OSPF-A Deep Study

N.Rajee Meena
Research Scholar, Department of Computer Science
Vels University, Chennai, Tamil Nadu, India.

Sreeja.V.S
Assistant Professor, Departmentof Computer Science
Vels University, Chennai, Tamil Nadu, India

Abstract- The scope of this study is to discover a link between larger network, or when they need very fast convergence. For this issue, OSPF has been introduced. The main aim of this study is to avoid the data flooding between the areas. Open Shortest Path First (OSPF) is not exclusive for single individual; single connected network can be controlled extraordinary levels. OSPF is a well channeled routing protocol. It has better managing properties because of differentiation in tiny parts in whole network. Construction of OSPF is critical since it is dealing with many protocols, packets and database.

Keywords - OSPF, Link-state Advertisement, Packet header, Router, protocol.

I.BACKGROUND ANALYSIS

OSPF protocol has been introduced to assist internet users to provide peak functional and open accessible Internal gateway protocol for TCP/IP protocol family. Since 1991, IGP for internet not finalized, meanwhile the developers of OSPF request that OSPF be considered for advancement to Draft Internet Standard.

The OSPF protocol is based on link-state technology, which is a departure from the Bellmen- Ford vector based algorithms used in traditional Internet routing protocols such as **RIP**. The authors of OSPF has founded new concepts in the routing protocol such as, Authentication of routing updates, Variable Length Subnet Masks (VLSM), Route Summarization, and so onwards.

II. INTRODUCTION

The routes of the first internet protocol (IP) are static and the loops have been used for defence applications, Likewise the Routing Information Protocol (RIP), the OSPF is also the distance vector algorithms. IP address depletion or IP address summarization needs to be concentrated. Hierarchy is not feasible in the routing protocol. Reliability of the physical layer was unknown because the network is flapping disrupted.

Routing protocols must provide stability, and security, and converge quickly. Internet and IP commonly associated with BGP, RIP and OSPF. OSPF and RIP are commonly associated within a single domain, because of that generically named as I**nterior Gateways Protocols (IGP)**.

OSPF has 3 versions, version 1 was never deployed in the real network, currently version 2 is deployed in IPV4 and Version 3 is deployed in IPV6 networks. It uses reserved multicast IP addresses **224.0.0.5 (all SPF routers) & 224.0.0.6 (all DR&BDR)** to form adjacency and exchange the updates.

OSPF uses bandwidth as metric to calculate an optimal path, If Multiple paths have same metric then the traffic will be load balanced between the paths. (It only supports equal cost load balancing). It is an open standard protocol and runs on IP; the protocol number for OSPF is 89. The OSPF protocol is classified under Interior gateway protocol. It also supports different authentications like Plain text and MD5 for secure routing.

The Open Shortest Path First (OSPF) protocol has unique features when comparing to RIP converges faster, need comparatively less network bandwidth, and can adopt for large networks. OSPF Version 2, described in RFC 1583, is rapidly replacing RIP in the Internet.

2.1 THE NEED FOR ROUTING PROTOCOLS

Swift change is possible with Routes. Mechanical device (hardware) performance related issues may cause the poor reach ability to assigned interface. Routers have an aligned channel to swift update routes that never depend on administrator to make changes. Routers use routing protocols to dynamically manage information received from their own interfaces and from other routers. Routing protocols can be configured to manage manually.

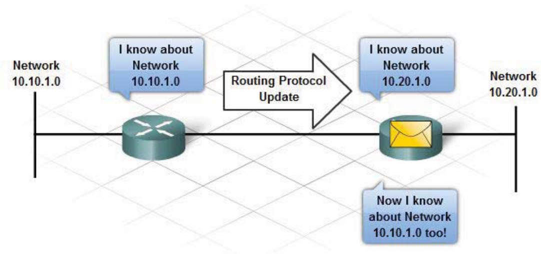


Fig: How routing tables of routers are been updated by a routing protocol

The Above Fig shows two routers, lets says router A and router B connected to two different networks with different IP address, 10.10.1.0 and 10.20.1.0 respectively. Router A uses routing protocol to informs router B that it is connected to a Network 10.10.1.0 while Router B tells Router of Network 10.20.1.0. They do this by updating their respective routing tables.

