Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparison of OSPF in IPv4 and IPv6

Shrinkhala Singhania
VIT University
India

Abstract— IPv6 is the replacement protocol of ipv4. In the year 2011, the last set of IPv4 addresses were bought by Microsoft. With the advent of IPv6, measures were taken for the smooth transition from IPv4 to IPv6 or the working of both the ip subnets in harmony. The traditional IPv4 routing protocols needed to be seamlessly replaced or made compatible with the IPv6 format. IPv6 has a simplified infrastructure and has lower maintenance cost with a wider address space range. The protocols have undergone some significant amount of changes in terms of packet header. Numerous fields have been added/removed in the packet. In this paper, we have done an in-depth comparison of the routing protocol OSPF v2 and v3 at packet level. A lab simulation has been performed and some major differences between the two have been highlighted.

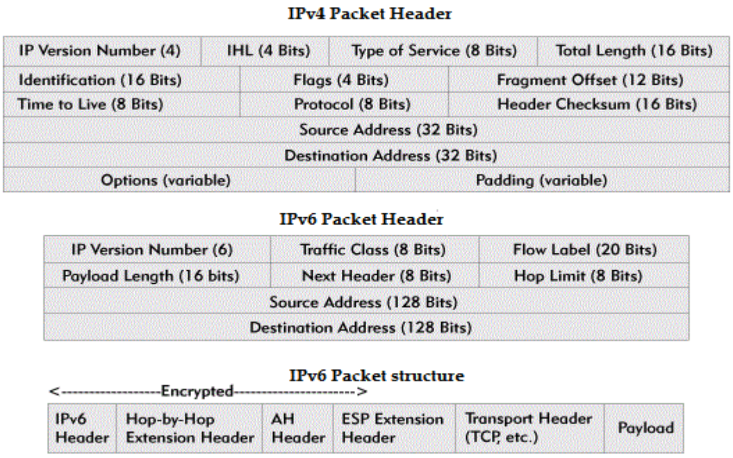
Keywords— IPv6, OSPFv2, OSPFv3, LSA, topology table, routing table, DR, BDR,

I. INTRODUCTION

IPv4 is the fourth revision of the IP protocol and it uses the 32bit addressing scheme. It was first deployed in the ARPANET in the year 1983.For anyone to reach out to the internet, they need a unique IP address. The limited address range of IPv4 (slightly over 4 billion addresses) could not meet the growing demands of the IT sector or the people in general. Network address translation (NAT) was one method introduced to keep a check on the depletion of the IPv4 addresses. Of the approximately four billion addresses allowed in IPv4, three ranges of address are reserved for use in private networks. These ranges are not routable outside of private networks, and private machines cannot directly communicate with public networks. They can, however, do so through network address translation. This helped in conservation of IPv4 addresses to some extent. However, the exhaustion of the address pool was inevitable and was anticipated in the 1980s itself. IPv6 addressing is the new version of internet address protocol and was introduced to support and eventually replace the linchpin of the internet, IPv4.

Ipv6 has a 128 bit addressing space. Apart from providing an enormous range of IP addresses (2^{128} IP addresses) to the internet users, IPv6 has many advantages. The addressing scheme of IPv4 is disjoint, whereas in IPv6 we have global address prefixes, so we do not have to rely on NAT rules or proxy servers. IPv6 is a streamlined version of IPv4. Excluding prioritized delivery traffic, IPv6 has fewer fields to process and fewer decisions to make in forwarding an IPv6 packet.

Unlike IPv4, the IPv6 header is a fixed size (40 bytes), which allows routers to process IPv6 packets faster. It's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection. Route convergence is faster in IPV6 compared to IPv4 when compared in real time traffic therefore resulting in efficient forwarding.



