

ignore lsa mospf

To suppress the sending of syslog messages when the router receives link-state advertisement (LSA) Type 6 Multicast OSPF (MOSPF) packets, which are unsupported, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of syslog messages, use the **no** form of this command.

ignore lsa mospf

no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. Each MOSPF packet causes the router to send a syslog message.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Cisco routers do not support LSA Type 6 MOSPF packets, and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages.

Examples

The following example configures the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
router ospf 109
 ignore lsa mospf
```

import ipv4

To configure an import map to import IPv4 prefixes from the global routing table to a VRF table, use the **import ipv4** command in VRF configuration submode. To remove the import map, use the **no** form of this command.

```
import ipv4 unicast | multicast [prefix-limit] route-map
```

```
no import ipv4 unicast | multicast [prefix-limit] route-map
```

Syntax Description

unicast	Specifies IPv4 unicast prefixes to import.
multicast	Specifies IPv4 multicast prefixes to import.
<i>prefix-limit</i>	(Optional) Specifies the number of prefixes to import. The range for this argument is a number from 1 to 2147483647.
<i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.

Defaults

No default behavior or values

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(29)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.

Usage Guidelines

IP prefixes that are defined for import are processed through a match clause in a route map. The prefixes that pass through the route map are imported into the VRF. A maximum of 5 VRFs per router can be configured to import IPv4 prefixes from the global routing table. 1000 prefixes per VRF are imported by default. You can manually configure from 1 to 2147483647 prefixes for each VRF. We recommend that you use caution if you manually configure the prefix import limit. Configuring the router to import too many prefixes can interrupt normal router operation. Only IPv4 unicast and multicast prefixes can be imported to a VRF with this feature. IPv4 prefixes imported into a VRF using this feature cannot be imported into a VPNv4 VRF.

No MPLS or Route Target Configuration is Required

No MPLS or route target (import/export) configuration is required.

Import Behavior

Import actions are triggered when a new routing update is received or when routes are withdrawn. During the initial BGP update period, the import action is postponed to allow BGP to converge more quickly. Once BGP converges, incremental BGP updates are evaluated immediately and qualified prefixes are imported as they are received.

Examples

The following example, beginning in global configuration mode, imports all unicast prefixes from the 10.24.240.0/22 subnet into the VRF named GREEN. An IP prefix list is used to define the imported IPv4 prefixes. The route map is attached to the Ethernet 0 interface. Unicast RPF verification for VRF GREEN is enabled.

```
ip prefix-list COLORADO permit 10.24.240.0/22
!
ip vrf GREEN
 rd 100:10
  import ipv4 unicast 1000 map UNICAST
 exit
route-map UNICAST permit 10
 match ip address prefix-list COLORADO
 exit
interface Ethernet 0
 ip policy route-map UNICAST
 ip verify unicast vrf GREEN permit
end
```

Related Commands

Command	Description
ip verify unicast vrf	Enables Unicast Reverse Path Forwarding verification for the specified VRF.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

inherit peer-policy

To configure a peer policy template to inherit the configuration from another peer policy template, use the **inherit peer-policy** command in policy-template configuration mode. To remove an inherit statement from a peer policy template, use the **no** form of this command.

inherit peer-policy *policy-template sequence-number*

no inherit peer-policy *policy-template sequence-number*

Syntax Description

<i>peer-policy</i>	Name of the peer policy template to be inherited.
<i>sequence-number</i>	Sequence number that sets the order in which the peer policy template is evaluated. Like a route-map sequence number, the lowest sequence number is evaluated first.

Defaults

No default behavior or values

Command Modes

Policy-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Usage Guidelines

The **inherit peer-policy** command is used to configure a peer policy template to inherit the configuration of another peer policy template. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number. However, peer policy templates do not fall through. Every sequence is evaluated. If a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.



Note

A Border Gateway Protocol (BGP) routing process cannot be configured to be a member of a peer group and to use peer templates for group configurations. You must use one method or the other. We recommend peer templates because they provide improved performance and scalability.

Examples

In the following example, a peer policy template named CUSTOMER-A is created. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in
Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

inherit peer-session

To configure a peer session template to inherit the configuration from another peer session template, use the **inherit peer-session** command in session-template configuration mode. To remove an inherit statement from a peer session template, use the **no** form of this command.

inherit peer-session *template-name*

no inherit peer-session *template-name*

Syntax Description

<i>template-name</i>	Name of the peer session template to inherit.
----------------------	---

Defaults

No default behavior or values

Command Modes

Session-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **inherit peer-session** command is used to configure a peer session template to inherit the configuration of another peer session template. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each indirectly inherited session template can also contain an indirectly inherited template. So, a peer can directly inherit only one peer session template and indirectly inherit up to seven additional indirectly inherited peer session templates, allowing you to apply up to a maximum of eight inherited peer session configurations.



Note

If you attempt to configure more than one inherit statement with a single peer session template, an error message will be displayed.

Indirectly inherited peer session templates are evaluated first, and the directly applied (locally configured) peer session template is evaluated last. If a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template. In other words, an overlapping statement from a local configuration will override the statement from the inherited configuration.

Examples

In the following example, a peer session template named CORE1 is created. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	Creates a peer session template and enters session-template configuration mode.

input-queue

The **input-queue** command defines the number of received, but not yet processed RIP update packets contained in the Routing Information Protocol (RIP) input queue. Use the **input-queue** command in router configuration mode. To remove the configured depth and restore the default depth, use the **no** form of this command.

input-queue *depth*

no input-queue

Syntax Description	<i>depth</i>	Numerical value associated with the maximum number of packets in the RIP input queue. The larger the numerical value, the larger the depth of the queue. The range is from 0 to 1024. The default is 50.
---------------------------	--------------	--

Defaults	A depth of 50.
-----------------	----------------

Command Modes	Router configuration
----------------------	----------------------

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

Usage Guidelines

Consider using the **input-queue** command if you have a high-end router that is sending at high speed to a low-speed router that might not be able to receive at the high speed. Configuring this command will help prevent the routing table from losing information.

Another way to prevent the routing table from losing information is to use the **output-delay** command to change the interpacket delay for RIP updates.

Examples

The following example sets the depth of the RIP input queue to 100:

```
router rip
 input-queue 100
```

Related Commands	Command	Description
	output-delay	Changes the interpacket delay for RIP updates sent.

ip as-path access-list

To configure an autonomous system path filter using a regular expression, use the **ip as-path access-list** command in global configuration mode. To delete the autonomous system path filter and remove it from the running configuration file, use the **no** form of this command.

