



mpls ldp atm vc-merge through mpls static binding ipv4

- [mpls ldp atm vc-merge, page 3](#)
- [mpls ldp autoconfig, page 5](#)
- [mpls ldp backoff, page 7](#)
- [mpls ldp discovery, page 9](#)
- [mpls ldp discovery transport-address, page 13](#)
- [mpls ldp explicit-null, page 15](#)
- [mpls ldp graceful-restart, page 17](#)
- [mpls ldp graceful-restart timers forwarding-holding, page 19](#)
- [mpls ldp graceful-restart timers max-recovery, page 21](#)
- [mpls ldp graceful-restart timers neighbor-liveness, page 23](#)
- [mpls ldp holdtime, page 25](#)
- [mpls ldp igp autoconfig, page 27](#)
- [mpls ldp igp sync, page 29](#)
- [mpls ldp igp sync holddown, page 31](#)
- [mpls ldp label, page 33](#)
- [mpls ldp logging neighbor-changes, page 35](#)
- [mpls ldp logging password configuration, page 37](#)
- [mpls ldp logging password rollover, page 39](#)
- [mpls ldp loop-detection, page 41](#)
- [mpls ldp maxhops, page 43](#)
- [mpls ldp neighbor implicit-withdraw, page 45](#)
- [mpls ldp neighbor labels accept, page 47](#)
- [mpls ldp neighbor password, page 49](#)

- [mpls ldp neighbor targeted, page 52](#)
- [mpls ldp nsr, page 54](#)
- [mpls ldp password fallback, page 56](#)
- [mpls ldp password option, page 59](#)
- [mpls ldp password required, page 63](#)
- [mpls ldp password rollover duration, page 65](#)
- [mpls ldp path-vector maxlength, page 67](#)
- [mpls ldp router-id, page 70](#)
- [mpls ldp session protection, page 73](#)
- [mpls ldp sync, page 75](#)
- [mpls ldp tcp pak-priority, page 77](#)
- [mpls load-balance per-label, page 79](#)
- [mpls mtu, page 81](#)
- [mpls netflow egress, page 86](#)
- [mpls oam, page 88](#)
- [mpls prefix-map, page 90](#)
- [mpls request-labels for, page 92](#)
- [mpls static binding ipv4, page 94](#)

mpls ldp atm vc-merge



Note

Effective with Cisco IOS Release 12.4(20)T, the **mpls ldp atm vc-merge** command is not available in Cisco IOS software.

To control whether the vc-merge (multipoint-to-point) capability is supported for unicast label virtual circuits (LVCs), use the **mpls ldp atm vc-merge** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp atm vc-merge

no mpls ldp atm vc-merge

Syntax Description

This command has no arguments or keywords.

Command Default

The ATM-VC merge capability is enabled by default if the hardware supports this feature; otherwise, the feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect MPLS IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E and implemented on the Catalyst 6500 switch and the Cisco 7600 router.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR c.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and implemented on the Cisco 10000(PRE-1) router.

Release	Modification
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

Use of VC merge helps conserve ATM labels by allowing incoming LSPs from different sources for the same destination to be merged onto a single outgoing VC.

Examples

In the following example, the ATM-VC merge capability is disabled:

```
Router# no mpls ldp atm vc-merge
```

Related Commands

Command	Description
show mpls atm-ldp capability	Displays the ATM MPLS capabilities negotiated with LDP neighbors for LC-ATM interfaces.

mpls ldp autoconfig

To enable Label Distribution Protocol (LDP) on interfaces for which an Open Shortest Path First (OSPF) instance or Intermediate System-to-Intermediate System (IS-IS) instance has been defined, use the **mpls ldp autoconfig** command in router configuration mode. To disable this feature, use the **no** form of this command.

For OSPF

mpls ldp autoconfig [*area area-id*]

no mpls ldp autoconfig [*area area-id*]

For IS-IS

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

no mpls ldp autoconfig

Syntax Description

<i>area area-id</i>	(Optional) Enables LDP on the interfaces belonging to the specified OSPF area.
<i>level-1</i> <i>level-2</i>	(Optional) Enables LDP for a specified IS-IS level. If an interface is enabled for the same level as autoconfiguration, then LDP is enabled over that interface. If the interface has a different level than autoconfiguration, LDP is not enabled. By default, without the use of these arguments, the configuration is applied to both the levels.

Command Default

LDP is not enabled on interfaces. If an OSPF area or an IS-IS level is not specified, LDP is enabled on all interfaces belonging to the OSPF or IS-IS process.

Command Modes

Router configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.0(32)SY	This command was modified to support IS-IS processes in Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

- You can specify this command multiple times to enable LDP on different routing areas with interfaces running OSPF.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails. LDP must be enabled globally by means of the global **mpls ip** command first.
- If the **mpls ldp autoconfig** command is configured, you cannot issue the global **no mpls ip** command. If you want to disable LDP, you must issue the **no mpls ldp autoconfig** command first.
- The **mpls ldp autoconfig** command is supported only with OSPF and IS-IS interior gateway protocols (IGPs).
- The MPLS LDP Autoconfiguration feature supports IS-IS only in Cisco IOS Release 12.0(32)SY.
- For interfaces running IS-IS processes, you can enable Multiprotocol Label Switching (MPLS) for each interface using the router mode command **mpls ldp autoconfig** or **mpls ldp igp autoconfig** at the interface level.
- For IS-IS interfaces, the level for which an interface is configured must be compatible with the level for which autoconfiguration is desired.
- For IS-IS interfaces, each application of the configuration command overwrites the earlier configuration. If initial autoconfiguration is enabled for level-1 and a later configuration specifies level-2, LDP is enabled only on IS-IS level-2 interfaces.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for OSPF area 5:

```
Router(config-router)# mpls ldp autoconfig area 5
```

Related Commands

Command	Description
mpls ldp igp autoconfig	Enables LDP on an interface.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp backoff

To configure parameters for the label distribution protocol (LDP) backoff mechanism, use the **mpls ldp backoff** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp backoff *initial-backoff maximum-backoff*

no mpls ldp backoff *initial-backoff maximum-backoff*

Syntax Description

<i>initial-backoff</i>	Number from 5 to 2147483, inclusive, that defines the initial backoff value in seconds. The default is 15 seconds.
<i>maximum-backoff</i>	Number from 5 to 2147483, inclusive, that defines the maximum backoff value in seconds. The default value is 120 seconds.

Command Default

The initial backoff value is 15 seconds and grows to a maximum value of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The LDP backoff mechanism prevents two incompatibly configured label switch routers (LSRs) from engaging in an unthrottled sequence of session setup failures. For example, an incompatibility arises when two neighboring routers attempt to perform LC-ATM (label-controlled ATM) but the two are using different ranges of VPI/VCI values for labels.

If a session setup attempt fails due to an incompatibility, each LSR delays its next attempt (that is, backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

The default settings correspond to the lowest settings for initial and maximum backoff values defined by the LDP protocol specification. You should change the settings from the default values only if such settings result in undesirable behavior.

Examples

The following command shows how to set the initial backoff delay to 30 seconds and the maximum backoff delay to 240 seconds:

```
Router(config)# mpls ldp backoff 30 240
```

Related Commands

Command	Description
show mpls ldp backoff	Displays information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery hello messages, or the hold time for a discovered LDP neighbor, or the neighbors from which requests for targeted hello messages may be honored, use the **mpls ldp discovery** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery {hello {holdtime| interval} seconds| targeted-hello {holdtime| interval} seconds| accept [from acl]}

no mpls ldp discovery {hello {holdtime| interval}| targeted-hello {holdtime| interval}| accept [from acl]}

Syntax Description

hello	Configures the intervals and hold times for directly connected neighbors.
holdtime	Defines the period of time a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. The default value for the holdtime keyword is 15 seconds for link hello messages and 90 seconds for targeted hello messages.
interval	Defines the period of time between the sending of consecutive hello messages. The default value for the interval keyword is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
<i>seconds</i>	Hold time or interval in seconds: <ul style="list-style-type: none"> • The default hold time is 15 seconds for link hello messages and 90 seconds for targeted hello messages. • The default interval is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
targeted-hello	Configures the intervals and hold times for neighbors that are not directly connected (for example, LDP sessions that run between the endpoints of an LSP tunnel).
accept	Configures the router to respond to requests for targeted hello messages from all neighbors or from neighbors specified by the optional acl argument.

from <i>acl</i>	<p>(Optional) The IP access list that specifies the neighbor from which requests for targeted hello messages may be honored.</p> <p>Caution Ensure that the access control list (ACL) is properly configured with the LDP sessions to be accepted. If no LDP entries are configured in the ACL, the ACL will allow all LDP sessions from any source.</p>
------------------------	---

Command Default None

Command Modes Global configuration (config)

Command History	Release	Modification
	11.1CT	This command was introduced.
	12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
	12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. Default values for the holdtime and interval keywords were changed.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The discovery hold time is set to the smaller of the following: the locally proposed hold time or the hold time proposed by the neighbor. The hello interval is selected so that within the hello hold time period at least three hellos messages are sent for a link hello and at least nine hello messages are sent for a targeted hello.