IPv4 Packet Header

IP Version Number (4)	IHL (4 Bits)	Type of Service (8 Bits)	Total Length (16 Bits)
Identification (16 Bits)	Flags (4 Bits)	Fragment Offset (12 Bits)	
Time to Live (8 Bits)	Protocol (8 Bits)	Header Checksum (16 Bits)	
Source Address (32 Bits)			
Destination Address (32 Bits)			
Options (variable)	Padding (variable)		

IPv6 Packet Header

IP Version Number (6)	Traffic Class (8 Bits)	Flow Label (20 Bits)
Payload Length (16 bits)	Next Header (8 Bits)	Hop Limit (8 Bits)
Source Address (128 Bits)		
Destination Address (128 Bits)		

IPv6 Packet structure

<------------------Encrypted---------------------->

IPv6 Header	Hop-by-Hop Extension Header	AH Header	ESP Extension Header	Transport Header (TCP, etc.)	Payload

Fig. 1 Packet Comparison IPv4 and IPv6

It is also said that IPv6 is more secure than IPv4 due to the incorporation of IPSec. Although the IETF mandates that all IPv6 nodes have IPsec available, the actual use of IPsec is optional. If all communications between two IPv6 nodes are encrypted then the network (which is usually trusted because it is centrally managed) becomes blind and cannot inspect the traffic or enforce a security policy. In short, IPsec on IPv6 should be reserved for the same cases as in IPv4: remote access virtual private networks (VPNs) or site-to-site VPNs.

IPv6 supports multicast over unicast. In multicast the sender (source) sends one copy of a single packet addressed to a group of receivers, this helps in saving network bandwidth. Features of QoS (Quality of Service) like traffic shaping, policing and queueing are supported on IPv6.

Till now the dynamic routing protocols were supporting only ipv4 traffic.With the growing dependency on ipv6 addressing a need for routing protocols compatible with ipv6 was also seen. In this paper we talk about the popular routing protocol OSPF and the differences in its packet structure between ipv6 and ipv4. We also highlight the advantages of the protocol when running over IPv6 as compared to IPv4.

II. ROUTING PROTOCOLS

Routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol’s choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available
- The main components of dynamic routing protocols include:

A. Data Structures:

Routing protocols typically use tables or databases for their operations. This information is kept in RAM.

B. Routing Protocol Messages:

Routing protocols use various types of messages to discover neighbouring routers, exchange routing information, and perform other tasks to learn and maintain accurate information about the network.

C. Algorithm:

An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination.

Compared to static routing, dynamic routing protocols require less administrative overhead. However, the expense of using dynamic routing protocols is dedicating part of a router’s resources for protocol operation, including CPU time and network link bandwidth. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice. Networks with moderate levels of complexity may have both static and dynamic routing configured.

III. OSPF- DETAILED DISCUSSION

There are two types of Interior routing protocols, namely, distance vector routing protocol and link state routing protocols.

In order to overcome the limitations of the distance vector routing protocols, the link state routing protocol was introduced. Unlike the distance vector, that uses the DUAL algorithm, the link state uses Dijkstra’s algorithm, also known as shortest path first. In distance vector routing protocol, like EIGRP, the routing table is periodically updated and each router only knows the path to its next hop. In link state routing protocol, like OSPF, by using link state advertisements (LSAs), each router builds its own view of the network, and also maintains a list of neighbours, a list of all routers in its area, and a list of the best paths to each destination. The protocol generates a routing update only when there is a change in the network topology.

The LSAs are transmitted to all the neighbouring devices using multicast address (224.0.0.5/FF02::5) and each device updates its database, known as Link State Database (LSDB), and then forwards the LSAs to all the neighbouring devices. The LSDB then calculates the best routes through the topology by applying the Dijkstra's algorithm. The best routes are then selected from the database and then placed in the routing table. In short, link state routers maintain three databases:

1) topology table
2) routing table
3) adjacency database (neighbour table)

A. OSPF Area Structure:

In link state routing protocols the network is partitioned into areas. The routers then flood the LSAs only within the area and therefore have a smaller topology database and hence the Dijkstra's calculation is easier and takes less time.

It uses a two-layer area hierarchy:

1) Backbone Area (transit area)- This area interconnects with other OSPF area types. The hierarchical area structure requires that all areas connect directly to the backbone area. Usually the end users are not found within the backbone area.

