Open Shortest Path First (OSPF)

JNCIA EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- Define the functions of OSPF packet types
- Define the functions of OSPF area types
- Define the functions of OSPF router types
- Identify the steps required to form an OSPF adjacency
- Identify the election criteria for an OSPF DR
- Describe the functions of the DR and BDR
- Identify CLI commands used to monitor and troubleshoot an OSPF network
In this chapter, we examine the Open Shortest Path First (OSPF) routing protocol. You’ll get a high-level view of the protocol design, but we also discuss basic configuration and troubleshooting commands used in a Juniper Networks environment.

We start by taking a look at how a link-state routing protocol provides interconnectivity within a network, exploring the underlying principles that govern how OSPF determines the best path to a destination. We follow this with a detailed discussion of the OSPF packet types and how two OSPF neighbors form an adjacency. We examine the evolution of an OSPF network and look at several methods that allow you to scale your OSPF deployment. This includes a review of OSPF link-state advertisements (LSAs), types of OSPF areas, and the various router designations within an OSPF network.

Throughout the chapter, we look at useful JUNOS software commands used to implement an OSPF network. Finally, we review some helpful troubleshooting and verification commands you can use.

Basic OSPF Operation

Before delving into the specific details of OSPF, let’s look at the theory behind its operation as well as the overall goals of the protocol. First, we discuss how a router utilizes a link-state routing protocol, and then we examine the exchange of link-state databases. We also discuss how the router uses the database to find a path to each destination.

Link-State Protocol Review

Once a link-state router begins operating on a network link, information associated with that logical network is added to its local link-state database. The local router then sends Hello messages on its operational links to determine whether other link-state routers are operating on the interfaces as well. When a remote router is located, the local router attempts to form an adjacency. This adjacency enables the two routers to advertise summary link-state database information to each other. This exchange is not the actual detailed database information, but is truly a summary of the data. Each router evaluates the summary data against its local link-state database to verify that it has the most up-to-date information. Should one side of the adjacency realize that it requires an update, that router requests the new information from the adjacent router. The update includes the actual data contained in the link-state database. This exchange process continues until both routers have identical link-state databases.
This common view of the link-state database forms the basis of the network topology. Each router uses the Dijkstra Algorithm to process the database information into a path to each destination in the network. Every link-state router uses the same algorithm to process its database, requiring each router to maintain consistent information to get the same results. This concept of a consistent database is a core requirement for link-state protocols and allows the protocols to ensure a loop-free topology. Since no loops exist, each router then makes consistent forwarding decisions for user data packets. Ensuring the proper advertisement of link-state updates and propagating these updates correctly are the only barriers to preventing loops.

**OSPF Defined**

The IETF has written numerous documents to define the behavior of routing protocols. This ensures that vendor implementations are consistent and interoperable. OSPF is no exception to this rule. The OSPF working group was formed in 1987 and has released numerous Requests for Comment (RFC), including RFC 1247, “OSPF Version 2,” which describes the routing behavior of OSPFv2, the basic foundation of the protocol. The most up-to-date RFC is published as RFC 2328, “OSPF Version 2,” and contains all the latest updates and modifications to the protocol. It is backward-compatible with each of the previous documents that specify OSPFv2.

Some of the more interesting RFCs include:

- RFC 1131, “OSPF Specification,” describes the first iteration of OSPF and was used in initial tests to determine whether the protocol worked. This RFC led to the creation of two working code bases that were used in test beds.
- RFC 1247, “OSPF Version 2,” addresses a number of issues discovered during the initial rollout of OSPFv1 and modified the protocol to allow for future modifications without generating backward-compatibility issues. OSPFv2 is not compatible with OSPFv1.
- RFC 1584, “Multicast Extensions to OSPF,” provides extensions to OSPF for the support of multicast IP traffic.
- RFC 1587, “The OSPF NSSA Option,” describes the operations of a not-so-stubby area.
- RFC 2328, “OSPF Version 2,” details the latest update to OSPFv2.

For a complete list of all RFCs pertaining to OSPF, please refer to the IETF website at [www.ietf.org](http://www.ietf.org).
Packet Types

We now examine the basic components that allow OSPF to communicate and distribute the information needed to determine routes to all end destinations. After discussing the packet header, we offer a detailed look at the structure of the five packet types used in OSPF.

Common Packet Header

All OSPF packets share a common 24-octet header. This header allows the receiving router to determine whether the packet is valid and should be processed.

Figure 6.1 shows the OSPF header fields, which include the following:

Version (1 octet)  This field details the current version of OSPF used by the local router. It is set to a value of 2, the default value.

Type (1 octet)  This field specifies the type of OSPF packet. Possible values include:
- 1—Hello packet
- 2—Database descriptor
- 3—Link-state request
- 4—Link-state update
- 5—Link-state acknowledgment

Packet Length (2 octets)  This field displays the total length, in octets, of the OSPF packet.

Router ID (4 octets)  The router ID of the advertising router appears in this field.

Area ID (4 octets)  This field contains the 32-bit area ID assigned to the interface used to send the OSPF packet.

Checksum (2 octets)  This field displays a standard IP checksum for the entire OSPF packet, excluding the 64-bit authentication field.

Authentication Type (2 octets)  The specific type of authentication used by OSPF is encoded in this field. Possible values are:
- 0—Null authentication
- 1—Simple password
- 2—MD5 cryptographic authentication

Authentication (8 octets)  This field displays the authentication data to verify the packet’s integrity.

Hello Packet

To establish and maintain a neighbor relationship, an OSPF-speaking router determines whether any directly connected routers also speak OSPF. The router sends an OSPF hello packet out all configured interfaces and awaits a response. The hello packet, type code 1, is addressed to the AllSPFRouters multicast address of 224.0.0.5 for broadcast and point-to-point
connections. Other connection types unicast the hello packet to their neighbor. Figure 6.2 details the format of the hello packet.

**FIGURE 6.1** The OSPF common header

![The OSPF common header diagram]

**FIGURE 6.2** The OSPF hello packet

![The OSPF hello packet diagram]

The packet includes the following fields:

**Network Mask (4 octets)** This field contains the subnet mask of the advertising OSPF interface. Unnumbered point-to-point interfaces and virtual links set this value to 0.0.0.0.

**Hello Interval (2 octets)** This field displays the value of the hello interval requested by the advertising router. Possible values range from 1 to 255, with a default value of 10 seconds.

**Options (1 octet)** The local router advertises its capabilities in this field. Each bit in the Options field represents a different function. The various bit definitions are:

- **Bit 7** The DN bit is used for loop prevention in a Virtual Private Network (VPN) environment. An OSPF router receiving an update with the bit set does not forward that update.
Bit 6  The O bit indicates that the local router supports opaque LSAs.
Bit 5  The DC bit indicates that the local router supports Demand Circuits. The JUNOS software does not use this feature.
Bit 4  The EA bit indicates that the local router supports the External Attributes LSA for carrying BGP information in an OSPF network. The JUNOS software does not use this feature.
Bit 3  The N/P bit describes the handling and support of not-so-stubby LSAs.
Bit 2  The MC bit indicates that the local router supports multicast OSPF LSAs. The JUNOS software does not use this feature.
Bit 1  The E bit describes the handling and support of external LSAs.
Bit 0  The T bit indicates that the local router supports TOS routing functionality. The JUNOS software does not use this feature.

Router Priority (1 octet)  This field contains the priority of the local router. The value is used in the election of the designated router and backup designated router. Possible values range from 0 to 255, with a default value of 128.

Router Dead Interval (4 octets)  This field shows the value of the dead interval requested by the advertising router. Possible values range from 1 to 65,535. The JUNOS software uses a default value of 40 seconds.

Designated Router (4 octets)  The interface address of the current designated router is displayed in this field. A value of 0.0.0.0 is used when no designated router has been elected.

Backup Designated Router (4 octets)  The interface address of the current backup designated router is displayed in this field. A value of 0.0.0.0 is used when no backup designated router has been elected.

Neighbor (Variable)  This field displays the router ID of all OSPF routers for which a hello packet has been received on the network segment.

The hello packet does not use all of the bit values defined in the Options field description above. We have included the definitions here as a reference guide.

Waiting on OSPFv3

One reason for moving to version 3 of OSPF is scalability of the protocol. Each time we need a new OSPF feature, we have to assign it a bit in the Options field. We already have bits assigned for multicast LSA, opaque LSA, TOS routing, and so forth. The problem is simple; we’ve used up all the bits in the Options field. As a result, the network community is having a difficult time scaling the protocol and adding new functionality.
Database Description Packet

After discovering its neighbors, the local router begins to form an adjacency with each neighbor (as discussed in the “Forming Adjacencies” section later in this chapter). This adjacency process requires that each router advertise its local database information. An OSPF router uses the Database Description (DD) packet for this purpose.

