# ROUTING PROTOCOLS ANALYSIS USING WIRESHARK

**Submitted By:**

Manjeet Singh

December 06, 2011

**Supervised By:**

Dr. Mike MacGregor

Shahnawaz Mir

# ACKNOWLEDGEMENTS

I am very thankful to respected Dr. Mike MacGregor the director of MINT program for giving me an opportunity to explore various routing protocols by assigning me such an interesting project titled “Routing Protocols Packets Analysis Using Wireshark as well as for their keen guidance.

I also express my deep sense of gratitude to my Program Co-ordinator respected Mr. Shahnawaz Mir for his able guidance and useful suggestions because of which I am able to complete the Project Work in time.

Finally I would like to present my heartfelt thanks to my respected parents for their kind support and blessings.

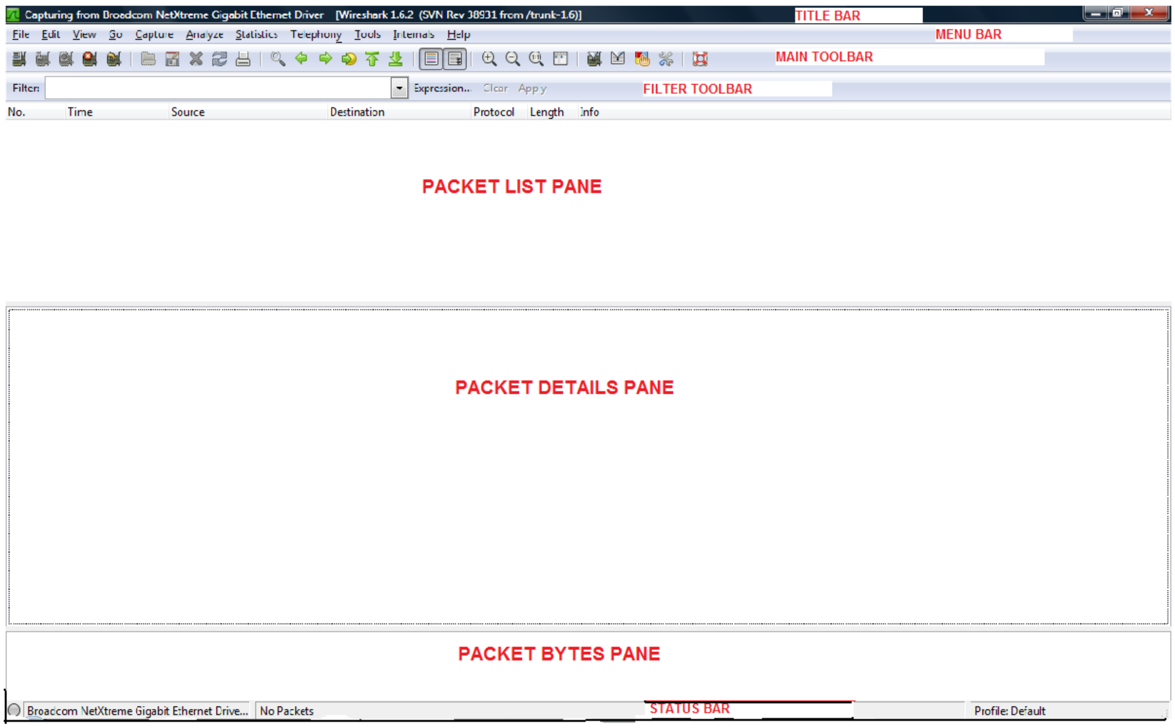
Manjeet Singh

## TABLE OF CONTENTS

# Introduction to Wireshark

Wireshark as defined by http://www.wireshark.org/about.html is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.
Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

WIRESHARK CAPTURING WINDOW




The above snapshot indicates the very first screen after selecting the capturing interface in the PC(for simplicity no data is captured). The various components of a Wireshark capturing window are mentioned in Red coloured text on th snapshot. These are:

1. **Title Bar :** Like in other GUI applications this indicates the software used and the filename (if no one is selected wireshark automatically chooses a default)
2. **Menu Bar :** This bar provides the access to various useful tools/functionalities associated with wireshark as saving a file, setting the interfaces parameters etc.
3. **Main Toolbar:** it provides the almost same functionalities plus some more as a user can find in Menu Bar. But it provides in a single click option like going to particular packet, zoom, help etc.
4. **Filter toolbar :** It is the most important toolbar when you are dealing with a large number of packets then with the help of filters the unnecessary packets can be ignored or important packets can only be displayed depending upon the filter created.

5. **Packet List Pane :** It is the important area of wireshark window as this is the place where packets are listed in the order in which they appear on the interface for the wireshark. It is having no. of useful sections for interpreting packets like Packet no., Time, Source , Destination, Protocol used, length and particular information about the packets.
6. **Packet Detail Pane:** Indicates the detail of the captured packet from Physical layer as well as the various protocols used to encapsulate the packet so as to make it transferrable over the wire. This is the most important area as it gives the information about the every component of the packet.
   The first section in a packet detail pane is titled as:
   - **Frame X,** where X indicates the captured frame number. Under this section various parameters related to time, frame length, marking, coloring rules and the various protocols used and their encapsulation are represented in a hierarchical way. For example the fig. below indicates an ARP request . Since no other protocol is required for ARP (being non-routable). It is encapsulated in ethernet frame as indicated by line: Protocols in frame are Ethernet and ARP.

```
⊟ Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Arrival Time: Nov 11, 2011 09:02:45.128369000 Mountain Standard Time
    Epoch Time: 1321027365.128369000 seconds
    [Time delta from previous captured frame: 0.489676000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 17.888226000 seconds]
    Frame Number: 15
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
⊟ Ethernet II, Src: HewlettP_ca:7b:fa (00:15:60:ca:7b:fa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
  ⊟ Source: HewlettP_ca:7b:fa (00:15:60:ca:7b:fa)
      Address: HewlettP_ca:7b:fa (00:15:60:ca:7b:fa)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: False]
    Sender MAC address: HewlettP_ca:7b:fa (00:15:60:ca:7b:fa)
    Sender IP address: 192.168.4.2 (192.168.4.2)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.2 (192.168.1.2)
```

   - The second section indicates the Ethernet source and destination addresses in hex. There indicated is IG(Individual/Group) and LG(Local/Global) bits which are interpreted as:
     IG bit= 0 Indicates the above mentioned address in the frame structure is an individual addtress, and IG= 1 indicates that this is a group address such as a multicast/broadcast group. For example it is set for ARP request (being broadcast)
     LG bit= 0 indicates it is a factory default address and is globally unique, LG=1 indicates it is not a factory default and is locally administered.
   - Third Section indicates the underlying protocol used in the above example it is ARP Request with the various ARP packet values.

7. Packet Byte Pane: this section tells us the actual binary values of the packet (the actual contents may be made so as to represent in Hex or in Binary).
8. Status Bar: this is the bottom portion of the display window of wireshark basically divided into 4 slots where first slot indicates in the form of the circular colored dot the level of information contained in the selected packet i.e warning, error ,note etc. The second slot (which gets changed because during the capture it indicates the interface but after saving that capture it indicates the location of stored file)indicates the location of the stored file on the system mentioning its size and time duration. Third section indicates the total no. of captured packets , displayed packets(this may be different from captured as if a filter is applied ),marked and load time taken for the

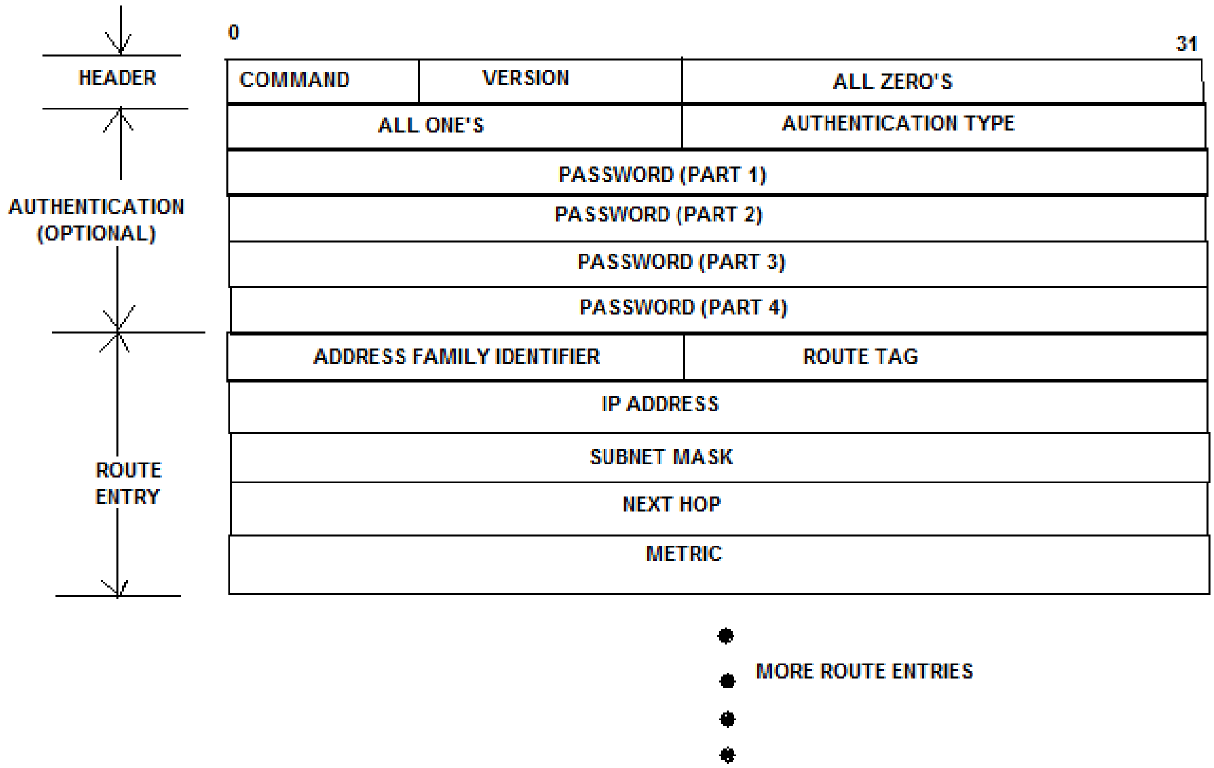
# RIPv2

It is an enhancement of RIPv1 and is defined in RFC1723.It also runs at UDP port 520 just like RIPv1 with maximum datagram size of 512.But in addition it supports

- Classless routing so carries subnet mask in RIPv2 packet
- Authentication
- Sends Multicast updates at class D address 224.0.0.9 instead of broadcast
- External route tags
- Next hop address is carried in RIPv2 packet

The maximum route entries that can be carried in RIPv2 update are 25 without authentication and 24 with authentication because the authentication information is carried at the place of first route entry when configured.

Fig. RIPv2 Packet Structure




***Packet Description:***

**Command(8 bits):** This field is same as that of RIPv1 i.e. five different commands are specified out of which the commonly used are 1= Request and 2=Response. Request is always multicast whereas response is usually multicast but it can be unicast if router is responding to any request. Because all the RIPv2 running router interfaces automatically become the members of multicast group 224.0.0.9. So a response may pass two or more networks.

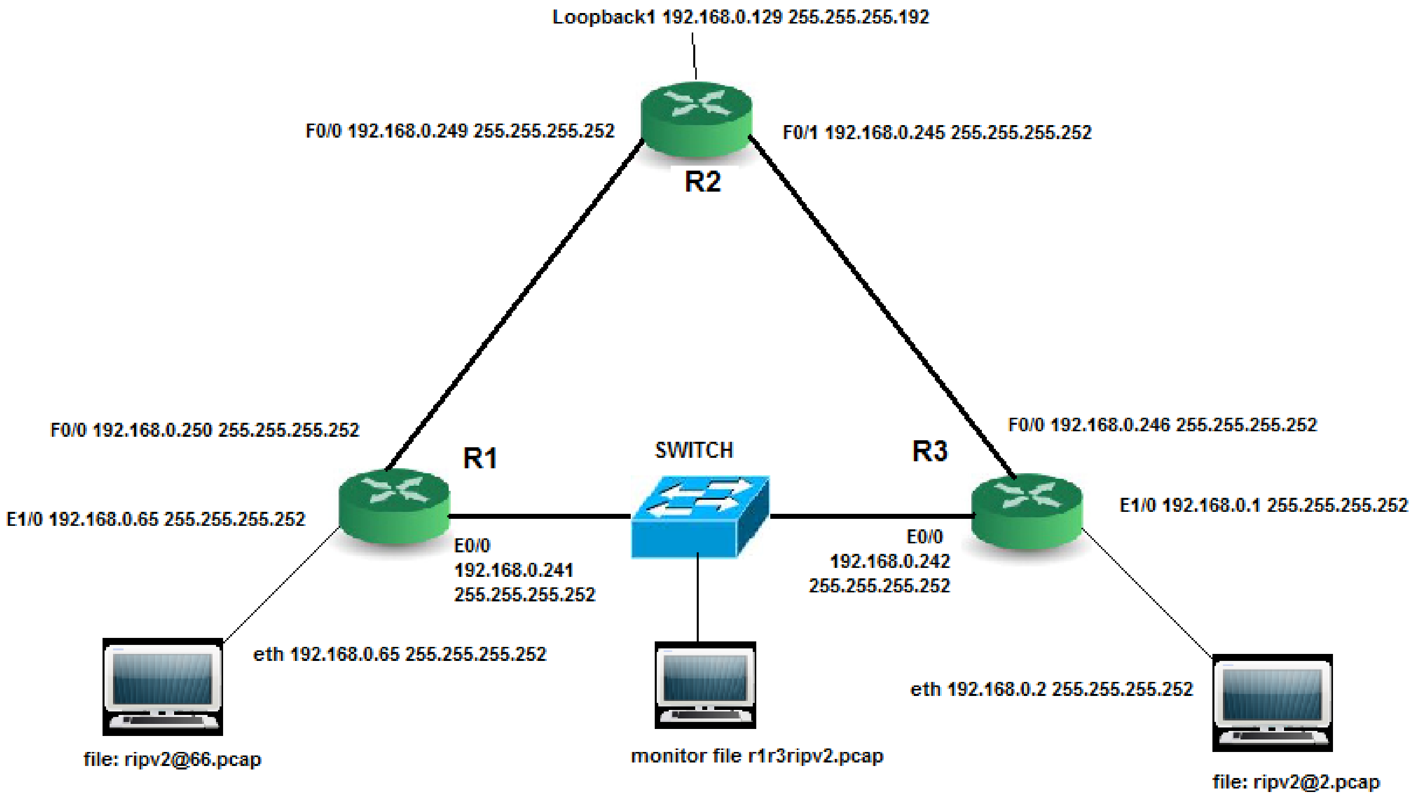
**Version(8 bits):** this is set equal to 2 indication RIPv2

**Address Field Identifier (16 bits):** It indicates the address family used such as IPv4. AFI= 2 for internet protocol. If AFI is all 1's it indicates the presence of authentication information in the rest of route entry field(16 bytes) where password is left justified with unused field all set to 0.

