Chapter 8: Troubleshooting OSPFv2

Instructor Materials

CCNP Enterprise: Advanced Routing

Chapter 8 Content

This chapter covers the following content:

- **Troubleshooting OSPFv2 Neighbor Adjacencies -** This section covers the reasons OSPFv2 neighbor adjacencies sometimes do not form and how to identify them.
- **Troubleshooting OSPFv2 Routes -** This section covers the reasons OSPFv2 routes might be missing from the link-state database (LSDB) and routing table and how to determine why they are missing.
- **Troubleshooting Miscellaneous OSPFv2 Issues -** This section focuses on tracking link-state advertisements (LSAs) through the network, route summarization, discontiguous areas, load balancing, and default routes.
- **OSPFv2 Trouble Tickets -** This section presents three trouble tickets that demonstrate how to use a structured troubleshooting process to solve a reported problem.

Troubleshooting OSPFv2 Neighbor Adjacencies

- This section focuses on the reasons an OSPF neighbor relationship might not form and how to identify them during the troubleshooting process.

OSPF Establishes Neighbor Relationships

OSPF establishes neighbor relationships by sending hello packets out interfaces participating in the OSPF process. You can enable the OSPF process on an interface and place it in an OSPF area using two methods:

1. Router OSPF configuration mode.

   R1(config)# **router ospf 1**
   R1(config-router)# **network 10.1.1.0 0.0.0.255 area 0**

2. Interface configuration mode.

   R1(config)# **interface g0/0**
   R1(config-if)# **ip ospf 1 area 51**

Show IP OSPF Neighbor

To verify OSPFv2 neighbors, you use the **show ip ospf neighbor** command.

Example 8-1 shows sample output of the show ip ospf neighbor command. It lists:

- **Neighbor ID** – The router ID (RID) of the neighbor
- **Priority** – The priority of the neighbor for the router election process
- **State** – Whether the neighbor is a DR, BDR, or DROTHER.
- **Dead Time** - How long the router waits until it declares the neighbor down if it does not hear another hello packet within that time (The default is 40 seconds on a LAN).
- **Address** - The neighbor's interface IP address from which the hello packet was sent
- **Interface** - The local router interface used to reach that neighbor

Example 8-1 *Verifying OSPF Neighbors with show ip ospf neighbor*

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.23.2        1    FULL/BDR        00:00:37    10.1.12.2       GigabitEthernet1/0
```

Troubleshooting OSPFv2 Neighbor Relationships

The following are some of the reasons an OSPFv2 neighbor relationship might not form:

- **Interface is down -** The interface must be up/up.
- **Interface not running the OSPF process -** If the interface is not enabled for OSPF, it does not send hello packets or form adjacencies.
- **Mismatched timers -** Hello and dead timers must match between neighbors.
- **Mismatched area numbers -** The two ends of a link must be in the same OSPF area.
- **Mismatched area type -** In addition to a normal OSPF area type, an area type could be a stub area or a not-so-stubby area (NSSA). The routers must agree on the type of area they are in.
- **Different subnets -** Neighbors must be in the same subnet.

Troubleshooting OSPFv2 Neighbor Relationships (Cont.)

- **Passive interface -** The passive interface feature suppresses the sending and receiving of hello packets while still allowing the interface's network to be advertised.
- **Mismatched authentication information -** Both OSPF interfaces must be configured for matching authentication
- **ACLs -** An ACL may be denying packets to the OSPF multicast address 224.0.0.5.
- **MTU mismatch -** The maximum transmission unit of neighboring interfaces must match.
- **Duplicate router IDs -** Router IDs must be unique.
- **Mismatched network types -** neighbors configured with a different OSPF network type might not form an adjacency.

Troubleshooting OSPFv2

Adjacency States

Adjacencies are not established upon the immediate receipt of hello messages. Rather, an adjacency transitions through the various states.

See Table 8-2 for adjacency states.

Table 8-2 Adjacency States

State	Description
Down	This state indicates that no hellos have been received from a neighbor.
Attempt	This state occurs after a router sends a unicast hello (as opposed to a multicast hello) to a configured neighbor and has not yet received a hello from that neighbor.
Init	This state occurs on a router that has received a hello message from its neighbor; however, the OSPF RID of the receiving router was not contained in the hello message. If a router remains in this state for a long period, something is probably preventing that router from correctly receiving hello packets from the neighboring router.
2-Way	This state occurs when two OSPF routers have received hello messages from each other, and each router saw its own OSPF RID in the hello message it received. The 2-Way state is an acceptable state to stay in between DROTHERs on an Ethernet LAN.
ExStart	This state occurs when the routers forming a full neighbor adjacency decide who will send their routing information first. This is accomplished using the RID. The router with the higher RID becomes the master, and the other one becomes the slave. The master sends the routing information first. In a multi-access network, the DR and BDR have to be determined before this state starts. However, the DR does not have to be the master because each master/slave election is on a per-neighbor basis. If a router remains in this state for a long period, a maximum transmission unit (MTU) mismatch could exist between the neighboring routers, or a duplicate OSPF RID might exist.
Exchange	This state occurs when the two routers forming an adjacency send one another database descriptor (DBD) packets containing information about a router's link-state database. Each router compares the DBD packets received from the other router to identify missing entries in its own database. If a router remains in this state for a long period, an MTU mismatch could exist between the neighboring routers.
Loading	Based on the missing link-state database entries identified in the Exchange state, the Loading state occurs when each neighboring router requests the other router to send those missing entries. If a router remains in this state for a long period, a packet might have been corrupted, or a router might have a memory issue. Alternatively, it is possible that such a condition could result from the neighboring routers having an MTU mismatch.
Full	This state indicates that the neighboring OSPF routers have successfully exchanged their link-state information with one another, and an adjacency has been formed.

OSPF Basic Configuration Errors

When an OSPF neighbor relationship does not form you need the assistance of an accurate physical and logical network diagram and the **show cdp neighbors** command to verify who should be the neighbors.

When troubleshooting OSPF adjacencies, you need to verify router OSPF configurations and status with various show commands like **show ip interface brief** and **show ip protocols**

- Router interfaces must be up/up if you plan on forming an OSPF neighbor adjacency.
- OSPF **passive-interface *interface*** command targeting the wrong interface will prevent hello packets from being sent and neighbor adjacency from forming.
- Router OSPF **network *ip_address wildcard_mask* area *area_id*** command or **ip ospf *process_id* area *area_id*** interface command configured on the wrong interfaces or in the wrong area IDs can also prevent neighbor relationships from forming.
- If an interface is enabled for OSPF with both the **network *ip_address wildcard_mask* area *area_id*** command and the **ip ospf *process_id* area *area_id*** command, the **ip ospf *process_id* area *area_id*** command takes precedence.

Mismatched Timers

OSPF timers must match for neighbor adjacencies to form (with EIGRP they do not). The hello timer defaults to 10 seconds for broadcast and point-to-point network types and 30 seconds for nonbroadcast and point-to-multipoint network types. The dead timer defaults to 40 seconds for broadcast and point-to-point network types and 120 seconds for nonbroadcast and point-to-multipoint network types.

Verify current timers on an OSPF interface, with the **show ip ospf interface *interface_type* *interface_number*** command

You can use the **debug ip ospf hello** command when troubleshooting adjacencies to reveal mismatched timers, as shown in Example 8-5. In this example, the packet received (R) has a dead timer of 44 and a hello timer of 11. The local device (C) has a dead timer of 40 and a hello timer of 10.

Example 8-5 *Using debug ip ospf hello to Identify Mismatched Timers*

