

Computer Networks 2 | CN2

Summary

CONTENTS

| | |
|--|-----------|
| 1. Routing | 2 |
| 2. OSPF (Open Shortest Path First) | 2 |
| 2.1. Network hierarchy | 2 |
| 2.2. Area types | 2 |
| 2.3. Router classification | 3 |
| 2.4. Network types | 4 |
| 2.5. Virtual links | 4 |
| 2.6. Link State Advertisement (LSA) Types | 4 |
| 2.7. Flooding | 5 |
| 2.8. Packet format | 5 |
| 2.8.1. Hello Packet | 5 |
| 2.8.2. Database Description Packet | 6 |
| 2.8.3. Link State Request Packet | 7 |
| 2.8.4. Link State Update Packet | 7 |
| 2.8.5. Link State Acknowledgement Packet | 8 |
| 2.9. Sub-Protocols | 8 |
| 2.9.1. Hello Protocol | 8 |
| 2.9.2. Database Synchronization Protocol | 8 |
| 2.10. Routing computation and Equal-Cost MultiPath | 9 |
| 3. IS-IS | 10 |
| 4. BGP | 10 |
| 5. BGP Advanced | 10 |
| 6. Network Design | 10 |
| 7. MPLS | 10 |
| 8. Overlay Technologies | 10 |
| 9. EVPN / VXLAN | 10 |
| 10. CND | 10 |
| 11. QoS | 10 |

1. ROUTING

TODO:

Table [AD] [Cost] [If] [Net]

```
Router# show ip route
```

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived

C - connected, S - static, E - EGP derived, B - BGP derived

* - candidate default route, IA - OSPF inter area route

E1 - OSPF external type 1 route, E2 - OSPF external type 2

```
route
```

```
Gateway of last resort is 131.119.254.240 to network 129.140.0.0
```

```
O E2 150.150.0.0 [160/5] via 131.119.254.6, 0:01:00, Ethernet2
```

```
E 192.67.131.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
```

```
O E2 192.68.132.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
```

```
O E2 130.130.0.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
```

```
E 128.128.0.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
```

```
E 129.129.0.0 [200/129] via 131.119.254.240, 0:02:22, Ethernet2
```

2. OSPF (OPEN SHORTEST PATH FIRST)

OSPF is an instance of a link state protocol designed for intra-domain routing in an IP network. OSPF gathers link state information from available routers and constructs a topology map of the network. It was introduced in 1989 and is widely used in large enterprise networks.

The used version of OSPF in IPv4 networks is known as OSPF version 2 (OSPFv2). OSPF for IPv6 networks is known as OSPFv3.

2.1. NETWORK HIERARCHY

OSPF provides the functionality to divide an intra-domain network into sub-domains, commonly referred to as areas. Every intra-domain must have a core area, referred to as a backbone area or top level area. All other areas connected to the backbone area are referred to as low-level areas. This means that the backbone area is in charge of summarizing the topology of one area to another area and vice versa. A core area is identified with Area ID 0. Areas are identified through a 32-bit area field. Area ID 0 is the same as 0.0.0.0.

TODO:

Network diagram

2.2. AREA TYPES

- Stubby = Eliminates all external routes (type 5)
- Totally stubby = Additionally eliminates all inter-area routes (type 3)

| Term | Definition |
|-------------------------|--|
| Area 0 Backbone Area | |
| Area 1 Stub Area | <ul style="list-style-type: none"> – Eliminates all external routes (type 5) – Creates a default route |

| <i>Term</i> | <i>Definition</i> |
|---|--|
| Area 2 Standart Area | – All routes present |
| Area 3 Totally Stubby Area | – Eliminates all external routes (type 5) – Eliminates all inter-area routes (type 3) – Creates a default route |
| Area 4 (NSSA) Not so Stubby Area | – Eliminates all external routes* (type 5) – No default route – Creates own area type 7 LSA * advertises area 4 ASBR redistributed external routes as LSA type 7 in area 4 itself. When traversing to a different OSPF area, it transforms them to a regular type 5 LSA |
| Area 5 (Totally NSSA) Totally Not so Stubby Area | – Eliminates all external routes* (type 5) – Eliminates all inter-area routes (type 3) – Creates a default route – Creates own area type 7 LSA * advertises area 5 ASBR redistributed external routes as LSA type 7 in area 5 itself. When traversing to a different OSPF area, it transforms them to a regular type 5 LSA |

