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 [**disable**]

no ip ospf flood-reduction

Syntax Description		
disable	(Optional) Disables the suppressing of unnecessary flooding of LSAs in stable topologies.	
	Note This keyword is available only in virtual network interface mode.	

Defaults

This command is disabled by default.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. The **disable** keyword was added. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

All routers supporting the Open Shortest Path First (OSPF) demand circuit are compatible and can interact with routers supporting flooding reduction.

If the **ip ospf flood-reduction** command is enabled for a virtual network and you want to disable it, use the **disable** keyword in virtual network interface configuration mode.

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

seconds	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 (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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 **no** or **default** 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	Inherits the global (router level) LLS settings for the interface that has been specified.
disable	(Optional) Disables LLS on a specified interface regardless of the global (router level) setting.

Defaults

LLS is enabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

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.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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 md5

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key md5** 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

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

Defaults

OSPF MD5 authentication is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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
 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 xvv560qle
 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 Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (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 [**disable**]

no ip ospf mtu-ignore

Syntax Description	disable	(Optional) Causes OSPF MTU mismatch detection to occur (because ignoring OSPF MTU mismatch detection is being disabled).
		✎ **Note** This keyword is available only in virtual network interface mode.

Defaults OSPF MTU mismatch detection is enabled.

Command Modes Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. The **disable** keyword was added. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange 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.

If the **ip ospf mtu-ignore** command is enabled for a virtual network and you want to disable it, use the **disable** keyword in virtual network interface configuration mode.

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

Usage Guidelines   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 Open Shortest Path First (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 (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **point-to-multipoint** keyword was added.
11.3AA	The **non-broadcast** keyword used with the **point-to-multipoint** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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.

Cisco IOS IP Routing: OSPF Command Reference

ip ospf prefix-suppression

To prevent Open Shortest Path First (OSPF) from advertising all IP prefixes that belong to a specific interface, except for prefixes that are associated with secondary IP addresses, use the **ip ospf prefix-suppression** command in interface configuration mode. To remove the per-interface configuration from the interface and allow the interface to inherit the IP prefix suppression setting from the router configuration, use the **no** form of this command.

ip ospf prefix-suppression [**disable**]

no ip ospf prefix-suppression

Syntax Description

disable	(Optional) Specifies that OSPF will advertise the interface IP prefix, regardless of the router mode configuration for IP prefix suppression.

Command Default All IP prefixes that are associated with the interface are advertised.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines You can suppress IP prefixes on a per-interface basis for all interface types by entering the **ip ospf prefix-suppression** command in interface configuration mode.

When the **ip ospf prefix-suppression** command is configured, it takes precedence over the **prefix-suppression** router configuration command. If the **prefix-suppression** router configuration command has been entered, the interfaces for the specified OSPF process will inherit the prefix suppression setting from the router configuration command.

When you enter the **ip ospf prefix-suppression** command, prefix generation for any interface type, including loopbacks and passive interfaces, is suppressed. Only prefixes associated with secondary IP addressees remain unaffected.

Examples The following example suppresses all IP prefixes, except for those associated with secondary IP addresses, for GigabitEthernet interface 1/1/1:

```
interface gigabitethernet 1/1/1
 ip ospf prefix-suppression
```

Related Commands	Command	Description
	prefix-suppression	Prevents OSPF from advertising all IP prefixes except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces for a specific OSPF process.

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

Syntax Description

number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default   Priority of 1

Command Modes   Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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 Open Shortest Path First (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 (Open Shortest Path First [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

seconds	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.

Command Default   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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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

seconds	Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

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.

The setting of the *seconds* argument should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should also be conservative, or needless LSA retransmissions may occur. The value should be larger for serial lines and virtual links.

Note It is recommended to use the same value for the *seconds* argument on neighbor OSPF routers. Using inconsistent values on neighbor routers can cause needless LSA retransmissions.

Examples

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

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

ip ospf shutdown

To initiate an Open Shortest Path First (OSPF) protocol graceful shutdown at the interface level, use the **ip ospf shutdown** command in interface configuration mode. To restart the OSPF protocol on an interface, use the **no** form of this command.

ip ospf shutdown [**disable**]

no ip ospf shutdown

Syntax Description

disable	(Optional) Disables the initiation of the OSPF graceful shutdown at the interface level; OSPF stays active at the interface level.

> ✎
> **Note** This keyword is available only in virtual network interface mode.

Command Default OSPF stays active at the interface level.

Command Modes Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.2S	This command was modified. The **disable** keyword was added. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines Use the **ip ospf shutdown** command to put OSPF in shutdown mode under a specific interface.

If the **ip ospf shutdown** command is enabled for a virtual network and you want to disable it, use the **disable** keyword in virtual network interface configuration mode.

Examples The following example shows how to initiate a graceful shutdown of the OSPF protocol on Ethernet interface 0/2:

```
Router(config)# interface ethernet 0/2
Router(config-if)# ip ospf shutdown
```

Related Commands

Command	Description
shutdown (router ospf)	Initiates a graceful shutdown of the OSPF protocol under the current instance.