The DD packet, type code 2, summarizes the local database by sending LSA headers to the remote router. The remote router analyzes these headers to determine whether it lacks any information within its own copy of the link-state database. Figure 6.3 details the format of the DD packet.

**FIGURE 6.3** The OSPF Database Description packet

![Diagram: DD packet format](image)

The fields include the following:

**Interface MTU (2 octets)** This field contains the MTU value, in octets, of the outgoing interface. When the interface is used on a virtual link, the field is set to a value of 0x0000.

**Options (1 octet)** The local router advertises its capabilities in this field. The bit values are discussed in the “Hello Packet” section earlier in this chapter.

**Flags (1 octet)** This field provides an OSPF router with the capability to exchange multiple DD packets with a neighbor during an adjacency formation. The flag definitions include the following:

- **Bits 3 through 7** These bit values are currently undefined and must be set to a value of 0.
- **Bit 2** The I bit, or Initial bit, designates whether this DD packet is the first in a series of packets. The first packet has a value of 1, while subsequent packets have a value of 0.
- **Bit 1** The M bit, or More bit, informs the remote router whether the DD packet is the last in a series. The last packet has a value of 0, while previous packets have a value of 1.
- **Bit 0** The MS bit, or Master/Slave bit, is used to indicate which OSPF router is in control of the database synchronization process. The master router uses a value of 1, while the slave uses a value of 0.

**DD Sequence Number (4 octets)** This field guarantees that all DD packets are received and processed during the synchronization process through use of a sequence number. The Master router initializes this field to a unique value in the first DD packet, with each subsequent packet being incremented by 1.
LSA Headers (Variable) This field carries the LSA headers describing the local router’s database information. Each header is 20 octets in length and uniquely identifies each LSA in the database. Each DD packet may contain multiple LSA headers.

**Link-State Request Packet**

During the database synchronization process, the local router may find that it is missing information or that its local copy is out of date. The local router acquires the needed database information by sending a *link-state request packet* to its neighboring router. This packet contains identifiers that uniquely describe the requested LSA. An individual link-state request packet may contain either a single set of identifiers or multiple sets to request multiple LSAs. The format of the link-state request packet, type code 3, is shown in Figure 6.4.

**FIGURE 6.4** The OSPF link-state request packet

<table>
<thead>
<tr>
<th>32 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

The unique LSA identifiers are:

**Link-State Type (4 octets)** This field displays the type of LSA being requested. The possible type codes include:

- 1—Router LSA
- 2—Network LSA
- 3—Network summary LSA
- 4—ASBR summary LSA
- 5—AS external LSA
- 6—Group membership LSA
- 7—NSSA external LSA
- 8—External attributes LSA
- 9—Opaque LSA (link-local scope)
- 10—Opaque LSA (area scope)
- 11—Opaque LSA (AS scope)

**Link-State ID (4 octets)** This field encodes information specific to the LSA. Each different type of advertisement places different information here.

**Advertising Router (4 octets)** The router ID of the OSPF router that first originated the LSA is encoded in this field.
Link-State Update Packet

Information in the link-state database is populated through a Link State Advertisement (LSA). Each LSA contains routing, metric, and topology information to describe a portion of the OSPF network. The local router advertises LSAs within a link-state update packet to its neighboring routers. This packet is reliably flooded throughout the network until each router has a copy. In addition, the local router advertises a link-state update packet in response to a link-state request for information. A link-state update, type code 4, is shown in Figure 6.5.

\[\text{FIGURE 6.5} \quad \text{The OSPF link-state update packet}\]

The two fields in the packet are:

**Number of LSAs (4 octets)** This field displays the number of LSAs carried within the link-state update packet.

**Link-State Advertisements (Variable)** The complete LSA is encoded within this variable-length field. Each type of LSA has a common header format along with specific data fields to describe its information. A link-state update may contain a single LSA or multiple LSAs.

Link-State Acknowledgment Packet

The reliable part of the OSPF reliable flooding paradigm arises from the fact that each router is required to explicitly acknowledge the receipt of each LSA. The local router accomplishes this with the link-state acknowledgment packet. The packet, type code 5, simply contains the common OSPF header followed by a list of LSA headers. This variable-length field allows the local router to acknowledge multiple LSAs using a single packet. Figure 6.6 displays the format of the link-state acknowledgment packet.

\[\text{FIGURE 6.6} \quad \text{The OSPF link-state acknowledgment packet}\]
Forming Adjacencies

Now that we’ve discussed the specific OSPF packet types, let’s explore their usage during the formation of an adjacency. This allows us to understand the interaction of the packet types as well as what the specific portions of the packets actually do.

Adjacency States

During the adjacency formation process, two OSPF routers transition through several states prior to becoming operational neighbors. The possible states include:

**Down**  *Down* is the starting state for all OSPF routers. A start event, such as configuring the protocol, transitions the router to the *Init* state. The local router may list a neighbor in this state when no hello packets have been received within the specified router dead interval for that interface.

**Init**  The *Init* state is reached when an OSPF router receives a hello packet but the local router ID is not listed in the received Neighbor field. This means that bidirectional communication has not been established between the peers.

**Attempt**  The *Attempt* state is valid only for Non-Broadcast Multi-Access (NBMA) networks. It means that a hello packet has not been received from the neighbor and the local router is going to send a Unicast hello packet to that neighbor within the specified hello interval period.

**2-Way**  The *2-Way* state indicates that the local router has received a hello packet with its own router ID in the Neighbor field. Thus, bidirectional communication has been established and the peers are now OSPF neighbors.

**ExStart**  In the *ExStart* state, the local router and its neighbor establish which router is in charge of the database synchronization process. The higher router ID of the two neighbors controls which router becomes the master.

**Exchange**  In the *Exchange* state, the local router and its neighbor exchange DD packets that describe their local databases.

**Loading**  Should the local router require complete LSA information from its neighbor, it transitions to the *Loading* state and begins to send link-state request packets.

**Full**  The *Full* state represents a fully functional OSPF adjacency, with the local router having received a complete link-state database from its peer. Both neighboring routers in this state add the adjacency to their local database and advertise the relationship in a link-state update packet.

These OSPF neighbor states can be seen in Figure 6.7.
FIGURE 6.7  Forming an OSPF adjacency

![Diagram showing OSPF adjacency formation process]

Figure 6.7 shows a generalized adjacency formation process and is not meant to represent every possible scenario in an OSPF network.

Example OSPF Adjacency

Figure 6.7 shows the Shiraz router with a complete link-state database. The Chardonnay router is configured and initialized into the network. The following steps then occur:

1. Chardonnay initiates the conversation by sending a hello packet to Shiraz using the 224.0.0.5 multicast address. The DR and BDR fields are set to 0.0.0.0 and the Neighbor field is empty because Chardonnay has yet to receive any OSPF packets from Shiraz.
2. Shiraz transitions to the $\texttt{Init}$ state (bidirectional communication has not been established) and responds to Chardonnay with a hello packet. Shiraz lists the router ID of Chardonnay, 192.168.1.1, in the Neighbor field of the packet and sets the DR and BDR fields to 0.0.0.0.

3. Chardonnay briefly transitions to the $\texttt{2-Way}$ state (bidirectional communication has been established), but quickly moves to the $\texttt{ExStart}$ state. Chardonnay and Shiraz are now OSPF neighbors. At this point, Chardonnay sends a DD packet to Shiraz. The flags of the DD packet are set to negotiate the Master/Slave relationship to determine which router controls the synchronization process. The I bit, the M bit, and the MS bit are all set to 1; Chardonnay is starting the conversation, has more information to send, and is going to control the conversation. In addition, a sequence number ($x$) is chosen to identify the DD packets in this conversation.

4. Shiraz has a higher router ID (192.168.2.2) than Chardonnay and should be the Master for the process. It therefore responds with its own DD packet using a different sequence number ($a$). Shiraz also sets the I, M, and MS bits to 1 to designate its role in the synchronization process.

5. Chardonnay recognizes Shiraz’s higher router ID and role as the Master by generating a new DD packet containing the sequence number advertised by Shiraz ($a$) and having both the MS and I bits set to 0. At this time, Chardonnay transitions to the $\texttt{Exchange}$ state.

6. Having completed the Master/Slave negotiation process, Shiraz also transitions to the $\texttt{Exchange}$ state and begins sending DD packets with higher sequence numbers that contain the database information.

7. Chardonnay acknowledges the receipt of all DD packets by sending its own DD packets with the same sequence number. These new DD packets contain the information in Chardonnay’s link-state database. As each router receives a DD packet, it notes which LSA headers in the received packet are not in its own local database. This header information is contained in a memory structure called the $\texttt{link-state request list}$.

