

# Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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 to configure a router to shut down a protocol temporarily without losing the protocol configuration.

- Information About OSPF TTL Security Check and OSPF Graceful Shutdown, on page 1
- How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown, on page 3
- Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown, on page 7
- Additional References, on page 7
- Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown, on page
   8

# Information About OSPF TTL Security Check and OSPF Graceful Shutdown

## **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. Since each device 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 that 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.

## **Transitioning Existing Networks to Use TTL Security Check**

If you currently 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 device at the other end of the link has had TTL security enabled you can start enforcing the hop limit for the 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 devices. The configuration information in each device consists of the other virtual endpoint (the other area border router [ABR]) and the nonbackbone area that the two devices 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** commands, 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 provides an effective and easy-to-deploy solution to protect OSPF neighbor sessions from CPU utilization-based attacks. 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. This solution greatly reduces the effectiveness of Denial of Service (DoS) attacks against an OSPF autonomous system.

## **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

## **Configuring TTL Security Check on All OSPF Interfaces**

#### **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	Enables privileged EXEC mode.
	Example:	• Enter your password if prompted.
	Device> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example:	
	Device# configure terminal	
Step 3	router ospf process-id	Enables OSPF routing, which places the device in router
	Example:	configuration mode.
	Device(config)# router ospf 109	
Step 4	ttl-security all-interfaces [ hops hop-count ]	Configures TTL security check on all OSPF interfaces.
	<pre>Example: Device(config-router)# ttl-security all-interfaces</pre>	<b>Note</b> 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	Returns to privileged EXEC mode.
	Example:	
	Device(config-router)# end	

## **Configuring TTL Security Check on a Per-Interface Basis**

#### **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	Enables privileged EXEC mode.
	Example:	• Enter your password if prompted.
	Device> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example:	
	Device# configure terminal	
Step 3	interface type number	Configures an interface type and enters interface
	Example:	configuration mode.
	<pre>Device(config)# interface GigabitEthernet 0/0/0</pre>	
Step 4	ip ospf ttl-security [hops hop-count   disable]	Configures TTL security check feature on a specific
	Example:	interface.
	Device (config-if) # in ospf ttl-security	• The <i>hop-count</i> argument range is from 1 to 254.
	Device (config fi) " ip obpi cor becaricy	• The <b>disable</b> keyword can be used to disable TTL security on an interface. It is useful only if the <b>ttl-security all-interfaces</b> comand initially enabled TTL security on all OSPF interfaces, in which case <b>disable</b> 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 GigabitEthernet interface 0/0/0.

	Command or Action	Purpose
Step 5	end	Returns to privileged EXEC mode.
	Example:	
	Device(config-if)# end	
Step 6	<pre>show ip ospf [process-id] interface [interface type interface-number] [brief] [multicast] [topology topology-name   base}]</pre>	(Optional) Displays OSPF-related interface information.
	Example:	
	Device# show ip ospf interface gigabitethernet 0/0/0	
Step 7	<b>show ip ospf neighbor</b> <i>interface-type interface-number</i> [ <i>neighbor-id</i> ][ <b>detail</b> ]	(Optional) Displays OSPF neighbor information on a per-interface basis.
	Example:	• If one side of the connection has TTL security enabled, the other side shows the neighbor in the INIT state.
	Device# show ip ospf neighbor 10.199.199.137	
Step 8	show ip ospf [process-id] traffic [interface-type	(Optional) Displays OSPF traffic statistics.
	interface-number]	• The number of times a TTL security check failed is
	Example:	included in the output.
	Device# show ip ospf traffic	
Step 9	debug ip ospf adj	(Optional) Initiates debugging of OSPF adjacency events.
	Example:	• Information about dropped packets, including interface type and number, neighbor IP address, and TTL value,
	Device# debug ip ospf adj	is included in the command output.

## **Configuring OSPF Graceful Shutdown on a Per-Interface Basis**

### **SUMMARY STEPS**

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

#### **DETAILED STEPS**

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example:	• Enter your password if prompted.
	Device> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example:	
	Device# configure terminal	
Step 3	interface type number	Configures an interface type and number and enters interface
	Example:	configuration mode.
	Device(config)# interface GigabitEthernet 0/1/0	
Step 4	ip ospf shutdown	Initiates an OSPF protocol graceful shutdown at the
	Example:	interface level.
	Device(config-if)# <b>ip ospf shutdown</b>	• When the <b>ip ospf shutdown</b> 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.
Step 5	end	Returns to privileged EXEC mode.
	Example:	
	Device(config-if)# <b>end</b>	
Step 6	<pre>show ip ospf [ process-id ] interface [ interface type interface-number ] [ brief ] [multicast] [topology topology-name / base}]</pre>	(Optional) Displays OSPF-related interface information.
	Example:	
	Device# show ip ospf interface GigabitEthernet 0/1/0	
Step 7	show ip ospf [ process-id ]	(Optional) Displays general information about OSPF routing
	Example:	processes.
	Device# <b>show ip ospf</b>	

## Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

## **Example: Transitioning an Existing Network to Use TTL Security Check**

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 device.
- 2. Configure TTL security with no hop count on the OSPF interface on the receiving side device.
- 3. Reconfigure the sending side OSPF interface with no hop count.

```
configure terminal
! Configure the following command on the sending side router.
interface gigabitethernet 0/1/0
ip ospf ttl-security hops 254
! Configure the next command on the receiving side router.
interface gigabitethernet 0/1/0
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 Topic	Document Title
Configuring OSPF	"Configuring OSPF"
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

#### **Related Documents**

#### **Standards**

Standard	Title	
No new or modified standards are supported and support for existing standards has not been modified.		]

#### **MIBs**

МІВ	MIBs Link
No new or modified MIBs are supported and support for existing MIBs has not been modified.	http://www.cisco.com/go/mibs

#### **RFCs**

RFC	Title	
No new or modified RFCs are supported and support for existing RFCs has not been modified.		

#### **Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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