Advantages of Dynamic routing protocols

- Large networks administrative and overheads will be easy.
- Flexible to avoid time consuming critical process of setting up the static routes
- It allows routers to accept the changes in networks and to modify the routing tables in line with the signals without administrator support.

Best route to destination network known as **routing algorithm** and majorly classified in to two

- Distance vector algorithm
- Link state algorithm

Technology used on said algorithms are completely different.

2.2 OSPF Router

OSPF routers are determined by a router's function and/or location within an OSPF area. Best routes for point of destination arrived by creating or by using prevailing table of the available routes and conditions with support of distance and cost algorithms of destination packets.

2.2.1 OSPF ROUTER TYPES

OSPF routers are classified into six types as below

- Designated Router (DR)
- Backup Designated Router (BDR)
- Internal and Backbone Router
- AB router and ASB router

2.2.1.1 Functions of Designated Router:

(i) Behalf of networks Designated Router originates a network-LSA. Set of routers attached to the network listed by LSA including designated router.

(ii) The Designated Router positioned adjacent to all other routers, because link state synchronized across adjacencies. Designated Router plays a central part in the synchronization process.

2.2.1.2 Backup Designated Router

In the Backup Designated Router the routers are adjacent to all routers on the network, and become Designated Router while the previous Designated Router fails to send the data. There is no need to generate a network-LSA for the network by the Backup Designated router.

The Hello Protocol elects the Backup Designated Router. It has a field to specify the Backup Designated Router for the routed network. The Backup Designated Router performs a lesser function during the flooding procedure than the Designated Router. On the other hand, the Hello packets on broadcast and NBMA networks elect the Designated Router and Backup Designated Router.

2.2.1.3 Internal Router

The devices that connect the router to only one OSPF area are called *internal routers*. Interfaces on internal routers are directly coupled to networks within a single area. By using the single copy of the basic routing algorithm, the router can link with an area. An internal router has all its interfaces in a single area.

2.2.1.4 Backbone Router

If the routing devices have one or more interfaces that connected to the OSPF backbone area is called Backbone Router. Routers interface to more than one area.

2.2.1.5 Area Border Router (ABR)

By connecting one or more areas to the main backbone network the Area Border Router can be established. The multiple copies of the link-state database is stored in memory, to build a link to the connected router.

Area border routers can run multiple copies of the basic algorithm, one copy for each attached area.

2.2.1.6 Autonomous System Boundary Router (ASBR)

Routing devices that replace routing information with other routing devices in non-OSPF networks are called Autonomous System boundary routers. The network can be an ABR, a backbone router, or an internal router. These are all depending upon the location of the Autonomous System boundary router.

An autonomous system boundary router (ASBR) is the gateway for the external routes; it can be located anywhere in the OSPF domain. It can be Internal/ Backbone/ABR.

2.3 OSPF Route Types

OSPF routes are classified into three types which are

1) Intra Area routes
2) Inter Area routes
3) External routes

2.3.1 Intra Area routes:

The routes are originated within the area and exchanged between the internal routers and ABR, In routing table the routes are denoted as O.

2.3.2 Inter Area routes:

The routes are originated at different areas and entering into one area via Area Border Routers, It's denoted as O IA in the routing table.

2.3.3 External Routes:

The routes are originated at different routing domain and injected into OSPF by redistribution at ASBR. These external routes are further classified into four types

1) External Type 1
2) External Type 2
3) NSSA External Type 1
4) NSSA External Type 2

2.4 OSPF application Area

Sub domains of OSPF network called area and it is a collection of logical OSPF networks, routers and links which is having same area of identification. A topological database should maintain by a router within a area.

A router should not be in more than three areas.

OSPF uses a two-layer area hierarchy:

(i) Backbone area
(ii) Non – Back bone area

2.4.1 Backbone area

Backbone area is called as Area 0, all the non-backbone areas must be connected with the backbone area (It can be either direct connection or through Virtual links).

