Cisco IOS IP Routing: OSPF Command Reference

April 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS IP Routing: OSPF Command Reference

CONTENTS

Introduction

This book describes the commands used to configure and monitor Open Shortest Path First (OSPF) routing capabilities and features.

For OSPF routing protocols configuration information and examples, refer to the *Cisco IOS IP Routing: OSPF Configuration Guide*.

OSPF Commands

area authentication

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication** [**message-digest**]

Syntax Description

area-id	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the *area-id* argument.

Defaults

Type 0 authentication (no authentication)

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **message-digest** 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.

Usage Guidelines

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the **ip ospf authentication-key** interface command to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** interface command.

To remove the authentication specification for an area, use the **no** form of this command with the **authentication** keyword.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example mandates authentication for areas 0 and 10.0.0.0 of OSPF routing process 201. Authentication keys are also provided.

```
interface ethernet 0
 ip address 192.168.251.201 255.255.255.0
 ip ospf authentication-key adcdefgh
!
interface ethernet 1
 ip address 10.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 network 192.168.0.0 0.0.255.255 area 0
 area 10.0.0.0 authentication
 area 0 authentication
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub area.
area stub	Defines an area as a stub area.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

area default-cost

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the **area default-cost** command in router address family topology or router configuration mode. To remove the assigned default route cost, use the **no** form of this command.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost** *cost*

Syntax Description

area-id	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
cost	Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

Command Default

cost: 1

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.
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

This command is used only on an Area Border Router (ABR) attached to a stub area or NSSA.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

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

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area stub	Defines an area as a stub area.

area filter-list

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command in router address family topology or router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**}

no area *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**}

Syntax Description

area-id	Identifier of the area for which filtering is configured. The identifier can be specified as either a decimal value or an IP address.
prefix	Indicates that a prefix list is used.
prefix-list-name	Name of a prefix list.
in	The prefix list is applied to prefixes advertised to the specified area from other areas.
out	The prefix list is applied to prefixes advertised out of the specified area to other areas.

Command Default

This command is disabled by default. The router will not filter prefixes.

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.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was made available in router address family topology configuration mode.

Usage Guidelines

With this feature enabled in the "in" direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the **area range** command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the "out" direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the **area range** command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the **area range** command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

Release 12.2(33)SRB

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

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
area 1 filter-list prefix AREA_1 in
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.

area nssa

To configure a not-so-stubby area (NSSA), use the **area nssa** command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]

Syntax Description

area-id	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).
metric	(Optional) Specifies the OSPF default metric.
metric-type	(Optional) Specifies the OSPF metric type for default routes.
no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.
nssa-only	(Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero.

Command Default

No NSSA area is defined.

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.
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.
15.0(1)M	This command was modified. The **nssa-only** keyword was added.
12.2(33)SRE	This command was modified. The **nssa-only** keyword was added.

Usage Guidelines

To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, including **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

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

Examples

The following example makes area 1 an NSSA area:

```
router ospf 1
 redistribute rip subnets
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa
```

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.

area nssa translate

To configure a not-so-stubby area (NSSA) and to configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, use the **area nssa translate** command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

area *area-id* **nssa translate type7** {[**always**] [**suppress-fa**]} [**default-information-originate** [**metric** *ospf-metric*] [**metric-type** *ospf-link-state-type*] [**nssa-only**]] [**no-ext-capability**] [**no-redistribution**] [**no-summary**]

no area *area-id* **nssa translate type7** {[**always**] [**suppress-fa**]} [**default-information-originate** [**metric** *ospf-metric*] [**metric-type** *ospf-link-state-type*] [**nssa-only**]] [**no-ext-capability**] [**no-redistribution**] [**no-summary**]

Syntax Description

area-id	Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
translate	Translates one type of link-state advertisement (LSA) to another type of LSA. This keyword takes effect only on an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR).
type7	(Required) Translates a Type-7 LSA to a Type-5 LSA. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.
always	(Optional) Configures an NSSA ABR router as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs. You can configure the **always** keyword only in router configuration mode, not in router address family topology configuration mode.
suppress-fa	(Optional) Suppresses the forwarding address of the Type-7 LSAs from being placed in the Type-5 LSAs. This keyword takes effect only on an NSSA ABR or an NSSA ASBR.
default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).
metric	(Optional) Configures the OSPF default metric.
ospf-metric	Specifies the OSPF default metric in the range from 0 to 16777214.
metric-type	(Optional) Configures the OSPF metric type for default routes.
ospf-link-state-type	Specifies OSPF metric type in the range from 1 to 2.
nssa-only	(Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero..
no-ext-capability	(Optional) Specifies that domain-specific capabilities are not sent to NSSA.
no-redistribution	(Optional) Specifies that the **redistribute** command will import routes only into the normal areas, not into the NSSA area. Used when the router is an NSSA ABR.
no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.

Command Default

The ABRs connecting an NSSA and the backbone areas elect one of them to translate LSAs, which means that a router might be elected as translator.

Command Modes

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

Release	Modification
12.2(15)T	This command was introduced.
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.
12.2(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.
15.1(2)S	This command was modified. Support for the **always** keyword was added.

Usage Guidelines

To configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, configure the **translate type7 suppress-fa** keywords. Consider the following caution.

Caution Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

If the the **no-redistribution** or **default-information-originate** keywords are used, two separate lines for the **area nssa** command appear in the configuration file for ease of readability. For example, if the **area 6 nssa translate type7 suppress-fa no-redistribution** command is configured, the following lines would appear in the configuration file:

```
router ospf 1
 area 6 nssa no-redistribution
 area 6 nssa translate type7 suppress-fa
```

Cisco IOS Release 15.1(2)S and later releases support RFC 3101 and include the **always** keyword, which allows you to configure an NSSA ABR router as a forced NSSA LSA translator. This means that the NSSA ABR router will unconditionally assume the role of LSA translator, preempting the default behavior, which would only include it among the candidates to be elected as translator.

Note Even a forced translator might not translate all LSAs; translation depends on the contents of each LSA.

You can configure the **always** keyword only in router configuration mode, not in router address family topology configuration mode.

To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature with this command, you you must do so in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples

The following example causes OSPF to translate Type-7 LSAs from area 1 to Type-5 LSAs, but not place the Type-7 forwarding address into the Type-5 LSAs. OSPF places 0.0.0.0 as the forwarding address in the Type-5 LSAs.

```
router ospf 2
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa translate type7 suppress-fa
```

The following example configures an NSSA ABR as a forced LSA translator.

```
Router(config-router)# area 10 nssa translate type7 always
```

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

area *area-id* **range** *ip-address ip-address-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address ip-address-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

Syntax Description

area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
ip-address	IP address.
ip-address-mask	IP address mask.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Command Default

This command is disabled by default.

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.
12.0(24)S	The **cost** keyword and *cost* argument were added.
12.2(15)T	The **cost** keyword and *cost* argument were added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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.
12.2(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

The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

Multiple **area range** router configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

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

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface ethernet 0
 ip address 192.168.110.201 255.255.255.0
!
interface ethernet 1
 ip address 192.168.120.201 255.255.255.0
!
router ospf 201
 network 192.168.110.0 0.0.0.255 area 0
 area 10.0.0.0 range 10.0.0.0 255.0.0.0
 area 0 range 192.168.110.0 255.255.0.0
```

Related Commands

Command	Description
area range (IPv6)	Consolidates and summarizes routes at an area boundary in an IPv6 network.

area sham-link

To configure a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) backbone, use the **area sham-link** command in router configuration mode. To remove the sham-link, use the **no** form of this command.

area *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**ttl-security hops** *hop-count*]

no area *area-id* **sham-link** *source-address destination-address*

Syntax Description

area-id	ID number of the Open Shortest Path First (OSPF) area assigned to the sham link. Valid values: numeric value from 1 to 4294967295 or valid IP address, in A.B.C.D format. There is no default.
source-address	IP address of the source PE router in the format: *ip-address* [*mask*].
destination-address	IP address of the destination PE route in the format: *ip-address* [*mask*].
cost *number*	(Optional) Specifies the OSPF cost to send IP packets over the sham-link interface. The *number* argument range is from 1 to 65535.
ttl-security hops *hop-count*	(Optional) Configures Time-to-Live (TTL) security on a sham link. The *hop-count* argument range is from 1 to 254.

Command Default

No default behavior or values

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST, and support for Cisco 12000 series Internet routers was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for Cisco 10000 series Internet routers 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.
12.2(33)SRC	The **ttl-security hops** *hop-count* keywords and argument were added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

In the MPLS VPN environment, several VPN client sites can be connected in the same OSPF area. If these sites are connected over a backdoor link in addition to the VPN backbone, all traffic passes over the backdoor link instead of over the VPN backbone. OSPF always selects intra-area routes over interarea (external) routes.

To correct this default OSPF behavior in an MPLS VPN, use the **area sham-link** command to configure a sham link between two PEs to connect the sites through the MPLS VPN backbone. A sham link represents an intra-area (unnumbered point-to-point) connection between PEs. All other routers in the area use the sham link to calculate intra-area shortest path first (SPF) routes to the remote site.

Configure the source and destination addresses of the sham link as a host route mask (255.255.255.255) on the PE routers that serve as the endpoints of the sham link. The source and destination IP addresses must belong to the VPN routing and forwarding instance (VRF) and be advertised by Border Gateway Protocol (BGP) to remote PE routers. The sham link endpoint addresses should not be advertised by OSPF.

Use the **ttl-security hops** *hop-count* keywords and argument to enable checking of TTL values on OSPF packets from neighbors or set TTL values sent to neighbors. This feature adds an extra layer of protection to OSPF.

Examples

The following example shows how to configure a sham link between two PE routers in an MPLS VPN backbone by using the **area sham-link** command on each router:

```
Router1(config)# interface loopback 55
Router1(config-if)# ip vrf forwarding v1
Router1(config-if)# ip address 10.0.0.1 255.255.255.255
!
Router1(config)# router ospf 2 vrf v1
Router1(config-router)# log-adjacency-changes
Router1(config-router)# area 120 sham-link 10.0.0.1 172.16.0.1 cost 1
Router1(config-router)# redistribute bgp 1 subnets
Router1(config-router)# network 10.2.0.1 255.255.255.255 area 1
Router1(config-router)# network 10.120.0.0 0.255.255.255 area 120
Router1(config-router)# network 10.140.0.0 0.255.255.255 area 120
!
Router2(config)# interface loopback 44
Router2(config-if)# ip vrf forwarding v1
Router2(config-if)# ip address 172.16.0.1 255.255.255.255
!
Router2(config)# router ospf 2 vrf v1
Router2(config-router)# log-adjacency-changes
Router2(config-router)# area 120 sham-link 172.16.0.1 10.0.0.1 cost 1
Router2(config-router)# redistribute bgp 1 subnets
Router2(config-router)# network 10.2.0.1 255.255.255.255 area 1
Router2(config-router)# network 10.120.0.0 0.255.255.255 area 120
Router2(config-router)# network 10.140.0.0 0.255.255.255 area 120
!
```

Related Commands

Command	Description
ttl-security hops	Enables checking of TTL values on OSPF packets from neighbors or setting TTL values sent to neighbors.

area stub

To define an area as a stub area, use the **area stub** command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Syntax Description

area-id	Identifier for the stub area; either a decimal value or an IP address.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Defaults

No stub area is defined.

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.
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

You must configure the **area stub** command on all routers and access servers in the stub area. Use the **area** router configuration command with the **default-cost** keyword to specify the cost of a default internal route sent into a stub area by an ABR.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** keyword of the **area** command. Use the **default-cost** keyword only on an ABR attached to the stub area. The **default-cost** keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note: To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

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

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area default-cost	Specifies a cost for the default summary route sent into a stub area.

area virtual-link

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command in router address family topology or router configuration mode. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

no area *area-id* **virtual-link** *router-id*

Syntax Description

area-id	Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
router-id	Router ID associated with the virtual link neighbor. The router ID appears in the **show ip ospf** or **show ipv6 display** command. There is no default.
hello-interval *seconds*	(Optional) Specifies the time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. Range is from 1 to 8192. The default is 10.
retransmit-interval *seconds*	(Optional) Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Range is from 1 to 8192. The default is 5.
transmit-delay *seconds*	(Optional) Specifies the estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Range is from 1 to 8192. The default value is 1.
dead-interval *seconds*	(Optional) Specifies the time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
ttl-security hops *hop-count*	(Optional) Configures Time-to-Live (TTL) security on a virtual link. The *hop-count* argument range is from 1 to 254.

Command Default

No OSPF virtual link is defined.

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.
12.0(24)S	Support for IPv6 was added.
12.2(15)T	Support for IPv6 was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
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.
12.2(33)SRB	This command was made available in router address family topology configuration mode.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **ttl-security hops** *hop-count* keywords and argument were added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Use the **ttl-security hops** *hop-count* keywords and argument to enable checking of TTL values on OSPF packets from neighbors or to set TTL values sent to neighbors. This feature adds an extra layer of protection to OSPF.

