predefined user roles

network-admin

mdc-admin

### Parameters

**all**: Enables LDP to use all redistributed routes to generate LSPs.

**prefix-list** *prefix-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. LDP uses only the redistributed routes permitted by the IPv6 prefix list to generate LSPs.

### Usage guidelines

LDP assigns labels to the routes that have been redistributed into LDP to generate LSPs. An LSP generation policy specifies the routes that LDP uses to generate LSPs.

The default LSP generation policy depends on the label distribution control mode.

- In Ordered mode, LDP can only use the following routes to generate LSPs:
  - Loopback interface address routes with a 128-bit prefix.
  - The routes with a 128-bit prefix that match the FECs of label mappings received from downstream LSRs.
- In Independent mode, LDP can use all routes with a 128-bit prefix to generate LSPs.

After you configure an LSP generation policy, LDP uses all redistributed routes or those permitted by the IPv6 prefix list to generate LSPs, regardless of the label distribution control mode.

As a best practice, use the default LSP generation policy.

### Examples

# Configure an LSP generation policy that enables LDP to use only redistributed routes 2001::1/64 to establish LSPs for the public network.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list egress-fec-list permit 2001::1 64
[Sysname] mpls ldp
[Sysname-ldp] ipv6 lsp-trigger prefix-list egress-fec-list
```

### Related commands

**ipv6 import bgp**

**ipv6 prefix-list** (*Layer 3—IP Services Command Reference*)

# mpls ldp ipv6 enable

Use **mpls ldp ipv6 enable** to enable IPv6 LDP on an interface.

Use **undo mpls ldp ipv6 enable** to disable IPv6 LDP on an interface.

### Syntax

**mpls ldp ipv6 enable**

**undo mpls ldp ipv6 enable**

### Default

IPv6 LDP is disabled on an interface.

### Views

Interface view

### Predefined user roles

network-admin

mdc-admin

### Usage guidelines

An up interface enabled with IPv6 LDP and MPLS sends IPv6 Link Hellos for neighbor discovery.

Before you enable IPv6 LDP on an interface, use the **mpls ldp** command in system view to enable LDP globally. If the interface is bound to a VPN instance, you must also use the **vpn-instance** command to enable LDP for the VPN instance.

An interface can be enabled with both IPv4 LDP and IPv6 LDP.

If an interface is enabled with only IPv6 LDP, LDP can send IPv6 Hellos only after you specify the LDP transport address by using the **mpls ldp transport-address** command.

### Examples

# Enable IPv6 LDP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] mpls ldp ipv6 enable
```

### Related commands

**display mpls ldp interface**

**mpls enable**

**mpls ldp**

**mpls ldp enable**

# mpls ldp transport-address

Use **mpls ldp transport-address** to specify the LDP IPv6 transport address.

Use **undo mpls ldp transport-address** to remove the configuration.

## Syntax

In interface view:

**mpls ldp transport-address** *ipv6-address*

**undo mpls ldp transport-address** *ipv6-address*

In LDP peer view:

**mpls ldp transport-address** *ipv6-address*

**undo mpls ldp transport-address**

## Default

No LDP IPv6 transport address is configured.

## Views

Interface view

LDP peer view

## Predefined user roles

network-admin

mdc-admin

## Parameters

*ipv6-address*: Specifies the LDP IPv6 transport address.

## Usage guidelines

Before two LSRs establish an IPv6 LDP session, they must establish a TCP connection by using the LDP IPv6 transport address.

If two LSRs have multiple links in between and you want to establish an IPv6 LDP session on each link, make sure all the links use the same IPv6 transport address.

## Examples

# Specify the LDP transport address as 2002::1 for the TCP connection established with peer 2001::1.

```
<Sysname> System-view
[Sysname] mpls ldp
[Sysname-ldp] targeted-peer 2001::1
[Sysname-ldp-peer-2001::1] mpls ldp transport-address 2002::1
```

## Related commands

**display mpls ldp discovery**

**targeted-peer**

# targeted-peer

Use **targeted-peer** to create a targeted IPv6 LDP peer and enter its view, or enter the view of an existing targeted IPv6 LDP peer. The device can send unsolicited IPv6 Targeted Hellos to the peer and can respond to IPv6 Targeted Hellos received from the peer.

Use **undo targeted-peer** to cancel the configuration.

## Syntax

**targeted-peer** *ipv6-address*

**undo targeted-peer** *ipv6-address*

## Default

No targeted LDP peers exist. The device does not send IPv6 Targeted Hellos to any peers, or respond to IPv6 Targeted Hellos received from any peers.

## Views

LDP view

## Predefined user roles

network-admin

mdc-admin

## Parameters

*ipv6-address*: Specifies the peer IPv6 address.

## Usage guidelines

After a targeted IPv6 LDP peer is created, LDP does not send IPv6 Targeted Hellos to the peer until you specify the LDP IPv6 transport address in LDP peer view.

To ensure a successful IPv6 Targeted Hello adjacency, make sure the following requirements are met:

- The peer IPv6 address configured on the local LSR is the same as the IPv6 transport address configured in LDP peer view on the peer.
- A route exists between the local IPv6 transport address and the peer IPv6 address.

## Examples

# Configure the device to send IPv6 Targeted Hellos to peer 2001::1, and enter LDP peer view.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] targeted-peer 2001::1
[Sysname-ldp-peer-2001::1]
```

## Related commands

**display mpls ldp discovery**

**display mpls ldp peer**