# Implementing OSPF in Cisco IOS



# Introduction

OSPF is an open standard link-state IP routing protocol defined by RFC 2328. OSPF is classified as an Interior Gateway Protocol routing within a single autonomous system. As a link-state routing protocol, a router running OSPF compiles a database of all the destinations throughout the network, how they are connected and the cost of the links. This database is the same on all routers in the OSPF network. Each router independently determines their best path to the destinations in this database.

OSPF uses IP protocol number 89. OSPF is its own transport layer protocol. The current versions of OSPF are OSPFv2 that supports IPv4 and OSPFv3 that supports IPv4 and IPv6. The two versions of OSPF are not compatible i.e., routers running OSPFv3 cannot form an IPv4 adjacency with routers running OSPFv2. To configure OSPF issue the global config mode command **`router ospf`** ***`process_id`*** where process_id is a value between 1 - 65535:

```
R1#configure terminal
R1(config)#router ospf 1
```

The process ID does not have to match on any of the routers in the OSPF domain.

For a router to learn and exchange routes with other OSPF routers in the same autonomous system, the router transitions through various stages to present accurate routing information to the global/VRF routing information base (RIB) or routing table. These stages include:

- **Step 1 - Neighbor Adjacency:** involves the discovery of neighbors and formation of neighbor relationships known as adjacencies. Once formed, the adjacent neighbors exchange all their learned routes.

- **Step 2 - Best Path Selection:** each router creates a local database of learned routes, known as the Link-State Database (LSDB). Using the information from the LSDB, OSPF generates a shortest path first tree (SPT) in which the local router is at the root of the tree. The shortest path to each node in the tree is determined and then presented to the global RIB for installation.
- **Step 3 - Neighbor and Topology Maintenance:** each router continually monitors the state of its neighbors and their links to ensure that its knowledge of the network is up-to-date.

# OSPF Neighbor Adjacency

## Adjacency Preconditions

For OSPF routers to exchange route information they need to become adjacent. For the routers to become adjacent, some preconditions must be met:

1. **Unique Router ID (RID):** The router ID is a value used to uniquely identify an OSPF-enabled router in the OSPF domain. The RID is usually in the form of an IPv4 address. The RIDs of the two routers must be unique. If a router has more than one OSPF process, then the RID for each OSPF process on the router must be unique. By default, the RID is determined automatically using the following method:
    a. Highest IPv4 address of any loopback interface.
    b. Highest IPv4 address of any physical interface if no loopback interfaces are configured with IPv4 addresses.

    The RID does not change until the OSPF process restarts. The RID can also be manually configured using the OSPF router mode command: **`router-id`** ***`router-id`***.

    The RID can be viewed using most OSPF **`show`** commands:

```
R1#show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Start time: 00:00:32.764, Time elapsed: 00:29:01.924
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border and autonomous system boundary router
Redistributing External Routes from,
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
..... .
```

2. **Interfaces must be OSPF active (in an Up state):** The interface through-which the adjacency is to be formed must have OSPF enabled on it and must not be in an OSPF passive state.
3. **Common Subnet:** Interfaces must share a common subnet on the primary IP address. By default, OSPF advertises the secondary IP address of an interface if it is enabled in the OSPF router mode or interface mode.
    **Note:** This precondition for a common subnet between potential OSPF neighbors

does not exist for OSPFv3 as IPv6 implementation does not require a common subnet. In OSPFv3, communicates using link local addresses.

4. **MTU:** Interface MTU must match. The default MTU is 1500. OSPF can be configured to ignore this precondition using the interface mode command: **`ip ospf mtu-ignore`**.

```
R1(config)# interface g0/0
R1(config-if)#ip ospf mtu-ignore
```

   However, ignoring MTU checks is not recommeded in production networks.

   **Troubleshooting Tip:** If a neighborship formation stops at EXSTART phase, then it is probable that the IP MTUs are mismatched.

5. **Need for a DR for the segment must match (OSPF network type):** The broadcast and non-broadcast OSPF network types require a Designated Router (DR) while the point-to-point and point-to-multipoint network types do not require a DR. This requirement or non-requirement of a DR must match on the interfaces of the two routers for them to form an adjacency.
6. **Matching Hello and Dead-interval timers:** Unlink EIGRP, with OSPF, the Hello timer and dead-interval timer values must match. A Hello packet is initially used for establishment of a neighbor relationship. After establishment of the neighbor relationship, the Hello packet acts as a kind of heartbeat; to prove presence of the neighbor. By default, it is 10 seconds on Ethernet networks. The dead-interval timer is used to determine when a neighbor can be considered as being down. By default, it is 40 seconds on Ethernet networks.
7. **Matching Authentication Type and Credentials:** OSPF supports null authentication, simple password authentication and the use of MD5 and SHA authentication. The authentication type must match as well as the password. If SHA authentication is configured, then the SHA type must match in addition to the key ID and password.
8. **Same Area ID:** An OSPF area is segregation of an OSPF domain. Each area is identified by the area ID value. Area ID for the segment must match.
9. **Matching Areas:** Area type flags must match i.e. whether normal, stubby or Not-So-Stubby Area(NSSA).
10. **Version:** The OSPF versions OSPv2 and OSPFv3 are not compatible. As a result, the OSPF versions in use in the network must be the same.

# OSPF Packet Types

OSPF uses five types of packets: Hello, Database Description (DBD), Link State Request (LSR), Link State Update (LSU), Link State Acknowledgement (LSAck). The Hello packet is used to communicate with neighbors and establish and maintain relationships with them. The other packet types are used to exchange link-state database information and to form adjacencies between each of these different participating devices. Together, these packets ensure that the information in the neigbor table and the LSDB is accurate and regularly updated.

OSPF routers exchange prefix information using unicast, multicast packets or both depending on the OSPF network type. If multicast packets are used, the OSPF multicast destination addresses used are:

- **AllSPFRouters** `224.0.0.5` with MAC address `01:00:5E:00:00:05`: All OSPF-enabled routers process packets arriving at the multicast address 224.0.0.5.
- **AllDRouters** `224.0.0.6` with MAC address `01:00:5E:00:00:06`. Only the DR and BDR process packets arriving at the multicast address 224.0.0.6

## OSPF Header

All OSPF packet types contain an OSPF header. This header contains information that is common to all OSPF packet types and is communicated between devices. The header contains the following fields:

- **Version:** version 2 for OSPv2 and 3 for OSPFv3.
- **Message Type:** type of OSPF packet. Hello packets have the value of 1.
- **Packet Length:** length of the packet.
- **Router ID:** used to uniquely identify a router in OSPF domain.
- **Area ID:** areas are used to define a hierarchy and control the size of the flooding domain.
- **Checksum:** Ensures integrity of the packet.

## Hello Packet

Hello packet (OSPF packet type 1) is sent out an OSPF device's enabled interfaces to announce the router's presence on a link/segment and its neighborship adjacency prerequisite conditions. The Hello packet is used for establishment and maintenance of neighborships.

It contains the following fields:

- **Network mask:** contains the subnet mask that is configured on the interface. OSPF uses this value to determine if the different devices are on the same subnet.
- **Hello Interval:** indicates the amount of time that goes by between the Hello packets. Acts as a keepalive between neighbors. It is usually ten (10) seconds on Ethernet networks.
- **Options:** communicates the different options that are supported by a device. It contains information that is used to determine whether a potential neighborship could be formed.
- **Priority:** Used together with the DR and BDR fields to determine which of the devices on a shared network becomes the DR and potentially BDR. Once selected, their IP addresses are populated into these fields.
- **Dead Interval:** used together with the Hello interval to determine whether a device has a problem and how much time is required before a device is considered down. The dead interval resets each time a Hello packet is received from a neighbor. If no Hello packets are received, by the time the dead Interval expires, then the neighborship is dropped, the SPF tree is recalculated and flooding takes place
- **Active Neighbor:** contains the list of devices that have successfully formed a neighborship with the local device i.e. a bi-directional relationship was established.

## Database Descriptor Packet (DBD/DDP)

DBD is used to share summaries of the LSDB. A device uses the DBD to communicate the summary of link-state information that it knows about. This is not the detailed link-state information itself but a summary of the known information. If the DBD packet from a neighbor contains information that the device does not have, the local device requests for additional information using a link-state request packet.

The DBD packet contains the following fields:

- **Interface MTU:** indicates the largest-sized IP datagram that is allowed on a link. It is one of the fields that must match between potential neighbors.
- **Options:** Relays the same information as in the Hello packet specifically, device capability information.
- **I,M, and MS bits:** Used to communicate the flow of information between neighbors:
    i. **I (Init bit):** indicates that this is the first bit in a series.
    ii. **M (More):** indicates that there are DBD packets coming.
    iii. **MS (Master-Slave):** indicates which of the devices becomes the master of the neighbors and controls the exchange of database information. When the MS bit is set to 1, a device believes that it becomes the master.
- **Sequence:** Used by devices to ensure the correct ordering of information between them. The determined master controls the sequence that will be used.
- List of known information that a device knows about.

## Link-State Request (LSR) Packet

The LSR packet is used to request for additional information on specific networks from neighbors. The LSR is usually sent when the router receives a DBD packet from a neighbor and it does not have some or all of the prefixes advertised in the DBD in its LSDB.

After exchange of DBD packets, OSPF peers become aware of the information that each knows about but not the specific information. To retrieve the details, the peers use a combination of LSR, LSU, LSAck packets.

The LSR packet contains the following fields:

- **Link State Type:** First field indicates the type of information that is being requested from a neighbor by referencing a specific LSA type.
- **Link State ID:** ID of the specific advertisement being requested. Allows the neighbor to know what specific information is being requested.
- **Advertising Router:** RID of the original OSPF device that advertised that it had the information being requested.

## Link-State Update (LSU) Packet

The link state update packet (OSPF packet type 4) contains details on one or more networks and is usually sent in response to an LSR. This packet type is the envelop into which OSPF's Link-State Advertisements(LSAs) are enclosed in. An LSU can contain one or many LSAs.

LSU is sent in response to an LSR. It contains two fields:

- **Number of LSA's:** Lists the number of LSAs that are included with the update.
- **LSA's:** contains all the LSA information. This field can be repeated.

OSPF packets containing prefix information are referred to as **Link-State Advertisements (LSAs)**. LSAs contain prefixes and their associated metric and are sent to neighboring routers. LSAs are stored, unaltered, in a local link-state database in the form in which the originating router sent them. All routers in the same area have identical LSDBs for that area. The Shortest Path Tree (SPT) differs for each router as each sees itself at the root of the SPT.

### Link-State Acknowledgement(LSAck) Packet

The link-state acknowledgement packet (OSPF packet type 5) is sent in response to an LSR and LSU. It contains the sequence number of the LSU/LSR that it is acknowledging. It is used to acknowledge receipt of requested information from LSR and LSU packets. Its format is similar to DBD packet type.

## Advertising Networks

For OSPF to advertise connected networks, it has to be enabled on the interfaces where the networks to be advertised have been configured. The area that the network will be resident in has to be added to the configuration. A network can only reside in one area. This can be done in two ways:

1. **Network statement:** using the OSPF router mode command **`network`** ***`network_address wild-card`*** **`area`** ***`area_id`***. A wild card mask is an inverse of the subnet mask. It allows one to be as general or as specific as possible.
```
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 10.10.0.0 0.0.255.255 area 0
```
It is possible to add all interfaces using a single **`network`** command. The following snippet adds all interfaces with a configured IP address to area 0.
```
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
```
2. **Interface command:** OSPF is enabled directly on the interface whose network is to be advertised. OSPF interface statement enables OSPF on the primary and secondary IP addresses. Advertisement of the secondary IP address can be disabled by addition of the **`secondaries none`** keyword. If the interface IP address is subsequently changed, the new IP address will still be automatically advertised without any further configuration.
```
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface g1/0
R1(config-if)# ip ospf 1 area 0
```

To view the OSPF configuration including interfaces on which OSPF has been activated on

including how OSPF was activated on the networks:

```
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 1.1.1.1
   It is an area border and autonomous system boundary router
  Redistributing External Routes from,
   Number of areas in this router is 2. 1 normal 0 stub 1 nssa
   Maximum path: 4
  Routing for Networks:
   10.0.12.1 0.0.0.0 area 0
  Routing on Interfaces Configured Explicitly (Area 0):
   FastEthernet3/0
  Routing on Interfaces Configured Explicitly (Area 10):
   GigabitEthernet1/0
  Routing Information Sources:
   Gateway Distance Last Update
   6.6.6.6 110 00:32:45
   2.2.2.2 110 00:32:45
  Distance: (default is 110)
R1#
```

# OSPF Adjacency States

OSPF neighbor adjacencies transition through up to eight states (depending on the network type). In some OSPF network types, the number of stages may be less: DOWN, ATTEMPT, INIT, 2WAAY, EXSTART, EXCHANGE, LOADING, FULL.