```
ip as-path access-list acl-number permit | deny regex
```

```
no ip as-path access-list acl-number
```

Syntax Description

<i>acl-number</i>	Number from 1 to 500 that specifies the as-path access-list number.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
<i>regex</i>	Regular expression that defines the as-path filter.
Note	Refer to the “Regular Expressions” appendix in the <i>Cisco IOS Terminal Services Configuration Guide</i> for information about configuring regular expressions.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	The range of values that can be entered for the <i>acl-number</i> argument was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The range values that can be entered for the <i>acl-number</i> argument was increased from 199 to 500 in Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **ip as-path access-list** command is configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the **permit** or **deny** condition applies. The autonomous system path should not contain the local autonomous system number.

Examples

In the following example, an autonomous system path access list (number 500) is defined to configure the router to not advertise any path through or from autonomous system 65535 to the 10.20.2.2 neighbor:

```
Router(config)# ip as-path access-list 500 deny _65535_
Router(config)# ip as-path access-list 500 deny ^65535$
Router(config)# !
Router(config)# router bgp 50000
Router(config-router)# neighbor 192.168.1.1 remote-as 65535
```

ip as-path access-list

```
Router(config-router)# neighbor 10.20.2.2 remote-as 40000
Router(config-router)# neighbor 10.20.2.2 filter-list 1 out
Router(config-router)# end
```

In the following example, the router is configured to deny all updates with private autonomous system paths:

```
Router(config)# ip as-path access-list 1 deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
Router(config)# ip as-path access-list 1 permit .*
```

Related Commands

Command	Description
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Applies a filter list to the specified neighbor.
neighbor prefix-list	Applies a prefix list to the specified neighbor.

ip authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **ip authentication key-chain eigrp** command in interface configuration mode. To disable such authentication, use the **no** form of this command.

ip authentication key-chain eigrp *as-number key-chain*

no ip authentication key-chain eigrp *as-number key-chain*

Syntax Description

<i>as-number</i>	Autonomous system number to which the authentication applies.
<i>key-chain</i>	Name of the authentication key chain.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example applies authentication to autonomous system 2 and identifies a key chain named SPORTS:

```
ip authentication key-chain eigrp 2 SPORTS
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication mode eigrp	Specifies the type of authentication used in EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ip authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the **ip authentication mode eigrp** command in interface configuration mode. To disable that type of authentication, use the **no** form of this command.

ip authentication mode eigrp *as-number* **md5**

no ip authentication mode eigrp *as-number* **md5**

Syntax Description

<i>as-number</i>	Autonomous system number.
md5	Keyed Message Digest 5 (MD5) authentication.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP packets in autonomous system 10:

```
ip authentication mode eigrp 10 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ip bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip bandwidth-percent eigrp *as-number percent*

no ip bandwidth-percent eigrp *as-number percent*

Syntax Description	<i>as-number</i>	Autonomous system number.
	<i>percent</i>	Percent of bandwidth that EIGRP may use.

Defaults 50 percent

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines EIGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples The following example allows EIGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
interface serial 0
 bandwidth 56
 ip bandwidth-percent eigrp 209 75
```

Related Commands	Command	Description
	bandwidth (interface)	Sets a bandwidth value for an interface.

ip bgp fast-external-fallover

To configure per-interface fast external fallover, use the **ip bgp fast-external-fallover** command in interface configuration mode. To remove a per-interface fast external fallover configuration, use the **no** form of this command.

ip bgp fast-external-fallover [permit | deny]

no ip bgp fast-external-fallover [permit | deny]

Syntax Description

permit	Allows per-interface fast external fallover.
deny	Prevents per-interface fast external fallover.

Defaults

Global fast external fallover is enabled by default in Cisco IOS software.

Command Modes

Interface configuration

Command History

Release	Modification
12.0ST	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.

Usage Guidelines

The **ip bgp fast-external-fallover** command is used to configure per-interface fast external fallover, overriding the global configuration. Entering the **permit** keyword enables fast external fallover. Entering the **deny** keyword disables fast external fallover. Entering the **no** form of this command, returns the router to the global configuration.

Examples

The following example enables per-interface fast-external-fallover on interface Ethernet 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip bgp fast-external-fallover permit
```

Related Commands

Command	Description
bgp fast-external-fallover	Configures global BGP fast external fall over.

ip bgp-community new-format

To configure BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number), use the **ip bgp-community new-format** command in global configuration mode. To configure BGP to display communities as a 32-bit number, use the **no** form of this command.

ip bgp-community new-format

no ip bgp-community new-format

Syntax Description

This command has no argument or keywords.

Defaults

BGP communities (also when entered in the AA:NN format) are displayed as a 32-bit numbers if this command is not enabled or if the **no** form is entered.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The **ip bgp-community new-format** command is used to configure the local router to display BGP communities in the AA:NN format to conform with RFC-1997. This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange. However, expanded IP community lists that match locally configured regular expressions may need to be updated to match on the AA:NN format instead of the 32-bit number.

RFC 1997, *BGP Communities Attribute*, specifies that a BGP community is made up of two parts that are each 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number defined by the network operator.

Examples

In the following example, a router that uses the 32-bit number community format is upgraded to use the AA:NN format:

```
Router(config)# ip bgp-community new-format
```

The following sample output shows how BGP community numbers are displayed when the **ip bgp-community new-format** command is enabled:

```
Router# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  10.0.33.35
  35
  10.0.33.35 from 10.0.33.35 (192.168.3.3)
    Origin incomplete, metric 10, localpref 100, valid, external
    Community: 1:1
```

■ ip bgp-community new-format