**Authentication type(16 bits):** As per RFC only authentication type supported is plain text with authentication type 2. But Cisco routers can support MD5 as well.

**Route Tag(16 bits):** used to tag the routes advertised by other protocols for identification.
**IP address(32 bits):** the IP address of the destination of the packet
**Subnt Mask(32 bits):** the mask used to identify the network and host portion of the IP address.
**Next Hop Address(32 bits):**indicates the next hop which is better than the advertising router all zeros indicates that the router is the best next hop for sending data
**Metric(16 Bits):** it indicate the metric of the routes carried in Ripv2 packet.

## RIPv2




NETWORK DIAGRAM FOR RIPV2 SHOWING FILES CAPTURED AT VARIOUS DEVICES AS WELL

The network used is 192.168.0.0/24
Three routers are used with following networks attached to each of these:

| Router | Network Attached |
|---|---|
| R1 | 192.168.0.64/26<br>192.168.0.248/30<br>192.168.0.240/30 |
| R2 | 192.168.0.128/26<br>192.168.0.248/30<br>192.168.0.244/30 |

| | |
|---|---|
| R3 | 192.168.0.0/26<br>192.168.0.240/30<br>192.168.0.244/30 |

The sequence in which the RIPv2 process is started is :

1. R1
2. R3(RIPv2 process starts 6.347621 seconds after that of R1)
3. R2

The regular RIPv2 updates are periodic with a theoretical time period of 30 secconds but it shows variability from 25.5 to 30 seconds. And a route is removed after two regular updates succeeding triggred update.

Split Horizon:

It can be observed on both the trace files. One of PC is connected to network 192.168.0.66/26 and one is connected to 192.168.0.0/26 . So these networks are not advertised on response packets received on these networks as shown below in snapshots:

```
⊞ Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
⊞ Ethernet II, Src: Cisco_db:78:c2 (00:0d:28:db:78:c2), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
⊞ Internet Protocol Version 4, Src: 192.168.0.65 (192.168.0.65), Dst: 224.0.0.9 (224.0.0.9)
⊞ User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
⊟ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  ⊟ IP Address: 192.168.0.240, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 192.168.0.240 (192.168.0.240)
      Netmask: 255.255.255.252 (255.255.255.252)
      Next Hop: 0.0.0.0 (0.0.0.0)
      Metric: 1
  ⊟ IP Address: 192.168.0.248, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 192.168.0.248 (192.168.0.248)
      Netmask: 255.255.255.252 (255.255.255.252)
      Next Hop: 0.0.0.0 (0.0.0.0)
      Metric: 1
```

The source address of above snapshot is 192.168.0.65 but in the rip response packet the associated network i.e. 192.168.0.64 is not advertised.

This can also be observed in a trace snapshot below where network 192.168. 0.0 is not advertised eventhough the source IP address is 192.168.0.1..

```
⊞ Frame 36: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
⊞ Ethernet II, Src: Cisco_db:6d:41 (00:0d:28:db:6d:41), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 224.0.0.9 (224.0.0.9)
⊞ User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
⊟ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  ⊞ IP Address: 192.168.0.64, Metric: 2
  ⊞ IP Address: 192.168.0.128, Metric: 2
  ⊞ IP Address: 192.168.0.240, Metric: 1
  ⊞ IP Address: 192.168.0.244, Metric: 1
  ⊞ IP Address: 192.168.0.248, Metric: 2
```

Moreover the distance vector nature of RIPv2 can also be observed from the TTL valueof 2 (so that the response does not ever passes the intended router) in th IP hearder as shown in the following snapshot:

```
⊟ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 224.0.0.9 (224.0.0.9)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 132
    Identification: 0x0000 (0)
  ⊞ Flags: 0x00
    Fragment offset: 0
  ⊟ Time to live: 2
    ⊞ [Expert Info (Note/Sequence): "Time To Live" != 1 for a packet sent to the Local Network Control Block (see RFC 3171)]
    Protocol: UDP (17)
  ⊞ Header checksum: 0x16f7 [correct]
    Source: 192.168.0.1 (192.168.0.1)
```

**Description of Ping 192.168.0.66 command initiated at PC (with IP =192.168.0.2)connected to R3 (***there is a long delay between the change of path occuring from R3-R2-R1 to R3-R1 as compared to the delay of path change from R3-R1 to R3-R2-R1. This is not any problem but it occurred because of a switch placed in between R3-R2 so as to observe the network packets, after the change switch took lot of time so as to learn and build a complete MAC address table and to forward the packets to associated IP's***). Moreover the time difference is shown only between RIPv2 messages so as to clearly interpret the RIPv2 operation and the display filter used was arp||icmp||rip so as to get only meaningful messages to be shown**

| **Packet No. in file ripv2@2** | **Time difference between individual RIPv2 packets in seconds (assuming packet 21 as reference)** | **Packet Description** |
|---|---|---|
| 21 | 0 | R1 sends RIPv2 request to all its interfaces(shown for example in packet 12 of r1r3ripv2) |
| 28 | 1.991766 | indicates that R1 has learned the directly connected routes of R3 |
| 38 | 8.009034 | (First normal RIPv2response)At this point the presence of all the networks in route table of R1 indicates that the RIPv2 has been fully converged on it.(i.e.within approx.10 seconds) .<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 2<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.240, Metric: 1<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2 |
| 39 | 0.267928 | Because the entry 192.168.0.128, metric 2,has been learned individually from R2. |
| 60, 79 | 25.862745, 25.689974 | Normal RIPv2 response containing all the network routes as in packet 38 |
| 83 | | so as to successfully ping the host connected to R1, the PC at 192.168.0.2 must know the MAC address of the nearest router so it sends ARP request to the IP mentioned as its default gateway |
| 84 | | router replies with its MAC address |
| 85-86, 88-89, 91-96, & | | These packets indicate the successful connectivity between two networks via two routers i.e. R3-R1. The TTL value of ping command indicates a difference of 2 between Request/Reply pair i.e. the path taken is the shortest one. Because RIP uses hop count as its metric so |

| | | |
|---|---|---|
| 99-100 | | minimum hops path is the preffred one as indicated by the ping command output when all the links are up. Moreover the time difference between first Request and its Reply is approximately 728 µ seconds more than the others. It is because of the time taken by the ARP Request/Reply on the target PC2. Below is some part of ping traces at PC1<br>Echo (ping) request id=0x0001, seq=2766/52746, ttl=128<br>Echo (ping) reply id=0x0001, seq=2766/52746, ttl=126<br>83 89.320677 HewlettP_ca:7b:fa Broadcast ARP<br>84 89.321440 Cisco_db:6d:41 HewlettP_ca:7b:fa ARP<br>85 89.321466 192.168.0.2 192.168.0.66 ICMP<br>86 89.323241 192.168.0.66 192.168.0.2 ICMP<br>88 90.308506 192.168.0.2 192.168.0.66 ICMP<br>89 90.309553 192.168.0.66 192.168.0.2 ICMP<br>The below figure indicates the delay caused by ARP on PC2:<br>115 83.234452 192.168.0.2 192.168.0.66 ICMP 74 Echo (ping) request id=0x0001, seq=2766/52746, ttl=126<br>116 83.234545 Universa_46:4c:2f Broadcast ARP 42 Who has 192.168.0.65? Tell 192.168.0.66<br>117 83.235248 Cisco_db:78:c2 Universa_46:4c:2f ARP 60 192.168.0.65 is at 00:0d:28:db:78:c2<br>118 83.235257 192.168.0.66 192.168.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2766/52746, ttl=128<br>119 84.221491 192.168.0.2 192.168.0.66 ICMP 74 Echo (ping) request id=0x0001, seq=2767/53002, ttl=126<br>120 84.221581 192.168.0.66 192.168.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2767/53002, ttl=128<br>122 85.235482 192.168.0.2 192.168.0.66 ICMP 74 Echo (ping) request id=0x0001, seq=2768/53258, ttl=126<br>123 85.235574 192.168.0.66 192.168.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2768/53258, ttl=128<br>Also the presence of two routers can be clearly observed from the TTL value of 126 of reply packets. |
| 102,106 | | the four packets didn't got any reply because of the R3-R1 broken connection |
| 108 | 19.891921 | the RIPv2 indicates the loss of network 192.168.0.64 and 192.168.0.240(because the link was broken) by changing the metric values to 16 and sending an immidiate response(at $81^{st}$ second) before its actual time(in our case it is approx. 6 min earlier than the regular response which is to be sent at approximately $87^{th}$ second)<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 16<br>⊞ IP Address: 192.168.0.240, Metric: 16 |
| 126 | 10.084634 | the RIPv2 update its regular response contents so as to reflect the lost networks<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 16<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.240, Metric: 16<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2 |
| 133-134, 138-139 | | Ping Request/Reply messages via changed route R3-R2-R1 which can be seen from the changed value of ping reply TTL from 126 (before R3-R1 link failure) to 125 (after R3-R1 link failure)<br>133 115.377742 192.168.0.2 192.168.0.66 ICMP 74 Echo (ping) request id=0x0001, seq=2776/55306, ttl=128<br>134 115.378633 192.168.0.66 192.168.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2776/55306, ttl=125<br>138 116.391775 192.168.0.2 192.168.0.66 ICMP 74 Echo (ping) request id=0x0001, seq=2777/55562, ttl=128<br>139 116.392616 192.168.0.66 192.168.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2777/55562, ttl=125 |

<table>
<tr><td>142</td><td>2.671915</td><td>because of the presence of alternative path to 192.168.0.64 it sends the indication of selection of that path with associated metric 3<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊟ IP Address: 192.168.0.64, Metric: 3<br>Address Family: IP (2)<br>Route Tag: 0<br>IP Address: 192.168.0.64 (192.168.0.64)<br>Netmask: 255.255.255.192 (255.255.255.192)<br>Next Hop: 0.0.0.0 (0.0.0.0)<br>Metric: 3</td></tr>
<tr><td>148-235</td><td></td><td>successful ping request reply messages via R3-R2-R1</td></tr>
<tr><td>237</td><td>27.024624</td><td>regular RIPv2 update indicating the new topology changes on the whole network<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 3<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.240, Metric: 16<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2</td></tr>
<tr><td>241-318</td><td></td><td>successful ping request reply messages via R3-R2-R1</td></tr>
<tr><td>319</td><td>28.915265</td><td>Regular RIPv2 response showing that after two response packets 126, 137 succeeding the responsepacket 108 the network with metric 16 was removed (three tims the normal response interval)and the new hops are adjusted accordingly:<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 3<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2</td></tr>
<tr><td>320-366</td><td></td><td>successful ping request reply messages via R3-R2-R1</td></tr>
<tr><td>367</td><td>16.122259</td><td>Indicates that the RIPv2 becomes aware of the activation of link 192.168.0.240<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊟ IP Address: 192.168.0.240, Metric: 1<br>Address Family: IP (2)<br>Route Tag: 0<br>IP Address: 192.168.0.240 (192.168.0.240)<br>Netmask: 255.255.255.252 (255.255.255.252)<br>Next Hop: 0.0.0.0 (0.0.0.0)<br>Metric: 1</td></tr>
<tr><td>368-402</td><td></td><td>successful ping request reply messages via R3-R2-R1</td></tr>
<tr><td>403</td><td>12.533029</td><td>Regular RIPv2 response indicating the new hop adjustments made by the rip process<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 3<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.240, Metric: 1<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2</td></tr>
</table>

| | | |
|---|---|---|
| 404-451 | | successful ping request reply messages via R3-R2-R1 |
| 453 | 19.146775 | The RIPv2 response indicating the availability of 192.168.0.64 network via the newly sensed activated path<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 2<br>(the delay seen in this case is caused by the switch inserted between routers R1 and R3 so as to make the accurate analysis) |
| 454-481 | | successful ping request reply messages via R3-R2-R1 |
| 483, 558 | 10.221168, 26.391168 | The are the packets indicating the normal RIPv2 response(s) with adjusted metrics and the network gets converged<br>⊟ Routing Information Protocol<br>Command: Response (2)<br>Version: RIPv2 (2)<br>⊞ IP Address: 192.168.0.64, Metric: 2<br>⊞ IP Address: 192.168.0.128, Metric: 2<br>⊞ IP Address: 192.168.0.240, Metric: 1<br>⊞ IP Address: 192.168.0.244, Metric: 1<br>⊞ IP Address: 192.168.0.248, Metric: 2 |
| 484-557 and 560-561 | | Successful ping Request/Reply pairs indicating the path of 2 hops R3-R1 choosen by the ripv2 process running on R3 |

The file ripv2initialconvergence.pcap indicates the RIPv2 messages exchanged immidiately after the initialization of RIPv2 process. For capturing this file all interfaces connecting R1-R2, R2-R3 and R3-R1 were port monitored at switch port F0/0/0. RIPv2 was started in sequence R1, R3 and R2

The packets 1 and 2 are the request and response respectively sent by R1's interfaces upon initialization of RIPv2 process at time 0(reference). 5 and 6 are the requests generated by R3 upon start up of RIPv2 at time 2.528668.Since R2 RIP has not been initialized yet so the R1-R3 connecting interface having ip 192.168.0.241 replies to both requests of R2 generated by R1 in packets 7 and 8 respectively this fact can be observed by change in destination MAC addresses of both packets

```
Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_db:78:bc (00:0d:28:db:78:bc), Dst: Cisco_db:6d:57 (00:0d:28:db:6d:57)
Internet Protocol Version 4, Src: 192.168.0.241 (192.168.0.241), Dst: 192.168.0.242 (192.168.0.242)
Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_db:78:bc (00:0d:28:db:78:bc), Dst: Cisco_16:fc:45 (00:0d:65:16:fc:45)
Internet Protocol Version 4, Src: 192.168.0.241 (192.168.0.241), Dst: 192.168.0.246 (192.168.0.246)
```

Moreover these unicast response packets have TTL value of 255 always so as to indicate that they can cross multiple routers. Next the packets 9 and 10 are the response packets generated by R3 advertising their updated routes. Packet 11 is normal response packet by R1's interface connecting R2. Then the RIP starts on R2 at 7.129050 and advertise Requests in packets 12 and 13. 14$^{th}$ packet is the unicast response by f0/0 of R3.15$^{th}$ and 16$^{th}$ are unicast r esponse by E0/0 (since the router has not established route to R1R2 dierctly, so it traverses the longer path of two hops) of R1 on segments R1R3 and R3R2 respectively as can be seen from their source MAC address changes and also a decrease in TTL value as well from 255 to 254.

```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_db:78:bc (00:0d:28:db:78:bc), Dst: Cisco_db:6d:57 (00:0d:28:db:6d:57)
Internet Protocol Version 4, Src: 192.168.0.241 (192.168.0.241), Dst: 192.168.0.245 (192.168.0.245)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Cap
  Total Length: 72
  Identification: 0x0000 (0)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
Frame 16: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_16:fc:45 (00:0d:65:16:fc:45), Dst: Cisco_59:5d:9f (00:1f:6c:59:5d:9f)
Internet Protocol Version 4, Src: 192.168.0.241 (192.168.0.241), Dst: 192.168.0.245 (192.168.0.245)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Cap
  Total Length: 72
  Identification: 0x0000 (0)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 254
  Protocol: UDP (17)
```