When the discovery hold time elapses for a neighbor discovered on an interface or for a neighbor discovered by means of a targeted hello message, the record associating the neighbor with that interface or the targeted hello message source is discarded. If an LDP session exists with a neighbor, but a discovery record no longer exists for that neighbor, the LDP session is terminated.

Setting the hold time too high causes LDP to be slow in detecting link outages; setting the hold time too low might cause LDP to terminate sessions when a hello message is dropped during traffic bursts on a link.

The exchange of targeted hello messages between two nondirectly connected neighbors (N1 and N2) may occur in the following ways:

- N1 may initiate the transmission of targeted hello messages to N2, and N2 may send targeted hello messages in response. In this situation, N1 is considered to be active and N2 is considered to be passive.

N1 targeted hello messages carry a request that N2 send targeted hello messages in response. To respond, N2 configuration must permit it to respond to N1. The **mpls ldp discovery targeted-hello accept** command is used to configure whether N1 must respond to requests for targeted hello messages.

- Both N1 and N2 may be configured to initiate the transmission of targeted hello messages to each other. In this situation, both are active.

Both, one, or neither of N1 and N2 may be passive, depending on whether they have been configured to respond to requests for targeted hello messages from the other.



Note

Normally, active transmission of targeted hello messages on a router is triggered by some configuration action, such as an **mpls ip** command on a traffic engineering tunnel interface.

Examples

The following example shows how to set the period of time to 30 seconds for which a neighbor discovered on an interface is remembered, if no hello messages are received:

```
Router# configure terminal
Router(config)# mpls ldp discovery hello holdtime 30
```

The following example shows how to configure the router to respond to requests for targeted hello messages from neighbors 209.165.200.225 and 209.165.200.234:

```
Router(config)# ip access standard TRGT-ACCEPT
Router(config-nacl)# permit 209.165.200.225
Router(config-nacl)# permit 209.165.200.234
Router(config-nacl)# exit
Router(config)# mpls ldp discovery targeted-hello from TRGT-ACCEPT
```

Related Commands

Command	Description
mpls ip	Enables MPLS forwarding of IPv4 packets along normally routed paths.
mpls ldp holdtime	Changes the time for which an LDP session is maintained in the absence of LDP messages from the session peer.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery transport-address

To specify the transport address advertised in the Label Distribution Protocol (LDP) discovery hello messages sent on an interface, use the **mpls ldp discovery transport-address** command in interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery transport-address {*interface* | *IP-address*}

no mpls ldp discovery transport-address

Syntax Description

interface	Specifies that the interface IP address should be advertised as the transport address.
<i>IP-address</i>	IP address advertised as the transport address.

Command Default

The default behavior when this command has not been issued for an interface depends on the interface type. Unless the interface is a label-controlled ATM (LC-ATM) interface, LDP advertises its LDP router ID as the transport address in LDP discovery hello messages sent from the interface. If the interface is an LC-ATM interface, no transport address is explicitly advertised in LDP discovery hello messages sent from the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

The establishment of an LDP session between two routers requires a session TCP connection by which label advertisements can be exchanged between the routers. To establish the session TCP connection, each router must know the transport address (IP address) of the other router.

The LDP discovery mechanism provides the means for a router to advertise the transport address for its end-of-session TCP connection. When the transport address advertisement is explicit, the transport address appears as part of the contents of discovery hello messages sent to the peer. When the transport address advertisement is implicit, the transport address is not included in the discovery hello messages, and the peer uses the source IP address of received hello messages as the peer transport address.

The `mpls ldp discovery transport-address` command provides the means to modify the default behavior described in the Command Default section of this document. When the **interface** keyword is specified, LDP advertises the IP address of the interface in LDP discovery hello messages sent from the interface. When the *IP-address* argument is specified, LDP advertises the specified IP address in LDP discovery hello messages sent from the interface.



Note

When a router has multiple links connecting it to its peer device, the router must advertise the same transport address in the LDP discovery hello messages it sends on all such interfaces.

Examples

The following example shows how to specify the LDP transport address for interface pos2/0 should be the interface IP address; it also shows how to specify the IP address 209.165.200.225 of interface pos3/1 should be the LDP transport address:

```
Router(config)# interface pos2/0
Router(config-if)# mpls ldp discovery transport-address interface
Router(config)# interface pos3/1
Router(config-if)# mpls ldp discovery transport-address 209.165.200.225
```

Related Commands

Command	Description
<code>show mpls ldp discovery</code>	Displays the status of the LDP discovery process.
<code>show mpls ldp neighbor</code>	Displays the status of LDP sessions.

mpls ldp explicit-null

To cause a router to advertise an Explicit Null label in situations where it would normally advertise an Implicit Null label, use the **mpls ldp explicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp explicit-null [*for prefix-acl* | *to peer-acl*] **for prefix-acl to peer-acl**

no mpls ldp explicit-null

Syntax Description

for prefix-acl	(Optional) Specifies prefixes for which Explicit Null should be advertised in place of Implicit Null.
to peer-acl	(Optional) Specifies Label Distribution Protocol (LDP) peers to which Explicit Null should be advertised in place of Implicit Null.

Command Default

Implicit Null is advertised for directly connected routes unless the command **mpls ldp explicit-null** has been executed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the previous hop (penultimate) router to do penultimate hop popping. Situations exist where it might be desirable to prevent the penultimate router from performing penultimate hop popping and to force it to replace the incoming label with the Explicit Null label.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes permitted by the *prefix-acl* argument to peers permitted by the *peer-acl* argument.

If you do not specify the *prefix-acl* argument in the command, Explicit Null is advertised in place of Implicit Null for all directly connected prefixes.

If you do not specify the *peer-acl* argument in the command, Explicit Null is advertised in place of Implicit Null to all peers.

Examples

The following command shows how to cause Explicit Null to be advertised for all directly connected routes to all LDP peers:

```
Router(config)# mpls ldp explicit-null
```

The following command sequence shows how to cause Explicit Null to be advertised for directly connected route 10.5.0.0 to all LDP peers and Implicit Null to be advertised for all other directly connected routes:

```
Router(config)# ip access-list standard adv-exp-null
Router(config-std-nacl)# permit 10.5.0.0
Router(config-std-nacl)# deny any
Router(config-std-nacl)# exit
Router(config)# mpls ldp explicit-null for adv-exp-null
```

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp graceful-restart

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart, use the **mpls ldp graceful-restart** command in global configuration mode. To disable LDP Graceful Restart, use the **no** form of this command.

mpls ldp graceful-restart

no mpls ldp graceful-restart

Syntax Description This command has no arguments or keywords.

Command Default LDP Graceful Restart is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(29)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines LDP Graceful Restart must be enabled before an LDP session is established.
Using the **no** form of the command disables the Graceful Restart functionality on all LDP sessions.

Examples The command in the following example enables LDP Graceful Restart on a router:

```
Router(config)# mpls ldp graceful-restart
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers forwarding-holding

To specify the amount of time the Multiprotocol Label Switching (MPLS) forwarding state should be preserved after the control plane restarts, use the **mpls ldp graceful-restart timers forwarding-holding** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers forwarding-holding *secs*

no mpls ldp graceful-restart timers forwarding-holding

Syntax Description

<i>secs</i>	The amount of time (in seconds) that the MPLS forwarding state should be preserved after the control plane restarts. The default is 600 seconds. The range is 30 to 600 seconds.
-------------	--

Command Default

After the control plane on the Cisco 7500 and Cisco 10000 series router restarts, the MPLS forwarding state is preserved for 600 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Configuring the local forwarding-holding timer to a value less than the IOS FT Reconnect Timeout of 120 seconds may prevent a Label Distribution Protocol (LDP) session from being established. Configure the forwarding-holding timer to less than 120 seconds only if an LDP neighbor has an FT Reconnect Timeout value of less than 120 seconds.

If the timer expires, all entries that are marked stale are deleted.

Examples

In the following example, the MPLS forwarding state is preserved for 300 seconds after the control plane restarts:

```
Router(config)# mpls ldp graceful-restart timers forwarding-holding 300
```

Related Commands

Command	Description
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-aliveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers max-recovery

To specify the amount of time a router should hold stale label-Forwarding Equivalence Class (FEC) bindings after a Label Distribution Protocol (LDP) session has been reestablished, use the **mpls ldp graceful-restart timers max-recovery** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers max-recovery *secs*

no mpls ldp graceful-restart timers max-recovery

Syntax Description

<i>secs</i>	The amount of time (in seconds) that the router should hold stale label-FEC bindings after an LDP session has been reestablished. The default is 120 seconds. The range is 15 to 600 seconds.
-------------	---

Command Default

Stale label-FEC bindings are held for 120 seconds after an LDP session has been reestablished.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

After the timer expires, all stale label-FEC bindings learned from the associated LDP session are removed, which results in the removal of any forwarding table entries that are based on those bindings.

Examples

In the following example, the router should hold stale label-FEC bindings after an LDP session has been reestablished for 180 seconds:

```
Router(config)# mpls ldp graceful-restart timers max-recovery 180
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers neighbor-liveness

To specify the upper bound on the amount of time a router should wait for a Label Distribution Protocol (LDP) session to be reestablished, use the **mpls ldp graceful-restart timers neighbor-liveness** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers neighbor-liveness *secs*

no mpls ldp graceful-restart timers neighbor-liveness

Syntax Description

<i>secs</i>	The amount of time (in seconds) that the router should wait for an LDP session to be reestablished. The default is 120 seconds. The range is 5 to 300 seconds.
-------------	--

Command Default

The default is a maximum of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The amount of time a router waits for an LDP session to be reestablished is the lesser of the following values:

- The value of the peer's fault tolerant (FT) type length value (TLV) reconnect timeout
- The value of the neighbor liveness timer

If the router cannot reestablish an LDP session with the neighbor in the time allotted, the router deletes the stale label-FEC bindings received from that neighbor.

