



# CHAPTER 40

## Monitoring Routing

---

You can monitor the following routing information on the security appliance:

- [OSPF LSAs](#)
- [OSPF Neighbors](#)
- [Routes](#)

### OSPF LSAs

You can view the LSAs stored in the security appliance OSPF database. There are 4 types of LSAs stored in the database, each with its own particular format. The following briefly describes the LSA types:

- Router LSAs (Type 1 LSAs) describe the routers attached to a network.
- Network LSAs (Type 2 LSAs) describe the networks attached to an OSPF router.
- Summary LSAs (Type 3 and Type 4 LSAs) condense routing information at area borders.
- External LSAs (Type 5 and Type 7 LSAs) describe routes to external networks.

To learn more about the information displayed for each LSAs type, see the following:

- [Type 1](#)
- [Type 2](#)
- [Type 3](#)
- [Type 4](#)
- [Type 5](#)
- [Type 7](#)

### Type 1

Type 1 LSAs are router link advertisements that are passed within an area by all OSPF routers. They describe the router links to the network. Type 1 LSAs are only flooded within a particular area.

The Type 1 pane displays all Type 1 LSAs received by the security appliance. Each row in the table represents a single LSA.

#### Fields

- Process—*Display only*. Displays the OSPF process for the LSA.

- **Area**—*Display only*. Displays the OSPF area for the LSA.
- **Router ID**—*Display only*. Displays the OSPF router ID of the router originating the LSA.
- **Advertiser**—*Display only*. Displays the ID of the router originating the LSA. For router LSAs, this is identical to the Router ID.
- **Age**—*Display only*. Displays the age of the link state.
- **Sequence #**—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- **Checksum**—*Display only*. Displays the checksum of the contents of the LSA.
- **Link Count**—*Display only*. Displays the number of interfaces detected for the router.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Type 2

Type 2 LSAs are network link advertisements that are flooded within an area by the Designated Router. They describe the routers attached to specific networks.

The Type 2 pane displays the IP address of the Designated Router that advertises the routes.

### Fields

- **Process**—*Display only*. Displays the OSPF process for the LSA.
- **Area**—*Display only*. Displays the OSPF area for the LSA.
- **Designated Router**—*Display only*. Displays the IP address of the Designated Router interface that sent the LSA.
- **Advertiser**—*Display only*. Displays the OSPF router ID of the Designated Router that sent the LSA.
- **Age**—*Display only*. Displays the age of the link state.
- **Sequence #**—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- **Checksum**—*Display only*. Displays the checksum of the contents of the LSA.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Type 3

Type 3 LSA are summary link advertisements that are passed between areas. They describe the networks within an area.

### Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Destination—*Display only*. Displays the address of the destination network being advertised.
- Advertiser—*Display only*. Displays the ID of the ABR that sent the LSA.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Type 4

Type 4 LSAs are summary link advertisements that are passed between areas. They describe the path to the ASBR. Type 4 LSAs do not get flooded into stub areas.

### Fields

- Process—*Display only*. Displays the OSPF process for the LSA.
- Area—*Display only*. Displays the OSPF area for the LSA.
- Router ID—*Display only*. Displays the router ID of the ASBR.
- Advertiser—*Display only*. Displays the ID of the ABR that sent the LSA.
- Age—*Display only*. Displays the age of the link state.

- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Type 5

Type 5 LSAs are passed between and flooded into areas by ASBRs. They describe routes external to the AS. Stub areas and NSSAs do not receive these LSAs.

**Fields**

- Process—*Display only*. Displays the OSPF process for the LSA.
- Network—*Display only*. Displays the address of the AS external network.
- Advertiser—*Display only*. Displays the router ID of the ASBR.
- Age—*Display only*. Displays the age of the link state.
- Sequence #—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- Checksum—*Display only*. Displays the checksum of the contents of the LSA.
- Tag—*Display only*. Displays the external route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Type 7

Type 7 LSAs are NSSA AS-external routes that are flooded by the ASBR. They are similar to Type 5 LSAs, but unlike Type 5 LSAs, which are flooded into multiple areas, Type 7 LSAs are only flooded into NSSAs. Type 7 LSAs are converted to Type 5 LSAs by ABRs before being flooded into the area backbone.

**Fields**

- **Process**—*Display only*. Displays the OSPF process for the LSA.
- **Area**—*Display only*. Displays the OSPF area for the LSA.
- **Network**—*Display only*. Displays the address of the external network.
- **Advertiser**—*Display only*. Displays the router ID of the ASBR that sent the LSA.
- **Age**—*Display only*. Displays the age of the link state.
- **Sequence #**—*Display only*. Displays the link state sequence number. The link state sequence number is used to detect old or duplicate LSAs.
- **Checksum**—*Display only*. Displays the checksum of the contents of the LSA.
- **Tag**—*Display only*. Displays the external route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## OSPF Neighbors

The OSPF Neighbor pane displays the OSPF neighbors dynamically discovered and statically configured OSPF neighbors on the security appliance.