TODO:

2.3. ROUTER CLASSIFICATION

The routers are classified into four different types according to [RFC 2328](#)

| <i>Term</i> | <i>Definition</i> |
|----------------------------|---|
| Internal Routers | A router with all directly connected networks belonging to the same area. These routers run a single copy of the basic routing algorithm. |
| Area Border Routers (ABR) | A router that attaches to multiple areas. Area border routers run multiple copies of the basic algorithm, one copy for each attached area. Area border routers condense the topological information of their attached areas for distribution to the backbone. The backbone in turn distributes the information to the other areas. |
| Backbone Routers | A router that has an interface to the backbone area. This includes all routers that interface to more than one area (i.e., area border routers). However, backbone routers do not have to be area border routers. Routers with all interfaces connecting to the backbone area are supported. |
| AS Boundary Routers (ASBR) | A router that exchanges routing information with routers belonging to other Autonomous Systems. Such a router advertises AS external routing information throughout the Autonomous System. The paths to each AS boundary router are known by every router in the AS. This classification is completely independent of the previous classifications: AS boundary routers may be internal or area border routers, and may or may not participate in the backbone. |

TODO:

Diagram

2.4. NETWORK TYPES

OSPF is designed to address four different types of networks:

Point-to-point networks refer to connecting a pair of routers directly by an interface/link.

Broadcast networks refer to networks such as LANs connected by a technology such as Ethernet. Broadcast networks, by nature, are multi-access where all routers in a broadcast network can receive a single transmitted packet. In such networks, a router is elected as a Designated Router (DR) and another as a Backup Designated Router (BDR).

Non-broadcast multi-access networks (NBMA) are networks where more than two routers may be connected without broadcast capability. Such networks require an extra configuration to emulate the operation of OSPF on a broadcast network. Like broadcast networks, NBMA networks elect a DR and a BDR.

Point-to-multipoint networks are also non-broadcast networks much like NBMA networks. However, OSPF's mode of operation is different and is similar to point-to-point links. The two most commonly used network types are point-to-point networks and broadcast networks.

TODO:

Diagram

2.5. VIRTUAL LINKS

OSPF Design Rule 1: Area 0 has to be contiguous. For example, if a backbone is partitioned into two parts due to a link failure, virtual links are used. In such a case, virtual links are tunnelled through a non-backbone area

TODO:

Diagram

OSPF Design Rule 2: A non-backbone area has to be connected to the backbone area. Virtual links are used to connect an area to the backbone using a non-backbone (transit) area. Virtual links are configured between two Area Border Routers.

TODO:

Diagram

2.6. LINK STATE ADVERTISEMENT (LSA) TYPES

OSPF floods routing information such as link state advertisements. The scope of flooding of OSPF packets depends on the LSA types. The four most commonly known LSA types are:

TODO:

Diagrams

| Term | Definition |
|-----------------------------|--|
| Router LSA (Type Code=1) | A Router LSA is the most basic link state advertisement that is generated for each interface. Every router generates a Router LSA that lists all the routers' outgoing interfaces. For each interface, the state and cost of the link are included. Such LSAs are generated for point-to-point links. Flooding of Router LSAs is restricted to the area where they originate. |

| <i>Term</i> | <i>Definition</i> |
|--------------------------------------|---|
| Network LSA (Type Code=2) | Network LSAs are applicable in broadcast and non-broadcast networks where they are generated by the DR. A Network LSA represents a LAN. All attached routers and the DR are listed in the Network LSA. Flooding of Network LSAs is also restricted to the area where they originate. |
| Network Summary LSA (Type Code=3) | Area Border Routers (ABR) generate Network Summary LSAs that are used for advertising destinations outside an area. Those LSAs are flooded in all the areas that are not totally stubby. |
| AS External LSA (Type Code=5) | AS External LSAs are generated by Autonomous System Boundary Routers. Destinations external to an OSPF AS are advertised using AS external LSAs. AS external LSAs are flooded in all the areas that are neither stub nor totally stubby. |

TODO:

Type 7

2.7. FLOODING

TODO:

Diagram?

OSPF sits directly on top of IP in the TCP/IP stack by using the IP protocol number 89. OSPF packets use the multicast destination MAC address 224.0.0.5. OSPF is required to provide its own reliable mechanism, instead of being able to use a reliable transport protocol such as TCP. OSPF addresses reliable delivery of packets through use of either an implicit or explicit acknowledgment.