Note In order for a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf** or the **show ipv6 ospf** command in privileged EXEC mode.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Release 12.2(33)SRB

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

Examples

The following example establishes a virtual link with default values for all optional parameters:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1 hello-interval 5
```

Related Commands

Command	Description
ttl-security hops	Enables checking of TTL values on OSPF packets from neighbors or setting TTL values sent to neighbors.
show ip ospf	Enables the display of general information about Open Shortest Path First (OSPF) routing processes.
show ipv6 ospf	Enables the display of general information about Open Shortest Path First (OSPF) routing processes.

auto-cost

To control how Open Shortest Path First (OSPF) calculates default metrics for the interface, use the **auto-cost** command in router configuration mode. To assign cost based only on the interface type, use the **no** form of this command.

auto-cost reference-bandwidth *mbps*

no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.

Defaults

100 Mbps

Command Modes

Router configuration

Command History

Release	Modification
11.2	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

In Cisco IOS Release 10.3 and later releases, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, and a T1 link will have a metric of 64.

The OSPF metric is calculated as the *ref-bw* value divided by the *bandwidth*, with *mbps* equal to 10^8 by default, and *bandwidth* determined by the **bandwidth** (interface) command. The calculation gives FDDI a metric of 1.

If you have multiple links with high bandwidth (such as FDDI or ATM), you might want to use a larger number to differentiate the cost on those links.

The value set by the **ip ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example changes the cost of the FDDI link to 10, while the gigabit Ethernet link remains at a cost of 1. Thus, the link costs are differentiated.

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ip ospf cost	Explicitly specifies the cost of sending a packet on an interface.

capability lls

To enable the use of the Link-Local Signalling (LLS) data block in originated Open Shortest Path First (OSPF) packets and reenable OSPF nonstop forwarding (NSF) awareness, use the **capability lls** command in router configuration mode. To disable LLS and OSPF NSF awareness, use the **no** form of this command.

capability lls

no capability lls

Syntax Description

This command has no arguments or keywords.

Command Default

LLS is enabled.

Command Modes

Router 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(31)SXH.

Usage Guidelines

You might want to disable NSF awareness by disabling the use of the LLS data block in originated OSPF packets. You might want to disable NSF awareness if the router has no applications using LLS.

If NSF is configured and you try to disable LLS, you will receive the error message, “OSPF Non-Stop Forwarding (NSF) must be disabled first.”

If LLS is disabled and you try to configure NSF, you will receive the error message, “OSPF Link-Local Signaling (LLS) capability must be enabled first.”

Examples

The following example disables LLS support and OSPF NSF awareness:

```
router ospf 2
 no capability lls
```

capability transit

To reenable Open Shortest Path First (OSPF) area capability transit after it has been disabled, use the **capability transit** command in router configuration mode. To disable OSPF area capability transit on all areas for a router process, use the **no** form of this command.

capability transit

no capability transit

Syntax Description

This command has no arguments or keywords.

Defaults

OSPF area capability transit is enabled.

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

Usage Guidelines

OSPF area capability transit is enabled by default, allowing the OSPF Area Border Router to install better-cost routes to the backbone area through the transit area instead of the virtual links. If you want to retain a traffic pattern through the virtual-link path, you can disable capability transit by entering the **no capability transit** command. If paths through the transit area are discovered, they are most likely to be more optimal paths, or at least equal to, the virtual-link path. To reenable capability transit, enter the **capability transit** command.

If you need to verify whether OSPF area capability transit is enabled for a specific routing process, enter the **show ip ospf** command.

Examples

The following example shows how to disable OSPF area capability transit on all areas for a router process named ospf 1. A **show ip ospf** command is issued first to display the current areas that have area capability transit enabled. The **no capability transit** command is then entered to disable OSPF area capability transit on all areas for the router process ospf 1.

```
Router# show ip ospf

 Routing Process "ospf 1" with ID 10.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
!Supports area transit capability
It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 8. Checksum Sum 0x02853F
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
!Number of areas transit capable is 1
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:02:21.524 ago
        SPF algorithm executed 11 times
        Area ranges are
        Number of LSA 49. Checksum Sum 0x19B5FA
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 38
        Flood list length 0
    Area 1
        Number of interfaces in this area is 3
       !This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 00:02:36.544 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 42. Checksum Sum 0x1756D5
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

Router(config)# router ospf 1
Router(router-config)# no capability transit
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.

capability vrf-lite

To suppress the provider edge (PE) specific checks on a router when the Open Shortest Path First (OSPF) process is associated with the VPN routing and forwarding instance (VRF), use the **capability vrf-lite** command in router configuration mode. To restore the checks, use the **no** form of this command.

capability vrf-lite

no capability vrf-lite

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. PE specific checks are performed if the process is associated with VRF command modes.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)B	This command was integrated into Cisco IOS Release 12.2(8)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(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 works only if the OSPF process is associated with the VRF.

When the OSPF process is associated with the VRF, several checks are performed when link-state advertisements (LSAs) are received. PE checks are needed to prevent loops when the PE is performing a mutual redistribution between OSPF and Border Gateway Protocol (BGP) interfaces.

Table 1 describes the PE checks performed when Type-3, Type-5, and Type-7 LSAs are received.

Table 1 PE Checks Performed

Type-3 LSA received	The DN bit is checked. If the DN bit is set, the Type-3 LSA is not considered during the shortest path first (SPF) calculation.
Type-5 or -7 LSA received	If the Tag in the LSA is equal to the VPN-tag, the Type-5 or-7 LSA is not considered during the SPF calculation.

In some situations, performing PE checks might not be desirable. The concept of VRFs can be used on a router that is not a PE router (that is, a router that is not running BGP). With the **capability vrf-lite** command, the checks can be turned off to allow correct population of the VRF routing table with routes to IP prefixes.

Examples

This example shows a router configured with multi-VRF:

```
router ospf 100 vrf grc
 capability vrf-lite
```

clear ip ospf

To clear redistribution based on the Open Shortest Path First (OSPF) routing process ID, use the **clear ip ospf** command in privileged EXEC mode.

clear ip ospf [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]}

Syntax Description

pid	(Optional) Process ID.
process	Reset OSPF process.
redistribution	Clear OSPF route redistribution.
counters	OSPF counters.
neighbor	(Optional) Neighbor statistics per interface.
neighbor-interface	(Optional) Neighbor interface.
neighbor-id	(Optional) Neighbor ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	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

Use the *pid* argument to clear only one OSPF process. If the *pid argument* is not specified, all OSPF processes are cleared.

Prior to Cisco IOS Release 12.2(33)SXH, when the **clear ip ospf process** command is executed, even if a local address is no longer available, the default router ID remains the same. In Cisco IOS Release 12.2(33)SXH, that behavior changed so that when the **clear ip ospf process** command is executed OSPF checks if the currently in-use router ID is still available as a local address. If it is not, OSPF runs a re-election and changes its router ID.

Examples

The following example shows how to clear all OSPF processes:

```
Router# clear ip ospf process
```

clear ip ospf force-spf

To start the shortest path first (SPF) algorithm without clearing the Open Shortest Path First (OSPF) database, use the **clear ip ospf force-spf** command in privileged EXEC mode.

clear ip ospf [*process-id*] **force-spf**

Syntax Description

process-id	(Optional) Process identifier (ID). The range is from 1 to 65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	The command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	The command was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **clear ip ospf force-spf** command is used in troubleshooting and for testing purposes. This command is used to verify if the currently computed routes are correct, to generate debug messages, and so on.

Examples

The following example shows how to start the SPF algorithm without first clearing the OSPF database:

```
Router# clear ip ospf 1000 force-spf
```

Related Commands

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

clear ip ospf traffic

To clear Open Shortest Path First (OSPF) traffic statistics, use the **clear ip ospf traffic** command in user EXEC or privileged EXEC mode.

clear ip ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) Process ID. If the *process-id* argument is included, only traffic statistics for the specified routing process are cleared.
interface-type	(Optional) Interface type.
interface-number	(Optional) interface number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.

Examples

The following example clears OSPF traffic statistics for the OSPF process 100:

```
Router# clear ip ospf 100 traffic
```

Related Commands

Command	Description
show ip ospf traffic statistics	Displays OSPF traffic statistics.

clear ipv6 ospf traffic

To reset counters and clear IPv6 OSPFv3 traffic statistics, use the **clear ipv6 ospf traffic** command privileged EXEC mode.

clear ipv6 ospf traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example resets the counters and clears the OSPFv3 traffics statistics:

```
Router# clear ipv6 ospf traffic
```

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.
show ipv6 ospf traffic	Displays OSPFv3 traffic statistics.

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

Compatible with RFC 1583.

Command Modes

Router configuration

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.

Usage Guidelines

This command is backward compatible with Cisco IOS Release 12.0.

To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the **no compatible rfc1583** command to enable the calculation method used per RFC 2328.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
router ospf 1
 compatible rfc1583
 !
```

compatible rfc1587

To replace RFC 3101 compatibility with RFC 1587 compatibility for route selection in not-so-stubby area (NSSA) Area Border Routers (ABRs), use the **compatible rfc1587** command in router configuration mode. To restore RFC 3101 compatibility, use the **no** form of this command.

compatible rfc1587

no compatible rfc1587

Syntax Description

This command has no arguments or keywords.

Command Default

Route selection is compatible with RFC 3101.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

In Cisco IOS Release 15.1(2)S and later releases, RFC 3101 replaces RFC 1587, and RFC 3101 behavior is automatically enabled. You can choose the route selection behavior by configuring a router to run as RFC 3101 or RFC 1587 compatible.

Examples

The following example specifies that the router process is compatible with RFC 1587:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# compatible rfc1587
```

default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the **default-information originate** command in router configuration or router address family topology configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route. **Note** The **always** keyword includes the following exception when the route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table and the **always** keyword is ignored.
metric *metric-value*	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The value used is specific to the protocol.
metric-type *type-value*	(Optional) External link type associated with the default route that is advertised into the OSPF routing domain. It can be one of the following values: • Type 1 external route • Type 2 external route The default is type 2 external route.
route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Command Default

This command is disabled by default. No default external route is generated into the OSPF routing domain.

Command Modes

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

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.

Release	Modification
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

Whenever you use the **redistribute** or the **default-information** router configuration command to redistribute routes into an OSPF routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.

Release 12.2(33)SRB

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

Examples

The following example specifies a metric of 100 for the default route that is redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
 redistribute eigrp 108 metric 100 subnets
 default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
default-metric	Sets default metric values for routes.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (OSPF)

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the **default-metric** command in router address family topology or router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol.

Defaults

Built-in, automatic metric translations, as appropriate for each routing protocol. The metric of redistributed connected and static routes is set to 0.

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.
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

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Note When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Release 12.2(33)SRB

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

Examples

The following example shows a router in autonomous system 109 using both the Routing Information Protocol (RIP) and the OSPF routing protocols. The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP metric of 10.

```
router rip
 default-metric 10
 redistribute ospf 109
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

discard-route

To reinstall an external or internal discard route that was previously removed, use the **discard-route** command in router address family topology configuration or router configuration mode. To remove an external or internal discard route, use the **no** form of this command.

discard-route [**external** [*distance*]] [**internal** [*distance*]]

no discard-route [**external** [*distance*]] [**internal** [*distance*]]

Syntax Description

external	(Optional) Specifies the discard-route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
internal	(Optional) Specifies the discard-route entry for summarized internal routes on the Area Border Router (ABR).
distance	(Optional) Administrative distance. A value between 1 and 254. The default administrative distance for external and internal discard routes is 254 and 110, respectively.

Defaults

External and internal discard-route entries are installed.

Command Modes

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

Command History

Release	Modification
12.1(1)T	This command was introduced.
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.
12.4(15)T	The *distance* argument was added.
12.2(33)SRC	The *distance* argument was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

External and internal discard-route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router that is performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the **no discard-route** command with the **external** or **internal** keyword.

Release 12.2(33)SRB

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

Release 12.4(15)T

Prior to Cisco IOS Release 12.4(15)T, both external and internal discard routes were installed using the default OSPF intra-area administrative distance 110. You can now modify this default distance for discard routes by entering a new administrative distance for the *distance* argument of the **discard-route** command.

Examples

The following display shows the discard-route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the **show ip route** command. See the router output that refers to Null0:

```
Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
C        172.16.0.128/25 is directly connected, Loopback1
O        172.16.0.0/24 is a summary, 00:00:14, Null0
C        172.16.0.0/25 is directly connected, Loopback0
      172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
C        172.31.0.128/25 is directly connected, Loopback3
O        172.31.0.0/24 is a summary, 00:00:02, Null0
C        172.31.0.0/25 is directly connected, Loopback2
C     192.168.0.0/24 is directly connected, Ethernet0/0

Router# show ip route ospf

      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O        172.16.0.0/24 is a summary, 00:00:29, Null0
      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
O        172.16.0.0/24 is a summary, 00:00:17, Null0
```

When the **no discard-route** command with the **internal** keyword is entered, notice the following route change, indicated by the router output that refers to Null0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router ospf 1
Router(config-router)# no discard-route internal
Router(config-router)# end

Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
C        172.16.0.128/25 is directly connected, Loopback1
C        172.16.0.0/25 is directly connected, Loopback0
      172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
C        172.31.0.128/25 is directly connected, Loopback3
O        172.31.0.0/24 is a summary, 00:00:02, Null0
C        172.31.0.0/25 is directly connected, Loopback2
C     192.168.0.0/24 is directly connected, Ethernet0/0

Router# show ip route ospf

      172.31.0.0/24 is variably subnetted, 3 subnets, 2 masks
O        172.16.0.0/24 is a summary, 00:04:14, Null0
```

Next, the **no discard-route** command with the **external** keyword is entered to remove the external discard route entry:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router ospf 1
Router(config-router)# no discard-route external
Router(config-router)# end
```

The following router output from the **show running-config** command confirms that both the external and internal discard routes have been removed from the routing table of the router. See the router output that refers to discard routes.

```
Router# show running-config

Building configuration...