8. Shiraz receives a DD packet with the M bit set to 0, which indicates that Chardonnay has sent all of the information in its database. Shiraz examines its link-state request list and finds no entries. It then transitions to the $\texttt{Full}$ state and continues sending DD packets to Chardonnay.

9. Chardonnay continues to advertise DD packets with the M bit set to 0 to Shiraz as acknowledgments. This indicates that it is still receiving DD packets from Shiraz and potentially adding information to its link-state request list. When Shiraz finally sends a DD packet with the M bit set to 0, Chardonnay examines its request list and finds multiple headers for which it needs information.

10. Chardonnay transitions to the $\texttt{Loading}$ state and begins requesting its missing data structures using link-state request packets. It receives the needed information from Shiraz in the form of a link-state update packet. This process continues until Chardonnay has emptied the link-state request list, at which point it transitions to the $\texttt{Full}$ state.

After both peers reach an OSPF adjacency state of $\texttt{Full}$, they maintain that adjacency using hello packets at the specified hello interval. Changes to the link-state database on either router are advertised using a link-state update; reliability is assured with a link-state acknowledgment packet.
Troubleshooting an Adjacency Formation

We've taken a fairly quick look at the formation of an OSPF adjacency. When everything is operating properly, forming an adjacency is quite simple. Unfortunately, things can sometimes be different in the real world. Let's look at three possible scenarios where your adjacency does not get to the Full state.

When an OSPF router first receives a hello packet, it verifies that the data in some fields matches its own locally configured information. Should any of the checked data be different, the hello packet is discarded and not processed. The data fields verified are the Area ID, Authentication, Network Mask (on broadcast networks), Hello Interval, Router Dead Interval, and Options fields. In situations where this information differs, the neighbor remains in the Down state because it can't process your advertised hello. These types of neighbors are not visible with any JUNOS software show command.

Firewalls and packet filters often cause OSPF to have trouble forming a neighbor relationship. For example, say the remote router you're trying to form an adjacency with has an inbound filter applied to its loopback interface. This filter allows only diagnostic pings and Secure Shell (SSH) traffic into the router for security reasons. Unfortunately for you, your partner forgot about allowing the IP routing protocols through the filter. In this situation, the remote router sends you a hello packet. You do not see your router ID in the Neighbor field and transition to the Init state. You then generate your own hello packet and send it to your neighbor, who doesn't receive it because of the filter. At the expiration of the hello interval, the remote router sends another hello packet to you. Again, your router ID is not listed in the Neighbor field. You remain in the Init state and send your own hello packet to the remote router. This process continues until the filter is altered on the remote router to allow OSPF packets (protocol ID 89) through.

Finally, your OSPF adjacency might get stuck in the ExStart state. This occurs due to a final check the routers perform. In the DD packet, each router advertises the IP MTU of the interface it is using. Should the local and remote routers not agree on the MTU of the network link, the database synchronization process stops and both neighbors remain in the ExStart state. This increases the robustness of the protocol because fragmentation of the OSPF packets no longer occurs. In an environment where both peers have the same interface type and default MTU settings, this situation rarely occurs. One classic example of this scenario is when two peers are connected using a Frame Relay-to-ATM connection. One peer uses Frame Relay encapsulation while the other peer is using ATM encapsulation. The intervening carrier makes the transition from one encapsulation type to the other. The default MTUs for these links do not match, and the OSPF adjacency sticks in the ExStart state unless you manually change one side or the other.
Evolution of an OSPF Network

We’ve now examined how a link-state protocol operates at a high level. In addition, we explored how OSPF forms neighbor relationships and synchronizes its link-state databases. We now need to look at the actual data within the database itself. This information is encoded within an LSA.

To help you correlate the LSA types with their use, we’ll base our discussion on a sample network. This allows us to see how the LSA advertises the status of a router and its connected subnets. Other discussion points include scaling your OSPF network and advertising external routing information. Let’s start with the basics first.

The Router LSA

The first step in building an OSPF network is advertising the networks connected to the local router. This information is contained in the router LSA, type code 1, which displays data about the local router. This includes all links connected to the router, the metrics of those interfaces, and the OSPF capabilities of the router.

Throughout the remainder of this chapter, we follow the common industry nomenclature by referring to LSAs by both their name (router LSA) as well as their type code (Type 1 LSA).

Figure 6.8 shows two routers, Shiraz and Chardonnay, in an OSPF network. Each generates a router LSA and places it into its local database. After becoming adjacent, both Shiraz and Chardonnay flood the Type 1 LSA to each other. This describes the directly connected networks of the router, including the loopback interfaces.

This is a fairly simple example, but consider a larger network consisting of multiple routers, as depicted in Figure 6.9.

As Shiraz now floods its Type 1 LSA into the network, Chardonnay re-floods the LSA to its connected neighbors. This is the expected behavior of a link-state protocol, because each router must maintain an identical link-state database. Figure 6.9 shows the router LSA only for Shiraz, but a similar procedure occurs for each router in the network. The end result is that each router has nine Type 1 LSAs in its local database, one for each router.
Broadcast Networks

In the “Forming Adjacencies” section earlier in this chapter, we discussed how two OSPF routers become neighbors. Each set of connected routers performs this peer-to-peer process. Broadcast segments in a network, such as an Ethernet link, pose a special problem to link-state protocols and their peer-to-peer nature. Multiple routers on the same physical segment share the resources of that link and produce a lot of redundant information.

Figure 6.10 shows an Ethernet segment with five routers physically attached: Sangria, Chardonnay, Cabernet, Shiraz, and Merlot. Each router on the segment sees an OSPF hello packet from all other routers because the packet is addressed to 224.0.0.5, AllSPFRouters. This prompts each router to form an adjacency with every other router on the segment, as seen in Figure 6.10. This default behavior results in 10 separate adjacencies formed for this single broadcast link.

FIGURE 6.9 Flooding the router LSA

FIGURE 6.10 OSPF peering on broadcast media
The ramifications of this process are twofold. First, each router reports the same set of information, the Ethernet link, to the rest of the OSPF network. Second, and perhaps more damaging, every router floods LSAs to each of its adjacent neighbors using the 224.0.0.5 multicast address. Using Figure 6.10 as a reference, assume that the Shiraz router receives a router LSA from some other router in the network. Shiraz floods that router LSA to each of its neighbors: Sangria, Chardonnay, Cabernet, and Merlot. Each of the four LSAs used the multicast destination address, so each router received the exact same LSA four times. To complicate matters, each of the four receiving routers re-floods the LSA to each of its adjacent neighbors, causing the duplication process to continue. This is clearly not an effective use of resources.

**Designated Routers**

OSPF avoids these problems through the use of a router known as the designated router (DR). Each broadcast segment in an OSPF network elects a designated router to act as the main point of contact for the network segment. Each router on the link must become adjacent with the DR, which handles all LSAs for the network. Each router sends the DR information using a new multicast destination address of 224.0.0.6, AllDRRouters. The designated router generates a network LSA, type code 2, to represent the broadcast segment to the rest of the network. Like the router LSA, the Type 2 LSA has an area-flooding scope ensuring that each router in the area receives a copy for the link-state database.

The use of a designated router virtually eliminates the excess flooding of LSAs on the segment at the expense of introducing a single point of failure—the DR itself. Avoiding this potential pitfall requires the election of another router on the segment, the backup designated router (BDR). The BDR also listens to the 224.0.0.6 multicast address and monitors the operations of the DR. Additionally, the BDR forms a Full adjacency relationship with all other routers on the segment. Should a problem arise with the designated router, the BDR immediately assumes the role of the DR for the segment. This mechanism provides for stability in the network.

Figure 6.11 displays the adjacencies formed on a broadcast segment when the DR (Sangria) and BDR (Chardonnay) routers are operational. While the total number of adjacencies didn’t drop dramatically—from 10 to 7—the savings in LSA flooding is what proves useful in this environment. When the Shiraz router now receives a router LSA from some other router in the network, it floods it only to the 224.0.0.6 address for the DR and the BDR. The designated router re-floods the LSA to the segment using the 224.0.0.5 address. Because each of the routers has an adjacency only with the DR/BDR pair, no further flooding of the LSA across the segment is needed, preserving the resources of the network.

**DR Elections**

Although the designated router is a logical responsibility, it is in fact an actual router on the broadcast segment. Some process is required to determine which router should assume this responsibility. This is the function of the designated router election.

A DR election occurs when no operational designated router is present. This information is gleaned from the hello packet field where the current DR address is encoded. The election of a DR is based on two separate criteria: the router ID and the router priority of each router. An
OSPF hello packet, complete with header, provides the required data. The router priority of all participating routers is examined first, with the highest priority router becoming the DR. Any router reporting a priority value of 0 is ineligible to become either the DR or the BDR. In the event of a priority tie, the router ID of each router is then examined. Again, the highest value results in that router becoming the designated router.