```
Local
 0.0.0.0 from 0.0.0.0 (10.0.33.34)
  Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

ip community-list

To create or configure a Border Gateway Protocol (BGP) community list and to control access to it, use the **ip community-list command** in global configuration command. To delete the community list, use the **no** form of this command.

```
ip community-list { standard | standard list-name { deny | permit } [community-number] [AA:NN]
  [internet] [local-AS] [no-advertise] [no-export] } | { expanded | expanded list-name { deny |
  permit } regexp }
```

```
no ip community-list standard | expanded | { expanded | standard } list-name
```

Syntax Description

<i>standard</i>	Configures a standard community list using a number from 1 to 99 to identify one or more permit or deny groups of communities.
standard <i>list-name</i>	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
<i>community-number</i>	(Optional) Specifies a community as a 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.
<i>AA:NN</i>	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.
local-as	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
<i>expanded</i>	Configures an expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded <i>list-name</i>	Configures a named expanded community list.
<i>regexp</i>	Configures a regular expression that is used to specify a pattern to match against an input string.
Note	Regular expressions can be used only with expanded community lists

Defaults

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the [neighbor send-community](#) command.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the [set community](#) command.

Once a permit value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values.

Community values entered in the new format (AA:NN) are converted to 32-bit numbers if the [ip bgp-community new-format](#) command is not enabled on the local router.

Defaults

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0	Support for the local-as community was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the [ip bgp-community new-format](#) command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the [neighbor send-community](#) command is configured for the specified neighbor. The BGP community attribute is defined in [RFC-1997](#) and [RFC-1998](#).

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in.

Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the *Regular Expressions* appendix of the *Cisco IOS Terminal Services Configuration Guide*.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

In the following example, a standard community list is configured that permits routes that from network 10 in autonomous system 50000:

```
Router(config)# ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Router(config)# ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Router(config)# ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list standard RED permit local-AS
Router(config)# ip community-list standard RED permit 40000:20
```

In the following example, an expanded community list is configured that will deny routes that carry communities from any private autonomous system:

```
Router(config)# ip community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

In the following example, a named expanded community list configured that denies routes from network 1 through 99 in autonomous system 50000:

```
Router(config)# ip community-list expanded BLUE deny 50000:[0-9][0-9]_
```

Related Commands

Command	Description
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set community	Sets the BGP communities attribute.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.

Command	Description
show ip bgp community	Displays routes that belong to specified BGP communities.
show ip bgp regexp	Displays routes that match a locally configured regular expression.

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** command in global configuration mode. To remove a route, use the **no** form of this command.

ip default-network *network-number*

no ip default-network *network-number*

Syntax Description

<i>network-number</i>	Number of the network.
-----------------------	------------------------

Defaults

If the router has a directly connected interface onto the specified network, the dynamic routing protocols running on that router will generate (or source) a default route. For Router Information Protocol (RIP), this is flagged as the pseudonetwork 0.0.0.0; for Interior Gateway Routing Protocol (IGRP), it is the network itself, flagged as an exterior route.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software uses both administrative distance and metric information to determine the default route. Multiple **ip default-network** commands can be given. All candidate default routes, both static (that is, flagged by the **ip default-network** command) and dynamic, appear in the routing table preceded by an asterisk.

If the IP routing table indicates that the specified network number is subnetted and a nonzero subnet number is specified, then the system will automatically configure a static summary route. This static summary route is configured instead of a default network. The effect of the static summary route is to cause traffic destined for subnets that are not explicitly listed in the IP routing table to be routed using the specified subnet.

Examples

The following example defines a static route to network 10.0.0.0 as the static default route:

```
ip route 10.0.0.0 255.0.0.0 10.108.3.4
ip default-network 10.0.0.0
```

If the following command was issued on a router not connected to network 10.140.0.0, the software might choose the path to that network as a default route when the network appeared in the routing table:

```
ip default-network 10.140.0.0
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip dvmrp metric

To configure the metric associated with a set of destinations for Distance Vector Multicast Routing Protocol (DVMRP) reports, use the **ip dvmrp metric** command in interface configuration mode. To disable this function, use the **no** form of this command.

```
ip dvmrp metric metric [route-map map-name] [mbgp] [mobile] [list access-list-number]
[protocol process-id] | dvmrp
```

```
no ip dvmrp metric metric [route-map map-name] [mbgp] [mobile] [list access-list-number]
[protocol process-id] | dvmrp
```

Syntax Description

<i>metric</i>	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
route-map <i>map-name</i>	(Optional) Names a route map. If you specify this keyword and argument, only the destinations that match the route map are reported with the configured metric. Unicast routes are subject to route map conditions before being injected into DVMRP. Route maps cannot be used for DVMRP routes.
mbgp	(Optional) Configures redistribution of only IP version 4 (IPv4) multicast routes into DVMRP.
<i>mobile</i>	(Optional) Configures redistribution of only mobile routes into DVMRP.
list <i>access-list-number</i>	(Optional) Names an access list. If you specify this keyword and argument, only the multicast destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.
<i>protocol</i>	(Optional) Name of a unicast routing protocol. Available protocols are: bgp , dvmrp , eigrp , isis , mobile , odr , ospf , rip , or static . If you specify these values, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
<i>process-id</i>	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured <i>metric</i> value, or filtered.

Defaults

No metric value is preconfigured. Only directly connected subnets and networks are advertised to neighboring DVMRP routers.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
11.1	The route-map keyword was added.

Release	Modification
11.1(20)CC	This mbgp keyword was added.
12.0(7)T	This mbgp keyword was added.

Usage Guidelines

When Protocol Independent Multicast (PIM) is configured on an interface and DVMRP neighbors are discovered, the Cisco IOS software sends DVMRP report messages for directly connected networks. The **ip dvmrp metric** command enables DVMRP report messages for multicast destinations that match the access list. Usually, the metric for these routes is 1. Under certain circumstances, you might want to tailor the metric used for various unicast routes. This command lets you configure the metric associated with a set of destinations for report messages sent out this interface.

You can use the *access-list-number* argument in conjunction with the *protocol* and *process-id* arguments to selectively list the destinations learned from a given routing protocol.

To display DVMRP activity, use the **debug ip dvmrp** command.