Current configuration : 1114 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
.
.
.
router ospf 1
 log-adjacency-changes
 no discard-route external
 no discard-route internal
 area 1 range 172.16.0.0 255.255.255.0
 summary-address 172.31.0.0 255.255.255.0
 redistribute rip subnets
 network 192.168.0.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 1
!
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.
show running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.

distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the **distance ospf** command in router address family topology or router configuration mode. To restore the default value, use the **no** form of this command.

distance ospf {**external** *dist1* | **inter-area** *dist2* | **intra-area** *dist3*}

no distance ospf

Syntax Description

external *dist1*	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255. The default value is 110.
inter-area *dist2*	(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255. The default value is 110.
intra-area *dist3*	(Optional) Sets the distance for all routes within an area. Range is 1 to 255. The default value is 110.

Command Default

dist1: 110

dist2: 110

dist3: 110

Command Modes

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

Command History

Release	Modification
11.1(14)	This command was introduced.
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

You must specify at least one of the keywords.

This command performs the same function as the **distance** command used with an access list. However, the **distance ospf** command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospf** command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Release 12.2(33)SRB

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

Examples

The following example changes the external distance to 200, making the route less reliable:

Router A Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Router B Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Related Commands

Command	Description
distance (IP)	Defines an administrative distance.

domain-id (OSPF)

To change the OSPF domain ID that is used during the redistribution of BGP VPNv4 routes to OSPF, use the **domain-id** command in router configuration mode. To restore the default value, use the **no** form of this command.

domain-id {*ip-address* [**secondary**] | **null** | **type** *type-value* **value** *hex-value* [**secondary**]}

no domain-id [*ip-address* [**secondary**] | **null** | **type** *type-value* **value** *hex-value* [**secondary**]]

Syntax Description

ip-address	OSPF domain ID in IP address format.
secondary	(Optional) Specifies the secondary domain ID in IP address format.
null	No domain ID is associated with the process.
type *type-value*	OSPF domain ID type in hexadecimal format.
value *hex-value*	OSPF domain ID value in hexadecimal format.
secondary	(Optional) Specifies the secondary domain ID type in hexadecimal format.

Command Default

The default value for the **domain-id** command is equal to the OSPF process ID.

Command Modes

Router configuration

Command History

Release	Modification
12.3(2)	This command was introduced.

Usage Guidelines

The domain ID is an 8-byte value that identifies the OSPF domain of the prefix. When the OSPF route is redistributed to the BGP VPNv4 route in the MPLS VPN context, the domain ID extended community is attached to the BGP update. The domain ID is used on the egress provider-edge (PE) router, when the BGP VPNv4 route is redistributed to OSPF to decide what type of link-state advertisement (LSA) to generate as a result of the redistribution of the BGP VPNv4 route.

Examples

The following example shows how to change the OSPF domain ID using the **domain-id** command where the primary domain ID is a valid IP address and the secondary domain ID is a valid hexadecimal value:

```
Router(config)# router ospf 100 vrf abcd
Router(config-router)# domain-id 10.2.3.4
Router(config-router)# domain-id type 0005 value CAFECAFECAFE secondary
```

domain-tag

To set the Open Shortest Path First (OSPF) domain tag value for Type-5 or Type-7 link-state advertisements (LSAs) when OSPF is used as a protocol between a provider edge (PE) router and customer edge (CE) router, use the **domain-tag** command in router configuration mode. To reinstate the default tag value, use the **no** form of this command.

domain-tag *tag-value*

no domain-tag *tag-value*

Syntax Description

tag-value	Tag value. A 32-bit value entered in decimal format. The default value is calculated based on the Border Gateway Protocol (BGP) autonomous system number of the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP autonomous system (AS) number of the MPLS VPN backbone. If a user specifies the *tag-value*, the value does not have to follow any particular format.

Defaults

The default value is calculated based on the BGP autonomous system number of the MPLS VPN backbone. The four highest bits are set to 1101 according to RFC 1745. The lowest 16 bits map the BGP autonomous system number of the MPLS VPN backbone.

Command Modes

Router configuration

Command History

Release	Modification
12.1(7)	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E.
12.1(7)EC	This command was integrated into Cisco IOS Release 12.1(7)EC.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(2)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When OSPF is used between a PE router and a CE router, BGP routes that come from the MPLS backbone are redistributed to OSPF. These redistributed routes can be announced in Type-3, Type-5, or Type-7 LSAs. If the redistribution of the BGP routes results in Type-5 or Type-7 LSAs, the External Route Tag will be set to the value of the tag. If another PE router receives a Type-5 or Type-7 LSA with an External Route Tag equal to the set tag value, it will ignore the LSA, therefore preventing the redistributed routes that originated from the MPLS backbone from returning via some other location on the MPLS backbone.

Examples

The following example configures the tag value 777:

```
Router(config)# router ospf 10 vrf grc
Router(config-router)# domain-tag 777
```

The **show ip ospf database** command is entered to verify that the tag value 777 has been applied to the External Route Tag:

```
Router# show ospf database external 192.168.50.1

            OSPF Router with ID (192.168.239.66) (Process ID 10)

               Type-5 AS External Link States

  LS age: 18
  Options: (No TOS-capability, DC)
  S Type: AS External Link
  Link State ID: 192.168.238.1 (External Network Number)
  Advertising Router: 192.168.239.66
  LS Seq Number: 80000002
  Checksum: 0xDAB0
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 777
.
.
.
              OSPF Router with ID (198.168.237.56) (Process ID 1)
```

Related Commands

Command	Description
show ospf database	Displays lists of information related to the OSPF database for a specific router.

ignore lsa mospf

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

ignore lsa mospf

no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
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

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

Examples

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

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

interface-id snmp-if-index

To configure Open Shortest Path First (OSPF) interfaces with Simple Network Management Protocol (SNMP) MIB-II interface Index (ifIndex) identification numbers, use the **interface-id snmp-if-index** command in router configuration mode. To revert to the original interface numbering, use the **no** form of this command.

interface-id snmp-if-index

no interface-id snmp-if-index

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP MIB-II ifIndex numbering for interfaces is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6

Usage Guidelines

The advantage to using SNMP MIB-II ifIndex numbers to identify OSPF interfaces is that the ifIndex number corresponds to the number that a user will see reported by SNMP. Using the SNMP MIB-II ifIndex is also suggested, but not required, by RFC 2328 for OSPFv2 and by RFC 2740 for OSPFv3.

If you want to use the SNMP MIB-II ifIndex numbers, all interfaces that have OSPF enabled must have an SNMP ifIndex number assigned or else OSPF will not be enabled on those interfaces.

Note A user may choose not to configure SNMP MIB-II ifIndex numbers in order to maintain consistent behavior across upgrades and among routers that may not have the functionality offered with Cisco IOS Release 12.4(6)T and later releases.

Examples

The following example configures the OSPF interfaces to use SNMP MIB-II ifIndex ID numbers. The output from the **show snmp mib ifmib ifindex** command verifies the configuration.

```
Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# interface-id snmp-if-index
Router(config-router)# end
```

```
Router# show snmp mib ifmib ifindex serial13/0

Serial13/0: Ifindex = 53
Router# show ip ospf 1 1 data router self-originate

            OSPF Router with ID (192.168.3.1) (Process ID 1)

                 Router Link States (Area 1)

  LS age: 66
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 192.168.3.1
  Advertising Router: 192.168.3.1
  LS Seq Number: 80000003
  Checksum: 0xE38F
  Length: 36
  Number of Links: 1

    Link connected to: another Router (point-to-point)
     (Link ID) Neighboring Router ID: 192.168.3.7
     (Link Data) Router Interface address: 0.0.0.49
      Number of MTID metrics: 0
       TOS 0 Metrics: 64
```

Related Commands

Command	Description
show snmp mib ifmib ifindex	Displays SNMP interface index identification numbers (ifIndex values) for all the system interfaces or the specified system interface.

ip ospf area

To enable Open Shortest Path First version 2 (OSPFv2) on an interface, use the **ip ospf area** command in interface configuration mode. To disable OSPFv2 on the interface, use the **no** form of this command.

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

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

Syntax Description

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

Command Default

If the **secondaries none** keywords are entered in the **no** form of this command, the secondary IP addresses will be advertised. If the **secondaries none** keywords are not present, OSPFv2 will be disabled.

Command Modes

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

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(1)SB	This command was integrated into Cisco IOS Release 12.2(1)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

OSPF is enabled on an interface when the network address for the interface matches the range of addresses that is specified by the **network area** command that is entered in router configuration mode. You can enable OSPFv2 explicitly on an interface with the **ip ospf area** command that is entered in interface configuration mode. This capability simplifies the configuration of unnumbered interfaces with different areas.

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

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

Examples

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

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

Related Commands

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

ip ospf authentication

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

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Syntax Description

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

Defaults

The area default is no authentication (null authentication).

Command Modes

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

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.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

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

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

Examples

The following example enables message-digest authentication:

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

Related Commands

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

ip ospf authentication-key

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

ip ospf authentication-key *password*

no ip ospf authentication-key

Syntax Description

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

Defaults

No password is specified.

Command Modes

Interface configuration (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

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

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

Examples

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

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

Related Commands

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

ip ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Open Shortest Path First (OSPF), use the **ip ospf bfd** command in interface configuration mode. To disable BFD on the OSPF interface, use the **disable** keyword. To remove the **ospf bfd** command, use the **no** form of this command.

ip ospf bfd [**disable**]

no ip ospf bfd

Syntax Description

disable	(Optional) Disables BFD for OSPF on a specified interface.

Defaults

When the **disable** keyword is not used, the default behavior is to enable BFD support for OSPF on the interface.

Command Modes

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

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
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

Enter the **ip ospf bfd** command to configure an OSPF interface to use BFD for failure detection. If you have used the **bfd-all interfaces** command in router configuration mode to globally configure all OSPF interfaces for an OSPF process to use BFD, you can enter the **ip ospf bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPF interface.

Examples

In the following example, the interface associated with OSPF, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# ip ospf bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

ip ospf cost

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

ip ospf cost *interface-cost*

no ip ospf cost *interface-cost*

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Defaults

No default cost is predefined.

Command Modes

Interface configuration (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

You can set the metric manually using this command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as this command is not used.

The link-state metric is advertised as the link cost in the router link advertisement. We do not support type of service (ToS), so you can assign only one cost per interface.

In general, the path cost is calculated using the following formula:

10^8 / bandwidth

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785
- 64-kbps serial link—Default cost is 1562
- T1 (1.544-Mbps serial link)—Default cost is 64
- E1 (2.048-Mbps serial link)—Default cost is 48
- 4-Mbps Token Ring—Default cost is 25

- Ethernet—Default cost is 10
- 16-Mbps Token Ring—Default cost is 6
- FDDI—Default cost is 1
- X25—Default cost is 5208
- Asynchronous—Default cost is 10,000
- ATM— Default cost is 1

Examples

The following example sets the interface cost value to 65:

```
ip ospf cost 65
```

ip ospf database-filter all out

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

ip ospf database-filter all out [**disable**]

no ip ospf database-filter all out

Syntax Description

disable	(Optional) Disables the filtering of outgoing LSAs to an OSPF interface; all outgoing LSAs are flooded to the interface. **Note** This keyword is available only in virtual network interface mode.

Defaults

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

Command Modes

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

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.
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

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

If the **ip ospf database-filter all out** 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 prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

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

Related Commands

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

ip ospf dead-interval

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

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

no ip ospf dead-interval

Syntax Description

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

Defaults

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

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.0(23)S	The **minimal** keyword, **hello-multiplier** keyword and *multiplier* argument were added to allow Open Shortest Path First (OSPF) support for fast hello packets.
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 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

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

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

OSPF Support for Fast Hello Packets

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

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

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

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

Examples

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

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

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

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

Related Commands

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

ip ospf demand-circuit

To configure Open Shortest Path First (OSPF) to treat the interface as an OSPF demand circuit, use the **ip ospf demand-circuit** command in interface configuration mode or virtual network interface configuration mode. To remove theOSPF demand circuit functionality from the interface, use the **no** form of this command.

ip ospf demand-circuit [**disable**] [**ignore**]

no ip ospf demand-circuit

Syntax Description

disable	(Optional) Disables OSPF from treating the interface as an OSPF demand circuit. **Note** This keyword is available only in virtual network interface mode.
ignore	(Optional) Ignores requests from other routers to operate the link in demand-circuit mode.

Defaults

The circuit is not an OSPF demand circuit.

Command Modes

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

Command History

Release	Modification
11.2	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** and **ignore** keywords were added. Support was added for this command in virtual network interface configuration mode.
15.1(4)M	This command was integrated into Cisco IOS Release15.1(4)M.

Usage Guidelines

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

If the **ip ospf demand-circuit** 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 configure an OSPF demand circuit for an ISDN on-demand circuit:

```
Router(config)# router ospf 1
Router(config-router)# network 10.0.3.0 255.255.255.0 area 0
Router(config-router)# exit
Router(config)# interface BRI0
Router(config-if)# ip ospf demand-circuit
```

The following example shows how to prevent OSPF demand circuit operation on a multipoint hub interface:

```
Router(config)# interface Dialer0
Router(config-if)# ip ospf network point-to-multipoint
Router(config-if)# ip ospf demand-circuit ignore
```

Related Commands

Command	Description
ip ospf network point-to-multipoint	Configures the OSPF network type to point-to-multipoint.
network area	Defines the interfaces and the area ID for the interfaces on which the OSPF runs.
router ospf	Configures the OSPF routing process.
show ip ospf	Displays information about OSPF routing processes.

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.

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.

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.

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.