Once a DR is elected for the segment, the remaining routers then elect the backup designated router for redundancy. The same criteria are used for this process—the router priority followed by the router ID. The failure of the current designated router causes the BDR to transition to the role of DR. A new election is performed to determine the new backup designated router.

The network in Figure 6.11 shows the router priority and router ID for the routers attached to the Ethernet segment. Assuming that the routers start within 40 seconds of each other, Sangria becomes the DR with its router priority of 100. The second highest priority value of 90 belongs to Chardonnay, making it the backup designated router. If Sangria disappears from the network, Chardonnay assumes the role of DR and a new election takes place. The Cabernet, Shiraz, and Merlot routers all share a priority of 50, so the router ID of each router is compared. Cabernet’s router ID of 10.0.0.50 is numerically higher than the other routers and it becomes the new BDR.

The wait time for electing the first designated router on the segment arises from an OSPF timer called the $\text{WaitTimer}$. It is set to the router dead interval (40 seconds by default) and helps to guarantee that all operational routers have the opportunity to receive and send hello packets before the election occurs.
When Sangria returns to the network, it does not automatically assume the DR role again. It receives a hello packet detailing Chardonnay as the current DR and Cabernet as the current BDR. Only when Cabernet becomes the DR (due to a failure of Chardonnay) does the priority of Sangria come into play and it is elected the new BDR. Cabernet will then have to fail in order for Sangria to once again become the designated router on this broadcast segment. This process is considered to be non-deterministic because the router with the best criteria is not guaranteed to be the designated router.

**Scaling an OSPF Network**

As the number of routers in the network grows, so does the amount of information in the link-state database. Additionally, each router requires more bandwidth and resources to flood the LSAs throughout the network. OSPF has mechanisms to limit the flooding scope of the LSAs and scale the network.

The building block for scaling an OSPF network is the concept of an area. OSPF areas limit the flooding of LSAs and control the size of the link-state database by retaining that data within the area boundary. Specific routers control this flooding process and allow certain information across the area boundary. Specifically, a network summary LSA is used to allow other portions of the OSPF network to retain database knowledge of the new area. We’ll explore each of these concepts in some more detail.

**OSPF Areas**

The primary purpose of an OSPF area is scalability of the protocol. Boundaries are defined in the network to limit the flooding of specific LSA types. Each newly created area is assigned a unique 32-bit area ID value. This is represented in a quad-octet format of 0.0.0.0, much like an IP address. Although the router works with area numbers in this fashion, most humans prefer to use whole numbers, such as area 0.

The JUNOS software automatically converts decimal values into quad-octet format. Area 0 becomes area 0.0.0.0, while area 300 becomes 0.0.1.44.

One of the newly defined areas, the backbone area, forms the core of the network. All other OSPF areas must connect to the backbone area. The backbone connects all areas and redistributes all non-backbone routing information between the areas.

The breakup of the OSPF network into areas also affects each router’s local link-state database. It is no longer identical to the databases on every other router in the domain, which appears at odds with the core tenet of link-state protocols. This apparent contradiction is resolved through a more concise definition of this requirement. Within OSPF, the link-state database must be identical on all routers within an area.
Router Types

The roles and responsibilities of specific OSPF routers are defined by their location in the network. The router types include:

**Internal router**  A router that maintains all operational interfaces within a single area is known as an *internal router*. An internal router may belong to any OSPF area.

**Backbone router**  A router that has at least one interface in area 0 is known as a *backbone router*.

**Area border router**  The *area border router (ABR)* connects one or more OSPF areas to the backbone. This means that at least one interface is within area 0 while another interface is in another area. The ABR plays a very important role in an OSPF network. We’ll see its responsibilities grow as we scale and expand our routing domain.

**Autonomous System boundary router**  An *Autonomous System boundary router (ASBR)* injects external routing knowledge into an OSPF network. ASBRs are discussed in more detail in the “Non-OSPF Routes” section later in this chapter.

Figure 6.12 displays our sample network with two areas, area 0 and area 10. Shiraz, Merlot, and Riesling are completely within area 10, making them internal area routers. Cabernet, on the other hand, is an internal backbone router because all its interfaces are within area 0. The Chardonnay router has interfaces in both area 10 and the backbone, making it an ABR.

**FIGURE 6.12**  Designating area boundaries
The area boundaries in Figure 6.12 result in router and network LSAs from area 10 remaining in that area. When Shiraz floods a Type 1 or Type 2 LSA into area 10, Chardonnay no longer floods those LSAs to all its OSPF neighbors. Instead, only other area 10 routers receive them—Merlot and Riesling, in our case. The reduced flooding scope introduces a problem for Cabernet, and other backbone routers, because they no longer receive network and metric information about Shiraz. OSPF mitigates this issue by allowing the ABR, Chardonnay, to advertise the required information in another LSA type.

**Real World Scenario**

**Design Considerations**

The use of OSPF areas is an effective tool in minimizing the flooding scope of LSAs. Placing area boundaries and determining which routers become ABRs can be quite arbitrary, but the good network architect should consider some factors.

One easy decision point involves physical connectivity and topology of the network. If you have a central campus and several regional offices, it might make sense to partition the network along those same lines. Forcing a logical OSPF design that differs greatly from your topology might cause more problems in the long run.

Additionally, it is generally a good idea to have more than one ABR connecting an area to the backbone. The lack of dual ABRs presents a single point of failure in your design. Should one of the routers fail, its partner maintains connectivity as well as a valid forwarding path. With only a single ABR, its failure segments the area from the backbone, and the area destinations become unreachable.

The resources and bandwidth capabilities of the routers in your network are other factors to consider. The ABRs must support a larger link-state database than the area routers. Calculating the SPF algorithm against this larger database requires more resources. Of course, some of these considerations greatly depend on the size of your network. In a stable network, a Juniper Networks router can support over 200 routers in a single area and maintain multiple links to different areas.

Finally, the backbone routers might pass more user traffic along their links since all inter-area traffic flows through the backbone and not directly between the non-backbone areas. This generally means that more powerful backbone routers and higher-speed links are placed in the backbone area.

**Network Summary LSA**

Routing knowledge crosses an area boundary in an OSPF network by using a network summary LSA, type code 3. By default, each Type 3 LSA matches a single router LSA or network LSA on a one-for-one basis. This correlation is taken a step further in that the network summary LSA also has an area-flooding scope. This means that an OSPF router floods the LSA only to other routers in its same area. Figure 6.13 illustrates this concept.
Shiraz is advertising its router LSA within area 10. Its flooding scope keeps the LSA contained to Chardonnay, Merlot, and Riesling, as we discussed in the “Router Types” section earlier in this chapter. Chardonnay’s role as an ABR allows it to generate a network summary LSA that contains the subnet information in the Type 1 LSA of Shiraz. This new Type 3 LSA is flooded into the backbone. All area 0 routers, including Cabernet and Sangria, receive this information and place it in their local databases. After running the SPF algorithm, the backbone routers have reachability to Shiraz and its connected subnets.

The flooding scope of the Type 3 LSA does cause a problem, however. A closer examination of Figure 6.13 shows that Sangria, the ABR for area 22, is not flooding the Type 3 LSA from Chardonnay into that non-backbone area. To provide for this type of situation, OSPF allows Sangria to generate its own network summary LSA that matches the information in Chardonnay’s version. Again, this generation of new LSAs is performed on a one-for-one basis. Sangria then floods the new Type 3 LSA into area 22.

Figure 6.14 shows the end result of this new LSA flooding: Every router in the OSPF network has reachability to every other router through a combination of router and network summary LSAs.
Non-OSPФ Routes

Both the router and network summary LSAs are effective at propagating internal OSPF routing knowledge throughout the network. They are not capable, however, of carrying external routing information. The AS external LSA, type code 5, was defined for this explicit purpose.

External routes in an OSPF network can come in multiple forms. Perhaps we need to redistribute some static routes, or we recently purchased a network that is not currently running OSPF. Some portions of our own network—a server farm, for example—may be incapable of running OSPF internally. In any case, we have a requirement for reachability to these networks from our OSPF routers.

Figure 6.15 shows Cabernet now connected to a server farm network, making it an ASBR. Each external network is advertised into OSPF in a separate Type 5 LSA. Unlike the router, network, and network summary LSAs, the AS external LSA has a domain-flooding scope. This means that the ABR no longer stops the flooding process, but instead continues it into its respective areas. A look at Figure 6.15 shows this flooding process; Shiraz receives the same unique LSA as do the routers in area 22.
While the Type 5 LSA provides the network information necessary to reach the external networks, the OSPF routers may not automatically begin using that data. The address of the ASBR, Cabernet in our case, must be known in the link-state database via a router LSA. Chardonnay, Sangria, and the other backbone routers meet this criterion, because they share an area 0 database with Cabernet. It is the routers in area 10 and 22 that are currently not able to utilize the AS external LSA.