Examples

The following example connects a PIM cloud to a DVMRP cloud. Access list 1 permits the sending of DVMRP reports to the DVMRP routers advertising all sources in the 172.16.35.0 network with a metric of 1. Access list 2 permits all other destinations, but the metric of 0 means that no DVMRP reports are sent for these destinations.

```
access-list 1 permit 172.16.35.0 0.0.0.255
access-list 1 deny 0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
interface tunnel 0
 ip dvmrp metric 1 list 1
 ip dvmrp metric 0 list 2
```

The following example redistributes IPv4 multicast routes into DVMRP neighbors with a metric of 1:

```
interface tunnel 0
 ip dvmrp metric 1 mbgp
```

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
ip dvmrp accept-filter	Configures an acceptance filter for incoming DVMRP reports.

ip extcommunity-list

To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.

Global Configuration Mode CLI

```
ip extcommunity-list expanded-list | expanded list-name {permit | deny} [regular-expression] |
standard-list | standard list-name {permit | deny} [rt value] [soo value]
```

```
no ip extcommunity-list expanded-list | expanded list-name | standard-list | standard list-name
```

To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode.

```
ip extcommunity-list expanded-list | expanded list-name | standard-list | standard list-name
```

```
no ip extcommunity-list expanded-list | expanded list-name | standard-list | standard list-name
```

Expanded IP Extended Community-List Configuration Mode CLI

```
[sequence-number] deny [regular-expression] | exit | permit [regular-expression] | resequence
[starting-sequence] [sequence-increment]
```

```
default {sequence-number | deny [regular-expression] | exit | permit [regular-expression] |
resequence [starting-sequence] [sequence-increment]}
```

```
no {sequence-number | deny [regular-expression] | permit [regular-expression] | resequence
[starting-sequence] [sequence-increment]}
```

Standard IP Extended Community-List Configuration Mode CLI

```
[sequence-number] deny [rt value] [soo value] | exit | permit [rt value] [soo value] | resequence
[starting-sequence] [sequence-increment]
```

```
default {sequence-number | deny [rt value] [soo value] | exit | permit [rt value] [soo value] |
resequence [starting-sequence] [sequence-increment]}
```

```
no {sequence-number | deny [rt value] [soo value] | permit [rt value] [soo value] | resequence
[starting-sequence] [sequence-increment]}
```

Syntax Description

<i>expanded-list</i>	An expanded list number from 100 to 500 that identifies one or more permit or deny groups of extended communities.
<i>standard-list</i>	A standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.
expanded <i>list-name</i>	Creates an expanded named extended community list and enters IP Extended community-list configuration mode.
standard <i>list-name</i>	Creates a standard named extended community list and enters IP Extended community-list configuration mode.

permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
<i>regular-expression</i>	(Optional) An input string pattern to match against.
rt	(Optional) Specifies the route target (RT) extended community attribute. The rt keyword can be configured only with standard extended community lists and not expanded community lists.
soo	(Optional) Specifies the site of origin (SOO) extended community attribute. The soo keyword can be configured only with standard extended community lists and not expanded community lists.
<i>value</i>	Specifies the route target or site of origin extended community value. This value can be entered in one of the following formats: <ul style="list-style-type: none"> autonomous-system-number : network-number ip-address : network-number
<i>sequence-number</i>	(Optional) The sequence number of a named or numbered extended community list. This value can be a number from 1 to 2147483647.
default	(Optional) Sets a keyword or argument to default behavior or value.
exit	(Optional) Exits from IP Extended community-list configuration mode.
resequence	(Optional) Changes the sequences of extended community list entries to the default sequence numbering or to the specified sequence numbering. Extended community entries are sequenced by ten number increments by default.
<i>starting-sequence</i>	(Optional) Specifies the number for the first entry in an extended community list.
<i>sequence-increment</i>	(Optional) Specifies the increment range for each subsequent extended community entry.

Defaults

Extended community exchange is not enabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command.

Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.

Extended community list entries start with the number 10 and increment by ten for each subsequent entry when no sequence number is specified, when default behavior is configured, and when an extended community list is resequenced without specifying the first entry number or the increment range for subsequent entries.

Command Modes

Global configuration
IP Extended community-list configuration

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.

Release	Modification
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(25)S	Support for the following was added in Cisco IOS Release 12.2(25)S: <ul style="list-style-type: none"> • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.3(11)T	Support for the following was added in Cisco IOS Release 12.3(11)T: <ul style="list-style-type: none"> • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists

Usage Guidelines

The **ip extcommunity-list** command is used to configure named or numbered extended community lists. Extended community attributes are used to filter routes for VPN routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). All of the standard rules of access lists apply to the configuration of extended community lists. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists. Regular expressions are supported in expanded extended community lists. For information about configuring regular expressions, see the *Regular Expressions* appendix of the *Cisco IOS Terminal Services Configuration Guide*.

Route Target Extended Community Attribute

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

Site of Origin Extended Community Attribute

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.

IP Extended Community-List Configuration Mode

Named and numbered extended community lists can be configured in IP Extended community-list configuration mode. To enter IP Extended community-list configuration mode, enter the **ip extcommunity-list** command with either the **expanded** or **standard** keyword followed by the extended community list name. This configuration mode supports all of the functions that are available in global configuration mode. In addition, you can perform the following operations:

- Configure sequence numbers for extended community list entries
- Resequence existing sequence numbers for extended community list entries
- Configure an extended community list to use default values

Extended Community List Processing

When multiple values are configured in the same extended community list statement, a logical AND condition is created. All extended community values must match to satisfy an AND condition. When multiple values are configured in separate extended community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

Standard Extended Community-List Configuration Example

In the following example, an extended community list is configured that permits routes from route target 64512:10 and site of origin 65400:20 and denies routes from route target 65424:30 and site of origin 64524:40. List 1 shows a logical OR condition; the first match is processed. List 2 shows a logical AND condition; all community values must match in order for list 2 to be processed.

```
Router(config)# ip extcommunity-list 1 permit rt 64512:10
Router(config)# ip extcommunity-list 1 permit soo 65400:20
Router(config)# ip extcommunity-list 2 deny rt 65424:30 soo 64524:40
```

