**Discovery 7: Implement Multiarea OSPF**

**Introduction**

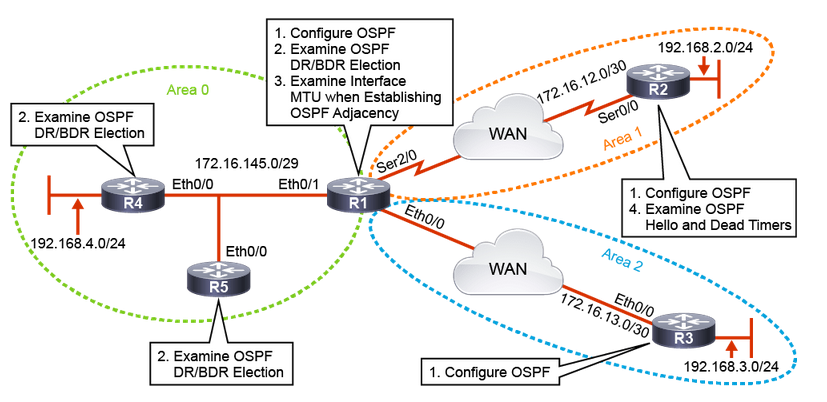
Through this discovery, you will learn how to configure and establish OSPF neighbor relationships in a multiarea environment. You will observe the impact of the interface MTU and OSPF hello and dead timer parameters on the OSPF neighbor relationship formation. In addition, you will learn about the roles of DR and BDR routers, and how to control how they are elected to those roles.

In this discovery, you will have access to five routers from R1 to R5. R4 and R5 are already preconfigured. You will be responsible for the configuration of R1, R2, and R3.

R1, R4, and R5 are connected to a common multiaccess GigabitEthernet segment. R1 and R2 are connected over a point to point GigabitEthernet link. R1 and R3 are connected over an GigabitEthernet WAN link.

Your configuration tasks are as follows:

* Enable OSPF on R1, R2, and R3
* Verify OSPF functionality
* Verify DR and BDR election
* Examine MTU-related OSPF Issues
* Modify OSPF timers

****

**Task 1: Enable OSPF on R1, R2, and R3**

**Activity**

**Step 1:** Configure OSPF on WAN and LAN interfaces on the R1 ABR. Use process ID number 1, and network commands for all directly connected networks.

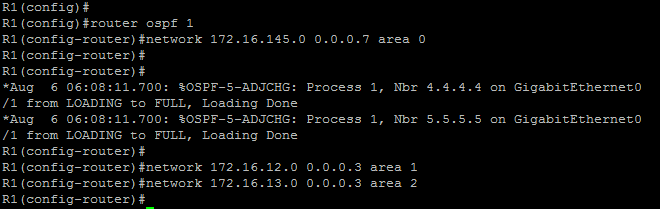
R1# configure terminal Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# router ospf 1

R1(config-router)# network 172.16.145.0 0.0.0.7 area 0

R1(config-router)# network 172.16.12.0 0.0.0.3 area 1

R1(config-router)# network 172.16.13.0 0.0.0.3 area 2



To enable the OSPF process on the router, use the router ospf process-id command. Process ID numbers on different sides of the link over which OSPF neighbor relationship will be established do not need to match. The OSPF process number ID is an internally used identification parameter for an OSPF routing process and has local significance. You can specify multiple OSPF routing processes in a router.

Notice that there are multiple ways to enable OSPF on an interface. To define interfaces on which OSPF process runs and to define the area ID for those interfaces, use the network ip-address wildcard-mask area area-id command. The combination of ip-address and wildcard-mask allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command.

Cisco IOS Software sequentially evaluates the ip-address wildcard-mask pair that is specified in the network command for each interface as follows:

* It performs a logical OR operation between the wildcard-mask argument and the interface primary IP address.
* It performs a logical OR operation between the wildcard-mask argument and the ip-address argument in the network command.
* The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the specified OSPF area

The area-id identifier is a 32-bit number that may be represented in integer or dotted-decimal format. If represented in dotted-decimal format, the area-id identifier does not represent the IP address, but it is only a way of writing the same number in integer format. For example, you may specify that an interface belongs to Area 1 using area 1 or area 0.0.0.1 notation in the network command. To establish OSPF full adjacency, two neighbor routers must be in the same area. Any individual interface can be only attached to a single area. If the address ranges specified for different areas overlap, Cisco IOS Software will adopt the first area in the network command list and ignore subsequent overlapping portions. You must pay special attention to ensure that address ranges do not overlap to avoid conflicts.

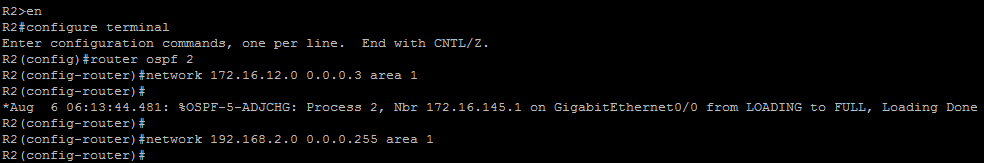
After entering the first network command, you should receive two console messages indicating that R4 and R5 are now OSPF neighbors.

**Step 2:** Configure OSPF on WAN and LAN interfaces on R2 and R3. On R2, use process ID number 2, and use the OSPF network command for both directly connected networks. On R3, use process ID number 3 and use the network command for the GigabitEthernet WAN link, and the OSPF interface configuration method for Loopback 0.

R2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)# router ospf 2

R2(config-router)# network 172.16.12.0 0.0.0.3 area 1

R2(config-router)# network 192.168.2.0 0.0.0.255 area 1

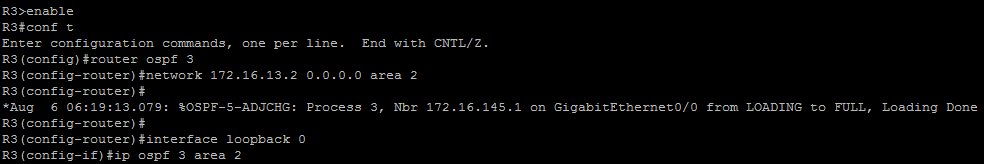


R3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)# router ospf 3

R3(config-router)# network 172.16.13.2 0.0.0.0 area 2

R3(config-router)# interface Loopback 0

R3(config-if)# ip ospf 3 area 2



Notice the use of the 0.0.0.0 wildcard mask with the network command on R3. This mask indicates that only the interface with the specific IP address listed will be enabled for OSPF.

Another method exists for enabling OSPF on an interface. R3’s loopback 0 interface is included in area 2 by using the ip ospf process-id area area-id command. This method explicitly adds the interface to area 2 without the use of the network command. This capability simplifies the configuration of unnumbered interfaces with different areas and ensures that any new interfaces brought online would not automatically be included in the routing process. This configuration method is also used for OSPFv3 since that routing protocol doesn’t allow the use of the network statement.

Notice that since OSPF is already enabled on R1, a neighbor adjacency is formed with that router when the network commands are entered on R2 and R3.