```
R1# debug ip ospf hello
OSPF hello debugging is on
R1#
OSPF-1 HELLO Gi1/0: Rcv hello from 2.2.2.2 area 1 10.1.12.2
OSPF-1 HELLO Gi1/0: Mismatched hello parameters from 10.1.12.2
OSPF-1 HELLO Gi1/0: Dead R 44 C 40, Hello R 11 C 10 Mask R 255.255.255.0 C
255.255.255.0
R1#
```

Mismatched Area Numbers

For OSPF routers to form neighbor adjacencies, their neighboring interfaces must be in the same area. You can verify the area an OSPF interface by using either one of the following show commands:

```
R1# show ip ospf interface interface_type interface_number
R1# show ip ospf interface brief
```

You can use a debug command when troubleshooting adjacencies to find mismatched area numbers:

```
R1# debug ip ospf adj
```

In Example 8-8. In this example, the packet received has an area ID of 1, and the local interface is participating in Area 2.

Example 8-8 *Using debug ip ospf adj to Identify Mismatched Area Numbers*

```
R1# debug ip ospf adj
OSPF adjacency debugging is on
R1#
OSPF-1 ADJ Gi1/0: Rcv pkt from 10.1.12.2, area 0.0.0.2, mismatched area 0.0.0.1 in
the header
R1# u all
All possible debugging has been turned off
```

Mismatched Area Type

For routers within an area to form adjacencies, they must agree on the area type. Within the hello packet, a stub area flag is designed to indicate the type of area the neighbor is in.

You can verify the types of areas connected to a router by using the **show ip protocols** command.

Example 8-9 displays the output of show ip protocols.

If there is a router with multiple areas connected to it, you can verify the areas and their type by using the **show ip ospf** command, as shown in Example 8-9.

In Example 8-10 , the **debug ip ospf hello** command is used to find mismatched area types.

Example 8-9 *Determining the Type of OSPF Areas*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Router ID 10.1.12.1
 Number of areas in this router is 1. 0 normal 1 stub 0 nssa
 Maximum path: 4
 Routing for Networks:
   10.1.1.1 0.0.0.0 area 1
 Routing on Interfaces Configured Explicitly (Area 1):
   GigabitEthernet1/0
 Routing Information Sources:
    Gateway         Distance      Last Update
   10.1.23.2        110           00:04:42
 Distance: (default is 110)

R1# show ip ospf
 Routing Process "ospf 1" with ID 10.1.12.1
 Start time: 02:23:19.824, Time elapsed: 02:08:52.184
 ...output omitted...
 Reference bandwidth unit is 100 mbps
  Area 1
   Number of interfaces in this area is 2
   It is a stub area
   Area has no authentication
   SPF algorithm last executed 00:05:46.800 ago
...output omitted...
```

Example 8-10 *Using debug ip ospf hello to Identify Mismatched Area Types*

```
R1# debug ip ospf hello
OSPF hello debugging is on
R1#
OSPF-1 HELLO Gi1/0: Rcv hello from 2.2.2.2 area 1 10.1.12.2
OSPF-1 HELLO Gi1/0: Hello from 10.1.12.2 with mismatched Stub/Transit area option bit
R1#
```

Subnets and Passive Interfaces

Different Subnets - To form an OSPF neighbor adjacency, the router interfaces must be on the same subnet.

Passive Interface - Ensures that rogue routers will not be able to form adjacencies with a legitimate router on an interface since it is not sending or receiving OSPF packets on that interface. However, if you configure the wrong interface as passive, a legitimate OSPF neighbor relationship is not formed.

Example 8-11 *Verifying That Neighboring Interfaces Are on the Same Subnet*

```
R1# show running-config interface gigabitEthernet 1/0
Building configuration...

Current configuration : 108 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 ip ospf 1 area 1
 negotiation auto
end

R2# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 ip address 10.1.12.2 255.255.255.0
 negotiation auto
end
```

Example 8-12 *Verifying Passive Interfaces with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Router ID 10.1.12.1
 Number of areas in this router is 1. 0 normal 1 stub 0 nssa
 Maximum path: 4
 Routing for Networks:
   10.1.1.1 0.0.0.0 area 1
 Routing on Interfaces Configured Explicitly (Area 1):
   GigabitEthernet1/0
 Passive Interface(s):
   GigabitEthernet0/0
 Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.23.2       110           00:00:03
 Distance: (default is 110)
```

Mismatched Authentication Information

Both routers must agree on the settings for a neighbor relationship to form. To verify whether authentication has been enabled for the entire area on a router, you use the **show ip ospf** command.

To verify the key ID being used on an interface-by-interface basis use the **show ip ospf interface *interface_type interface_number*** command.

In addition, you must verify the case-sensitive key string that is being used by using the **show running-config** command.

If you configure authentication on an interface-by-interface basis you need to check the output of **show ip ospf interface** command.

You can use the **debug ip ospf adj** command to find mismatched authentication information.

Example 8-13 *Verifying OSPF Area Authentication*

