Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

First Published: January 14, 2008
Last Updated: October 2, 2009

This module describes configuration tasks to configure various options involving Open Shortest Path First (OSPF). This module contains tasks that use commands to configure a lightweight security mechanism to protect OSPF sessions from CPU utilization-based attacks and configure a router to shut down a protocol temporarily without losing the protocol configuration.

Finding Feature Information in This Module

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown" section on page 9.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

To configure the OSPF features in this module, you should understand the following concepts:

- TTL Security Check for OSPF, page 2
- OSPF Graceful Shutdown, page 3

TTL Security Check for OSPF

When the TTL Security Check feature is enabled, OSPF sends outgoing packets with an IP header Time-to-Live (TTL) value of 255 and discards incoming packets that have TTL values less than a configurable threshold. Because each router that forwards an IP packet decrements the TTL, packets received via a direct (one hop) connection will have a value of 255. Packets that cross two hops will have a value of 254, and so on. The receive threshold is configured in terms of the maximum number of hops a packet may have traveled. The value for this hop-count argument is a number from 1 to 254, with a default of 1.

The TTL Security Check feature may be configured under the OSPF router submode, in which case it applies to all the interfaces on which OSPF runs, or it may be configured on a per-interface basis.

Use of TTL Security Check in Existing Networks

If you have OSPF running in your network and want to implement TTL security on an interface-by-interface basis without any network interruptions, use the **ip ospf ttl-security** command and set the *hop-count* argument to 254. This setting causes outgoing packets to be sent with a TTL value of 255, but allows any value for input packets. Later, once the router at the other end of the link has had TTL security enabled, you can start enforcing the hop limit for incoming packets by using the same **ip ospf ttl-security** command with no hop count specified. This process ensures that OSPF packets will not be dropped because of a temporary mismatch in TTL security.

TTL Security Check for OSPF Virtual and Sham Links

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a *virtual link*. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other Area Border Router [ABR]) and the nonbackbone area that the two routers have in common (called the *transit area*). Note that virtual links cannot be configured through stub areas. *Sham links* are similar to virtual links in many ways, but sham links are used in Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) networks to connect provider edge (PE) routers across the MPLS backbone.

To establish a virtual link or a sham link, use the **area virtual-link** or **area sham-link cost** command, respectively, in router configuration mode. To configure the TTL Security Check feature on a virtual link or a sham link, configure the **ttl-security** keyword and the *hop-count* argument in either command. Note that the *hop-count* argument value is mandatory in this case.

Benefits of the OSPF Support for TTL Security Check

The OSPF Support for TTL Security Check feature protects OSPF neighbor sessions from CPU utilization-based attacks and reduces the effectiveness of Denial of Service (DoS) attacks against an OSPF autonomous system. When this feature is enabled, a host cannot attack an OSPF session if the host is not a member of the local or remote OSPF network or if the host is not directly connected to a network segment between the local and remote OSPF networks.

OSPF Graceful Shutdown

The OSPF Graceful Shutdown feature provides the ability to temporarily shut down the OSPF protocol in the least disruptive manner and notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path. A graceful shutdown of the OSPF protocol can be initiated using the **shutdown** command in router configuration mode.

This feature also provides the ability to shut down OSPF on a specific interface. In this case, OSPF will not advertise the interface or form adjacencies over it; however, all of the OSPF interface configuration will be retained. To initiate a graceful shutdown of an interface, use the **ip ospf shutdown** command in interface configuration mode.

How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown

This section contains the following tasks:

- Configuring TTL Security Check on All OSPF Interfaces, page 3
- Configuring TTL Security Check on a per-Interface Basis, page 4
- Configuring OSPF Graceful Shutdown on a per-Interface Basis, page 6

Configuring TTL Security Check on All OSPF Interfaces

Perform this task to configure TTL security check on all OSPF interfaces. This ensures that OSPF neighbor sessions are protected from CPU utilization-based attacks and reduces the effectiveness of Denial of Service (DoS) attacks against an OSPF autonomous system.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **ttl-security all-interfaces** [**hops** *hop-count*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 109`	Enables OSPF routing, which places the device in router configuration mode.
Step 4	**ttl security all-interfaces** [**hops** *hop-count*] **Example:** `Router(config-router)# ttl security all-interfaces`	Configures TTL security check on all OSPF interfaces. **Note** This configuration step applies only to normal OSPF interfaces. This step does not apply to virtual links or sham links that require TTL security protection. Virtual links and sham links must be configured independently.

Step 5	**end**
	Example:
	`Router(config-router)# end`
		Returns to privileged EXEC mode.