Expanded Extended Community-List Configuration Example

In the following example, an expanded extended community list is configured to deny advertisements from any path through or from autonomous system 65534 from being advertised to the 192.168.1.2 neighbor:

```
Router(config)# ip extcommunity-list 500 deny _65412_
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 172.16.1.1 remote-as 65412
Router(config-router-af)# neighbor 172.16.1.1 neighbor send-community extended
Router(config-router-af)# neighbor 192.168.1.2 remote-as 65534
Router(config-router-af)# neighbor 192.168.1.2 neighbor send-community extended
Router(config-router-af)# end
```

Named Extended Community-List Configuration Example

In the following example, a named extended community list is configured that will permit routes only from route target 65505:50. All other routes are implicitly denied.

```
Router(config)# ip extcommunity-list standard NAMED_LIST permit rt 65505:50
```

IP Extended Community-List Configuration Mode Example

In the following example, an expanded named extended community list is configured in IP Extended community-list configuration mode. A list entry is created with a sequence number 10 that will permit a route target or route origin pattern that matches any network number extended community from autonomous system 65412.

```
Router(config)# ip extcommunity-list RED
Router(config-extcom-list)# 10 permit 65412:[0-9][0-9][0-9][0-9][0-9]_
Router(config-extcom-list)# exit
```

Extended Community-List Resequencing Example

In the following example, the first list entry is resequenced to the number 50 and each subsequent entry is configured to increment by 100:

```
Router(config)# ip extcommunity-list BLUE
Router(config-extcom-list)# resequence 50 100
Router(config-extcom-list)# exit
```

Related Commands	Command	Description
	export map	Configures an export route map for a VRF.
	match extcommunity	Matches a BGP VPN extended community list.
	set extcommunity	Sets BGP extended community attributes.
	show ip extcommunity-list	Displays routes that are permitted by the extended community list.
	show route-map	Displays configured route maps.

ip fast-convergence

To reduce packet loss when the metric of a path is changed, or to fast-flood Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs), use the **ip fast-convergence** command in router configuration mode. To disable packet loss reduction or fast-flooding, use the **no** version of this command.

ip fast-convergence

no ip fast-convergence



Note

Effective with Release 12.3(7)T, the **ip fast-convergence** command is replaced by the **fast-flood** command. See the **fast-flood** command for more information.

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced to reduce packet loss.
12.2(10)T	This command was modified to enable fast-flooding.
12.3(7)T	This command was replaced by the fast-flood command.

Usage Guidelines

To reduce packet loss when the metric of a path is changed, use the **ip fast-convergence** command. Entering the **ip fast-convergence** command is especially helpful when Multiprotocol Label Switching (MPLS) traffic engineering with Fast Reroute (FFR) is deployed.

If you are running Cisco IOS Release 12.2(11)T or a later release, you can enter the **ip fast-convergence** command to configure the router to flood the first five LSPs that invoke SPF before running SPF. When you speed up the LSP flooding process, you improve overall network convergence time. We recommend that you enable the fast-flooding of LSPs before the router runs the SPF computation, in order to achieve a faster convergence time.

Examples

In the following example, the **ip fast-convergence** command is entered to configure the router to flood the first five LSPs that invoke SPF, before the SPF computation is started. When the **show running-configuration** command is entered, the output confirms that fast-flooding has been enabled on the router.

```
Router> enable
Router# configure terminal
Router(config)# router isis
```

```
Router(config-router)# ip fast-convergence
Router(config-router)# end
Router# show running-configuration

fast-flood
```

Related Commands

Command	Description
incremental-spf	Enables incremental SPF.

ip hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process designated by an autonomous system number, use the **ip hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip hello-interval eigrp *as-number seconds*

no ip hello-interval eigrp *as-number seconds*

Syntax Description

<i>as-number</i>	Autonomous system number.
<i>seconds</i>	Hello interval (in seconds). The range is from 1 to 65535.

Defaults

For low-speed, nonbroadcast multiaccess (NBMA) networks: 60 seconds
 For all other networks: 5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds:

```
interface ethernet 0
 ip hello-interval eigrp 109 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hold-time eigrp	Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.

ip hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) routing process designated by the autonomous system number, use the **ip hold-time eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip hold-time eigrp *as-number seconds*

no ip hold-time eigrp *as-number seconds*

Syntax Description

<i>as-number</i>	Autonomous system number.
<i>seconds</i>	Hold time (in seconds). The range is from 1 to 65535.

Defaults

For low-speed, nonbroadcast multiaccess (NBMA) networks: 180 seconds
 For all other networks: 15 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

```
interface ethernet 0
 ip hold-time eigrp 109 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hello-interval eigrp	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

ip local policy route-map

To identify a route map to use for local policy routing, use the **ip local policy route-map** command in global configuration mode. To disable local policy routing, use the **no** form of this command.

ip local policy route-map *map-tag*

no ip local policy route-map *map-tag*

Syntax Description	<i>map-tag</i>	Name of the route map to use for local policy routing. The name must match a <i>map-tag</i> value specified by a route-map command.
---------------------------	----------------	--

Defaults	Packets that are generated by the router are not policy routed.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	Packets that are generated by the router are not normally policy routed. However, you can use this command to policy route such packets. You might enable local policy routing if you want packets originated at the router to take a route other than the obvious shortest path.
-------------------------	---

The **ip local policy route-map** command identifies a route map to use for local policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which packets should be policy routed. The **set** commands specify the *set actions*—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples	The following example sends packets with a destination IP address matching that allowed by extended access list 131 to the router at IP address 172.130.3.20:
-----------------	---

```
ip local policy route-map xyz
!
route-map xyz
 match ip address 131
 set ip next-hop 172.130.3.20
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
show ip local policy	Displays the route map used for local policy routing.

ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command in global configuration mode. To remove the buffer, use the **no** form of this command.