- An **implicit acknowledgment** means that a duplicate of the LSA as an update is sent back to the router from which it received the update.
- An **explicit acknowledgment** means that the receiving router sends a link state acknowledgment packet on receiving a link state update.

Since a router may not receive acknowledgment from its neighbor to whom it sent a link state update message, a router is required to track a link state retransmission list of outstanding updates.

- An LSA is retransmitted, always as unicast, on a periodic basis until an acknowledgment is received, or the adjacency is no longer available.
- A router floods all its LSAs every 30 minutes, regardless of whether the content of the LSA such as the metric value has changed. Hence, the Link State Database (LSDB) is always synchronized between all routers in an area

2.8. PACKET FORMAT

OSPF has 5 packet types:

- 1) hello
- 2) database description (DBD or DD)
- 3) link state request (LSR)
- 4) link state update (LSU)
- 5) link state acknowledgement (LSAck)

2.8.1. Hello Packet

The primary purpose of the hello packet is to establish and maintain adjacencies. The hello packet is also used in the election process of the Designated Router and Backup Designated Router in broadcast networks. Moreover, it is used for negotiating optional capabilities.

| | | |
|--------------------------|---------|----------|
| ← 32 bit → | | |
| Network Mask | | |
| Hello Interval | Options | Priority |
| Router Dead Interval | | |
| Designated Router | | |
| Backup Designated Router | | |
| Neighbors (4 bytes each) | | |

| Field | Definition |
|-----------------------------------|---|
| Network Mask (32 bit) | This is the address mask of the router interface from which this packet is sent. |
| Hello Interval (16 bit) | This field designates the time difference in seconds between any two hello packets. The sending and the receiving routers are required to maintain the same value. Otherwise, a neighbor relationship between these two routers is not established. For point-to-point and broadcast networks, the default value is 10 sec, while for other network types the default value used is 30 sec. |
| Options (8 bit) | Options fields allow compatibility with a neighboring router to be checked. |
| Priority (8 bit) | This field is used when electing the designated router and the backup designated router. |
| Router Dead Interval (32 bit) | This is the length of time in which a router will declare a neighbor to be dead if it does not receive a hello packet. This interval needs to be larger than the hello interval. The neighbors also need to agree on the value of this parameter. This way, a routing packet that is received and does not match this field on a receiving router's interface folder is dropped. The default value is typically four times the default value for the hello interval. In point-to-point networks and broadcast networks, the default value used is 40 sec while in other network types, the default value used is 120 sec. |
| Designated Router (32 bit) | DR (BDR) field lists the IP address of the interface of the DR (BDR) on the network, but not its router ID. If the DR (BDR) field is 0.0.0.0, this means that there is no DR (BDR). |
| Neighbors (4 bytes each) (32 bit) | This field is repeated for each router from which the originating router has received a valid Hello recently, meaning in the past Router Dead Interval. |

2.8.2. Database Description Packet

The database description packet contains a summary of all the LSAs (not the entire LSAs) that the neighboring router has in its LSDB. The OSPF database description packet has the following key features and fields:

| | | |
|--------------------|---------|------------------------|
| ← 32 bit → | | |
| Interface MTU | Options | 0 0 0 0 0 I M MS |
| DD Sequence Number | | |

| |
|-------------|
| ← 32 bit → |
| LSA Headers |

| <i>Field</i> | <i>Definition</i> |
|-----------------------------|---|
| Interface MTU (16 bit) | This field indicates the size of the largest transmission unit the interface can handle without fragmentation. |
| Options (8 bit) | Options fields consist of several bit-level fields. The most interesting one is the E-bit which is set when the attached area is capable of processing AS-external-LSAs. |
| I (1 bit) | I-bit (initial-bit) is initialized to 1 for the initial packet that starts a database description session; for other packets for the same session, this field is set to 0. |
| M (1 bit) | M-bit (more-bit) is used to indicate that this packet is not the last packet for the database description session by setting it to 1; the last packet for this session is set to 0. |
| MS (1 bit) | MS-bit (master-slave bit) is used to indicate that the originator is the master by setting this field to 1, while the slave sets this field to 0. |
| DD Sequence Number (32 bit) | This field is used for incrementing the sequence numbers of packets from the side of the master during a database description session. The master sets the initial value for the sequence number. |
| LSA Headers (32 bit) | This field lists headers of the link state advertisements in the originator's link state database. |