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.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Modes

User EXEC
Privileged EXEC

Command History

Mainline Release	Modification
10.0	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
0S Release	**Modification**
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S and the output was expanded to display link-state advertisement (LSA) throttling timers.
12.0(31)S	Support for the Bidirectional Forwarding Detection (BFD) feature was added.
S Release	**Modification**
12.2(14)S	Support for displaying packet pacing timers was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and support for the BFD feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified to show additional information if redistribution is configured with the new nssa-only keyword.
T Release	**Modification**
12.2(4)T	This command was modified to show packet pacing timers in the displayed output.
12.2(15)T	This command was modified to show additional information if the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured.
12.3(2)T	The output of this command was expanded to display LSA throttling timers and the limit on redistributed routes.
12.4(4)T	Support for the BFD feature was added.

Examples

The following is sample output from the **show ip ospf** command when entered without a specific OSPF process ID:

```
Router# show ip ospf
```

```
  Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  LSA group pacing timer 100 secs
  Interface flood pacing timer 55 msecs
  Retransmission pacing timer 100 msecs
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  External flood list length 0
     Area BACKBONE(0)
         Number of interfaces in this area is 2
         Area has message digest authentication
         SPF algorithm executed 4 times
         Area ranges are
         Number of LSA 4. Checksum Sum 0x29BEB
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 3
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
     Area 172.16.26.0
         Number of interfaces in this area is 0
         Area has no authentication
         SPF algorithm executed 1 times
         Area ranges are
            192.168.0.0/16 Passive Advertise
         Number of LSA 1. Checksum Sum 0x44FD
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 1
         Number of indication LSA 1
         Number of DoNotAge LSA 0
         Flood list length 0
```

Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the **show ip ospf** command to verify that the BFD feature has been enabled for OSPF process 123. The relevant command output is shown in bold in the output.

```
Router# show ip ospf

 Routing Process "ospf 123" with ID 172.16.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
   BFD is enabled
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:00:03.708 ago
        SPF algorithm executed 27 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00AEF1
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip ospf Field Descriptions

Field	Description
Routing process "ospf 201" with ID 10.0.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
SPF schedule delay	Delay time (in seconds) of SPF calculations.
Minimum LSA interval	Minimum interval (in seconds) between link-state advertisements.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router.
External flood list length	External flood list length.
BFD is enabled	BFD has been enabled on the OSPF process.

The following is an excerpt of output from the **show ip ospf** command when the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured:

```
Router# show ip ospf
.
.
.
Area 2
   Number of interfaces in this area is 4
   It is a NSSA area
   Perform type-7/type-5 LSA translation, suppress forwarding address
.
.
```

```
.
Routing Process "ospf 1" with ID 192.168.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip ospf Field Descriptions

Field	Description
Area	OSPF area and tag.
Number of interfaces...	Number of interfaces configured in the area.
It is...	Possible types are internal, area border, or autonomous system boundary.
Routing process “ospf 1” with ID 192.168.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
Initial SPF schedule delay	Delay time of SPF calculations at startup.
Minimum hold time	Minimum hold time (in milliseconds) between consecutive SPF calculations.
Maximum wait time	Maximum wait time (in milliseconds) between consecutive SPF calculations.
Incremental-SPF	Status of incremental SPF calculations.
Minimum LSA...	Minimum time interval (in seconds) between link-state advertisements, and maximum arrival time (in milliseconds) of link-state advertisements,
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of...	Number and type of link-state advertisements that have been received.
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.

Table 3 show ip ospf Field Descriptions (continued)

Field	Description
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router listed by type.
External flood list length	External flood list length.

The following is sample output from the **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timers throttle spf** command.

```
Router# show ip ospf 1

 Routing Process "ospf 1" with ID 10.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip ospf Field Descriptions

Field	Description
Routing process “ospf 1” with ID 10.0.0.1	Process ID and OSPF router ID.
Supports ...	Number of Types of Service supported.
It is ...	Possible types are internal, area border, or autonomous system boundary router.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistribution maximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **redistribution maximum-prefix** command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before initial SPF schedule for SPF throttling. Configured with the **timers throttle spf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.

Table 4 show ip ospf Field Descriptions (continued)

Field	Description
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Initial LSA throttle delay 100 msecs
 Minimum hold time for LSA throttle 10000 msecs
 Maximum wait time for LSA throttle 45000 msecs
Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area 24
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 04:28:18.396 ago
        SPF algorithm executed 8 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x23EB9
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The following is sample **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timers throttle spf** command.

```
Router# show ip ospf 1

 Routing Process "ospf 1" with ID 192.168.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip ospf Field Descriptions

Field	Description
Routing process “ospf 1” with ID 192.168.0.0.	Process ID and OSPF router ID.
Supports ...	Number of TOS supported.
It is ...	Possible types are internal, area border, or autonomous system boundary routers.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the **redistribution maximum-prefix** command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the **redistribution maximum-prefix** command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before the initial SPF schedule for SPF throttling. Configured with the **timers throttle spf** command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the **timers throttle spf** command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Initial LSA throttle delay 100 msecs
 Minimum hold time for LSA throttle 10000 msecs
 Maximum wait time for LSA throttle 45000 msecs
Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
```

```
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
   Area 24
       Number of interfaces in this area is 2
       Area has no authentication
       SPF algorithm last executed 04:28:18.396 ago
       SPF algorithm executed 8 times
       Area ranges are
       Number of LSA 4. Checksum Sum 0x23EB9
       Number of opaque link LSA 0. Checksum Sum 0x0
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

show ip ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** command in privileged EXEC mode.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

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.

Examples

The following is sample output from the **show ip ospf border-routers** command:

```
Router# show ip ospf border-routers

OSPF Process 109 internal Routing Table

Codes:  i - Intra-area route, I - Inter-area route

i 192.168.97.53   [10] via 172.16.1.53,   Serial0, ABR,  Area 0.0.0.3, SPF 3
i 192.168.103.51  [10] via 192.168.96.51, Serial0, ABR,  Area 0.0.0.3, SPF 3
I 192.168.103.52  [22] via 192.168.96.51, Serial0, ASBR, Area 0.0.0.3, SPF 3
I 192.168.103.52  [22] via 172.16.1.53,   Serial0, ASBR, Area 0.0.0.3, SPF 3
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip ospf border-routers Field Descriptions

Field	Description
192.168.97.53	Router ID of the destination.
[10]	Cost of using this route.
via 172.16.1.53	Next hop toward the destination.
Serial0	Interface type for the outgoing interface.
ABR	The router type of the destination; it is either an ABR or ASBR or both.

Table 6 show ip ospf border-routers Field Descriptions (continued)

Field	Description
Area	The area ID of the area from which this route is learned.
SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

show ip ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ip ospf database** command in EXEC mode.

show ip ospf [*process-id area-id*] **database**

show ip ospf [*process-id area-id*] **database** [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**database-summary**]

show ip ospf [*process-id*] **database** [**external**] [*link-state-id*]

show ip ospf [*process-id*] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**nssa-external**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**nssa-external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**router**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**router**] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
area-id	(Optional) Area number associated with the OSPF address range defined in the **network** router configuration command used to define the particular area.
adv-router [*ip-address*]	(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as **self-originate**).
link-state-id	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address. When the link state advertisement is describing a network, the *link-state-id* can take one of two forms: The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements). A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).
asbr-summary	(Optional) Displays information only about the autonomous system boundary router summary LSAs.
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database, and the total.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the NSSA external LSAs.
router	(Optional) Displays information only about the router LSAs.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
summary	(Optional) Displays information only about the summary LSAs.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **database-summary** keyword was added.

Release	Modification
12.0	The following keywords were added: • **self-originate** • **adv-router**
12.0(25)S	The output of the **show ip ospf database database-summary** command was increased to include Self-originated Type-7 and Self-originated Type-5 output.
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.

Usage Guidelines

The various forms of this command deliver information about different OSPF link state advertisements.

Examples

The following is sample output from the **show ip ospf database** command when no arguments or keywords are used:

```
Router# show ip ospf database

OSPF Router with id(192.168.239.66) (Process ID 300)

                 Displaying Router Link States(Area 0.0.0.0)

  Link ID       ADV Router    Age        Seq#     Checksum  Link count
172.16.21.6   172.16.21.6    1731    0x80002CFB    0x69BC       8
172.16.21.5   172.16.21.5    1112    0x800009D2    0xA2B8       5
172.16.1.2    172.16.1.2     1662    0x80000A98    0x4CB6       9
172.16.1.1    172.16.1.1     1115    0x800009B6    0x5F2C       1
172.16.1.5    172.16.1.5     1691    0x80002BC     0x2A1A       5
172.16.65.6   172.16.65.6    1395    0x80001947    0xEEE1       4
172.16.241.5  172.16.241.5   1161    0x8000007C    0x7C70       1
172.16.27.6   172.16.27.6    1723    0x80000548    0x8641       4
172.16.70.6   172.16.70.6    1485    0x80000B97    0xEB84       6

                Displaying Net Link States(Area 0.0.0.0)

  Link ID       ADV Router      Age        Seq#       Checksum
172.16.1.3  192.168.239.66     1245    0x800000EC      0x82E

                Displaying Summary Net Link States(Area 0.0.0.0)

  Link ID       ADV Router       Age        Seq#        Checksum
172.16.240.0   172.16.241.5    1152      0x80000077      0x7A05
172.16.241.0   172.16.241.5    1152      0x80000070      0xAEB7
172.16.244.0   172.16.241.5    1152      0x80000071      0x95CB
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip ospf Database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router's ID.
Age	Link state age.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	Fletcher checksum of the complete contents of the link state advertisement.
Link count	Number of interfaces detected for router.

The following is sample output from the **show ip ospf database** command with the **asbr-summary** keyword:

```
Router# show ip ospf database asbr-summary

OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Summary ASB Link States(Area 0.0.0.0)

    LS age: 1463
    Options: (No TOS-capability)
    LS Type: Summary Links(AS Boundary Router)
    Link State ID: 172.16.245.1 (AS Boundary Router address)
    Advertising Router: 172.16.241.5
    LS Seq Number: 80000072
    Checksum: 0x3548
    Length: 28
    Network Mask: 0.0.0.0 TOS: 0  Metric: 1
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip ospf database asbr-summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (autonomous system boundary router).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.

Table 8 show ip ospf database asbr-summary Field Descriptions (continued)

Field	Description
TOS	Type of service.
Metric	Link state metric.

The following is sample output from the **show ip ospf database** command with the **external** keyword:

```
Router# show ip ospf database external

OSPF Router with id(192.168.239.66) (Autonomous system 300)

                   Displaying AS External Link States

LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
       Metric Type: 2 (Larger than any link state path)
       TOS: 0
       Metric: 1
       Forward Address: 0.0.0.0
       External Route Tag: 0
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip ospf database external Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (external network number).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence number (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
Metric Type	External Type.
TOS	Type of service.
Metric	Link state metric.

Table 9 show ip ospf database external Field Descriptions (continued)

Field	Description
Forward Address	Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
External Route Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The following is sample output from the **show ip ospf database** command with the **network** keyword:

```
Router# show ip ospf database network

 OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Net Link States(Area 0.0.0.0)

LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 172.16.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
        Attached Router: 192.168.239.66
        Attached Router: 172.16.241.5
        Attached Router: 172.16.1.1
        Attached Router: 172.16.54.5
        Attached Router: 172.16.1.5
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip ospf database network Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID 300	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type:	Link state type.
Link State ID	Link state ID of designated router.
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.

Table 10 show ip ospf database network Field Descriptions (continued)

Field	Description
AS Boundary Router	Definition of router type.
Attached Router	List of routers attached to the network, by IP address.

The following is sample output from the **show ip ospf database** command with the **router** keyword:

```
Router# show ip ospf database router

OSPF Router with id(192.168.239.66) (Process ID 300)

Displaying Router Link States(Area 0.0.0.0)

LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 172.16.21.6
Advertising Router: 172.16.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
155   Number of Links: 8

Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 172.16.21.5
(Link Data) Router Interface address: 172.16.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip ospf database router Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID.
Advertising Router	Advertising router’s ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
AS Boundary Router	Definition of router type.
Number of Links	Number of active links.
link ID	Link type.

Table 11 show ip ospf database router Field Descriptions (continued)

Field	Description
Link Data	Router interface address.
TOS	Type of service metric (Type 0 only).

The following is sample output from **show ip ospf database** command with the **summary** keyword:

```
Router# show ip ospf database summary

       OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Summary Net Link States(Area 0.0.0.0)

LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 172.16.240.0 (summary Network Number)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0   TOS: 0  Metric: 1
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip ospf database summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link state age.
Options	Type of service options (Type 0 only).
LS Type	Link state type.
Link State ID	Link state ID (summary network number).
Advertising Router	Advertising router's ID.
LS Seq Number	Link state sequence (detects old or duplicate link state advertisements).
Checksum	LS checksum (Fletcher checksum of the complete contents of the link state advertisement).
Length	Length in bytes of the link state advertisement.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link state metric.

The following is sample output from **show ip ospf database** command with the **database-summary** keyword:

```
Router# show ip ospf database database-summary

OSPF Router with ID (10.0.0.1) (Process ID 1)
```

```
Area 0 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   0        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
    Self-originated Type-7  0
Opaque Link     0        0        0
  Opaque Area   0        0        0
  Subtotal      3        0        0

Process 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   0        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Type-5 Ext    0        0        0
      Self-originated Type-5  200
Opaque AS       0        0        0
  Total       203        0        0
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip ospf database database-summary Field Descriptions

Field	Description
Area 0 database summary	Area number.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that area.
Network	Number of network link state advertisements in that area.
Summary Net	Number of summary link state advertisements in that area.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.
Type-7 Ext	Type-7 LSA count.
Self-originated Type-7	Self-originated Type-7 LSA.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count
Subtotal	Sum of LSAs for that area.
Delete	Number of link state advertisements that are marked “Deleted” in that area.
Maxage	Number of link state advertisements that are marked “Maxaged” in that area.
Process 1 database summary	Database summary for the process.
Count	Count of LSAs of the type identified in the first column.
Router	Number of router link state advertisements in that process.