Once again, the ABR solves our problem by generating a new LSA type. For each ASBR reachable by a router LSA, the ABR creates an **ASBR summary LSA**, type code 4, and injects it into the appropriate area. This LSA provides reachability information to the ASBR itself. Like a Type 3 LSA, the ASBR summary LSA has area scope and is generated by an ABR. Using Figure 6.15 as a guide, Chardonnay generates a Type 4 LSA and floods it to Shiraz, Merlot, and Riesling. Sangria accomplishes the same task for area 22. All OSPF routers in the domain now have routing knowledge of the server farm network, and each router is able to use the information in the AS external LSA.
Additional Scaling Techniques

In our example, the creation of areas assisted in scaling the size of our OSPF network through a reduction in LSA flooding requirements and processing. It did not, however, affect the size of the link-state database itself. Each router in the network still has information in its database for each internal and external route. Some vendor implementations may have trouble with a large database, particularly older or smaller-scale routers. For networks in this situation, you may alter the behavior of an OSPF area to reduce the size of the link-state database. Three varieties of areas accomplish this: a stub area, a totally stubby area, and a not-so-stubby area.

We examine each of these area types in turn, using Figure 6.16 as a starting point. In this figure, both the ABRs of Chardonnay and Sangria are flooding summary LSAs, ASBR summary LSAs, and AS external LSAs into their respective areas. The Type 3 LSAs represent backbone networks as well as networks from the opposite area. The Type 5 LSAs are for the server farm networks, while the Type 4 LSAs represent the ASBR of Cabernet.

**Figure 6.16** A full OSPF database

**Stub Areas**

An OSPF stub area provides for a smaller link-state database by restricting the presence of AS external LSAs within the area. Since a single Type 5 LSA is generated for each external route,
the potential number of LSAs in an OSPF network can be quite sizeable. Some OSPF areas do not benefit from the explicit routing knowledge provided by the Type 5 LSAs.

The Shiraz router in area 10, for example, may have 5,000 external routes in its database. Each of those routes uses Chardonnay, the ABR, as the next hop in the routing table. From a reachability standpoint, Shiraz can send user data packets using these explicit routes or by using a default 0.0.0.0 /0 route that also points to Chardonnay. Either way, the data packets reach the ABR, which has explicit routing knowledge of the external routes and forwards the packets through the backbone to the ASBR. The disadvantage of forwarding potentially unroutable packets is outweighed by the large reduction in the size of the link-state database and the internal processing that database requires.

The responsibility for enforcing an OSPF stub area rests with the ABR. Under normal circumstances, the ABR re-floods the Type 5 LSAs into the area. When configured as a stub area, however, the ABR simply does not flood the AS external LSAs into the area. To provide the required IP reachability, the ABR should instead generate a summary LSA for the default route and inject that into the stub area.

Figure 6.17 shows area 10 as a stub area. Chardonnay is no longer forwarding the AS external LSAs into the area. Type 3 LSAs representing internal OSPF networks continue to be flooded, and Chardonnay generates its 0.0.0.0 /0 summary LSA for area 10 as well. The area routers Shiraz, Merlot, and Riesling still have reachability to the server farm networks, and the link-state database on those routers has been greatly reduced.

**Figure 6.17** An OSPF stub area
A closer examination of Figure 6.17 also reveals that Chardonnay is no longer generating ASBR summary LSAs as well. Recall from the “Non-OSPF Routes” section earlier in this chapter that the Type 4 LSAs allow OSPF routers simply to use the AS external LSAs in their databases. In a stub environment, the Type 5 LSAs are not present in the area routers, so the need for the ASBR summary LSAs is moot. The ABR, therefore, stops generating those LSAs as well.

**Totally Stubby Areas**

The stub area concept is expanded and carried one step further with a *totally stubby area*. A summary LSA default route replaces the Type 5 LSAs in the stub area. The area routers forward all external traffic to the ABR. This single ABR is also the exit point for all backbone and inter-area traffic. This allows us to further reduce the link-state database by preventing the generation of summary LSAs on the ABR.

In Figure 6.18, we’ve changed area 10 into a totally stubby area. The ABR, Chardonnay, has stopped creating and flooding Type 3 LSAs for the backbone and for area 22 routes. The default Type 3 LSA is generated to provide reachability to all routes outside area 10. The basic operation of the stub area did not change in this situation. Types 4 and 5 LSAs are still not present in the area 10 routers. Shiraz, Merlot, and Riesling have only LSAs originated in area 10 and the default summary LSA in their databases.

**FIGURE 6.18** An OSPF totally stubby area
**Not-So-Stubby Area**

The exclusion of AS external LSAs in a stub area means that an ASBR is not permitted to operate within the confines of that area. This restriction may prove beneficial in the majority of circumstances, but the possibility exists for an exception. Suppose that your OSPF network requires connectivity to a partner that is using RIP within its network. Because of physical necessity, this partner can connect only to the Muscat router in area 22. The routers in this area have been suffering from similar database issues that caused area 10 to become stub. The plan was to make area 22 a stub area as well, but the new requirement for an ASBR may negate this change. This exact set of circumstances led to the development of the **not-so-stubby area (NSSA)**.

A not-so-stubby area is an OSPF stub area that allows some external routes to be present in the database. This is accomplished with a new **NSSA external LSA**, type code 7. The Type 7 LSA carries external routing information from the ASBR within the NSSA. It has an area flooding scope, so only routers in the NSSA receive the Type 7 LSA. The external routing information within the LSA is converted by the ABR into an AS external LSA at the area boundary. The ABR floods the Type 5 LSA into the OSPF domain, and no other routers in the network are aware of the NSSA configuration.

Area 22 in our sample network is configured as an NSSA, as seen in Figure 6.19. The Muscat router is connected to the partner network and is injecting Type 7 LSAs into area 22. These are flooded within the area to all other OSPF routers. Sangria, the ABR, converts the Type 7 LSA into an AS external LSA. It then floods the new Type 5 LSA into the backbone. In addition, Sangria generates a Type 4 LSA, because the ASBR is in another area, and floods that into area 0 as well. The operation of the rest of the OSPF network does not change based on the NSSA configuration in area 22, and IP reachability is achieved by all internal and external networks.

**OSPF Configuration**

The configuration of an OSPF network on a Juniper Networks router is an extremely straightforward task. The router simply needs to know which interfaces are assigned to which OSPF areas. All configuration is accomplished within the `edit protocols ospf` hierarchy.

**Single OSPF Area**

The most basic OSPF network is a single-area design, so let's start there. Figure 6.20 shows a single-area OSPF network.
FIGURE 6.19  An OSPF not-so-stubby area

FIGURE 6.20  An OSPF single-area network
The Chablis router in area 0 is a backbone router with all interfaces within the area. This allows you to configure OSPF using two commands:

```
[edit protocols ospf]
user@Chablis# set area 0 interface all
user@Chablis# set area 0 interface fxp0 disable
```

This results in the configuration of Chablis appearing like so:

```
[edit protocols ospf]
user@Chablis# show
area 0.0.0.0 {
  interface all;
  interface fxp0.0 {
    disable;
  }
}
```

Instead of explicitly specifying each of the interfaces on Chablis that should run OSPF, we have informed the router to operate the protocol on all configured IPv4 interfaces. To prevent the router from forming OSPF adjacencies across the management interface of `fxp0.0`, we explicitly disabled that interface in the configuration.

---

Within the configuration of a protocol, any reference to a specific interface supersedes the parameters of the `interface all` statement.

---

The opposite approach of configuration is taken with the Chardonnay router; each interface is referenced explicitly:

```
[edit protocols ospf]
user@Chardonnay# set area 0 interface so-0/0/1
user@Chardonnay# set area 0 interface at-0/1/0.100
```

This results in the following configuration:

```
[edit protocols ospf]
user@Chardonnay# show
area 0.0.0.0 {
  interface so-0/0/1.0;
  interface at-0/1/0.100;
}
```

Each physical interface and logical unit number, if appropriate, is configured within the desired area. The `so-0/0/1` interface connects Chardonnay to the Sherry router. The logical
unit was omitted from the set command because the JUNOS software assumes a unit value of 0 if none is provided. The same process is not as effective for the connection to the Bordeaux router. This connection is using an ATM virtual circuit identifier (VCI) of 100 on logical unit 100. Had the logical unit not been specified, the router would have assumed unit 0 and Chardonnay wouldn’t have been able to communicate with Bordeaux.

Multiple OSPF Areas

The configuration of a multiarea OSPF network is not much different than that of a single-area network. All area routers and backbone routers place all interfaces within their respective areas. It is the ABRs that have the extra work to do. Figure 6.21 shows a multiarea OSPF network.