```
R1# show ip ospf
Routing Process "ospf 1" with ID 10.1.12.1
 Start time: 02:23:19.824, Time elapsed: 02:46:34.488
...output omitted...
 Reference bandwidth unit is 100 mbps
  Area 1
    Number of interfaces in this area is 2
    It is a stub area
    Area has message digest authentication
    SPF algorithm last executed 00:25:12.220 ago
...output omitted...
```

Example 8-15 *Using debug ip ospf adj to Identify Mismatched Authentication Information*

```
R1# debug ip ospf adj
OSPF adjacency debugging is on
R1#
OSPF-1 ADJ Gi1/0: Rcv pkt from 10.1.12.2 : Mismatched Authentication type. Input
packet specified type 0, we use type 1
R1#
```

ACL and MTU Mismatch

ACL (Access List) - If an ACL is applied to an interface, and the ACL is not permitting OSPF packets, a neighbor relationship does not form. Notice that ACL 100 is applied inbound on interface GigabitEthernet1/0. Note that outbound ACLs do not affect OSPF packets. Therefore, if there is an outbound ACL configured on an interface and a neighbor adjacency is not forming, the ACL is not the problem because the outbound ACL does not apply to OSPF packets generated on the local router.

MTU Mismatch - For OSPF routers to become neighbors and achieve full adjacency, the interface of each router forming the adjacency must have the same MTU. If they don't, the routers can see each other but get stuck in the ExStart/Exchange states. In Example 8-18, the output of show ip ospf neighbor indicates that R1 is stuck in the Exchange state, and that R2 is stuck in the ExStart state. To solve this issue, you can manually modify the MTU values of the interfaces so that they match, or you can use the **ip ospf mtu-ignore** interface configuration command, which stops OSPF from comparing the MTU when trying to form an adjacency.

Example 8-18 *Symptoms of an MTU Mismatch (Stuck in ExStart/Exchange)*

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.23.2         1   EXCHANGE/DR     00:00:38    10.1.12.2       GigabitEthernet1/0

R2# show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface


10.1.12.1         1   EXSTART/BDR     00:00:37    10.1.12.1       GigabitEthernet0/0
```

Troubleshooting OSPFv2

Duplicate Router ID

OSPF neighbor relationships do not form between routers if they have the same RID. When a duplicate RID exists, you receive a syslog message similar to the following:

%OSPF-4-DUP_RTRID_NBR: OSPF detected duplicate router-id 10.1.23.2 from 10.1.12.2 on interface GigabitEthernet1/0

If you manually change the RID with the **router-id *ip_address*** command in router OSPF configuration mode, you must reset the OSPF process by using the **clear ip ospf process** command in order for it to take effect.

Example 8-21 *Verifying an OSPF RID*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Router ID 10.1.23.2
 Number of areas in this router is 1. 0 normal 1 stub 0 nssa
 Maximum path: 4
 Routing for Networks:
   10.1.1.1 0.0.0.0 area 1
 Routing on Interfaces Configured Explicitly (Area 1):
   GigabitEthernet1/0
 Passive Interface(s):
   Ethernet0/0
   GigabitEthernet0/0
 Routing Information Sources:
    Gateway          Distance       Last Update
    10.1.23.2        110            00:05:31
 Distance: (default is 110)
```

Mismatched Network Types

OSPF supports multiple network types. Different network types have different default values. Therefore, if two OSPF routers that are trying to form a neighbor adjacency are configured with noncompatible network types, a neighbor relationship does not form.

For example, if the network type is Broadcast on R1's interface and NBMA on R2's interface, the timers do not match, and the adjacency does not form. Table 8-3 lists the OSPF network types and their characteristics.

To determine the network type associated with an OSPF-enabled interface, you can issue the command **show ip ospf interface *interface_type* *interface_number***.

Table 8-3 OSPF Network Types and Characteristics

Type	Default	Neighbors	DR/BDR	Timers
Broadcast	Default on LAN interfaces	Discovered automatically	DR and BDR elected automatically	Hello: 10 Dead: 40
NBMA (nonbroadcast)	Default on Frame Relay main and point-to-multipoint interfaces	Statically configured	DR must be manually configured on the hub router	Hello: 30 Dead: 120
Point-to-point	Default on point-to-point serial and point-to-point Frame Relay subinterfaces	Discovered automatically	No DR or BDR	Hello: 10 Dead: 40
Point-to-multipoint	(Not a default) Optimal for hub-and-spoke topologies (Frame Relay)	Discovered automatically	No DR or BDR	Hello: 30 Dead: 120
Point-to-multipoint nonbroadcast	(Not a default) Optimal for hub-and-spoke topologies (Frame Relay) that do not support broadcast or multicast traffic	Statically Configured	No DR or BDR	Hello: 30 Dead: 120

Troubleshooting OSPFv2 Routes

- This section examines the reasons OSPF routes might be missing and how to determine the reason a route is missing.

Common Reasons for Missing OSPFv2 Routes

OSPF routers receive LSAs from every router within the same area. Every router in an area must have exactly the same link-state database (LSDB) for that area. If you have no neighbors, you will not learn any routes.

Following is a list of common reasons OSPF routes might be missing either from the LSDB or the routing table:

- **Interface not running the OSPF process -** If the interface is not participating in the OSPF process, the network the interface is part of is not injected into the OSPF process and is therefore not advertised to neighbors.
- **Better source of information -** If exactly the same network is learned from a more reliable source, it is used instead of the OSPF-learned information.
- **Route filtering -** A filter might be preventing a route from being installed in the routing table.
- **Stub area configuration -** If the wrong type of stub area is chosen, you might be receiving a default route instead of the actual route.
- **Interface is shut down -** The OSPF-enabled interface must be up/up for the network associated with the interface to be advertised.
- **Wrong designated router elected -** In a hub-and-spoke environment, if the wrong router is the DR, routes are not exchanged properly.
- **Duplicate RIDs -** If there are two or more routers with the same RID, routes are missing in the topology.

Route Filtering

A distribute list applied to an OSPF process controls which routes are installed into the routing table from the LSDB. Note that this differs from EIGRP, where the distribute list controls routes sent and received between neighbors. The reason this difference exists is that all OSPF routers in an area must have the same LSDB.
To apply a route filter to OSPF, the distribute list is applied in OSPF configuration mode inbound (meaning into the routing table), and the routes installed are controlled by ACLs, prefix lists, or route maps.

When troubleshooting route filtering for OSPF, consider the following:

- Is the distribute list applied in the correct direction?
- If the distribute list is using an ACL, is the ACL correct?
- If the distribute list is using a prefix list, is the prefix list correct?
- If the distribute list is using a route map, is the route map correct?
- The **show ip protocols** command identifies whether a distribute list is applied to the OSPF process.

Example 8-29 *Verifying Route Filters with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is (prefix-list) TEST
```

Troubleshooting OSPFv2 Routes
Route Filtering (Cont.)