2) Non-backbone area - The main purpose of this area is to connect the end users with the resources. For traffic to reach this area it has to cross the transit area, i.e. two normal areas usually are not connected directly.

Routers that make up only non-backbone areas are known as internal routers and all their interfaces are present in one area only. An area border router (ABR) connects area 0 to non-backbone areas. An ASBR (autonomous system boundary router) is the point where the route redistribution takes place, where two different routing administrations meet.

The ospf routers establish neighborship adjacencies with its neighbouring routers. This is done by exchanging hello packets. Once they become adjacent they exchange link-state information to synchronize the database. Recommended font sizes are shown in Table 1.

Each area in OPSF is labelled with a unique 32 bit area ID. Two routers in the same area have a common area id. In order for two routers to establish adjacency, a two-way communication is required. For this hello packets are periodically exchanged. Following are the conditions to be satisfied for two routers to become neighbours:

1) The area id should match
2) Both OSPF v2 and v3 have the provision for configuring a password for authentication.OSPFv2 uses only md5 authentication, whereas v3 provides 3des as an option as well. However, unlike ospf v2 , ospfv3 uses the IPSec extension Headers to provide authentication and encryption. Packet level discussion is done at a later stage in this paper.
3) The hello and dead intervals of the hello packets (used as keepalives) should match. This is a way of keeping a track of the existence of the neighbour device.
4) The stub area flag field should also match.

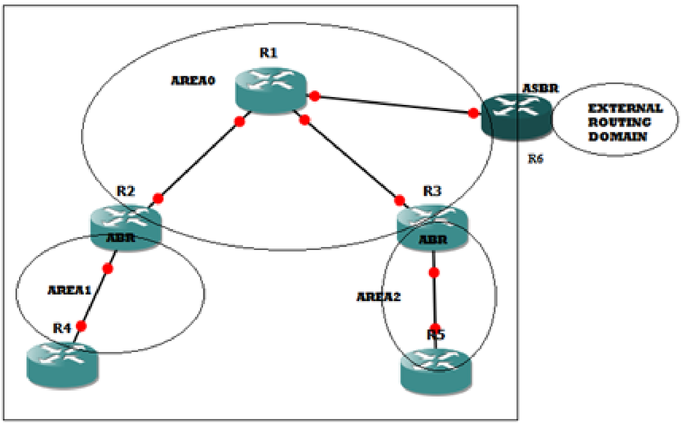


Fig. 2 OSPF Topology

B. Calculation of the OSPF metric:

The best path is calculated with respect to the lowest total cost of the links to a specific destination and is put in the routing table (using Dijkstra's mathematical algorithm). For OSPF, the interface cost is calculated based on its configured bandwidth. This cost is an indication of the overhead required to send packets across a certain interface.

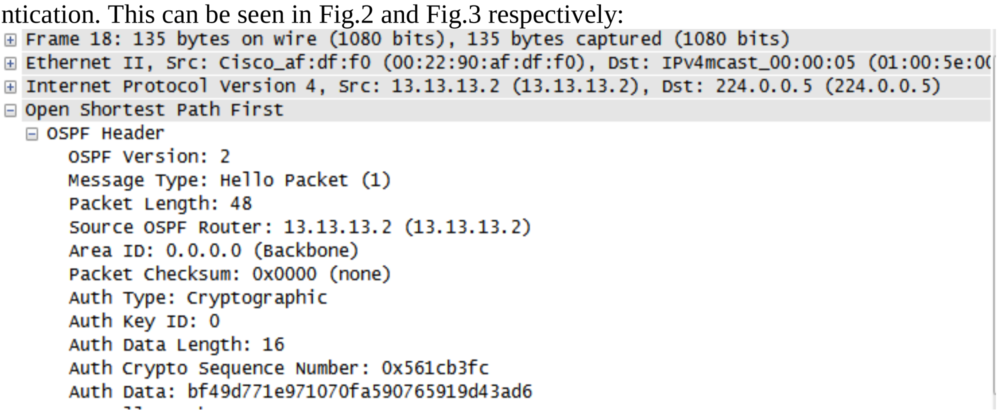
Cost = 100,000,000/bandwidth in b/s

Cost is inversely proportional to the bandwidth of a link. Only one cost is assigned to an interface and is advertised as the link costs in the router link advertisements.