2.8.3. Link State Request Packet

The link state request packet is used for pulling information. Once the database description has been received from a neighbor, a router knows which LSAs are not in its LSDB and will request the entire missing LSAs from that neighbor. The fields are repeated for each unique entry:

| |
|--------------------|
| ← 32 bit → |
| Link State Type |
| Link State ID |
| Advertising Router |

| <i>Field</i> | <i>Definition</i> |
|-----------------------------|--|
| Link State Type (32 bit) | This field identifies a link state type such as a router or network. |
| Link State ID (32 bit) | This field is dictated by the link state type. |
| Advertising Router (32 bit) | This is the address of the router that has generated this LSA. |

2.8.4. Link State Update Packet

This packet is the answer to a Link State Request Packet. It contains the first field to be the number of LSAs followed by information on LSAs that match the LSA packet format. A link state update packet can contain one or more LSAs.

| |
|----------------|
| ← 32 bit → |
| Number of LSAs |

| | |
|------------|--|
| ← 32 bit → | |
| LSAs | |
| ... | |
| LSAs | |

2.8.5. Link State Acknowledgement Packet

Link State Acknowledgment Packets are OSPF packet type 5. Each newly received LSA must be acknowledged. This is usually done by sending Link State Acknowledgment packets. However, acknowledgments can also be accomplished implicitly by sending Link State Update packets.

Many acknowledgments may be grouped together into a single Link State Acknowledgment packet. Such a packet is sent back out the interface which received the LSAs.

A Link State Acknowledgment Packet contains a regular OSPF header with the type field set to 5 and a set of one or more LSA headers as payload.

TODO:

descriptions, OSPF Header

| | | |
|----------------|------|---------------|
| ← 32 bit → | | |
| Version | Type | Packet Length |
| Router ID | | |
| Area ID | | |
| CheckSum | | AuType |
| Authentication | | |
| Authentication | | |
| LSA Headers... | | |

2.9. SUB-PROTOCOLS

2.9.1. Hello Protocol

During initialization/activation, the hello protocol is used for neighbor discovery as well as to agree on several parameters before two routers become neighbors.

- When using the hello protocol, logical adjacencies are established for point-to-point, point-to-multipoint, and virtual link networks.
- For broadcast and NBMA networks, not all routers become logically adjacent. The hello protocol is used for electing Designated Routers and Backup Designated Routers.

While its name seems to imply that the hello protocol is just responsible for the initialization, it is actually much more than that. After initialization, for all network types the hello protocol is used for keeping alive connectivity which ensures bidirectional communication between neighbors. If the keep alive hello messages are not received within a certain time interval that was agreed upon during initialization, the link/connectivity between the routers is assumed to be not available.

2.9.2. Database Synchronization Protocol

TODO:

chronos diagram

TODO:

shorten description

Beyond basic initialization to discover neighbors, two adjacent routers need to build adjacencies. A complete link state advertisement of all links in the database of each router can be exchanged, but a special database description process is used to optimize this step. During the database description phase, only headers of link state advertisements are exchanged. Headers serve as adequate information to check if one side has the latest LSA. Since such a synchronization process may require exchange of header information about many LSAs, the database synchronization process allows for such exchanges to be split into multiple chunks.

These chunks are communicated using database description packets by indicating whether a chunk is an initial packet (using I-bit), or a continuation/more packet or last packet (using M-bit). One side needs to serve as a master (MS-bit) while the other side serves as a slave. The neighbor with the lower router ID becomes the slave.

- 1) Exchange Start: After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multi-access networks), the routers transition to the exstart state. In this state, the neighboring routers establish a master/slave relationship (the router with the highest Router-ID becomes the master) and determine the initial database descriptor (DBD) sequence number to use while exchanging DBD packets.
- 2) Exchange: Once the master/slave relationship has been negotiated, the neighboring routers transition into the exchange state. In this state, the routers exchange DBD packets, which describe their entire link-state database.
- 3) Loading: When the last step of synchronization has been completed.
- 4) Full: For link-state requests and updates (entire LSAs), for which either side requires updated information, communication occurs in full state until there are no more link-state requests.

2.10. ROUTING COMPUTATION AND EQUAL-COST MULTIPATH**TODO:**

all this stuff

3. IS-IS

4. BGP

5. BGP ADVANCED

6. NETWORK DESIGN

7. MPLS

8. OVERLAY TECHNOLOGIES

9. EVPN / VXLAN

10. CND

11. QOS