**Fields**

- **Neighbor**—*Display only*. Displays the neighbor router ID.
- **Priority**—*Display only*. Displays the router priority.
- **State**—*Display only*. Displays the OSPF state for the neighbor:
  - **Down**—This is the first OSPF neighbor state. It means that no hello packets have been received from this neighbor, but hello packets can still be sent to the neighbor in this state.  
During the fully adjacent neighbor state, if the security appliance does not receive hello packet from a neighbor within the dead interval time, or if the manually configured neighbor is being removed from the configuration, then the neighbor state changes from Full to Down.
  - **Attempt**—This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the security appliance sends unicast hello packets every poll interval to the neighbor from which hellos have not been received within the dead interval.
  - **Init**—This state specifies that the security appliance has received a hello packet from its neighbor, but the ID of the receiving router was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the router ID of the sender in its hello packet as an acknowledgment that it received a valid hello packet.

- 2-Way—This state designates that bi-directional communication has been established between the security appliance and the neighbor. Bi-directional means that each device has seen the hello packet from the other device. This state is attained when the router receiving the hello packet sees its own Router ID within the neighbor field of the received hello packet. At this state, the security appliance decides whether to become adjacent with this neighbor. On broadcast media and non-broadcast multiaccess networks, a the security appliance becomes full only with the designated router and the backup designated router; it stays in the 2-way state with all other neighbors. On point-to-point and point-to-multipoint networks, the security appliance becomes full with all connected neighbors.

At the end of this stage, the DR and BDR for broadcast and non-broadcast multiaccess networks are elected.

**Note**

Receiving a Database Descriptor packet from a neighbor in the Init state will also cause a transition to 2-way state.

- Exstart—Once the DR and BDR are elected, the actual process of exchanging link state information begins between the security appliance and the DR and BDR.

In this state, the security appliance and the DR and BDR establish a master-slave relationship and choose the initial sequence number for adjacency formation. The device with the higher router ID becomes the master and starts the exchange and is therefore the only device that can increment the sequence number.

**Note**

DR/BDR election occurs by virtue of a higher priority configured on the device instead of highest router ID. Therefore, it is possible that a DR plays the role of slave in this state. Master/slave election is on a per-neighbor basis. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR.

- Exchange—In the exchange state, OSPF neighbors exchange DBD packets. Database descriptors contain LSA headers only and describe the contents of the entire link state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link state request packets and link state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link state database to check if new or more current link state information is available with the neighbor.
- Loading—In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link state request packets. The neighbor then provides the requested link state information in link state update packets. During the adjacency, if a the security appliance receives an outdated or missing LSA, it requests that LSA by sending a link state request packet. All link state update packets are acknowledged.
- Full—In this state, the neighbors are fully adjacent with each other. All the router and network LSAs are exchanged and the router databases are fully synchronized.
 

Full is the normal state for an OSPF router. The only exception to this is the 2-way state, which is normal in a broadcast network. Routers achieve the full state with their DR and BDR only. Neighbors always see each other as 2-way.

  - Dead Time—*Display only*. Displays the amount of time remaining that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.
  - Address—*Display only*. Displays the IP address of the interface to which this neighbor is directly connected.

- Interface—*Display only*. Displays the interface on which the OSPF neighbor has formed adjacency.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

## Routes

The Routes pane displays the statically configured, connected, and discovered routes in the security appliance routing table.

### Fields

- Protocol—*Display only*. Displays the origin of the route information.
  - RIP—The route was derived using RIP.
  - OSPF—The route was derived using OSPF.
  - CONNECTED—The route is a network directly connected to the interface.
  - STATIC—The route is statically defined.
- Type—*Display only*. Displays the type of route. It can be one of the following values:
  - - (dash)—Indicates that the type column does not apply to the specified route.
  - IA—The route is an OSPF interarea route.
  - E1—The route is an OSPF external type 1 route.
  - E2—The route is an OSPF external type 2 route.
  - N1—The route is an OSPF not so stubby area (NSSA) external type 1 route.
  - N2—The route is an OSPF NSSA external type 2 route.
- Destination—*Display only*. Displays the IP address/netmask of the destination network.
- Gateway—*Display only*. Displays the IP address of the next router to the remote network.
- Interface—*Display only*. Displays the interface through which the specified network can be reached.
- [AD/Metric]—*Display only*. Displays the administrative distance/metric for the route.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