**Step 3:** On R1, R2 and R3, configure the OSPF router ID using the router-id command. Use ID 1.1.1.1 for R1, 2.2.2.2 for R2 and 3.3.3.3 for R3.

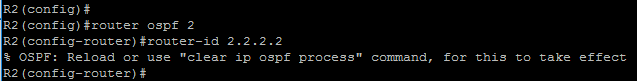
R1(config)#router ospf 1

R1(config-router)# router-id 1.1.1.1



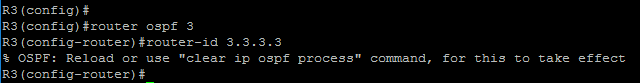
R2(config)#router ospf 2

R2(config-router)# router-id 2.2.2.2



R3(config)#router ospf 3

R3(config-router)# router-id 3.3.3.3



The OSPF router ID is a fundamental parameter when you want to run the OSPF process. To start the OSPF process, Cisco IOS Software must be able to identify a unique router ID. At least one primary IP address on an interface in the up/up state must be configured for the router to be able to choose the router ID, otherwise an error message is logged and the OSPF process does not start.

To choose the OSPF router ID at the time of OSPF process initialization, the router uses the following criteria:

* Use the router ID specified in the router-id ip-address command. You can configure an arbitrary value in the IP address format, but this value must be unique. If the IP address that is specified with the router-id command overlaps with the router ID of another already active OSPF process, the router-id command fails.
* Use the highest IP address of all active loopback interfaces on the router.
* Use the highest IP address among all active nonloopback interfaces.

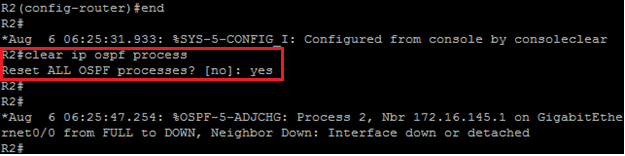
After the three-step OSPF router ID selection process has ended, and if the router is still not able to select an OSPF router ID, an error message will be logged. An OSPF process that failed to select a router ID, retries the selection process every time that an IP address becomes available, the interface changes its state to up/up, or, an IP address is configured on the interface.

**Step 4:** Start by clearing the OSPF routing process on R2 and R3 to allow the manually configured router ID to take effect.

R2# clear ip ospf process

Reset ALL OSPF processes? [no]: yes

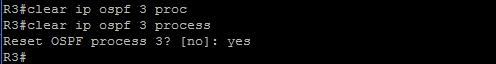
R2#



R3# clear ip ospf 3 process

process Reset OSPF process 3? [no]: yes

R3#



Once an OSPF router ID is selected, it is not changed, even if the interface that is used to select it changes its operational state or IP address. To change the OSPF router ID, you must reset the OSPF process with the clear ip ospf process command or reload the router.

In production networks, the OSPF router ID cannot be changed easily. Change of the OSPF router ID requires reset of all OSPF adjacencies, resulting in a temporary routing outage. The router also must originate new copies of all its own LSAs with the new router ID.

You can either clear the specific OSPF process by specifying the process ID, or you can reset all OSPF processes using the clear ip ospf process command.

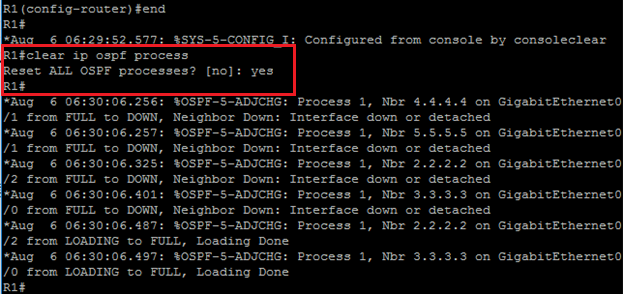
When the clear ip ospf process command is entered on R2 and R3, notice that the router ID being advertised by R1 is 172.16.145.1. R1 has no loopback interfaces and it didn’t have a manually configured router ID when the OSPF process was enabled. R1 chose the highest IP address among all active nonloopback interfaces as its initial router ID.

**Step 5:** Clear the OSPF routing process on R1 to allow the manually configured router ID to take effect.

R1# clear ip ospf process

Reset ALL OSPF processes? [no]: yes

R1#



The OSPF neighbor adjacencies messages show that all routers are now using manually configured router IDs.

**Note**

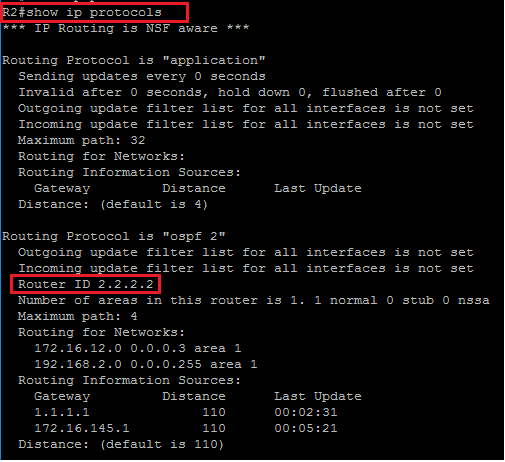
You might notice a console message on R2 or R3 indicating that the 172.16.145.1 neighbor is down because the Dead timer is expired. This occurrence is normal OSPF behavior and allows the neighbor table to flush incorrect entries since R1 is now using the 1.1.1.1 router ID instead.

**Task 2: Verify OSPF Functionality**

**Activity**

**Step 1:** Verify the newly configured OSPF router ID on R2 and R3 using the show ip protocol command.

R2# show ip protocols

****

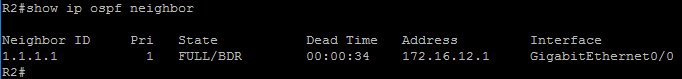
R3# show ip protocols | include ID



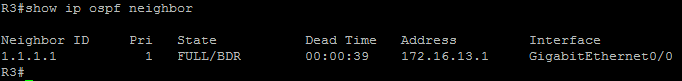
You can verify the newly configured OSPF router ID using the show ip protocols command. The large output of this command can, optionally, be filtered using the pipe function.