It is responsible for distribution of routing updates between the non-backbone areas. It should be spreadable, but no need to be physically spreadable. Area 0 cannot be configured as Stub/Totally Stub/NSSA/Totally NSSA. All OSPF areas must connect to the backbone area.

2.4.2 Standard Area:

It is default area type in OSPF domain, all type of OSPF routes (O, O IA, O E1, O E2) are allowed in this area.

2.5 Link-state advertisement

The link-state advertisement (LSA) is a basic communication means of the OSPF routing protocol for the Internet Protocol (IP). Within the same area the router communicates with other local routers. Scalability is the main issue in OSPF protocol. A simple update on a router's link status, so one will be sent when a link is connected, disconnected, or otherwise changed.

The LSA types are described below:

• Router LSA (Type 1) – In this Type1, there is a list of all links local to the router. The status and "cost" of those links are generated by all routers in OSPF. Within the local area the routers are snowed under.
• Network LSA (Type 2) –Designated Routers established this type in OSPF, and inherits all routers that are to be attached to the Designated Router.
• Network Summary LSA (Type 3) –It can have a list of all destination networks within an area. Inter-area communication has been happened in this type by sending between areas.
• ASBR Summary LSA (Type 4) –Established by ABRs in OSPF, and have a route to any ASBRs in the OSPF system. ABR send the Type 4 LSAs into its local area. The internal routers should know how to exit the Autonomous System.
• External LSA (Type 5) – Generated by ASBRs in OSPF, and the routes to destination networks outside the local Autonomous System are provided. Default route can be passed to all areas in the OSPF system.

2.6 OSPF Process:

The OSPF network constructs and sustains three non identical tables:

• Neighbor table – containing all neighboring routers.
• Topology table – containing possible routes in all linked networks within area.
• Routing table – contain the best route for each known network.

2.7 OSPF Neighbors

Adjacency is defined as the relationships between the neighbor with other routers in the same network. Network can share the routing information after establishing the adjacency in the area.

Unique router ID for each OSPF router and following are the ways to determine the router

• It can be specified manual.
• The Router ID can be configured by highest IP address on Loopback interface on the router.
• If there is no loopback interface, the highest IP address can be used on any Physical interface and it become the Router ID.

Some of the Conditions are Area ID, Area Type (stub, NSSA, etc.), Prefix, Subnet Mask, Hello Interval, Dead Interval, Network Type (broadcast, point-to-point, etc.), Authentication

2.7.1 OSPF Neighbor States:

While forming OSPF adjacency the OSPF routers will move to multiple states, these states are listed as below

1. Down state
2. Attempt state
3. Init state
4. 2-Way state
5. Exstart state
6. Exchange state
7. Loading state
8. Full state

2.7.1.1 Down:

It is the initial state in the Ospf neighbor conversation. This state indicates that no hellos heard from that interface or from the neighbor (if adjacency was already formed) within the Router Dead Interval. If a neighbor transition to down state from any other state, the LS Retransmission list, LS Request list and Database Summary list are cleared.

2.7.1.2 Attempt:

This state only involved for manually configured neighbors in the Non-Broadcast Multi Access Network. In this state router will send unicast hello packets to the neighbors either to form new adjacency or recover the adjacency with neighbor from which the hellos were never reached within the Dead interval.

2.7.1.3 Init:

This state indicates the router has received hellos within the specified dead interval.

2.7.1.4Way:

Two-way communication has been recognized between that routers which mean the routers seen their own Router IDs in the neighbor field of the hellos. It means that each router has seen the other's hello packet.

In this state Designated and Backup Designated Routers will be elected for Broadcast and Non-Broadcast Multi-access networks. In Broadcast and NBMA networks all routers have full adjacency only with DR & BDR. The Adjacency between DR OTHER stays in 2-way.

2.7.1.5 Exstart:

By exchanging the process of link state information the DR and BDR are preferred. In this state, the routers and their DR and BDR The relationship of master-slave is created by DR and BDR and chooses the initial sequence number for formation of adjacency. The Master that having the higher router ID started to exchange by increment the sequence number. The relationships are formed between routers to determine who will start to exchange.

2.7.1.6 Exchange:

In this stage the routers are exchanging Database Descriptors (DBDs). The description of the router's Topology Database is taken in DBDs.