Examples

The command in the following example sets the amount of time that the router should wait for an LDP session to be reestablished to 30 seconds:

```
Router(config)# mpls ldp graceful-restart timers neighbor-liveness 30
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.

mpls ldp holdtime

To change the time for which an Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer, use the **mpls ldp holdtime** command in global configuration mode. To disable this command, use the **no** form of the command.

mpls ldp holdtime *seconds*

no mpls ldp holdtime *seconds*

Syntax Description

<i>seconds</i>	Number from 15 to 65535 that defines the time, in seconds, an LDP session is maintained in the absence of LDP messages from the session peer. The default is 180.
----------------	---

Command Default

The default value for the *seconds* argument is 180.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)s	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an LDP session is established between two LSRs, the hold time used for the session is the lower of the values configured on the two LSRs.

Examples

The following example shows how to configure the hold time of LDP sessions for 30 seconds:

```
Router# mpls ldp holdtime 30
```

Related Commands

Command	Description
show mpls ldp parameters	Displays the current LDP parameter.
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.

mpls ldp igp autoconfig

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration on an interface that belongs to an Open Shortest Path First (OSPF) area, use the **mpls ldp igp autoconfig** command in interface configuration mode. To disable MPLS LDP autoconfiguration, use the **no** form of the command.

mpls ldp igp autoconfig

no mpls ldp igp autoconfig

Syntax Description This command has no arguments or keywords.

Command Default This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. So, by default, all interfaces are enabled for LDP.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	12.0(30)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
	Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
	Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. To disable LDP on selected interfaces, use the **no mpls ldp igp autoconfig** command.

Examples The following example shows how to disable LDP on interface POS1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp autoconfig
```

Related Commands

Command	Description
mpls ldp autoconfig	Globally enables LDP on all interfaces that belong to an OSPF area.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp igp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on an interface that belongs to an Open Shortest Path First (OSPF) process, use the **mpls ldp igp sync** command in interface configuration mode. To disable MPLS LDP-IGP synchronization, use the **no** form of the command.

mpls ldp igp sync [*delay seconds*]

no mpls ldp igp sync [*delay*]

Syntax Description

delay	(Optional) Sets a delay timer for MPLS LDP-IGP synchronization.
<i>seconds</i>	(Optional) Delay time, in seconds. The range is 5 to 60 seconds.

Command Default

If MPLS LDP-IGP synchronization is enabled on an OSPF process, MPLS LDP-IGP synchronization is enabled by default on all interfaces configured for the process. A delay timer is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.0(32)S	The optional delay seconds keyword and argument were added.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

This command works with the **mpls ldp sync** command, which enables MPLS LDP-IGP synchronization on all interfaces that belong to an OSPF process. To disable MPLS LDP-IGP synchronization on a selected interface, use the **no mpls ldp igp sync** command in the configuration for that interface.

Use the **mpls ldp igp sync delay seconds** command to configure a delay time for MPLS LDP and IGP synchronization on an interface-by-interface basis. To remove the delay timer from a specified interface, use the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP-IGP synchronization enabled.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks that synchronization is still valid and notifies the OSPF process.
- If the delay time is not configured, synchronization is disabled or down, or an interface is removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

Examples

The following example shows how to disable MPLS LDP-IGP synchronization on POS interface 1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp sync
```

The following example shows how to set a delay timer of 45 seconds for MPLS LDP-IGP synchronization on FastEthernet interface 0/0:

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# mpls ldp igp sync delay 45
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp igp sync holddown

To specify how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) synchronization to be achieved, use the **mpls ldp igp sync holddown** command in global configuration mode. To disable the hold-down timer, use the **no** form of this command.

mpls ldp igp sync holddown *milliseconds*

no mpls ldp igp sync holddown

Syntax Description

<i>milliseconds</i>	The number of milliseconds an IGP should wait for an LDP session to be established. The range is 1 to 2147483647.
---------------------	---

Command Default

An IGP will wait indefinitely for LDP synchronization to be achieved.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command enables you to limit the amount of time an IGP waits for LDP synchronization to be achieved.

Examples

In the following example, the IGP is limited to 10,000 milliseconds (10 seconds):

```
Router(config)# mpls ldp igp sync holddown 10000
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp label

To enter MPLS LDP label configuration mode to specify how Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation, use the **mpls ldp label** command in global configuration mode. To remove all local label allocation filters configured in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation without a session reset, use the **no** form of this command.

mpls ldp label

no mpls ldp label

Syntax Description This command has no arguments or keywords.

Command Default LDP label configuration mode commands are not available.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SRC	This command was introduced.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines After you enter the **mpls ldp label** command, you can specify a prefix list or host routes to filter prefixes for MPLS LDP local label allocation.

Use the **no** form of the command to remove prefix filtering for local label allocation and restore the default LDP local allocation behavior without resetting the session.

A maximum of one filter configuration is allowed for the global table.

Examples The following example shows how to enter MPLS LDP label configuration mode, specify the prefix list named list1 to filter prefixes for MPLS LDP local label allocation, and exit MPLS LDP label configuration mode:

```
configure terminal
!
mpls ldp label
 allocate global prefix-list list1
exit
```

The following examples shows how to remove all local label allocation filters in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation:

```
configure terminal
!
no mpls ldp label
```

Related Commands

Command	Description
allocate	Configures local label allocation filters for learned routes for MPLS LDP.

mpls ldp logging neighbor-changes

To generate system error logging (syslog) messages when Label Distribution Protocol (LDP) sessions go down, use the **mpls ldp logging neighbor-changes** command in global configuration mode. To disable generating syslog messages, use the **no** form of this command.

mpls ldp logging neighbor-changes

no mpls ldp logging neighbor-changes

Syntax Description This command has no arguments or keywords.

Command Default Logging is enabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.0(24)S	This command was introduced.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(14)T	This command was integrated into Cisco IOS Release 12.2(14)T.
	12.0(31)S	The log message is updated to show a VPN routing/forwarding instance (VRF) information and the reason for an LDP neighbor going down.
	12.3(15)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
	12.4(1)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
	12.2(28)S	The log message is updated to show VRF information and the reason for an LDP neighbor going down.

Usage Guidelines Use the **mpls ldp logging neighbor-changes** command to generate syslog messages when an LDP session goes down. The command also provides VRF information about the LDP neighbor and the reason for the LDP session going down. Some of the reasons for an LDP session going down are the following:

- An LDP was disabled globally by configuration.
- An LDP was disabled on an interface.

Examples

The following example generates syslog messages when LDP sessions go down:

```
Router(config)# mpls ldp logging neighbor-changes
```

The following output shows the log entries when an LDP session with neighbor 192.168.1.100:0 goes down and comes up. The session went down because the discovery hold timer expired. The VRF table identifier for the neighbor is 1.

```
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is DOWN (Disc hold timer expired)
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is UP
```

mpls ldp logging password configuration

To enable the display password configuration change events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password configuration** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password configuration [*rate-limit num*]

no mpls ldp logging password configuration

Syntax Description

rate-limit <i>num</i>	(Optional) Specifies a rate limit of 1 to 60 messages per minute.
------------------------------	---

Command Default

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is configured or an existing password has been changed or deleted.

Related Commands

Command	Description
mpls ldp logging password rollover	Enables the display password rollover events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.

Command	Description
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp logging password rollover

To enable the display password rollover events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password rollover** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password rollover [*rate-limit num*]

no mpls ldp logging password rollover

Syntax Description

rate-limit <i>num</i>	(Optional) Specifies a rate limit of 1 to 60 messages per minute.
------------------------------	---

Command Default

Logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is used for authentication or when authentication is disabled.

Related Commands

Command	Description
mpls ldp logging password configuration	Enables the display password configuration change events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.

Command	Description
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp loop-detection

To enable the label distribution protocol (LDP) optional loop detection mechanism, use the **mpls ldp loop-detection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp loop-detection

no mpls ldp loop-detection

Syntax Description

This command has no optional keywords or arguments.

Command Default

LDP loop detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The LDP loop detection mechanism is intended for use in networks of devices that do not use time-to-live mechanisms (for example, ATM switches) that cannot fairly allocate device resources among traffic flows.

The LDP loop detection mechanism is used with the Downstream on Demand method of label distribution, supplementing the Downstream on Demand hop count mechanism to detect looping LSPs that might occur during routing transitions.