C. Differences between OSPF running on IPv4 and on IPv6:

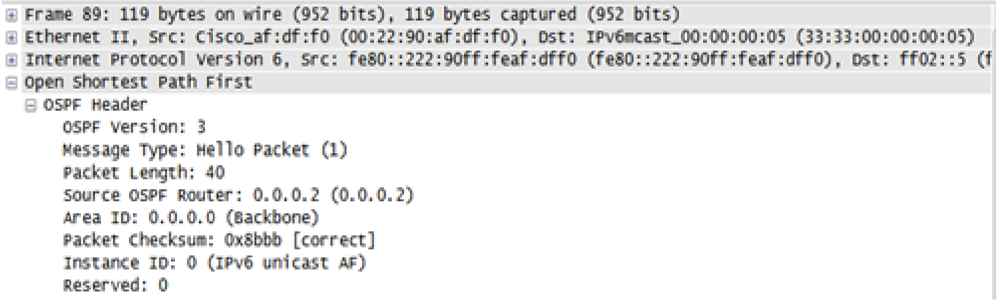
A lab was setup representing the above topology (Fig.1). Based on the traffic captured on the devices, the following differences were then pointed out:

1) The OSPFv3 packets are encapsulated in a 16-byte header frame of IPv6.As mentioned earlier, the authentication header present in OPSFv2 has been removed from OSPFv3 and it relies on the IPsec for authentication. This can be seen in Fig.2 and Fig.3 respectively:



```
⊞ Frame 18: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
⊞ Ethernet II, Src: Cisco_af:df:f0 (00:22:90:af:df:f0), Dst: IPv4mcast_00:00:05 (01:00:5e:0(
⊞ Internet Protocol Version 4, Src: 13.13.13.2 (13.13.13.2), Dst: 224.0.0.5 (224.0.0.5)
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 13.13.13.2 (13.13.13.2)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0x0000 (none)
      Auth Type: Cryptographic
      Auth Key ID: 0
      Auth Data Length: 16
      Auth Crypto Sequence Number: 0x561cb3fc
      Auth Data: bf49d771e971070fa590765919d43ad6
```

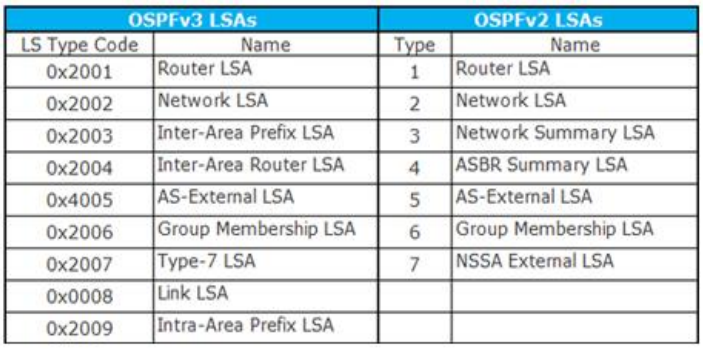
Fig. 3 OSPFv2 Header



```
⊞ Frame 89: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
⊞ Ethernet II, Src: Cisco_af:df:f0 (00:22:90:af:df:f0), Dst: IPv6mcast_00:00:00:05 (33:33:00:00:00:05)
⊞ Internet Protocol Version 6, Src: fe80::222:90ff:feaf:dff0 (fe80::222:90ff:feaf:dff0), Dst: ff02::5 (f
⊟ Open Shortest Path First
  ⊟ OSPF Header
      OSPF Version: 3
      Message Type: Hello Packet (1)
      Packet Length: 40
      Source OSPF Router: 0.0.0.2 (0.0.0.2)
      Area ID: 0.0.0.0 (Backbone)
      Packet Checksum: 0x8bbb [correct]
      Instance ID: 0 (IPv6 unicast AF)
      Reserved: 0
```

Fig. 4 OSPFv3 Header

2) OSPFv3 has the same packets as OSPv2.In addition 2 LSAs have been introduced and type 3 and 4 has been renamed.