To verify the entries in the prefix list, you issue the **show ip prefix-list TEST** command, as shown in Example 8-30. If an ACL is applied, you issue the **show access-list** command. If a route map is applied, you issue the **show route-map** command. As shown in Example 8-30, you can verify the command that was used to apply the distribute list in the running configuration.

Notice in Example 8-31 that the LSDB still has the 10.1.23.0/24 network listed, but it is not installed in the routing table because of the distribute list that is denying 10.1.23.0/24 from being installed.

Example 8-30 *Verifying the OSPF Distribute List and Prefix List*

```
R1# show ip prefix-list TEST
ip prefix-list TEST: 2 entries
 seq 5 deny 10.1.23.0/24
 seq 10 permit 0.0.0.0/0 le 32

R1# show run | section router ospf 1
router ospf 1
 area 1 authentication message-digest
 passive-interface default
 no passive-interface GigabitEthernet1/0
 network 10.1.1.1 0.0.0.0 area 1
 distribute-list prefix TEST in
```

Example 8-31 *Verifying OSPF Routes and LSDB After a Distribute List Is Applied*

```
R1# show ip ospf database

            OSPF Router with ID (10.1.12.1) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.12.1       10.1.12.1       16          0x80000011 0x005B49 2
10.1.23.2       10.1.23.2       13          0x80000033 0x00DBA9 1

                Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.12.2       10.1.23.2       12          0x8000000D 0x00A70D

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.3.0        10.1.23.2       16          0x80000002 0x00DB2C
10.1.23.0       10.1.23.2       16          0x80000002 0x00F4FF
203.0.113.0     10.1.23.2       16          0x80000002 0x005286

                Summary ASB Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.23.3       10.1.23.2       18          0x80000001 0x00CA27

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         10.1.23.3       779         0x80000005 0x00AF9B 1
R1# show ip route
...output omitted...

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.1.12.2, 00:00:02, GigabitEthernet1/0
 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0
O IA 10.1.3.0/24 [110/3] via 10.1.12.2, 00:00:02, GigabitEthernet1/0
C 10.1.12.0/24 is directly connected, GigabitEthernet1/0
L 10.1.12.1/32 is directly connected, GigabitEthernet1/0
O IA 203.0.113.0/24 [110/3] via 10.1.12.2, 00:00:02, GigabitEthernet1/0
```

Stub Area Configuration

Stub areas or NSSAs, suppress Type 5 External LSAs from entering an area at the ABR. Totally stubby areas and totally NSSAs, suppress Type 5 External and Type 3 Summary LSAs from entering an area at the ABR. The routes that would have been learned from the Type 5 and Type 3 LSAs are now replaced by a default route.

With only a default route, the router loses visibility of the overall network, which could produce suboptimal routing in redundant environments.

If you are expecting a Type 5 or Type 3 LSA for a specific route, but it is not showing up in the area, you should verify whether the area is a stub area or an NSSA and determine what types of routes are being suppressed. You can verify whether the area connected to the router is a stub area or an NSSA by using the **show ip ospf** command, as shown in Example 8-32.

Example 8-32 *Determining the Type of OSPF Areas*

```
R1# show ip ospf
 Routing Process "ospf 1" with ID 10.1.12.1
 Start time: 02:23:19.824, Time elapsed: 02:08:52.184
 ...output omitted...
 Reference bandwidth unit is 100 mbps
  Area 1
   Number of interfaces in this area is 2
   It is a stub area
   Area has no authentication
   SPF algorithm last executed 00:05:46.800 ago
...output omitted...
```

Stub Area Configuration (Cont.)

With totally stubby areas or totally NSSAs you configure the **no-summary** keyword on the ABR. It is not needed on the other routers. Therefore, it is best to review the output of **show ip ospf** on the ABR.

In Example 8-33, R2 is configured to suppress Type 3 and Type 5 LSAs from entering Area 1 and replacing them with a default route. So even though R1 appears to be in a stub area, it is really in a totally stubby area, based on the configuration of R2.

Example 8-33 *Determining the Type of OSPF Area on the ABR*

```
R2# show ip ospf
Routing Process "ospf 1" with ID 10.1.23.2
 Start time: 02:39:09.376, Time elapsed: 15:19:40.352
...output omitted...
 Flood list length 0
  Area 1
   Number of interfaces in this area is 1
   It is a stub area, no summary LSA in this area
   Generates stub default route with cost 1
   Area has no authentication
...output omitted...
```

Wrong DR Elected

In a subnet with multiple routers it does not matter which router is elected as the DR (multi-access Ethernet topology or a full-mesh Frame Relay topology) because every router is able to reach the DR.

It does matter who the DR is over a hub-and-spoke nonbroadcast multi-access (NBMA) network such as Frame Relay or with a Dynamic Multipoint VPN (DMVPN), because the underlying Layer 2 topology does not line up with the Layer 3 addressing.

Figure 8-3 shows a hub-and-spoke Frame Relay or DMVPN network.

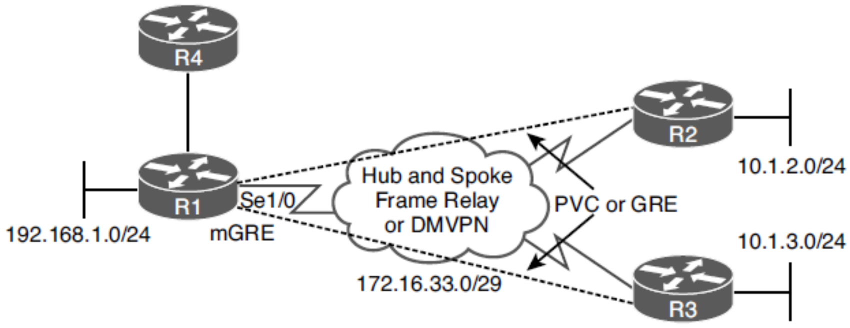

Figure 8-3 *Hub-and-Spoke Topology*

Wrong DR Elected (Cont.)