In 17th packet R1interface f0/0 sends unicast response to R2's request. Similar to packet 15th and 16th (generated by E0/0 of R1 in respone to multicast request received from R2's f0/1) R3 sends unicast response for R2's request recived at its interface E0/0 In packets 18 and 19 captured from interface R1R3 and R1R2 respectively.

```
Frame 18: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_db:6d:57 (00:0d:28:db:6d:57), Dst: Cisco_db:78:bc (00:0d:28:db:78:bc)
Internet Protocol Version 4, Src: 192.168.0.242 (192.168.0.242), Dst: 192.168.0.249 (192.168.0.249)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Cap
  Total Length: 72
  Identification: 0x0000 (0)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
Frame 19: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_05:bb:02 (00:0c:ce:05:bb:02), Dst: Cisco_59:5d:9e (00:1f:6c:59:5d:9e)
Internet Protocol Version 4, Src: 192.168.0.242 (192.168.0.242), Dst: 192.168.0.249 (192.168.0.249)
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capa
  Total Length: 72
  Identification: 0x0000 (0)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 254
  Protocol: UDP (17)
```

In packets 20 and 21 R2 starts advertising its routes from interfaces F0/1 and F0/0. Since these are all mulicast packets captured between 3 point to point links so while sending updates router will not send on a link the routes learned by that link. This is proved from packets multicast by R2 on R2R1 link as below:
Since R2 has learned the networks 192.168.0.0 and 192.168.0.244 via R3 from the path R3R1R2. So R2 while sending its multicast on link R2R1 because of split horizon

```
Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
⊞ IP Address: 192.168.0.0, Metric: 2
⊞ IP Address: 192.168.0.128, Metric: 1
⊞ IP Address: 192.168.0.244, Metric: 1
```

will not advertise the network 192.168.0.240 which it is using for sending updates to R1 on R2R1 link. For similar reason while sending unicast response to R2 via path R3R1R2 the sending router R3 has suppressed the route 192.168.0.240 because it using this network for sending update. So this is the reason of missing route

192.168.0.240 in the response packets R2 since that captured packet was flowing through R2R1 link and it has learnt 192.168.0.240 via that link.

Further the interface f0/1 of R2 having IP address 192.168.0.245 has learned routes from two update sources namely 192.168.0.246 and 192.168.0.241 as can be seen in packets 14,15 an16. First it learned about 4 routes from 192.168.0.246 on link R3R2 as

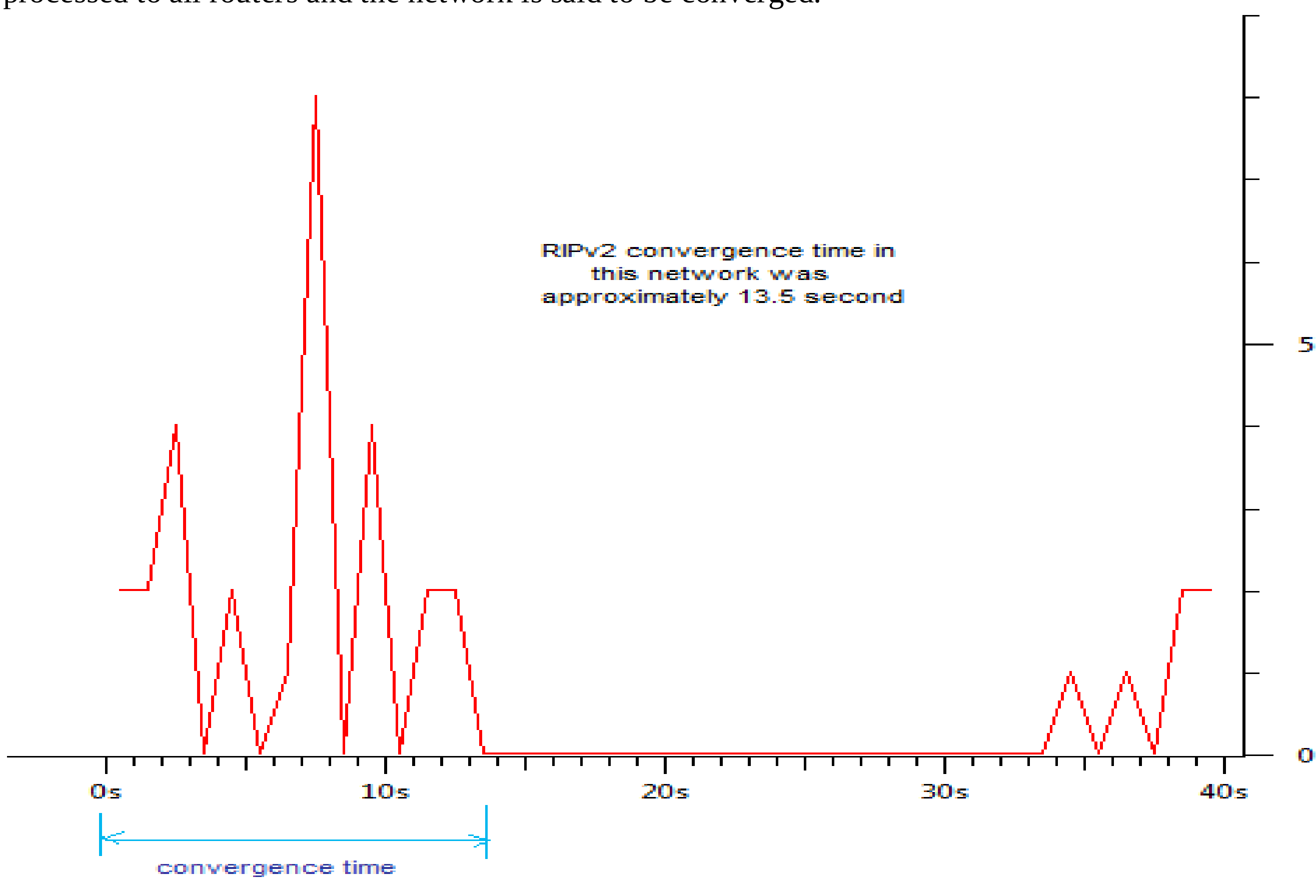
```
   Source: 192.168.0.246 (192.168.0.246)
   Destination: 192.168.0.245 (192.168.0.245)
User Datagram Protocol, Src Port: router (520),
Routing Information Protocol
   Command: Response (2)
   Version: RIPv2 (2)
⊞ IP Address: 192.168.0.0, Metric: 1
⊞ IP Address: 192.168.0.64, Metric: 2
⊞ IP Address: 192.168.0.240, Metric: 1
⊞ IP Address: 192.168.0.248, Metric: 2
```

after that it learned about the 2 already present routes from R1 in packet 16

```
   Source: 192.168.0.241 (192.168.0.241)
   Destination: 192.168.0.245 (192.168.0.245)
User Datagram Protocol, Src Port: router (520)
Routing Information Protocol
   Command: Response (2)
   Version: RIPv2 (2)
⊞ IP Address: 192.168.0.64, Metric: 1
⊞ IP Address: 192.168.0.248, Metric: 1
```

While sending the routes R1 will suppressed 192.168.0.240 which was processed by R3 in the next update from the same MAC address not listing 192.168.0.240 .So for sending its update on link R2R3 it will not send the routes 192.168.0.0, 192.168.0.240 and 192.168.0.244.

Packets 22 and 23 are simple advertisements by R1 and in packets 24 and 25 routers has sent their newly learned route 192.168.0.128. So after packet 26th it can be said that all the network information has been processed to all routers and the network is said to be converged.



# EIGRP(ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

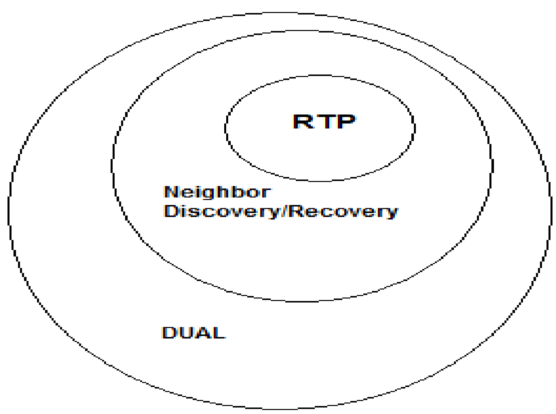
It is a CISCO proprietary interior gateway protocol having ID 88. It is an enhanced version of IGRP. So it also uses a composite metric for route calculations which involves Bandwidth, Load , Delay and Reliability. But the metric is multiplied by 256. The formula used is:

$256*((K_1*BW) + (K_2*BW)/(256\text{-}Load) + (K_3*Delay)*(K_5/(Reliability + K_4)))$

where $K_1$ , $K_2$, $K_3$, $K_4$, $K_5$ , are weights having default values of 1 for $K_1$ , $K_3$ and 0 for $K_2$, $K_4$ and $K_5$ . BW is the minimum bandwidth of the outgoing interface towards destination. So using default values the new metric= 256(BW + Delay). It supports unequal load cost balancing and an unreachable route/broken link is signaled by making delay value 0xFFFFFFFF.

EIGRP is different from other Distance Vector Routing Protocols in the sense that the updates are not periodic and these are only sent in case of an event(like metric change) and only to nodes which might get affected by that change. For this purpose the new algorithm called DUAL (Diffusing Update Algorithm) is used which maintains loop free topology at every single step while converging.But DUAL itself might not accomplish the task and so two more supporting processes called Reliable Transport Protocol and Neighbor Discovery/Recovery provides a stable and reliable platform for the operation of DUAL.

Fig. Layered Structure for implementing DUAL in EIGRP




First adjacency is established so as to transfer routing information and for each route in the updates received by a router. Then it will calculate the distance to each destination using the distance and cost advertised by other router(s).The lowest calculated distance to the destination becomes the Feasible Distance(FD) for that destination. If a neighbor's advertised distance is less than the router's FD then that neighbor becomes Feasible Successor(FS). The presence of a FS speeds up the re-convergence. On every EIGRP running routers two types of tables are created and stored:

1. Neighbor Table which include the information about directly connected neighbors
2. Topology Table stores information about every destination reachable by EIGRP running adjacent routers for which one or more FS's exists

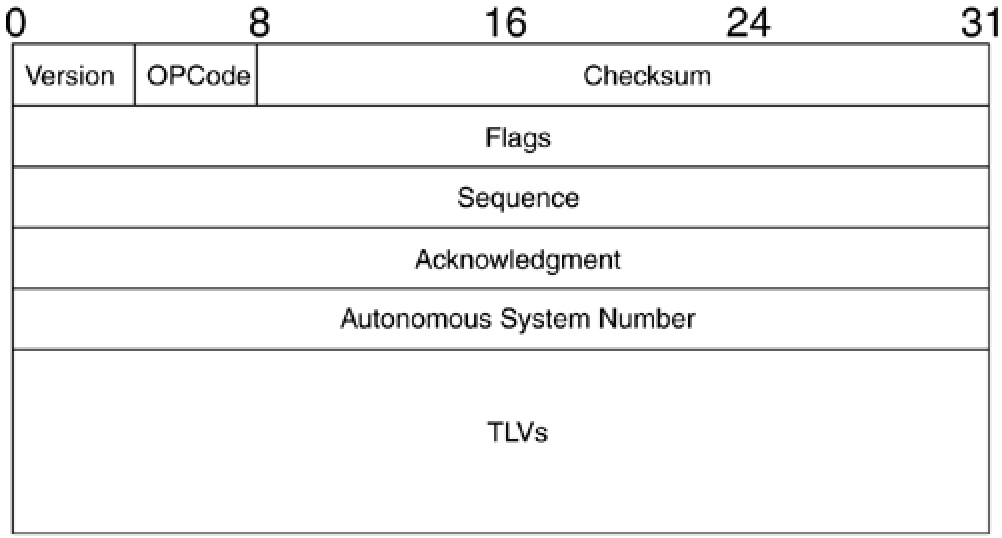



**Fig. EIGRP packet**

Following are the EIGRP packet fields:

**Version:** The version of EIGRP is 2

**Opcode:** The following table indicates the four most commonly used opcode types

| Opcode | Type |
|---|---|
| 1 | Update |
| 3 | Query |
| 4 | Reply |
| 5 | Hello |

**Checksum :** the 16 bits checksum calculated on the entire EIGRP packet but not including the IP header.

**Flag:** this a 32 bit value with the following meanings

0x00000001 indicates that the entries contained in the message are the first entries for establishing a new neighbor connection

0x00000002 is conditional receive bit used for proprietary protocol of CISCO called Reliable Multicast algorithm

**Sequence Number:** It is a 32 bit value indicating the sequence number used by Reliable Transport Protocol

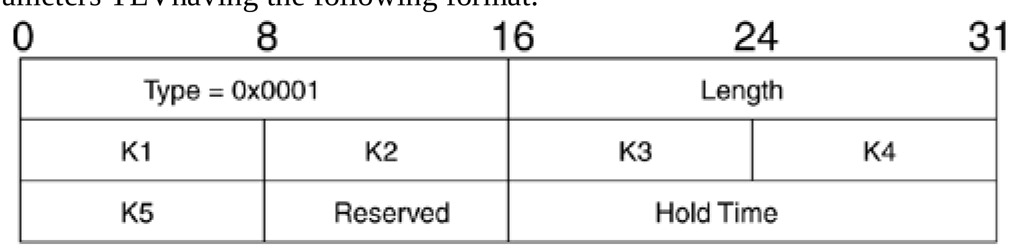
**Acknowledgement :** 32 bit field used to send acknowledgement of an EIGRP packet

**AS no. :** 32 bit field used to indicate the Autonomous Number used in EIGRP.

**TLV field :** there are 4 types of TLV types-

- General TLV types
- IP- Specific TLV types
- AppleTalk-Specific TLV Types
- IPX-Specific TLV types

Out of these the most common types of TLV are subtypes of General TLV one of 96 bits called EIGRP parameters TLVhaving the following format:



```
EIGRP Parameters
   Type: EIGRP Parameters (1)
   Size: 12
   K1: 1
   K2: 0
   K3: 1
   K4: 0
   K5: 0
   Reserved: 0
   Hold Time: 15

00000001 00000000 01011110 00000000 00000000 00001010 00000000 00001010
11110100 00110100 11010110 01000000 00001000 00000000 01000101 11000000
00000000 00111100 00000000 00000000 00000000 00000000 00000010 01011000
11111101 10110110 11000000 10101000 00011001 01000001 11100000 00000000
00000000 00001010 00000010 00000101 11101110 11001010 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000010 00000000 00000001
00000000 00001100 00000001 00000000 00000001 00000000 00000000 00000000
00000000 00001111 00000000 00000100 00000000 00001000 00001100 00000100
00000001 00000010
```