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

seconds	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 (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

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
```

ip ospf ttl-security

To configure the Time-to-Live (TTL) security check feature on a specific interface, use the **ip ospf ttl-security** command in interface configuration mode. To disable TTL security on an interface, use the **no** form of this command.

ip ospf ttl-security [**hops** *hop-count* | **disable**]

no ip ospf ttl-security

Syntax Description

hops *hop-count*	(Optional) Configures the maximum number of IP hops. The *hop-count* argument range is from 1 to 254.
disable	(Optional) Disables TTL security on an interface.

Command Default

TTL security is disabled on all Open Shortest Path First (OSPF) interfaces.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip ospf ttl-security** command to configure TTL security on a specific interface.

The **disable** keyword can be used to disable TTL security on a specific interface but is only useful if the **ttl-security all-interfaces** command was used in router mode to first configure TTL security on all OSPF interfaces. In this way, all OSPF interfaces can be configured with TTL security and then individual interfaces can be disabled. This can save time as opposed to configuring each interface one-by-one from the start.

Examples

The following example shows how to effectively use the **disable** keyword to disable TTL security on Ethernet interface 0/0 after the feature has first been configured on all OSPF interfaces:

```
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# ttl-security all-interfaces
Router(config-router)# exit
Router(config)# interface ethernet 0/0
Router(config-if)# ip ospf ttl-security disable
```

Related Commands	Command	Description
	ttl-security all-interfaces	Configures TTL security check on all OSPF interfaces.

limit retransmissions

To change or remove the limit in the number of retransmissions of database exchange and update packets for both demand and non-demand circuits, use the **limit retransmissions** command in router configuration mode. To reset the maximum number of retransmissions back to the default value of 24, use the **no** form of this command.

> **limit retransmissions** [**dc** {*max-number* | **disable**}] [**non-dc** {*max-number* | **disable**}]

> **no limit transmissions** [**dc** | **non-dc**]

Syntax Description		
dc	Demand circuit retransmissions.	
max-number	Maximum number of retransmissions. Range from 1 to 255.	
non-dc	Nondemand circuit retransmissions.	
disable	Disables or removes the limit to the number of retransmissions.	

Defaults Maximum number of retransmissions is 24.

Command Modes Router configuration

Command History	Release	Modification
	12.2(11)T	This command was introduced.

Usage Guidelines Cisco IOS Release 12.2(4)T added a limit to the number of retransmissions of database exchange and update packets for both demand and nondemand circuits. The retransmission of these packets stops once this retry limit is reached, thus preventing unnecessary use of the link in continual retransmission of the packets if, for some reason, a neighbor is not responding during adjacency forming.

The limit for both demand circuit and nondemand circuit retransmissions is 24.

The **limit-retransmissions** command allows you to either remove (disable) the limit or change the maximum number of retransmissions to be a number from 1 to 255. The configuration of this command provides for backward compatibility for previous or other releases of Cisco IOS Software or other routers that do not have this feature.

Note The limit to the number of retransmissions does not apply for update packets on nonbroadcast multiaccess (NBMA) point-to-multipoint direct circuits. In this situation, the dead timer is used to end communication with nonresponding neighbors and thus stop the retransmissions.

Cisco IOS IP Routing: OSPF Command Reference

Examples

The following example shows how to set the maximum number of demand circuit retransmissions to 10:

```
limit retransmissions dc 10
```

The following example shows how to remove the limit for the number of demand circuit retransmissions:

```
limit retransmissions dc disable
```

The following example shows how to set the maximum number of demand circuit retransmissions to 10 and to set the maximum number of nondemand circuit retransmissions to 20:

```
limit retransmissions dc 10 non-dc 20
```

The following example shows how to set the maximum number of demand circuit retransmissions to 10, and to remove the limit for the number of nondemand circuit retransmissions:

```
limit retransmissions dc 10 non-dc disable
```

The following example shows how to reset both the demand circuit and nondemand circuit maximum number of retransmissions back to the default of 24:

```
no limit retransmissions
```

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

local-rib-criteria

To specify that the OSPF local Routing Information Base (RIB) will be used for route validation, use the **local-rib-criteria** command in router configuration mode. To remove local RIB route validation, use the **no** form of this command.

> **local-rib-criteria** [**forwarding-address**] [**inter-area-summary**] [**nssa-translation**]

> **no local-rib-criteria** [**forwarding-address**] [**inter-area-summary**] [**nssa-translation**]

Syntax Description		
	forwarding-address	(Optional) Specifies that the local RIB is to be used only for route validation criteria for external or NSSA forwarding addresses.
	inter-area-summary	(Optional) Specifies that the local RIB is to be used only for route validation criteria for inter-area summaries.
	nssa-translation	(Optional) Specifies that the local RIB is to be used only for route validation criteria for NSSA translation.

Command Default   The global RIB (not the local RIB) is used for route validation.

Command Modes   Router configuration (config-router)

Command History	Release	Modification
	12.4(15)T	This command was introduced.

Usage Guidelines   If the **local-rib-criteria** is command is entered without any optional keywords, the local RIB will be used as criteria for all of the options (forwarding address, inter-area summary, and NSSA translation).

You can enter the **local-rib-criteria** command with one or more of the optional keywords to configure the OSPF routing process to use the local RIB only for forwarding address, inter-area-summary, or NSSA translation route generation.

Note   It is recommended to keep the default behavior (the global RIB is used for route validation). Although entering the **local-rib-criteria** command alone or with one or more of the optional keywords may result in slightly faster network convergence in some cases, you may potentially cause a problem such as a routing loop or black hole.

Note   When the **forwarding-address** keyword is entered to specify that forwarding-address verification is modified to use the local RIB, packet forwarding will still be dependent on the global RIB. If the global RIB contains a more preferred or more specific route from a different protocol, this preferred route still will still be used for packet forwarding.

Examples   The following example specifies that the local RIB should be used as the criteria for NSSA translation:

```
router ospf 23
 local-rib-criteria nssa-translation
```

The following example enables all local RIB criteria options:

```
router ospf 1
 local-rib-criteria
```

The following example specifies that the local RIB will be used only for inter-area summary route generation:

```
router ospf 1
 local-rib-criteria inter-area-summary
```

log-adjacency-changes

To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

> **log-adjacency-changes** [**detail**]

> **no log-adjacency-changes** [**detail**]

Syntax Description	**detail**	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default   Enabled

Command Modes   Router configuration

Command History	Release	Modification
	11.2	This command was introduced as **ospf log-adjacency-changes**.
	12.1	The **ospf** keyword was omitted and the **detail** keyword was added.
	12.2(15)T	Support for IPv6 was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   This command allows you to know about OSPF neighbors going up or down without turning on the **debug ip ospf packet** command or the **debug ipv6 ospf adjacency** command. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output than the **debug** command provides. The **log-adjacency-changes** command is on by default but only up/down (full/down) events are reported, unless the **detail** keyword is also used.

Examples   The following example configures the router to send a syslog message when an OSPF neighbor state changes:

```
log-adjacency-changes detail
```

Related Commands	Command	Description
	debug ip ospf packet	Displays information about each OSPF packet received for IPv4.
	debug ipv6 ospf	Displays debugging information for OSPF for IPv6.

max-lsa

To limit the number of nonself-generated link-state advertisements (LSAs) that an Open Shortest Path First (OSPF) routing process can keep in the OSPF link-state database (LSDB), use the **max-lsa** command in router configuration mode. To remove the limit of non self-generated LSAs that an OSPF routing process can keep in the OSPF LSDB, use the **no** form of this command.

> **max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*]

> **no max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*]

Syntax Description

maximum-number	Maximum number of nonself-generated LSAs the OSPF process can keep in the OSPF LSBD.
threshold-percentage	(Optional) The percentage of the maximum LSA number, as specified by the *maximum-number* argument, at which a warning message is logged. The default is 75 percent.
warning-only	(Optional) Specifies that only a warning message is sent when the maximum limit for LSAs is exceeded. Disabled by default.
ignore-time *minutes*	(Optional) Specifies the time, in minutes, to ignore all neighbors after the maximum limit of LSAs has been exceeded. The default is 5 minutes.
ignore-count *count-number*	(Optional) Specifies the number of times the OSPF process can consecutively be placed into the ignore state. The default is 5 times.
reset-time *minutes*	(Optional) Specifies the time, in minutes, after which the ignore count is reset to zero. The default is 10 minutes.

Defaults

The number of nonself-generated LSAs that an OSPF routing process can keep in the OSPF LSDB is not limited.

threshold-percentage: 75 percent
warning-only warning message: disabled
ignore-time *minutes*: 5 minutes
ignore-count *count-number*: 5 times
reset-time *minutes*: *10 minutes*

Command Modes

Router 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.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To prevent the OSPF process from endlessly changing from the normal state of operation to the ignore state as a result of the LSA count exceeding the maximum configured number immediately after it returns from the ignore state to the normal state of operation, the OSPF process keeps a counter on how many times the process went into the ignore state. This counter is called the ignore count. If the ignore count exceeds the maximum number of LSAs that is specified by the **ignore-count** keyword and *counter-number* argument, the OSPF process remains in the ignore state permanently. To return the OSPF process to the state of normal operation, enter the **clear ip ospf** command.

If the router is placed into a permanent ignore state, we recommend that you identify and correct the cause of the problem involving the router that is generating the LSAs, or, if possible, increase the limit that has been configured by the **max-lsa** command before you try to bring the router back into normal operation.

If the router that has generated large numbers of LSAs is not reachable, these LSAs cannot be removed from the OSPF area and domain. As a result, any other router leaving the ignore state and returning to normal operation may reach the ignore state again. We recommend that you take one of the following actions in order to bring the router back into the network:

- Temporarily increase the LSA limit to account for the stale LSAs.

- Wait until the stale LSAs are removed as a result of reaching their maximum age.

- Make sure that the router that has generated the large number of LSAs is connected to the network and is no longer generating large numbers of LSAs.

When the **warning-only** keyword is used, the OSPF process never enters the ignore state. When the LSA count exceeds the maximum limit that is specified by the *maximum-number* argument, only an error message is logged and the OSPF process continues in its normal operation.

When the **max-lsa** command is entered for the first time or when any of the parameters of the command are changed, the OSPF process undergoes a soft-reset procedure.

Examples

The following example sets a limit of 12,000 LSAs that can be received before the OSPF process enters the ignore state:

```
Router(config)# router ospf 100
Router(config-router)# router-id 209.165.201.0
Router(config-router)# log-adjacency-changes
Router(config-router)# max-lsa 12000
Router(config-router)# network 209.165.201.1 255.255.255.255
```

In the following example, an OSPF process has remained in the ignore state permanently. When the **clear ip ospf** command is entered the OSPF process returns to the state of normal operation and clears redistribution based on the OSPF routing process ID.