Table 13 show ip ospf database database-summary Field Descriptions (continued)

Field	Description
Network	Number of network link state advertisements in that process.
Summary Net	Number of summary link state advertisements in that process.
Summary ASBR	Number of summary autonomous system boundary router (ASBR) link state advertisements in that process.
Type-7 Ext	Type-7 LSA count.
Opaque Link	Type-9 LSA count.
Opaque Area	Type-10 LSA count.
Type-5 Ext	Type-5 LSA count.
Self-Originated Type-5	Self-originated Type-5 LSA count.
Opaque AS	Type-11 LSA count.
Total	Sum of LSAs for that process.
Delete	Number of link state advertisements that are marked “Deleted” in that process.
Maxage	Number of link state advertisements that are marked “Maxaged” in that process.

show ip ospf events

To display the IP Open Shortest Path First (OSPF) events information, use the **show ip ospf events** command in user EXEC or privileged EXEC mode.

show ip ospf events [**generic**] [**interface**] [**lsa**] [**neighbor**] [**reverse**] [**rib**] [**spf**]

Syntax Description

generic	(Optional) Displays the generic event information.
interface	(Optional) Displays the interface state change event information.
lsa	(Optional) Displays the OSPF Link State Advertisements (LSA) arrival and LSA generation event information.
neighbor	(Optional) Displays the neighbor state change event information.
reverse	(Optional) Displays the events in reverse order.
rib	(Optional) Displays the Routing Information Base (RIB) update, delete, and redistribution event information.
spf	(Optional) Displays the Shortest Path First (SPF) scheduling and SPF run information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(33)SRC	This command was introduced in a release earlier than Cisco IOS Release 12.3(33)SRC.
12.3(33)SRD	This command was integrated into a release earlier than Cisco IOS Release 12.3(33)SRD.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show ip ospf events** command. The fields are self-explanatory.

```
Router# show ip ospf events

OSPF Router with ID (4.4.4.4) (Process ID 1)

1    Jan 22 01:51:03.090: DB free:  1.1.1.10x6CF250 103
2    Jan 22 01:51:03.090: delete MAXAGE lsa:  0x666CF2500x666CF250
3    Jan 22 01:50:56.086: DB free:  1.1.1.10x6025D4 103
4    Jan 22 01:50:56.086: DB free:  1.1.1.10x6D59A0 103
5    Jan 22 01:50:56.082: Insert MAXAGE lsa:  0x666D59A01.1.1.1
6    Jan 22 01:50:55.590: Timer Exp:  if_ack_delayed0x64782774
7    Jan 22 01:50:55.590: Timer Exp:  if_ack_delayed0x64786CB4
8    Jan 22 01:50:55.586: Timer Exp:  if_ack_delayed0x647CD1A8
9    Jan 22 01:50:55.586: Timer Exp:  if_ack_delayed0x647C8134
10   Jan 22 01:50:53.586: Insert MAXAGE lsa:  0x666025D41.1.1.1
11   Jan 22 01:50:53.586: Rcv Changed Type-3 LSA, LSID 1.1.1.1, Adv-Rtr 3.3.3.3, Seq#
80000002, Age 3600, Area 1
12   Jan 22 01:50:53.586: Insert MAXAGE lsa:  0x666D59A01.1.1.1
```

```
13   Jan 22 01:50:53.586: Generate Changed Type-3 LSA, LSID 1.1.1.1, Seq# 80000002, Age
3600, Area 0
14   Jan 22 01:50:53.290: End of SPF, Topo Base, SPF time 4ms, next wait-interval 200ms
15   Jan 22 01:50:53.290: Generic:  ospf_external_route_sync0x1
16   Jan 22 01:50:53.290: Generic:  ospf_external_route_sync0x0
17   Jan 22 01:50:53.290: Generic:  ospf_external_route_sync0x0
18   Jan 22 01:50:53.290: Starting External processing, Topo Base in area 1
19   Jan 22 01:50:53.290: Starting External processing, Topo Base in area 0
20   Jan 22 01:50:53.286: Starting External processing, Topo Base
21   Jan 22 01:50:53.286: Generic:  ospf_inter_route_sync0x0
22   Jan 22 01:50:53.286: Starting summary processing, Topo Base, Area 0
23   Jan 22 01:50:53.286: Generic:  ospf_inter_route_sync0x1
24   Jan 22 01:50:53.286: Generic:  post_spf_intra0x0
25   Jan 22 01:50:53.286: Generic:  ospf_intra_route_sync0x1
26   Jan 22 01:50:53.286: Generic:  update_rtr_route0x1
27   Jan 22 01:50:53.286: Generic:  update_rtr_route0x1
28   Jan 22 01:50:53.286: Generic:  update_rtr_route0x1
29   Jan 22 01:50:53.286: Starting Intra-Area SPF, Topo Base, Area 1, spf_type Full
30   Jan 22 01:50:53.286: Starting SPF, Topo Base, wait-interval 200ms
31   Jan 22 01:50:53.118: Rcv New Type-3 LSA, LSID 1.1.1.1, Adv-Rtr 3.3.3.3, Seq#
80000001, Age 1, Area 1
32   Jan 22 01:50:53.118: DB add:  1.1.1.10x6025D4 103
33   Jan 22 01:50:53.090: Insert MAXAGE lsa:  0x666CF2501.1.1.1
34   Jan 22 01:50:53.090: Rcv Changed Type-3 LSA, LSID 1.1.1.1, Adv-Rtr 3.3.3.3, Seq#
80000002, Age 3600, Area 0
35   Jan 22 01:50:53.086: Rcv Changed Type-1 LSA, LSID 1.1.1.1, Adv-Rtr 1.1.1.1, Seq#
80000008, Age 2, Area 1
36   Jan 22 01:50:53.086: Schedule SPF, Topo Base, Area 1, spf-type Full, Change in LSA
Type R, LSID 1.1.1.1, Adv-Rtr 1.1.1.1
37   Jan 22 01:50:46.310: Timer Exp:  exfaddr0x0
38   Jan 22 01:50:16.310: Timer Exp:  exfaddr0x0
```

show ip ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ip ospf flood-list** command in EXEC mode.

show ip ospf flood-list *interface-type interface-number*

Syntax Description

interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

EXEC

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

Use this command to observe OSPF packet pacing.

Examples

The following is sample output of the **show ip ospf flood-list** command:

```
Router# show ip ospf flood-list ethernet 1

 Interface Ethernet1, Queue length 20
 Link state flooding due in 12 msec

 Type  LS ID            ADV RTR           Seq NO      Age    Checksum
    5  10.2.195.0       192.168.0.163     0x80000009  0      0xFB61
    5  10.1.192.0       192.168.0.163     0x80000009  0      0x2938
    5  10.2.194.0       192.168.0.163     0x80000009  0      0x757
    5  10.1.193.0       192.168.0.163     0x80000009  0      0x1E42
    5  10.2.193.0       192.168.0.163     0x80000009  0      0x124D
    5  10.1.194.0       192.168.0.163     0x80000009  0      0x134C
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip ospf flood-list Field Descriptions

Field	Description
Interface Ethernet1	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state flooding due in	Length of time before next link-state transmission.
Type	Type of LSA.

Table 14 show ip ospf flood-list Field Descriptions (continued)

Field	Description
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ip ospf interface

To display interface information related to Open Shortest Path First (OSPF), use the **show ip ospf interface** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **interface** [*type number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}]

Syntax Description

process-id	(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. Range is from 1 to 65535.
type	(Optional) Interface type. If the *type* argument is included, only information for the specified interface type is included.
number	(Optional) Interface number. If the *number* argument is included, only information for the specified interface number is included.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.
multicast	(Optional) Displays multicast information.
topology *topology-name*	(Optional) Displays OSPF-related information about the named topology instance.
topology base	(Optional) Displays OSPF-related information about the base topology.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(25)S	The **brief** keyword was added.
12.2(15)T	The **brief** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **multicast**, **topology**, **base**, and *topology-name* keywords and argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for the OSPF TTL Security Check feature was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Examples

The following is sample output from the **show ip ospf interface** command when Ethernet interface 0/0 is specified:

```
Router# show ip ospf interface ethernet 0/0
```

```
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.254.202/24, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.1, Interface address 192.168.254.202
  Backup Designated router (ID) 192.168.254.10, Interface address 192.168.254.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.254.10  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Cisco IOS Release 12.2(33)SRB

The following sample output from the **show ip ospf interface brief topology VOICE** command shows a summary of information, including a confirmation that the Multitopology Routing (MTR) VOICE topology is configured in the interface configuration:

```
Router# show ip ospf interface brief topology VOICE

VOICE Topology (MTID 10)

Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               10.0.0.2/32        1     LOOP  0/0
Se2/0        1     0               10.1.0.2/30        10    P2P   1/1
```

The following sample output from the **show ip ospf interface topology VOICE** command displays details of the MTR VOICE topology for the interface. When the command is entered without the **brief** keyword, more information is displayed.

```
Router# show ip ospf interface topology VOICE

                 VOICE Topology (MTID 10)

Loopback0 is up, line protocol is up
   Internet Address 10.0.0.2/32, Area 0
   Process ID 1, Router ID 10.0.0.2, Network Type LOOPBACK
   Topology-MTID    Cost    Disabled    Shutdown      Topology Name
         10          1        no          no            VOICE
   Loopback interface is treated as a stub Host Serial2/0 is up, line protocol is up
   Internet Address 10.1.0.2/30, Area 0
   Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT
   Topology-MTID    Cost    Disabled    Shutdown      Topology Name
         10          10       no          no            VOICE
   Transmit Delay is 1 sec, State POINT_TO_POINT
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     oob-resync timeout 40
     Hello due in 00:00:03
   Supports Link-local Signaling (LLS)
   Cisco NSF helper support enabled
   IETF NSF helper support enabled
   Index 1/1, flood queue length 0
   Next 0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 1
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.0.0.1
   Suppress hello for 0 neighbor(s)
```

Cisco IOS Release 12.2(33)SRC

The following sample output from the **show ip ospf interface** command displays details about the configured Time-to-Live (TTL) limits:

```
Router# show ip ospf interface ethernet 0
.
.
.
Strict TTL checking enabled
! or a message similar to the following is displayed
Strict TTL checking enabled, up to 4 hops allowed
.
.
.
```

Table 15 describes the significant fields shown in the displays.

Table 15 show ip ospf interface Field Descriptions

Field	Description
Ethernet	Status of the physical link and operational status of the protocol.
Process ID	OSPF process ID.
Area	OSPF area.
Cost	Administrative cost assigned to the interface.
State	Operational state of the interface.
Nbrs F/C	OSPF neighbor count.
Internet Address	Interface IP address, subnet mask, and area address.
Topology-MTID	MTR topology Multitopology Identifier (MTID). A number assigned so that the protocol can identify the topology associated with information that it sends to its peers.
Transmit Delay	Transmit delay in seconds, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Strict TTL checking enabled	Only one hop is allowed.
Strict TTL checking enabled, up to 4 hops allowed	A set number of hops has been explicitly configured.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

show ip ospf max-metric

To display IP Open Shortest Path First (OSPF) max-metric origination information, use the **show ip ospf max-metric** command in user EXEC or privileged EXEC mode.

show ip ospf max-metric [**multicast topology** | **topology**] [*topology-name* | **base**]

Syntax Description

multicast	(Optional) Specifies the multicast topology.
topology	(Optional) Specifies the unicast or the multicast topology.
topology-name	(Optional) The multicast topology name.
base	(Optional) Specifies the multicast or unicast base topology.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Mainline Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show ip ospf max-metric** command. The fields are self-explanatory.

```
Router# show ip ospf max-metric

OSPF Router with ID (190.0.30.1) (Process ID 2)

Base Topology (MTID 0)Start time: 3d12h, Time elapsed: 00:01:07.964
Originating router-LSAs with maximum metric
Condition: always, State: active
Advertise external-LSAs with metric 16711680
```

show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in privileged EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.
neighbor-id	(Optional) Neighbor hostname or IP address in A.B.C.D format.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
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.
12.2(33)SRC	Support for the OSPF TTL Security Check feature was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Examples

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor:

```
Router# show ip ospf neighbor

Neighbor ID    Pri   State        Dead Time     Address         Interface
10.199.199.137  1    FULL/DR       0:00:31    192.168.80.37      Ethernet0
172.16.48.1     1    FULL/DROTHER  0:00:33    172.16.48.1        Fddi0
172.16.48.200   1    FULL/DROTHER  0:00:33    172.16.48.200      Fddi0
10.199.199.137  5    FULL/DR       0:00:33    172.16.48.189      Fddi0
```

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
Router# show ip ospf neighbor 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:04
 Neighbor 10.199.199.137, interface address 172.16.48.189
```

```
    In the area 0.0.0.0 via interface Fddi0
    Neighbor priority is 5, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:03
```

If you specify the interface along with the neighbor ID, the system displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
Router# show ip ospf neighbor ethernet 0 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:37
    Link State retransmission due in 0:00:04
```

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
Router# show ip ospf neighbor fddi 0

   ID           Pri   State         Dead Time     Address         Interface
172.16.48.1      1    FULL/DROTHER  0:00:33    172.16.48.1       Fddi0
172.16.48.200    1    FULL/DROTHER  0:00:32    172.16.48.200     Fddi0
10.199.199.137   5    FULL/DR       0:00:32    172.16.48.189     Fddi0
```

The following is sample output from the **show ip ospf neighbor detail** command:

```
Router# show ip ospf neighbor detail

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface GigabitEthernet1/0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
   Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Table 16 describes the significant fields shown in the displays.