1. **DOWN:** Initial state of any neighborship. It indicates that no OSPF packets have been sent to or received from any neighbor. In this state, no hello packets have been received from a neighbor. Additionally, the OSPF-enabled interface of the local router may be shutdown.
2. **ATTEMPT:** A unicast hello packet has been sent to a neighbor but no hello packet has been received back. This state applies to an OSPF neighborship that is manually configured using the OSPF process command **`neighbor 10.2.3.4`** in NBMA environments.
3. **INIT:** A hello packet has been received from the neighbor but no bi-directional relationship has been established. The neighbor has not yet acknowledged the local router as a neighbor by including its RID in its hello packet header's 'Active Neighbor' field.
4. **2-WAY:** Hello received from neighbor and neighbor has acknowledged the local router as a neighbor by including the local router RID in its 'Active Neighbor' field of the hello packet header.
    - In **broadcast and non-broadcast** networks, DROther routers complete their adjacency formation with each other at the 2-Way stage.
    - **Election of the DR/BDR roles is also started**. The router with the highest priority becomes master during DR election. If there is a tie, then the router with the highest RID becomes the DR.
    - **Need for adjacency determined:** the need for an adjacency is determined and

whether the formation of an adjacency is also possible.
    - At this point, no link-state information has been exchanged yet.
5. **EXSTART:** This state is reached by devices that have determined that they need to reach the FULL state of adjacency.
    - Devices begin the process to exchange complete link-state information.
    - The master/slave relationship is developed with the master being the router with the higher RID. The interface priority is not used in the determination of the master/slave relationship.
    - The master controls aspects of the adjacency formation by choosing the starting sequence number for the database descriptor packets (DDP or DBD) that are used for actual exchange.
    - The master is the only device that is permitted to retransmit database descriptor packets.
    - The slave only sends acknowledgements for the DBD packets received from the master. These packets contain the matching link-state sequence number of the packets from the master.
    - The master/slave role applies only to the local network connection between the two neighbors and does not influence the DR/BDR/DROther roles.
6. **EXCHANGE:** DDP or DBD packets are sent in unicast. A summary of the LSDB is exchanged through DBD packets. DBD sequence number is used for reliable acknowledgment / re-transmission.
    - Link-state information is compared between devices.
    - Database descriptor packets are used to relay link state lists.
    - If no new information is required from the neighbor, the state transitions to the FULL state.
    - If new information will be added to the request list, then this list is sent to the neighbor and the device transitions to LOADING.
7. **LOADING:** LSRs are sent requesting for additional information about particular LSAs that the local router does not have. Unicast LSUs are sent for missing links.
8. **FULL:** LSDBs of the routers are fully synchronized.
    - Hello packets are exchanged until a network change occurs.
    - In OSPF network types requiring the presence of DR and BDR:
        - All DROthers reach the FULL state only with the DR and BDR.
        - DROthers remain at the 2WAY state with each other.
        - DR and BDR reach FULL state with each other.

To view the OSPF adjacency stages in real-time, run the privileged-exec command **`debug ospf adj`**:

```
R1#debug ip ospf adj
OSPF adjacency debugging is on
R1#
*Aug 11 20:39:07.311: OSPF-1 ADJ Gi0/0: Send with youngest Key 0
*Aug 11 20:39:07.375: OSPF-1 ADJ Gi0/0: 2 Way Communication to 2.2.2.2, state 2WAY
*Aug 11 20:39:07.375: OSPF-1 ADJ Gi0/0: Neighbor change event
*Aug 11 20:39:07.375: OSPF-1 ADJ Gi0/0: DR/BDR election
*Aug 11 20:39:07.379: OSPF-1 ADJ Gi0/0: Elect BDR 2.2.2.2
*Aug 11 20:39:07.379: OSPF-1 ADJ Gi0/0: Elect DR 1.1.1.1
*Aug 11 20:39:07.379: OSPF-1 ADJ Gi0/0: DR: 1.1.1.1 (Id) BDR: 2.2.2.2 (Id)
*Aug 11 20:39:07.383: OSPF-1 ADJ Gi0/0: Nbr 2.2.2.2: Prepare dbase exchange
```

```
*Aug 11 20:39:07.387: OSPF-1 ADJ Gi0/0: Send DBD to 2.2.2.2 seq 0x24C9 opt 0x52 flag 0x7 len 32
*Aug 11 20:39:07.387: OSPF-1 ADJ Gi0/0: Send with youngest Key 0
*Aug 11 20:39:07.391: OSPF-1 ADJ Gi0/0: Neighbor change event
*Aug 11 20:39:07.391: OSPF-1 ADJ Gi0/0: DR/BDR election
*Aug 11 20:39:07.391: OSPF-1 ADJ Gi0/0: Elect BDR 2.2.2.2
*Aug 11 20:39:07.395: OSPF-1 ADJ Gi0/0: Elect DR 1.1.1.1
*Aug 11 20:39:07.395: OSPF-
R1#1 ADJ Gi0/0: DR: 1.1.1.1 (Id) BDR: 2.2.2.2 (Id)
*Aug 11 20:39:07.399: OSPF-1 ADJ Gi0/0: Neighbor change event
*Aug 11 20:39:07.399: OSPF-1 ADJ Gi0/0: DR/BDR election
*Aug 11 20:39:07.403: OSPF-1 ADJ Gi0/0: Elect BDR 2.2.2.2
*Aug 11 20:39:07.403: OSPF-1 ADJ Gi0/0: Elect DR 1.1.1.1
*Aug 11 20:39:07.403: OSPF-1 ADJ Gi0/0: DR: 1.1.1.1 (Id) BDR: 2.2.2.2 (Id)
*Aug 11 20:39:07.411: OSPF-1 ADJ Gi0/0: Rcv DBD from 2.2.2.2 seq 0x22D5 opt 0x52 flag 0x7 len
32 mtu 1500 state EXSTART
*Aug 11 20:39:07.411: OSPF-1 ADJ Gi0/0: NBR Negotiation Done. We are the SLAVE
*Aug 11 20:39:07.415: OSPF-1 ADJ Gi0/0: Nbr 2.2.2.2: Summary list built, size 2
*Aug 11 20:39:07.415: OSPF-1 ADJ Gi0/0: Send DBD to 2.2.2.2 seq 0x22D5 opt 0x52 flag 0x2 len 72
*Aug 11 20:39:07.419: OSPF-1 ADJ Gi0/0: Send with youngest Key 0
*Aug 11 20:39:07.531: OSPF-1 ADJ Gi0/0: Rcv DBD from 2.2.2.2 seq 0x22D6 opt 0x52 flag 0x1 len
52 mtu 1500 state EXCHANGE
*Aug 11 20:39:07.531: OSPF-1 ADJ Gi0/0: Exchange Done with 2.2.2.2
*Aug 11 20:39:07.535: OSPF-1 ADJ Gi0/0: Send with youngest Key 0
*Aug 11 20:39:07.535: OSPF-1 ADJ Gi0/0: Send LS REQ to 2.2.2.2 length 36 LS
R1#A count 1
*Aug 11 20:39:07.539: OSPF-1 ADJ Gi0/0: Send DBD to 2.2.2.2 seq 0x22D6 opt 0x52 flag 0x0 len 32
*Aug 11 20:39:07.539: OSPF-1 ADJ Gi0/0: Send with youngest Key 0
*Aug 11 20:39:07.643: OSPF-1 ADJ Gi0/0: Rcv LS UPD from 2.2.2.2 length 88 LSA count 1
*Aug 11 20:39:07.647: OSPF-1 ADJ Gi0/0: Synchronized with 2.2.2.2, state FULL
*Aug 11 20:39:07.647: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/0 from LOADING
to FULL, Loading Done
*Aug 11 20:39:07.651: OSPF-1 ADJ Gi0/0: Rcv LS REQ from 2.2.2.2 length 48 LSA count 2
```

# Neighbor Table

A router running OSPF builds and maintains two data structures or databases from which it develops an accurate picture of the network: neighbor table and link-state database (LSDB).

The OSPF neighbor table contains directly connected neighbors that share network information. To view the neighbor table, issue the commands in the following sections. Below are the interface IP addresses of the local OSPF device:

```
R1#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.255.1.5      YES manual up                    up
GigabitEthernet1/0         10.255.254.1    YES NVRAM  up                    up
GigabitEthernet2/0         10.255.1.1      YES NVRAM  up                    up
FastEthernet3/0            10.255.1.33     YES NVRAM  up                    up
GigabitEthernet4/0         10.255.254.13   YES NVRAM  up                    up
```

**show ip ospf neighbor**

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.9           1   FULL/BDR        00:00:32    10.255.1.6      GigabitEthernet0/0
2.2.2.2           1   FULL/DROTHER    00:00:32    10.255.1.34     FastEthernet3/0
3.3.3.3           1   FULL/DROTHER    00:00:33    10.255.1.35     FastEthernet3/0
9.9.9.9           1   FULL/BDR        00:00:39    10.255.1.36     FastEthernet3/0
2.2.2.2           1   FULL/BDR        00:00:39    10.255.1.2      GigabitEthernet2/0
7.7.7.7           1   FULL/BDR        00:00:31    10.255.254.2    GigabitEthernet1/0
10.10.10.10       1   FULL/BDR        00:00:33    10.255.254.14   GigabitEthernet4/0
```

From the output, the following can be learned:

- **Neighbor ID:** The RID of the neighbor. From the command output, it can be noted that the local OSPF router has formed a neighborship with neighbors with RID 9.9.9.9 and 2.2.2.2 over two interfaces.
- **Pri:** the priority of the interface of the neighbor through which this neighbor relationship was formed.
- **State:** Adjacency state and DR/BDR/DROTHER role of the neighbor on the link. On links that do not require formation of DR/BDR, this field is blank.
- **Dead time:** Count-down timer to zero (0). This value gets reset to the value of the dead-interval timer when a Hello packet is received. On an Ethernet link with default dead-interval and hello timer values, the dead time value will range from 31 - 39.
- **Address:** IP address of the interface of the neighbor through which this neighborship was formed.

**`show ip ospf neighbor` *`RID`***

The command **`show ip ospf neighbor` *`RID`*** can be used to view details of the neighborship that a router has with its neighbor.

```
R1#show ip ospf neighbor 2.2.2.2
Neighbor 2.2.2.2, interface address 10.255.1.34
   In the area 0.0.0.0 via interface FastEthernet3/0
   Neighbor priority is 1, State is FULL, 6 state changes
   DR is 10.255.1.33 BDR is 10.255.1.36
   Options is 0x12 in Hello (E-bit, L-bit)
   Options is 0x52 in DBD (E-bit, L-bit, O-bit)
   LLS Options is 0x1 (LR)
   Dead timer due in 00:00:37
   Neighbor is up for 05:50:19
   Index 1/1, retransmission queue length 0, number of retransmission 1
   First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
   Last retransmission scan length is 1, maximum is 1
   Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 2.2.2.2, interface address 10.255.1.2
   In the area 0.0.0.0 via interface GigabitEthernet2/0
   Neighbor priority is 1, State is FULL, 6 state changes
   DR is 10.255.1.1 BDR is 10.255.1.2
   Options is 0x12 in Hello (E-bit, L-bit)
   Options is 0x52 in DBD (E-bit, L-bit, O-bit)
   LLS Options is 0x1 (LR)
   Dead timer due in 00:00:37
   Neighbor is up for 05:49:56
   Index 2/2, 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
R1#
```

From the above output, the following information can be learned about the neighborship:

- **Interfaces through which neighborship was formed:** Router R1 has formed a neighborship with OSPF device with RID 2.2.2.2 over two interfaces FastEthernet3/0 and GigabitEthernet2/0.
- **Duration of the neighborship:** In this instance, the neighborship has been up for 5 hours and 50 minutes through the interface FastEthernet3/0 and 05 hours and 49

minutes via interface GigabitEthernet2/0.
- **DR/BDR/DROther role:** on broadcast and non-broadcast networks that require a DR/BDR, the role or the OSPF neighbor can be learned. In this instance, the local device is a DR on network segment through interface FastEthernet 3/0 and GigabitEthernet2/0.
- **Options:** options have been set on the Hello packets and DBD packets:
  - **E-bit:** the neighbor is capable of redistribution.
  - **L-bit:** the neighbor has enabled LLS (link-local signaling). LLS allows for the extension of existing OSPF packets in order to provide additional bit space. The additional bit space enables greater information per packet exchange between OSPF neighbors. This functionality is used, for example, by the OSPF Nonstop Forwarding (NSF) Awareness feature that allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. With the LLS option enabled, the LLS data block contains NSF relevant options. In this instance, the neighbor 2.2.2.2 has enabled LSDB Resynchronization (LR) enabled on both interfaces. NSF is discussed in some detail in the subsequent sections.
- **Priority:** the neighbor 2.2.2.2 priority is set to 1 (default) on both interfaces.

**`show ip ospf neighbor`** ***`interface-id`***

The above command is used to view the neighborships formed through the specified interface. The optional **`detail`** keyword can be appended to the command to view detailed OSPF related information regarding the neighbor.