Examples

The following command sets the LDP loop detection mechanism on:

```
Router(config)# mpls ldp loop-detection
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.

mpls ldp maxhops

To limit the number of hops permitted in a label switched path (LSP) established by the Downstream on Demand method of label distribution, use the **mpls ldp maxhops** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp maxhops *number*

no mpls ldp maxhops

Syntax Description

<i>number</i>	Number from 1 to 255, inclusive, that defines the maximum hop count. The default is 254.
---------------	--

Command Default

The default is 254 hops.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was updated with MPLS command syntax and terminology.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an ATM label switch router (LSR) initiates a request for a label binding, it sets the hop count value in the Label Request message to 1. Subsequent ATM-LSRs along the path to the edge of the ATM label switching region increment the hop count before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if the hop count value in the request equals or exceeds the maxhops value. Instead, the ATM LSR returns an error message that specifies that the maximum allowable hop count has been reached. This threshold is used to prevent forwarding loops in the setting up of label switch paths across an ATM region.

Examples

The following example sets the hop count limit to 10:

```
Router(config)# mpls ldp maxhops 10
```

Related Commands

Command	Description
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp neighbor implicit-withdraw

To configure the advertisement of a new label for a Forwarding Equivalence Class (FEC) without the withdrawal of the previously advertised label, use the **mpls ldp neighbor implicit-withdraw** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [*vrf vpn-name*] *ip-addr* **implicit-withdraw**

no mpls ldp neighbor [*vrf vpn-name*] *ip-addr* [**implicit-withdraw**]

Syntax Description

<i>vrf vpn-name</i>	(Optional) VPN routing and forwarding instance for the specified neighbor.
<i>ip-addr</i>	Router ID (IP address) that identifies a neighbor.

Command Default

When the **vrf** keyword is not specified in this command, the label distribution protocol (LDP) neighbor is configured in the default routing domain.

If this command is not configured, when it is necessary for LDP to change the label it has advertised to a neighbor for some prefix, it will withdraw the previously advertised label before advertising the new label to the neighbor.

For the no form of the command, if the **implicit-withdraw** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(21)ST	This command was modified to add the implicit-withdraw keyword.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was implemented on the Cisco 10000(PRE-1) router.
12.2(13)T	This command was implemented on the Cisco 2600 and 3600 routers.
12.2(14)S	This command was implemented on the Cisco 7200 and 7500 series routers and integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, in Cisco IOS Release 12.0(21)ST and later, LDP withdraws the previously advertised label by using a withdraw message before advertising a new label for a FEC. In Cisco IOS releases prior to 12.0(21)ST, LDP did not withdraw a previously advertised label before advertising a new label for a FEC. In those older releases, the new label advertisement served as an implied withdraw and LDP did not send a withdraw message. To cause LDP now to operate as it did in releases before Cisco IOS release 12.0(21)ST--that is, to make LDP now advertise a new label for a FEC without first withdrawing the previously advertised label--use this command's **implicit-withdraw** keyword.

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Using the **implicit-withdraw** keyword avoids generating the overhead from an exchange of label withdraw and label release messages.

To disable the **implicit-withdraw** option, use the **no** form of the command with the **implicit-withdraw** keyword. This returns the router to the default, which requires that LDP withdraw the previously advertised label for a FEC before advertising a new label.

```
Router(config)# no
mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Examples

In the following example, LDP does not send a label-withdraw message to the neighbor whose router ID is 10.10.10.10 when a need exists to change the previously advertised label for a FEC:

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor labels accept

To configure a label switching router (LSR) to filter label distribution protocol (LDP) inbound label bindings from a particular LDP peer, use the **mpls ldp neighbor labels accept** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*

no mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*

Syntax Description

vrf <i>vpn-name</i>	(Optional) Specifies VPN routing and forwarding instance (<i>vpn-name</i>) for accepting labels.
<i>nbr-address</i>	Specifies address of the LDP peer whose advertisements are to be filtered.
labels accept <i>acl</i>	Specifies the prefixes (access control list) that are acceptable (permitted).

Command Default

If the **vrf** keyword is not specified, the specified LDP neighbor is configured in the default routing domain.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The specified ACL is used to filter label bindings advertised by the specified neighbor. If the prefix part of the label binding is permitted by the ACL, the router will accept the binding. If the prefix is denied, the router will not accept or store the binding.

This functionality is particularly useful when two different entities manage peer LSRs; that is, the recipient cannot perform filtering by altering the configuration of the sender. This is likely to occur in an Multiprotocol Label Switching (MPLS) virtual private network (VPN) that is using the LDP-based Carrier Supporting Carrier

(CSC) feature. In that situation, the backbone carrier may want to restrict the set of label bindings that its provider edge (PE) router may learn from an adjacent customer edge (CE) router that a customer carrier operates.

When inbound label binding filtering is configured, certain configuration changes may require a router to retain bindings that it previously discarded. For example:

- Inbound filtering is disabled.
- An inbound filtering ACL is redefined to be less restrictive.

A router does not maintain a record of the set of bindings it previously discarded. Therefore, it cannot ask its neighbors to readvertise just those bindings. In addition, LDP (as defined by RFC 3036) does not provide a means for a router to signal its neighbors to readvertise all label bindings. Consequently, to relearn label bindings following such configuration changes, you must reset the LDP session or sessions by using the **clear mpls ldp neighbor** command.



Note

The **mpls ldp neighbor labels accept** command has no effect on an LC-ATM interface. Such an interface behaves as though this command had not been executed. The **mpls ldp request-labels** ACL command, which is supported for LC-ATM, controls which label bindings are requested (accepted) from neighbors.

Examples

The following example specifies that the LSR accepts inbound label bindings from neighbor 10.19.19.19 in vrf vpn1 for prefixes permitted by the ACL named aclone:

```
Router(config)# mpls ldp neighbor vrf vpn1 10.19.19.19 label accept aclone
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
mpls ldp advertise-labels	Controls the distribution of locally assigned (incoming) labels by means of LDP.
show ip access list	Displays the list of configured access lists and their definitions.
show mpls ldp neighbor	Displays the status of the LDP sessions.

mpls ldp neighbor password

To configure a password for computing message digest algorithm 5 (MD5) checksums for the session TCP connection with the specified neighbor, use the **mpls ldp neighbor password** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* **password** *password*

no mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* [**password** *password*]

Syntax Description

<i>vrf vpn-name</i>	(Optional) VPN routing and forwarding instance for the specified neighbor.
<i>ip-address</i>	Router ID (IP address) that identifies a neighbor.
<i>password</i>	Password used for computing MD5 checksums for the session TCP connection with the specified neighbor.

Command Default

Unless the TCP MD5 Signature Option is explicitly configured with the password for session TCP connections, the option is not used. When the **vrf** name is not specified in this command, the Label Distribution Protocol (LDP) neighbor is configured in the default routing domain. For the **no** form of the command, if the password is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	This command was integrated in Cisco IOS Release 12.0(33)S.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You can invoke authentication between two LDP peers, verifying each segment sent on the TCP connection between the peers. To do so, you must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

The authentication capability uses the MD5 algorithm. MD5, an algorithm used in conjunction with SNMP, verifies the integrity of the communication, authenticates the origin of the message, and checks for timeliness.

Invoking the **mpls ldp neighbor password** command causes the generation and checking of the MD5 digest for every segment sent on the TCP connection.

Configuring a password for an LDP neighbor causes an existing LDP session to be torn down and a new session to be established.

If a router has a password configured for a neighbor, but the neighbor router does not have a password configured, a message such as the following appears on the console while the two routers attempt to establish an LDP session:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:646
```

Similarly, if the two routers have different passwords configured, a message such as the following appears on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:646
```

Examples

In the following example, the password (password1) is configured as the password for use with MD5 for the neighbor whose router ID is 139.27.0.15:

```
Router(config)# mpls ldp neighbor 139.27.0.15 password password1
```

In the following example, the password (password1) is configured as the password for use with MD5 for the LDP neighbor having router ID 4.4.4.4 in the VPN routing and forwarding instance named vpn1:

```
Router(config)# mpls ldp neighbor vrf vpn1 4.4.4.4 password password1
```

Related Commands

Command	Description
mpls ldp neighbor implicit-withdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor targeted

To set up a targeted session with a specified neighbor, use the **mpls ldp neighbor targeted** command in global configuration mode. To disable a targeted session, use the **no** form of this command.

mpls ldp neighbor [*vrf vpn-name*] *ip-addr* **targeted** [**ldp**|**tdp**]

no mpls ldp neighbor [*vrf vpn-name*] *ip-addr* [**targeted** [**ldp**|**tdp**]]

Syntax Description

<i>vrf vpn-name</i>	(Optional) VPN routing and forwarding (VRF) instance for a specified neighbor.
<i>ip-addr</i>	Router ID (IP address) that identifies a neighbor.
ldp	(Optional) Specifies Label Distribution Protocol (LDP) as the label protocol for the targeted session.
tdp	(Optional) Specifies Tag Distribution Protocol (TDP) as the label protocol for the targeted session.

Command Default

When the **targeted** keyword is not specified, a targeted session is not set up with the neighbor. For the no form of the command, if the **targeted** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the label protocol for the targeted session, the label protocol specified with the **mpls label protocol** command is used. If the **mpls label protocol** command is not configured, then LDP is used for the targeted session.

Use the **mpls ldp neighbor targeted** command when you need to set up a targeted session and other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you would use this command to set up a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the links directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

Examples

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using TDP as the label protocol:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using LDP as the label protocol:

```
Router(config)# mpls label protocol ldp
```

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

Another way to set up a targeted session using LDP without changing the default label protocol is as follows:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted ldp
```

Related Commands

Commands	Description
mpls ldp neighbor implicit-withdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor password	Configure a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.

mpls ldp nsr

To enable nonstop routing (NSR) for Label Distribution Protocol (LDP) link and targeted sessions, use the **mpls ldp nsr** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mpls ldp nsr

no mpls ldp nsr

This command has no arguments or keywords.