Other is Software version which is of 64 bits

```
Software Version: IOS=12.4, EIGRP=1.2
   Type: Software Version (4)
   Size: 8
   IOS release version: 12.4
   EIGRP release version: 1.2

00000000 00000000 00000000 00000000 00000000 00000010 00000000 00000001
00000000 00001100 00000001 00000000 00000001 00000000 00000000 00000000
00000000 00001111 00000000 00000100 00000000 00001000 00001100 00000100
00000001 00000010
```

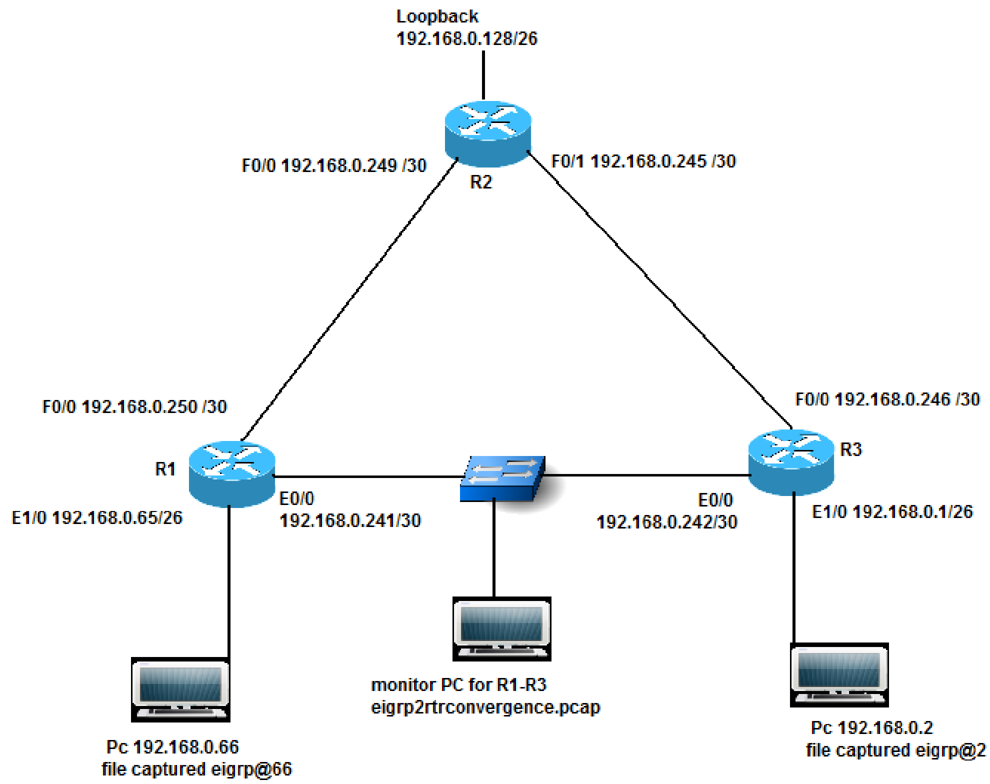



Fig.EIGRP network diagram

The trace file at monitor has been taken after disabling fast Ethernet ports on R1 and R3.

Since EIGRP is a distance vector protocol which behaves as a link state protocol so I have shown the convergence of two routers R1 and R3 independent of the other so that the packets between them while forming an adjacency can be observed. The file used is eigrp2rtrconvergence.pcap

| Packet No. | Description |
|---|---|
| 1,2 and 3<br>Cisco EIGRP<br>Version: 2<br>Opcode: Hello/Ack (5)<br>Checksum: 0xeecd<br>Flags: 0x00000000<br>Sequence: 0<br>Acknowledge: 0<br>Autonomous System: 1<br>EIGRP Parameters<br>Type: EIGRP Parameters (1)<br>Size: 12<br>K1: 1<br>K2: 0<br>K3: 1<br>K4: 0<br>K5: 0<br>Reserved: 0<br>Hold Time: 15<br>Software Version: IOS=12.2, EIGRP=1.2<br>Type: Software Version (4)<br>Size: 8<br>IOS release version: 12.2<br>EIGRP release version: 1.2 | Hello packet of R1: Since it is a normal Hello packet so its Sequence and Acknowledge are both zero. It indicates the autonomous system used being 1<br>Moreover it contains two TLV variabless<br>1. The parameters used for calculation of composite metric are bandwidth and delay because K1 and K3 are both 1 and others i.e.K2=K4=K5 are all 0. It also indicates the Hold Time i.e. time after which router will declare the neighbor dead if no hello is received within 15 seconds.<br>These values must match on both the routers so as them to form an adjacency and become neighbors.<br>2. Software version TLV which is 8 octets long and tells the version of the IOS of router and EIGRP process running. |
| 4 | the Hello packet of R3 |
| 5 | It is an Update packet with<br>Sequence 1 and Acknowledge 0.<br>With this packet router sends its internal route(s). |

| | |
|---|---|
| Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0xd307<br>⊟ Flags: 0x00000009<br>.... .... .... .... .... .... .... ...1 = Init: True<br>.... .... .... .... .... .... .... ..0. = Conditional Receive: False<br>.... .... .... .... .... .... .... .0.. = Restart: False<br>.... .... .... .... .... .... .... 1... = End Of Table: True<br>Sequence: 1<br>Acknowledge: 0<br>Autonomous System: 1<br>⊟ IP internal route = 192.168.0.64/26<br>Type: IP internal route (258)<br>Size: 29<br>Next Hop: 0.0.0.0 (0.0.0.0)<br>Delay: 25600<br>Bandwidth: 256000<br>MTU: 1500<br>Hop Count: 0<br>Reliability: 255<br>Load: 1<br>Reserved: 0 | The Init flag when set indicates the initial exchange of topology table. End of table indicates there will be no more update packets.The next hop field is 0.0.0.0 indicates router is connected directly to advertised network.<br>Delay(32 bits): The configured delay in units of 10 microseconds<br>Bandwidth(256*min. configured BW):<br>Maximum Transmission Unit on that network is 1500<br>Hop count is 0 because of being directly connected<br>Reliability(8 bits) dynamically calculated metric which indicates how reliable is link for transmission 255 indicates maximum reliability<br>Load(8 bits): 1 indicates the minimal loaded link and 255 is maximum loaded<br>Out of these MTU and Hop Count are never used for metric calculations |
| 6 | Hello of R1 |
| 7<br>Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0x4708<br>⊞ Flags: 0x00000009<br>Sequence: 1<br>Acknowledge: 0<br>Autonomous System: 1<br>⊟ IP internal route = 192.168.0.0/26<br>Type: IP internal route (258)<br>Size: 29<br>Next Hop: 0.0.0.0 (0.0.0.0)<br>Delay: 25600<br>Bandwidth: 256000<br>MTU: 1500<br>Hop Count: 0<br>Reliability: 203<br>Load: 1<br>Reserved: 0<br>Prefix Length: 26<br>Destination: 192.168.0.0 | R3 sends its internal routes to R1<br>the other difference is Prefix length which indicates the Subnet Mask used in this case is 26 i.e. 255.255.255.192 |
| 8<br>Cisco EIGRP<br>Version: 2<br>Opcode: Hello/Ack (5)<br>Checksum: 0x4100<br>⊞ Flags: 0x00000000<br>Sequence: 0<br>Acknowledge: 0<br>Autonomous System: 1<br>⊞ EIGRP Parameters<br>⊞ Software Version: IOS=12.2, EIGRP=1.2<br>⊟ Sequence<br>Type: Sequence (3)<br>Size: 9<br>Address length: 4<br>IP Address: 192.168.0.242 (192.168.0.242)<br>⊟ Next multicast sequence: 2<br>Type: Next multicast sequence (5)<br>Size: 8<br>Next Multicast Sequence: 2 | R1 sends its sequence number for next multicast. This packet contains 4 TLV's out of which two are<br>Sequence TLV(9 bytes): which tells about the target IP address and its length<br>Next Multicast Sequence(8 octets): it indicates the next sequence number for the multicast. Here the value is 2 and it is equal to the sequence of next packet. |
| 9 | Sequence=2, Acknowledge=0<br>This multicast is having the sequence no. 2 as |

| | |
|---|---|
| Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0xab0d<br>Flags: 0x00000002<br>Sequence: 2<br>Acknowledge: 0<br>Autonomous System: 1<br>IP internal route = 192.168.0.0/26 - Destination unreachable<br>Type: IP internal route (258)<br>Size: 29<br>Next Hop: 0.0.0.0 (0.0.0.0)<br>Delay: 4294967295<br>Bandwidth: 256000<br>MTU: 1500<br>Hop Count: 1<br>Reliability: 203<br>Load: 1<br>Reserved: 0<br>Prefix Length: 26<br>Destination: 192.168.0.0<br>[Expert Info (Note/Response): Destination unreachable]<br>[Message: Destination unreachable]<br>[Severity level: Note]<br>[Group: Response] | advertised by previous packet.<br>In this packet the conditional flag bit is set flag bit is set which indicates the proprietary Cisco Reliable Multicast.<br>In this packet router R1 multicasts the learned route as unreachable by setting its delay to maximum i.e. all 32 bits set having decimal equivalent 4294967295. |
| 10 | Hello packet generated by R3 |
| 11<br>Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0x4708<br>Flags: 0x00000009<br>Sequence: 1<br>Acknowledge: 0<br>Autonomous System: 1<br>IP internal route = 192.168.0.0/26 | Since R3 is the only router having that route its again sends its internal route with Sequence 1 and Ack 0 |
| 12<br>Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0xd306<br>Flags: 0x00000009<br>Sequence: 1<br>Acknowledge: 1<br>Autonomous System: 1<br>IP internal route = 192.168.0.64/26 | In response to above packet R1 sends its routes and acknowledges packet 11 because the Seq no. is the no. of R1 and acknowledge 1 indicates that this packet was sent in response to 11th packet |
| 13<br>Cisco EIGRP<br>Version: 2<br>Opcode: Hello/Ack (5)<br>Checksum: 0xfdf8<br>Flags: 0x00000000<br>Sequence: 0<br>Acknowledge: 1<br>Autonomous System: 1 | R3 explicitly acknowledges the packet 12 |
| 14 | R1 sets the metric of learned route to infinite so as to feasibility condition to occur with Sequence 2 and acknowledge 1 |

| | |
|---|---|
| Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0xab0e<br>⊞ Flags: 0x00000000<br>Sequence: 2<br>Acknowledge: 1<br>Autonomous System: 1<br>⊞ IP internal route = 192.168.0.0/26 - Destination unreachable | |
| 15<br>Cisco EIGRP<br>Version: 2<br>Opcode: Hello/Ack (5)<br>Checksum: 0xfdf7<br>⊞ Flags: 0x00000000<br>Sequence: 0<br>Acknowledge: 2<br>Autonomous System: 1 | R3 explicitly acknowledges the packet 14 as can be seen from the matching of Sequence and acknowledge of both packets |
| 16<br>Cisco EIGRP<br>Version: 2<br>Opcode: Update (1)<br>Checksum: 0x370f<br>⊞ Flags: 0x00000000<br>Sequence: 2<br>Acknowledge: 0<br>Autonomous System: 1<br>⊞ IP internal route = 192.168.0.64/26 - Destination unreachable | R3 sets the metric infinite for its learned route so as to met Feasibility condition |
| 17<br>Cisco EIGRP<br>Version: 2<br>Opcode: Hello/Ack (5)<br>Checksum: 0xfdf7<br>⊞ Flags: 0x00000000<br>Sequence: 0<br>Acknowledge: 2<br>Autonomous System: 1 | R1 acknowledges R3 as can be seen from the value of Acknowledge equal to 2and the network gets stable |
| 18-23 | These are the alternating Hello's of both routers so as to maintain converged connectivity |

Next is the graphical description of EIGRP ping command run from PC connected to router R3 at 192.168.0.2 for PC connected to router R1 at 192.168.0.66. The file name is eigrp@2.pcap .The ARP and other traffic was filtered by using appropriate capture filter. For capturing this file the link between R3 and R2 is changed to state down and then up so as to observe the convergence in the network.

```
C:\Users\ABC>ping 192.168.0.66 -t

Pinging 192.168.0.66 with 32 bytes of data:
Reply from 192.168.0.66: bytes=32 time=2ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Request timed out.
Request timed out.
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
```

Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=126
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
Reply from 192.168.0.66: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.0.66:
Packets: Sent = 46, Received = 44, Lost = 2 (4% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms

The following graph depicts the whole process

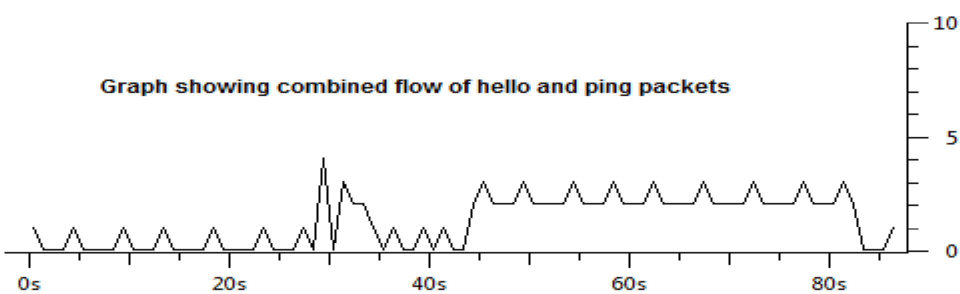



**Figure 1**

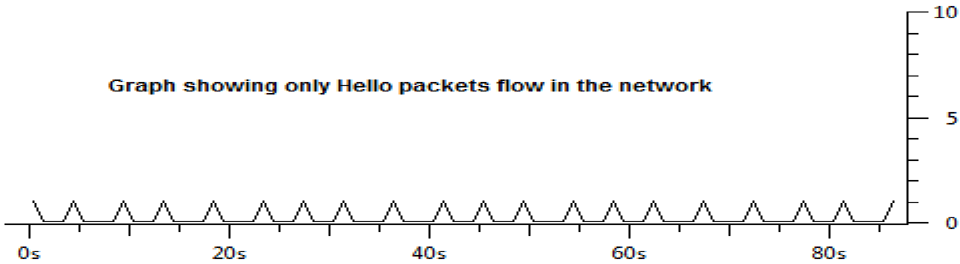



Figure 2

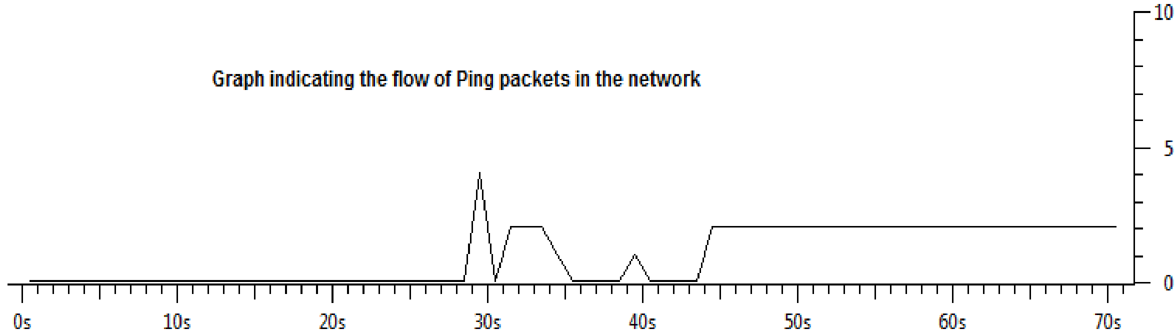



Figure 3

Since the link R1-R3 was not altered there are hello packets differing by approximately 5 seconds interval seen in figure 2.The ping starts at packet 8 on $29^{th}$ second and there occurs a successful request/reply sequence . The triangular peaks indicates the initial ping route establishment variations, There are two peaks the bigger one indicates the longer route selection and shorter one indicates the shorter route selection attempt whereas the zero levels indicate no data transfer in progress and the Y-axis value of 2 indicates the successful and stable ping operation in progress. The two packets were lost at the first decreasing slope at $34.05^{th}$ second indicating no reply and at 39.01th second another request was sent but the decreasing slope indicates no reply. But the request originating at 44.02th second got a response indicating the network gets converged in about 10 seconds.