Figure 8-4 shows the wrong DR placement.

The DR router needs to be reachable through a single hop because of how OSPF neighbor relationships are formed and how routers communicate with the DR. Hellos are established with the multicast address 224.0.0.5, and the DR is reachable at the multicast address 224.0.0.6. Packets destined to these two multicast addresses are not relayed by other routers.

Because the DR is responsible for relaying learned routes in a multi-access network, it needs to be centrally located. In this case, you need to control who the DR is. It must be R1 to ensure that all routers are able to send LSAs to it and receive LSAs from it, as shown in Figure 8-5.

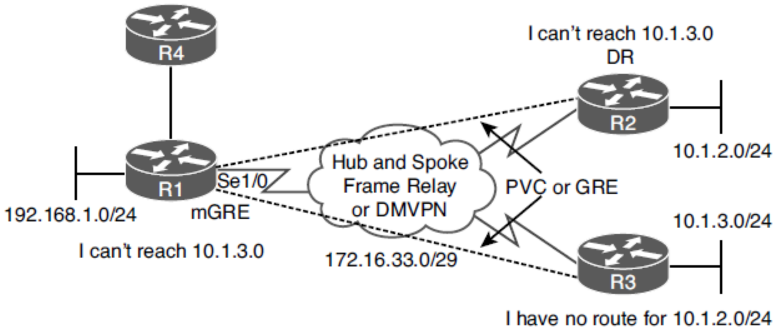

Figure 8-4 *Wrong DR Placement*

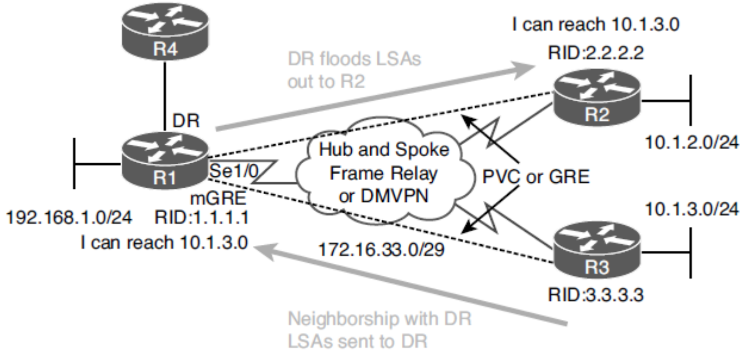

Figure 8-5 *Correct DR Placement*

Duplicate Router IDs

The OSPF router ID (RID) is used in forming neighbor relationships and to determine which router is advertising a specific LSA, it is imperative that the RIDs are unique in the domain.

If there are duplicate RIDs, the network issues can vary. Having duplicate RIDs in different areas would cause the physical OSPF topology to be different from the way the SPF algorithm sees it. This can cause routing issues because some routes may not be passed between areas, causing the LSDB and the routing tables to be incomplete.

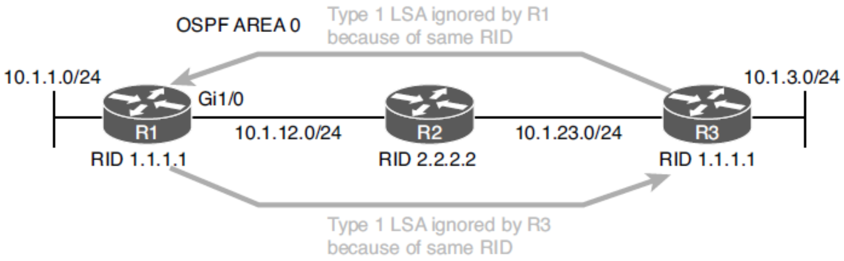

Figure 8-6 *Duplicate RIDs in the Same Area*

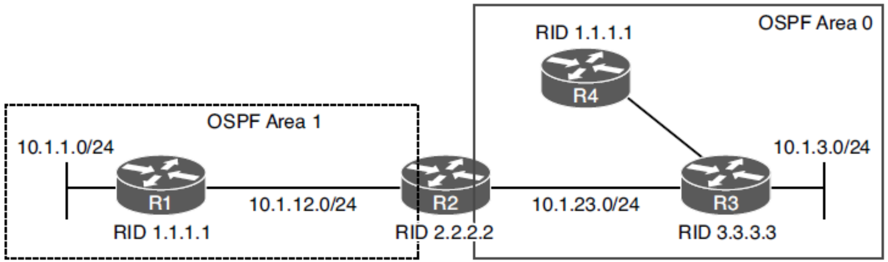

Figure 8-7 *Duplicate RIDs in Different Areas*

Troubleshooting Miscellaneous OSPFv2 Issues

- This section looks at tracking LSAs through the network, route summarization, discontiguous areas, load balancing, and default routes.

Tracking OSPF Advertisements Through a Network

The following steps describe how network 192.168.1.0/24, connected to R1, is learned by the LSDBs of routers R2, R3, R4, and R5:

Step 1. Router R1 creates a Type 1 LSA for the 192.168.1.0/24 network and floods it into Area 1

Step 2. Router R2 receives the router LSA for 192.168.1.0/24 and places it in the Area 1 LSDB. R2 runs the SPF algorithm to determine the best path to reach the 192.168.1.0/24 network. The best result is placed in R2's routing table (RIB).

Step 3. Router R2 informs Area 0 routers about network 192.168.1.0/24 by injecting a Type 3 LSA about the network into the LSDB of Area 0 and flooding it into Area 0. This LSA includes the cost to reach the 192.168.1.0/24 network, from the perspective of router R2.