**Step 2:** Investigate the OSPF adjacency on R2 and R3 using the show ip ospf neighbor command.

R2# show ip ospf neighbor



R3# show ip ospf neighbor

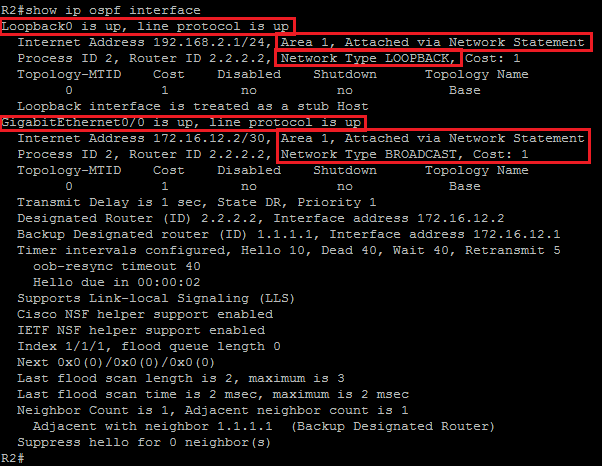


The command show ip ospf neighbor displays OSPF neighbor information on a per-interface basis. The significant fields of the output are as follows:

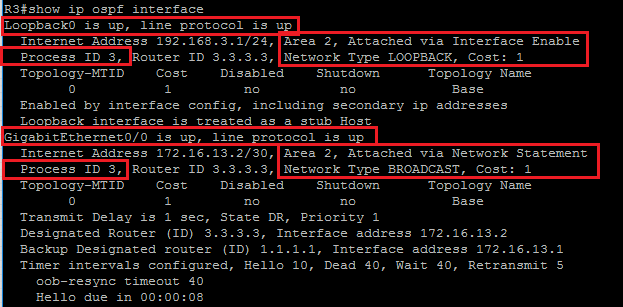
* Neighbor ID: Represents the neighbor router ID
* Priority: Priority on the neighbor interface that is used for the DR, and BDR election
* State: The FULL state represents the final stage of the OSPF neighbor establishment process and denotes that the local router has established full neighbor adjacency with the remote OSPF neighbor. The hyphen (“-“) indicates that a designated router wasn’t needed for this type of network. The GigabitEthernetinterface is treated by OSPF as a point-to-point link since only 2 routers will ever be on this segment. DR means that the DR, and BDR election process has been completed and the remote router with the router ID 1.1.1.1 has been elected as the DR.
* Dead Time: Represents the value of the dead timer. When this timer expires, the router terminates the neighbor relationship. Each time that the router receives an OSPF hello packet from a specific neighbor, it resets the dead timer back to its full value.
* Address: The primary IP address of the neighbor router
* Interface: The local interface over which the OSPF neighbor relationship is established

**Step 3:** Verify OSPF enabled interfaces on R2 and R3 using the show ip ospf interface command.

R2# show ip ospf interface



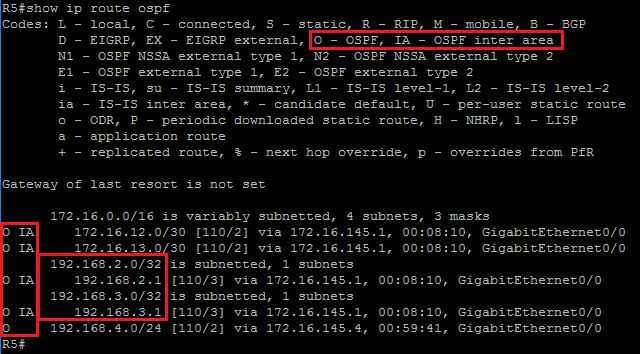
R3# show ip ospf interface



The output of the show ip ospf interface command shows you all interfaces that are enabled in the OSPF process. For each enabled interface, you can see detailed information such as OSPF area ID, OSPF process ID, and how the interface was included into the OSPF process. In the output, you can see that both interfaces on R3 were included via the network statement, which is configured with the network command. R2 shows that Loopback 0 was included via the explicit interface configuration method, and GigabitEthernet0/0 was included via the network statement.

**Step 4:** Verify OSPF routes in the routing table on R5 using the show ip route ospf command.

R5# show ip route ospf



Among routes that are originated within an OSPF autonomous system, OSPF clearly distinguishes two types of routes: intra-area routes and interarea routes. Intra-area routes are routes that are originated and learned in the same local area. The character “O” is the code for the intra-area routes in the routing table. The second type is interarea routes, which originate in other areas and are inserted into the local area to which your router belongs. The characters “O IA” are the code for the interarea routes in the routing table. Interarea routes are inserted into other areas by the ABR.

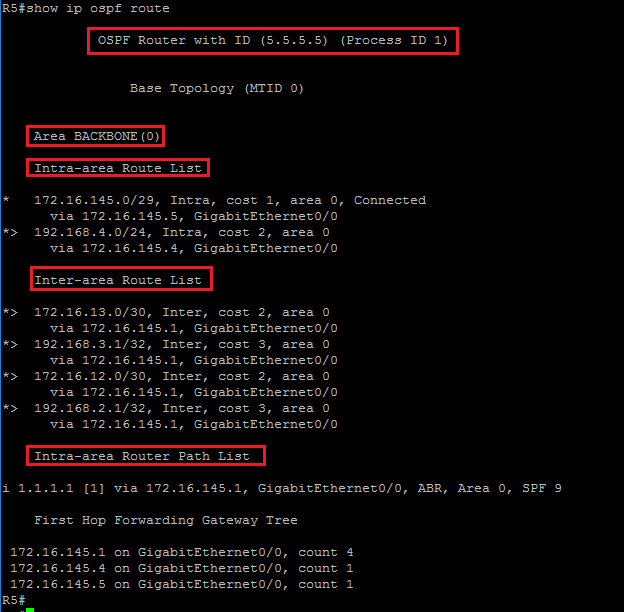
The prefix 192.168.4.0/24 is an example of an intra-area route from the perspective of R5. It originated from router R4, which is part of Area 0, the same area as R5.

The prefixes from R2 and R3, which is part of Area 1 and area 2, are shown in the routing table on R5 as interarea routes. The prefixes were inserted into Area 0 as interarea routes by R1, which plays the role of ABR.

The prefixes 192.168.2.0/24 and 192.168.3.0/24 configured on the Loopback interfaces of R2 and R3 are displayed in the R5 routing table as host routes 192.168.2.1/32 and 192.168.3.1/32. By default, OSPF will advertise any subnet that is configured on the loopback interface as /32 host route. To change this default behavior, you can change the OSPF network type on the loopback interface from default loopback to point-to-point, using the ip ospf network point-to-point interface command.

**Step 5:** Observe OSPF routes on R5 by entering the show ip ospf route command.

R5# show ip ospf route



The command show ip ospf route gives you clearly separated lists of intra-area and interarea routes. In addition, the output of the command gives you essential information about Area Border Routers, including the router ID, IP address in the current area, the interface that advertises routes into the area, and the area ID.

For the interarea routes, the metric for the route (cost), area into which route is distributed, and the interface over which the route is inserted are displayed.

**OSPF Neighbor States**

OSPF neighbors go through multiple neighbor states before forming a full OSPF adjacency.