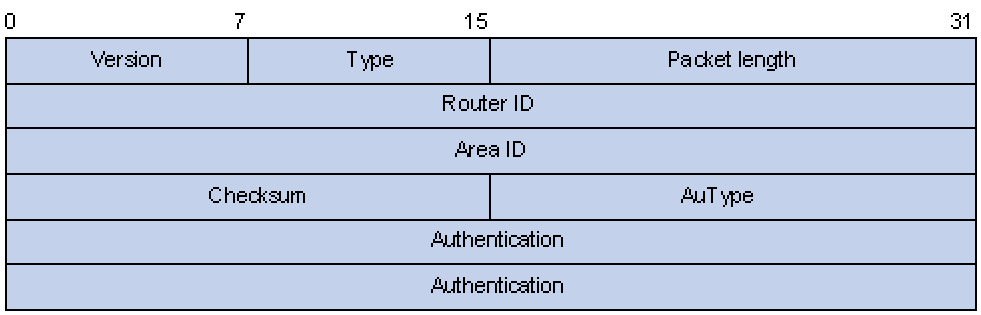
# OSPFv2 (Open Shortest Path First version 2)

OSPF is the link-state Interior Gateway Protocol which uses SPF algorithm and having protocol number 89.Ospf packets are directly encapsulated in IP header. It is fully classless protocol which is having three versions OSPFv1, OSPFv2 and OSPFv3 defined in RFC 1131, RFC 2328 and RFC 5340 respectively. The most commonly used version for IPv4 is OSPFv2 and for IPv6 is OSPFv3. Supports equal cost load balancing and support the concept of areas. All other areas must be connected to the backbone area. Moreover it defines 5 network types:

- Point-to-point Networks
- Broadcast Networks
- NBNA Networks
- Point-to-multipoint Network
- Virtual Links

**Operation:** OSPF running routers sends hello packets on their active interfaces and they form adjacencies with interfaces of other routers if the Hello packet parameters match. After establishing adjacency they send their link states in the form of special packets called Link State Advertisements by following Shortest Path First algorithm thereby building database of whole network in every router. After the network gets fully converged only Hello's are sent. For making the analysis and troubleshooting easy various types of Routers and Area's are defined resulting in various types of packets.

**OSPF Packet Header** (first 24 bytes) is the first component of every OSPF packet. It has the following structure:




**Version(8 Bits):** This indicates the OSPF version currently two version are supported Version 2 and Version 3. For version 2 it has value 00000010.

**Type(8 bits):** It indicates the packet types. Currently there exist 5 packet types resulting in 5 valid type fields:

| Type (corresponding Binary value) | Meaning |
|---|---|
| 1 (00000001) | Hello PAcket |
| 2 (00000010) | Database Description |
| 3 (00000011) | Link State Request |
| 4 (00000100) | Link State Update |
| 5 (00000101) | Link State Acknowledgement |

**Packet Length(16 bits):** It indicates the total length of OSPF packet in bytes or octets.

**Router ID(32 bits):** It indicates the 32 bit length dotted decimal notation ID configured or automatically chosen by the router.

**Area ID(32 bits):** Since there are various types of routers for OSPF and so are the areas. This field indicates the area ID of the source of the packet. All backbone areas are 0.0.0.0

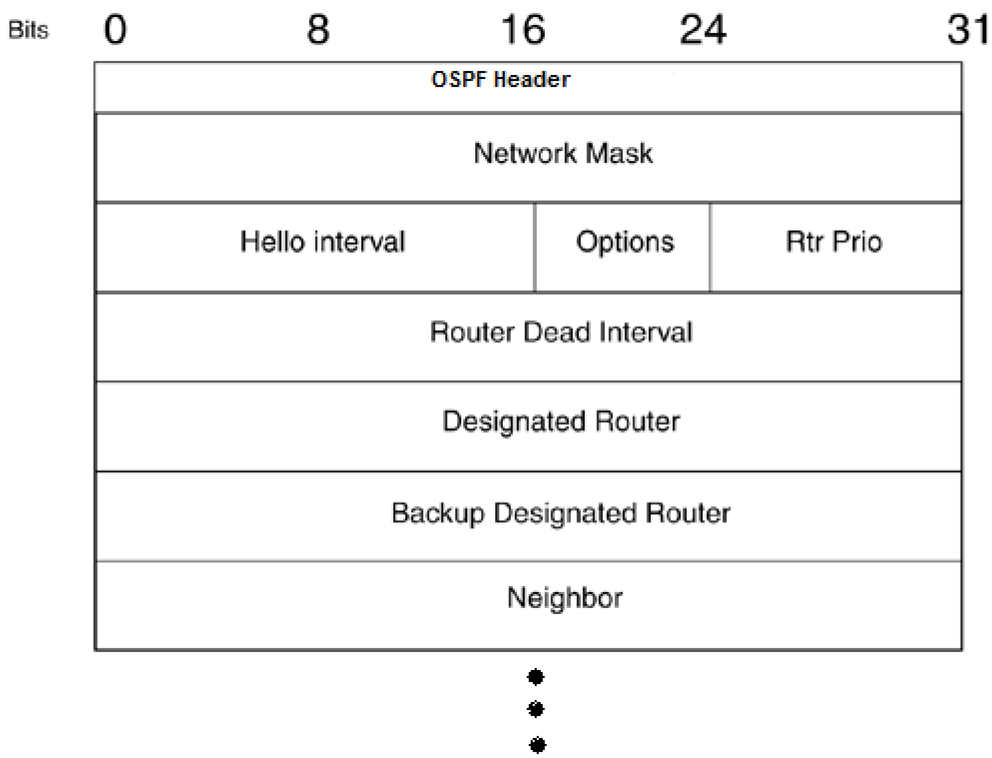
**Checksum(16 Bits):** This indicates the standard checksum of the whole packet.

Au Type(6 Bits): It indicates the Authentication type. Authentication supported can be Plain Text or MD5 results in Au Type 1 and 2 respectively. If Au Type =0 it means no authentication. For Au Type=1 the next 32 bits contains the password. For Au Type=2 the 32 bits contain Key ID, Authentication data length and Cryptographic sequence number.

OSPFv2 packets are classified into 5 types all containing the same header.These are:

***1. Hello Packet***

It is identified by Type field value of 1 from header.




**Network Mask (32 bits):** The subnet mask of the source interface of the packet . It must match on both source and destination interface.

**Hello Interval (16 bits):** The frequency of hello packets(in seconds)

**Options (8 bits):**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Reserved | Opaque LSA | Demand Circiut Capability | External Attribute | N/P (NSSA) | Multicast OSPF | E (external LSA's are allowed) | ToS (0) |

**Router Priority(8 bits)**: this 8 bit field is used to set the priority of a router for the selection of Designated Router and Backup Designated Router. Default is 1

**Router Dead Interval (32 bits):** the number of seconds after which a neighbor is declared dead. By default it is 4 times that of Hello.

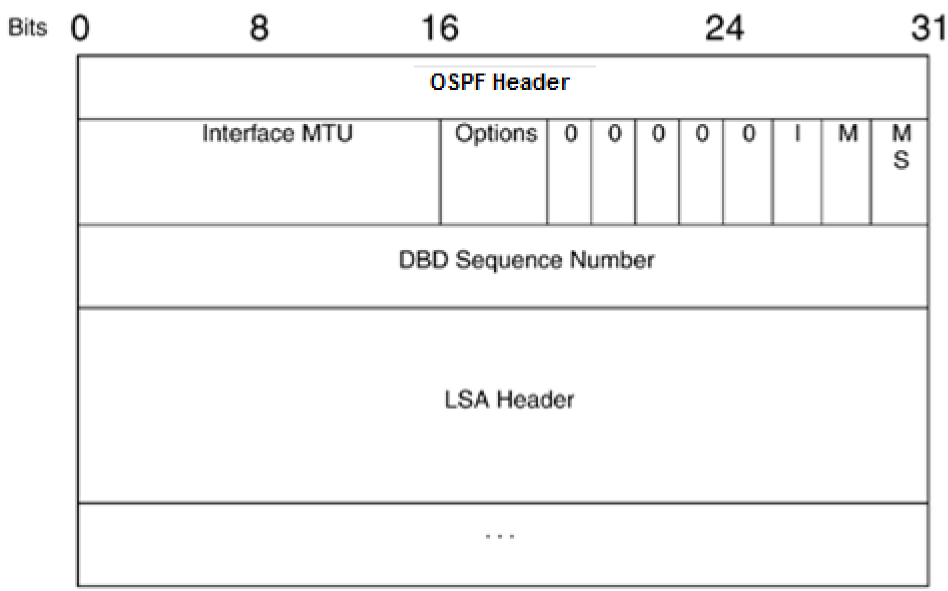
**Designated Router (32 bits): IP** address of the interface of the DR on the network

**Backup designated router(32 bits):** IP address of the interface of BDR on the network.

**Neighbor (32 bits):** it is the router ID of each neighbor from which Hello packets are received

### *2. Database Description Packet*

Identified from type field of value 2 in the header.




**Interface MTU(16 bits**): it is the size in octets of the maximum packet that can be sent from an interface without fragmentation.

**Options(8 bits):** this field is same as shown in above packet

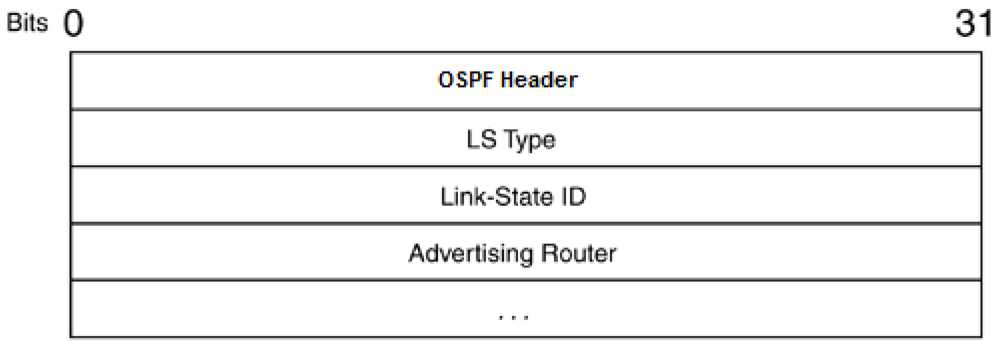
8 bits:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | **Initial Bit** (I=1 implies this is the first packet) | **More Bit** (when 1 it indicates there are more packets) | **M/S Bit** (1 and 0 indicates the router is acting as Master and slave respectively) |

**Database Description Sequence Number(32 BIts):** Controlled by master and is used during database exchange process

**LSA Header(variable):** Gives partial/complete list of the LSA's of the source database.

***3. Link State Request Packet***




**LS Type(32 bits):** It indicates the type of LSA out of which most commonly used are given in table below

| LS Type | Description |
|---|---|
| 1 | Router LSA |
| 2 | Network LSA |
| 3 | Network Summary LSA |
| 4 | ASBR Summary LSA |
| 5 | AS External LSA |

**Link State ID(32 bits) :** This field depends upon the type of LSA

**Advertising Router (32 bIts):** it is the ID of the source router of LSA's

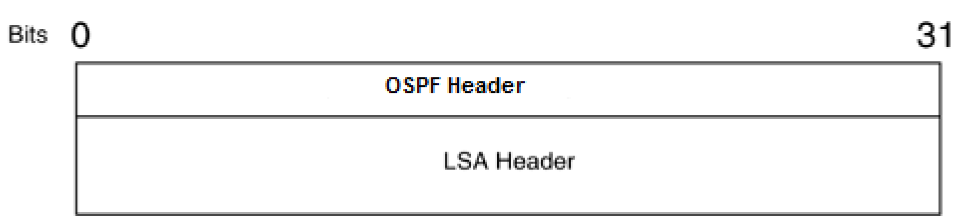
***4. Link State Update Packet***

| |
|---|
| OSPF Header |
| Number of LSA's |
| LSA's |

**Number of LSA's(32 bits):** It tells us the number of LSA's include in the update packet

**LSA's(variable):** the particular LSA's

***5. Link State Acknowledgement Packet***




This packet is used to acknowledge LSA's individually. For this purpose their headers are sent.