```
Router(config-router)# clear ip ospf 100 process
```

Related Commands

Command	Description
clear ip ospf	Clears redistribution based on the OSPF routing process ID.

max-metric router-lsa

To configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric router-lsa** command in router address family topology or router configuration mode. To disable the advertisement of a maximum metric, use the **no** form of this command.

> **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** {*seconds* | **wait-for-bgp**}] [**summary-lsa** [*max-metric-value*]]

> **no max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** {*seconds* | **wait-for-bgp**}] [**summary-lsa** [*max-metric-value*]]

Syntax Description		
	external-lsa	(Optional) Configures the router to override the external LSA metric with the maximum metric value.
	max-metric-value	(Optional) Maximum metric value for LSAs. The configurable range is from 1 to 16777215. The default value is 16711680.
	include-stub	(Optional) Configures the router to advertise the maximum metric for stub links in router LSAs.
	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.
	seconds	(Optional) Maximum metric value for the specified time interval. The configurable range is from 5 to 86400 seconds. There is no default timer value for this configuration option.
	wait-for-bgp	(Optional) Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.
	summary-lsa	(Optional) Configures the router to override the summary LSA metric with the maximum metric value.

Command Default Router link-state advertisements (LSAs) are originated with normal link metrics.

Command Modes Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)

Command History	Release	Modification
	12.0(15)S	This command was introduced.
	12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.4(10)	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.

Cisco IOS IP Routing: OSPF Command Reference ■

Release	Modification
12.4(11)T	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB2	The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family topology configuration mode. The **include-stub**, **summary-lsa**, and **external-lsa** keywords and the *max-metric-value* argument were made available under router configuration mode.

Usage Guidelines

Enabling the **max-metric router-lsa** command will cause a router to originate LSAs with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links, which allows BGP routing tables to converge without attracting transit traffic (if there are not alternate lower cost paths around the router). The router will advertise accurate (normal) metrics after the configured or default timers expire or after BGP sends a notification that routing tables have converged.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

The **max-metric router-lsa** command is useful in the following situations:

- Reloading a router. After a router is reloaded, Interior Gateway Protocols (IGPs) converge very quickly, and other routers may try to forward traffic through the newly reloaded router. If the router is still building BGP routing tables, packets destined for other networks that the router has not learned through BGP may be dropped. In the case of an Internet backbone router, a large number of packets may be dropped.

- Introducing a router into a network without routing traffic through it. You may want to connect a router to an OSPF network but not want real traffic flowing through the router if there are better alternate paths. If there are no alternate paths, this router would still accept transit traffic as before.

- Gracefully removing a router from a network. This feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down.

Note You should not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

Note In older OSPF implementations (RFC 1247 and earlier implementations), the router link costs in received LSAs with a metric of LSInfinity are not used during SPF calculations, which means that no transit traffic will be sent to the routers that originate these LSAs.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **max-metric router-lsa** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples

The following example configures a router that is running OSPF to advertise a maximum metric for 100 seconds:

```
Router(config)# router ospf 100
Router(config-router)# max-metric router-lsa on-startup 100
```

The following example configures a router to advertise a maximum metric until BGP routing tables converge or until the default timer expires (600 seconds):

```
Router(config)# router ospf 100
Router(config-router)# max-metric router-lsa on-startup wait-for-bgp
```

The following example configures a router that is running OSPF to advertise a maximum metric, which causes neighbor routers to select alternate paths for transit traffic before the router shuts down:

```
Router(config)# router ospf 100
Router(config-router)# max-metric router-lsa
Router(config-router)# end
```

The following example configures stub links to be advertised with the maximum-metric in routers LSAs.

```
Router(config)# router ospf 1
Router(config-router)# router-id 10.1.1.1
Router(config-router)# max-metric router-lsa include-stub
Router(config-router)# end
```

Entering the **show ip ospf max-metric** command with the **include-stub** keyword displays output that confirms that stub links are advertised with the maximum metric.

```
Router# show ip ospf max-metric

Routing Process "ospf 1" with ID 10.1.1.1
 Start time: 00:00:03.524, Time elapsed: 01:02:28.292
 Originating router-LSAs with maximum metric
    Condition: always, State: active
    Advertise stub links with maximum metric in router-LSAs
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf database	Displays lists of information related to the OSPF database for a specific router.

Cisco IOS IP Routing: OSPF Command Reference ■

neighbor (OSPF)

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **neighbor** command in router address family topology or router configuration mode. To remove a configuration, use the **no** form of this command.

> **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all**]

> **no neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all**]

Syntax Description		
	ip-address	Interface IP address of the neighbor.
	priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
	poll-interval *seconds*	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces. The range is from 0 to 4294967295 seconds.
	cost *number*	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the **ip ospf cost** command. For point-to-multipoint interfaces, the cost keyword and the *number* argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
	database-filter all	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

Command Default   This command is disabled by default. No configuration is specified.

Command Modes   Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)

Command History	Release	Modification
	10.0	This command was introduced.
	11.3AA	The **cost** keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SRB	This command was made available in router address family topology configuration mode.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network. Refer to the **x25 map** and **frame-relay map** commands in the "X.25 Commands" and "Frame Relay Commands" chapters, respectively, in the *Cisco IOS Wide-Area Networking Command Reference* for more detail.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the Router Dead Interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

Note   You cannot use the **neighbor (OSPF)** command to specify an Open Shortest Path First (OSPF) neighbor on non-broadcast networks within an OSPF Virtual Private Network (VPN) routing instance.

Prior to Cisco IOS Release 12.0, the **neighbor** command applied to NBMA networks only. With Release 12.0, the **neighbor** command applies to NBMA networks and point-to-multipoint networks. On NBMA networks, the **cost** keyword is not accepted.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **neighbor** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples   The following example declares a router at address 192.168.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
 neighbor 192.168.3.4 priority 1 poll-interval 180
```

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

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

Related Commands	Command	Description
	ip ospf priority	Sets the router priority, which helps determine the designated router for this network.

neighbor database-filter all out

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) neighbor, use the **neighbor database-filter all out** command in router configuration mode. To restore the forwarding of LSAs to the neighbor, use the **no** form of this command.

neighbor *ip-address* **database-filter all out** [**cost** *metric*]

no neighbor *ip-address* **database-filter all out**

Syntax Description		
	ip-address	IP address of the neighbor to which outgoing LSAs are blocked.
	cost *metric*	(Optional) Cost metric configured for the specified neighbor. The range of this value is from 0 to 65535.

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

Command Modes   Router configuration

Command History

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

Usage Guidelines   This command performs the same function that the **ip ospf database-filter all out** command performs on an interface basis.

Examples   The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 10.2.3.4:

```
router ospf 109
 neighbor 10.2.3.4 database-filter all out
```

Related Commands

Command	Description
ip ospf database-filter all out	Filters outgoing LSAs to an OSPF interface.

network area

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces defined with the *ip-address wildcard-mask* pair, use the **no** form of this command.

> **network** *ip-address wildcard-mask* **area** *area-id*

> **no network** *ip-address wildcard-mask* **area** *area-id*

Syntax Description

ip-address	IP address.
wildcard-mask	IP-address-type mask that includes "don't care" bits.
area-id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id argument*.

Defaults   This command is disabled by default.

Command Modes   Router configuration

Command History

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

Usage Guidelines   The *ip-address* and *wildcard-mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard-mask* argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.

For OSPF to operate on the interface, the primary address of the interface must be covered by the **network area** command. If the **network area** command covers only the secondary address, it will not enable OSPF over that interface.

The Cisco IOS software sequentially evaluates the *ip-address wildcard-mask* pair for each interface as follows:

1. The *wildcard-mask* argument is logically ORed with the interface IP address.

2. The *wildcard-mask* argument is logically ORed with the *ip-address* argument in the **network** command.

3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

There is no limit to the number of **network area** commands you can use on the router.

Note Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the **network** command list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap in order to avoid inadvertent conflicts.

When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.

For example, consider the following configuration:

```
router ospf 1
 network 192.168.129.16 0.0.0.3 area 20
 network 192.168.129.40 0.0.0.3 area 20
 network 192.168.129.44 0.0.0.3 area 20
 network 192.168.129.96 0.0.0.3 area 20
 network 192.168.128.0  0.0.127.255 area 20
!
```

Enter the following:

```
no network 192.168.129.40 0.0.0.3 area 20
```

Interfaces falling into the network range 192.168.129.40/0.0.0.3 will still remain active because the superset, 192.168.128.0/0.0.127.255, exists for area 20. A more specific network statement will cause interfaces belonging to that range to be removed from a different area only if a less specific network statement (superset) exists.

Consider a configuration such as the following:

```
!
router ospf 1
 network 192.168.128.0 0.0.127.255 area 20
!
```

If the following network statement is entered:

```
network 192.168.129.96 0.0.0.3 area 40
```

then interfaces belonging to range 192.168.129.96/0.0.0.3, if any, are removed from area 20 and moved to area 40. Network statements with identical ranges but with different area IDs are considered as area changes. For example, the following network statements will cause interfaces belonging to network range 192.168.129.40/0.0.0.3 to move from area 20 to area 40:

```
network 192.168.129.40 0.0.0.3 area 20
network 192.168.129.40 0.0.0.3 area 40
```

Examples The following partial example initializes OSPF routing process 109, and defines four OSPF areas: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for all other networks.

```
interface ethernet 0
 ip address 10.108.20.1 255.255.255.0
router ospf 109
 network 10.108.20.0 0.0.0.255 area 10.9.50.0
 network 10.108.0.0 0.0.255.255 area 2
```

```
network 10.109.10.0 0.0.0.255 area 3
network 0.0.0.0 255.255.255.255 area 0
```

Related Commands	Command	Description
	router ospf	Configures an OSPF routing process.

nsf (OSPF)

✎
Note Effective with Cisco IOS Release 12.0(32)S, the **nsf (OSPF)** command has been replaced by the **nsf cisco** [**enforce global**] command. See the **nsf cisco** [**enforce global**] command for more information.

To configure Cisco nonstop forwarding (NSF) operations for Open Shortest Path First (OSPF), use the **nsf** command in router configuration mode. To disable Cisco NSF for OSPF, use the **no** form of this command.

nsf [**enforce global**]

no nsf [**enforce global**]

Syntax Description

enforce global	(Optional) Cancels NSF restart when non-NSF-aware neighboring networking devices are detected.

Command Default This command is disabled by default; therefore, NSF operations for OSPF is not configured.

Command Modes Router configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.0(32)S	This command was replaced by the **nsf cisco** [**enforce global**] command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines The user must configure NSF operation for OSPF only if a router is expected to perform NSF during restart. For users to have full NSF benefits, all OSPF neighbors of the specified router must be NSF-aware.

If neighbors that are not NSF-aware are detected on a network interface, NSF restart is aborted on the interface; however, NSF restart will continue on other interfaces. This functionality applies to the default NSF mode of operation when NSF is configured.

If the user configures the optional **enforce global** keywords, NSF restart will be canceled for the entire process when neighbors that are not NSF-aware are detected on any network interface during restart. NSF restart will also be canceled for the entire process if a neighbor adjacency reset is detected on any interface or if an OSPF interface goes down. To revert to the default NSF mode, enter the **no nsf enforce global** command.

Examples   The following example enters router configuration mode and cancels the NSF restart for the entire OSPF process if neighbors that are not NSF-aware are detected on any network interface during restart:

```
Router(config)# router ospf 1
Router(config-router)# nsf enforce global
```

Related Commands

Command	Description
debug ip ospf nsf	Displays debugging messages related to OSPF NSF commands.
router ospf	Enables OSPF routing and places the router in router configuration mode.

nsf cisco

To enable Cisco nonstop forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf cisco** command in router configuration mode. To disable Cisco NSF, use the **no** form of this command.

> **nsf cisco** [**enforce global**]

> **no nsf cisco** [**enforce global**]

Syntax Description	**enforce global**	(Optional) Cancels NSF restart when non-NSF-aware neighboring networking devices are detected.

Command Default   This command is disabled by default; therefore, Cisco NSF operations are disabled on a router that is running OSPF.

Command Modes   Router configuration

Command History

Release	Modification
12.0(32)S	This command was introduced. This command replaces the **nsf** (OSPF) command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines   For Cisco IOS Release 12.0(32)S and later releases, the **nsf cisco** [**enforce global**] command replaces the **nsf** [**enforce global**] command for OSPF.

To enable Cisco NSF on an OSPF router, you need to enter the **nsf cisco** command. When a router has Cisco NSF enabled, the router is said to be NSF-capable and will operate in graceful restart mode—the OSPF router process performs non-stop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighbor routers of the NSF-capable router will be NSF-aware and will operate in NSF helper mode. When the NSF-capable router is performing graceful restart, the neighbor router helps with the non-stop forwarding recovery.

During the NSF restart process, if neighbors that are not NSF-aware are detected on a network interface, NSF restart is aborted on the interface; however, NSF restart will continue on other interfaces. This functionality applies to the default NSF mode of operation when Cisco NSF is configured. If the user configures the **nsf cisco** command with the optional **enforce global** keywords, NSF restart will be canceled for the entire process when neighbors that are not NSF-aware are detected on any network interface during restart. The NSF restart will also be canceled for the entire process when a neighbor adjacency reset is detected on any interface or when an OSPF interface goes down. To revert to the default NSF behavior, enter the **no nsf cisco enforce global** command.

Examples   The following example enables Cisco NSF on a router and causes the NSF restart to be canceled for the entire OSPF process if neighbors that are not NSF-aware are detected on any network interface during the restart.

```
router ospf 24
 nsf cisco enforce global
```

Related Commands

Command	Description
nsf cisco helper disable	Disables NSF helper mode on a router.
nsf ietf	Enables NSF (graceful restart) on a router.
nsf ietf helper disable	Disables NSF helper mode on a router.
nsf ietf helper strict-lsa-checking	Enables strict LSA checking on a router.

nsf cisco helper disable

To disable Cisco nonstop forwarding (NSF) helper mode on a Cisco router that is running Open Shortest Path First (OSPF), use the **nsf cisco helper disable** command in router configuration mode. To reenable Cisco NSF helper mode, use the **no** form of this command.

> **nsf cisco helper disable**

> **no nsf cisco helper disable**

Syntax Description   This command has no arguments or keywords.

Command Default   This command is enabled by default; therefore, NSF helper mode is disabled on a Cisco router that is running OSPF.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines   When a router in an OSPF process has NSF enabled, the router is said to be NSF-capable and will operate in graceful restart mode—the OSPF router process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighboring routers of the NSF-capable router will be NSF-aware and will operate in NSF helper mode. When the NSF-capable router is performing graceful restart, the helper routers assist in the nonstop forwarding recovery process. If you do not want the router to help the restarting neighbor with nonstop forwarding recovery, enter the **nsf cisco helper disable** command.

Examples   The following example disables NSF helper mode for the Cisco router on OSPF process 3:

```
router ospf 3
 nsf cisco helper disable
```

Related Commands	Command	Description
	nsf cisco	Enables Cisco NSF on a Cisco router.
	nsf ietf	Enables IETF nonstop forwarding operations on a router that is running OSPF.
	nsf ietf helper disable	Disables IETF NSF helper mode on a router.
	nsf ietf helper strict-lsa-checking	Enables strict LSA checking on a router.

nsf ietf

To enable IETF nonstop forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf ietf** command in router configuration mode. To disable IETF NSF, use the **no** form of this command.

nsf ietf [**restart-interval** *seconds*]

no nsf ietf [**restart-interval** *seconds*]

Syntax Description

restart-interval *seconds*	(Optional) Specifies length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default is 120.

Command Default

This command is disabled by default; therefore, IETF NSF operations are disabled on a router that is running OSPF.

Command Modes

Router configuration

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable IETF NSF on an OSPF router, enter the **nsf ietf** command. When a router has NSF enabled, the router is said to be NSF-capable and will operate in graceful restart mode—the OSPF router process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighbor routers of the NSF-capable router will be NSF-aware and will operate in NSF helper mode. When the NSF-capable router is performing graceful restart, the neighbor router helps in the nonstop forwarding recovery.

Examples

The following example enables IETF NSF (graceful restart) on a router, changing the graceful restart interval to 200 seconds:

```
router ospf 24
 nsf ietf restart-interval 200
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF (graceful restart) on a router.
nsf cisco helper disable	Disables Cisco NSF helper mode on a router.

Command	Description
nsf ietf helper disable	Disables IETF NSF helper mode on a router.
nsf ietf helper strict-lsa-checking	Enables strict LSA checking on a router.

nsf ietf helper disable

To disable Internet Engineering Task Force (IETF) nonstop forwarding (NSF) helper mode on a router that is running Open Shortest Path First (OSPF), use the **nsf ietf helper disable** command in router configuration mode. To reenable IETF NSF helper mode, use the **no** form of this command.

nsf ietf helper disable

no nsf ietf helper disable

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default; therefore, IETF NSF helper mode is enabled on a router that is running OSPF.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines   When a router in an OSPF process has NSF enabled, the router is said to be NSF-capable and will operate in graceful restart mode—the OSPF router process performs nonstop forwarding recovery due to a Route Processor (RP) switchover. By default, the neighboring routers of the NSF-capable router will be NSF-aware and will operate in NSF helper mode. When the NSF-capable router is performing graceful restart, the helper routers assist in the nonstop forwarding recovery process. If you do not want the router to help the restarting neighbor with nonstop forwarding recovery, enter the **nsf ietf helper disable** command.