Table 16 show ip ospf neighbor detail Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state. If one OSPF neighbor has enabled TTL security, the other side of the connection will show the neighbor in INIT state.
state changes	Number of state changes since the neighbor was created.This value can be reset using the **clear ip ospf counters neighbor** command.

Table 16 show ip ospf neighbor detail Field Descriptions (continued)

Field	Description
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
LLS Options..., last OOB-Resync	Link-Local Signaling and out-of-band (OOB) link-state database resynchronization performed hours:minutes:seconds ago. This is Nonstop Forwarding (NSF) information. The field indicates the last successful out-of-band resynchronization with the NSF-capable router.
Dead timer due in	Expected time in hours:minutes:seconds before Cisco IOS software will declare the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into the two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been re-sent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

Cisco IOS Release 12.2(33)SRC

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor. If one OSPF neighbor has enabled TTL security, the other side of the connection will show the neighbor in INIT state.

```
Router# show ip ospf neighbor

Neighbor ID   Pri   State        Dead Time     Address         Interface
10.199.199.137  1    FULL/DR       0:00:31    192.168.80.37      Ethernet0
172.16.48.1     1    FULL/DROTHER  0:00:33    172.16.48.1        Fddi0
172.16.48.200   1    FULL/DROTHER  0:00:33    172.16.48.200      Fddi0
10.199.199.137  5    FULL/DR       0:00:33    172.16.48.189      Fddi0
172.16.1.201   1   INIT/DROTHER  00.00.35  10.1.1.201        Ethernet0/0
```

show ip ospf nsf

To display IP Open Shortest Path First (OSPF) Nonstop Forwarding (NSF) state information, use the **show ip ospf nsf** command in user EXEC or privileged EXEC mode.

show ip ospf nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Mainline Release	Modification
12.2(33)SXI	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show ip ospf nsf** command. The fields are self-explanatory.

```
Router# show ip ospf nsf

Routing Process "ospf 2" IETF NSF helper support enabled
Cisco NSF helper support enabled OSPF restart state is NO_RESTART
Handle 1786466308, Router ID 190.0.30.1, checkpoint Router ID 0.0.0.0
Config wait timer interval 10, timer not running
Dbase wait timer interval 120, timer not running
```

show ip ospf nsr

To display IP Open Shortest Path First (OSPF) nonstop routing (NSR) status information, use the **show ip ospf nsr** command in privileged EXEC mode.

show ip ospf [*process-id***] nsr** [[**objects**] | [**statistics**]]

Syntax Description

process-id	(Optional) Process ID. If this argument is used, only information for the specified OSPF routing process is included.
objects	(Optional) Displays information on the OSPF NSR objects in the different OSPF routing processes.
statistics	(Optional) Displays OSPF NSR statistical information for the different OSPF routing processes.

Command Modes

Privileged EXEC (#)

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.

Examples

The following sample output from the **show ip ospf nsr** command shows that OSPF on the standby RP is fully synchronized and ready to continue operation if the active RP fails or if a manual switchover is performed. NSR is configured and enabled for the “ospf 1” OSPF routing process. The fields are self-explanatory.

```
Router# show ip ospf 1 nsr

Active RP
Operating in duplex mode
Redundancy state: ACTIVE
Peer redundancy state: STANDBY HOT
Checkpoint peer ready
Checkpoint messages enabled
ISSU negotiation complete
ISSU versions compatible

Routing Process "ospf 1" with ID 10.1.1.100
NSR configured
Checkpoint message sequence number: 6360
Standby synchronization state: synchronized
Bulk sync operations:  1
Next sync check time:  18:48:27.097 PST Fri Dec 10 2010
LSA Count: 3301, Checksum Sum 0x06750217
```

Related Commands

Command	Description
nsr	Enables NSR on a router that is running OSPF.

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ip ospf request-list** command in EXEC mode.

show ip ospf request-list [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface from this neighbor.

Command Modes

EXEC

Command History

Release	Modification
10.2	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 information displayed by the **show ip ospf request-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ip ospf request-list** command:

```
Router# show ip ospf request-list serial 0

             OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface Serial0 address 172.16.1.12

  Type  LS ID          ADV RTR         Seq NO      Age    Checksum
     1  192.168.1.12     192.168.1.12      0x8000020D  8      0x6572
```

Table 17 describes the significant fields shown in the displays.

Table 17 show ip ospf request-list Field Descriptions

Field	Description
Type	LSA-type.
LS ID	IP address of the neighbor router.

Table 17 show ip ospf request-list Field Descriptions (continued)

Field	Description
ADV RTR	IP address of the advertising router.
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ip ospf retransmission-list** command in EXEC mode.

show ip ospf retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface-neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

EXEC

Command History

Release	Modification
10.2	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 information displayed by the **show ip ospf retransmission-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ip ospf retransmission-list** command:

```
Router# show ip ospf retransmission-list serial 0

             OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface Serial0 address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2

  Type  LS ID            ADV RTR          Seq NO      Age    Checksum
     1  192.168.1.12     192.168.1.12     0x80000210  0      0xB196
```

Table 18 describes the significant fields shown in the displays.

Table 18 show ip ospf retransmission-list Field Descriptions

Field	Description
Type	LSA-type.
LS ID	IP address of the neighbor router.
ADV RTR	IP address of the advertising router.

Table 18 show ip ospf retransmission-list Field Descriptions (continued)

Field	Description
Seq NO	Packet sequence number of the LSA.
Age	Age, in seconds, of the LSA.
Checksum	Checksum number of the LSA.

show ip ospf rib

To display information for the OSPF local Routing Information Base (RIB) or locally redistributed routes, use the **show ip ospf rib** command in privileged EXEC mode.

show ip ospf *process-id* **rib** [**redistribution**] [*network-prefix*] [*network-mask*] [**detail**]

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.
redistribution	(Optional) Displays IP OSPF redistribution RIB information.
network-prefix	(Optional) Network prefix. Displays paths for a specific route.
network-mask	(Optional) IP address mask. Displays paths for all routes under a major network.
detail	(Optional) Displays more detailed information about the OSPF local RIB.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If the *network-prefix* and *network-mask* arguments are both entered, only the route that matches the network prefix and IP address mask is displayed. If only the *prefix* argument is entered, a longest prefix lookup is performed and the matching route is displayed.

Examples

The following example displays information about locally redistributed routes:

```
Router# show ip ospf 1 rib redistribution 192.168.240.0

OSPF Redistribution for Process 1
192.168.240/20, metric 0, tag 0, from OSPF Router 130
 Attributes 0x1000220, event 1
  via Ethernet0/0
OSPF Redistribution Process 130
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip ospf rib redistribution Field Descriptions

Field	Description
OSPF Redistribution for Process 1	Routing redistribution information for OSPF process 1.
192.168.240/20	Network number and mask.
metric 0	OSPF metric type.

Table 19 show ip ospf rib redistribution Field Descriptions (continued)

Field	Description
tag 0	OSPF process tag identifier.
from OSPF Router	OSPF router from which routing information was redistributed.
Attributes 0x1000220	OSPF attribute.
event	OSPF redistribution event 1.
Via Ethernet0/0	The interface through which routing information has been redistributed.
OSPF Redistribution Process	Routing redistribution information for OSPF process 13.

show ip ospf sham-links

To display information about all sham links configured for a provider edge (PE) router in the Virtual Private Network (VPN) backbone, use the **show ip ospf sham-links** command in EXEC mode.

show ip ospf sham-links

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST, and support for Cisco 12000 series Internet Routers was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and support for Cisco 10000 series Internet Routers 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.

Usage Guidelines

Use this command to display Open Shortest Path First (OSPF) information about the sham-links configured on a PE router.

Examples

The following example shows sample output from the **show ip ospf sham-links** command for a PE router in the VPN backbone:

```
Router1# show ip ospf sham-links

Sham Link OSPF_SL0 to address 10.44.0.1 is up
 Area 120 source address 10.0.0.1
   Run as demand circuit
   DoNotAge LSA allowed., Cost of using 1
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
     Adjacency State FULL (Hello suppressed)
     Index 2/2, retransmission queue length 0, number of retransmission 27
     First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
     Last retransmission scan length is 0, maximum is 2
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ip ospf statistics

To display Open Shortest Path First (OSPF) shortest path first (SPF) calculation statistics, use the **show ip ospf statistics** command in user EXEC or privileged EXEC mode.

show ip ospf statistics [**detail**]

Syntax Description

detail	(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	The command was integrated into Cisco IOS Release 12.2(18)S.
12.3(2)T	The command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

The **show ip ospf statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ip ospf statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following is sample output from the **show ip ospf statistics** command that shows a single line of information for each SPF calculation:

```
Router# show ip ospf statistics

OSPF process ID 200
------------------------------------------

  Area 0: SPF algorithm executed 10 times

  Area 200: SPF algorithm executed 8 times

  Summary OSPF SPF statistic

  SPF calculation time
Delta T    Intra   D-Intra   Summ   D-Summ   Ext   D-Ext   Total   Reason
08:17:16   0       0         0      0       0      0       0       R,
08:16:47   0       0         0      0       0      0       0       R, N,
08:16:37   0       0         0      0       0      0       0       R, X
00:04:40   208     40        208    44      220    0       720     R, N, SN, X
00:03:15   0       112       4      108     8      96      328     R, N, SN, X
00:02:55   164     40        176    44      188    0       612     R, N, SN, X
00:01:49   0       4         4      0       4      4       16      R, N, SN, X
00:01:48   0       0         4      0       4      0       12      R, N, SN, SA, X
```

```
00:01:43   0       0          4      0       4      0       8       R,
00:00:53   164     40         176    44      188    0       612     R, N, SN, X
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip ospf statistics Field Descriptions

Field	Description
OSPF process ID	A unique value assigned to the OSPF process in the configuration.
Area	OSPF area ID.
SPF algorithm executed	Number of times SPF algorithm has been executed for the particular area.
Delta T	Amount of time in milliseconds that has passed from when SPF started its calculation to the current time.
Intra	Time in milliseconds for the SPF algorithm to process intra-area LSAs and install intra-area routes in the routing table.
D-Intra	Time in milliseconds for the SPF algorithm to delete invalid intra-area routes from the routing table.
Summ	Time in milliseconds for the SPF algorithm to process interarea LSAs and install interarea routes in the routing table.
D-Summ	Time in milliseconds for the SPF algorithm to delete invalid interarea routes from the routing table.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and install external and NSSA routes in the routing table.
D-Ext	Time in milliseconds for the SPF algorithm to delete invalid external and NSSA routes from the routing table.
Total	Total duration time, in milliseconds, for the SPF algorithm process.
Reason	Record of reasons causing SPF to be executed: • N—A change in a network LSA (type 2) has occurred. • R—A change in a router LSA (type 1) has occurred. • SA—A change in a Summary autonomous system boundary router (ASBR) (SA) LSA has occurred. • SN—A change in a Summary Network (SN) LSA has occurred. • X—A change in an External Type-7 (X7) LSA has occurred.

The following is sample output from the **show ip ospf statistics** command with the **detail** keyword entered to show the statistics separately for a specific area:

```
Router# show ip ospf statistics detail

SPF 7 executed 2d17h ago, SPF type Full

  SPF calculation time (in msec):

  SPT   Intra   D-Intr   Summ   D-Summ   Ext7   D-Ext7   Total

  0     0       0        0      0        0      0        0
  LSIDs processed R:4 N:1 Stub:5 SN:17 SA:1 X7:0

  Change record R,

  LSIDs changed 1

  Last 10 LSIDs:

2.0.0.202(R)
```

Table 21 describes the significant fields shown in the display.

Table 21 show ip ospf statistics detail Field Descriptions

Field	Description
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds requires to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) link-state advertisements (LSAs) and install external and NSSA routes in the routing table.
Total	Total duration time, in milliseconds, for the SPF algorithm process. **Note** Total time is the sum of previous times excluding the SPT time, which is already included in the Intra time.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N—Network LSA. • R—Router LSA. • SA—Summary autonomous system boundary router (ASBR) (SA) LSA. • SN—Summary Network (SN) LSA. • Stub—Stub links. • X7—External Type-7 (X7) LSA.

Table 21 show ip ospf statistics detail Field Descriptions (continued)

Field	Description
LSIDs changed	Number of LSAs changed between this SPF calculation and the previous one. LSA changes force SPF to be scheduled.
Last 10 LSIDs	List of last ten Intra area LSAs that have changed between this SPF calculation and the previous one. LSID types: • R—Router LSA (type 1) • N—Network LSA (type 2)

show ip ospf summary-address

To display a list of all summary address redistribution information configured under an Open Shortest Path First (OSPF) process, use the **show ip ospf summary-address** command in EXEC mode.

show ip ospf [*process-id*] **summary-address**

Syntax Description

process-id	(Optional) OSPF area ID.

Command Modes

EXEC

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 *process-id* argument can be entered as a decimal number or as an IP address format.

Examples

Cisco IOS Release 10.0 and 12.2SX

The following is sample output from the **show ip ospf summary-address** command:

```
Router# show ip ospf summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric 4294967295, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric 4294967295, Type 0, Tag 10
```

Cisco IOS Release 12.2SR

The following is sample output from the **show ip ospf summary-address** command:

```
Router# show ip ospf summary-address

OSPF Router with ID(10.1.1.1)(Process ID 1)

10.2.0.0/255.255.0.0 Metric 4294967295, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric 4294967295, Type 0, Tag 10
```

Table 22 describes the significant fields shown in the displays.

Table 22 show ip ospf summary-address Field Descriptions

Field	Description
10.2.0.0/255.255.0.0	IP address and mask of the router for the OSPF process.
Metric 4294967295	OSPF metric type.
Type 0	Type of LSA.
Tag 0	OSPF process tag identifier.

show ip ospf timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ip ospf timers rate-limit** command in privileged EXEC mode.

show ip ospf timers rate-limit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(25)S	This command was introduced.
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.

Usage Guidelines

Use this command if you need to see when LSAs in the queue will be sent.

Examples

The following is sample output from the **show ip ospf timers rate-limit** command:

```
Router# show ip ospf timers rate-limit

LSAID: 10.1.1.1    Type: 1   Adv Rtr: 172.16.2.2 Due in: 00:00:00.028
LSAID: 172.16.4.1   Type: 3   Adv Rtr: 172.16.2.2 Due in: 00:00:00.028
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip ospf timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of advertising router.
Due in	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ip ospf traffic

To display Open Shortest Path First (OSPF) traffic statistics, use the **show ip ospf traffic** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) Process ID. If the *process-id* argument is included, only information for the specified routing process is displayed.
interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.