OSPF routers progress through seven states:

* Down: No active neighbor detected
* INIT: Hello packet is received from neighbor
* 2-WAY: Own router ID in received hello
* Exstart: Master and slave roles determined
* Exchange: Database description packets sent
* Loading: Exchange of LSRs and LSUs
* Full: Neighbors fully adjacent

The following is a summary of the states that an interface passes through before establishing as adjacency with another router:

* DOWN: No information has been received on the segment.
* INIT: The interface has detected a hello packet coming from a neighbor, but bidirectional communication has not yet been established.
* 2-WAY: There is bidirectional communication with a neighbor. The router has seen itself in the hello packets coming from a neighbor. At the end of this stage, the DR, and BDR election will be performed if necessary. When routers are in the 2-WAY state, they must decide whether to proceed in building an adjacency. The decision is based on whether one of the routers is a DR or BDR or if the link is a point-to-point or a virtual link.
* EXSTART: Routers are trying to establish the initial sequence number that is going to be used in the information exchange packets. The sequence number ensures that routers always get the most recent information. One router will become the master and the other will become the slave. The master router will poll the slave for information.
* EXCHANGE: Routers will describe their entire LSDB by sending database description packets (DBD). In this state, packets may be flooded to other interfaces on the router.
* LOADING: In this state, routers are finalizing the information exchange. Routers have built a link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.
* FULL: In this state, adjacency is complete. The neighboring routers are fully adjacent. Adjacent routers will have similar LSDBs.

**Step 6:** Observe the OSPF neighbor adjacency formation and OSPF packet types on R3 using the **debug ip ospf adj** and **clear ip ospf process** commands. Disable debug when the OSPF session is re-established.

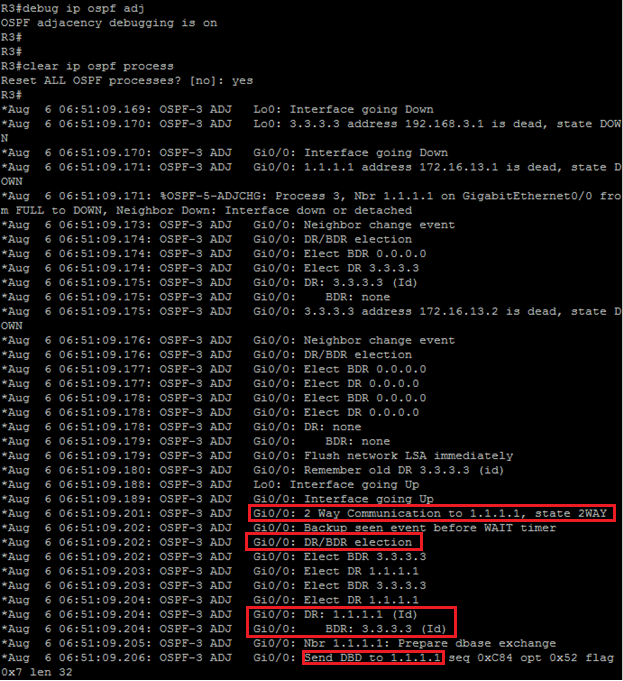
R3# debug ip ospf adj

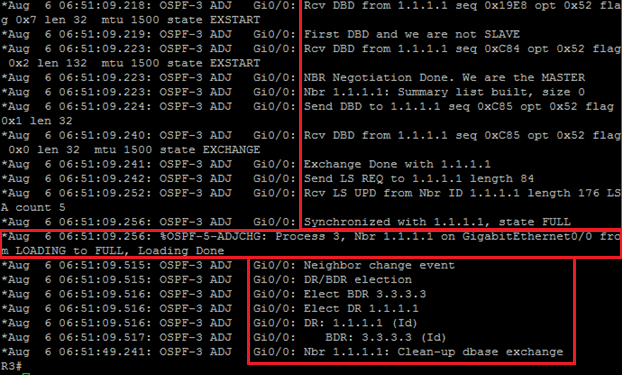
OSPF adjacency debugging is on

R3# clear ip ospf process

Reset ALL OSPF processes? [no]: yes

R3# undebug all





An OSPF adjacency is established in several steps. First, routers that intend to establish full OSPF neighbor adjacency exchange OSPF hello packets. Both OSPF neighbors are in the DOWN state (the initial state of a neighbor conversation that indicates that no hello’s have been heard from the neighbor). When a router receives a hello from the neighbor but has not yet seen its own router ID in the neighbor hello packet, it will transit to the INIT state. In this state, the router will record all neighbor router IDs and start including them in hellos sent to the neighbors. When the router sees its own router ID in the hello packet that is received from the neighbor, it will transit to the 2-WAY state. This state means that bidirectional communication with the neighbor has been established.

On broadcast links, OSPF neighbors first determine DR and BDR roles, which optimize the exchange of information in broadcast segments.

In the next step, the routers start to exchange the content of OSPF databases. The first phase of this process is to determine the master/slave relationship and choose the initial sequence number for adjacency formation. To accomplish that phase, the routers exchange DBD packets. When the router receives the initial DBD packet, it transitions the state of the neighbor from which this packet is received to the EXSTART state, populates its Database Summary list with the LSAs that describe the content of the neighbor database, and sends its own empty DBD packet. In the DBD exchange process, the router with the higher router ID will become master and it will be the only router that can increment sequence numbers.

With master/slave selection complete, the database exchange can start. R3 will transit R1’s neighbor state to EXCHANGE. In this state, R3 describes its database to R1 by sending DBD packets, which contain the headers of all LSAs in the Database Summary list. The Database Summary list gives the description of all LSAs in the router’s database, but not the full content of the OSPF database. To describe the content of the database, one or multiple DBD packets may be exchanged. The router compares the content of its own Database Summary list with the list received from the neighbor, and if there are differences, it adds the missing LSAs to the Link State Request list. At this point, the routers enter the LOADING state. R3 sends an LSR packet to the neighbor, requesting full content of the missing LSAs from the LS Request list. R1 replies with the LSU packets, which contain the full version of the missing LSAs.

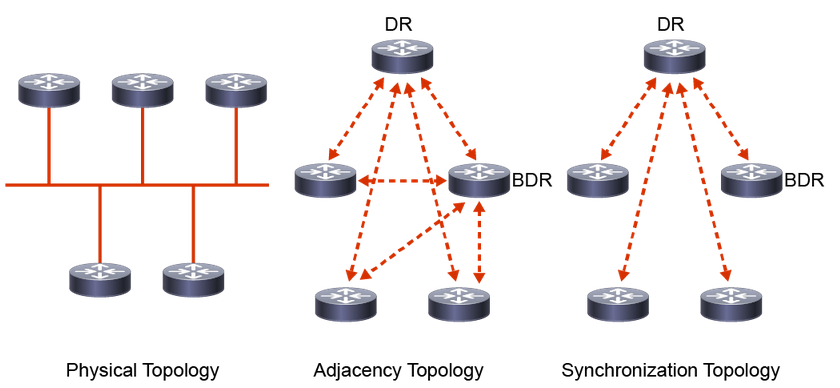
Finally, when neighbors have the full version of the LS database, both neighbors will transit to the FULL state, which means that databases on the routers are synchronized and neighbors are fully adjacent.

**Task 3: Verify DR and BDR Election**

**Activity**

Optimizing OSPF Adjacency Behavior

* DR/BDR election occurs on multiaccess broadcast and nonbroadcast networks
* The DR/BDR election improves network functioning in the following ways:
  + Reducing routing update traffic
  + Managing link state synchronization



Multiaccess networks, either broadcast (such as GigabitEthernet) or nonbroadcast (such as Frame Relay), represent interesting issues for OSPF. All routers sharing the common segment will be part of the same IP subnet. When forming adjacency on a multiaccess network, every router will try to establish full OSPF adjacency with all other routers on the segment. This behavior may not represent an issue for the smaller multiaccess broadcast networks, but it may represent an issue for the NBMA, where, usually, you do not have full-mesh PVC topology. This issue in NBMA networks manifests itself in the inability for neighbors to synchronize their OSPF databases directly among themselves. A logical solution, in this case, is to have a central point of OSPF adjacency responsible for the database synchronization and advertisement of the segment to the other routers.