Examples   The following example disables IETF NSF helper mode on a router on OSPF process 4:

```
router ospf 4
 nsf ietf helper disable
```

Related Commands	Command	Description
	nsf cisco	Enables Cisco NSF on a router.
	nsf cisco helper disable	Disables Cisco NSF helper mode on a router.
	nsf ietf	Enables IETF nonstop forwarding operations on a router that is running OSPF.
	nsf ietf helper strict-lsa-checking	Enables strict LSA checking on a router.

nsf ietf helper strict-lsa-checking

To enable strict link-state advertisement (LSA) checking on routers in an Open Shortest Path First (OSPF) process, use the **nsf ietf helper strict-lsa-checking** command in router configuration mode. To disable strict LSA checking, use the **no** form of this command.

> **nsf ietf helper strict-lsa-checking**

> **no nsf ietf helper strict-lsa-checking**

Syntax Description   This command has no arguments or keywords.

Command Default   This command is disabled by default; therefore, strict LSA checking is not done on routers in an OSPF process.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines   To enable strict LSA checking on both NSF-aware and NSF-capable routers, enter the **nsf ietf helper strict-lsa-checking** command. However, strict LSA checking will not become effective until the router becomes a helper router during an IETF graceful restart process. With strict LSA checking enabled, the helper router will terminate the helping process of the restarting router if it detects that there is a change to an LSA that would be flooded to the restarting router or if there is a changed LSA on the retransmission list of the restarting router when the graceful restart process is initiated.

Examples   The following example enables strict LSA checking on a router on OSPF process 12:

```
router ospf 12
 nsf ietf helper strict-lsa-checking
```

Related Commands	Command	Description
	nsf cisco	Enables Cisco NSF on a router.
	nsf cisco helper disable	Disables Cisco NSF helper mode on a router.
	nsf ietf	Enables IETF nonstop forwarding operations on a router that is running OSPF.
	nsf ietf helper disable	Disables IETF NSF helper mode on a router.

nsr

To enable nonstop routing (NSR) operations on a router that is running Open Shortest Path First (OSPF), use the **nsr** command in router configuration mode. To disable NSR and return to the default, use the **no** form of this command.

nsr

no nsr

Syntax Description   This command has no arguments or keywords.

Command Default   NSR is disabled.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines   This command enables NSR on an OSPF router. With NSR enabled, a router with redundant Route Processors (RPs) is allowed to maintain its OSPF state and adjacencies across planned and RP switchovers. It does this by checkpointing state information from OSPF on the active RP to the standby RP. Later, following a switchover to the standby RP, OSPF can use this checkpointed information to continue operation without interruption.

This command is present only in images for platforms that have a hardware or software redundancy capability.

Examples   The following example enables NSR on an OSPF router:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# nsr
```

Related Commands

Command	Description
show ip ospf nsr	Displays OSPF NSR status information.

prefix-suppression

To prevent Open Shortest Path First (OSPF) from advertising all IP prefixes except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces for a specific OSPF process, use the **prefix-suppression** command in router configuration mode. To advertise all IP prefixes, use the **no** form of this command.

prefix-suppression

no prefix-suppression

Syntax Description   This command has no arguments or keywords.

Command Default   All IP prefixes are advertised.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines   You can globally suppress all IP prefixes (except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces) for an entire OSPF process by using the **prefix-suppression** command in router configuration mode. You can also suppress IP prefixes on a per-interface basis by using the **ip ospf prefix-suppression** command in interface configuration mode. When the **ip ospf prefix-suppression** command is configured, it takes precedence over the **prefix-suppression** router configuration command.

Examples   The following example globally suppresses all IP prefixes except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces for OSPF process 4:

```
router ospf 4
 prefix-suppression
```

Related Commands

Command	Description
ip ospf prefix-suppression	Prevents OSPF from advertising all IP prefixes that belong to a specific interface, except for IP prefixes that are associated with secondary IP addresses.

process-min-time percent

Note Effective with Cisco IOS 15.1(1)T release, the **process-min-time percent** command is not available in Cisco IOS 15.1(1)T and later releases. Improvements in Cisco IOS scheduler have made this command unnecessary.

To specify the minimum percentage of CPU process time OSPF takes before the CPU should yield to a process with a higher priority, use the **process-min-time percent** command in router configuration mode. To disable this function, use the **no** form of this command.

process-min-time percent *percentage*

no process-min-time percent

Syntax Description

percentage	Percentage of CPU process time to be used before trying to release the CPU for other processes. The valid value range is from 1 to 100. The default is 25.

Command Default The default is 25 percent.

Command Modes Router configuration (config-router)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 320.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)T	This command was removed.

Usage Guidelines

Note Use this command under the direction of Cisco TAC only.

This command is supported by OSPFv2 and OSPFv3.

Use the **process-min-time percent** command to configure the minimum percentage of the process maximum time. Lowering the minimum percentage of CPU usage that a process can utilize is useful in some circumstances to ensure equitable division of CPU resources among different tasks. Once the percentage has been exceeded, CPU control may be given to a higher priority process.

The process maximum time is set using the **process-max-time** command. Use the **process-min-time percent** command in conjunction with the **process-max-time** command.

Examples   The following example shows how to set the percentage of CPU process time to be used before releasing the CPU:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# process-min-time percent 35
```

The following example shows how to return to the default setting in IPv4:

```
Router# configure terminal
Router(config)# router ospf
Router(config-router)# no process-min-time percent
```

Related Commands

Command	Description
process-max-time	Configures the amount of time after which a process should voluntarily yield to another process.

redistribute maximum-prefix

To limit the number of prefixes redistributed into Open Shortest Path First (OSPF) or to generate a warning when the number of prefixes redistributed into OSPF reaches a maximum, use the **redistribute maximum-prefix** command in router configuration mode. To remove the values, use the **no** form of this command.