2.7.1.7 Loading:

The routers are finally exchanging Link State Advertisements, contain information about all links connected to each router.

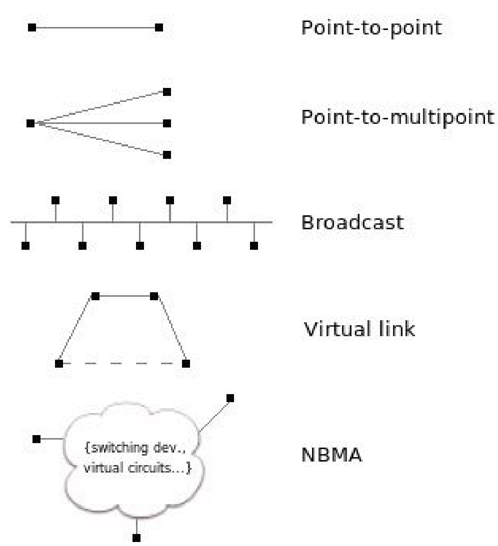
2.7.1.8 Full:

The routers are fully coordinated. The topology table of all routers in the area should be identical.

Depending on the "role" of the neighbour, the state may appear as:

• Full/DR
• Full/BDR
• Full/DR Other

2.8 OSPF Network Types



2.9 OSPF Packet Types

There are five packet types used in OSPF. **Version (1 octet)**

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

Type (1 octet)

This field specifies the type of OSPF packet. Possible values include:

- Hello packet
- Database descriptor
- Link-state request
- Link-state update
- Link-state acknowledgment

Packet Length (2 octets)

This field displays the total length, in octets, of the OSPF packet.

Router ID (4 octets)

The router ID of the advertising router appears in this field.

Area ID (4 octets)

This field contains the 32-bit area ID assigned to the interface used to send the OSPF packet.

Checksum (2 octets)

This field displays a standard IP checksum for the entire OSPF packet, excluding the 64-bit authentication field.

Authentication Type (2 octets)
The specific type of authentication used by OSPF is encoded in this field. Possible values are:

0—Null authentication
1—Simple password
2—MD5 cryptographic authentication
Authentication (8 octets)
This field displays the authentication data to verify the packet's integrity.

2.9.1 Hello Packet

To establish and maintain a neighbor relationship, an OSPF-speaking router determines whether any directly connected routers also speak OSPF. The router sends an *OSPF hello packet* out all configured interfaces and awaits a response.

The hello packet, type code 1, is addressed to the All SPF Routers multicast address of 224.0.0.5 for broadcast and point-to-point connections. Other connection types unicast the hello packet to their neighbor.

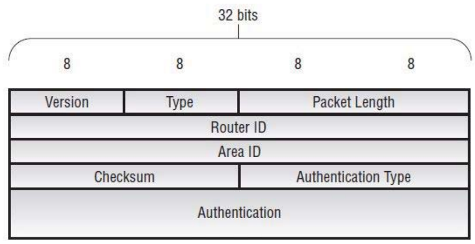
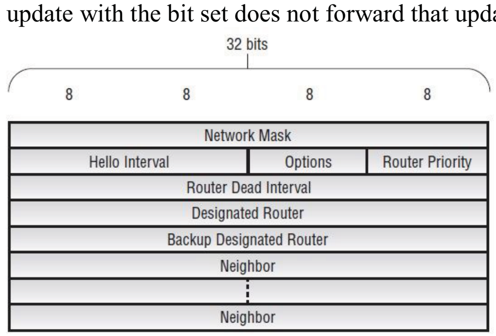


Fig. The OSPF Common Header

The packet includes the following fields:
Network Mask (4 octets)
This field contains the subnet mask of the advertising OSPF interface. virtual links set this value to 0.0.0.0.

Hello Interval (2 octets)
This field displays the value of the *hello interval* requested by the advertising router. Possible values range from 1 to 255, with a default value of 10 seconds.
Options (1 octet)
Each bit in the Options field represents a different function. The various bit definitions are:

Bit 7
The DN bit is used for loop prevention in a Virtual Private Network (VPN) environment.
An OSPF router receiving an update with the bit set does not forward that update.