Configuring TTL Security Check on a per-Interface Basis

Perform this task to configure TTL security check on an individual interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf ttl-security** [**hops** *hop-count* | **disable**]
5. **end**
6. **show ip ospf** [*process-id*] **interface** [*interface-type interface-number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}]
7. **show ip ospf neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]
8. **show ip ospf** [*process-id*] **traffic** [*interface-type interface-number*]
9. **debug ip ospf adj**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf ttl-security** [**hops** *hop-count* | **disable**] **Example:** `Router(config-if)# ip ospf ttl-security disable`	Configures the TTL Security Check feature on a specific interface. • The *hop-count* argument range is from 1 to 254. • The **disable** keyword can be used to disable TTL security on an interface. It is useful only if TTL security was initially enabled on all OSPF interfaces, in which case the **disable** keyword can be used as an override or to turn off TTL security on a specific interface. • In the example, TTL security is being disabled on Ethernet interface 0/0.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 6	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}] **Example:** `Router# show ip ospf interface ethernet 0`	(Optional) Displays OSPF-related interface information. • In Cisco IOS Release 12.2(33)SRC, the output now includes configured TTL limits.
Step 7	**show ip ospf neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**] **Example:** `Router# show ip ospf neighbor 10.199.199.137`	(Optional) Displays OSPF neighbor information on a per-interface basis. • If one side of the connection has TTL security enabled, the other side shows the neighbor in the INIT state.

	Command or Action	Purpose
Step 8	**show ip ospf** [*process-id*] **traffic** [*interface-type interface-number*] **Example:** `Router# show ip ospf traffic`	(Optional) Displays OSPF traffic statistics. • The number of times a TTL security check failed is included in the output.
Step 9	**debug ip ospf adj** **Example:** `Router# debug ip ospf adj`	(Optional) Initiates debugging of OSPF adjacency events. • Information about dropped packets, including interface type and number, neighbor IP address, and TTL value, is included in the command output.

Configuring OSPF Graceful Shutdown on a per-Interface Basis

Perform this task to configure a graceful shutdown on a individual OSPF interface.

When the **ip ospf shutdown** interface command is entered, the interface on which it is configured sends a link-state update advising its neighbors that is going down, which allows those neighbors to begin routing OSPF traffic around this router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf shutdown**
5. **end**
6. **show ip ospf** [*process-id*] **interface** [*type number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}]
7. **show ip ospf** [*process-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and number and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip ospf shutdown** **Example:** Router(config-if)# ip ospf shutdown	Initiates an OSPF protocol graceful shutdown at the interface level.
Step 5	**end** **Example:** Router(config-if)# **end**	Returns to privileged EXEC mode.
Step 6	**show ip ospf** [*process-id*] **interface** [*type number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}] **Example:** Router# show ip ospf interface ethernet 0/1	(Optional) Displays OSPF-related interface information. • In Cisco IOS Release 12.2(33)SRC, the output was enhanced to show that the protocol instance on this specific interface is shut down.
Step 7	**show ip ospf** [*process-id*] **Example:** Router# **s**how ip ospf	(Optional) Displays general information about OSPF routing processes. • In Cisco IOS Release 12.2(33)SRC, the output was enhanced to show that the protocol instance on this specific interface is shut down.

Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

This section provides the following configuration example:

- Use of TTL Security Check in Existing Networks: Example, page 7

Use of TTL Security Check in Existing Networks: Example

The following example shows how to enable TTL security in an existing OSPF network on a per-interface basis.

Configuring TTL security in an existing network is a three-step process:

1. Configure TTL security with a hop count of 254 on the OSPF interface on the *sending* side router.
2. Configure TTL security with no hop count on the OSPF interface on the *receiving* side router.
3. Reconfigure the *sending* side OSPF interface with no hop count.

```
configure terminal
  ! Configure the following command on the sending side router.
  interface ethernet 0/1
  ip ospf ttl-security hops 254
  ! Configure the next command on the receiving side router.
  interface ethernet 0/1
  ip ospf ttl-security
  ! Reconfigure the sending side with no hop count.
  ip ospf ttl-security
  end
```

Additional References

The following sections provide references related to the OSPF TTL Security Check and OSPF Graceful Shutdown features.

Related Documents

Related Topic	Document Title
IP routing commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*

MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(33)SRC, 12.2(33)SB, 15.0(1)M, or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

Feature Name	Releases	Feature Information
OSPF Graceful Shutdown	12.2(33)SRC 12.2(33)SB 15.0(1)M	This feature provides the ability to temporarily shut down a protocol in the least disruptive manner and notify its neighbors that it is going away. A graceful shutdown of a protocol can be initiated on all OSPF interfaces or on a specific interface. The following sections provide information about this feature: • OSPF Graceful Shutdown, page 3 • Configuring OSPF Graceful Shutdown on a per-Interface Basis, page 6 The following commands were introduced or modified: **ip ospf shutdown**, **show ip ospf interface**, and **show ip ospf**, **shutdown** (router OSPF). In Cisco IOS Release 12.2(33)SB, support was added for the Cisco 10000 series routers.
OSPF TTL Security Check	12.2(33)SRC 15.0(1)M	This feature increases protection against OSPF DoS attacks, enables checking of TTL values on OSPF packets from neighbors, and allows users to set TTL values sent to neighbors. The following sections provide information about this feature: • TTL Security Check for OSPF, page 2 • Configuring TTL Security Check on All OSPF Interfaces, page 3 • Configuring TTL Security Check on a per-Interface Basis, page 4 The following commands were introduced or modified: **area sham-link cost**, **area virtual-link**, **debug ip ospf adj**, **ip ospf ttl-security**, **show ip ospf interface**, **show ip ospf neighbor**, **show ip ospf traffic**, and **ttl-security all-interfaces**,.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.