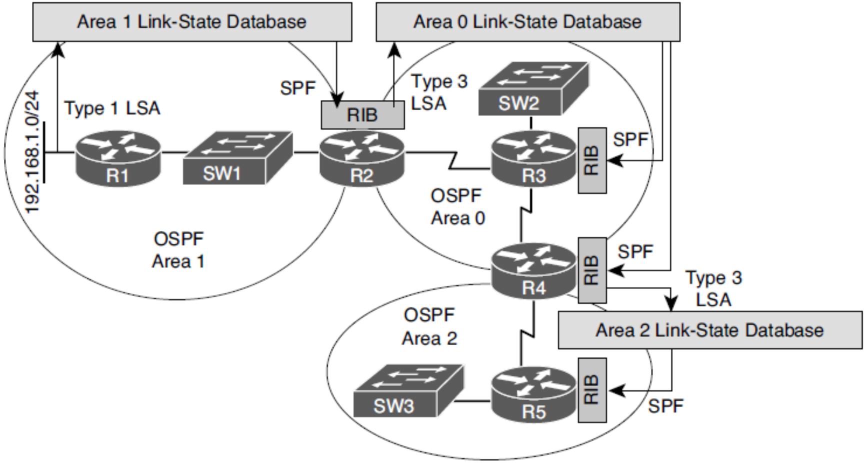

Figure 8-8 *Tracking an OSPF Advertisement*

Tracking OSPF Advertisements Through a Network (Cont.)

Step 4. Each of the other Area 0 routers, R3 and R4, receives the Type 3 LSA and adds it to its Area 0 LSDB. These routers run the SPF algorithm to determine the cost to reach R2. This cost is then added to the cost R2 advertised in its Type 3 LSA, and the result is stored in the RIBs

Step 5. Router R4 informs Area 2 routers about network 192.168.1.0/24 by injecting a Type 3 LSA about the network into the LSDB of Area 2 and flooding it into Area 2. This LSA includes the cost to reach the 192.168.1.0/24 network, from the perspective of R4.

Step 6. Each of the routers in Area 2 receives the Type 3 LSA and adds it to its Area 2 LSDB. These routers run the SPF algorithm to determine the cost to reach R4. This cost is then added to the cost router R4 advertised in its Type 3 LSA, and the result is stored in the RIB of the routers.

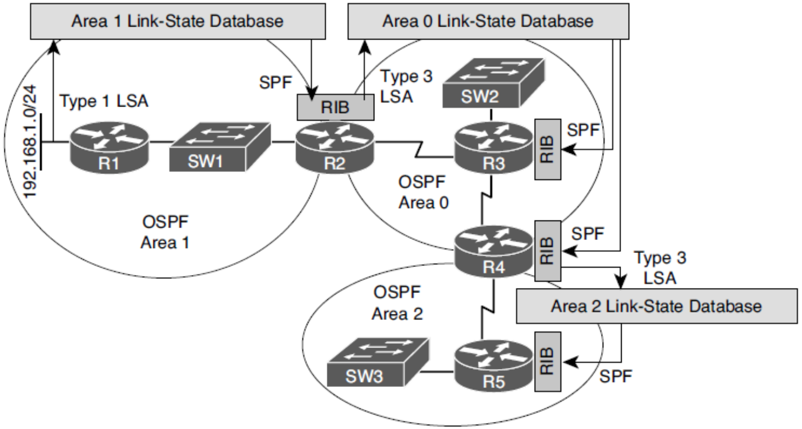

Figure 8-8 *Tracking an OSPF Advertisement*

Types of OSPFv2 LSAs

To successfully troubleshoot OSPF-related issues, you should have a solid understanding of how OSPF routers discover networks and the different types of OSPF LSAs.

Table 8-4 lists the LSA types you commonly encounter when troubleshooting a Cisco-based OSPF network.

Table 8-4 OSPF LSAs

LSA Type	Description
1	All OSPF routers source Type 1 LSAs. These advertisements list information about directly connected subnets, the OSPF connection types of a router, and the known OSPF adjacencies of a router. A Type 1 LSA is not sent out its local area.
2	The designated router on a multi-access network sends a Type 2 LSA for that network if the network contains at least two routers. A Type 2 LSA contains a list of routers connected to the multi-access network and, like a Type 1 LSA, is constrained to its local area.
3	A Type 3 LSA is sourced by an ABR. Each Type 3 LSA sent into an area contains information about a network reachable in a different area. Note that network information is exchanged only between the backbone area and a nonbackbone area, as opposed to being exchanged between two nonbackbone areas.
4	Much like a Type 3 LSA, a Type 4 LSA is sourced by an ABR. However, instead of containing information about OSPF networks, a Type 4 LSA contains information stating how to reach an autonomous system boundary router (ASBR).
5	A Type 5 LSA is sourced by an ASBR and contains information about networks reachable outside the OSPF domain. A Type 5 LSA is sent to all OSPF areas except for stub areas. Note that the ABR for a stub area sends default route information into the stub area rather than sending the network-specific Type 5 LSAs.
7	A Type 7 LSA is sourced from an ASBR within an NSSA. Whereas a stub area cannot connect to an external autonomous system, an NSSA can. The Type 7 LSA exists only in the NSSA; therefore, the external routes are announced by the ABR(s) of the NSSA into Area 0 using Type 5 LSAs. In addition, as with a stub area, external routes known to another OSPF area are not forwarded into an NSSA since Type 5 LSAs are not permitted in an NSSA.

Route Summarization

With OSPF, manual route summarization is enabled on an area-by-area basis on an ABR and on an ASBR to summarize external routes being injected into an area.

When troubleshooting route summarization, you need to keep in mind the following:

- Did you enable route summarization on the correct router?
- Did you enable route summarization for the correct area?
- Did you create the appropriate summary route?

Remember that interarea summaries are created on ABRs with the **area *area-id* range *ip-prefix*** command and that external summaries are created on ASBRs with the **summary-address *ip-prefix/length*** command.

When a summary route is created on a router, so is a summary route to Null0:

```
R2# show ip route | include Null
O 10.1.0.0/16 is a summary, 00:16:07, Null0
```

This route to Null0 is created and installed in the routing table to prevent routing loops. It is imperative that this route be in the table to ensure that if a packet received by this router and destined to a network that falls within the summary, but for which the router does not know how to reach (longer match), it is dropped.

Discontiguous Areas and Virtual Links

In a multiarea OSPF network, the backbone area (Area 0) must exist, and all other areas must connect to Area 0. If an area is not physically adjacent to Area 0, routes are not successfully learned by all routers in the OSPF domain. To solve this issue, a virtual link can be configured to logically connect the nonadjacent area with Area 0.