Command Default

When the **show ip ospf traffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per-OSPF process statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.4(6)T	Support for the OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3 feature was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRC	Support for the OSPF TTL Security Check feature was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPF process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the *interface-type* and *interface-number* arguments. To reset counters and clear statistics, use the **clear ip ospf traffic** command.

Examples

Cisco IOS Release 12.0(28)S

The following is sample output from the **show ip ospf traffic** command.

```
Router# show ip ospf traffic

OSPF statistics:
  Rcvd: 5300 total, 730 checksum errors
        333 hello, 10 database desc, 3 link state req
        24 link state updates, 13 link state acks

  Sent: 264 total
        222 hello, 12 database desc, 3 link state req
        17 link state updates, 12 link state acks

           OSPF Router with ID (10.0.1.2) (Process ID 100)

OSPF queues statistic for process ID 100:

  OSPF Hello queue size 0, no limit, max size 3
  OSPF Router queue size 0, limit 200, drops 0, max size 3

Interface statistics:

    Interface Loopback0

OSPF packets received/sent
     Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx:  0        0        0        0        0        0        0
Tx:  0        0        0        0        0        0        0

OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, LLS 0,
  Authentication 0,

OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,

     Interface Serial3/0

  OSPF packets received/sent
      Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx:   0        111      3        1        7        6        128
Tx:   0        111      4        1        12       5        133

  OSPF header errors
    Length 0, Checksum 0, Version 0, Bad Source 0,
    No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
    Self Originated 0, Duplicate ID 0, LLS 0,
    Authentication 0,

  OSPF LSA errors
    Type 0, Length 0, Data 0, Checksum 0,

    Interface Serial2/0

  OSPF packets received/sent
      Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx:   0        0        0        0        0        0        0
Tx:   0        0        0        0        0        0        0
  OSPF header errors
    Length 0, Checksum 0, Version 0, Bad Source 0,
    No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
    Self Originated 0, Duplicate ID 0, LLS 0,
    Authentication 0,

OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,

  Interface Ethernet0/0
  OSPF packets received/sent
       Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx:    0        222      7        2        17       7        255
Tx:    0        111      8        2        5        7        133

OSPF header errors
  Length 0, Checksum 730, Version 800, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 3387, Duplicate ID 0, LLS 0,
  Authentication 0,

OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,

Summary traffic statistics for process ID 100:
  Rcvd: 5300 total, 4917 errors
        333 hello, 10 database desc, 3 link state req
        24 link state upds, 13 link state acks, 0 invalid
  Sent: 266 total
        222 hello, 12 database desc, 3 link state req
        17 link state upds, 12 link state acks, 0 invalid
```

Table 24 describes the significant fields shown in the display.

Table 24 show ip ospf traffic Field Descriptions

Field	Description
OSPF statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPF queues statistic for process ID	Statistics specific to Cisco IOS software.
OSPF Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPF hello process for all received OSPF packets.
OSPF Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPF process ID.
OSPF packets received/sent	Number of OSPF packets received and sent on the interface, sorted by packet types.
OSPF header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPF packet. The discarded packet is counted under the appropriate discard reason. Number of packets dropped due to TTL security check is displayed if that feature has been configured.

Table 24 show ip ospf traffic Field Descriptions (continued)

Field	Description
OSPF LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPF process. **Note** The OSPF process ID is a unique value assigned to the OSPF process in the configuration. The value for the received errors is the sum of the OSPF header errors that are detected by the OSPF process, unlike the sum of the checksum errors that are listed in the global OSPF statistics.

Cisco IOS Release 12.2(33)SRC

The following is sample output from the **show ip ospf traffic** command. The output has been modified to include the number of packets dropped due a TTL security check.

```
Router# show ip ospf traffic
.
.
.
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, LLS 0,
  Authentication 0, TTL Check Fail 2,
.
```

Cisco IOS Release 12.4(6)T

The following is sample output from the **show ip ospf traffic** command that displays the detailed traffic information for OSPF packets received and sent on each OSPF interface and OSPF process.

```
Router# show ip ospf traffic

OSPF statistics:
.
.
.

    Interface Ethernet0/0.1

OSPF packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0

  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216

.
.
.
    Interface Serial2/0

OSPF packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   528
  RX DB des     4                    148
  RX LS req     1                    60
  RX LS upd     3                    216
  RX LS ack     2                    128
  RX Total      21                   1080

  TX Failed     0                    0
  TX Hello      14                   1104
  TX DB des     3                    252
  TX LS req     1                    56
  TX LS upd     3                    392
  TX LS ack     2                    128
  TX Total      23                   1932
.
.
.
    Interface Ethernet0/0

OSPF packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      13                   620
  RX DB des     3                    116
  RX LS req     1                    36
  RX LS upd     3                    228
  RX LS ack     4                    216
  RX Total      24                   1216

  TX Failed     0                    0
  TX Hello      17                   1344
  TX DB des     4                    276
  TX LS req     1                    56
  TX LS upd     7                    656
  TX LS ack     2                    128
  TX Total      31                   2460

.
.
.

Summary traffic statistics for process ID 1:

OSPF packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      24                   1148
  RX DB des     7                    264
  RX LS req     2                    96
  RX LS upd     6                    444
  RX LS ack     6                    344
  RX Total      45                   2296

  TX Failed     0                    0
  TX Hello      31                   2448
  TX DB des     7                    528
  TX LS req     2                    112
  TX LS upd     10                   1048
  TX LS ack     4                    256
  TX Total      54                   4392

OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,

OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

To start collecting new statistics, reset the counters and clear the traffic statistics by entering the **clear ip ospf traffic** command as follows:

```
Router# clear ip ospf traffic
```

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffics statistics.
show ipv6 ospf traffic	Displays OSPFv3 traffic statistics.

show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ip ospf virtual-links** command in EXEC mode.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

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 information displayed by the **show ip ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ip ospf virtual-links** command:

```
Router# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Table 25 describes the significant fields shown in the display.

Table 25 show ip ospf virtual-links Field Descriptions

Field	Description
Virtual Link to router 192.168.101.2 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Transit area 0.0.0.1	The transit area through which the virtual link is formed.
via interface Ethernet0	The interface through which the virtual link is formed.
Cost of using 10	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.

Table 25 show ip ospf virtual-links Field Descriptions (continued)

Field	Description
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:08	When the next hello is expected from the neighbor.
Adjacency State FULL	The adjacency state between the neighbors.

show ipv6 ospf traffic

To display IPv6 Open Shortest Path First Version 3 (OSPFv3) traffic statistics, use the **show ipv6 ospf traffic** command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) OSPF process ID for which you want traffic statistics (for example, queue statistics, statistics for each interface under the OSPF process, and per OSPF process statistics).
interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.

Command Default

When the **show ipv6 ospf traffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per OSPF process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPF process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the *interface-type* and *interface-number* arguments. To reset counters and clear statistics, use the **clear ipv6 ospf traffic** command.

Examples

The following example shows the display output for the **show ipv6 ospf traffic** command for OSPFv3:

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored

  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)

OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2


Interface statistics:


    Interface Serial2/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852

  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


    Interface Ethernet0/0

OSPFv3 packets received/sent

  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960

  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308

OSPFv3 header errors
```

```
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,


Summary traffic statistics for process ID 6:

OSPFv3 packets received/sent

  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      11                    436
  RX DB des     7                     316
  RX LS req     2                     104
  RX LS upd     9                     692
  RX LS ack     4                     264
  RX Total      33                    1812

  TX Failed     0                     0
  TX Hello      19                    724
  TX DB des     12                    456
  TX LS req     2                     104
  TX LS upd     8                     628
  TX LS ack     6                     296
  TX Total      47                    2208

OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The network administrator wants to start collecting new statistics, resetting the counters and clearing the traffic statistics by entering the **clear ipv6 ospf traffic** command as follows:

```
Router# clear ipv6 ospf traffic
```

Table 26 describes the significant fields shown in the display.

Table 26 show ipv6 ospf traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPF hello process for all received OSPF packets.

Table 26 show ipv6 ospf traffic Field Descriptions (continued)

Field	Description
Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPF process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPF statistics.

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.

shutdown (router OSPF)

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the **shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

OSPF stays active under the current instance.

Command Modes

Router configuration (config-router)

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.

Usage Guidelines

Use the **shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

Examples

The following example shows how to enable a graceful shutdown of the OSPF protocol:

```
Router(config)# router ospf 1
Router(config-router)# shutdown
```

Related Commands

Command	Description
ip ospf shutdown	Initiates a graceful shutdown on a specific OSPF interface.

snmp-server enable traps ospf

To enable all Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF), use the **snmp-server enable traps ospf** command in global configuration mode. To disable all SNMP notifications for OSPF, use the **no** form of this command.

snmp-server enable traps ospf

no snmp-server enable traps ospf

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications for OSPF are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

If you wish to enable or disable specific OSPF SNMP notifications, enter one or more of the following commands of the following commands:

[**no**] **snmp-server enable traps ospf cisco-specific errors**

[**no**] **snmp-server enable traps ospf cisco-specific lsa**

[**no**] **snmp-server enable traps ospf cisco-specific retransmit**

[**no**] **snmp-server enable traps ospf cisco-specific state-change**

[**no**] **snmp-server enable traps ospf errors**

[**no**] **snmp-server enable traps ospf lsa**

[**no**] **snmp-server enable traps ospf retransmit**

[**no**] **snmp-server enable traps ospf state-change**

Examples

The following exampleglobally enables SNMP notifications for OSPF:

```
Router(config)# snmp-server enable traps ospf
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) configuration mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors** command in global configuration mode. To disable SNMP notifications for OSPF configuration mismatch errors, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors [**config-error**] [**virt-config-error**]

no snmp-server enable traps ospf cisco-specific errors [**config-error**] [**virt-config-error**]

Syntax Description

config-error	(Optional) Enables SNMP notifications only for configuration mismatch errors on nonvirtual interfaces.
virt-config-error	(Optional) Enables SNMP notifications only for configuration mismatch errors on virtual interfaces.

Command Default

SNMP notifications for OSPF configuration mismatch errors are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

To enable the SNMP notifications for OSPF configuration errors for both virtual and nonvirtual interfaces, enter the **snmp-server enable traps ospf cisco-specific errors** command in global configuration mode without the optional keywords.

Examples

The following example enables the router to send OSPF configuration mismatch errors only for nonvirtual interfaces:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors config-error

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error

no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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 the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors shamlink

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) sham-link errors, use the **snmp-server enable traps ospf cisco-specific errors shamlink** command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]

no snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]

Syntax Description

authentication	(Optional) Enables SNMP notifications only for authentication failures on OSPF sham-link interfaces.
bad-packet	(Optional) Enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces.
config	(Optional) Enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF sham-link errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(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 the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send OSPF sham-link error notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific lsa

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) opaque link-state advertisements (LSAs), use the **snmp-server enable traps ospf cisco-specific lsa** command in global configuration mode. To disable SNMP notifications for OSPF opaque LSAs, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific lsa [**lsa-maxage**] [**lsa-originate**]

no snmp-server enable traps ospf cisco-specific lsa [**lsa-maxage**] [**lsa-originate**]

Syntax Description

lsa-maxage	(Optional) Enables SNMP notifications only for opaque OSPF LSAs that have reached the maximum age.
lsa-originate	(Optional) Enables SNMP notifications only for opaque OSPF LSAs that are newly originated.

Command Default

SNMP notifications for OSPF opaque LSAs are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **snmp-server enable traps ospf cisco-specific lsa** command enables the traps that are defined by the CISCO-OSPF-TRAP-MIB for opaque LSAs. An opaque link-state advertisement (LSA) is used in MPLS traffic engineering to distribute attributes such as capacity and topology of links in a network. The scope of this LSA can be confined to the local network (Type 9, Link-Local), OSPF area (Type 20, Area-Local), or Autonomous System (Type 11, AS scope). The information in an opaque LSA can be used by an external application across the OSPF network. To enable the cospfMaxAgeLsa trap, enter the **snmp-server enable traps ospf cisco-specific lsa** command with the **lsa-maxage** keyword. To enable the cospfOriginateLsa trap, enter the **snmp-server enable traps ospf cisco-specific lsa** command with the **lsa-originate** keyword. When you enter the **snmp-server enable traps ospf cisco-specific lsa** command without either keyword, both traps will be enabled.

Examples

The following example enables the router to send OSPF opaque LSA notifications to the host at the address myhost.cisco.com using the community string defined as public whenever new opaque LSAs are created:

```
Router(config)# snmp-server enable traps ospf cisco-specific lsa lsa-originate
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.
snmp-server host	Specifies a recipient (target host) for SNMP notification operations.

snmp-server enable traps ospf cisco-specific retransmit

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) retransmission errors, use the **snmp-server enable traps ospf cisco-specific retransmit** command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

no snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

Syntax Description

packets	(Optional) Enables SNMP notifications only for packet retransmissions on nonvirtual interfaces.
shamlink	(Optional) Enables SNMP notifications only for sham-link retransmission notifications.
virt-packets	(Optional) Enables SNMP notifications only for packet retransmissions on virtual interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF retransmission errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink** keyword and related options were added.
12.3(14)T	Support was added for the **shamlink** keyword and related options.
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.