Command Default

NSR for LDP is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Examples

The following example shows how to enable NSR for LDP and verify the configuration:

```
Device(config)# mpls ldp nsr
Device(config)# exit
Device# show mpls ldp parameters

LDP Feature Set Manager: State Initialized
  LDP features:
    Auto-Configuration
    Basic
    ICFM
    IP-over-MPLS
    IGP-Sync
    LLAF
    TCP-MD5-Rollover
    TDP
    NSR
Protocol version: 1
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
LDP NSR: Enabled
```

Related Commands

Command	Description
clear mpls ldp nsr statistics	Clears NSR statistics and counters for LDP sessions.

Command	Description
debug mpls ldp nsr	Enables the display of MPLS LDP NSR debugging events for all NSR sessions or for the specified peer.
show mpls ldp nsr	Displays NSR related information for LDP.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp password fallback

To configure a message digest algorithm 5 (MD5) password for Label Distribution Protocol (LDP) sessions with peers, use the **mpls ldp password fallback** command in global configuration mode. To remove the MD5 password, use the **no** form of this command.

mpls ldp [*vrf vrf-name*] **password fallback** {*key-chain keychain-name* | [0| 7] *password*}

no mpls ldp [*vrf vrf-name*] **password fallback**

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
key-chain <i>keychain-name</i>	(Optional) Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0 7	(Optional) Specifies whether the password that follows is encrypted: <ul style="list-style-type: none"> • 0 specifies an unencrypted password. • 7 specifies an encrypted password.
<i>password</i>	Specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table.

Command Default

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	The key-chain <i>keychain-name</i> keyword-argument pair argument was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the default password for the VRF routing table. The VRF routing table name is specified by the *vrf-name* argument when you configure the **vrf** keyword for the command. If you do not include the **vrf** keyword in the command, the command specifies the default password for the global routing table. The password configured by this command is the password used for sessions between peers, if neither of the following commands applies: the **mpls ldp neighbor password** command or the **mpls ldp password option** command.

If you configure a type 7 (encrypted) password, the password is saved in encrypted form.

If you configure a type 0 (clear-text) password, it can be saved in clear-text form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, then the type 0 password is converted and saved in encrypted form.
- If the **service password-encryption** command is disabled, then the type 0 password is saved in clear-text (nonencrypted) form.

When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in clear-text form is converted into encrypted form, and displayed and saved in encrypted form.

Examples

The following example shows how to configure an MD5 password for an LDP session with peers in VRF vpn1:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls ldp vrf vpn1 password fallback secure
Router(config)# exit
Router#
```

The password, secure, would be encrypted. It is shown here as you would enter it on the command line.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.

Command	Description
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password option

To configure a message digest algorithm 5 (MD5) password for Label Distribution Protocol (LDP) sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **mpls ldp password option** command in global configuration mode. To disable an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **no** form of this command.

mpls ldp[vrf *vrf-name*]**password option** *number* **for** *acl*{**key-chain** *keychain-name*| [**0**| **7**]}*password*
no mpls ldp [*vrf vrf-name*] **password option** *number*

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance configured on the label switch router (LSR).
<i>number</i>	The option number. A comparison of the <i>number</i> argument from several commands by the software sets up the order in which LDP evaluates access lists in the definition of a password for the neighbor. The valid range is from 1 to 32767.
for <i>acl</i>	Specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access lists can be used for the <i>acl</i> argument.
key-chain <i>keychain-name</i>	Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0	(Optional) Specifies that the password is an unencrypted password.
7	(Optional) Specifies that the password is an encrypted password.
<i>password</i>	Specifies the MD5 password to be used for the specified LDP sessions.

Command Default The MD5 password for LDP is disabled.

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.0(32)SRB.
12.0(33)S	This command was modified. The key-chain <i>keychain-name</i> keyword-argument pair was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(1)S	This command was modified. Support for a warning message to be displayed when the MD5 key from the key chain is truncated to the first 25 characters was added.

Usage Guidelines

This command specifies the *password* argument as the MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by an access list specified in the *acl* argument. This password is used if a password is not specified by the **mpls ldp password option** command.

When a configuration includes multiple **mpls ldp password option** commands, the *number* argument defines the order in which the command access lists are evaluated.

A configuration for a VRF can include zero, one, or multiple **mpls ldp password option** commands.

You can specify the passwords as unencrypted text (type 0) or in encrypted format (type 7). If you configure a type 7 password, the password is saved in encrypted form. If you configure a type 0 password, the password can be saved in unencrypted form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, the type 0 password is converted and saved in encrypted form.

When you enter a **show running-config** command, if the **service password-encryption** command is enabled, a password saved in unencrypted form is converted into encrypted form, and is then displayed and saved in encrypted form.

- If the **service password-encryption** command is disabled, the type 0 password is saved in unencrypted form.

The MD5 password and the generated key chain key are limited to 25 characters. If the password and key are more than 25 characters, the encryption is performed only on the first 25 characters and the remaining characters are truncated.

The following is an example of the message displayed when the MD5 password exceeds 25 characters:

```
Router(config)# mpls ldp password option 7 for acl1 password123456789123456789123456789
```

```
% Unencrypted password has been truncated to 25 characters.
```

The following is an example of the message displayed when you configure the **service password-encryption** **key-chain** keyword to generate a password:

```
Router(config)# mpls ldp password option 0 for acl1 key-chain MyKeyChain
```

The key chain “MyKeyChain” consists of a series of keys, each with an acceptance interval:

```
Key-chain MyKeyChain:
  key 1 -- text "first_key"
    accept lifetime (00:00:00 GMT Jan 1 2010) - (18:58:00 GMT Dec 8 2010)
    send lifetime (00:00:00 GMT Jan 1 2010) - (18:56:00 GMT Dec 8 2010)
  key 10 -- text "10_key_ten_begin"
    accept lifetime (18:52:00 GMT Dec 8 2010) - (960 seconds)
    send lifetime (18:55:00 GMT Dec 8 2010) - (600 seconds)
  key 20 -- text "20_key_20_20_20_20_20_20_20_20_20_20_20_20_20_20_"
    accept lifetime (19:02:00 GMT Dec 8 2010) - (960 seconds)
    send lifetime (19:05:00 GMT Dec 8 2010) - (600 seconds)
  key 30 -- text "30_key_30_30_30_30_30_30_30_30_30_30_30_30_30_30_"
    accept lifetime (19:12:00 GMT Dec 8 2010) - (960 seconds)
    send lifetime (19:15:00 GMT Dec 8 2010) - (600 seconds)
  key 40 -- text "key_forty_endgame"
    accept lifetime (19:12:00 GMT Dec 8 2010) - (infinite) [valid now]
    send lifetime (19:15:00 GMT Dec 8 2010) - (infinite) [valid now]
```

A [valid now] key is selected as the current MD5 password. If the selected key exceeds 25 characters, only the first 25 characters are used for the MD5 password. When you configure the **mpls ldp password option** command with the **key-chain** keyword, a notification is displayed to remind you that the MD5 password used may be shorter than the key string:

key-chain

```
% Only first 25 characters of key chain keys can be used for MD5 encryption
```



Note

This notification is displayed every 15 minutes. If it has been less than 15 minutes since you last entered the **mpls ldp password option** command with the keyword, this notification is not displayed.

Whenever LDP truncates a key from a key chain for the encrypted LDP session, a notice message of the following format is also logged:

```
%LDP-5-PWDKEYTRUNC: MD5 digest uses 25 chars of longer transmit/receive key(s) for peer
<Routerid>
```

The following is an example of a log created when a key chain key exceeds 25 characters:

```
*Dec 17 02:45:31.831: %LDP-5-PWDKEYTRUNC: MD5 digest uses 25 chars of longer transmit/receive
key(s) for peer 3.3.3.30
```

Examples

The following example shows how to configure an MD5 password for an LDP session with neighbors whose LDP router IDs are permitted by access list 10:

```
Router> enable
Router# configure terminal
Router(config)# mpls ldp password option 6 for 10
password1
Router(config)# exit
```

The password, called password1 in the above example, is unencrypted.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password required

To specify that Label Distribution Protocol (LDP) must use a password for an attempt to establish a session between LDP peers, use the **mpls ldp password required** command in global configuration mode. To remove the requirement that a password be used for a session with LDP, use the **no** form of this command.

mpls ldp [*vrf vrf-name*] **password required** [*for acl*]

no mpls ldp [*vrf vrf-name*] **password required** [*for acl*]

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
for <i>acl</i>	(Optional) Access list name or number that specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the <i>acl</i> argument.

Command Default

If the **vrf** keyword is not specified in the command, the command applies to the global routing table.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies that LDP must always use a password for an attempt to establish a session. If LDP cannot determine the password to use for an LDP session with a neighbor, an LDP session is not established.

The **vrf** keyword is available when you have configured a VRF on the LSR. If you specify a *vrf-name* argument and a VRF with that name is not configured on the LSR, a warning message is displayed and the command is discarded. If you remove a VRF, you also delete the password configured for that VRF.

Each VRF or global routing table can have zero or one **mpls ldp password required** command.

Examples

The following example shows how to specify that LDP must use a password for an attempt to establish a session between LDP peers:

```
Router> enable
Router# configure terminal
Router(config)# mpls ldp password required
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions
show mpls ldp neighbor password mpls	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password rollover duration

To configure the duration before the new password takes effect on an MPLS label switch router (LSR), use the **mpls ldp password rollover duration** command in global configuration mode. To disable duration of a password rollover, use the **no** form of this command.

mpls ldp [*vrf vrf-name*] **password rollover duration** *minutes*

no mpls ldp [*vrf vrf-name*] **password rollover duration** *minutes*

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a Virtual Private Network (VPN) routing/forwarding instance (VRF) configured on the label switch router (LSR).
<i>minutes</i>	Specifies the time, in minutes, before password rollover occurs on this router. The range is 5 to 65535.