As the number of routers on the segment grows, the number of OSPF adjacencies increases exponentially. Every router must synchronize its OSPF database with every other router, and in the case of many routers on segment, this behavior leads to inefficiency. Another issue arises when every router on the segment advertises all its adjacencies to other routers in the network. If you have full-mesh OSPF adjacencies, the other OSPF routers will receive a large amount of redundant link-state information. The solution for this problem is again to establish a central point with which every other router forms an adjacency, and which advertises the segment to the rest of the network.

The routers on the multiaccess segment elect a DR and a BDR that centralize communication for all routers that are connected to the segment. The DR and BDR improve network functionality in the following ways:

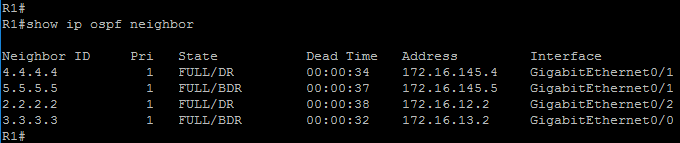
* Reducing routing update traffic: The DR and BDR act as a central point of contact for link-state information exchange on a multiaccess network. Therefore, each router must establish a full adjacency with the DR, and the BDR. Each router, rather than exchanging link-state information with every other router on the segment, sends the link-state information to the DR and BDR only by using the dedicated multicast address 224.0.0.6. The DR represents the multiaccess network in the sense that it sends link-state information from each router to all other routers in the network. This flooding process significantly reduces the router-related traffic on the segment.
* Managing link-state synchronization: The DR and BDR ensure that the other routers on the network have the same link-state information about the common segment. In this way, the DR, and BDR reduce the number of routing errors.

When the DR is operating, the BDR does not perform any DR functions. Instead, the BDR receives all the information, but the DR performs the LSA forwarding and LSDB synchronization tasks. The BDR performs the DR tasks only if the DR fails. When the DR fails, the BDR automatically becomes the new DR, and a new BDR election occurs.

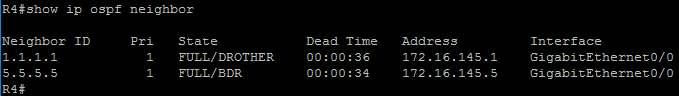
**Step 1:** Examine the DR/BDR status on R1, R4, and R5 using the show ip ospf neighbor command.

Routers R1, R4, and R5 are all connected to the same shared network segment, where OSPF will automatically try to optimize adjacencies.

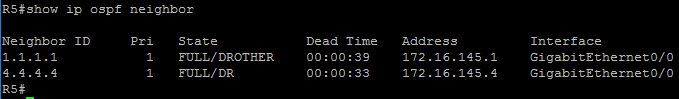
R1# show ip ospf neighbor



R4# show ip ospf neighbor



R5# show ip ospf neighbor



When R1, R4, and R5 start establishing OSPF neighbor adjacency, they will first send OSPF hello packets to discover which OSPF neighbors are active on the common GigabitEthernet segment. After the bidirectional communication between routers is established and they are all in OSPF neighbor 2-WAY state, the DR/BDR election process begins. The OSPF hello packet contains three specific fields that are used for the DR/BDR election: Designated Router, Backup Designated Router, and Router Priority.

The Designated Router and Backup Designate Router fields are populated with a list of routers claiming to be DR, and BDR. From all routers that are listed, the router with the highest priority becomes the DR, and the router with the next highest priority becomes the BDR. If the priority values are equal, the router with the highest OSPF router ID becomes the DR, and the router with the next highest OSPF router ID becomes BDR.

The DR/BDR election process takes place on broadcast and nonbroadcast multiaccess networks. The main difference between the two is the type of IP address that is used in the hello packet. On the multiaccess broadcast networks, routers use multicast destination IP address 224.0.0.6 to communicate with the DR (called AllDRRouters) and the DR uses multicast destination IP address 224.0.0.5 to communicate with all other non-DR routers (called AllSPFRouters). On NBMA networks, the DR and adjacent routers communicate using unicast.

The procedure of DR/BDR election occurs not only when the network first becomes active, but also when the DR becomes unavailable. In this case, the BDR will immediately become the DR, and the election of the new BDR starts.

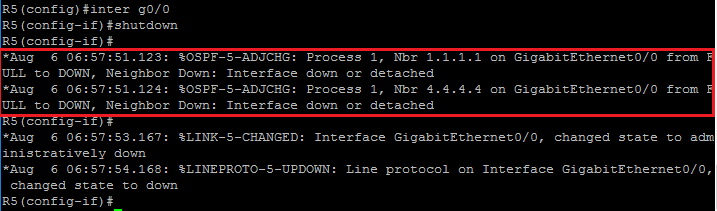
In the topology, R5 has been elected as the DR, and R4 as the BDR, due to the highest router-id values on the segment. R1 became DROTHER. On the multiaccess segment, it is normal behavior that the router in DROTHER status is fully adjacent with DR/BDR, and in a 2-WAY state with all other DROTHER routers present on the segment.

**Step 2:** On R5, shut down the interface towards R1 and R4. Re-examine DR/BDR status on R1 and R4.

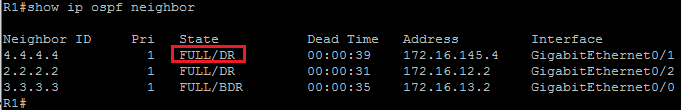
After you shut down the interface, wait until the neighbor adjacencies expire before re-examining the DR/BDR state.

R5(config)# interface G 0/0

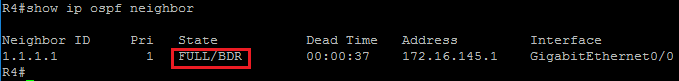
R5(config-if)# shutdown



R1# show ip ospf neighbor



R4# show ip ospf neighbor



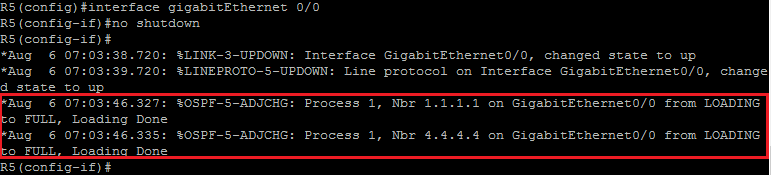
When you shut down GigabitEthernet 0/0 on R5, the DR router on the segment becomes unavailable but because shutting down the GigabitEthernet 0/0 interface on R5 is seen as an indirect loss of adjacency, R1 will only declare R5 down after the Dead timer of 40 seconds has expired. This issue also applies to R4. After the Dead timer expires, a new DR/BDR election takes place. The output of the show ip ospf neighbor command shows that R4 has become the DR, and R1 the BDR.