Examples

The following example enables the router to send OSPF sham-link retransmission notifications:

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf cisco-specific state-change** command in global configuration mode. To disable OSPF transition state change SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

no snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

Syntax Description

nssa-trans-change	(Optional) Enables only not-so-stubby area (NSSA) translator state changes trap for the OSPF area.
shamlink	(Optional) Enables only the sham-link transition state changes trap for the OSPF area.
interface	(Optional) Enables only the sham-link interface state changes trap for the OSPF area.
interface-old	(Optional) Enables only the replaced interface transition state changes trap for the OSPF area.
neighbor	(Optional) Enables only the sham-link neighbor transition state changes trap for the OSPF area.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF transition state changes are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink**, **interface-old**, and **neighbor** keywords were added.
12.3(14)T	Support was added for the **shamlink**, **interface-old**, and **neighbor** keywords.
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

You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.

Examples

The following example enables the router to send OSPF sham-link transition state change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.

snmp-server enable traps ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the **snmp-server enable traps ospf errors** command in global configuration mode. To disable SNMP notifications for OSPF errors, use the **no** form of this command.

snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

no snmp-server enable traps ospf errors [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

Syntax Description

authentication-failure	(Optional) Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
bad-packet	(Optional) Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
config-error	(Optional) Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.
virt-authentication-failure	(Optional) Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
virt-bad-packet	(Optional) Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
virt-config-error	(Optional) Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Command Default

SNMP notifications for OSPF errors are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S. Support was added for the OSPF MIB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

When you enter the **snmp-server enable traps ospf errors** command without any optional keywords, all OSPF error traps will be enabled. To enable only one or more OSPF error traps, enter one or more of the optional keywords.

Examples

The following example enables the router to send all OSPF error notifications:

```
Router(config)# snmp-server enable traps ospf errors
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf lsa

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the **snmp-server enable traps ospf lsa** command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the **no** form of this command.

snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

no snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

Syntax Description

lsa-maxage	(Optional) Enables only the ospfMaxAgeLsa trap. Allows SNMP notifications to be sent when an LSA in the OSPF link-state database of the router has reached the maximum age.
lsa-originate	(Optional) Enables only the ospfOriginateLsa trap. Enables SNMP notifications when a new LSA has been originated by the router as a result of a topology change.

Command Default

SNMP notifications for OSPF LSAs are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S. Support was added for the OSPF MIB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **snmp-server enable traps ospf lsa** command enables the traps for standard LSAs that are defined by the OSPF-MIB. To enable the ospfMaxAgeLsa trap, enter the **snmp-server enable traps ospf lsa** command with the **lsa-maxage** keyword. To enable the ospfOriginateLsa trap, enter the **snmp-server enable traps ospf lsa** command with the **lsa-originate** keyword. When the ospfOriginateLsa trap is enabled, it will not be invoked for simple LSA refreshes that take place every 30 minutes or when an LSA has reached its maximum age and is being flushed. When you enter the **snmp-server enable traps ospf lsa** command without either keyword, both traps will be enabled.

To enable the traps that are defined by the CISCO-OSPF-TRAP-MIB for opaque LSAs, enter the **snmp-server enable traps ospf cisco-specific lsa** command in global configuration mode.

Examples

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
Router(config)# snmp-server enable traps ospf lsa lsa-originate
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf rate-limit

To limit the number of Open Shortest Path First (OSPF) traps that are sent during a specified number of seconds, use the **snmp-server enable traps ospf rate-limit** command in global configuration mode. To disable the limit placed on the number of OSPF traps sent during a specified number of seconds, use the **no** form of this command.

snmp-server enable traps ospf rate-limit *seconds trap-number*

no snmp-server enable traps ospf rate-limit *seconds trap-number*

Syntax Description

seconds	Sets the rate limit window size, in seconds. A number from 2 to 60. The default value is 10.
trap-number	Sets the maximum number of traps sent during the window time. A number from 0 to 300. The default number is 7.

Command Default

No limit is placed on the number of OSPF traps sent.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

There is a possibility that a router sends trap bursts, which can drain network resources in a small interval of time. It is recommended that you enter the **snmp-server enable traps ospf rate-limit** command to configure a sliding window mechanism that will limit the number of traps that are sent within a specified number of seconds.

Examples

The following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent.

```
Router(config)# snmp-server enable traps ospf rate-limit 40 50
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf retransmit

To enable Simple Network Management Protocol (SNMP) notifications when packets are re-sent in an Open Shortest Path First (OSPF) network, use the **snmp-server enable traps ospf retransmit** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf retransmit [**packets**] [**virt-packets**]

no snmp-server enable traps ospf retransmit [**packets**] [**virt-packets**]

Syntax Description

packets	(Optional) Enables only the ospfTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a nonvirtual interface.
virt-packets	(Optional) Enables only the ospfVirtTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a virtual interface.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

To enable the ospfTXRetransmit trap so that SNMP notifications are sent only when packets from nonvirtual interfaces are re-sent, enter the **snmp-server enable traps ospf retransmit** command with the **packets** keyword. To enable the ospfTxRetransmit trap so that SNMP notifications are sent only when packets from virtual interfaces are re-sent, enter the **snmp-server enable traps ospf retransmit** command with the **virt-packets** keyword. When you enter the **snmp-server enable traps ospf retransmit** command without either keyword, both traps will be enabled.

Examples

The following example enables the router to send SNMP notifications when packets are re-sent by virtual interfaces:

```
Router(config)# snmp-server enable traps ospf retransmit virt-packets
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf state-change** command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the **no** form of this command.

snmp-server enable traps ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

no snmp-server enable traps ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

Syntax Description

if-state-change	(Optional) Enables only the ospfIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF interface.
neighbor-state-change	(Optional) Enables only the ospfNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF neighbor.
virtif-state-change	(Optional) Enables only the ospfVirtIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF interface.
virtneighbor-state-change	(Optional) Enables only the ospfVirtNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF neighbor.

Command Default

SNMP notifications for OSPF transition state changes are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

To enable all traps for transition state changes, enter the **snmp-server enable traps ospf state-change** command without of the optional keywords.

Examples

The following example enables the router to send SNMP notifications for transition state changes for virtual interfaces and virtual neighbors:

```
Router(config)# snmp-server enable traps ospf state-change virtif-state-change
virtneighbor-state-change
```

Related Commands

Command	Description
snmp-server enable traps ospf	Enables all SNMP notifications for OSPF.
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific lsa	Enables SNMP notifications for OSPF opaque LSAs.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF Cisco-specific retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF Cisco-specific transition state changes.
snmp-server enable traps ospf errors	Enables SNMP notifications for OSPF errors.
snmp-server enable traps ospf lsa	Enables SNMP notifications for OSPF LSAs.
snmp-server enable traps ospf rate-limit	Limits the number of OSPF traps that are sent during a specified number of seconds.
snmp-server enable traps ospf retransmit	Enables SNMP notifications for OSPF packet retransmissions.

summary-address (OSPF)

To create aggregate addresses for Open Shortest Path First (OSPF), use the **summary-address** command in router configuration mode. To restore the default, use the **no** form of this command.

summary-address {*ip-address mask* | *prefix mask*} [**not-advertise**] [**tag** *tag*] [**nssa-only**]

no summary-address {*ip-address mask* | *prefix mask*} [**not-advertise**] [**tag** *tag*] [**nssa-only**]

Syntax Description

ip-address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
prefix	IP route prefix for the destination.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair. This keyword applies to OSPF only.
tag *tag*	(Optional) Specifies the tag value that can be used as a "match" value for controlling redistribution via route maps. This keyword applies to OSPF only.
nssa-only	(Optional) Sets the nssa-only attribute for the summary route (if any) generated for the specified prefix, which limits the summary to not-so-stubby-area (NSSA) areas.

Defaults

This command behavior 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.
15.0(1)M	This command was modified. The **nssa-only** keyword was added.
12.2(33)SRE	This command was modified. The **nssa-only** keyword was added.

Usage Guidelines

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

OSPF does not support the **summary-address 0.0.0.0 0.0.0.0** command.

Examples

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from OSPF neighbors, use the **timers lsa arrival** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*

no timers lsa arrival

Syntax Description

milliseconds	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
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.

Usage Guidelines

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
show ip ospf timers rate-limit	Displays all of the LSAs in the rate limit queue.
timers throttle lsa all	Sets rate-limiting values for LSAs being generated.

timers pacing flood

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*

no timers pacing flood

Syntax Description

milliseconds	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 milliseconds to 100 milliseconds. The default value is 33 milliseconds.

Defaults

33 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring Open Shortest Path First (OSPF) flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF transmission queue. This command allows you to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced.

The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. Do not change the packet pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default flood timer values.

Examples

The following example configures LSA flood packet-pacing updates to occur in 55-millisecond intervals for Open Shortest Path First (OSPF) routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing flood 55
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing lsa-group

To change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Syntax Description

seconds	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

Defaults

The default interval for this command is 240 seconds. OSPF LSA group pacing is enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(4)T	The syntax of this command was changed from **timers lsa-group-pacing** to **timers pacing lsa-group**.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced. The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. Do not change the packet pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes the risks associated with changing the default timer values.

Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example configures OSPF group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing lsa-group 60
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission

To configure link-state advertisement (LSA) retransmission packet pacing, use the **timers pacing retransmission** command in router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

Syntax Description

milliseconds	The time (in milliseconds) at which LSAs in the retransmission queue are paced. The configurable range is from 5 milliseconds to 200 milliseconds. The default value is 66 milliseconds.

Defaults

66 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring Open Shortest Path First (OSPF) retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue. This command allows you to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced. The default settings for OSPF packet retransmission pacing timers are suitable for the majority of OSPF deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 55-millisecond intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing retransmission 55
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.

timers throttle lsa all

To set rate-limiting values for Open Shortest Path First (OSPF) link-state advertisement (LSA) generation, use the **timers throttle lsa all** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa all *start-interval hold-interval max-interval*

no timers throttle lsa all

Syntax Description

start-interval	Minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF topology change. The generation of the next LSA is not before the start interval. The range is 0 to 600,000 milliseconds. The default is 0 milliseconds, which means no delay; the LSA is sent immediately.
hold-interval	Incremental time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation. The range is 1 to 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Maximum wait time in milliseconds between generation of the same LSA. The range is 1 to 600,000 milliseconds. The default value is 5000 milliseconds.

Defaults

start-interval: 0 milliseconds
hold-interval: 5000 milliseconds
max-interval: 5000 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
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.

Usage Guidelines

The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the *hold-interval* value of the **timers throttle lsa all** command.

Examples

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
show ip ospf	Displays information about OSPF routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle spf

To turn on OSPF shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SFP calculation after a change, in milliseconds. Range is from 1 to 600000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is 1 to 600000.

Command Default

SPF throttling is not set.

Command Modes

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

Command History

Release	Modification
12.2(14)S	This command was introduced. This command replaces the **timers spf-interval** command.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
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 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

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Release 12.2(33)SRB

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

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

ttl-security all-interfaces

To enable Time-to-Live (TT)L security check on all OSPF interfaces, use the **ttl-security all-interfaces** command in interface configuration mode. To disable TTL security check, use the **no** form of this command.

ttl-security all-interfaces [hops *hop-count*]

no ttl-security all-interfaces

Syntax Description

hops *hop-count*	(Optional) Configures the maximum number of IP hops allowed. The *hop-count* argument range is from 1 to 254.

Command Default

TTL security check is disabled on OSPF interfaces.

Command Modes

Interface configuration (config-if)

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.

Usage Guidelines

Use the **ttl-security all-interfaces** command to enable TTL security check on all OSPF interfaces.

This command applies only to normal OSPF interfaces. It does not apply to virtual or sham links that require TTL security protection. Virtual and sham links must be configured independently.

As a convenience, this command can be used to globally enable TTL security check on all OSPF interfaces. Then the **ip ospf ttl-security disable** command in interface configuration mode can be used to disable TTL security on an interface-by-interface basis.

Examples

The following example shows how to enable TTL security check on all OSPF interfaces:

```
Router(config)# router ospf 1
Router(config-router)# ttl-security all-interfaces
```

Related Commands

Command	Description
ip ospf ttl-security	Configures TTL security check on a specific interface.