```
R1#show ip ospf neighbor FastEthernet3/0

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DROTHER    00:00:38    10.255.1.34     FastEthernet3/0
3.3.3.3           1   FULL/DROTHER    00:00:31    10.255.1.35     FastEthernet3/0
9.9.9.9           1   FULL/BDR        00:00:35    10.255.1.36     FastEthernet3/0
```

# OSPF Media Dependencies and Network Types

Different network types are defined to deal with different media characteristics. Network types control:

- How hello packets and updates are sent.
- Who forms an adjacency
- How the next-hop is calculated.

The OSPF network type does not need to match to form an adjacency but it does need to be compatible such as a common need for a DR/BDR for the segment. Other attributes have to match such as timer values. OSPF network types include the following:

- **Broadcast networks:** default network type on multi-access broadcast media such as ethernet. Supports dynamic neighbor discovery. This network type requires the election of a designated router (DR) and back-up designated router (BDR). Hello and LSU packets from DROthers are sent as multicast to 224.0.0.6 (AllDRouters) and with

destination MAC address. 01:00:5E:00:00:06. The DR and BDR process packets sent to this address. The DR acknowledges the packet with an LSAck and sends a multicast update to all other routers AllSPFRouters with a destination address of 224.0.0.5 and MAC address 01:00:5E:00:00:05. In broadcast networks, the hello interval is 10 seconds, dead interval 40 seconds, wait time 40 seconds.
- **Nonbroadcast:** Default on NBMA networks such as frame-relay, DMVPN topologies. Interfaces do not support broadcast or multicast as a result, dynamic neighbor discovery is not supported. Neighbors are manually configured using the router OSPF command **`neighbor neighbor_ip_address`**. Hello packets are therefore sent in unicast. Information flooding is not supported DR and BDR election is required for this network type. The hello interval is 30 seconds, dead-interval 120 seconds, wait timer 120 seconds. A DR decreases the exchanges required.
- **Point-to-point:** default on point-to-point media such as HDLC, PPP, GRE. Supports dynamic neighbor discovery with Hello packets sent in multicast to address 224.0.0.5. Supports only two neighbors on the link. The hello interval is 10 seconds, dead interval 40 seconds. A DR and BDR election is not required for this network.
- **Point-to-multipoint:** Typically used on a spoke-hub topology. This network type can be treated as a collection of point-to-point links. It assumes that all the devices on the shared network are individually reachable to each other essentially like an Ethernet network lacking broadcast capability. Supports dynamic neighbor discovery. Hello packets are sent to multicast address 224.0.0.5. Special next-hop processing takes place with the next hop being set to the neighbor's IP address that sent the LSU. Point-to-multipoint network type is usually the best design option for partial mesh NBMA networks. In point-to-multipoint networks, the interface's IP address is advertised as /32 host route. Point-to-multipoint is not a default for any medium type. The hello interval is 30 seconds, dead-interval 120 seconds. DR and BDR election does not happen in this network type.
- **Point-to-multipoint Non-Broadcast:** Same as point-to-multipoint but sends Neighbors are manually defined using the router OSPF command **`neighbor neighbor_ip_address`** resulting in Hello packets being sent in unicast. Allows for per-VC OSPF cost over NBMA. Special next-hop processing.
- **Loopback:** Special case for loopback and looped-back interfaces. Advertises link with /32 subnet mask as a host route. The Hello timer is 30 seconds and dead-interval timer is 120 seconds.

The use/non-use of LSA Type 2 determines whether OSPF network types can be compatible or not. Network types that use Type 2 LSAs include: broadcast and non-broadcast. Others do not.

The OSPF network type of an interface can be changed from its default using the interface mode command: **`ip ospf network network_type.`** **`network_type`** can be either of: broadcast, non-broadcast, point-to-point, point-to-multipoint.

```
R1(config)#interface fa3/0
R1(config-if)#ip ospf network point-to-point
R1(config-if)#do show ip ospf interface fa3/0
FastEthernet3/0 is up, line protocol is up
  Internet Address 10.0.16.1/30, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
```

```
...
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 250 msec, Dead 1, Wait 1, Retransmit 5
  oob-resync timeout 40
  Hello due in 73 msec
```

Broadcast networks with only two OSPF peers can be configured to point-to-point network type. This makes the adjacency complete faster eliminating the unnecessary DR/BDR election and OSPF Type 2 LSA advertisements.

## OSPF Interfaces

To view interfaces on which OSPF has been activated i.e., interfaces whose IP addresses or networks are being advertised by OSPF, issue the following commands:

**`show ip ospf interface brief`**

The **`brief`** keyword formats the output to display a list of the interfaces that on which OSPF is enabled.

```
R4#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo1          4     0.0.0.0         10.1.1.1/24        1     LOOP  0/0
Lo2          4     0.0.0.0         10.1.2.1/24        1     LOOP  0/0
Lo3          4     0.0.0.0         10.1.3.1/24        1     LOOP  0/0
Lo4          4     0.0.0.0         10.1.4.1/24        1     LOOP  0/0
Fa3/0        4     0.0.0.0         10.255.1.27/29     1     BDR   3/3
Gi1/0        4     0.0.0.0         10.255.1.10/30     1     DR    1/1
```

From the above output the following is displayed:

- **Interface:** the interface name on which OSPF is enabled.
- **PID:** the OSPF process ID under which the interface network is being advertised. An interface can only operate under one OSPF process. Advertising the network in which the interface resides in another OSPF process Y results in the interface being assigned to the OSPF process Y.
- **Area:** the area that the interface is assigned to. In this instance, all interfaces are in the backbone area.
- **IP Address/Mask:** the interface IP address and subnet mask.
- **Cost:** the metric cost. The cost is calculated using the formula $\text{reference bandwidth} \div \text{interface bandwidth}$ The default reference bandwidth value is 100mbps
- **State:**
- **Nbrs F/C:** Neighborships configured on that interface and those that are in the FULL adjacency state.

**NOTE:** When viewing interfaces, the command **`show ip ospf interface`** displays all interfaces whether passive or active.

**`show ip ospf interface`**

```
R4#show ip ospf interface
```

```
Loopback2 is up, line protocol is up
  Internet Address 10.1.2.1/24, Area 0.0.0.0, Attached via Network Statement
  Process ID 4, Router ID 4.4.4.4, Network Type LOOPBACK, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
        0 1 no no Base
  Loopback interface is treated as a stub Host
Loopback3 is up, line protocol is up
  Internet Address 10.1.3.1/24, Area 0.0.0.0, Attached via Network Statement
  Process ID 4, Router ID 4.4.4.4, Network Type LOOPBACK, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
   0 1 no no Base
  Loopback interface is treated as a stub Host
Loopback4 is up, line protocol is up
  Internet Address 10.1.4.1/24, Area 0.0.0.0, Attached via Network Statement
  Process ID 4, Router ID 4.4.4.4, Network Type LOOPBACK, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
   0 1 no no Base
  Loopback interface is treated as a stub Host
Loopback1 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0.0.0.0, Attached via Interface Enable
  Process ID 4, Router ID 4.4.4.4, Network Type LOOPBACK, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
   0 1 no no Base
  Enabled by interface config, including secondary ip addresses
  Loopback interface is treated as a stub Host
FastEthernet3/0 is up, line protocol is up
  Internet Address 10.255.1.27/29, Area 0.0.0.0, Attached via Interface Enable
  Process ID 4, Router ID 4.4.4.4, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
   0 1 no no Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 5.5.5.5, Interface address 10.255.1.28
  Backup Designated router (ID) 2.2.2.2, Interface address 10.255.1.25
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 10
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 3, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
    Adjacent with neighbor 5.5.5.5 (Designated Router)
  Suppress hello for 0 neighbor(s)
GigabitEthernet1/0 is up, line protocol is up
  Internet Address 10.255.1.10/30, Area 0.0.0.0, Attached via Interface Enable
  Process ID 4, Router ID 4.4.4.4, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
   0 1 no no Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.255.1.9
  Backup Designated router (ID) 4.4.4.4, Interface address 10.255.1.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 7
```

```
  Last flood scan time is 4 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2 (Designated Router)
  Suppress hello for 0 neighbor(s)
R4#
```

The following can be learned about the configuration and operational mode of OSPF interfaces:

- OSPF network type
- Cost on the interface
- How the OSPF was enabled on the interface i.e., through the interface mode command **`ip ospf *process-id* area *area-id*`** or using the OSPF router mode command **`network *network-address wilcard* area *area-id* .`**
- OSPF process ID that the interface is associated with.
- Hello and dead-interval timer values.
- Non-stop forwarding (NSF) support. Additionally, link-local signaling support is confirmed.
- IP addresses of the DR and BDR on that segment for broadcast and nonbroadcast OSPF network types.
- Number of adjacencies created through the interface.
- OSPF priority for the interface.
- The flood queue length.
- Number of Hello packets suppressed from neighbors.

# Hello and Dead Interval Timers

The hello interval and dead intervals can be modified to values different from the default values. In gigabit-ethernet networks, hello intervals of 10 seconds are rather long. They can be reduced to shorter durations of say 5 seconds:

```
R1(config)#interface Te3/0
R1(config-if)#ip ospf hello-interval 5
```

The dead interval is automatically modified to four times the value of the hello-interval.

OSPF Hello packets can be sent in sub-seconds using the interface command **`ip ospf dead-interval minimal hello-multiplier *multiplier*`**. The ***`multiplier`*** is the number of hello packets sent per second;

```
R1(config)#interface fa3/0
R1(config-if)#ip ospf dead-interval minimal hello-multiplier 4
R1(config-if)#end
R1#show ip ospf interface fa3/0
FastEthernet3/0 is up, line protocol is up
Internet Address 10.0.16.1/30, Area 0, Attached via Interface Enable
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST , Cost: 1
. . . .
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 10.0.16.1
No backup designated router on this network
Timer intervals configured, Hello 250 msec, Dead 1, Wait 1, Retransmit 5
oob-resync timeout 40
```

```
Hello due in 58 msec
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
.....
R1#
```

Where 4 implies four hello packets are to be sent per second.

BFD is a more optimum option to OSPF sub-second OSPF hello intervals. BFD is more light-weight.

# Designated Router(DR)and Backup Designated Router(BDR)

If multiple routers in multi-access networks are to form adjacencies, the total number of adjacencies established is determined by the formula: `Total = n * (n - 1)/2`. All these routers will be sending hello and update packets to each and every one of them. In order to reduce the number of adjacencies (and OSPF packets) on a segment in a multi-access network, OSPF elects one router to be a designated router and another to act as a backup designated router to replace the designated router in case of its failure.

Additionally, the SPF algorithm calculates paths based on the point-to-point links. In a neighbor relationship that contains more than two OSPF peers, a pseudonode is elected. The pseudonode is a virtual network node that forms point-to-point relationships with all the other devices on that node. It acts as central point forming multiple virtual point-to-point links with all the OSPF peers on that node. These virtual links have a cost of zero(0) so that they do not alter the cost of the physical link.

The BDR takes over the responsibilities of the DR should there be a problem.

## DR/BDR Election

A router initialising OSPF on an interface waits the duration of the wait timer listening for the presence of other OSPF routers announcing their DR status before declaring its DR status (if more favourable). In broadcast networks, the wait timer is 40 seconds, non broadcast networks, 120 seconds. DR election is based on interface priority and router ID (RID). Usually, the first router to initialize OSPF on an interface within a given number of seconds on a segment becomes the DR regardless of its interface priority or RID. OSPF deems a router more preferrable for DR if:

1. The interface of the router has the highest priority for that segment. The priority is any value between 1 - 255. The default priority is one (1).
2. The router has the highest OSPF RID in that segment. The RID of a router is determined by:
    i. if configured, the highest IP address configured on any "up" loopback interfaces.
    ii. the highest physical interface IP address
    iii. manual configuration of the RID using the OSPF process command: **`router-id`** ***`rid`***

Unlike BGP, the OSPF RID is not a routable address. It is possible to have a valid RID such as

255.255.255.255

The interface priority is a value from 1 to 255 inclusive. To change the router interface priority to 200:

```
R1(config)#interface g0/0
R1(config-if)#ip ospf priority ?
<0-255> Priority
R1(config-if)#ip ospf priority 200
R1(config-if)#do show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.0.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
   ....
  Transmit Delay is 1 sec, State BDR, Priority 200
```

A value of zero makes the router ineligible for DR/BDR election.

The DR and BDR roles can not be preempted by a router with higher interface priority or RID values. The election of a DR/BDR can be forced by clearing the OSPF process. This can be done using the following command:

```
R1#
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R1#
*Aug 11 22:03:11.495: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
*Aug 11 22:03:11.767: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/0 from LOADING
to FULL, Loading Done
```

## DR Operation

A DR is used in broadcast and non-broadcast networks and its primary role DR is:

- it orignitates information for the shared network.
- It facilitates synchronization

A DR controls information exchange.

A Designated Router forms a FULL adjacency with all routers on the link. The other routers (DROthers) form 2-WAY adjacencies with each other. The BDR forms FULL adjacencies with all other routers as well. The DR listens for LSUs on the multicast address 224.0.0.6. A router (DROther) with an update sends it to the multicast address 224.0.0.6. After receiving an LSU, the DR sends a unicast LSAck to that router to acknowledge receiving the update. The DR then floods the LSU(s) to the segment using 224.0.0.5. The DR does not modify the next-hop value of this LSU. The BDR is used for redundancy. It does not flood any updates but receives all updates sent to the DR.

The use of a DR can be inefficient if only two devices are connected in a segment. On networks that require DR operation (such as broadcast) and only two devices are present, it may be more efficient to statically configure the interfaces with a network type that does not require a DR for example a P2P network type.

## Link State Advertisements (LSAs)

LSAs are pieces of information that are stored within the LSDB. Multiple types of LSAs exist and the ones used depend on the OSPF design. LSAs are used to share link state information between devices. LSAs are used by OSPF routers to form and maintain neighbor relationships and to share prefix information. LSAs contain a sequence number as a form of version control to overcome problems that might be caused during LSA propagation. All LSAs are stored in the link-state database (LSDB) can can be viewed by running the command: `show ip ospf database`

The originating router resends an LSA after every 1800 seconds (30 minutes). LSAs with age 3600 seconds (1hr) are deemed invalid and purged from the LSDB. OSPF uses this as a method of route withdrawal.

# OSPF Communication

### OSPFv2 LSA Types

OSPF LSAs type 1,3,5 and 7 advertise prefixes while LSA types 2 and 4 advertise router IDs. Which LSA types are sent or present on a segment depends on the router's type, OSPF network type and area type.

1. **Type 1 Router LSA:** advertises a router's OSPF enabled networks within an area.
2. **Type 2 Network LSA:** advertises a multi-access network segment attached to a DR.
3. **Type 3 Summary:** advertises network prefixes that originated from a different area.
4. **Type 4 ASBR-Summary:** advertises a summary LSA for a specific ASBR.
5. **Type 5 External:** advertises external redistributed routes.
6. **Type 7 NSSA External:** advertises redistributed routes in Not-So-Stubby Areas (NSSA).

LSA types 1,2 are intra-area LSAs while LSA 3, 4 are inter-area LSAs. LSA Type 5, 7 advertise external routes. In single area topologies, Type 1, 2 and 5 are utilised.

Regardless of the type of LSA used, some fields are common to all LSAs:

- LSA age
- Miscellaneous (Misc) options: used to indicate the type of capabilities supported by the advertised portion of the routing domain.
- LSA Type: used to indicate the type of LSA to follow in the same packet and the way it should be intepreted.
- Link State ID: Content of LS ID differs depending on the type of LSA being described.
    - Type 1 LSA: origin router ID
    - Type 2 LSA: DR interface IP address
    - Type 5 LSA: Destination network's IP address
- Advertising router
- Link state sequence number
- Checksum: used to verify the integrity of the LSA.

- Length

The link state age and sequence number are used for comparison to determine the most up-to-date information. If multiple copies of the same LSA exist, the one with the newest information is used.

## Type 1 Router LSA

A type 1 LSA contains lists of all OSPF-enabled interfaces on a router and their associated cost. It is originated by all OSPF devices in the network. It is used to describe the networks that a device is attached to and the device's network placement. Type 1 LSAs can be used to describe one or many interfaces and networks. The type of connection is indicated in the Type field. There are four Type fields that exist: Type 1 - 4.

- **Link Type 1:** defines a point to point connection such as a serial connection. The type also formats the fields within the LSA so that it can be referenced.
  - The link ID is the neighbor's router-ID.
  - The link data is the origin router interface IP address.
- **Link Type 2:** defines a transit network. This type of network uses a DR and potentially a BDR.
  - The link ID is DR IP address.
  - The link data is the origin router interface IP address.
- **Link Type 3:** indicates ta stub network; these are networks that have no other OSPF device such as an access LAN. It is used along with a point-to-point router LSA that describe the subnet that the links occupy. (link type 1 LSA). With this type, the link ID is the subnet number and the link data is the subnet mask.
- **Link Type 4:** indicates a virtual link. Virtual links are used to connect OSPF areas that are unable to connect to the backbone area.
  - **Link ID:** neighbor router ID.
  - **Link data:** connecting device IP address.

The router LSA contains three different flags that indicate the role that a router has in a network:

1. **E Bit:** used to indicate whether a device is a boundary router with another routing domain usually using redistribution.
2. **B Bit:** used to indicate whether a device is an area border router.
3. **V Bit:** usd to indicate whether a device is an end-point for a virtual-link. A virtual-link implies an area border router.

Type 1 LSAs can be viewed by running the command: **`show ip ospf database router`**