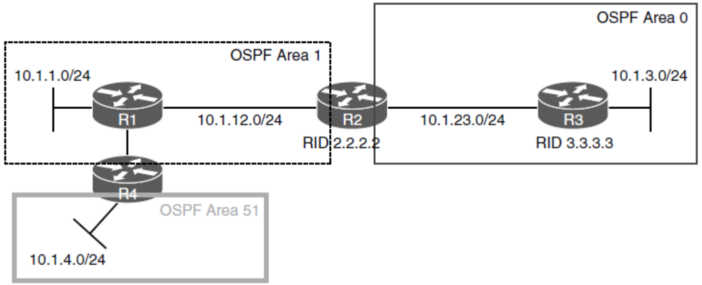

Figure 8-9 *Area 51 Not Directly Connected to Area 0*

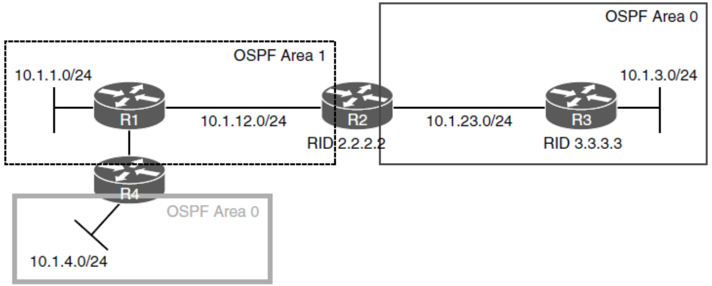

Figure 8-10 *Discontiguous Area 0*

A virtual link is created between the routers connected to the transit area (Area 1) by using their RIDs and the transit area number. The router OSPF configuration mode command on R2 is **area 1 virtual-link 4.4.4.4**, and the command on R4 is **area 1 virtual-link 2.2.2.2**. Common virtual link mistakes are, not configuring the area with the transit area or incorrectly configuring the router-ids

Verifying Virtual Links

Example 8-40 Notice the local interface is OSPF_VL0, which refers to the virtual link interface.

Example 8-41 shows the output of **show ip ospf virtual-links**, which provides more details about the virtual link. It is not only important to verify that the virtual link is up but that the state is full, which indicates that LSAs have been successfully exchanged.

Example 8-40 *Verifying a Neighbor Relationship over a Virtual Link*

```
R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           0   FULL/  -           -        10.1.14.4       OSPF_VL0
3.3.3.3           1   FULL/BDR        00:00:34    10.1.23.3       GigabitEthernet1/0
1.1.1.1           1   FULL/BDR        00:00:35    10.1.12.1       GigabitEthernet0/0
```

Example 8-41 *Verifying the Virtual Link*

```
R2# show ip ospf virtual-links
Virtual Link OSPF_VL0 to router 4.4.4.4 is up
 Run as demand circuit
 DoNotAge LSA allowed.
 Transit area 1, via interface GigabitEthernet0/0
 Topology-MTID Cost Disabled Shutdown Topology Name
       0         64    no       no       Base
 Transmit Delay is 1 sec, State POINT_TO_POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:09
 Adjacency State FULL (Hello suppressed)
 Index 2/3, retransmission queue length 0, number of retransmission 0
 First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
 Last retransmission scan length is 0, maximum is 0
 Last retransmission scan time is 0 msec, maximum is 0 msec
```

Load Balancing

OSPF supports only equal-cost load balancing. Therefore, when troubleshooting load balancing for OSPF, your two primary points of concern are the overall end-to-end cost and the maximum number of paths permitted for load balancing. To verify the maximum number of equal-cost paths an OSPF router is currently configured to support, use the **show ip protocols** command, as shown in Example 8-42.

If your topology is showing multiple paths to reach certain networks in your organization but they are not all showing up in the routing table, it is than likely because they are not equal-cost paths or the maximum paths value is configured too low.