Bit 6
The O bit indicates that the local router supports opaque LSAs.
Bit 5
The DC bit indicates that the local router supports Demand Circuits. The JUNOS software does not use this feature.

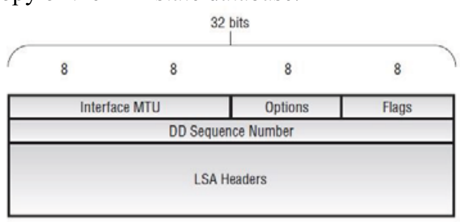
Bit 4
The EA bit indicates that the local router supports the External Attributes LSA for carrying BGP information in an OSPF network. The JUNOS software does not use this feature.
Bit 3

The N/P bit describes the handling and support of not-so-stubby LSAs.
Bit 2
The MC bit indicates that the local router supports multicast OSPF LSAs. The JUNOS software does not use this feature.
Bit 1
The E bit describes the handling and support of external LSAs.
Bit 0
The T bit indicates that the local router supports TOS routing functionality. The JUNOS software does not use this feature.

Router Priority (1 octet)
This field contains the priority of the local router. The value is used in the election of the designated router and backup designated router. Possible values range from 0 to 255, with a default value of 128.
Router Dead Interval (4 octets)
This field shows the value of the *dead interval* requested by the advertising router. Possible values range from 1 to 65,535. The JUNOS software uses a default value of 40 seconds.
Designated Router (4 octets)
The interface address of the current designated router is displayed in this field. A value of 0.0.0.0 is used when no designated router has been elected.
Backup Designated Router (4 octets)
The interface address of the current backup designated
Router is displayed in this field. A value of 0.0.0.0 is used when no backup designated router has been elected.
Neighbor (Variable)
This field displays the router ID of all OSPF routers for which a hello packet has been received on the network segment.

2.9.2 DATABASE DESCRIPTION PACKET

After discovering its neighbors, the local router begins to form an adjacency with each neighbour. This adjacency process requires that each router advertise its local database information. An OSPF router uses the *Database Description (DD) packet* for this purpose. The DD packet, type code 2, summarizes the local database by sending LSA headers to the remote router. The remote router analyzes these headers to determine whether it lacks any information within its own copy of the link-state database.



The fields include the following:
Interface MTU (2 octets)
This field contains the MTU value, in octets, of the outgoing interface. When the interface is used on a virtual link, the field is set to a value of 0x0000.
Options (1 octet)
The local router advertises its capabilities in this field. **Flags (1 octet)**
This field provides an OSPF router with the capability to exchange multiple DD packets with a neighbor during an adjacency formation. The flag definitions include the following:
Bits 3 through 7
These bit values are currently undefined and must be set to a value of 0.
Bit 2
The I bit, or Initial bit, designates whether this DD packet is the first in a series of packets. The first packet has a value of 1, while subsequent packets have a value of 0.
Bit 1
The M bit, or More bit, informs the remote router whether the DD packet is the last in a series. The last packet has a value of 0, while previous packets have a value of 1.
Bit 0
The MS bit, or Master/Slave bit, is used to indicate which OSPF router is in control of the database synchronization process. The master router uses a value of 1, while the slave uses a value of 0.
DD Sequence Number (4 octets)

This field guarantees that all DD packets are received and processed during the synchronization process through use of a sequence number. The Master router initializes this field to a unique value in the first DD packet, with each subsequent packet being incremented by 1.

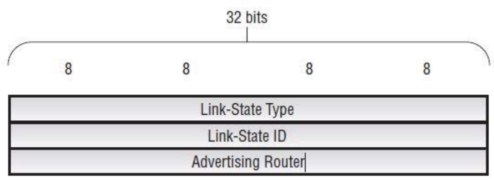
LSA Headers (Variable)

Each header is 20 octets in length and uniquely identifies each LSA in the database. Each DD packet may contain multiple LSA headers.

2.9.3 LINK- STATE REQUEST PACKET

During the database synchronization process, the local router may find that it is missing information or that its local copy is out of date. The local router acquires the needed database information by sending a *link-state request packet* to its neighbouring router.