Command Default

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A lossless password rollover takes effect after the configured duration when passwords are configured without the use of a key chain.

Examples

The following example shows how to configure the duration before the new password takes effect on an LSR so there is enough time to successfully change all the passwords on all of the routers. In this example, a duration of 10 minutes is configured before the rollover occurs.

```
mpls ldp password rollover duration 10
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp path-vector maxlength

To set the maximum number of router IDs permitted in a path vector type, length, value (TLV) used to perform path vector loop detection, use the **mpls ldp path-vector maxlength** command in global configuration mode. To return the path vector maximum length to the default behavior, use the **no** form of this command.

mpls ldp path-vector maxlength *number*

no mpls ldp path-vector maxlength

Syntax Description

<i>number</i>	<p>Number from 0 to 254, inclusive, that defines the maximum number of 4-octet router IDs permitted in the path vector.</p> <p>The default behavior configured with the no form of this command is to track and use the value set by the mpls ldp maxhops command (1 to 255).</p> <p>A value of 0 disables the path-vector loop detection feature.</p>
---------------	--

Command Default

If you do not configure this command, the default path vector maximum length value is whatever value is configured for the **mpls ldp maxhops** command. If you reconfigure the maximum hops value, the path vector maximum length value automatically changes to the new maximum hops value. If the **mpls ldp maxhops** command is not configured, the default value is 254.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(19)	This command was introduced.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

When an ATM label switch router (LSR) initiates a request for a label binding, and path vector loop detection is enabled, the request includes a path vector TLV that contains the router ID of the requesting router. Subsequent ATM LSRs along the path to the edge of the ATM label switching region add their router IDs to the path vector before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if a loop is detected by the path vector feature.

Instead, the ATM LSR returns an error message that specifies that a loop has been detected. A loop is detected if either of the following occurs:

- The path vector length in the request equals or exceeds the configured Path Vector Limit value configured by the **mpls ldp path-vector maxlength** command.
- The receiving ATM LSR finds its own router ID within the path vector list.

Like the maximum hop count, the path vector limit threshold is used to prevent forwarding loops in the setting up of label switch path (LSPs) across an ATM region.

If you configured the **mpls ldp loop-detection** command for ATM LSRs that are sending and receiving Label Request and Label Map messages, you might want to inhibit the use of the path vector for loop detection (**mpls ldp path-vector maxlength 0** command).

To return the maximum path vector length to its default value, which is whatever value is configured for the **mpls ldp maxhops** command, use the **no mpls ldp path-vector maxlength** command.

Examples

The following example shows how to set the maximum path vector length to 100 router IDs:

```
configure terminal
mpls ldp path-vector maxlength 100
exit
```

The following example shows the maximum path vector length set to 254, which is verified by you looking at the output from the **show mpls ldp parameters** command or the **show mpls ldp neighbors detail** command:

```
configure terminal
mpls ldp path-vector maxlength 254
exit
Router# show mpls ldp parameters

Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 4
Downstream on Demand Path Vector Limit: 254    !Verifies maximum path-vector length is 254.
!
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: on
Router#
Router# show mpls ldp neighbor detail
Peer LDP Ident: 10.0.3.33:1; Local LDP Ident 10.0.2.93:1
TCP connection: 10.0.3.33.53366 - 10.0.2.93.646
State: Oper; Msgs sent/rcvd: 132/123; Downstream on demand
Up time: 00:24:27; UID: 5; Peer Id 0;
LDP discovery sources:
Switch1.1; Src IP addr: 10.0.3.33
holdtime: 15000 ms, hello interval: 5000 ms
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Clients: TC ATM
Path Vector Loop Detection Peer/Local: On/On
Path Vector Limit Peer/Local: 4/254    ! Verifies the maximum path-vector length is 254.
Router#
```

Related Commands

Command	Description
mpls ldp loop-detection	Enables the LDP optional loop detection mechanism.

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.
show mpls ldp neighbors	Displays the status of LDP sessions.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

mpls ldp router-id [*vrf vrf-name*] *interface* [**force**]

no mpls ldp router-id [*vrf vrf-name*] [*interface* [**force**]]

Cisco CMTS Routers

mpls ldp router-id **gigabitethernet** *slot/subslot/port* [**force**]

no mpls ldp router-id **gigabitethernet** *slot/subslot/port* [**force**]

Syntax Description

<i>vrf vrf-name</i>	(Optional) Selects the interface as the LDP router ID for the named Virtual Private Network (VPN) routing and forwarding (VRF) table. The selected interface must be associated with the named VRF.
<i>interface</i>	The specified interface to be used as the LDP router ID, provided that the interface is operational.
gigabitethernet <i>slot /subslot/port</i>	Specifies the location of the Gigabit Ethernet interface.
force	(Optional) Alters the behavior of the mpls ldp router-id command, as described in the "Usage Guidelines" section.

Command Default

If the **mpls ldp router-id** command is not executed, the router determines the LDP router ID as follows:

- 1 The router examines the IP addresses of all operational interfaces.
- 2 If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
- 3 Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(10)ST	This command was introduced.

Release	Modification
12.0(14)ST	The force keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.4(5)	The vrf vrf-name keyword and argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **mpls ldp router-id** command allows you to use the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

- 1 The router considers all the IP addresses of all operational interfaces.
- 2 If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- If the loopback interface has been explicitly shut down.
- If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

- 1 Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

The following behaviors apply to the default VRF as well as to VRFs that you explicitly configure with the **vrf vrf-name** keyword and argument pair:

- The interface you select as the router ID of the VRF must be associated with the VRF.
- If the interface is no longer associated with the VRF, the **mpls ldp router-id** command that uses the interface is removed.
- If the selected interface is deleted, the **mpls ldp router-id** command that uses the interface is removed.
- If you delete a VRF that you configured, the **mpls ldp router-id** command for the deleted VRF is removed. The default VRF cannot be deleted.

Examples

The following example shows that the POS2/0/0 interface has been specified as the preferred interface for the LDP router ID. The IP address of that interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id pos2/0/0
```

The following example shows that the Ethernet 1/0 interface, which is associated with the VRF vpn-1, is the preferred interface. The IP address of the interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id vrf vpn-1 eth1/0
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp session protection

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration for existing LDP sessions or when new sessions are established, use the **mpls ldp session protection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp session protection [*vrf vpn-name*] [*for acl*] [*duration {infinite| seconds}*]

no mpls ldp session protection [*vrf vpn-name*] [*for acl*] [*duration {infinite| seconds}*]

Syntax Description

vrf <i>vpn-name</i>	(Optional) Specifies a VPN routing and forwarding instance (<i>vpn-name</i>) for accepting labels. This keyword is available when the router has at least one VRF configured.
for <i>acl</i>	(Optional) Specifies a standard IP access control list that contains the prefixes that are to be protected.
duration	(Optional) Specifies the time that the LDP Targeted Hello Adjacency should be retained after a link is lost. Note If you use this keyword, you must select either the infinite keyword or the <i>seconds</i> argument.
infinite	Specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost.
<i>seconds</i>	Specifies the time in seconds that the LDP Targeted Hello Adjacency should be retained after a link is lost. The valid range of values is 30 to 2,147,483 seconds.

Command Default LDP sessions are not established.

Command Modes Global configuration (config)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers

If you issue the **mpls ldp session protection** command without the **duration** keyword, then session protection is enabled for 86400 seconds (24 hours) meaning that the LDP Targeted Hello Adjacency is retained for 24 hours after a link is lost. This is the default timeout.

If you issue the **mpls ldp session protection duration infinite** command, then session protection is enabled forever meaning that the LDP Targeted Hello Adjacency is retained forever after a link is lost.