Note that because shutting down the GigabitEthernet 0/0 interface on R5 is seen as an indirect loss of adjacency, R1 will only declare R5 down after the Dead timer of 40 seconds has expired. This issue will also apply to R4.

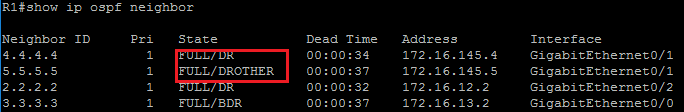
**Step 3:** On R5, enable the interface towards R1 and R4. Examine the DR/BDR status on R1, R4, and R5.

R5(config)# interface G 0/0

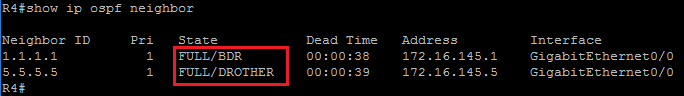
R5(config-if)# no shutdown

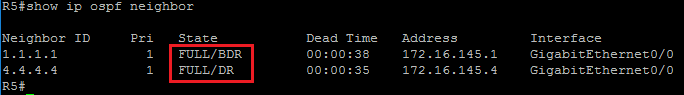


R1# show ip ospf neighbor



R4# show ip ospf neighbor

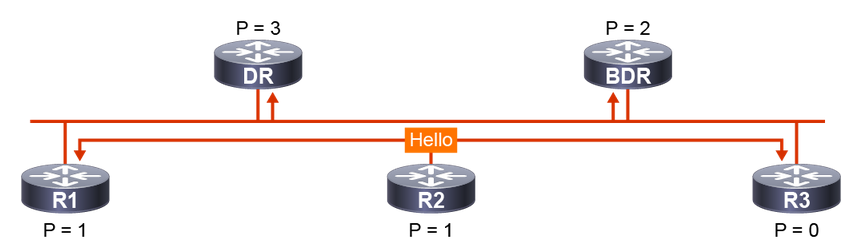


R5# show ip ospf neighbor

When you re-enable R5 in the GigabitEthernet 0/0 interface, a new DR/BDR election process will not take place, although R5 has the highest OSPF router ID on the segment. Once the DR and BDR are elected, they are not pre-empted. This rule makes a multiaccess segment more stable by preventing the election process from occurring when a new router becomes active. It means that the first two DR-eligible routers on the link will be elected as DR and BDR. A new election will occur only when one of them fails.

Using OSPF Priority in the DR/BDR Election

* OSPF hello packet that is used in DR/BDR election contains Router Priority field.
* The router with the highest OSPF priority will be elected as DR.
* The router with the second-highest OSPF priority will be elected as BDR.
* The router with the priority set to 0 does not participate in the DR/BDR election and is not eligible to become the DR/BDR.



One of the fields in the OSPF hello packet that is used in the DR/BDR election process is the Router Priority field. Every broadcast and nonbroadcast multiaccess OSPF-enabled interface has an assigned priority value, which is a number between 0 and 255. By default, in Cisco IOS Software, the OSPF interface priority value is 1. You can manually change it using either the ip ospf priority interface level command. To elect a DR, and BDR, the routers view the OSPF priority value of other routers during the hello packet exchange process and then use the following conditions to determine which router to select:

* The router with the highest priority value is elected as the DR.
* The router with the second-highest priority value is the BDR.
* If there is a tie, where two routers have the same priority value, the router ID is used as the tie-breaker. The router with the highest router ID becomes the DR. The router with the second-highest router ID becomes the BDR.
* A router with a priority that is set to 0 cannot become the DR or BDR. A router that is not the DR or BDR is called a DROTHER.

**Step 4:** On R1, configure OSPF priority using ip ospf priority interface level command. Clear the OSPF process on R4 to re-initiate the DR/BDR election process.

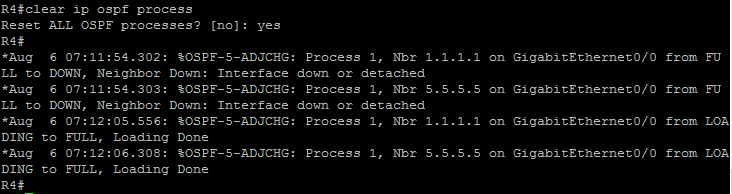
Setting the OSPF interface priority globally to a value higher than 1 will influence the DB/BDR election in favor of R1.

R1(config)# interface G 0/1

R1(config-if)# ip ospf priority 100

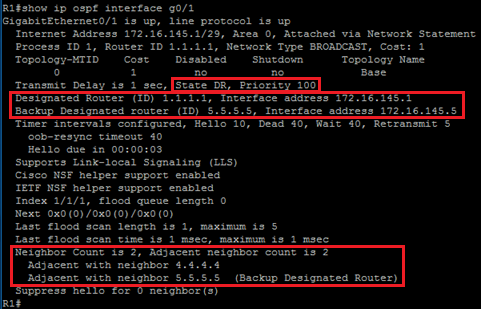


R4# clear ip ospf process

In this step, you set the OSPF interface priority value to 100. In this way, you influence the DR/BDR election and the R1 router will become the DR after you clear the OSPF process on the current DR, R4.

**Step 5:** On R1, verify that it has been elected as a new DR by entering the show ip ospf interface GigabitEthernet 0/1 command.

R1# show ip ospf interface G 0/1



The output of the show ip ospf interface command on R1 shows that R1 is elected as the DR, and R5 is elected as the BDR. R1 is fully adjacent with two neighbors, R4 and R5.

**Step 6:** On R4 and R5, set the OSPF priority on the GigabitEthernet 0/0 interfaces to 0 using the ip ospf priority level command.

R4(config)# interface G 0/0

R4(config-if)# ip ospf priority 0



R5(config)# interface G 0/0

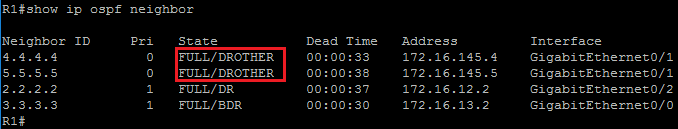
R5(config-if)# ip ospf priority 0

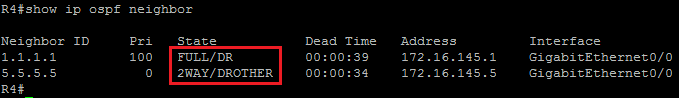


Setting the OSPF priority to a value of 0 on the GigabitEthernet 0/0 interfaces of R4 and R5 causes these two routers to not participate in DR/BDR election. They will not be eligible to become DR/BDR. Such routers will have the DROTHER function.

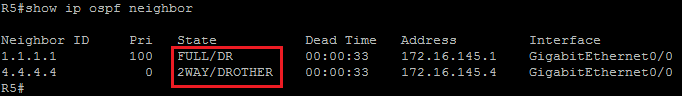
**Step 7:** Verify DR/BDR status on R1, R4, and R5.