**LSA Header**

The various types of LSA's begin with LSA header which is:

<table>
<tr><td>Age(16 Bits)</td><td colspan="2">Options<br>(8 Bits)</td><td>Type(8 Bits)</td></tr>
<tr><td colspan="4">Link State ID(32 Bits)</td></tr>
<tr><td colspan="4">Advertising Router (32 Bits)</td></tr>
<tr><td colspan="4">Sequence NUmber(32 Bits)</td></tr>
<tr><td colspan="2">Checksum(16 bits)</td><td colspan="2">Length(16 BIts)</td></tr>
</table>

**Age:** Time in seconds, since the LSA was originated

**Options:** Same as discussed in the DD packet above

**Type:** Indicates the type of LSA

**Link State ID:** it depends upon the link state type

**Advertising Router** : the router ID of the router that originated the LSA

**Sequence Number:** It is an incrementing number which indicates the most recent LSA

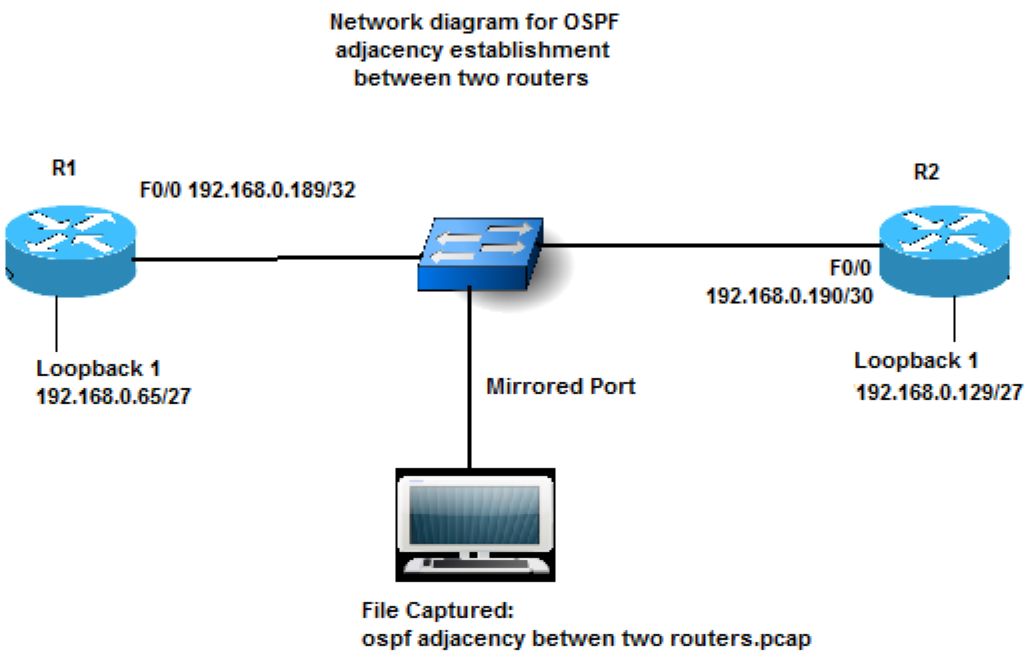
**Checksum:** This is the value of Fletcher checksum calculated over the entire LSA packet except the variable age

**Length:** The size of LSA in octets

## OSPF adjacency establishment between two routers

Two routers are having one loopback address on each and the routers were connected via Ethernet cable. First OSPF initializes on R1 and after that on R2. The whole process has been explained via two ways:

1. Packet Wise
2. Graphically




Packet Wise Illustration:

| Packet No. | Description |
|---|---|
| 1<br>Open Shortest Path First<br>⊞ OSPF Header<br>⊞ OSPF Hello Packet<br>⊞ OSPF LLS Data Block | This is the Hello packet sent by R1 which contains 3 elements:<br>1. OSPF Header which tells us about the contents of an OSPF packet<br>⊟ OSPF Header<br>OSPF Version: 2<br>Message Type: Hello Packet (1)<br>Packet Length: 44<br>Source OSPF Router: 192.168.0.65 (192.168.0.65)<br>Area ID: 0.0.0.0 (Backbone)<br>Packet Checksum: 0x2ab9 [correct]<br>Auth Type: Null<br>Auth Data (none)<br>It shows that the OSPF version 2 has been used for this Hello packet which is of 44 bytes in length and it originated from router interface having IP 192.168.0.65(OSPF running router uses the loopback addresses as source by default because they never gets down) which is a part of Backbone area. Next it shows the header checksum and the fact that the message is not authenticated.<br>2. Hello Packet |

| | |
|---|---|
| | ⊟ OSPF Hello Packet<br>Network Mask: 255.255.255.252<br>Hello Interval: 10 seconds<br>⊟ Options: 0x12 (L, E)<br>0... .... = DN: DN-bit is NOT set<br>.0.. .... = O: O-bit is NOT set<br>..0. .... = DC: Demand Circuits are NOT supported<br>...1 .... = L: The packet contains LLS data block<br>.... 0... = NP: NSSA is NOT supported<br>.... .0.. = MC: NOT Multicast Capable<br>.... ..1. = E: External Routing Capability<br>.... ...0 = MT: NO Multi-Topology Routing<br>Router Priority: 1<br>Router Dead Interval: 40 seconds<br>Designated Router: 0.0.0.0<br>Backup Designated Router: 0.0.0.0<br>It shows that a /30 mask has been used on the sending routers interface and the router will resend hello packets after an interval of 10 seconds. The fourth bit of options field indicates that the router can perform Link Local signaling and contains corresponding data block. E bit indicates the router is also capable of receiving AS external LSA’s. Moreover it indicates the router priority is 1 i.e. the default and the router will declare the neighbor dead if after establishing adjacency no hello is received within 40 seconds. DR and BDR field are both zero indicating the election is not happened yet.<br>3. OSPF LLS Data Block<br>⊟ OSPF LLS Data Block<br>Checksum: 0xfff6<br>LLS Data Length: 12 bytes<br>⊟ Extended options TLV<br>Type: 1<br>Length: 4<br>⊟ Options: 0x00000001 (LR)<br>.... .... .... .... .... .... .... ..0. = RS: Restart Signal (RS-bit) is NOT set<br>.... .... .... .... .... .... .... ...1 = LR: LSDB Resynchronization (LR-bit) is SET<br>This block is used of Link Local Signaling. The checksum field indicates the calculated checksum for the contents of LLS block only. Next is the length of the LLS block which is 12 bytes. It contains one of the two extended options TLV of type 1 which is used to signal some link-specific OSPF capabilities the other is type 2 Cryptographic Authentication TLV. Cisco Non Stop Forwarding is a feature that minimizes the time in case of route switch over. RS bit signal that whether the router is capable of NSF or not.LR bit indicates the router is capable of Out Of Band LSDB resynchronization. |
| 2 | The Hello packet generated by R2. This is having all the same parameters as in packet 1 except the source and destination MAC an IP addreses. |
| 3,5,7 | Hello of R1<br>The header remains except packet length change from 44 to 48. This is because the router R1 has learned about the active neighbor R2 from its first hello packet and is now advertised in its hellos. |

<table>
<tr><td></td><td><pre>OSPF Header
  OSPF Version: 2
  Message Type: Hello Packet (1)
  Packet Length: 48
  Source OSPF Router: 192.168.0.65 (192.168.0.65)
  Area ID: 0.0.0.0 (Backbone)
  Packet Checksum: 0x698b [correct]
  Auth Type: Null
  Auth Data (none)
OSPF Hello Packet
  Network Mask: 255.255.255.252
  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
  Router Priority: 1
  Router Dead Interval: 40 seconds
  Designated Router: 0.0.0.0
  Backup Designated Router: 0.0.0.0
  Active Neighbor: 192.168.0.129</pre></td></tr>
<tr><td>4,6,8</td><td>Hello of R2 having the same changes where active neighbor will be loopback of R1</td></tr>
<tr><td>9</td><td>The election for DR and BDR has been held showing in their respective fields in hello packet for the physical interface of R1 the interface of R2 are both DR and BDR since it is having the bigger IP’s<pre>OSPF Hello Packet
  Network Mask: 255.255.255.252
  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
  Router Priority: 1
  Router Dead Interval: 40 seconds
  Designated Router: 192.168.0.190
  Backup Designated Router: 192.168.0.190
  Active Neighbor: 192.168.0.129</pre></td></tr>
<tr><td>10</td><td>Similarly the R2 advertises its DR and BDR’s<pre>OSPF Hello Packet
  Network Mask: 255.255.255.252
  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
  Router Priority: 1
  Router Dead Interval: 40 seconds
  Designated Router: 192.168.0.190
  Backup Designated Router: 192.168.0.189
  Active Neighbor: 192.168.0.65</pre></td></tr>
<tr><td>11</td><td>R2 being the DR starts Link State exchange process via LSU’s. It contains the number of LSA’s in the update packet which in this case is 1.It tells the LS Type which is Router LSA since it is advertised by routers within an area. It has left 49 seconds to become invalid as the do not age parameter is not set. It contains following sections:<br>1. Options field</td></tr>
</table>

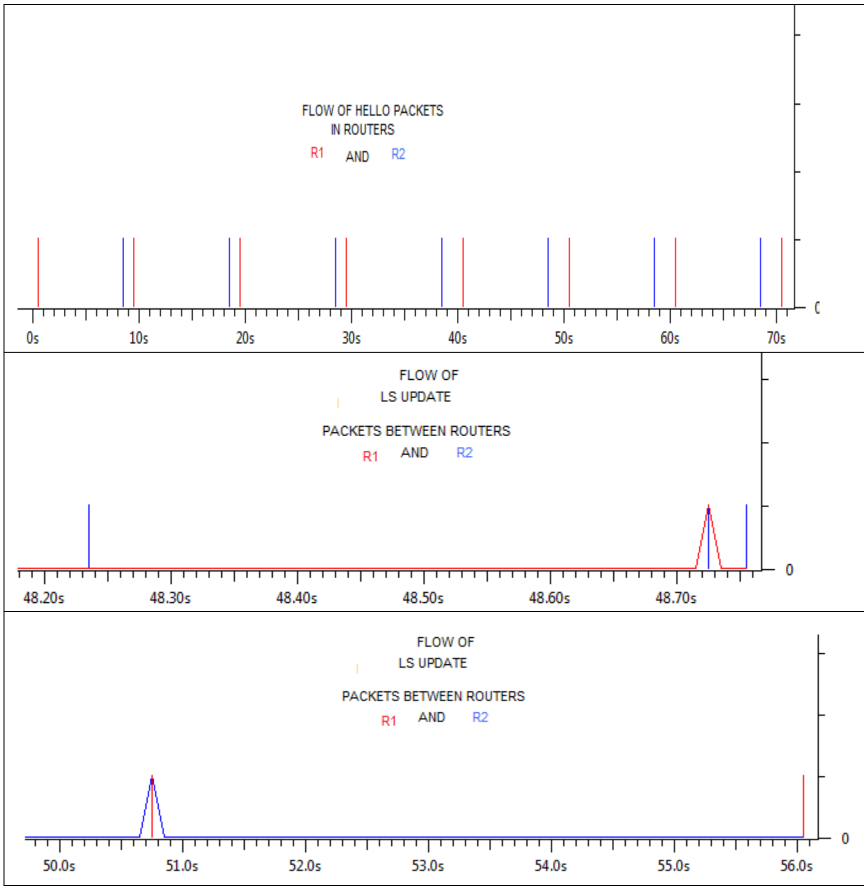
| | |
|---|---|
| LS Update Packet<br>Number of LSAs: 1<br>LS Type: Router-LSA<br>LS Age: 49 seconds<br>Do Not Age: False<br>Options: 0x22 (DC, E)<br>Link-State Advertisement Type: Router-LSA (1)<br>Link State ID: 192.168.0.65<br>Advertising Router: 192.168.0.65 (192.168.0.65)<br>LS Sequence Number: 0x80000001<br>LS Checksum: 0x8d70<br>Length: 48<br>Flags: 0x00<br>Number of Links: 2<br>Type: Stub ID: 192.168.0.188 Data: 255.255.255.252 Metric: 1<br>Type: Stub ID: 192.168.0.65 Data: 255.255.255.255 Metric: 1 | Options: 0x22 (DC, E)<br>0... .... = DN: DN-bit is NOT set<br>.0.. .... = O: O-bit is NOT set<br>..1. .... = DC: Demand Circuits are supported<br>...0 .... = L: The packet does NOT contain LLS data block<br>.... 0... = NP: NSSA is NOT supported<br>.... .0.. = MC: NOT Multicast Capable<br>.... ..1. = E: External Routing Capability<br>.... ...0 = MT: NO Multi-Topology Routing<br>Link-State Advertisement Type: Router-LSA (1)<br>Link State ID: 192.168.0.65<br>Advertising Router: 192.168.0.65 (192.168.0.65)<br>LS Sequence Number: 0x80000001<br>LS Checksum: 0x8d70<br>Length: 48<br>Indicating the support of demand circuits and AS external LSA's routing capability. The originating routers ID is indicated in LSID and advertising router field. Then comes the LS sequence, checksum and length in bytes.<br>2. Flags<br>Flags: 0x00<br>.... .0.. = V: NO Virtual link endpoint<br>.... ..0. = E: NO AS boundary router<br>.... ...0 = B: NO Area border router<br>Number of Links: 2<br>indicate that router is not an ABR, ASBR or virtual link end point.It also indicates the no. of networks being advertised being 2.<br>3. Type<br>Type: Stub ID: 192.168.0.188 Data: 255.255.255.252 Metric: 1<br>IP network/subnet number: 192.168.0.188<br>Link Data: 255.255.255.252<br>Link Type: 3 - Connection to a stub network<br>Number of TOS metrics: 0<br>TOS 0 metric: 1<br>Indicates the one network 192.168.0.188 is having 255.255.255.252 subnet mask (advertised as link data)with metric 1 and is connected to a stub network. No type of TOS metric is supported .<br>Type: Stub ID: 192.168.0.65 Data: 255.255.255.255 Metric: 1<br>IP network/subnet number: 192.168.0.65<br>Link Data: 255.255.255.255<br>Link Type: 3 - Connection to a stub network<br>Number of TOS metrics: 0<br>TOS 0 metric: 1<br>this presents the same information as above for 192.168.0.65 |
| 12 | The R2 being DR advertises this Network-LSA<br>LS Update Packet<br>Number of LSAs: 1<br>LS Type: Network-LSA<br>LS Age: 1 seconds<br>Do Not Age: False<br>Options: 0x22 (DC, E)<br>0... .... = DN: DN-bit is NOT set<br>.0.. .... = O: O-bit is NOT set<br>..1. .... = DC: Demand Circuits are supported<br>...0 .... = L: The packet does NOT contain LLS data block<br>.... 0... = NP: NSSA is NOT supported<br>.... .0.. = MC: NOT Multicast Capable<br>.... ..1. = E: External Routing Capability<br>.... ...0 = MT: NO Multi-Topology Routing<br>Link-State Advertisement Type: Network-LSA (2)<br>Link State ID: 192.168.0.190<br>Advertising Router: 192.168.0.129 (192.168.0.129)<br>LS Sequence Number: 0x80000001<br>LS Checksum: 0xaee5<br>Length: 32<br>Netmask: 255.255.255.252<br>Attached Router: 192.168.0.129<br>Attached Router: 192.168.0.65<br>It tells about the interface IP address acting as an active OSPF router. |
| 13 | The R1 send its Router LSA |