```
R1#show ip ospf database router

          OSPF Router with ID (1.1.1.1) (Process ID 1)

              Router Link States (Area 0)

  LS age: 73
  Options: (No TOS-capability, DC)
  LS Type: Router Links
```

```
Link State ID: 1.1.1.1
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x8F5C
Length: 48
Area Border Router
AS Boundary Router
Number of Links: 2

  Link connected to: a Transit Network
   (Link ID) Designated Router address: 10.0.12.1
   (Link Data) Router Interface address: 10.0.12.1
    Number of MTID metrics: 0
     TOS 0 Metrics: 1

  Link connected to: a Stub Network
   (Link ID) Network/subnet number: 10.0.16.0
   (Link Data) Network Mask: 255.255.255.252
    Number of MTID metrics: 0
     TOS 0 Metrics: 1



Adv Router is not-reachable in topology Base with MTID 0
LS age: 2
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 2.2.2.2
Advertising Router: 2.2.2.2
LS Seq Number: 80000002
Checksum: 0xA7BD
Length: 60
Number of Links: 3

  Link connected to: a Stub Network
    (Link ID) Network/subnet number: 10.0.210.1
    (Link Data) Network Mask: 255.255.255.255
     Number of MTID metrics: 0
      TOS 0 Metrics: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 10.0.12.1
    (Link Data) Router Interface address: 10.0.12.2
     Number of MTID metrics: 0
      TOS 0 Metrics: 100

  Link connected to: a Stub Network
    (Link ID) Network/subnet number: 10.0.26.0
    (Link Data) Network Mask: 255.255.255.252
     Number of MTID metrics: 0
      TOS 0 Metrics: 10



            Router Link States (Area 10)

LS age: 73
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 1.1.1.1
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x3FC3
Length: 36
Area Border Router
AS Boundary Router
```

```
Number of Links: 1

  Link connected to: a Stub Network
   (Link ID) Network/subnet number: 10.10.13.0
   (Link Data) Network Mask: 255.255.255.252
    Number of MTID metrics: 0
     TOS 0 Metrics: 1
```

The Link ID value identifies the object that the link connects to, which could be: the router ID, IP address of the interface of the DR, network address. A type 1 LSA is capable of advertising multiple links in one LSA. In an area, all routers have an identical LSDB for that area.

Links advertised in a type 1 LSA include stub links, point-to-point links, transit links. A stub link is a link without an OSPF neighbor; such as a link to connecting end-user devices to the network. With a stub network, the traffic in this segment is either originating from this segment or has its destination in this segment. For a stub link advertisement, the Link ID is the network address and the link data is the subnet mask.

For a transit network, neither the source nor the destination of the packets is on the link. Traffic on this link is in transit. A transit network indicates the presence of a Designated Router (DR) on the segment/link. For transit links, the link ID is the RID of the DR, and link data is the interface IP address of the local router in that segment. If the link ID and link data values are the same, then the advertising router is the DR. The subnet mask of a transit link is contained in a type 2 LSA that is advertised by the DR in that segment. If the transit link has one neighbor and that neighbor becomes unavailable, the local router changes the type of link from transit to stub. Transit links imply the existence of a neighbor and that the network type is broadcast or non-broadcast.

Point-to-point links do not necessarily require IP addressing. IP unnumbered can be used. With IP unnumbered configuration, the IP address is borrowed from another interface of the router to represent the point-to-point link in the LSDB. The point-to-point link has as a single entry in the LSDB. If IP addressing is used on the interfaces of a point-to-point link, it is represented by two entries in the LSDB: (1) as a point-to-point link and (2) as a stub network. The point-to-point Link ID is the neighbor's RID. The link data is the ip address of the router's interface in that segment. The stub link entry for this point-to-point link; the link ID is the network address of the point-to-point link. The link data is the subnet mask of the point-to-point network. If the network type is point-to-point or point-to-multipoint, the type 1 LSA entry contains the neighbor ID.

In multi-area OSPF domains the ABRs and ASBRs flip a bit in the OSPF packet (hello) to indicate their role as an ABR and/or ASBR.

In the global/VRF RIB, type 1 LSAs received from other routers in the same area appear as intra-area routers with the code "O"

## Type 2 LSA Network

The DR is the only router on a multi-access segment that advertises the type 2 LSA. A type 2 LSA identifies all the routers attached to that network segment. It lists the routers that are

adjacent to the DR. When a DR is not used, this type of information is listed in a Type 1 LSA.

It is used to reduce redundant information in database and flooding scalability issues. Type 1 LSAs advertise transit networks without subnet mask information. Type 2 LSAs include subnet mask information for transit links. The DR advertises its IP address, subnet mask and attached routers including itself. If a DR is not elected, a type 2 LSA is not present. To view type 2 LSAs: issue the privileged command: **`show ip ospf database network`**

```
R2#show ip ospf database network

          OSPF Router with ID (2.2.2.2) (Process ID 2)

              Net Link States (Area 0)

  Routing Bit Set on this LSA in topology Base with MTID 0
  LS age: 40
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 10.0.12.1 (address of Designated Router)
  Advertising Router: 1.1.1.1
  LS Seq Number: 80000002
  Checksum: 0xE232
  Length: 32
  Network Mask: /30
        Attached Router: 1.1.1.1
        Attached Router: 2.2.2.2
```

The fields of a Type 2 LSA include:

- **Network mask:** usd to indicate the specific addresses that are included within the advertisement.
- **Attached routers:** lists all the devices that are fully adjacent with the DR.

Type 1 and type 2 LSAs are used for building the routing topology within an area. The Link ID of a type 2 LSA is IP address of the DR interface in the segment. The advertising router is the RID of the DR, the attached router is the RID of all the OSPF neighbors on that link.

## Type 3 LSA - Network

ABRs act as a sort of default gateway between area 0 and a neighboring non-backbone area. Type 3 LSAs contain networks that are reachable in other areas through the ABR. Type 3 LSAs include the route cost but hide the ABR's actual path to the destination, SPF is not run for ABR advertised type 3 LSA routes. This is because the ABR has already run SPF for those routes (in their source area) from itself to the source routers when they were received as type 1 LSAs. Additionally, the local routers have already run SPF for the route from themselves to the ABR. LSA type 3 are used to advertise summaries of link-state information to other areas. ABRs follow three fundamental rules when creating type 3 LSAs:

1. Type 1 LSAs received from any area, the ABR creates a type 3 LSA for the backbone area and non-backbone area.
2. Type 3 LSAs received from area 0, the ABR creates a new type 3 LSA for only non-backbone areas.
3. Type 3 LSAs received from a non-backbone area are only inserted into the LSDB of the

source area. ABRs do not create a type 3 LSA for the other areas (including a segmented area 0). This enforces the two-tier hierarchy of OSPF.

The advertising router for a type 3 LSA is the last ABR that advertises the prefix.

LSA types 1,2 do not cross borders to other areas. An ABR extracts prefix information from type 1 and type 2 LSAs and inserts them into a type 3 LSA for advertisement into another area. If an ABR receives a type 3 LSA (sourced from a non-backbone area and injected to the backbone area), it changes the advertising router to itself and forwards the LSA to the second non-backbone area. Unlike a type 5 LSA, a Type 3 LSA is modified at every ABR. To view type 3 LSAs, issue the following command: `show ip ospf database summary`

```
R2#show ip ospf database summary

          OSPF Router with ID (2.2.2.2) (Process ID 2)

              Summary Net Link States (Area 0)

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 69
 Options: (No TOS-capability, DC, Upward)
 LS Type: Summary Links(Network)
 Link State ID: 10.7.7.0 (summary Network Number)
 Advertising Router: 6.6.6.6
 LS Seq Number: 80000002
 Checksum: 0xE820
 Length: 28
 Network Mask: /29
        MTID: 0      Metric: 10

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 172
 Options: (No TOS-capability, DC, Upward)
 LS Type: Summary Links(Network)
 Link State ID: 10.10.13.0 (summary Network Number)
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000003
 Checksum: 0xD443
 Length: 28
 Network Mask: /30
        MTID: 0      Metric: 1

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 1571
 Options: (No TOS-capability, DC, Upward)
 LS Type: Summary Links(Network)
 Link State ID: 10.10.31.1 (summary Network Number)
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000001
 Checksum: 0x24DE
 Length: 28
 Network Mask: /32
        MTID: 0     Metric: 2

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 1571
 Options: (No TOS-capability, DC, Upward)
 LS Type: Summary Links(Network)
 Link State ID: 10.10.34.0 (summary Network Number)
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000001
 Checksum: 0xFA09
```

```
  Length: 28
  Network Mask: /30
        MTID: 0      Metric: 2
```

The LSID value is the advertised summary network number. Type 3 LSAs appear as inter-area routes with the code "O IA" in the global / VRF RIB. One type 3 LSA is generated per prefix. If a received type 1 LSA contains five prefixes, the ABR will create five type 3 LSAs with one for each prefix. A type 3 LSA is advertised into the neighboring area by the ABR. If a second ABR is to advertise the type 3 LSA into a third area (after receiving it through the backbone), only the advertising router field is updated by the second ABR. Type 3 LSAs appear in the RIB as inter-area routes with the code "O IA".

```
R2#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 4 masks
O        10.0.16.0/30 [110/101] via 10.0.12.1, 00:57:46, GigabitEthernet0/0
O IA     10.7.7.0/29 [110/20] via 10.0.26.2, 00:47:06, GigabitEthernet1/0
O IA     10.10.13.0/30 [110/101] via 10.0.12.1, 00:57:46, GigabitEthernet0/0
O IA     10.10.31.1/32 [110/102] via 10.0.12.1, 00:42:34, GigabitEthernet0/0
O IA     10.10.34.0/30 [110/102] via 10.0.12.1, 00:42:34, GigabitEthernet0/0
      172.30.0.0/30 is subnetted, 1 subnets
O E2     172.30.45.0 [110/20] via 10.0.12.1, 00:19:44, GigabitEthernet0/0
      172.31.0.0/24 is subnetted, 3 subnets
O E2     172.31.10.0 [110/20] via 10.0.12.1, 00:19:35, GigabitEthernet0/0
O E2     172.31.11.0 [110/20] via 10.0.12.1, 00:19:35, GigabitEthernet0/0
O E2     172.31.12.0 [110/20] via 10.0.12.1, 00:19:35, GigabitEthernet0/0
O     192.168.6.0/24 [110/20] via 10.0.26.2, 00:47:06, GigabitEthernet1/0
```

## Type 5 External LSA

Type 5 LSAs are used to advertise network reachability information that was redistributed from another routing domain. Type 5 LSAs are generated by an Autonomous-System Boundary Router (ASBR) to advertise the routes that the ASBR is redistributing. Type 5 LSAs are flooded throughout the OSPF domain to non-stubby areas with only the LSA age modified. They do not belong to any specific area. In the LSDB, type 5 LSAs are listed at the bottom of the output.

Fields included with an external LSA:

- **Network mask:** indicates specific advertised addresses.
- **Metric:** Indicates the cost to reach the destination. Its calculation and use is determined by the external metric type bit.
- **External metric type:** determines metric interpretation and calculation. two available types include:
    1. **Type 1:** advertises a route with a seed metric. OSPF then adds to it.
    2. **Type 2:** advertises a route with a static cost. This cost does not change within the

OSPF network. This metric type is the default Type 5 LSA with most vendors. It most often works fine with a single connection point. If there are multiple connection points, the Type 1 external metric type is preferred.

- **Forwarding address:** indicates where traffic is forwarded to reach the advertised destination. Often set to 0.0.0.0 indicating a destination of LSA source i.e., the originator of the LSA should be forwarded the traffic.

Type 5 LSAs can be viewed in greater detail using the privileged mode command: `show ip ospf database external`