If you issue the **mpls ldp session protection duration seconds** command, then session protection is enabled for the number of seconds indicated meaning that the LDP Targeted Hello Adjacency is retained for that amount of time. For example, if you issued **mpls ldp session protection duration 100**, then the LDP Targeted Hello Adjacency is retained for 100 seconds after a link is lost.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for LDP sessions for peers whose router IDs are listed in access control list rtr4:

```
Router(config)# mpls ldp session protection for rtr4
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
show mpls ldp neighbor	Displays the contents of the LDP.

mpls ldp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on interfaces for an Open Shortest Path First (OSPF) process or an Intermediate System-to-Intermediate System (IS-IS) process, use the **mpls ldp sync** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp sync

no mpls ldp sync

Syntax Description This command has no arguments or keywords.

Command Default MPLS LDP-IGP synchronization is not enabled on interfaces belonging to the OSPF or IS-IS processes.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.0(30)S	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	12.0(32)SY	This command is supported on interfaces running IS-IS processes in Cisco IOS Release 12.0(32)SY.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
	Cisco IOS XE Release 3.6S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines If the **mpls ldp sync** command is configured, you cannot enter the global **no mpls ip** command. If you want to disable LDP synchronization, you must enter the **no mpls ldp igp sync** command first.

The **mpls ldp sync** command is supported with OSPF or IS-IS. Other IGP's are not supported.

Examples In the following example, MPLS LDP-IGP synchronization is enabled for an OSPF process or an IS-IS process:

```
Router(config-router)# mpls ldp sync
```

Related Commands

Command	Description
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
no mpls ip	Disables hop-by-hop forwarding.
show isis mpls ldp	Displays synchronization and autoconfiguration information about interfaces belonging to IS-IS processes.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp tcp pak-priority

To give high priority to Label Distribution Protocol (LDP) messages sent by a router locally using Transmission Control Protocol (TCP) connections, use the **mpls ldp tcp pak-priority** command in global configuration mode. To keep LDP messages at normal priority, use the **no** form of this command.

mpls ldp tcp pak-priority

no mpls ldp tcp pak-priority

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled.

Command Modes Global configuration (config)

Release	Modification
12.3	This command was introduced.

Usage Guidelines This command allows you to set high priority for LDP messages sent by a router locally using TCP connections. During heavy network traffic, LDP session keepalive messages can be dropped from the outgoing interface output queue. As a result, keepalives can timeout causing LDP sessions to go down.

First, to avoid session loss due to keepalive timeouts, configure the quality of service (QoS) and differentiated services code point (DSCP) for packets with type of service (ToS) bits set to 6. This configuration guarantees that packets with a ToS bit precedence value of 6 receive a specified percentage of the bandwidth of the designated outgoing links. Second, if you still experience a problem, use the **mpls ldp tcp pak-priority** command.



Note Previously established LDP sessions are not affected when you issue the **no mpls ldp tcp pak-priority** or the **mpls ldp tcp pak-priority** command.

Examples The following example gives LDP session messages sent by a router high priority locally:

```
Router(config)# mpls ldp tcp pak-priority
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
debug mpls ldp transport connections	Displays information about the TCP connections used to support LDP sessions.
match ip precedence	Identifies IP precedence values as match criteria.
match mpls experimental	Configures a class map to use the specified value of the EXP field as a match criterion.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

mpls load-balance per-label

To enable the load balancing for the tag-to-tag traffic, use the **mpls load-balance per-label** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls load-balance per-label

no mpls load-balance per-label

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines When you enable load balancing for the tag-to-tag traffic, the traffic is balanced based on the incoming label (per prefix) among Multiprotocol Label Switching (MPLS) interfaces. Each MPLS interface supports an equal number of incoming labels.

You can use the **show mpls ttfib** command to display the incoming label (indicated by an asterisk) that is included in the load balancer.

Examples This example shows how to enable the load balancing for the tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable the load balancing for the tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

Related Commands	Command	Description
	show mpls ttfib	Displays information about the MPLS TTFIB table.

mpls mtu

To set the per-interface Multiprotocol Label Switching (MPLS) maximum transmission unit (MTU) for labeled packets, or to set the maximum MTU on the L3VPN profile, use the **mpls mtu** command in interface configuration mode or L3VPN encapsulation configuration mode respectively. To restore the MPLS MTU to the default value, use the **no** form of this command.

Interface Configuration Mode

mpls mtu [*override*] *bytes*

no mpls mtu

L3VPN Encapsulation Configuration Mode

mpls mtu max

no mpls mtu max

Syntax Description

override	(Optional) Allows you to set the MPLS MTU to a value higher than the interface MTU value on interfaces (such as Ethernet) that have a default interface MTU value of 1580 or less. The override keyword is not available for interface types that do not have a default MTU value of 1580 or less.
<i>bytes</i>	The MTU in bytes includes the label stack in the value.
max	Sets the MPLS MTU value to the maximum value in Generic Router Encapsulation (GRE) tunnels and L3VPN profiles.

Command Default

The default MPLS MTU is the MTU that is configured for the interface.

Command Modes

Interface configuration (config-if) L3VPN encapsulation configuration (config-l3vpn-encap-ip)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to incorporate the new MPLS terminology.
12.2(25)S	This command was modified. The maximum allowable MPLS MTU values were changed. See the “Usage Guidelines for Cisco IOS Release 12.2(25)S” section for more information.

Release	Modification
12.2(27)SBC	This command was modified. The MPLS MTU value cannot be set larger than the interface MTU value. The override keyword was added. See the “Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases” section for more information.
12.(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.6.0	This command was modified. The maximum keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(2)S	This command was modified. This command was made available in L3VPN encapsulation configuration mode. The maximum keyword was replaced with the max keyword.

Usage Guidelines

Usage Guidelines for Cisco IOS Release 12.2(25)S



Caution

Although you can set the MPLS MTU to a value greater than the interface MTU, you can set the MPLS MTU to less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU conditions. A best practice is to set the interface MTU of the core-facing interface to a value greater than either the IP MTU or the interface MTU of the edge-facing interface.

If the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU to a value higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and for interfaces where the MTU is 1500 bytes, the MPLS MTU range is from 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the system will not accept the MPLS MTU setting. You must reconfigure the MPLS MTU setting to conform to the guidelines.

Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases

In Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases, you cannot set the MPLS MTU to a value larger than the interface MTU value. This is to prevent conditions such as dropped packets, data corruption, and high CPU rates.

- If you attempt to set the MPLS MTU to a value higher than the interface MTU value, the software displays the following error, which prompts you to set the interface MTU to a higher value before you set the MPLS MTU value:

```
% Please increase interface mtu to xxxx and then set mpls mtu
```

- If you have an interface with a default interface MTU value of 1580 or less (such as an Ethernet interface), the **mpls mtu** command provides the **override** keyword, which allows you to set the MPLS MTU to a value higher than the interface MTU value. The **override** keyword is not available for interface types that do not have a default interface MTU value of 1580 or less.



Note

The **override** keyword is supported in 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases.

- If you have configuration files with MPLS MTU values that are larger than the interface MTU values and you upgrade to Cisco IOS Release 2.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, or a later release, the software does not change the MPLS MTU value. When you reboot the router, the software accepts whatever values are set for the MPLS MTU and the interface MTU. The following error message is displayed during system initialization:

```
Setting the mpls mtu to xxxx on interface x/x, which is higher than the interface MTU xxxx.  
This could lead to packet forwarding problems including packet drops.  
Set the MPLS MTU values lower than the interface MTU values.
```



Caution

If you do not set the MPLS MTU to a value less than or equal to the interface MTU, data corruption, dropped packets, and high CPU conditions can occur.

- Changing the interface MTU can also modify the IP MTU, Connectionless Network Service (CLNS) MTU, and other MTU values, if they depend on the value of the interface MTU. The Open Shortest Path First (OSPF) routing protocol requires that the IP MTU values match on both ends of the link. Similarly, the Intermediate System-to-Intermediate System (IS-IS) routing protocol requires that the CLNS MTU values match on both ends of the link. If the values on both ends of the link do not match, IS-IS or OSPF cannot complete its initialization.

Usage Guidelines for Cisco IOS XE Release 2.6.0 and Cisco IOS Release 15.1(1)T

- You can set the MPLS MTU value for a GRE tunnel interface to either the default value or the maximum value that is supported by the platform for the interface.
- The **mpls mtu max** command allows previously dropped packets to pass through the GRE tunnel by fragmentation on the underlying physical interface.
- The MPLS MTU value cannot be greater than the interface MTU value for non-GRE tunnels.

Usage Guidelines for Cisco IOS Release 15.1(2)S

- You can use the **mpls mtu max** command in L3VPN encapsulation configuration mode to set the MPLS MTU to the maximum value on L3VPN profiles.
- The **no** form of this command restores the MPLS MTU to the default value.

General Usage Guidelines

- ATM interfaces cannot accommodate packets that exceed the Segmentation and Reassembly (SAR) buffer size because labels are added to the packet. The *bytes* argument refers to the number of bytes in the packet before the addition of any labels. If each label is 4 bytes, the maximum value of bytes on an ATM interface is the physical MTU minus 4*x bytes, where x is the number of labels expected in the received packet.
- If a labeled IPv4 packet exceeds the MPLS MTU size for the interface, the Cisco IOS software fragments the packet. If a labeled non-IPv4 packet exceeds the MPLS MTU size, the packet is dropped.
- All devices on a physical medium must have the same MPLS MTU value in order for MPLS to interoperate.
- The MTU for labeled packets on an interface is determined as follows:
 - If the **mpls mtu bytes** command has been used to configure an MPLS MTU, the MTU for labeled packets is the *bytes* value.
 - Otherwise, the MTU for labeled packets is the default MTU for the interface.
- Because labeling a packet makes it large due to the label stack, you may want the MPLS MTU to be larger than the interface MTU or IP MTU in order to prevent the fragmentation of the labeled packets, which would not be fragmented if they were unlabeled. In Cisco IOS Release 12.2(25)S and later releases, the MPLS MTU cannot be larger than the interface MTU.
- Changing the interface MTU value (using the **mtu** command) can affect the MPLS MTU of the interface. If the MPLS MTU value is the same as the interface MTU value (this is the default value), and you change the interface MTU value, the MPLS MTU value will automatically be set to this new MTU. However, the reverse is not true; changing the MPLS MTU value has no effect on the interface MTU.