```
ip multicast [vrf vrf-name] cache-headers [rtp]
```

```
no ip multicast [vrf vrf-name] cache-headers
```

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1	The rtp keyword was added.
12.0(23)S	The vrf keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

You can store IP multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- User Datagram Protocol (UDP) port numbers
- Packet length



Note

This command allocates a circular buffer of approximately 32 KB. Do not configure this command if you are low on memory.

Use the **show ip mpacket** command to display the buffer.

Examples

The following example allocates a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache header buffer.
show ip mpacket quality	Displays an RTP data quality based on packets captured in the IP multicast cache header buffer.

ip next-hop-self eigrp

To instruct EIGRP that the IP next hop is itself, use the **ip next-hop-self eigrp** command in interface configuration mode. To instruct EIGRP to use the received next hop rather than itself, use the **no** form of this command.

ip next-hop-self eigrp *autonomous-system-number*

no ip next-hop-self eigrp *autonomous-system-number*

Syntax Description

autonomous-system-number Autonomous system number.

Defaults

EIGRP always sets the IP next-hop value to be itself.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

EIGRP will, by default, set the IP next-hop value to be itself for routes that it is advertising, even when advertising those routes back out the same interface where it learned them. To change this default, you must use the **no ip next-hop-self eigrp** interface configuration command to instruct EIGRP to use the received next hop value when advertising these routes. Some exceptions to this guideline follow:

- If spoke-to-spoke dynamic tunnels are not wanted, then the **no ip next-hop-self eigrp** command is not needed.
- If spoke-to-spoke dynamic tunnels are wanted, then you must use process switching on the tunnel interface on the spoke routers. Otherwise, you will need to use a different routing protocol over Dynamic Multipoint VPN (DMVPN).

Examples

The following example changes the default IP next hop value and instructs EIGRP to use the received next hop value:

```
interface serial 0
no ip next-hop-self eigrp 101
```

ip ospf area

To enable OSPFv2 on an interface, use the **ip ospf area** command in interface configuration mode. To disable OSPFv2 on the interface, use the **no** form of this command.

ip ospf *process-id* **area** *area-id* [**secondaries none**]

no ip ospf *process-id* **area** [**secondaries none**]

Syntax Description

<i>process-id</i>	A decimal in the range from 1 to 65535 that identifies the process ID.
<i>area-id</i>	A decimal value in the range from 0 to 4294967295, or an IP address.
secondaries none	(Optional) Prevents secondary IP addresses on the interface from being advertised.

Defaults

If the **secondaries** keyword is entered in the **no** form of this command, the secondary IP addresses will be advertised. If the **secondaries** keyword is not present, OSPFv2 will be disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(1)SB	This command was integrated into Cisco IOS Release 12.2(1)SB.

Usage Guidelines

OSPF is enabled on an interface when the network address for the interface matches the range of addresses that is specified by the **network area** command that is entered in router configuration mode. For Cisco IOS releases 12.0(29)S, 12.3(11)T and 12.2(1)SB, you can enable OSPFv2 explicitly on an interface with the **ip ospf area** command that is entered in interface configuration mode. This capability simplifies the configuration of unnumbered interfaces with different areas.

The **ip ospf area** command that is entered in interface configuration mode will take supersede the effects of the **network area** command. Therefore, an interface that is configured with the **ip ospf area** command in interface configuration mode will not be affected by the **network area** command.



Note

If you later disable the **ip ospf area** command, the interface still will run OSPFv2 as long as its network address matches the range of addresses that are specified by the **network area** command.

Examples

The following example enables OSPFv2 on Ethernet interface 0/0/2 and prevents secondary IP addresses from being advertised:

```
Router(config)# interface Ethernet0/0/2
Router(config-if)# ip ospf 10 area 0 secondaries none
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface configuration mode.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.
show ip ospf interface	Displays OSPF-related interface information.

ip ospf authentication

To specify the authentication type for an interface, use the **ip ospf authentication** command in interface configuration mode. To remove the authentication type for an interface, use the **no** form of this command.

ip ospf authentication [message-digest | null]

no ip ospf authentication

Syntax Description	message-digest	(Optional) Specifies that message-digest authentication will be used.
	null	(Optional) No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.

Defaults The area default is no authentication (null authentication).

Command Modes Interface configuration

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines Before using the **ip ospf authentication** command, configure a password for the interface using the **ip ospf authentication-key** command. If you use the **ip ospf authentication message-digest** command, configure the message-digest key for the interface with the **ip ospf message-digest-key** command.

For backward compatibility, authentication type for an area is still supported. If the authentication type is not specified for an interface, the authentication type for the area will be used (the area default is null authentication).

Examples The following example enables message-digest authentication:

```
ip ospf authentication message-digest
```

Related Commands	Command	Description
	area authentication	Enables authentication for an OSPF area.
	ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
	ip ospf message-digest-key	Enables OSPF MD5 authentication.

ip ospf authentication-key

To assign a password to be used by neighboring routers that are using the OSPF simple password authentication, use the **ip ospf authentication-key** command in interface configuration mode. To remove a previously assigned OSPF password, use the **no** form of this command.

ip ospf authentication-key *password*

no ip ospf authentication-key

Syntax Description

<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.
-----------------	--

Defaults

No password is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The password created by this command is used as a “key” that is inserted directly into the OSPF header when the Cisco IOS software originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.



Note

The Cisco IOS software will use this key only when authentication is enabled for an area with the **area authentication** router configuration command.

Examples

The following example enables the authentication key with the string yourpass:

```
ip ospf authentication-key yourpass
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies authentication type for an interface.

ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** command in interface configuration mode. To reset the path cost to the default value, use the **no** form of this command.

ip ospf cost *interface-cost*

no ip ospf cost *interface-cost*

Syntax Description	<i>interface-cost</i>	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.
---------------------------	-----------------------	--

Defaults	No default cost is predefined.
-----------------	--------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	<p>You can set the metric manually using this command, if you need to change the default. Using the bandwidth command changes the link cost as long as this command is not used.</p> <p>The link-state metric is advertised as the link cost in the router link advertisement. We do not support type of service (ToS), so you can assign only one cost per interface.</p> <p>In general, the path cost is calculated using the following formula:</p> $10^8 / \text{bandwidth}$ <p>Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.</p> <ul style="list-style-type: none"> • 56-kbps serial link—Default cost is 1785 • 64-kbps serial link—Default cost is 1562 • T1 (1.544-Mbps serial link)—Default cost is 64 • E1 (2.048-Mbps serial link)—Default cost is 48 • 4-Mbps Token Ring—Default cost is 25 • Ethernet—Default cost is 10 • 16-Mbps Token Ring—Default cost is 6 • FDDI—Default cost is 1 • X25—Default cost is 5208 • Asynchronous—Default cost is 10,000
-------------------------	---

- ATM— Default cost is 1

Examples

The following example sets the interface cost value to 65:

```
ip ospf cost 65
```

ip ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an OSPF interface, use the **ip ospf database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ip ospf database-filter all out

no ip ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command performs the same function that the **neighbor database-filter** command performs on a neighbor basis.

Examples

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ip ospf database-filter all out
```

Related Commands

Command	Description
neighbor database-filter	Filters outgoing LSAs to an OSPF neighbor.

ip ospf dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the **ip ospf dead-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip ospf dead-interval { *seconds* | **minimal hello-multiplier multiplier** }

no ip ospf dead-interval

Syntax Description

<i>seconds</i>	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network.
minimal	Sets the dead interval to 1 second. Using this keyword requires that the hello-multiplier keyword and <i>multiplier</i> argument are also configured.
hello-multiplier multiplier	Integer value in the range from 3 to 20, representing the number of hello packets sent during 1 second.

Defaults

seconds: Four times the interval set by the **ip ospf hello-interval** command.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(23)S	The minimal keyword, hello-multiplier keyword and <i>multiplier</i> argument were added to allow OSPF Support for Fast Hello Packets.

Usage Guidelines

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network.

Specifying a smaller dead interval (*seconds*) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

OSPF Support for Fast Hello Packets

By specifying the **minimal** and **hello-multiplier** keywords with a *multiplier* argument, you are enabling OSPF fast hello packets. The **minimal** keyword sets the dead interval to 1 second, and the **hello-multiplier** value sets the number of hello packets sent during that 1 second, thus providing subsecond or “fast” hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

Use the **show ip ospf interface** command to verify the dead interval and fast hello interval.

Examples

The following example sets the OSPF dead interval to 20 seconds:

```
interface ethernet 1
 ip ospf dead-interval 20
```

The following example configures OSPF fast hello packets; the dead interval is 1 second and there are 5 hello packets sent every second:

```
interface ethernet 1
 ip ospf dead-interval minimal hello-multiplier 5
```

Related Commands

Command	Description
ip ospf hello-interval	Interval between hello packets that the Cisco IOS software sends on the interface.
show ip ospf interface	Displays OSPF-related information.

ip ospf demand-circuit

To configure OSPF to treat the interface as an OSPF demand circuit, use the **ip ospf demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ip ospf demand-circuit

no ip ospf demand-circuit

Syntax Description This command has no arguments or keywords.

Defaults The circuit is not a demand circuit.

Command Modes Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must be configured with this command.

Examples

The following example sets the configuration for an ISDN on-demand circuit:

```
router ospf 1
 network 10.0.3.0 255.255.255.0 area 0
 interface BRI0
 ip ospf demand-circuit
```

ip ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ip ospf flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip ospf flood-reduction

no ip ospf flood-reduction

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines All routers supporting the OSPF demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples The following example reduces the flooding of unnecessary LSAs on serial interface 0:

```
interface serial 0
 ip ospf flood-reduction
```

Related Commands	Command	Description
	show ip ospf interface	Displays OSPF-related interface information.
	show ip ospf neighbor	Displays OSPF-neighbor information on a per-interface basis.

ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the **ip ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Syntax Description	<i>seconds</i>	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.
---------------------------	----------------	--

Defaults	10 seconds (Ethernet) 30 seconds (nonbroadcast)
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.
-------------------------	--

Examples The following example sets the interval between hello packets to 15 seconds:

```
interface ethernet 1
 ip ospf hello-interval 15
```

Related Commands	Command	Description
	ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.

ip ospf lls

To enable Link-Local Signaling (LLS) on an interface, regardless of the router-level LLS setting, use the **ip ospf lls** command in interface configuration mode. To reconfigure the router-level LLS setting on the specific interface, use the **default** or **no** version of this command.

ip ospf lls [disable]

{no | default} ip ospf lls [disable]

Syntax Description

no	Restores the default LLS setting for the interface that has been configured at the router level.
default	Specified interface will inherit the global (router level) LLS settings.
disable	(Optional) Disables LLS on a specified interface regardless of the global (router level) setting.

Defaults

LLS is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

By default, each Open Shortest Path First (OSPF) interface inherits the LLS setting from the router level. The **ip ospf lls** interface-level command takes precedence over the **capability lls** router-level command. For example, if you have entered the **no capability lls** command to disable LLS at the router level, you can use the **ip ospf lls** command to selectively enable LLS for specific interfaces, in order to allow the router to enable OSPF nonstop forwarding (NSF) awareness only for these specified interfaces.

To unconfigure the interface LLS setting, enter either the **default ip ospf lls** command or the **no ip ospf lls** command to restore the default LLS setting for the interface that has been configured at the router level. For example, if the **capability lls** command is enabled (by default) at the router level, you can use either the **default ip ospf lls** command or the **no ip ospf lls** command to disable LLS on specific interfaces, for instance, to interoperate on network segments where there are routers that do not properly handle LLS.



Note

If the network is running OSPF with the LLS feature enabled by default, LLS is globally enabled for all interfaces. If a router in the network is connected to a non-Cisco device that is not in compliance with RFC 2328, there may be network difficulties involving the forming of OSPF neighbors. In this situation, we recommend that you use the **ip ospf lls** command with the **disable** keyword to disable LLS on the router that is connected to the non-Cisco device.

Examples

In following example, LLS is disabled on Ethernet interface 2/0:

```
Router(config)# interface Ethernet2/0
Router(config-if)# ip address 10.1.145.2 255.255.0.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# ip ospf message-digest-key 1 md5 testing
Router(config-if)# ip ospf lls disable
```

Related Commands

Command	Description
capability lls	Enables the use of the LLS data block in originated OSPF packets and reenables OSPF NSF awareness.
show ip ospf interface	Displays OSPF-related interface information.

ip ospf message-digest-key

To enable OSPF Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key** command in interface configuration mode. To remove an old MD5 key, use the **no** form of this command.

ip ospf message-digest-key *key-id encryption-type md5 key*

no ip ospf message-digest-key *key-id*

Syntax Description		
	<i>key-id</i>	An identifier in the range from 1 to 255.
	<i>encryption-type</i>	Specifies the encryption level. The range is from 0 to 7. 0 specifies no encryption. 7 specifies a proprietary level of encryption.
	<i>key</i>	Alphanumeric password of up to 16 bytes.