```
R2#show ip ospf database external

             OSPF Router with ID (2.2.2.2) (Process ID 2)

                 Type-5 AS External Link States

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 1450
 Options: (No TOS-capability, DC, Upward)
 LS Type: AS External Link
 Link State ID: 172.30.45.0 (External Network Number )
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000008
 Checksum: 0x491F
 Length: 36
 Network Mask: /30
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 10.10.34.2
        External Route Tag: 0

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 1450
 Options: (No TOS-capability, DC, Upward)
 LS Type: AS External Link
 Link State ID: 172.31.10.0 (External Network Number )
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000008
 Checksum: 0xD1B5
 Length: 36
 Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 10.10.34.2
        External Route Tag: 0

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 1450
 Options: (No TOS-capability, DC, Upward)
 LS Type: AS External Link
 Link State ID: 172.31.11.0 (External Network Number )
 Advertising Router: 1.1.1.1
 LS Seq Number: 80000008
 Checksum: 0xC6BF
 Length: 36
 Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 10.10.34.2
        External Route Tag: 0
```

```
  Routing Bit Set on this LSA in topology Base with MTID 0
  LS age: 1450
  Options: (No TOS-capability, DC, Upward)
  LS Type: AS External Link
  Link State ID: 172.31.12.0 (External Network Number )
  Advertising Router: 1.1.1.1
  LS Seq Number: 80000008
  Checksum: 0xBBC9
  Length: 36
  Network Mask: /24
         Metric Type: 2 (Larger than any link state path)
         MTID: 0
         Metric: 20
         Forward Address: 10.10.34.2
         External Route Tag: 0
R2#
```

A type 5 LSA includes a forwarding address field. A forwarding address of 0.0.0.0 implies that traffic to the external routes should be forwarded to the ASBR that is the advertising router for the external routes. If the forwarding address is not 0.0.0.0 , say it is 10.10.34.2 (as in the above output), and this address is not configured on the advertising router, then one implication is that the advertising router is implementing Type 7 to Type 5 LSA translation and is there an ABR to an NSSA area. In this case, this ABR will double as an ASBR because of the type 7/type 5 LSA translation.

By default, external routes are redistributed as type 2 external routes (with code "O E2") with a metric of 20. LSAs include forward address that indicate who should I route towards to reach the link. Usually, this is the ASBR but it could be set to another router in some designs. A route tag is included in this LSA.

```
R2#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 4 masks
O     10.0.16.0/30 [110/101] via 10.0.12.1, 04:25:30, GigabitEthernet0/0
O IA     10.7.7.0/29 [110/20] via 10.0.26.2, 04:14:50, GigabitEthernet1/0
O IA     10.10.13.0/30 [110/101] via 10.0.12.1, 04:25:30, GigabitEthernet0/0
O IA     10.10.31.1/32 [110/102] via 10.0.12.1, 04:10:18, GigabitEthernet0/0
O IA     10.10.34.0/30 [110/102] via 10.0.12.1, 04:10:18, GigabitEthernet0/0
      172.30.0.0/30 is subnetted, 1 subnets
O E2     172.30.45.0 [110/20] via 10.0.12.1, 00:45:59, GigabitEthernet0/0
      172.31.0.0/24 is subnetted, 3 subnets
O E2     172.31.10.0 [110/20] via 10.0.12.1, 00:45:59, GigabitEthernet0/0
O E2     172.31.11.0 [110/20] via 10.0.12.1, 00:45:59, GigabitEthernet0/0
O E2     172.31.12.0 [110/20] via 10.0.12.1, 00:45:59, GigabitEthernet0/0
O     192.168.6.0/24 [110/20] via 10.0.26.2, 04:14:50, GigabitEthernet1/0
```

### External Type 1 vs Type 2

External routes are classified as Type 1 or Type 2. The main differences between Type 1 and

Type 2 external OSPF routes are as follows:

- The Type 1 metric equals the redistribution metric plus the total path metric to the ASBR. In other words, as the LSA propagates away from the originating ASBR, the metric increases.
- The Type 2 metric equals only the redistribution metric (by default 20). The metric is the same for the router next to the ASBR as the router 30 hops away from the originating ASBR. This is the default external metric type used by OSPF.

Type 1 is preferred to type 2. If there's a tie in type 2 routes, then the cost to reach the ASBR (forwarding metric) is the tie-breaker.

Type 5 LSAs are advertised domain-wide across multiple areas. Type 1 and Type 2 LSAs are advertised in only their area of origin.

## Type 4 LSA (ASBR-Summary)

Type 4 LSAs are generated by ABRs. Type 4 LSAs provide a way for routers to locate the ASBR when the router is in a different area from the ASBR. They provide information on the ABR's reachability to the ASBR in other areas. It includes the cost but does not include the ABR's actual path to the destination. SPF is not run for type 4 LSAs. It is created by the first ABR in the area where the ASBR is resident and provides a summary route strictly for the ASBR of a type 5 LSA.

The structure of Type 3 and Type 4 LSAs are identical. The only difference is how the information is populated. The LS ID is set to the ASBR router-ID. The network mask is set to 0.0.0.0 indicating that a single address is being advertised.

To view type 4 LSAs:`show ip ospf database asbr-summary`

```
R8#show ip ospf database asbr-summary

               OSPF Router with ID (8.8.8.8) (Process ID 8)

                    Summary ASB Link States (Area 7)

  Adv Router is not-reachable in topology Base with MTID 0
  LS age: 1017
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 1.1.1.1 (AS Boundary Router address)
  Advertising Router: 6.6.6.6
  LS Seq Number: 8000000A
  Checksum: 0x7240
  Length: 28
  Network Mask: /0
         MTID: 0      Metric: 100

  LS age: 709
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 1.1.1.1 (AS Boundary Router address)
  Advertising Router: 8.8.8.8
  LS Seq Number: 80000001
  Checksum: 0x5260
  Length: 28
```

```
Network Mask: /0
       MTID: 0      Metric: 101
```

The type 4 LSA does not contain prefix information but router ID information on how the ASBR can be accessed from another area. Therefore, type 4 LSA information does not appear in the RIB.

The ASBR generates type 1 LSA with a flipped bit to identify as an ASBR. ABRs in the same area as the ASBR will notice the flipped bit triggering the generation of type 4 LSA to enable routers forward traffic to external networks towards the ASBR. Type 4 LSAs have the advertising router field updated by the ABR as the advertising router.

## Type 7 LSA NSSA

Stubby areas prevent type 5 LSA propagation. Implementation of route redistribution is therefore not possible in a stubby area. However, local redistribution can be implemented in a not-so-stubby area (NSSA) while still preventing type 5 LSAs from being propagated into the NSSA. An ASBR advertises networks external to OSPF into NSSA as type 7 LSAs. These cannnot be advertised outside the NSSA. This LSA includes a route tag. The NSSA ABR converts a type 7 LSA to a type 5 LSA. This makes the ABR have dual role of ABR and ASBR for other areas. This second ABR generates a type 4 LSA. To view type 7 LSAs: `show ip ospf database nssa-external`

```
R3#show ip ospf database nssa-external

            OSPF Router with ID (3.3.3.3) (Process ID 3)

                Type-7 AS External Link States (Area 10)

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 415
 Options: (No TOS-capability, Type 7/5 translation, DC, Upward)
 LS Type: AS External Link
 Link State ID: 172.30.45.0 (External Network Number )
 Advertising Router: 4.4.4.4
 LS Seq Number: 80000006
 Checksum: 0x5EF5
 Length: 36
 Network Mask: /30
       Metric Type: 2 (Larger than any link state path)
       MTID: 0
       Metric: 20
       Forward Address: 10.10.34.2
       External Route Tag: 0

 Routing Bit Set on this LSA in topology Base with MTID 0
 LS age: 414
 Options: (No TOS-capability, Type 7/5 translation, DC, Upward)
 LS Type: AS External Link
 Link State ID: 172.31.10.0 (External Network Number )
 Advertising Router: 4.4.4.4
 LS Seq Number: 80000006
 Checksum: 0xE68C
 Length: 36
 Network Mask: /24
       Metric Type: 2 (Larger than any link state path)
       MTID: 0
       Metric: 20
       Forward Address: 10.10.34.2
```

```
        External Route Tag: 0

  Routing Bit Set on this LSA in topology Base with MTID 0
  LS age: 414
  Options: (No TOS-capability, Type 7/5 translation, DC, Upward)
  LS Type: AS External Link
  Link State ID: 172.31.11.0 (External Network Number )
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000006
  Checksum: 0xDB96
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 10.10.34.2
        External Route Tag: 0

  Routing Bit Set on this LSA in topology Base with MTID 0
  LS age: 415
  Options: (No TOS-capability, Type 7/5 translation, DC, Upward)
  LS Type: AS External Link
  Link State ID: 172.31.12.0 (External Network Number )
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000006
  Checksum: 0xD0A0
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        MTID: 0
        Metric: 20
        Forward Address: 10.10.34.2
        External Route Tag: 0
R3#
```

The default NSSA route type advertisement is NSSA LSA type 2 and appear in the RIB as "O N2" routes.

```
R3#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 4 masks
O IA     10.0.12.0/30 [110/2] via 10.10.13.1, 04:39:36, GigabitEthernet1/0
O IA     10.0.16.0/30 [110/2] via 10.10.13.1, 04:39:36, GigabitEthernet1/0
O IA     10.0.26.0/30 [110/12] via 10.10.13.1, 04:39:36, GigabitEthernet1/0
O IA     10.0.210.1/32 [110/3] via 10.10.13.1, 04:39:36, GigabitEthernet1/0
O IA     10.7.7.0/29 [110/12] via 10.10.13.1, 04:38:30, GigabitEthernet1/0
      172.30.0.0/30 is subnetted, 1 subnets
O N2     172.30.45.0 [110/20] via 10.10.34.2, 00:16:51, GigabitEthernet0/0
      172.31.0.0/24 is subnetted, 3 subnets
O N2     172.31.10.0 [110/20] via 10.10.34.2, 00:16:51, GigabitEthernet0/0
O N2     172.31.11.0 [110/20] via 10.10.34.2, 00:16:51, GigabitEthernet0/0
O N2     172.31.12.0 [110/20] via 10.10.34.2, 00:16:51, GigabitEthernet0/0
O IA     192.168.6.0/24 [110/12] via 10.10.13.1, 04:38:30, GigabitEthernet1/0
R3#
```

# OSPF Hierarchy

## OSPF Areas

An OSPF area is used to group together different networks often for the purpose of increasing the efficiency of OSPF, its LSDB and the amount to time to converge. It introduces hierarchy to an OSPF domain.

An OSPF area is used to segment a large OSPF domain. An area defines a flooding domain. All devices in the area agree on the topology with features such as authentication type, area type i.e. normal, stubby, not-so-stubby area (NSSA). Changes inside the area require LSA flooding and full SPF execution. All routers in an area execute SPF algorithm when the network changes for example when links fail, when failed links are restored, new routes added, existing routes withdrawn.

Inter-area routing is similar to distance vector because routers in another area do not have a detailed view of the local area. So they rely on the type 3 network summary LSAs. Changes such as the addition of a new network, link flapping/failure outside the area don't always require LSA flooding or SPF limiting the impact on router resources.

To determine the OSPF areas that a router is participating in:

```
R1(config-if)#do show ip ospf interface brief
Interface    PID     Area     IP Address/Mask     Cost     State     Nbrs F/C
Gi0/0        1       0        10.0.12.1/30        1        DR        1/1
Fa3/0        1       0        10.0.16.1/30        1        P2P       0/0
Gi1/0        1       10       10.10.13.1/30       1        P2P       0/0
R1(config-if)#do show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Start time: 00:00:32.764, Time elapsed: 01:57:36.228
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border and autonomous system boundary router
Redistributing External Routes from,
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 1 normal 0 stub 1 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
```

```
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
       Number of interfaces in this area is 2
       Area has message digest authentication
       SPF algorithm last executed 00:58:20.520 ago
       SPF algorithm executed 3 times
       Area ranges are
       Number of LSA 4. Checksum Sum 0x03233A
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
    Area 10
       Number of interfaces in this area is 1
       It is a NSSA area
       Perform type-7/type-5 LSA translation
       Area has no authentication
       SPF algorithm last executed 01:57:24.284 ago
       SPF algorithm executed 2 times
       Area ranges are
       Number of LSA 5. Checksum Sum 0x035534
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0