FIGURE 6.21 An OSPF multiarea network

Our single-area network has grown and Chardonnay has become an ABR for area 10 with connections to the routers of Shiraz, Merlot, and Riesling. The configuration of Chardonnay for area 0 is already completed. We now add the interfaces within area 10:

[edit protocols ospf]
user@Chardonnay# set area 10 interface so-0/0/2
user@Chardonnay# set area 10 interface so-0/0/0
user@Chardonnay# set area 10 interface so-0/0/3
Chardonnay’s configuration now appears as:

```
[edit protocols ospf]
user@Chardonnay# show
area 0.0.0.0 {
    interface so-0/0/1.0;
    interface at-0/1/0.100;
}
area 0.0.0.10 {
    interface so-0/0/2.0;
    interface so-0/0/0.0;
    interface so-0/0/3.0;
}
```

**J UNOS software Commands**

After deploying and configuring the OSPF network, you must verify the operation of the network. Additionally, you may need to do some network troubleshooting. The JUNOS software provides many `show` commands to use for this purpose. We’ll examine a few of the basic commands, using Figure 6.21 as a sample network.

**Troubleshooting Your Configuration**

Once you’ve committed your configuration to the router and returned to the user operational mode, you may find that the network isn’t quite right. Configuration issues often appear as problems with your OSPF interfaces and neighbors. We have the ability to verify these issues within the software.

**show ospf interface**

The first troubleshooting step is often to determine the state of the local router’s interfaces. Each configured OSPF interface must be operational before any packets are sent. A non-operational interface means that no neighbors will be located, no adjacencies will form, and the link-state database won’t be populated. The `show ospf interface` command provides insight into this information:

```
user@Chardonnay> show ospf interface
Interface   State   Area    DR ID       BDR ID       Nbrs
at-0/1/0.100 PtToPt   0.0.0.0  0.0.0.0     0.0.0.0     1
so-0/0/1.0   PtToPt   0.0.0.0  0.0.0.0     0.0.0.0     1
so-0/0/0.0   PtToPt   0.0.0.10 0.0.0.0     0.0.0.0     1
so-0/0/2.0   PtToPt   0.0.0.10 0.0.0.0     0.0.0.0     1
so-0/0/3.0   PtToPt   0.0.0.10 0.0.0.0     0.0.0.0     1
```
Chapter 6 • Open Shortest Path First (OSPF)

The various fields in the command output are:

**Interface** Configured OSPF interfaces that are physically present in the router are displayed in this column. Failure to properly enter a logical unit value results in the interface not appearing in this output.

**State** The current state of the interface is displayed in this column. Possible values include:
- **BDR**—The local router is the backup designated router.
- **Down**—The interface is not currently operational.
- **DR**—The local router is the designated router.
- **DRother**—The local router is neither the DR nor the BDR.
- **PtToPt**—This is a point-to-point interface.

**Area** This field displays the current area ID assigned to the interface.

**DR ID** The router ID of the current designated router is displayed in this column. Point-to-point interfaces use a value of 0.0.0.0.

**BDR ID** The router ID of the current backup designated router is displayed in this column. Point-to-point interfaces use a value of 0.0.0.0.

**Nbrs** The value in this column represents the total number of OSPF neighbors discovered across this interface.

**show ospf neighbor**

Once you are certain the interfaces are properly assigned and operational, you should check the status of the neighbor’s adjacency by using the `show ospf neighbor` command:

```
user@Chardonnay> show ospf neighbor

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.46</td>
<td>at-0/1/0.100</td>
<td>Full</td>
<td>10.0.1.103</td>
<td>128</td>
<td>36</td>
</tr>
<tr>
<td>10.0.1.34</td>
<td>so-0/0/1.0</td>
<td>Full</td>
<td>10.0.1.102</td>
<td>128</td>
<td>35</td>
</tr>
<tr>
<td>10.0.1.9</td>
<td>so-0/0/0.0</td>
<td>Full</td>
<td>10.0.1.21</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>10.0.1.5</td>
<td>so-0/0/2.0</td>
<td>Full</td>
<td>10.0.1.22</td>
<td>128</td>
<td>32</td>
</tr>
<tr>
<td>10.0.1.1</td>
<td>so-0/0/3.0</td>
<td>Full</td>
<td>10.0.1.23</td>
<td>128</td>
<td>39</td>
</tr>
</tbody>
</table>
```

The fields in this output represent:

**Address** The physical interface IP address of the neighbor is displayed in this column.

**Interface** This column shows the OSPF interface that the neighbor is reachable across.

**State** The current OSPF adjacency state is displayed here. The possible state values are discussed in the “Forming Adjacencies” section earlier in this chapter.

**ID** This field shows the router ID of the neighbor. This is used with the **Pri** field to elect a **DR** or **BDR** on a broadcast segment.
Pri  The router priority is displayed in this field. This value is used with the ID field to elect a DR or BDR on a broadcast or NBMA segment.

Dead  The time remaining until the OSPF neighbor is declared unreachable appears in this column. Each received hello packet resets this timer to the router dead interval value.

clear ospf neighbor

It may be necessary to reset the peer session to a neighbor. This may occur if the remote router is malfunctioning or if you want to refresh the link-state database with new information. This is accomplished with the `clear ospf neighbor neighbor-address` command. The optional `neighbor-address` switch clears that specific neighbor. The `clear ospf neighbor` command, with no switches, clears all OSPF neighbors.

Troubleshooting the Routing Protocol

After the local router has found its neighbors and formed its adjacencies, flooding of LSAs ensues. This populates the link-state database and the Dijkstra calculation is performed. In addition, the periodic transmission of hello and link-state update packets is performed to maintain the adjacencies and the consistency of the database. Various commands provide some visibility to these processes.

show ospf database

The `show ospf database` command is an excellent tool in troubleshooting OSPF. If the information is not in the database, it will not appear in the routing table. The output shows summary information about each LSA on a per-area basis:

```
user@Shiraz> show ospf database

OSPF link state database, area 0.0.0.10

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>*10.0.1.21</td>
<td>10.0.1.21</td>
<td>0x80000004</td>
<td>2965</td>
<td>0x2</td>
<td>0x3407</td>
<td>60</td>
</tr>
<tr>
<td>Router</td>
<td>10.0.1.22</td>
<td>10.0.1.22</td>
<td>0x80000004</td>
<td>2971</td>
<td>0x2</td>
<td>0xb58a</td>
<td>60</td>
</tr>
<tr>
<td>Router</td>
<td>10.0.1.23</td>
<td>10.0.1.23</td>
<td>0x80000008</td>
<td>2800</td>
<td>0x2</td>
<td>0x2f12</td>
<td>60</td>
</tr>
<tr>
<td>Router</td>
<td>10.0.1.101</td>
<td>10.0.1.101</td>
<td>0x8000000c</td>
<td>1328</td>
<td>0x2</td>
<td>0x6d4</td>
<td>108</td>
</tr>
<tr>
<td>Summary</td>
<td>10.0.1.0</td>
<td>10.0.1.101</td>
<td>0x80000005</td>
<td>728</td>
<td>0x2</td>
<td>0x3525</td>
<td>28</td>
</tr>
<tr>
<td>ASBRSum</td>
<td>10.0.1.105</td>
<td>10.0.1.101</td>
<td>0x80000006</td>
<td>128</td>
<td>0x2</td>
<td>0xf976</td>
<td>28</td>
</tr>
</tbody>
</table>

OSPF external link state database

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extern</td>
<td>192.168.1.0</td>
<td>10.0.1.105</td>
<td>0x80000034</td>
<td>306</td>
<td>0x2</td>
<td>0xe5da</td>
<td>36</td>
</tr>
<tr>
<td>Extern</td>
<td>192.168.2.0</td>
<td>10.0.1.105</td>
<td>0x80000034</td>
<td>5</td>
<td>0x2</td>
<td>0xdae4</td>
<td>36</td>
</tr>
<tr>
<td>Extern</td>
<td>192.168.3.0</td>
<td>10.0.1.105</td>
<td>0x80000033</td>
<td>1206</td>
<td>0x2</td>
<td>0xd1ed</td>
<td>36</td>
</tr>
<tr>
<td>Extern</td>
<td>192.168.4.0</td>
<td>10.0.1.105</td>
<td>0x80000033</td>
<td>907</td>
<td>0x2</td>
<td>0xc6f7</td>
<td>36</td>
</tr>
</tbody>
</table>
Chapter 6 • Open Shortest Path First (OSPF)

The fields in the command output represent the following information:

**Type**  The LSA type is displayed in this field. The possible names include:
- **Router**—Type 1 router LSA
- **Network**—Type 2 network LSA
- **Summary**—Type 3 network summary LSA
- **ASBRSum**—Type 4 ASBR summary LSA
- **Extern**—Type 5 AS external LSA
- **NSSA**—Type 7 NSSA external LSA

**ID**  This field shows the Link-State ID field from the LSA. This value is used to provide uniqueness for each LSA. Entries marked with an asterisk (*) are LSAs generated by the local router.

**Adv Rtr**  The router ID of the originating router for each LSA is displayed in this field.

**Seq**  The sequence number assists the router to determine the most recent version of the LSA.

**Age**  This field displays the current age of the LSA. All LSAs begin with a lifetime of 0 and increment to a defined MaxAge of 3600 seconds. Each LSA must be refreshed before the MaxAge value is reached.

**Opt**  The Options field from the OSPF header is displayed in this column. The possible bit values are discussed in the “Hello Packet” section earlier in this chapter.

**Cksum**  The calculated checksum value of the LSA is stored in this field. Each router calculates a new checksum when the LSA is received and verifies the value against the received value to ensure packet integrity.

**Len**  This field displays the total length of the LSA.

**clear ospf database**

By default, stale information in the link-state database is purged once the LSA Age reaches the MaxAge of 3600 seconds. You can start this process manually with the `clear ospf database` command. This command deletes all information in your local link-state database. Newly flooded LSAs repopulate the database, and the local router recalculates the SPF algorithm. The use of the `purge` option sets all LSAs in the current database to the MaxAge of 3600 and floods that information into the network. Again, newly flooded LSAs repopulate the database.

In our example, once the link-state database on Shiraz is purged, we issue `show ospf database` to display the new LSAs with ages of 2 and 3 seconds:

```
user@Shiraz> clear ospf database purge
user@Shiraz> show ospf database

OSPF link state database, area 0.0.0.10
```
The use of the `clear ospf database` command removes information from your local OSPF database in the hopes that your neighbors advertise routing information back to the local router. Additionally, each OSPF adjacency is reset. This is a disruptive procedure that causes the local router to lose routing information, if only temporarily. This command should be used with caution on production networks.

**show ospf log**

The `show ospf log` command displays how often the SPF algorithm is being initiated and how long each operation takes to finish. Certain OSPF events repeating themselves in rapid succession may be a sign of an inadvertently injected routing loop or an LSA that is taking too long to propagate across the network. Most commonly, a network link that is flapping consistently causes the router to recalculate SPF on a rapid basis.

The output of the `show ospf log` command displays the most recent occurrence of each OSPF event. The longest instance of each category is also displayed. Finally, you can view a history of events the local router has performed.

```
user@Shiraz> show ospf log

Last instance of each event type

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:17:29</td>
<td>SPF</td>
<td>0.000073</td>
</tr>
<tr>
<td>00:17:29</td>
<td>Stub</td>
<td>0.000067</td>
</tr>
<tr>
<td>00:17:29</td>
<td>Interarea</td>
<td>0.000025</td>
</tr>
<tr>
<td>00:17:29</td>
<td>External</td>
<td>0.000003</td>
</tr>
<tr>
<td>00:17:29</td>
<td>NSSA</td>
<td>0.000003</td>
</tr>
<tr>
<td>00:17:29</td>
<td>Cleanup</td>
<td>0.000083</td>
</tr>
</tbody>
</table>

Maximum length of each event type

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:17:57</td>
<td>SPF</td>
<td>0.000116</td>
</tr>
<tr>
<td>00:22:41</td>
<td>Stub</td>
<td>0.000365</td>
</tr>
<tr>
<td>20:00:18</td>
<td>Interarea</td>
<td>0.000132</td>
</tr>
<tr>
<td>01:19:43</td>
<td>External</td>
<td>0.000042</td>
</tr>
</tbody>
</table>
```
show ospf statistics

The `show ospf statistics` command displays counters based on the OSPF packet type. Both the total number of packets and the number in the last 5 seconds is shown. Additionally, you can see the total number of LSA retransmissions with this command. If this value rapidly increases, it means your OSPF neighbor is not acknowledging its receipt of your LSAs. The remote router is either overworked or malfunctioning. Finally, the number and types of errors seen by the local router are displayed:

```
user@Shiraz> show ospf statistics

Packet type | Total Sent | Total Received | Last 5 seconds Sent | Last 5 seconds Received
>Hello | 24 | 45 | 0 | 0
>DbD | 24 | 16 | 0 | 0
>LSReq | 6 | 7 | 0 | 0
>LSUpdate | 375 | 2260 | 0 | 0
>LSAck | 2236 | 368 | 0 | 0

LSAs retransmitted: 2, last 5 seconds: 0

Flood queue depth: 0
Total rexmit entries: 0, db summaries: 0, lsreq entries: 0

Receive errors:
  25 stub area mismatches
  4 nssa mismatches
```
Viewing OSPF Routes

The purpose of utilizing OSPF as a routing protocol is to place routes in the routing table for forwarding traffic. The SPF algorithm generates the routes based on information found in the link-state database. The JUNOS software provides the ability to view those routes after the SPF calculation and after they are placed in the routing table.

*show ospf route*

The `show ospf route` command displays the results of the SPF algorithm. These are the routes that OSPF is handing off to the routing table. Each destination route includes a type (internal versus external), the LSA type used to find the route, a metric, and an outgoing interface name or IP address:

```
user@Chardonnay> show ospf route
Prefix               Path   Route       NH   Metric  NextHop       Nexthop
Type   Type        Type         Interface     addr/label
10.0.1.21/32         Intra  Router      IP   1       so-0/0/0.0
10.0.1.102/32        Intra  Router      IP   1       so-0/0/1.0
10.0.1.103/32        Intra  Router      IP   1       at-0/1/0.100
10.0.1.104/32        Intra  Router      IP   2       at-0/1/0.100
                 so-0/0/1.0
10.0.1.105/32        Intra  AS BR       IP   2       so-0/0/1.0
10.0.1.106/32        Intra  Router      IP   3       at-0/1/0.100
                 so-0/0/1.0
```

*show route protocol ospf*

The `show route protocol ospf` command displays routes after they have been placed in the routing table. As such, each route is displayed in a similar format to routes from other protocols. Additionally, each route may not be placed in the forwarding table due to the JUNOS software protocol preference values.

The Chardonnay router has OSPF routes in the routing table that are not marked as active. The 10.0.1.0/30 route is a good example. Most likely, Chardonnay also has a Direct route to this same subnet and prefers that version due to its preference value of 0.