> **redistribute maximum-prefix** *maximum* [*percentage*] [**warning-only** | **withdraw**]

> **no redistribute maximum-prefix**

Syntax Description		
maximum	Integer from 1 to 4294967295 that specifies the maximum number of IP prefixes that can be redistributed into OSPF.	
	When the **warning-only** keyword is configured, the *maximum* value specifies the number of prefixes that can be redistributed into OSPF before the system logs a warning message. Redistribution is not limited.	
	The maximum number of IP prefixes that are allowed to be redistributed into OSPF, or the number of prefixes allowed to be redistributed into OSPF before the system logs a warning message, depends on whether the **warning-only** keyword is present.	
	• There is no default value for the *maximum* argument.	
	• If the **warning-only** keyword is also configured, this value does not limit redistribution; it is simply the number of redistributed prefixes that, when reached, causes a warning message to be logged.	
percentage	(Optional) Integer from 1 to 100 that specifies the threshold value, as a percentage, at which a warning message should be generated.	
	• The *percentage* default is 75.	
warning-only	(Optional) Causes a warning message to be logged when the number of prefixes defined by the *maximum* argument has been exceeded. Additional redistribution is not prevented.	
withdraw	(Optional) Prevents additional redistribution when the number of prefixes defined by the *maximum* argument has been exceeded.	
	Also, IS-IS rebuilds link-state PDUs (LSPs) without the external (redistributed) IP prefixes.	

Command Default   The percentage default is 75.

Command Modes   Router configuration (config-router)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If someone mistakenly injects a large number of IP prefixes into IS-IS, perhaps by redistributing Border Gateway Protocol (BGP) into IS-IS, the network can be severely flooded. Limiting the number of redistributed prefixes prevents this potential problem.

When the **redistribute maximum-prefix** command is configured and the number of redistributed prefixes reaches the maximum value configured, no more prefixes will be redistributed (unless the **warning-only** keyword was configured).

The redistribution limit applies only to external IP prefixes. Default prefixes and summarized prefixes are not limited.

The limit is tracked separately for each not-so-stubby-area (NSSA) because redistribution to NSSAs is done independently for each NSSA and independently of all other regular areas.

Select a *maximum* value based on your knowledge of how many prefixes are redistributed on the router to the OSPF process.

Examples

Examples for IS-IS Protocol

The following example shows how to set a maximum of 600 prefixes that can be redistributed into IS-IS. If the number of prefixes redistributed reaches 75 percent of 600 (450 prefixes), a warning message is logged.

```
router isis
 redistribute maximum-prefix 600
```

The following example shows how to set a maximum of 1200 prefixes that can be redistributed into IS-IS. If the number of prefixes redistributed reaches 80 percent of 1200 (960 prefixes), a warning message is logged.

```
router isis
 redistribute maximum-prefix 1200 80
```

The following example shows how to allow two warning messages to be logged. The first message is logged when the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second message is logged when the number of redistributed prefixes reaches 600. However, the number of redistributed prefixes is not limited.

```
router isis
 redistribute maximum-prefix 600 85 warning-only
```

Examples for OSPF Routing Protocol

The following example shows how to set a maximum of 2000 prefixes that can be redistributed into OSPF process when the number of prefixes redistributed reaches 75 percent of 2000 (1500 prefixes), a warning message is logged. Another warning is logged when the limit is reached, and no more prefixes are redistributed.

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 2000
```

The following example shows how to set a maximum of 1200 prefixes that can be redistributed into OSPF process when the number of prefixes redistributed reaches 80 percent of 1200 (960 prefixes), a warning message is logged. Another warning is logged when the limit is reached, and no more prefixes are redistributed.

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 1200 80
```

The following example shows how to allow two warning messages to be logged. The first message is logged when the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second message is logged when the number of redistributed prefixes reaches 600. However, the number of redistributed prefixes is not limited.

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 600 85 warning-only
```

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-id* [**vrf** *vpn-name*]

no router ospf *process-id* [**vrf** *vpn-name*]

Syntax Description	*process-id*	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
	vrf *vpn-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.

Defaults   No OSPF routing process is defined.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The **vrf** keyword and *vpn-name* arguments were added to identify a VPN.
12.0(9)ST	The **vrf** keyword and *vpn-name* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   You can specify multiple OSPF routing processes in each router.

After you enter the **router ospf** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

Examples   The following example configures an OSPF routing process and assign a process number of 109:

```
Router(config)# router ospf 109
```

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF instance processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
```

```
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```

The following example shows usage of the **maximum-paths** option:

```
Router> enable
Router# configure terminal
Router(config)# router ospf
Router(config-router)# maximum-paths?
Router(config-router)# 20
Router(config-router)# exit
```

Related Commands	Command	Description
	network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) to use the previous OSPF router ID behavior, use the **no** form of this command.

router-id *ip-address*

no router-id *ip-address*

Syntax Description	*ip-address*	Router ID in IP address format.

Defaults No OSPF routing process is defined.

Command Modes Router configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **clear ip ospf** command.

Examples The following example specifies a fixed router-id:

```
router-id 10.1.1.1
```

Related Commands

Command	Description
clear ip ospf	Clears redistribution based on the OSPF routing process ID.
router ospf	Configures the OSPF routing process.