R1(config-if)#
```

If the output of the command `show ip ospf` shows that the router is participating in more than one area, then the router is an ABR.

Stub areas and not-so-stubby-areas are standards based areas. Totally stubby and totally NSSA are non-standard (vendor specific) area types.

In networks that are single area, any area number can be used and prefix exchange will take place. In multi-area OSPF networks, area zero (0) must be configured with inter-area traffic transiting area 0.

OSPF networks are built on a two-level hierarchical topology: backbone area (area 0) and non-backbone area.

## Backbone Area (Area 0)

At the center of an OSPF hierarchy is area 0 also known as the backbone area. It is u sed to summarize topology information between other areas. Traffic from one area to another must transit area 0. Area 0 must be contiguous. The only exception to this is the use of a virtual link.

## Non-backbone Area

Must use connections through area 0 to reach other areas. Nonbackbone areas are referred to as normal areas. All non-backbone areas must connect to the backbone area directly or through a virtual-link.

Non-backbone areas can be configured as stub areas. Non-backbone areas configured as stub areas affect the way link-state information is shared between the different areas and the types of LSAs used. The types of stub areas include: stubby area, not-so-stubby-area (NSSA), totally stubby area and totally NSSA. Stubby areas provde one way of reducing the number of external OSPF routes in an area. To configure a stubby area, every router in the stubby area needs to be configured as a stub. Stubby areas are identified by the area flag in the hello packet.

**Stubby Area**

Stub areas prohibit type 5 and thereby preventing type 4 LSAs from being generated. When a type 5 LSA reaches the ABR, it generates a type 3 default route for the stub area. All external routes (originated from outside the stub area) are replaced with a single entry, a default route.

Stub areas are often used when there is a single exit point from an area into the backbone. If multiple exit points exist, sub-optimal routing may result if an area is configured as a stub area.

Configuration of stubby areas is good for low-end or heavily-loaded routers. The three rules of stubby areas:

1. Area 0 cannot be a stubby area.
2. A stubby area can not be transit area for a virtual link.
3. An ASBR can not be present in a stubby area.

Configuration **`#area 1 stub`**. All routers in the stub area should have the above command configured.

**Totally Stubby Area**

A totally stubby area is similar to a stubby area. However, it prohibits type 3, 4 and 5 LSAs. ABR generates a default route after receiving type 3 and 5 LSAs. Totally stubby areas do not allow redistribution inside of them implying that ASBRs are not allowed in stub or totally stubby areas. At the ABR, the configuration; **`area 1 stub no-summary`**

Totally stubby areas are suitable for areas with a single exit point to the backbone. Multiple exit points can cause suboptimal external and inter-area route paths.

**Not-So-Stubby Area (NSSA)**

NSSAs provide a way to get around the ASBR restriction of stubby areas and totally stubby areas. Like stubby areas, NSSA areas apply stub area rules such as prohibiting type 5 LSA from entering at the ABR. However, NSSAs allow for local redistribution. The ASBR advertises external networks with Type 7 LSAs (NSSA LSA). Type 7 LSAs carry information common to type 5 LSAs. The format of a Type 7 LSA is almost identical to a Type 5 LSA. The only exceptions are:

- Link state type is different
- Additional propagate(P) flag is added. The P bit tells the ABR to translate Type 7 LSA to Type 5 LSA and advertise it to the rest of the OSPF domain. For propagation, the forwarding address must be set in this type of LSA. If it is not set, the ABR does not process the translation. If this happens, then the Type 7 LSA link-state information is limited to being advertised only within the NSSA.

The ABR does not automatically advertise a default route when a type 5 LSA is blocked. The ABR of an NSSA area can be configured to advertise a default route using the command: **`area 1 nssa default-information-originate`** If the optional **`default-information-originate`** keyword is appended, the ABR generates a type 7 default route into the NSSA.

**Verification**

```
#show ip ospf
#show ip protocols
```

A Type 7 LSA is area-specific to the area they were generated in. They are similar to LSA Types 1 and 2 interms of how they are flooded. The ABR of an NSSA translates a type 7 LSA to type 5 LSA for area 0. While an NSSA cannot be a transit area, it can host an ASBR.

NSSAs are often seen with service providers.

### Totally Not-So-Stubby Area (Totally NSSA)

Normal NSSAs allow Type 3 LSAs. Totally NSSAs prohibits Type 3,4,5 LSAs but allows for local redistribution. When the ABR receives a Type 3 or 5 LSA, it generates a default route automatically on Cisco devices. Devices from some other vendors do not generate this default route automatically. The default route is a type 3 LSA route. The type 7 LSA arriving at the ABR of a totally NSSA is translated into a Type 5 LSA. To configure a Totally NSSA, on the ABR, enter the following command: **`#area 1 nssa no-summary`**

## OSPF Router Types

- **Backbone Router:** these are routers that have at least one interface in area 0 (backbone). It can be an internal router as well as an ABR
- **Internal Routers:** all links of the router are in one non-backbone area.
- **Area Border Router (ABR):** router has links in both area 0 and non-backbone area. The ABR summarizes information between area 0 and non-backbone area.
- **Autonomous System Boundary Router (ASBR):** has at least one link in the OSPF domain and another link in a non-OSPF domain for example IS-IS, EIGRP, BGP, RIP domain. The ASBR redistributes routes to and/or from other routing domains and OSPF.

The router type can be verified by using the following commands:

```
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 1.1.1.1
  It is an area border and autonomous system boundary router
 Redistributing External Routes from,
  Number of areas in this router is 2. 1 normal 0 stub 1 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.12.1 0.0.0.0 area 0
...
```

Other commands such `#show ip ospf` can display the router's type.

### OSPF Route Types

Multiple OSPF route types exist:

- **Intra-area:** sourced within an area. In OSPF areas without an other area attached have intra-area routes.
- **Inter-area:** route sourced from OSPF area X that appears in another OSPF area Y.
- **External routes:** Sourced from another routing domain. These are advertised as Type 5 LSAs and appear as external type 1 and external type 2 routes.

## Shortest Path First (SPF) Operation

SPF requires a completed link-state database as input. The output of the SPF algorithm is the shortest path tree (SPT).

If there is a tie in cost, both paths are installed into the routing table.

## Neighbor and Topology Maintenance

Once adjacencies have been established and SPT built, the OSPF state machine tracks neighbor and topology changes. Hello packets are used to monitor the availability of neighbors. LSUs update neighbors of network changes such as link failures, addition or removal of networks, change of link OSPF network types.

### Tracking Topology Changes

When a new LSA is received, it is checked against the LSDB for changes such as:

- Sequence number: to track new LSAs.
- Age: used to keep information updated and withdraw old information. Periodic flooding occurs every 30 minutes (1800 secs) - paranoid update. LSAs whose LSA age is equal to the MaxAge value 3600 seconds are purged from the LSDB as they are considered invalid.
- Checksum: used to verify that transmission and memory corruption have not affected a packet.

### LSA Flooding

When a change is detected in the network, a new LSA is generated and flooded out all OSPF links in the area. OSPF does not use split-horizon. Self-originated LSAs are simply dropped. Not all LSA changes require SPF to calculate for example link up/down event vs sequence number, age.

The method used for flooding will depend on multiple things:

- on the state of a device's LSDB.
- Specific network types used on a device's network interfaces

If new information is found within the contents of a database descripter packet, then the device forms a list of those that it needs to add or update. The determination of whether information should be updated if a copy already exists in the LSDB is primarily based on the link state sequence number. Each LSA that is advertised both within the contents of a database descripter packet and within the different link state packets contains a sequence number that is specific to it. It is incremented everytime that an update is received for it. It is this number that is used for comparison by OSPF devices where multiple copies of the same LSA exist. If a device finds a copy that is more up-to-date than it has, then the device adds it to the ones that it requests from that neighbor.

Other fields, in addition to the LS sequence number, are used for the tie-break over the question of which LSA is more up-to-date. This sommetines happens when more than one device uses the same sequence number when they update an LSA and flood it. If multiple devices use the same sequence number:

- First, the checksum is verified.
- The link state age is used to break any tie.

Flooding method depends on the network type:

- Multicast is used if multiple devices are being updated at the same time. This is often seen on broadcast networks that use DR. The DR sends the update to the address 224.0.0.5.
- Unicast communications is should be used for communications between two devices. This is common on interfaces that do not support multicast.

# OSPF Virtual Links

Discontiguous areas arise when a non-backbone area is not directly connected to the backone. Also, when the backbone is split-up into two or more sections with each section separated by a non-backbone area. Discontiguous areas cause the ABR not to be reachable via SPT. An ABR can only advertise routes between areas when one of the areas it is connected to is the backbone(area 0).

Discontiguous areas are eliminated by adding new area 0 links and adjacencies. The links could be either physical or virtual for example GRE. OSPF virtual-links are a form of virtual area 0 adjacencies. They are used to form multi-hop unicast area 0 adjacency. Virtual-links follow the already built shortest path first tree (SPT) between ABRs to connect to the

backbone.

As part of a two-tier hierarchy, area zero (0) must be contiguous. As indicated earlier, ABRs follow three fundamental rules when creating type 3 LSAs:

1. Type 1 LSAs received from any area, the ABR creates a type 3 LSA for the backbone area and non-backbone area.
2. Type 3 LSAs received from area 0, the ABR creates a new type 3 LSA for only non-backbone areas.
3. Type 3 LSAs received from a non-backbone area are only inserted into the LSDB of the source area. ABRs do not create a type 3 LSA for the other areas (including a segmented area 0).

The tunnel (of a virtual-link) belongs to the backbone area and therefore the router terminating the virtual link becomes an ABR. The area in which the virtual-link endpoints are established is known as the transit area. Each router identifies the remote router by its RID. The virtual-link can be one hop or multiple hops away from the remote virtual-link endpoint. The virtual link is built using type 1 LSAs where the neighbor state is type 4 LSA. A virtual-link inherits costs from SPT cost between end-points. The cost must be below 65535. A virtual-link runs as a demand circuit so errors in configuration could be hidden until flooding occurs. Configuration: (on both virtual-link endpoints)

```
R6(config)#router ospf 6
R6(config-router)#area 7 virtual-link 8.8.8.8
R6(config-router)#end

-----------------------------------

R8(config)#router ospf 8
R8(config-router)#area 7 virtual-link 6.6.6.6
R8(config-router)#end
*Aug 15 14:59:34.035: %SYS-5-CONFIG_I: Configured from console by console
R8#
R8#show ip ospf virtual-links
Virtual Link OSPF_VL0 to router 6.6.6.6 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 7, via interface GigabitEthernet0/0
 Topology-MTID     Cost     Disabled     Shutdown     Topology Name
      0              1           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 00:00:03
    Adjacency State FULL (Hello suppressed)
    Index 1/2, 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
  Message digest authentication enabled
    Youngest key id is 1
R8#
R8#show ip ospf interface
OSPF_VL0 is up, line protocol is up
  Internet Address 10.7.7.3/29, Area 0, Attached via Not Attached
  Process ID 8, Router ID 8.8.8.8, Network Type VIRTUAL_LINK, Cost: 1
  Topology-MTID     Cost     Disabled     Shutdown     Topology Name
       0              1           no          no           Base
  Configured as demand circuit
```

```
  Run as demand circuit
  DoNotAge LSA allowed
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 6.6.6.6 (Hello suppressed)
  Suppress hello for 1 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.7.7.3/29, Area 7, Attached via Interface Enable
  Process ID 8, Router ID 8.8.8.8, Network Type BROADCAST, Cost: 1
  Topology-MTID     Cost     Disabled     Shutdown     Topology Name
       0              1           no          no           Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 6.6.6.6, Interface address 10.7.7.1
  Backup Designated router (ID) 8.8.8.8, Interface address 10.7.7.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 6.6.6.6 (Designated Router)
  Suppress hello for 0 neighbor(s)
R8#
```

The commands `show ip ospf virtual-link` and `show ip ospf interface` as indicated in the above command output verifies the operational state of the virtual-link.

Hello packets are suppressed for virtual-links.

### Virtual-link Preconditions

- End-points must be reachable via a normal area (not a stub area). OSPF stubby areas cannot be a transit area for a virtual-link.
- Transit area must not have filtering applied i.e. LSA type 3 filters, distribute-lists.

## Link-State Database (LSDB)

Every OSPF device has a link-state database (LSDB). Devices inside the same area have the same LSDB. The Link-State Database (LSDB) contains the details of all the networks in the local area and summary information about networks in other areas and external networks. To view a summary of the LSDB, use the command **`show ip ospf database`**.

LSDBs are populated by Type 1 to Type 7 LSAs. On receiving an LSA, the information is integrity checked and then placed into the LSDB. This process continues domain wide until the LSDB of all routers in the same area are the same (synchronized). This process is referred to as flooding. To view the LSDB, issue the command **`show ip ospf database`**.

```
R1#show ip ospf database

           OSPF Router with ID (1.1.1.1) (Process ID 1)

               Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         477         0x8000000A 0x00C502 2
2.2.2.2         2.2.2.2         247         0x8000000A 0x0066CD 3
6.6.6.6         6.6.6.6         3514        0x80000004 0x00F749 4
8.8.8.8         8.8.8.8         3    (DNA) 0x80000002 0x00BDFD 1

               Net Link States (Area 0)

Link ID         ADV Router       Age         Seq#       Checksum
10.0.12.2       2.2.2.2          725         0x80000005 0x00A468
10.0.26.1       2.2.2.2          247         0x80000005 0x000FDC

               Summary Net Link States (Area 0)

Link ID         ADV Router       Age         Seq# Checksum
10.7.7.0        6.6.6.6          874         0x80000003 0x00E621
10.7.7.0        8.8.8.8          13   (DNA) 0x80000001 0x0054B6
10.10.13.0      1.1.1.1          477         0x8000000A 0x00C64A
10.10.31.1      1.1.1.1          1130        0x80000001 0x0024DE
10.10.34.0      1.1.1.1          1130        0x80000001 0x00FA09

               Router Link States (Area 10)

Link ID         ADV Router       Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1          1134        0x80000005 0x0015AC 2
3.3.3.3         3.3.3.3          1135        0x80000002 0x00A193 4

               Summary Net Link States (Area 10)

Link ID         ADV Router       Age         Seq#         Checksum
10.0.12.0       1.1.1.1          720         0x80000003 0x00FD1F
10.0.16.0       1.1.1.1          477         0x80000005 0x00CD49
10.0.26.0       1.1.1.1          229         0x80000007 0x00BF41
10.0.210.1      1.1.1.1          229         0x80000007 0x007DCF
10.7.7.0        1.1.1.1          229         0x80000007 0x00897D
192.168.6.0     1.1.1.1          229         0x80000007 0x00E3C4
R1#
```

The ultimate goal of any OSPF network design is to make the link-state database (LSDB) as stable as possible.

The output of the command **`show ip ospf database`** displays a summary of the LSDB. To view the the details of any LSDB entry, one has to open up the LSAs that are stored in the LSDB. LSDB entries are organised according to the areas that the OSPF device is operating in. For a router with interfaces in more than one area, the LSAs are organised according to the area that the router is a member of.

# OSPF Path Selection

The decision on the path the next hop for traffic is based on the path metric. Metric is the cummulative OSPF interface cost along the path. The cost is calculated as follows;

`reference bandwidth / interface bandwidth.`

The default OSPF reference bandwidth is 100mbps. With this default reference bandwidth, OSPF is unable to differentiate between fastethernet(100mbps), gigabitethernet(1000mbps), ten gigabitethernet(10000) or high speeds. All interfaces from fastethernet or faster will have an OSPF cost of one (1). It is imperative to modify the defaylt reference bandwidth in network environments with interfaces having gigabitethernet or faster interfaces so that OSPF can make more accurate path selection decisions. This default reference bandwidth can be modified with the OSPF router mode command: `auto-cost reference-bandwidth` *`bandwidth`* The bandwidth value is in megabits per second.