R1# show ip ospf neighbor



R4# show ip ospf neighbor

R5# show ip ospf neighbor



Output of the show ip ospf neighbor command on R1 shows that R1 is fully adjacent with R4 and R5 and that R4 and R5 have DROTHER functions. R4 is fully adjacent with the DR router R1 while it maintains 2-WAY state with its peer DROTHER router R5. Similarly, R5 is fully adjacent with DR R1 and maintains 2-WAY state with DROTHER router R4. 2-WAY state between non-DR/BDR routers on the segment is normal behavior, they do not synchronize LSDBs directly but over DR/BDR. By maintaining 2-WAY state, DROTHER routers keep other DROTHER peers informed about their presence on the network.

**Task 4: Examine MTU-Related OSPF Issues**

**Activity**

Importance of MTU

* IP MTU determines the maximum size of the packet that can be forwarded without fragmentation.
* Mismatched MTUs can lead to an inconsistent OSPF database.
* OSPF requires the same MTUs to be configured on both sides of the link.
* OSPF neighbors with mismatched MTUs are stuck in the EXSTART adjacency state.

The IP MTU parameter determines the maximum size of the IP packet that can be forwarded out the interface without the fragmentation. If a packet with an IP MTU larger than the maximum arrives at the router interface, it will either be discarded if the DF bit in the packet header is set, or it will be fragmented. OSPF packets completely rely on IP for the possible fragmentation. Although RFC 2328 does not recommend OSPF packet fragmentation, there may arise a situation in which the size of the OSPF packet has greater value than the interface IP MTU. If MTUs are mismatched between two neighbors, this condition can introduce issues with the exchange of link-state packets, resulting in continuous retransmissions.

To prevent such issues, OSPF requires that the same IP MTU is configured on both sides of the link. If neighbors have mismatched IP MTU configured, they will not be able to form full OSPF adjacency. They will be stuck in the EXSTART adjacency state.

**Step 1:** Change the IP MTU size on R3 GigabitEthernet0/0 interface to 1400.

R3(config)# interface G 0/0

R3(config-if)# ip mtu 1400



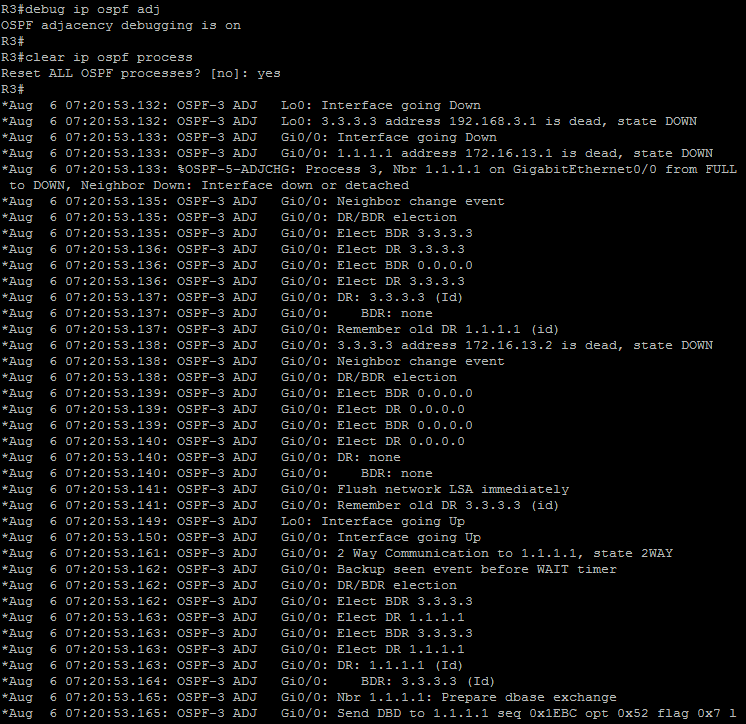
You have changed the IP MTU size on the R3 GigabitEthernet 0/0 interface to create a mismatch between IP MTU sizes on the link between R3 and R1. This mismatch will generate a situation in which R3 and R1 are not able to synchronize their OSPF databases and a new full adjacency between them will never be established.

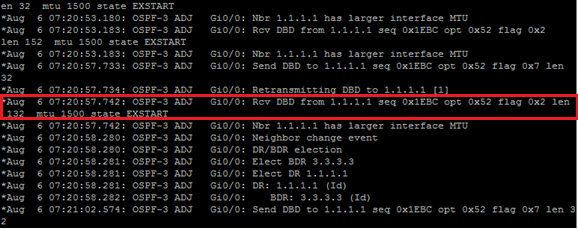
**Step 2:** Enable debugging of the OSPF adjacency on R3, using the debug ip ospf adj command. Clear the OSPF process to reset the adjacency and disable debug when the OSPF session is re-established.

R3# debug ip ospf adj

R3# clear ip ospf process

Reset ALL OSPF processes? [no]: yes

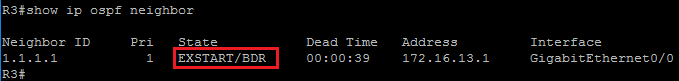




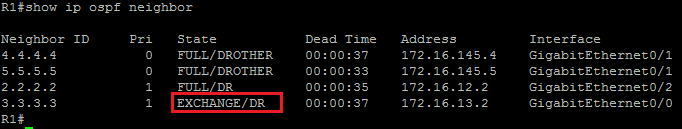
The DBD packet carries information about the largest non-fragmented packet that can be sent from the neighbor. In this situation, IP MTU values on different sides of the link are not equal. R3 will receive a DBD packet with an IP MTU size 1500, which is greater than its own MTU size of 1400. This condition will result in the inability of both R3 and R1 to establish full neighbor adjacency, and the output of the debug command will display "Nbr has larger interface MTU” message. Mismatched neighbors will stay in EXSTART state. To form full OSPF adjacency, IP MTU needs to match on both sides of the link.

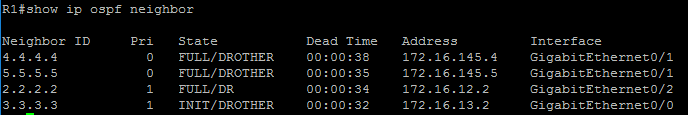
**Step 3:** Verify the OSPF neighbor state on R3 and R1.

R3# show ip ospf neighbor



R1# show ip ospf neighbor



R1# show ip ospf neighbor

Mismatching interface IP MTU sizes on opposite sides of the OSPF link result in the inability to form full adjacency. R3, which detected that R1 has a higher MTU, keeps neighbor adjacency in EXSTART state. R1 continues to retransmit an initial BDB packet to R3, but R3 is not able to acknowledge them due to the unequal IP MTU. On R1, you can observe how the OSPF adjacency state with R3 is unstable. The adjacency gets to the EXCHANGE state, but it is then terminated, starting again from the INIT state up to the EXCHANGE state in a cycle.