<table>
<tr><td></td><td>
<pre>
LS Type: Router-LSA
  LS Age: 1 seconds
  Do Not Age: False
⊟ Options: 0x22 (DC, E)
    0... .... = DN: DN-bit is NOT set
    .0.. .... = O: O-bit is NOT set
    ..1. .... = DC: Demand Circuits are supported
    ...0 .... = L: The packet does NOT contain 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
  Link-State Advertisement Type: Router-LSA (1)
  Link State ID: 192.168.0.65
  Advertising Router: 192.168.0.65 (192.168.0.65)
  LS Sequence Number: 0x80000002
  LS Checksum: 0x4b86
  Length: 48
</pre>
The only change from the Router LSA of R2 being LS age and Sequence number because they are dependent upon the most recent version of LSA<br>
Flags field indicate the presence of 2 links
<pre>
Flags: 0x00
  .... .0.. = V: NO Virtual link endpoint
  .... ..0. = E: NO AS boundary router
  .... ...0 = B: NO Area border router
Number of Links: 2
</pre>
Next comes the Type fields
<pre>
Type: Transit  ID: 192.168.0.190   Data: 192.168.0.189   Metric: 1
  IP address of Designated Router: 192.168.0.190
  Link Data: 192.168.0.189
  Link Type: 2 - Connection to a transit network
  Number of TOS metrics: 0
  TOS 0 metric: 1
</pre>
Shows the next hop for 190 is 189 thus indicating the network type of 192.168.0.190 for R1 is transit having metric of 1. Link ID is connected interface of R1 and Link type is 2 indicating connection to a transit network. So it can be concluded that under default settings the DR becomes the transit router for BDR.
<pre>
Type: Stub     ID: 192.168.0.65    Data: 255.255.255.255 Metric: 1
  IP network/subnet number: 192.168.0.65
  Link Data: 255.255.255.255
  Link Type: 3 - Connection to a stub network
  Number of TOS metrics: 0
  TOS 0 metric: 1
</pre>
This indicates the connected loopback is considered as a stub network.
</td></tr>
<tr><td>14</td><td>
after listening update from R1, R2 sends its modified update(and latest too indicated by incremented sequence number) packet having 2 LSA's (instead of having one as in packet 11) out of which first indicates its interfaces one loopback being stub and other active interface having connected to transit network
<pre>
Type: Stub     ID: 192.168.0.129   Data: 255.255.255.255 Metric: 1
  IP network/subnet number: 192.168.0.129
  Link Data: 255.255.255.255
  Link Type: 3 - Connection to a stub network
  Number of TOS metrics: 0
  TOS 0 metric: 1
Type: Transit  ID: 192.168.0.190   Data: 192.168.0.190   Metric: 1
  IP address of Designated Router: 192.168.0.190
  Link Data: 192.168.0.190
  Link Type: 2 - Connection to a transit network
  Number of TOS metrics: 0
  TOS 0 metric: 1
</pre>
and the second which is updated packet 11$^{th}$,using information of 13$^{th}$ , indicates the interface 190 is having next hop 189 and is acting as a transit network which can reach stub network 192.168.0.65
</td></tr>
</table>

| | |
|---|---|
| | Link-State Advertisement Type: Router-LSA (1)<br>Link State ID: 192.168.0.65<br>Advertising Router: 192.168.0.65 (192.168.0.65)<br>LS Sequence Number: 0x80000002<br>LS Checksum: 0x4b86<br>Length: 48<br>Type: Transit ID: 192.168.0.190 Data: 192.168.0.189 Metric: 1<br>IP address of Designated Router: 192.168.0.190<br>Link Data: 192.168.0.189<br>Link Type: 2 - Connection to a transit network<br>Number of TOS metrics: 0<br>TOS 0 metric: 1<br>Type: Stub ID: 192.168.0.65 Data: 255.255.255.255 Metric: 1<br>IP network/subnet number: 192.168.0.65<br>Link Data: 255.255.255.255<br>Link Type: 3 - Connection to a stub network<br>Number of TOS metrics: 0<br>TOS 0 metric: 1 |
| 15 | Hello of R1 since the routers are done with the exchange of their link states so now the R1 indicates itself as BDR<br>Options: 0x12 (L, E)<br>Router Priority: 1<br>Router Dead Interval: 40 seconds<br>Designated Router: 192.168.0.190<br>Backup Designated Router: 192.168.0.189<br>Active Neighbor: 192.168.0.129 |
| 16, 18 | These are the link state acknowledgement by R1 the type 5 is shown in header with appropriate sequence numbers(Packet no. 18 corresponds to Packet no. 14th updates as is clear from sequence number).<br>OSPF Header<br>OSPF Version: 2<br>Message Type: LS Acknowledge (5)<br>Packet Length: 84<br>Source OSPF Router: 192.168.0.65 (192.168.0.65)<br>Area ID: 0.0.0.0 (Backbone)<br>Packet Checksum: 0x2359 [correct]<br>Auth Type: Null<br>Auth Data (none)<br>R2 sends these so as to explicitly acknowledge the updates from R1 by sending the headers of updates. |
| 17 | R1 sends acknowledgement for the received updates from R2<br>OSPF Header<br>OSPF Version: 2<br>Message Type: LS Acknowledge (5)<br>Packet Length: 64<br>Source OSPF Router: 192.168.0.129 (192.168.0.129)<br>Area ID: 0.0.0.0 (Backbone)<br>Packet Checksum: 0x1b5c [correct]<br>Auth Type: Null<br>Auth Data (none)<br>LSA Header<br>LS Age: 48 seconds<br>Do Not Age: False<br>⊞ Options: 0x22 (DC, E)<br>Link-State Advertisement Type: Router-LSA (1)<br>Link State ID: 192.168.0.65<br>Advertising Router: 192.168.0.65 (192.168.0.65)<br>LS Sequence Number: 0x80000001<br>LS Checksum: 0x8d70<br>Length: 48<br>LSA Header<br>LS Age: 1 seconds<br>Do Not Age: False<br>⊞ Options: 0x22 (DC, E)<br>Link-State Advertisement Type: Router-LSA (1)<br>Link State ID: 192.168.0.65<br>Advertising Router: 192.168.0.65 (192.168.0.65)<br>LS Sequence Number: 0x80000002<br>LS Checksum: 0x4b86<br>Length: 48 |
| 19-22 | These are the alternate Hello's by active connected interfaces of R2 and R1 indicating the stable connection |

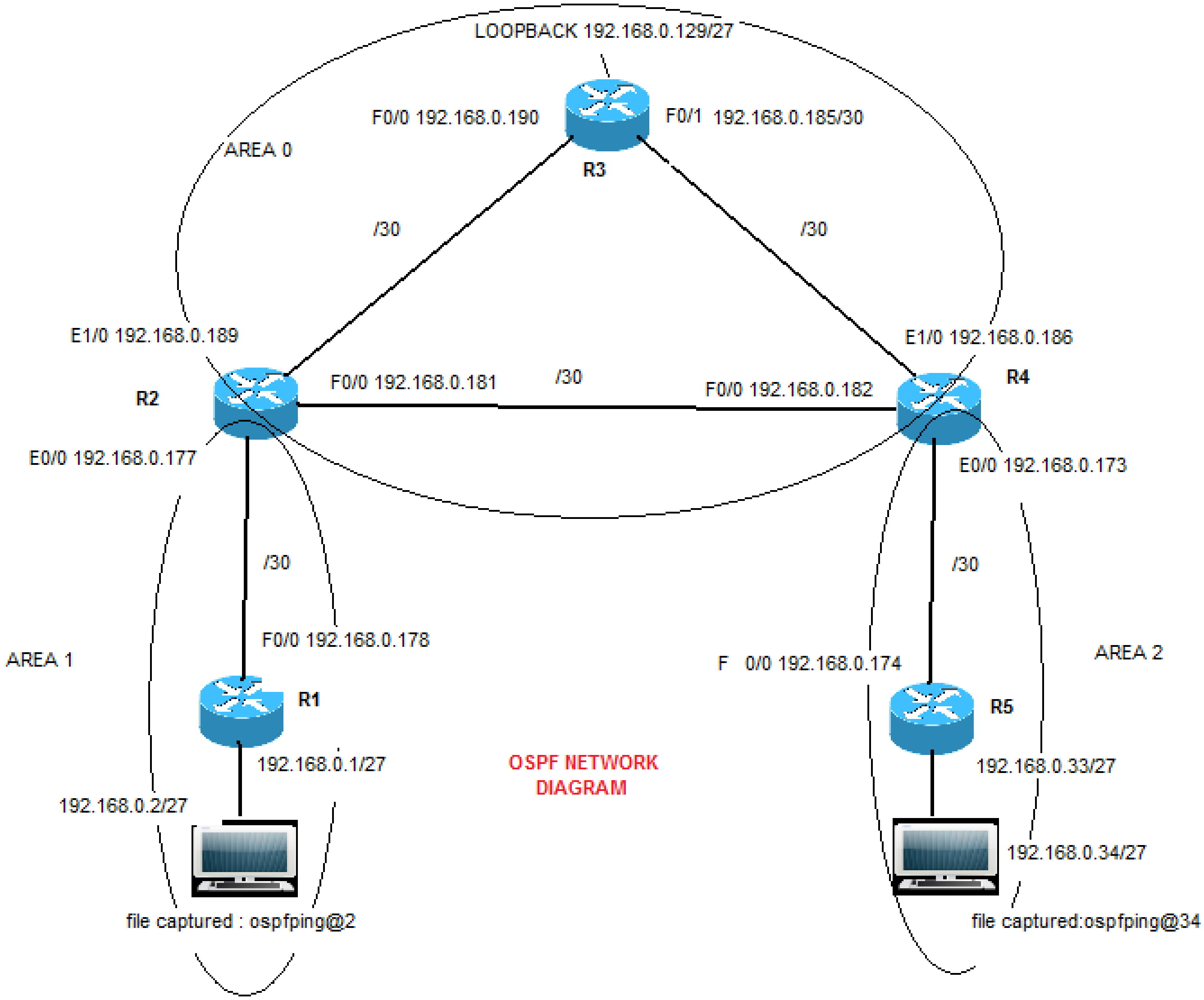
Graphically :

It is very interesting to explain the convergence because of the presence of only 3 types of packets namely Hello, Update and Acknowledgement.




Red bars indicate packets generated by router R1 and blue bars indicate the packets generated by R2. First figure indicates R1 starts OSPF hellos first having an interval of approximately 10 seconds and then R2. R1 has sent 1 LS updates at 48.726581th second and R2 at 48.236280, 48.725079 and 48.756822 seconds out of which two are before R1's hello because being DR. The LS acknowledgements have been transferred at 50.733554 and 50.042197 by R1 and at 50.736735 by R2. So the whole process gets completed within 56 seconds.

**<u>ospfping@34.pcap graphical description</u>**


LOOPBACK 192.168.0.129/27
F0/0 192.168.0.190
F0/1 192.168.0.185/30
AREA 0
R3
/30
/30
E1/0 192.168.0.189
E1/0 192.168.0.186
R2
F0/0 192.168.0.181
/30
F0/0 192.168.0.182
R4
E0/0 192.168.0.177
E0/0 192.168.0.173
/30
/30
F0/0 192.168.0.178
AREA 1
F 0/0 192.168.0.174
AREA 2
R1
R5
192.168.0.1/27
OSPF NETWORK
DIAGRAM
192.168.0.33/27
192.168.0.2/27
192.168.0.34/27
file captured : ospfping@2
file captured:ospfping@34

The output of command prompt is:

C:\Users\ABC>ping 192.168.0.2 -t

1. Pinging 192.168.0.2 with 32 bytes of data:
2. Reply from 192.168.0.2: bytes=32 time=2ms TTL=124
3. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
4. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
5. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
6. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
7. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
8. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
9. Request timed out.
10. Request timed out.
11. Reply from 192.168.0.173: Destination host unreachable.
12. Reply from 192.168.0.173: Destination host unreachable.
13. Reply from 192.168.0.173: Destination host unreachable.
14. Reply from 192.168.0.2: bytes=32 time=3ms TTL=123
15. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
16. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
17. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
18. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
19. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
20. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
21. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
22. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
23. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
24. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
25. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
26. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
27. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123

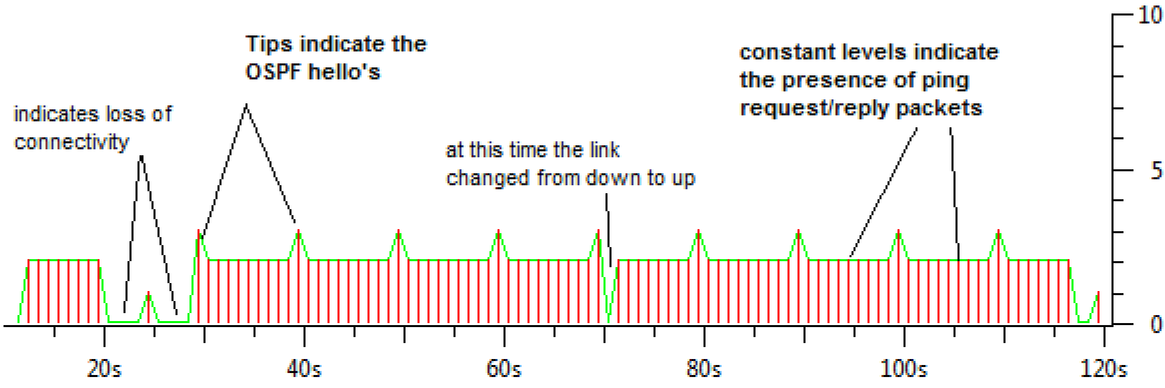
52. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
53. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
54. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
55. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
56. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
57. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
58. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
59. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
60. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
61. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
62. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
63. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
64. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
65. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
66. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
67. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
68. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
69. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
70. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
71. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
72. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
73. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
74. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
75. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
76. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
77. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
78. Reply from 192.168.0.2: bytes=32 time=1ms

28. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
29. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
30. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
31. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
32. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
33. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
34. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
35. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
36. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
37. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
38. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
39. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
40. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
41. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
42. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
43. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
44. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
45. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
46. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
47. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
48. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
49. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
50. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
51. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123

TTL=123

79. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
80. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
81. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
82. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
83. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
84. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
85. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
86. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
87. Reply from 192.168.0.2: bytes=32 time=1ms TTL=123
88. Reply from 192.168.0.2: bytes=32 time=2ms TTL=124
89. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
90. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
91. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
92. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
93. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
94. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
95. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
96. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124
97. Reply from 192.168.0.2: bytes=32 time=1ms TTL=124

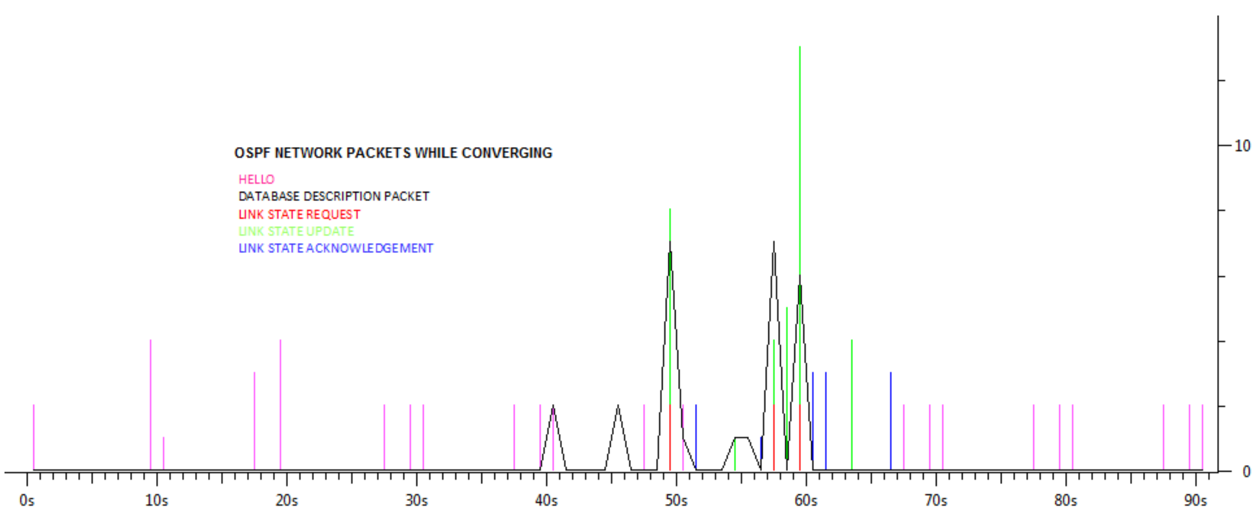
Ping statistics for 192.168.0.2:
Packets: Sent = 96, Received = 94, Lost = 2 (2% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms




opspping@34.pcap

Packets 3 to 16 indicates the successful ping request/reply pairs via 4 routers (R5-R4-R2-R1) as is clear from change in TTL value from 128 of request sent to 124 of reply received. There occurs a connection break between R4-R2 so the packets 17 and 19 went un-responded while the router R4 is establishing alternative path three consecutive pings in packets 20, 23 and 25 are replied back by interface e0/0 of R4 as Destination unreachable. After that the alternative path has been selected as can be seen from TTL values of ping replies now gets changed to 123 indicating the presence of 5 routers(R5-R4-R3-R2-R1) in the path. At near about 105$^{th}$ packet (shown in graph below after 69.993546$^{th}$second) there occurs a delay of 1.012523seconds for the next ping request (but the ping packet is not dropped may be because of the internal router processing/storage) which indicates the change of link state between R4 and R2 from down to up. But the change in route has not occurred yet because of the time delay caused by the switch and the processing time required by the OSPF calculations. The change occurs at 182$^{nd}$ request at approximately 107$^{th}$ second whose reply took 840µseconds more to respond than the previous because of the change. Moreover the TTL value's of reply packets has been changed from 123 to 124.

