CHAPTER 46

Configuring OSPF TTL Security Check

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

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 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 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 interfaceby- interface basis without any network interruptions, use the **ip ospf ttl-security** command and set the hopcount 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 the incoming packets by using the same **ip ospf ttl-security** command with no hop count specified. This process ensure 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** 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.

How to Configure OSPF TTL Security Check

Configuring TTL Security Check on All OSPF Interfaces

Follow these steps to configure TTL security check on all OSPF interfaces

	Command	Purpose
Step 1	**enable**	Enables priveleged EXEC mode
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**router ospf** *process-id*	Enables OSPF routing, which places the device in router configuration mode.

	Command	Purpose
Step 4	**ttl security all-interfaces** [**hops** *hop-count*]	Configures TTL security check on all OSPF interfaces. **Note** This configuration step applies only to normal OSPF interaces. 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 priveleged EXEC mode.

Configuring TTL Security Check on a Per-Interface Basis

Follow these steps to configure TTL security check on a per-interface basis.

	Command	Purpose
Step 1	**enable**	Enables priveleged EXEC mode
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**interface** *type number*	Enters configuration mode. **Note** The card number is always 0.
Step 4	**ip ospf ttl-security** [**hops** *hop-count* | **disable**]	Configures 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 the **ttl-security all-interfaces** comand initially enabled TTL security on all OSPF interfaces, in which case **disable** can be used as an override or to turn off TTL security on a specific interface.
Step 5	**end**	Returns to priveleged EXEC mode.
Step 6	**show ip ospf** [*process-id*] **interface** [*interface type interface-number*] [**brief**] [**multicast**] [**topology** *topology-name* | **base**}]	(Optional) Displays OSPF-related interface information.
Step 7	**show ip ospf neighbor** *interface-type interface number* [*neighbor-id*][**detail**]	(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.
Step 8	**show ip ospf** [*process-id*] **traffic** [*interface-type interface-number*]	(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**	(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.

Configuration Examples for OSPF TTL Security Check

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-interfacebasis.

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

Step 1 Configure TTL security with a hop count of 254 on the OSPF interface on the sending side router.

Step 2 Configure TTL security with no hop count on the OSPF interface on the receiving side router.

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