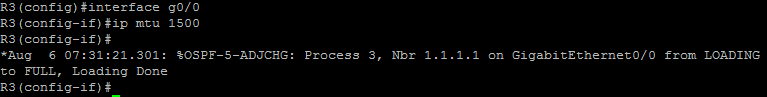
**Note**

The recommended way to fix such issues is to make sure that the IP MTU matches between OSPF neighbors.

**Step 4:** Change the IP MTU size on R3 GigabitEthernet0/0 interface to 1500 to match the value on R1.

R3(config)# interface G 0/0

R3(config-if)# ip mtu 1500



When the MTU mismatch is corrected, the OSPF neighbor adjacency is re-established.

**Task 5: Modify OSPF Timers**

**Activity**

Manipulating OSPF Timers

* OSPF uses hello and dead timers to monitor neighbor reachability.
* To form an OSPF neighbor adjacency, hello and dead interval timers must match.
* OSPF hello timer default values:
  + Broadcast and point-to-point links: 10 seconds
  + All other OSPF network types: 30 seconds
* Default value for OSPF dead timer is four times the hello interval.
* The debug ip ospf hello command can be used to see a mismatch in hello timers.

Like EIGRP, OSPF uses two timers to check neighbor reachability. These two timers are named hello and dead intervals. The values of the hello and dead intervals are carried in the OSPF hello packet, which serves as a keepalive message with the purpose of acknowledging the router presence on the segment. The hello interval specifies the frequency of sending OSPF hello packets in seconds. The SPF dead timer specifies how long a router waits to receive a hello packet before it declares the neighbor router down.

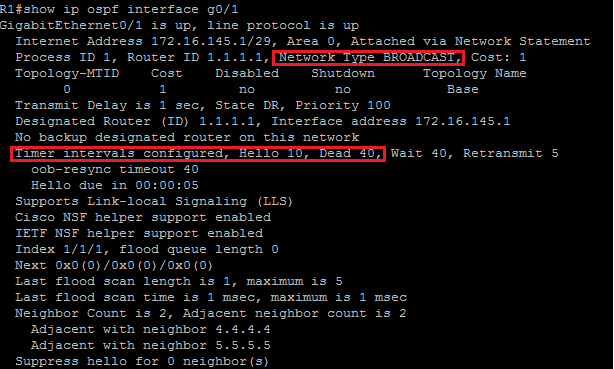
OSPF requires that both the hello and dead timers are identical for all routers on the segment to become OSPF neighbors. The default value of the OSPF hello timer on multiaccess broadcast and point-to-point links is 10 seconds and on all other network types, including nonbroadcast (NBMA), is 30 seconds. Once you set up the hello interval, the default value of the dead interval will automatically be four times the hello interval. For broadcast and point-to-point links, it is 40 seconds and for all other OSPF network types, it is 120 seconds.

To detect faster topological changes, you can lower the value of the OSPF hello interval, with the downside of having more routing traffic on the link.

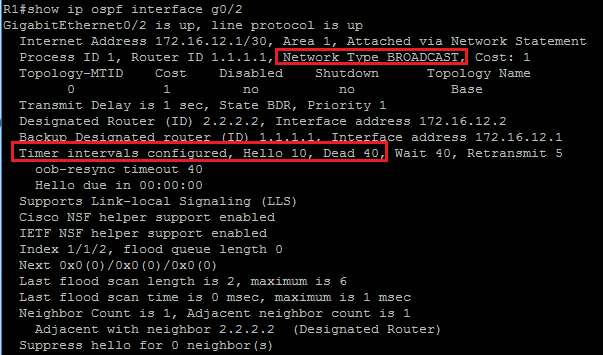
To investigate the mismatch of the hello timers, use the debug ip ospf hello command.

**Step 1:** On R1, investigate hello and dead timer values on GigabitEthernet 0/1 and GigabitEthernet0/2 interfaces, using the show ip ospf interface command.

R1# show ip ospf interface G 0/1



R1# show ip ospf interface G 0/2



The default value of the OSPF hello interval on broadcast multiaccess (GigabitEthernet) and point-to-point links are 10 seconds, while the default value of the dead interval is four times hello, or 40 seconds. The default values of the OSPF hello and dead timers on all other OSPF network types, including nonbroadcast (NBMA) such as Frame Relay, is 30 seconds and 120 seconds, respectively.

On low-speed links, you may want to alter the default OSPF timer values to achieve faster convergence. The negative aspect of lowering the OSPF hello interval is the overhead of more frequent routing updates, causing higher router utilization, and more traffic on the link.

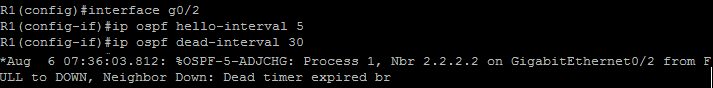
**Step 2:** On R1, lower the default OSPF hello and dead intervals on the G 0/2 interface.

The OSPF timer can be changed using the ip ospf hello-interval and ip ospf dead-interval interface commands.

R1(config-if)# interface g 0/2

R1(config-if)# ip ospf hello-interval 5

R1(config-if)# ip ospf dead-interval 30



Once you change the default OSPF hello and dead interval values on the GigabitEthernet link, both routers will detect a hello timer mismatch. As a result, the dead timer will not be refreshed, so it will expire, declaring the OSPF neighbor relationship as down.

**Note**

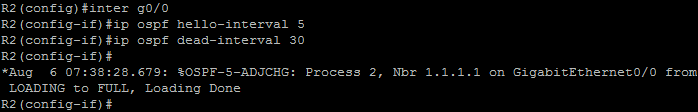
When changing only the OSPF hello interval, OSPF automatically changes the dead interval to four times the hello interval, unless otherwise specified.

**Step 3:** On R2, lower the default OSPF hello and dead timers on the G 0/0 interface so that they match the respective values that are configured on R1.

R2(config)# interface G 0/0

R2(config-if)# ip ospf hello-interval 5

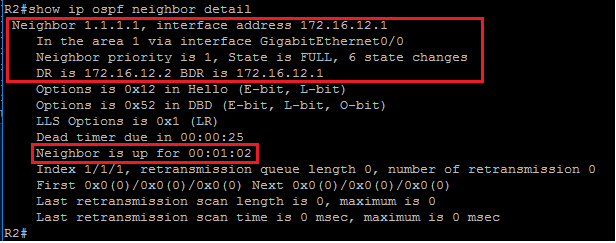
R2(config-if)# ip ospf dead-interval 30



When you change the OSPF hello and dead timers on R2 so that they match the timers on R1, both routers on the link will be able to establish adjacency on the GigabitEthernet link. After that, the routers will exchange and synchronize link-state databases and form FULL neighbor adjacency.

**Step 4:** On R2, verify the OSPF neighbor state using the show ip ospf neighbor detail command.

R2# show ip ospf neighbor detail



The output of the show ip ospf neighbor detail command confirms that full OSPF adjacency with R1 is established. The output also shows additional information regarding the neighbor router ID and how long the neighbor session has been established. Notice that since OSPF is treating this interface as network type POINT-TO-POINT, the neighbor priority is automatically set to 0, and the DR and BDR addresses are set to 0.0.0.0.