```
user@Chardonnay> show route protocol ospf
inet.0: 34 destinations, 40 routes (34 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.1.0/30         [OSPF/10] 03:02:40, metric 1
> via so-0/0/3.0
10.0.1.4/30         [OSPF/10] 03:02:40, metric 1
> via so-0/0/2.0
```
### Summary

In this chapter, we reviewed the mechanisms behind a link-state routing protocol. We then explored how OSPF applies these principles by first establishing adjacencies and then flooding network information. We saw how OSPF stores the information in the link-state database and uses the Dijkstra SPF Algorithm to determine the best path to an end destination.

We discussed the various OSPF packet types and how each packet plays a role in forming an adjacency. We then discussed the different types of LSAs used by OSPF. Our discussion focused on a sample network that grew from a single area into multiple areas. Our network grew to connect to external networks, leading to an examination of the various OSPF area types.

Finally, we saw how to configure OSPF on a Juniper Networks router and reviewed several commands that the JUNOS software makes available for the monitoring and troubleshooting of an OSPF network.

<table>
<thead>
<tr>
<th>Address</th>
<th>[OSPF/10] 03:02:40, metric 1</th>
<th>via so-0/0/0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.8/30</td>
<td>[OSPF/10] 03:02:40, metric 1</td>
<td>via so-0/0/0.0</td>
</tr>
<tr>
<td>10.0.1.21/32</td>
<td>*[OSPF/10] 02:25:42, metric 1</td>
<td>via so-0/0/0.0</td>
</tr>
<tr>
<td>10.0.1.32/30</td>
<td>[OSPF/10] 03:02:40, metric 1</td>
<td>via so-0/0/1.0</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>*[OSPF/150] 03:02:40, metric 0, tag 0</td>
<td>via so-0/0/1.0</td>
</tr>
<tr>
<td>192.168.2.0/24</td>
<td>*[OSPF/150] 03:02:40, metric 0, tag 0</td>
<td>via so-0/0/1.0</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>*[OSPF/150] 03:02:40, metric 0, tag 0</td>
<td>via so-0/0/1.0</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>*[OSPF/150] 03:02:40, metric 0, tag 0</td>
<td>via so-0/0/1.0</td>
</tr>
<tr>
<td>224.0.0.5/32</td>
<td>*[OSPF/10] 5d 17:20:57, metric 1</td>
<td></td>
</tr>
</tbody>
</table>

A detailed explanation of this output is discussed in Chapter 3, “Protocol-Independent Routing.” This chapter also includes an explanation of the JUNOS software preference values.
Exam Essentials

Be able to describe the OSPF packet types. OSPF has five different packet types: hello, Database Description, link-state request, link-state update, and link-state acknowledgment.

Define the functions of the various OSPF area types. An OSPF stub area prevents the flooding of Type 4 and Type 5 LSAs. A totally stubby area restricts the flooding of Type 3 LSAs by the ABR. An otherwise stub area may have external routes injected by an ASBR if configured to be a not-so-stubby area. These routes are carried in a Type 7 LSA.

Identify the different types of OSPF routers. The four basic types of OSPF routers include an internal router, a backbone router, an area border router, and an Autonomous System boundary router.

Describe the steps for forming an OSPF adjacency and the possible adjacency states. Two OSPF routers become adjacent when they exchange hello and Database Description packets, at a minimum. The adjacency process follows a specified set of steps that result in various adjacency states. Those states include Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, and Full.

Identify the election criteria for an OSPF DR. The two criteria used to elect a designated router are the router priority and the router ID.

Be able to describe the different link-state advertisements. The JUNOS software utilizes six different LSA types: router, network, network summary, ASBR summary, AS external, and NSSA external LSAs.
Key Terms

Before you take the exam, be certain you are familiar with the following terms:

- 2-Way
- area
- area border router (ABR)
- AS external LSA
- ASBR summary LSA
- Attempt
- Autonomous System boundary router (ASBR)
- backbone area
- backbone router
- backup designated router (BDR)
- Database Description (DD) packet
- dead interval
- designated router (DR)
- Dijkstra Algorithm
- Down
- Exchange
- ExStart
- Full
- hello interval
- Init
- internal router
- link-state acknowledgment
- Link State Advertisement
- link-state database
- link-state request list
- link-state request packet
- link-state update
- Loading
- neighbors
- network LSA
- network summary LSA
- not-so-stubby area (NSSA)
- NSSA external LSA
- OSPF hello packet
- router ID
- router LSA
- router priority
- stub area
- totally stubby area
- virtual circuit identifier (VCI)
Review Questions

1. How does an OSPF router confirm that its neighbor has received a link-state update?
   A. It relies on the underlying TCP protocol to acknowledge receipt.
   B. It receives a link-state update with an incremented sequence number.
   C. It receives a link-state update with the same sequence number it sent.
   D. It receives a link-state acknowledgment packet containing header information for the LSAs that it sent.

2. Which OSPF packet is used to summarize the link-state database during adjacency formation?
   A. Link-state advertisement
   B. Database Description
   C. Link-state request
   D. Link-state update

3. Should an OSPF link fail, which packet would advertise the network change?
   A. Link-state advertisement
   B. Database Description
   C. Link-state request
   D. Link-state update

4. Which of the following is not a reason to deploy areas in your OSPF network?
   A. To scale the size of the network
   B. To reduce the number of DRs
   C. To minimize processor utilization
   D. To minimize database size

5. A stub area eliminates which type of LSA?
   A. Type 1
   B. Type 2
   C. Type 3
   D. Type 4

6. A not-so-stubby area is used if you want to allow what kind of LSA?
   A. NSSA external
   B. Summary
   C. AS external
   D. Router
7. Which of the following routers serves as a gateway to external networks?
   A. ABR
   B. ASBR
   C. DR
   D. BDR

8. Which router will convert Type 7 LSAs into Type 5 LSAs?
   A. ABR
   B. ASBR
   C. DR
   D. BDR

9. If a router has one interface in the backbone area and four interfaces in non-backbone areas, what kind of router is it?
   A. ABR
   B. ASBR
   C. DR
   D. BDR

10. Two routers forming an adjacency have just finished exchanging DD packets. What happens next?
    A. They exchange hello packets to agree on authentication.
    B. They exchange LSAs when their network changes.
    C. They send link-state requests to get additional database information.
    D. They transition to an ExStart adjacency.

11. What state is a router in after it receives a hello packet with no known neighbors listed?
    A. Init
    B. Start
    C. Down
    D. 2-Way

12. When sending its DD packet, the local router sets the MS bit to 1. What does this mean?
    A. The router is claiming to be the DR.
    B. The router is trying to control the database exchange.
    C. The router has additional information to send.
    D. The router has no more information to send.
13. Four OSPF routers come online at the same time. Based on the properties shown, which router would be elected DR?
   A. Priority = 50, router ID = 10.0.1.10
   B. Priority = 50, router ID = 10.0.100.100
   C. Priority = 25, router ID = 10.0.1.100
   D. Priority = 100, router ID = 1.0.1.10

14. Assume that the current DR has a router priority of 100. When will it lose control of the DR responsibility?
   A. When a router with a higher priority joins the network
   B. When a router with a higher router ID joins the network
   C. When a router with a higher interface address joins the network
   D. When it stops sending hello packets

15. What is the default router priority in the JUNOS software?
   A. 0
   B. 32
   C. 64
   D. 128

16. Which router originates a Type 2 LSA?
   A. DR
   B. BDR
   C. ABR
   D. ASBR

17. Which router plays backup to the node in control of a broadcast network?
   A. DR
   B. BDR
   C. ABR
   D. ASBR

18. You want to know which routers in your network are injecting external routes. Which command would be helpful?
   A. show ospf neighbor
   B. show ospf gateway
   C. show ospf database
   D. show ospf statistics
19. Which command allows you to verify that your interfaces are configured for the correct OSPF areas?
   A. show ospf neighbor
   B. show ospf database
   C. show ospf interface
   D. show ospf statistics

20. Which OSPF command provides information about connected routers?
   A. show ospf neighbor
   B. show ospf adjacency
   C. show ospf interface
   D. show ospf statistics
Answers to Review Questions

1. D. OSPF handles its own acknowledgments via the link-state acknowledgment packet. The packet contains the LSA headers that describe the LSAs that are being acknowledged.

2. B. The Database Description packet is used during adjacency formation to summarize the OSPF database. Based on the summarized database, the receiving router will request additional information via request packets. Detailed information will be provided via an update packet, which is acknowledged by an acknowledgment packet.

3. D. When a network experiences a change, a link-state update packet is used to advertise the new status in the network.

4. B. A DR is used on broadcast networks and serves as the primary point of contact to minimize point-to-point peering and bandwidth utilization. Establishing an OSPF area will not affect whether a DR is needed.

5. D. A stub area is used to eliminate the existence of AS external Type 5 LSAs. When Type 5 LSAs are not allowed in a stub area, then the Type 4 LSAs that describe the location of the ASBR are not needed either.

6. A. A not-so-stubby area is used when you want to allow external routes into a stub area. The definition of a stub area eliminates Type 5 LSAs. Since Type 3 and Type 1 LSAs already exist in a stub area, you are trying to allow NSSA external LSAs, or Type 7 LSAs.

7. B. An ASBR injects AS external LSAs into the OSPF domain. These LSAs contain non-OSPF network information.

8. A. The ABR to a not-so-stubby area will convert Type 7 LSAs to Type 5 LSAs by default. This is necessary since Type 7 LSAs can exist only in an NSSA.

9. A. A router with at least one interface in the backbone and any number of interfaces in non-backbone areas is an area border router.

10. C. When routers forming an adjacency finish exchanging DD packets, they start sending request packets, if needed, to acquire additional database information for unknown or out-of-date LSAs.

11. A. When a router receives a hello packet with no known neighbors, it is a sign that a new neighbor is looking for OSPF-speaking devices. This is the first communication that the local router is receiving from the new neighbor, so the local router will transition to the Init state.

12. B. When a router sets the MS bit to 1, it is attempting to control the exchange of DD packets.

13. D. Even though this router has the lowest router ID, router priority is the first tiebreaker in DR election. This router’s priority is the highest of all shown.

14. D. In OSPF, DR ownership is nonpreemptive. This means that the only time a DR will lose control of its responsibilities is when it ceases to function properly.

15. D. The JUNOS software default router priority setting is 128.
16. A. Only a designated router can originate the Type 2 LSA for a broadcast or NBMA network.

17. B. The backup designated router is responsible for monitoring the network segment and the DR. In the event of a DR failure, the BDR is to take over as DR.

18. C. By viewing the OSPF database, you can look for AS external summary LSAs. These will list the routers that are injecting non-OSPF routes into your network.

19. C. Answer C will show you directly which area each interface is configured for. While the other options may give you clues that the interface is not properly configured, they will not tell you which area each interface is configured for.

20. A. Only answer A will provide you with information regarding neighboring OSPF routers. Answer B is not a valid command, while answers C and D detail information about the local router.