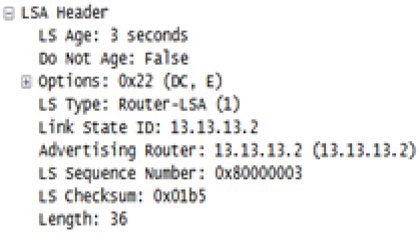
OSPFv3 LSAs		OSPFv2 LSAs	
LS Type Code	Name	Type	Name
0x2001	Router LSA	1	Router LSA
0x2002	Network LSA	2	Network LSA
0x2003	Inter-Area Prefix LSA	3	Network Summary LSA
0x2004	Inter-Area Router LSA	4	ASBR Summary LSA
0x4005	AS-External LSA	5	AS-External LSA
0x2006	Group Membership LSA	6	Group Membership LSA
0x2007	Type-7 LSA	7	NSSA External LSA
0x0008	Link LSA		
0x2009	Intra-Area Prefix LSA		

Fig. 5 LSA Types

1) Link LSA:
   In OSPFv3, Router LSAs contain no address information. The router generates a separate Link LSA for each link it is attached to. A Link-LSA provides the router's link-local address and other addresses on this link to all other routers attached to the link.
2) Intra Area Prefix LSA:
   In OSPFv3 the Type 1 and 2 LSAs do not carry route information, which is therefore carried by Intra Area Prefix LSAs. An Intra-Area-Prefix-LSA can advertise one or more IPv6 address prefixes.
3) An OSPFv2 router discards any unknown LSAs received, whereas OSPFv3 uses the U bit in the LS Type field of LSAs to indicate the mode of processing an unknown LSA:
   1) If the U bit is set to 1, the unknown LSA will be flooded within the range specified in its LS Type field.
   2) If the U bit is set to 0, the unknown LSA will be flooded on the link

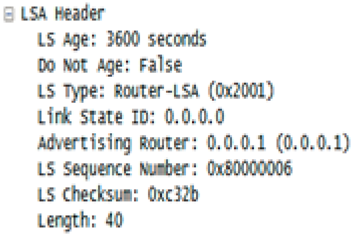
.

4) The difference in the LSA headers can be seen below:



```
⊟ LSA Header
    LS Age: 3 seconds
    Do Not Age: False
  ⊞ Options: 0x22 (DC, E)
    LS Type: Router-LSA (1)
    Link State ID: 13.13.13.2
    Advertising Router: 13.13.13.2 (13.13.13.2)
    LS Sequence Number: 0x80000003
    LS Checksum: 0x01b5
    Length: 36
```

Fig. 6 LSA Header – OSPFv2



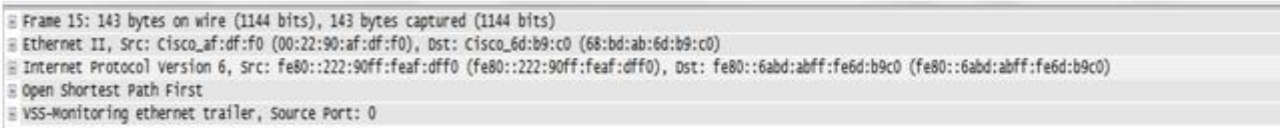
```
⊟ LSA Header
    LS Age: 3600 seconds
    Do Not Age: False
    LS Type: Router-LSA (0x2001)
    Link State ID: 0.0.0.0
    Advertising Router: 0.0.0.1 (0.0.0.1)
    LS Sequence Number: 0x80000006
    LS Checksum: 0xc32b
    Length: 40
```

Fig. 7 LSA Header-OSPFv3

The header is the same, except that the Options field has been removed in OSPFv3 LSA header.