Example 8-42 *Verifying the Maximum Number of Paths for Load Balancing*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is (prefix-list) TEST
 Router ID 1.1.1.1
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 Maximum path: 4
 Routing for Networks:
   10.1.1.1 0.0.0.0 area 1
 Routing on Interfaces Configured Explicitly (Area 1):
   GigabitEthernet1/0
...output omitted...
```

OSPFv2 Trouble Tickets

- This section presents three trouble tickets related to troubleshooting OSPF related issues

Trouble Ticket 8-1

All trouble tickets in this section are based on the topology shown in Figure 8-12.

Problem: Users in the 10.1.1.0/24 network indicate that they are not able to access resources in the 192.168.1.0/24 network.

As always, the first item on the list for troubleshooting is to verify the problem. You access a PC in the 10.1.1.0/24 network and ping an IP address in the 192.168.1.0/24 network; the ping is successful (0% loss), as shown in Example 8-43. However, notice that the reply is from the default gateway at 10.1.1.1, and it states Destination host unreachable. Therefore, the ping is actually technically not successful.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

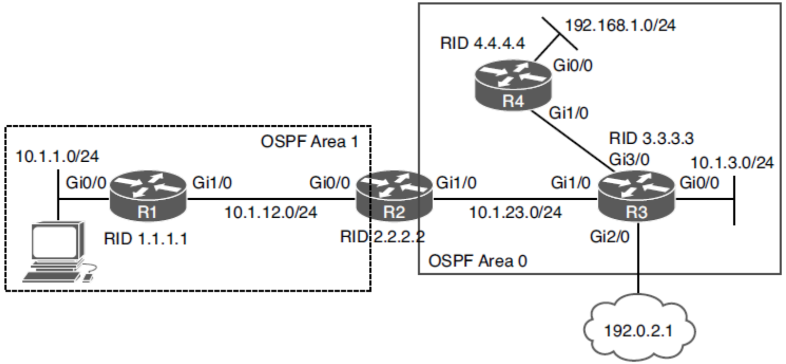

Figure 8-12 *OSPFv2 Trouble Tickets Topology*

Example 8-43 *Destination Unreachable Result from a ping Command on a PC*

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data;

Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.
Reply from 10.1.1.1: Destination host unreachable.

Ping statistics for 192.168.1.10:
 Packets: Sent = 4, Received = 4, lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

OSPFv2 Trouble Tickets
Trouble Ticket 8-2

Problem: Users in the 10.1.1.0/24 network indicate that they are not able to access resources in the 192.168.1.0/24 network.

As always, the first item on the list for troubleshooting is to verify the problem. You access a PC in the 10.1.1.0/24 network and ping an IP address in the 192.168.1.0/24 network, and it is successful (0% loss), as shown in Example 8-57. However, notice that the reply is from 10.1.23.2, and it states TTL expired in transit. Therefore, it was technically not successful.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

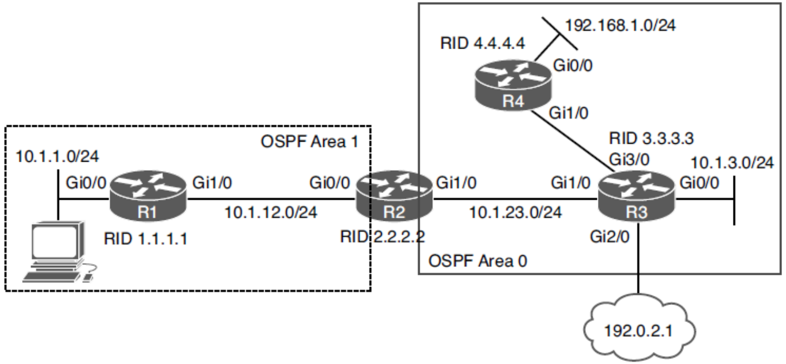

Figure 8-12 *OSPFv2 Trouble Tickets Topology*

Example 8-57 *TTL Expired in Transit Result from the ping Command on PC*

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.1.23.2: TTL expired in transit.
Reply from 10.1.23.2: TTL expired in transit.
Reply from 10.1.23.2: TTL expired in transit.
Reply from 10.1.23.2: TTL expired in transit.

Ping statistics for 192.168.1.10:
 Packets: sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Trouble Ticket 8-3

All trouble tickets in this section are based on the topology shown in Figure 8-12.

Problem: Routers R1 and R2 are not forming a neighbor adjacency

The first item on the list for troubleshooting is to verify the problem. You access R1 and issue the show ip ospf neighbor command, as shown in Example 8-64, and it confirms that there is no neighbor relationship with R2.

Refer to your text for next steps and examples to troubleshoot and resolve this trouble ticket.

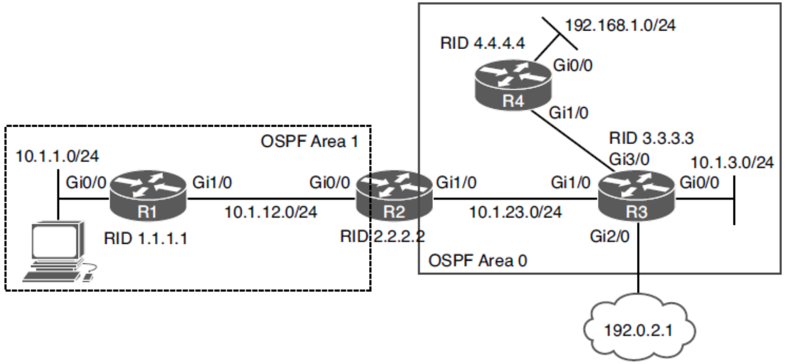

Figure 8-12 *OSPFv2 Trouble Tickets Topology*

Example 8-64 *Verifying R1's OSPF Neighbors*

```
R1# show ip ospf neighbor
R1#
```

Prepare for the Exam

Key Topics for Chapter 8

Description
Verifying OSPF neighbors with **show ip ospf neighbor**
Reasons an OSPF neighbor relationship might not form
Adjacency states
Verifying OSPF interfaces with **show ip ospf interface brief**
Displaying OSPF interface timers on R1 Gigabit Ethernet 1/0
Mismatched area numbers
Determining the type of OSPF areas
The passive interface feature and troubleshooting passive interface issues
Verifying OSPF area authentication

Key Topics for Chapter 8 (Cont.)

Description
Verifying OSPF authentication key
MTU mismatch
OSPF network types and characteristics
Reasons an OSPF route might be missing from either the LSDB or the routing table
Considerations when troubleshooting router filtering
Stub area configuration
The importance of the DR election in a hub-and-spoke multi-access network
OSPFv2 LSAs
Considerations when troubleshooting route summarization issues
Verifying the virtual link

Prepare for the Exam
Key Terms for Chapter 8

Term	
OSPF interface table	OSPFv3
OSPF neighbor table	address families
OSPF link-state database (LSDB)	designated router
link-state advertisement (LSA)	backup designated router
Dijkstra's shortest path first (SPF) algorithm	stub area
OSPF area	totally stubby area
virtual link	NSSA
OSPF area border router (ABR)	totally NSSA
OSPF autonomous system boundary router (ASBR)	

Prepare for the Exam

Command Reference for Chapter 8

Task	Command Syntax
Display the IPv4 routing protocols enabled on the device; for OSPFv2, display whether any route filters are applied, the RID, the number of areas the router is participating in, the types of areas, the maximum paths for load balancing, the network area command, the interfaces explicitly participating in the routing process, passive interfaces, routing information sources, and the AD show ip protocols	**show ip protocols**
Display general OSPF parameters, including the PID, the RID, the reference bandwidth, the areas configured on the router, the types of areas (stub, totally stubby, NSSA, and totally NSSA), and area authentication	**show ip ospf**
Display the interfaces that are participating in the OSPF process	**show ip ospf interface brief**
Display detailed information about the interfaces participating in the OSPF process, including interface IPv4 address and mask, area ID, PID, RID, network type, cost, DR/BDR, priority, and timers	**show ip ospf interface**

Command Reference for Chapter 8 (Cont.)

Task	Command Syntax
Display the OSPF devices that have formed a neighbor adjacency with the local router	**show ip ospf neighbor**
Display the OSPF routes that have been installed in the IPv4 routing table	**show ip route ospf**
Display the OSPF link-state database	**show ip ospf database**
Provide information about the status of OSPF virtual links that are required for areas not physically adjacent to the backbone area (that is, Area 0)	**show ip ospf virtual-links**
Display real-time information related to the exchange of OSPF hello packets; useful for identifying mismatched OSPF timers and mismatched OSPF area types	**debug ip ospf hello**
Display the transmission and reception of OSPF packets in real time	**debug ip ospf packet**

Prepare for the Exam

Command Reference for Chapter 8 (Cont.)

Task	Command Syntax
Display real-time updates about the formation of an OSPF adjacency; useful for identifying mismatched area IDs and authentication information	**debug ip ospf adj**
Display real-time information about OSPF events, including the transmission and reception of hello messages and LSAs; might be useful on a router that appears to be ignoring hello messages received from a neighboring router	**debug ip ospf events**