Examples

The following example shows how to set the MPLS MTU value:

```
Router(config-if)# mpls mtu 1520
The following example shows the MPLS MTU value for a serial interface:
Router (config)# interface Serial4/0
Router (config-if)# mtu 1520
Router (config-if)# ip unnumbered Loopback0
Router (config-if)# mpls mtu 1510
Router (config-if)# mpls traffic-eng tunnels
Router (config-if)# mpls ip
Router (config-if)# serial restart-delay 0
Router (config-if)# ip rsvp bandwidth 2000 2000
```

The following example displays the maximum labeled packet size for the Fast Ethernet interface, which is common in an MPLS core carrying MPLS Virtual Private Network (VPN) traffic:

```
Router (config)# interface Fastethernet0
Router (config-if)# mpls mtu override 1508
The following example shows how to set the MPLS MTU value to the maximum MTU on L3VPN profiles:
Router (config)# l3vpn encapsulation ip profile
Router (config-l3vpn-encap-ip)# mpls mtu max
```

Related Commands

Command	Description
mtu	Sets the MTU size for the interface.
show mpls interfaces detail	Displays detailed information about the interfaces that are configured for label switching.

mpls netflow egress

To enable Multiprotocol Label Switching (MPLS) egress NetFlow accounting on an interface, use the **mpls netflow egress** command in interface configuration mode. To disable MPLS egress NetFlow accounting, use the **no** form of this command.

mpls netflow egress

no mpls netflow egress

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	12.0(10)ST	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines Use this command to configure the provider edge (PE) to customer edge (CE) interface of a PE router.

Examples The following example shows how to enable MPLS egress NetFlow accounting on the egress PE interface that connects to the CE interface at the destination Virtual Private Network (VPN) site:

```
Router(config-if)# mpls netflow egress
```

Related Commands

Command	Description
debug mpls netflow	Enables debugging of MPLS egress NetFlow accounting.

Command	Description
show mpls forwarding-table	Displays a message that the quick flag is set for all prefixes learned from the MPLS egress NetFlow accounting enabled interface.
show mpls interfaces	Displays the value of the output_feature_state.

mpls oam

To enter MPLS OAM configuration mode for customizing the default behavior of echo packets, use the **mpls oam** command in global configuration mode. To disable MPLS OAM functionality, use the **no** format of this command.

mpls oam

no mpls oam

Syntax Description

This command has no arguments or keywords.

Command Default

Customizing the default behavior of echo packets is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	The no and default keywords were removed.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

After you enter the **mpls oam** command, you can enter the **echo** command in MPLS OAM configuration mode to specify the revision number of the echo packet's default values or to send the vendor's extension type, length, values (TLVs) with the echo packet.

Examples

The following example enters MPLS OAM configuration mode for customizing the default behavior of echo packets:

```
mpls oam
```


Related Commands

Command	Description
echo	Customizes the default behavior of echo packets.
ping mpls	Checks MPLS LSP connectivity.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

mpls prefix-map



Note

Effective with Cisco IOS Release 12.4(20)T, the **mpls prefix-map** command is not available in Cisco IOS software.

To configure a router to use a specified quality of service (QoS) map when a label destination prefix matches the specified access list, use the **mpls prefix-map** command in ATM subinterface submode.

mpls prefix-map *prefix-map* **access-list** *access-list* **cos-map** *cos-map*

Syntax Description

<i>prefix-map</i>	Unique number for a prefix map.
access-list <i>access-list</i>	Unique number for a simple IP access list.
cos-map <i>cos-map</i>	Unique number for a QoS map.

Command Default

No access list is linked to a QoS map.

Command Modes

ATM subinterface submode (config-subif)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.4(20)T	This command was removed.

Usage Guidelines

This **mpls prefix-map** command links an access list to a QoS map when a label distribution prefix matches the specified access list.

Examples

The following example shows how to link an access list to a QoS map:

```
Router(config-subif)# mpls prefix-map 55 access-list 55 cos-map 55
```

Related Commands

Command	Description
show mpls prefix-map	Displays the prefix map used to assign a QoS map to network prefixes that match a standard IP access list.

mpls request-labels for



Note

Effective with Cisco IOS Release 12.4(20)T, the **mpls request-labels for** command is not available in Cisco IOS software.

To restrict the creation of label switched paths (LSPs) through the use of access lists on the label switch controller (LSC) or label edge router (LER), use the **mpls request-labels for** command in global configuration mode. To restrict the creation of LSPs through the use of access lists on the LSC or LER, use the **no** form of this command.

mpls request-labels for *access-list*

no mpls request-labels for

Syntax Description

access-list

A named or numbered standard IP access list.

Command Default

No LSPs are created using access lists on the LCS or LER.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.
12.4(20)T	This command was removed.

Usage Guidelines

The command includes the following usage guidelines:

- You can specify either an access list number or name.
- When you create an access list, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
- If you omit the mask from an IP host address access list specification, 0.0.0.0 is assumed to be the mask.

Examples

The following example shows how to prevent headend label switched controlled virtual circuits (LVCs) from being established from the LSC to all 192.168.x.x destinations. The following commands are added to the LSC configuration:

```
Router(config)# mpls request-labels for 1
Router(config)# access-list 1 deny 192.168.0.0 0.255.255.255
Router(config)# access-list 1 permit any
```

Related Commands

Command	Description
access-list	Creates access lists.
ip access-list	Permits or denies access to IP addresses.

mpls static binding ipv4

To bind a prefix to a local or remote label, use the **mpls static binding ipv4** command in global configuration mode. To remove the binding between the prefix and label, use the **no** form of this command.

mpls static binding ipv4 *prefix mask* {*label*| **input** *label*| **output** *next hop* {**explicit-null**| **implicit-null**| *label*}}

no mpls static binding ipv4 *prefix mask* {*label*| **input** *label*| **output** *next hop* {**explicit-null**| **implicit-null**| *label*}}

Syntax Description

<i>prefix mask</i>	Specifies the prefix and mask to bind to a label. (When you do not use the input or output keyword, the specified label is an incoming label.) Note Without the arguments, the no form of the command removes all static bindings.
<i>label</i>	Binds a prefix or a mask to a local (incoming) label. (When you do not use the input or output keyword, the specified label is an incoming label.)
input <i>label</i>	Binds the specified label to the prefix and mask as a local (incoming) label.
output <i>next hop explicit-null</i>	Binds the Internet Engineering Task Force (IETF) Multiprotocol Label Switching (MPLS) IPv4 explicit null label (0) as a remote (outgoing) label.
output <i>next hop implicit-null</i>	Binds the IETF MPLS implicit null label (3) as a remote (outgoing) label.
output <i>next hop label</i>	Binds the specified label to the prefix/mask as a remote (outgoing) label.

Command Default

Prefixes are not bound to local or remote labels.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The command output changed.
Cisco IOS XE Release 3.5S	This command was implemented on the Cisco ASR 903 series routers.

Usage Guidelines

The **mpls static binding ipv4** command pushes bindings into Label Distribution Protocol (LDP). LDP then needs to match the binding with a route in the Routing Information Base (RIB) or Forwarding Information Base (FIB) before installing forwarding information.

The **mpls static binding ipv4** command installs the specified bindings into the LDP Label Information Base (LIB). LDP will install the binding labels for forwarding use if or when the binding prefix or mask matches a known route.

Static label bindings are not supported for local prefixes, which are connected networks, summarized routes, default routes, and supernets. These prefixes use implicit-null or explicit-null as the local label.

If you do not specify the **input** or the **output** keyword, input (local label) is assumed.

For the **no** form of the command:

- If you specify the command name without any keywords or arguments, all static bindings are removed.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

In the following example, the **mpls static binding ipv4** command configures a static prefix and label binding before the label range is reconfigured to define a range for static assignment. The output of the command indicates that the binding has been accepted, but cannot be used for MPLS forwarding until you configure a range of labels for static assignment that includes that label.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
% Specified label 55 for 10.0.0.0/8 out of configured
% range for static labels. Cannot be used for forwarding until
% range is extended.
Router(config)# end
```

The following **mpls static binding ipv4** commands configure input and output labels for several prefixes:

```
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 input 17
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 output 10.13.0.8 explicit-null
Router(config)# end
```

The following **show mpls static binding ipv4** command displays the configured bindings:

```
Router# show mpls static binding ipv4
```

```
10.0.0.0/8: Incoming label: 55
  Outgoing labels:
    10.0.0.66    2607
10.66.0.0/24: Incoming label: 17
  Outgoing labels:
    10.13.0.8    explicit-null
```

Related Commands

Command	Description
show mpls forwarding-table	Displays labels currently being used for MPLS forwarding.
show mpls label range	Displays statically configured label bindings.