```
R8(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
      Please ensure reference bandwidth is consistent across all routers.
R8(config-router)#do show ip ospf
 Routing Process "ospf 8" with ID 8.8.8.8
 Start time: 00:00:40.364, Time elapsed: 01:49:26.920
 Supports only single TOS(TOS0) routes
 .......
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 Number of areas transit capable is 1
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled

 Reference bandwidth unit is 10000 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 01:49:00.076 ago
        SPF algorithm executed 2 times
........
```

The reference bandwidth should be set to the same value for all routers in the OSPF domain, otherwise sub-optimal routing may occur. Type 1 LSAs include the cost of each link which is in the range 1 - 65535.

OSPF best path selection criteria (in order of preference);

1. Intra-area path with the lowest metric
2. Inter-area path with the lowest metric
3. External type 1 path with the lowest metric
4. NSSA type 1 path with the lowest metric
5. External type 2 paths with the lowest metric
6. External type 2 paths with the lowest forwarding metric
7. NSSA type 2 path with the lowest metric.

External routes are classified as type 1 or type 2.

- type 1 routes are preferred to type 2.
- type 1 metric is the combined metric of the path to the ASBR and redistribution

metric.
- type 2 metric equals only the redistribution metric. This metric is the same for all routers in the OSPF domain regardless of whether they are one hop from the ASBR or fifty hops away from the ASBR.
- Existence of N1 or N2 routes implies that E1 and E2 routes will not be existent in that area.

In a proper network design, the above mentioned path criteria should not be used in path selection. Ideally, routes should only be advertised from a single source. The path selection criteria should only be used as a tie-breaker in a network with extraordinary circumstances.

### Virtual-Link Costs

Virtual-links inherit their cost from SPT cost between the virtual-link endpoints. SPT cost may exceed maximum link cost. Virtual-link must have cost below 65535 to initialise. Link costs higher than 65535 could occur if reference bandwidth is higher and virtual-link transits legacy links.

# OSPF Optimization

There are a variety of methods that can increase the efficiency of OSPF. These methods are in the areas of:

- Accelerating OSPF convergence
- Controlling OSPF LSA generation and propagation.
- Altering Shortest Path First behaviour.
- Reducing the size of the LSDB.
- Reducing the effects of restarts on OSPF.

## Accelerating OSPF Convergence

OSPF convergence can be increased through the use of fast Hellos and the use of Bi-Directional Forward Detection (BFD). On most networks, OSPF's Hello and dead-interval timers are 10 seconds and 40 seconds respectively. On the networks of today, these timers are too long for failure detection and convergence. OSPF default timer values are therefore not often the best method to use for failure detection. Most lower layer protocols are faster such as Ethernet. The Hello and Dead-Interval timers are often altered during the design of an OSPF network.

Fast Hellos timer values can be configured. This allows for sub-second hello interval values. This can be implemented using the hello multiplier command.

### BFD

Not specific to OSPF, BFD provides a lightweight failure detection. The failures are processed at the line-card level without the involvement of the processor. BFD operates

primarily at the data plane and not at the control plane hence allowing for operation on the line card. BFD relies on the routing protocol neighborship establishment process to begin working.

BFD supports two operating modes: asynchronous and demand modes.

- **Asynchronous mode:** supporting syystems send packets back and forth to one another. If this stops, then controlling protocol is notified and the session drops. Asynchronous mode is generally used in production networks.
- **Demand Mode:** BFD assumes that another method is used to verify connectivity.

#### Echo Function

Echo function can be used in either BFD mode. Devices are configured to send echo packets towards a control system with the expectation of having them loopback to the remote system. This verifies the path to the remote system as well as the forwarding path of the remote system. BFD sessions can be configured independently in both directions.

# Controlling OSPF LSA Generation and Propagation

LSA throttling, LSA flood pacing, LSA group pacing and LSA retransmisssion pacing.

## LSA Throttling

LSA Throttling provides a way of limiting LSAs specifically the generation of repeat same LSAs (with same LSAID, LSA Type and Advertising router ID) when the topology changes. Here, an initial update is sent then rate limited and can't be resent for another five seconds. A similar condition is happends on recieved updates. Waiting for 5 seconds slows convergence.

LSA throttling alters how OSPF handles the generation of OSPF update packets. This is done through the modification of the LSA start-interval, LSA hold-interval and LSA max-interval. An initial update packet is sent immediately on generation. The generation of the second packet in based on the start-interval. If an event occurs and the OSPF device needs to send an additional update packet, it waits until the OSPF start interval expires. At this point, the OSPF hold interval begins. If an event occurs during this hold interval, the device waits to send that update packet till that hold interval expires. If this happens, the next LSA hold interval is doubled. This means that at the end of the initial hold interval, the update is sent but the next update packet is held until the twice the hold interval unless the LSA max-interval is reached. The LSA max-interval in this case is used as a ceiling controlling how long the hold-interval could eventually become. This doubling happens everytime an additional event occurs within the current hold interval. When the max-interval is reached, it is used as the hold-interval to delay LSA update packet generation until it expires. This remains true until no events occur within two hold-intervals or max-intervals depending on the situation. At this point, the process repeats and the start interval is used if an event occurs.

LSA throttling improves convergence and slows down update generation time during periods of instability in the network.

### Update Packet Pacing

This is different from LSA throttling because it affects the behaviour of OSPF packets that are not locally generated. Three different update timers that can be modified include: flood pacing, retransmission pacing, group pacing.

Flood pacing controls the packet spacing between consecutive update packets in the OSPF transmission queue. By default, on Cisco equipment, if multiple packets exist in the transmission queue, they are sent every 33ms.

Retransmission Pacing feature is similar to flood pacing feature but it affects the retransmission queue. By default, on Cisco equipment, if multiple packets exist in the retransmission queue, they are sent every 66ms.

Group packing controls how LSAs are refreshed by an OSPF device. The typical LSA refresh rate is 30minutes. If each individual LSA works on its own independent timer, then packets could be transmitted all the time especially in large networks. To mitigate this, LSA group pacing was introduced. Group pacing allows LSAs that are expiring within the same general time to be sent simultaneously. On Cisco equipment, the default is set to 240 seconds. All LSAs expiring within 240 seconds are updated at the same time. This increases efficiency and lowers demand.

Pacing timers defaults generally work well and are not recommended to be modified. Modification will require extensive testing to ensure that the intended result is accomplished.

## Altering Shortest Path First behaviour

Processing of SPF algorithm can be altered using PSF throttling and incremental SPF.

### Shortest Path First Throttling

SPF throttling operates similar to LSA throttling. It controls when SPF is run after an event occurs. This is done through the configuration of three parameters: SPF start-interval, SPF hold-interval and SPF max-interval. When an event initially occurs, the start-interval begins, once it expires, SPF is run using the new information. At this point, the hold-interval starts to count down. If any new event occurs during this hold-interval, then the SPF process is run once it expires. A new hold-interval begins but with twice the configured hold-interval time. If no event occurs within two hold-intervals, then the process resets and is governed by the start-interval. The process of doubling the hold-interval when additional events occur continues until the hold-interval timer reaches the max-interval time. The max-interval acts as a timer ceiling. Once it is reached, SPF runs every max-interval as long as additional events continue to occur. If no events occur within two max-intervals, then the process resets. By default, on Cisco equipment, the start-interval is 5seconds and max-interval 10

seconds.

### Incremental SPF (iSPF)

When enabled, iSPF changes when and how SPF is run. Normally, when a Type 1 or 2 LSA change occurs, all devices within an area process it and SPF is run. Often this is not required as it may not affect the SPT for every device. This results in many nodes running SPF when they do not need to.

iSPF changes the rules making the running of SPF conditional based on three conditions:

- **Addition of a new leaf node:** Events such as the addition of a new leaf node do not affect SPT on existing devices. Additional full SPF run is not neededd. iSPF prevents full SPF run on non-local devices. On local devices however, a full SPF run is still required.
- **Change alters the SPT of a device:** If a link failure occurs on a path that is not the shortest path, then full SPF run is not required. iSPF steps in and limits it.
- **Whether a limited change happens to the current SPT:** iSPF limits the devices that fully run SPF to only the local devices and devices that are downstream from the failure. Upstream devices do not need to run SPF.

The need for iSPF should be carefully considered before it is deployed.

## Reducing the Size of the LSDB

Reducing the size of the LSDB can be accomplished through the use of the following methods:

- Stub areas
- LSA Summarization
- LSA Type 3 filtering
- Prefix suppression

### Stub Areas

Limit the type of LSAs in an area. Stub areas limit Type 4 and 5 LSAs. These are replaced with a summary Type 3 LSA. Totally stubby areas extend this restriction to include Type 3 LSAs. These features reduce the size of the LSAs. Stub areas need to be configured for areas that have a single exit to the backbone area.

### Summarization

Two types of summarization exist:

- **Area summarization:** configured between areas on the ABR. Controls inter-area routes. When performing summarization;
    - only intra-area routes are summarized. Inter-area routes in the area are regenerated as normal. An ABR must be part of the area where the targeted entries are sourced from for them to be summarized.

    - Metric used for the summary is based on the lowest existing metric of the component routes of the summary. In some circumstances, it may be better to configure a static summary metric.

  Area summarization limits the inter-area database entries. This provides protection from processing of remote network changes as they occur in other areas.
- **External summarization:** configured on the ASBR for external routes being redistributed into the OSPF domain. It is a good idea to limit the number of individual routes being redistributed. This summary can be configured at the ASBR. If the IP addressing of the external routes is not contiguous, external summarization may cause problems; summarization may not be configured efficiently.

## Type 3 LSA Filtering

Type 3 LSA filtering provides for control of the Type 3 LSAs that can be advertised into and area or advertised out of an area at an ABR. Type 3 filtering provides for granular control over advertisements. Caution should be taken with configuration.

## Prefix Suppression

Implemented in Cisco's version of OSPF. Provides for the suppression of all connected prefixes. This can be implemented globally or at the interface. When configured globally, all connected prefixes that are not configured on loopback interfaces, configured as secondary, or configured on passive interfaces are suppressed. When configured this way, individual interfaces can have prefix suppression disabled to allow their configured prefixes advertised. When prefix suppression is configured on a local interface, all addresses configured are suppressed including secondary addresses.

Prefix suppression is very handy especially on large networks to reduce the size of the LSDB with a large number of transit links whose addresses are not often used. The suppression of these addresses domain-wide can considerably reduce the size of the LSDB. Such prefix suppression, though does complicate troubleshooting because these intermediate links cannot be accessed.

## OSPF Network Types

Some OSPF network types utilize additional LSAs. It is a good idea to comprehensively assess whether it is appropriate from a network design perspective to maintain the network type defaults. This is often seen with Ethernet used to connect two only two devices. Broadcast networks require the use of Type 2 LSAs, perform a master/slave election; actions which increase the neighbor formation process and also increase the size of the LSDB. In such cases, a broadcast network type can be replaced with a point-to-point link to reduce the LSDB size and reduce the neighbor formation process.

## Reducing the Effects of Restarts on OSPF

These actions are covered in RFC 3623 through graceful restart. Graceful restart allows for the restarting of OSPF without affecting the forwarding of traffic. This is done by tweaking

normal OSPF operation.

In normal operation, a device is restarted through a hard restart (powered off and on using the power switch) or a soft restart (through software). In a hard restart, there is no way to avoid dropping adjacencies as no Hello packets will be received. This type of restart is not recommended.

In a soft restart, the OSPF devices alert neighbors of an impending restart by flushing all LSAs that it originated and sending out empty Hello packets that result in neighborships being dropped immediately. With this type of shutdown, neighbors know immediately that a device is going to become unavailable and are able to make the appropriate adjustments to the link state database and eventually the routing table. Regardless of the selection, traffic is interrupted especially if the routing device does not separately implement duties of the control plane and data plane. Many routing devices offload data-plane functions to the line cards and the processor handles the control-plane functions.

With graceful restart, the control-plane can be restarted without affecting traffic. For this to function, the data-plane and control-plane functions must be separated. The device must modify the normal behaviour of OSPF when a restart occurs.

Nortmally, a device notifies its neighbors of a shutdown by advertising LSAs with a max age. The neighbors rerun SPF to determine how the SPT is affected affecting normal traffic. With graceful restart:

- The restarting device communicates with its neighbors and lets them know that a restart is upcoming.
- If the neighbors support this, they lock the neighborship between them and the restarting device and maintain the appearance of a full adjacency.
- The neighbors continue to send traffic to the device as normal even though the normal OSPF messages expected to be received are not.
- The communications between the restarting device and its neighbors are made possible through the use of the **Grace LSA**. This LSA is sent on all the OSPF interfaces with a link-local scope and lets its neighbors prepare for a restart. It also includes an expected grace period. This period indicates the amount of time that these neighboring devices should expect to maintain the illusion of a full adjacency.
- Grace LSAs continue to be sent until they are acknowledged. If no acknowledgement is received, then the restarting device terminates the graceful restart and restarts normally.
- On restart, the restarting device does not originate or flush any LSAs. It continues to use its re-restart routing tables until all neighborships come back into normal operation. Part of this process is similar to a device coming up normally. When successful, the data-path through the device remains uninterrupted.
- Once this process is complete, the restarting router flushes the Grace LSA, runs through the normal SPF process and re-originates its LSAs.

The graceful restart feature defines duties for two modes of operation: one for the restarting device and another for the neighboring devices (helper devices). The mode for these devices is typically referred to as helper mode. On Cisco devices, the functions of

graceful restart are referred to as **non-stop forwarding (NSF)**. Devices that support NSF directly are referrred to as **NSF-capable**. Those devices that support helper mode are referred to as **NSF-aware**

# Administrative Distance

There may be scenarios where more than one routing source is informing a router about the path to a given network. Routers use the administrative distance as a measure of the trustworthiness of a routing source. Administrative distance is a value ranging from 1 to 255 with 255 being an untrustworth source. The lower the AD, the more trustworthy the routing source.

The default administrative distance for OSPF is 110. When implementing traffic engineering, some situations may require the modification of the default AD of OSPF. To change the default AD, use the router OSPF mode command `distance` *`value`* where value is in the range 1 - 255.