5) Instance ID is a new field that is used to have multiple OSPF process instance per link. In order for 2 instances to talk to each other they need to have the same instance ID. By default it is 0 and for any additional instance it is increased, Instance ID has local link significance only.

6) In OSPFv2 for two routers to establish neighborship, they should belong to the same subnet. However, OSPFv3 runs on a per-link basis. Different ipv6 subnets can be assigned to a single link and the two routers can still establish neighborship. Therefore unlike OSPFv2, OSPFv3 does not require a network mass to form adjacency.
7) IPv6 has two kinds of addresses - link local and global address. The global address is required to reach out to the internet, without any need of NAT. The link local address is used just for the local network and they are not routable. In OSPF v6 the router uses the link local address associated with an interface to send the ospf packets and also learns the link local addresses of its neighbours as the next hops. This can be seen in the packet captures taken below:



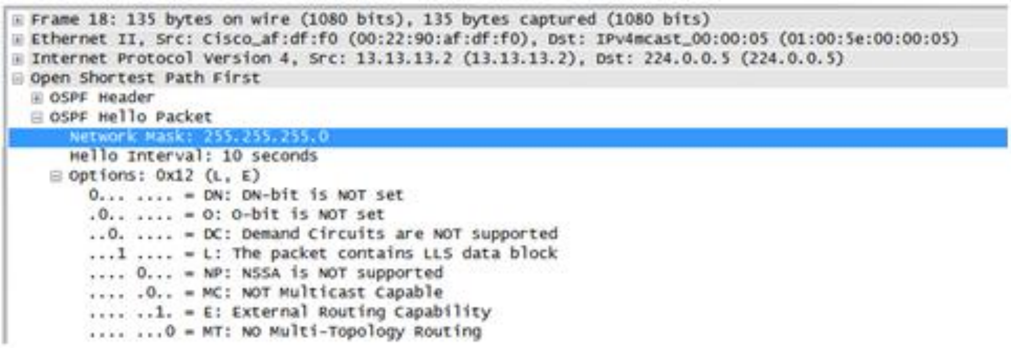
```
Frame 15: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
Ethernet II, Src: Cisco_af:df:f0 (00:22:90:af:df:f0), Dst: Cisco_6d:b9:c0 (68:bd:ab:6d:b9:c0)
Internet Protocol Version 6, Src: fe80::222:90ff:feaf:dff0 (fe80::222:90ff:feaf:dff0), Dst: fe80::6abd:abff:fe6d:b9c0 (fe80::6abd:abff:fe6d:b9c0)
Open Shortest Path First
VSS-Monitoring ethernet trailer, Source Port: 0
```

Fig. 8 Link local addresses

8) For OSPFv2, the multicast address is 224.0.0.5 for SFR routers and 224.0.0.6 for DR routers. For OSPFv3, FF02::5 for SFR routers and FF02::6 for DR routers.
9) In OSPFv2 the options field is 8bit long, whereas in OSPFv3 it is 24 bits long. Two additional bits have been introduced in OPSFv3 - R bit and V6 bit. As per RFC5340 the purpose of the bits is:

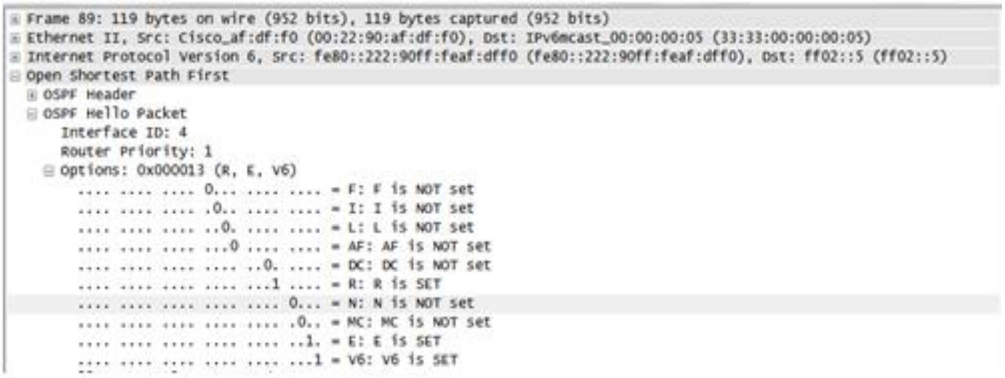
V6-bit: If this bit is clear, the router/link should be excluded from IPv6 routing calculations.

