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 minimum 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.