```
#distance <1 - 255>
#show ip route ospf
```

To modify the AD of routes from a specific router;

```
#distance 109 4.4.4.4 255.255.255.255
```

ACL can be used for changing the AD of specific routes from a specific router.

```
#distance 109 4.4.4.4 255.255.255.255 ALC_10Routes
```

# OSPF Traffic Engineering

## Interface Cost

OSPF uses egress interface costs of an upstream router for metric calculation.

```
#ip ospf cost <1 - 65535>
```

The link cost can be modified by changing the default values for:

- **Interface bandwidth:** using the interface command `bandwidth` *`value`* with the bandwidth value in kilobits per second:

  ```
  R8(config)#interface g0/0
  R8(config-if)#bandwidth 10000
  R8(config-if)#do show interface g0/0
  GigabitEthernet0/0 is up, line protocol is up
    Hardware is i82543 (Livengood), address is ca08.05b3.0008 (bia ca08.05b3.0008)
    Internet address is 10.7.7.3/29
    MTU 1500 bytes, BW 10000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full Duplex, 1Gbps, link type is auto, media type is SX
  ...
  ```

  However, it is not recommended to modify the OSPF interface cost by modifying the interface bandwidth as this modification affects not only OSPF metric calculation but potentially other metric calculations say for any other routing protocol.
- **Interface cost:** modifying the OSPF interface cost using the interface mode command: value where value is between 1 - 65535.

  ```
  R8(config-if)#do show ip ospf interface brief
  ```

```
Interface     PID   Area            IP Address/Mask      Cost    State    Nbrs F/C
VL0           8     0               10.7.7.3/29          1000    P2P      1/1
Gi0/0         8     7               10.7.7.3/29          1000    BDR      1/1
R8(config-if)#ip ospf cost ?
<1-65535> Cost

R8(config-if)#ip ospf cost 1
R8(config-if)#do show ip ospf interface brief
Interface     PID   Area            IP Address/Mask Cost State Nbrs F/C
VL0           8     0 10.7.7.3/29 1000 P2P 1/1
Gi0/0         8     7 10.7.7.3/29 1 BDR 1/1
R8(config-if)#
```

- **Process auto-cost:** Modification of the default reference bandwidth implicitly changes the OSPF cost for certain paths.
- **Process neighbor cost:** In NBMA networks, neighbors are statically configured using the OSPF router mode command `neighbor RID`. A static cost can be assigned for the link to this neighbor.

# Default Routes

On a router with a default route (usually static), the default route can be propagated through OSPF using the command:

```
#default-information originate
```

The above command only works if the local router has a default route. To propagate a default route regardless of whether the local router has a default route;

```
#default-information originate always
```

The default route gets propagated as an external type 2 LSA. To modify characteristics of the default route;

```
default-information originate metric <1 - 65535> metric-type <1 | 2>
```

# OSPF Summarization and Filtering

OSPF scalability is achieved by minimising the topology graph complexity (number of routers) and volume of reachability information (number of prefixes). Topology summarization is achieved through implementation of OSPF areas. NLRI summarization reduces the number of routes in the RIB.

# NLRI Summarization

OSPF summarization is implemented in two ways:

- Per-prefix summarization
- Per-LSA summarization: remove all inter-area routes and replace them with the shortest possible match, a default route (essence of stub areas).

Prefix summarization can only occur between areas and at the OSPF domain boundary with an external domain. Filtering is enforced at common transit points i.e. ABR. ABR controls

which LSAs enter the area. Network layer reachability information removed is replaced with a default route. All routers in the area must agree on the stub flag.

Internal summarization is performed by ABR and summarizes type 1 LSAs into type 3. External summarization summarizes type 5 into type 5 and type 7 into type 7 LSAs by ASBR.

### Summary Discard Route

When summarizing, OSPF creates a local discard route to Null0. The goal is to drop traffic if longest match is summary. Summary router cannot fall back to default route. Discard route can be disabled with the command: `#no discard-route`

### OSPF Route Summarization

#### Inter-Area Summarization

Link flaps in aggregate prefixes do not trigger SPF calculations in other areas. Summarization is configured on the ABR connected to the area with the source component routes.

```
#area 0 range 10.0.0.0 255.255.128.0
```

If multiple ABRs exist to a given area, summarization should be implemented on all the ABRs that connect to the area whose routes are to be summarized. A summary discard route is installed on the ABR as a loop prevention mechanism. The default metric for the summary LSA is the smallest metric associated with a component network in the aggregated summary route. A cost can be configured to reduce CPU load or as part of traffic engineering.

```
#area o range 10.0.0.0 255.255.0.0 cost 1000
```

Routes can be filtered using the area summarization command by preventing type 3 LSAs from being advertised into another area by appending the `not-advertise` keyword.

```
#area 0 range 10.0.0.0 255.255.0.0 not-advertise
```

Filtering routes using the 'not-advertise' keyword only works on ABRs that are directly donnected to the area whose networks are to the filtered.

#### External Summarization

External summarisation is performed on the redistributing ASBR. In the OSPF process `#summary-address 10.0.0.0 255.255.0.0` A discard route is installed.

## Route Filtering

OSPF route filtering can be implemented through the implementation of:

- stubby areas

- ABR and ASBR route filtering

### Area Filter-List

An ABR is able to filter routes from areas that it is not directly connected to. Filtering routes using a filter list at the ABR is a two-step process that involves creation of a prefix list and application of the prefix list in the OSPF process area command using the filter-list keyword.

```
#ip prefix-list PL_FILTER_120 deny 10.1.120.0/24
#ip prefix-list PL_FILTER_120 permit 0.0.0.0/0 le 32
#area 1 filter-list prefix PL_FILTER_120 in
```

Using the filter list, routes can be filtered as they leave an area or as the enter an area. Either filtering option yields similar results.

#### Local OSPF Route Filtering

Local OSPF route filtering involves preventing a router from installing a network from the LSDB into the RIB. This involves two steps: (1) identification of the route (using an ACL, prefix-list, route-map) and applying the filtering using a distribute-list command.

```
#distribute-list 10 in
```

The filtered route still exists in the LSDB. It is advertised to other routers in LSUs. However, it is not installed into the global/VRF RIB from the LSDB.

#### Filtering at ASBR

Filtering can be applied on the ASBR during redistribution or special treatment of routes can be implemented such as seed-metric, metric type for specific routes using a route-map. It involves the following steps:

1. **Step 1:** Identify the "interesting" using an ACL or prefix list.
   `#access-list 1 permit 10.1.1.0`
2. **Step 2:** Create a route-map:
   `#route-map no16 deny 10 #match ip address 1 #route-map no16 permit 20 #set metric 6789 #set metric-type type-1`
3. **Step 3**: Apply the route-map
   `#redistribute static subnets route-map no16`

### Default Router Propagation

To advertise an existing local router's default route: `#default-information originate`

## Factors Influencing OSPF Scalability

Scaling is determined by the utilization of three router resources: memory, CPU, and interface bandwidth. The workload that OSPF imposes on a router depends on these factors:

- Number of adjacent neighbors for any one router: OSPF floods all link-state changes

to all routers in an area. Routers with many neighbors have the most work to do when link-state changes occur. In general, any one router should have no more than 60 neighbors.
- Number of adjacent routers in an area: OSPF uses a CPU-intensive algorithm. The number of calculations that must be performed given n link-state packets is proportional to n log n. As a result, the larger and more unstable the area, the greater the likelihood for performance problems associated with routing protocol recalculation. Generally, an area should have no more than 50 routers. Areas that suffer with unstable links should be smaller.
- Number of areas supported by any one router: A router must run the link-state algorithm for each link-state change that occurs for every area in which the router resides. Every ABR is in at least two areas (the backbone and one adjacent area). In general, to maximize stability, one router should not be in more than three areas.
- Designated router (DR) selection: In general, the DR and backup designated router (BDR) on a multiaccess link (for example, Ethernet) have the most OSPF work to do. It is a good idea to select routers that are not already heavily loaded with CPU-intensive activities to be the DR and BDR. In addition, it is generally not a good idea to select the same router to be the DR on many multiaccess links simultaneously.
  The first and most important decision when designing an OSPF network is to determine which routers and links are to be included in the backbone area and which are to be included in each adjacent area.

# OSPF Security

## Security Threat Vectors and Motivations

A threat vector is a method or mechanism used to attack a specific system. There are ways that OSPF is attacked.

OSPF is an interior gateway protocol and therefore not exposed to the insecure public Internet. In the design of an OSPF network, OSPF devices should not be allowed to communicate with devices in the public Internet. Because of this, a layer of security is created that protects the OSPF domain from the Internet.As such for an attack on OSPF, some kind of internal access may be required. Multiple ways exist to achieve internal access:

- Gaining wired or wireless network access.
- Exploitation of an insecure system.

OSPF attacks involve listening to OSPF traffic. Listening to OSPF traffic provide the opportunity to modify how this traffic is forwarded. Listening to OSPF traffic can be carried out through packet capture. OSPFv2 traffic does not encrypt traffic. Based on packet captures, it is possible to determine the network design as it offers a comprehensive network view. Through the packet capture, it is possible to determine some of the security mechanisms used to secure OSPF.

The threats to unauthorized access to OSPF could result in the introduction of false link state information that could affect performance and network traffic in a number of different ways:

- **Traffic re-routing** to overwhelm sections of the OSPF domain with link congestion. Traffic re-routing could be done along a longer path to add additional delay.
- **Traffic to nowhere** to cause traffic to never reach its destination.
- **Introduce constant recalculations** to reduce performance of the routing devices themselves through constant changing of link state information being advertised.

# OSPF Security Mechanisms

OSPF requires neighborship formation with multiple matching parameters. RFC 7474 introduced possibilities to lower risks of replay attacks.

# Secure OSPF Communication and Interaction

OSPF supports adjacency authentication to protect the control-plane from routing injection attacks. Every OSPF packet header includes authentication information i.e. hello, LSU, LSR. Three types of authentication are supported:

- Type 0 null: offers no authentication at all
- Type 1 - Simple password option uses cleartext password
- Type 2 - Cryptographic MD5 or SHA). RFC 5709 introduced SHA authentication which uses SHA-1, SHA-256, SHA-384 and SHA-512.

Authentication can be enabled on:

- the OSPF process `#area 0 authentication`
- link level: `ip ospf authentication`

The link level configuration overrides the process level authentication configuration. The password is always configured on the link; `#ip ospf authentication-key password #ip ospf message-digest-key 1 md5 password` Key IDs must match.

Setting area authentication for area zero will require all virtual links to configure that type of authentication. A virtual-link is a member of area zero.

### Verification of Authentication

```
#show ip ospf #show ip ospf interface #show key chain
```

With SHA/MD5 authentication, the packet is not encrypted. A digest of the key ID and password is embedded in the packet header.

# Virtual-link Authentication

A virtual-link is an area 0 interface. It inherits area 0 authentication configurations. The

virtual-link is the interface, the key configuration goes at the interface. Type can be configured globally or at the interface.

The virtual-link runs as a demand circuit. Always clear the virtual-link after configuring authentication.

```
#area 0 virtual-link 4.4.4.4 authentication message-digest
```

OSPF supports the following SHA algorithms: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512. OSPF supports the use of key chains.

```
#ip ospf authentication key-chain OSPF_KEY_CHAIN
```

To define a key chain:

```
#key chain OSPF_KEY_CHAIN
#key 1
#key-string PASSWORD
#cryptographic-algorithm HMAC-SHA-384
```

## Recommendations

It is recommended to implement the highest authentication level supportable on a device. Best to use OSPFv3 to manage IPv4 networks. Though it uses IPv6 for security, it is more secure. Implement the use of passive interfaces. This revents OSPF communications on an interface lowering the possibility of unwanted traffic injection. All interfaces can be configured as passive by default.

# Troubleshooting

Common reasons for sub-optimal traffic flow;

- Auto-cost reference bandwidth is not configured the same throughout the OSPF domain.
- Summarization is not consistently applied on ABRs for inter-area summarization.
- Problems with route redistribution that do not address issues with route feedback.