R-bit: This bit (the `Router' bit) indicates whether the originator is an active router. If the router bit is clear, then routes that transit the advertising node cannot be computed. Clearing the router bit would be appropriate for a multi-homed host that wants to participate in routing, but does not want to forward non - locally addressed packets.



```
Frame 18: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
Ethernet II, Src: Cisco_af:df:f0 (00:22:90:af:df:f0), Dst: IPv4mcast_00:00:05 (01:00:5e:00:00:05)
Internet Protocol Version 4, Src: 13.13.13.2 (13.13.13.2), Dst: 224.0.0.5 (224.0.0.5)
Open Shortest Path First
  OSPF Header
  OSPF Hello Packet
    Network Mask: 255.255.255.0
    Hello Interval: 10 seconds
   Options: 0x12 (L, E)
      0... .... = DN: DN-bit is NOT set
      .0.. .... = O: O-bit is NOT set
      ..0. .... = DC: Demand Circuits are NOT supported
      ...1 .... = L: The packet contains LLS data block
      .... 0... = NP: NSSA is NOT supported
      .... .0.. = MC: NOT Multicast Capable
      .... ..1. = E: External Routing Capability
      .... ...0 = MT: NO Multi-Topology Routing
```

Fig. 9 Options field OSPFv2



```
Frame 89: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
Ethernet II, Src: Cisco_af:df:f0 (00:22:90:af:df:f0), Dst: IPv6mcast_00:00:00:05 (33:33:00:00:00:05)
Internet Protocol Version 6, Src: fe80::222:90ff:feaf:dff0 (fe80::222:90ff:feaf:dff0), Dst: ff02::5 (ff02::5)
Open Shortest Path First
  OSPF Header
  OSPF Hello Packet
    Interface ID: 4
    Router Priority: 1
   Options: 0x000013 (R, E, V6)
      .... .... .... 0... .... .... = F: F is NOT set
      .... .... .... .0.. .... .... = I: I is NOT set
      .... .... .... ..0. .... .... = L: L is NOT set
      .... .... .... ...0 .... .... = AF: AF is NOT set
      .... .... .... .... ..0. .... = DC: DC is NOT set
      .... .... .... .... ...1 .... = R: R is SET
      .... .... .... .... .... 0... = N: N is NOT set
      .... .... .... .... .... .0.. = MC: MC is NOT set
      .... .... .... .... .... ..1. = E: E is SET
      .... .... .... .... .... ...1 = V6: V6 is SET
```

Fig. 10 Options field OSPFv3

IV. CONCLUSIONS

This paper has compared the IPv4 and IPv6 versions of popular routing protocol OSPF and identified the changes made to these protocols to incorporate IPv6 Support. The new features and changes of these protocols have been highlighted and discussed. OSPF has advantages in large networks where its hierarchical nature increases scalability. Future work will involve calculating route metrics for real time traffic to evaluate which version of the protocol has a faster route convergence rate.

REFERENCES

[1] IPv6 RFC [Online]. Available: https://www.ietf.org/rfc/rfc2460.txt

[2] OSPFv6 RFC [Online]. Available: https://tools.ietf.org/html/rfc5340#appendix-A.2

[3] Alex Hinds, Anthony Atojoko and Shao Ying Zhu, *Evaluation of OSPF and EIGRP Routing Protocols for IPv6,* International Journal of Future Computer and Communication, Vol. 2, No. 4, August 2013