This packet contains identifiers that uniquely describe the requested LSA. An individual link-state request packet may contain either a single set of identifiers or multiple sets to request multiple LSAs.



The unique LSA identifiers are:

Link-State Type (4 octets)

This field displays the type of LSA being requested.

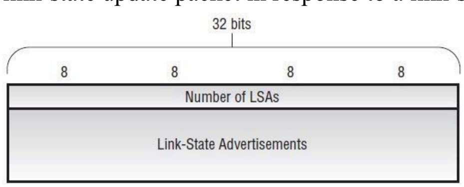
Link-State ID (4 octets) This field encodes information specific to the LSA. Each different type of advertisement places different information here.

Advertising Router (4 octets) The router ID of the OSPF router that first originated the LSA is encoded in this field.

2.9.4 LINK-STATE UPDATE PACKET

Information in the link-state database is populated through a *Link State Advertisement (LSA)*. The local router advertises LSAs within a *link-state update* packet to its neighboring routers.

This packet is reliably flooded throughout the network until each router has a copy. In addition, the local router advertises a link-state update packet in response to a link-state request for information.



The two fields in the packet are:

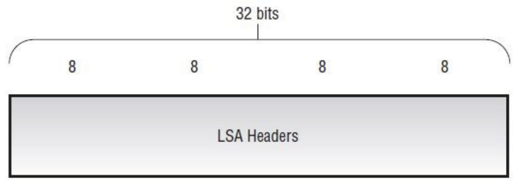
Number of LSAs (4 octets) this field displays the number of LSAs carried within the link state update packet.

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

2.9.5 LINK-STATE ACKNOWLEDGEMENT PACKET

The *reliable* part of the OSPF reliable flooding paradigm arises from the fact that each router is required to explicitly acknowledge the receipt of each LSA. The local router accomplishes this with the *link-state acknowledgment* packet.

The packet, type code 5, simply contains the common OSPF header followed by a list of LSA headers. This variable-length field allows the local router to acknowledge multiple LSAs using a single packet.



III. RESULTS AND FINDINGS

2.10 OSPF FEATURES

OSPF is a well-developed routing protocol. It is suitable for most of networks, especially enterprise network. It has features such as:

1) OSPF gets benefits from the algorithm itself (Link state and shortest path first algorithm), because it is a loop free routing protocol.
2) Recalculation can be easily done and it takes less time to calculate the shortest path.
3) Support load balancing to find the cost of the path.
4) The route information will not increase very rapidly with network expanding.
5) There is an undersized possible of Overload.
67) The two types of packet authentication modes. There are common clear text authentication mode; and cipher text authentication mode with MD5 algorithm.
8) OSPF is suitable for all dimension network， and it can support more than thousands routers at most.

2.11 ADVANTAGES OF OSPF

- OSPF is an unwrap standard, not related to any particular hawker.
- Using multicasting within areas, there is a possible to find the path.
- After initialization, OSPF send the updates on routing table sections; it does not send the entire routing table, which in turn conserves network bandwidth.
- Areas on the OSPF networks can be logically segmented to improve organization, and decrease the size of routing tables.

III. CONCLUSION

OSPF works on a distributed topology database which has to be known by all nodes so that they can define the routes to all the destinations. It is the most generally used protocol within the Internal Gateway Protocol (IGP) group.

This protocol is capable to deal with much structure of networks, such as broadcast, point- to point, point -to- multipoint and NBMA networks, because it provides a specific boundary which permits a node interact efficiently with a routed network. For the ever growing IP networks of today there is a scalable routing solution.

Quick convergence and the robustness of link-state database exchanges are the key features of OSPF networks. Also important is OSPF's improved design for network security.

REFERENCES

[1] E. M. Rover and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications, vol.2
[2] Deepankar Medhi, Karthikeyan Ramasamy, "Network routing : algorithms, protocols, and architectures"
[3] Adrian Farrel, "The Internet and Its Protocols: A Comparative Approach"
[4] Nohl, A.R, Molnar, G "The convergence of the OSPF routing protocol".