Defaults OSPF MD5 authentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
 ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
 ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
```

ip ospf message-digest-key

```
no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

**Note**

If the **service password-encryption** command is not used when implementing OSPF MD5 authentication, the MD5 secret will be stored as plain text in NVRAM.

Examples

The following example sets a new key 19 with the password *8ry4222*:

```
interface ethernet 1
 ip ospf message-digest-key 10 md5 xv560qle
 ip ospf message-digest-key 19 md5 8ry4222
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies authentication type for an interface.
service password-encryption	Encrypts a password.

ip ospf mtu-ignore

To disable OSPF MTU mismatch detection on receiving DBD packets, use the **ip ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Syntax Description This command has no keywords or arguments.

Defaults OSPF MTU mismatch detection is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(3)	This command was introduced.

Usage Guidelines OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange Database Descriptor (DBD) packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Examples The following example disables MTU mismatch detection on receiving DBD packets:

```
interface serial 0/0
 ip ospf mtu-ignore
```

ip ospf name-lookup

To configure OSPF to look up Domain Name System (DNS) names for use in all OSPF **show EXEC** command displays, use the **ip ospf name-lookup** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ospf name-lookup

no ip ospf name-lookup

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples The following example configures OSPF to look up DNS names for use in all OSPF **show EXEC** command displays:

```
ip ospf name-lookup
```

ip ospf network

To configure the OSPF network type to a type other than the default for a given medium, use the **ip ospf network** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
ip ospf network { broadcast | non-broadcast | { point-to-multipoint [non-broadcast] |
point-to-point } }
```

```
no ip ospf network
```

Syntax Description		
broadcast	Sets the network type to broadcast.	
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).	
point-to-multipoint [non-broadcast]	Sets the network type to point-to-multipoint. The optional non-broadcast keyword sets the point-to-multipoint network to be nonbroadcast. If you use the non-broadcast keyword, the neighbor command is required.	
point-to-point	Sets the network type to point-to-point.	

Defaults Depends on the network type.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The point-to-multipoint keyword was added.
	11.3 AA	The non-broadcast keyword used with the point-to-multipoint keyword was added.

Usage Guidelines Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure nonbroadcast multiaccess networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service (SMDS)) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, there are other configurations where this assumption is not true. For example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, this command will be ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

The following example sets your OSPF network as a broadcast network:

```
interface serial 0
 ip address 192.168.77.17 255.255.255.0
 ip ospf network broadcast
 encapsulation frame-relay
```

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.
x25 map	Sets up the LAN protocols-to-remote host mapping.

ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ip ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf priority *number-value*

no ip ospf priority *number-value*

Syntax Description	<i>number-value</i>	A number value that specifies the priority of the router. The range is from 0 to 255.
---------------------------	---------------------	---

Defaults	Priority of 1
-----------------	---------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure OSPF for nonbroadcast networks using the **neighbor** router configuration command for OSPF.

Examples

The following example sets the router priority value to 4:

```
interface ethernet 0
 ip ospf priority 4
```

Related Commands	Command	Description
	ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.
	neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.

ip ospf resync-timeout

To configure how long the router will wait before taking a neighbor adjacency down if the out-of-band resynchronization (oob-resync) has not taken place since the time a restart signal (OSPF Hello packet with RS-bit set) was received from the neighbor, use the **ip ospf resync-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip ospf resync-timeout *seconds*

no ip ospf resync-timeout

Syntax Description

<i>seconds</i>	Number of seconds the router will wait before taking a neighbor adjacency down if the out-of-band resynchronization (oob-resync) has not taken place since the time a restart signal (OSPF Hello packet with RS-bit set) was received from the neighbor. The value is in the range from 1 to 65535 seconds. The default value is 40 seconds or the value set for the OSPF dead interval for the interface, whichever is greater.
----------------	--

Defaults

The default value is 40 seconds or the value set for the interface's OSPF dead interval, whichever is greater.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When an OSPF nonstop forwarding (NSF) router performs a route processor (RP) switchover, it notifies its neighbors, via a special Hello packet, of such action and requests that each neighbor help resynchronize the Link State Database.

When a neighbor (that is NSF-aware) receives the special Hello packet from the NSF-capable router, it starts a resync timeout timer and waits to synchronize its database with the NSF-capable router. If the NSF-capable router does not initiate the database resynchronization process before the resync-timeout timer expires, the NSF-aware neighbor will take down the adjacency with the NSF-capable router.

By default, the resync-timeout timer is set to 40 seconds or the dead interval of the interface, whichever is greater. (By default, the dead interval is 4 times the hello interval; the hello interval defaults to 10 seconds for Ethernet or 30 seconds for nonbroadcast.) The **ip ospf resync-timeout** command allows the resync-timeout to be changed and independent of the dead interval or default value.

Examples

This example sets the OSPF resync-timeout interval to 50 seconds:

```
interface GigabitEthernet 6/0/0
 ip ospf resync-timeout 50
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval at which hello packets must not be seen before neighbors declare the router down.
ip ospf hello-interval	Sets the interval between hello packets that the software sends on the interface.

ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Syntax Description	<i>seconds</i>	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.
---------------------------	----------------	---

Defaults	5 seconds
-----------------	-----------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	<p>When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.</p> <p>The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.</p>
-------------------------	--

Examples	The following example sets the retransmit interval value to 8 seconds:
-----------------	--

```
interface ethernet 2
 ip ospf retransmit-interval 8
```

ip ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ip ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Syntax Description	<i>seconds</i>	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.
---------------------------	----------------	--

Defaults	1 second
-----------------	----------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples The following example sets the retransmit delay value to 3 seconds:

```
interface ethernet 0
 ip ospf transmit-delay 3
```