**FOLLOWING GRAPH SHOWS THE INITIAL CONVERGENCE OF THE ENTIRE NETWORK**



As can be seen first router R2 starts up after 50 µ seconds of the start and after that R3 and R4 respectively. After building the adjacency between them the database description packets exchange starts at 40.000854 seconds and LS request, LS update and LS acknowledgement exchange starts at approximately 50 seconds between three routers resulting in exchange of links and the last acknowledgement occurs at $66.367030^{th}$ second causing the complete convergence of the network so the network gets converged within 26.366176 seconds.

# IS-IS (Intermediate System to Intermediate System)

Originally this Interior Gateway Protocol is an ISO standard defined in ISO: 10589. IETF has redefined in RFC 1142 as an internet standard IGP. It works directly from layer 2 so IS-IS packets are encapsulated in LLC header and then in Ethernet frame for transmission. IS-IS has been identified by Intra domain Routing Discriminator : 0x83

It uses ISO address called Network Entity Title which describe the AREA ID and Device/System ID of the device and is having the following structure.

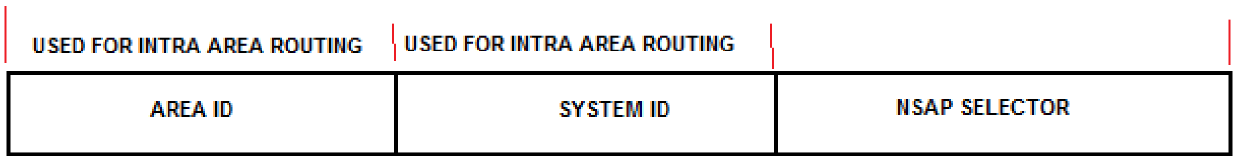



Fig. NET Structure

NET varies from 8 to 20 octets in length. Within the routing domain system ID should be unique and since MAC address is of 48 bits so usually it is of 6 octets in length. NSAP(Network Service Access Point describes an attachment to a particular service at the network layer of a node) Selector is the 1 octet field usually set to all 0's so as to indicate that the address is an NET, the address of node's network layer itself.

Operation:

IS-IS running routers send hello packets periodically so as to discover neighbors and to form adjacencies. The adjacency is formed as soon as hellos are received and the parameters advertised in hello's need not be same for adjacency establishment. After that the LSP's are exchanged so as to build L1 and L2 link state databases. After that SPF algorithm is used for constructing route table.

There are basically 2 types of areas defined in IS-IS : Level 1 and Level 2 out of which level 2 is the backbone area. Routers residing in Level 1 are called L1 routers and routers residing in L2 are called L2 routers whereas the routers connecting L1 and L2 areas are called L1/L2 routers. Moreover the areas are divided by links and not routers and a router will completely be within an area. So there are following types of adjacencies established:

- L1-L1 routers adjacency
- L1-L2 routers adjacency
- L2-L2 routers adjacency

The IS-IS areas are a set of adjacencies identified with the help of same Area ID's. Since anL1/ L2 router can form adjacencies with both L1 and L2 routers the areas can overlap. But L1 only routers form L1 adjacency with L1/L2 router(s) and L2 routers form L2 adjacency with L1/L2 router(s).But for forming adjacencies the area ID's must match.

IS-IS packets are called PDU's(Packet Data Units)

Types: IS-IS uses 9 PDU types

**1. Hello Packets**

- LAN level 1 hello packets(PDU type 15)
- LAN Level 2 hello packets(PDU type 16)
- Point-to-point hello packets(PDU type 17)

**2. Link State packets**

- Level 1 link-state packets(PDU type 18)
- Level 2 link state packets (PDU type 20)

**3. Sequence number packets**

- Level 1 complete sequence number packets(PDU Type 24)
- Level 2 complete sequence number packets(PDU Type 25)

- Level 1 partial sequence number packets(PDU Type 26)
- Level 2 partial sequence number packets(PDU Type 27)

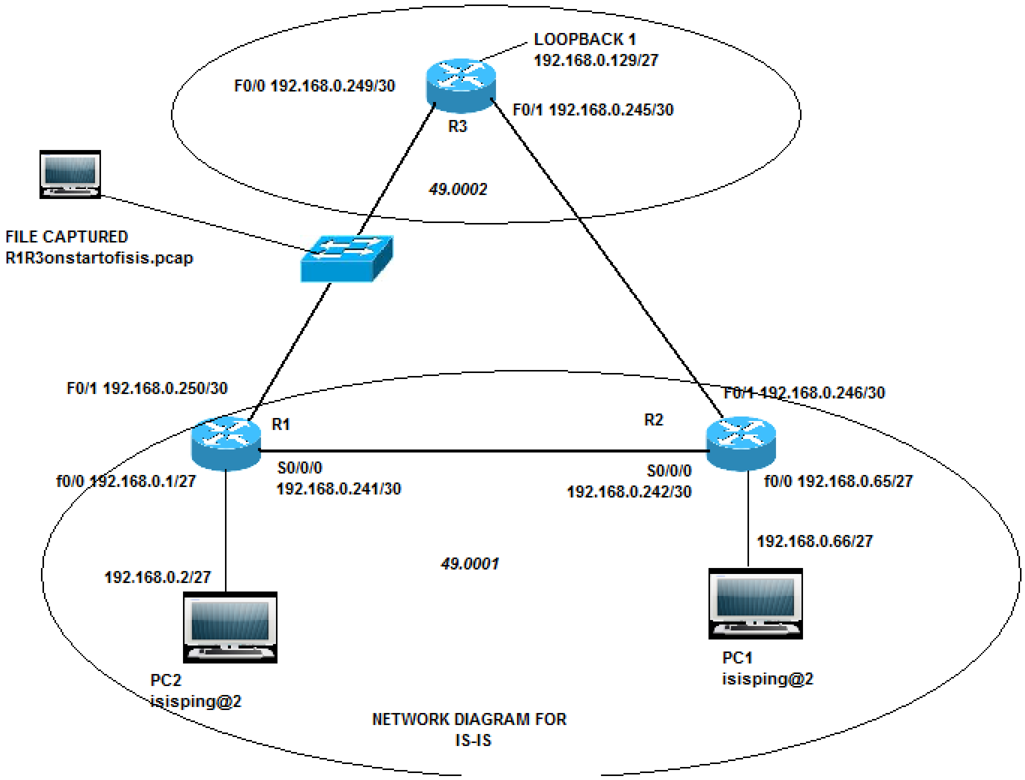
The first 8 octets of all the PDU's are called header and are same.

| | | | |
|---|---|---|---|
| Intradomain Routing Protocol Discriminator(8 bits) | | | |
| Length Indicator(8 bits) | | | |
| Version/Protocol ID Extension (8 bits) | | | |
| ID Length (8 bits) | | | |
| R | R | R | PDU Type (5 bits) |
| Version (8 bits) | | | |
| Reserved (8 bits) | | | |
| Maximum Area Addresses (8 bits) | | | |

**Intradomain Routing Protocol Discriminator:** 0x83
**Length Indicator:** The length of Header in octets
**Version/Protocol ID Extension :** 1
**ID Length :** the length of System ID field of NSAP address and NET's used in this routing domain.It can be:

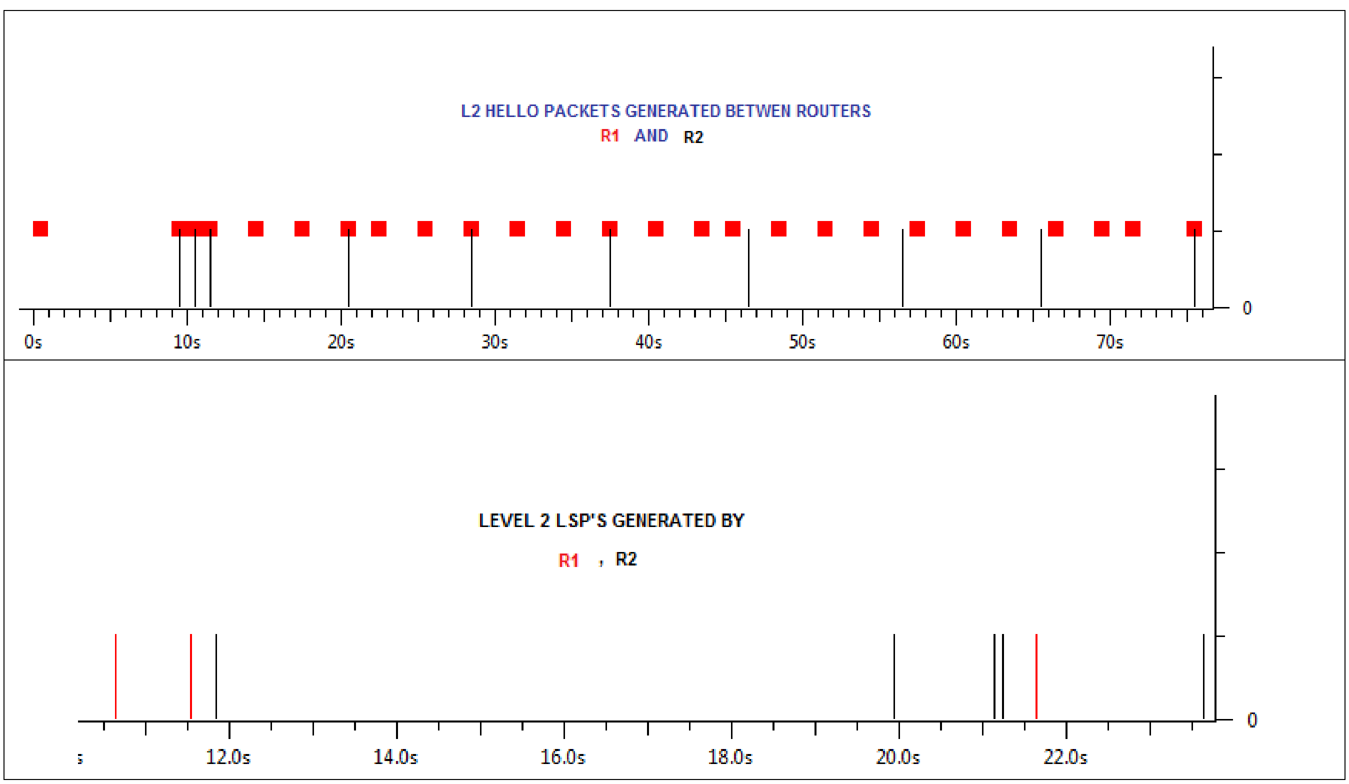
- An integer between 1 and 8 indicating a system ID field of same length in octets
- 0 indicating a system ID field of 6 octets
- 255 indicating a null system ID

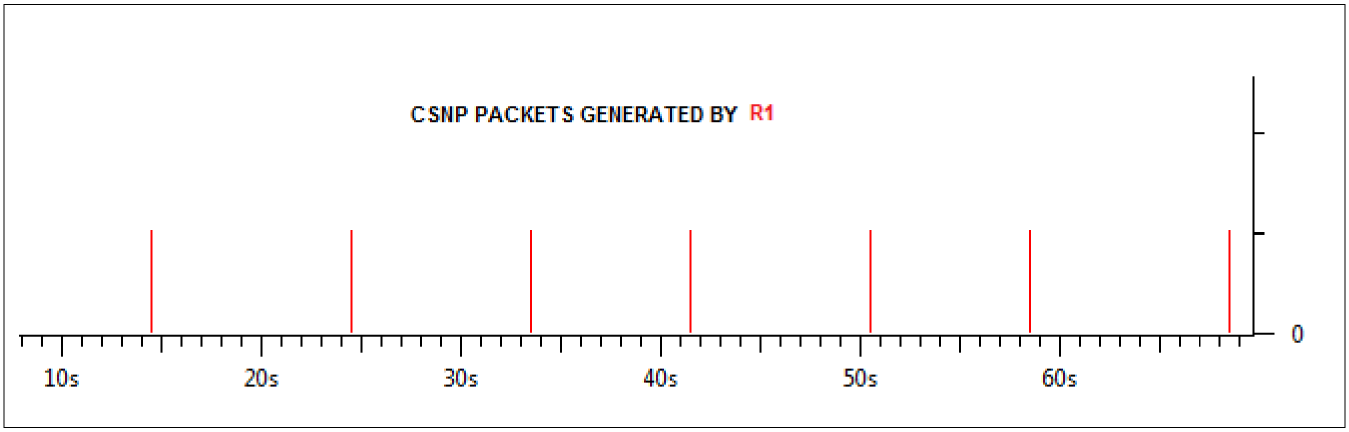
**R, R, R :** reserved always 0
**PDU type :** the packet PDU type
**Version:** 1
**Reserved:** All 0's
**Maximum Area Addresses:** 0 indicates the default value of 3 areas. But can support up to 254



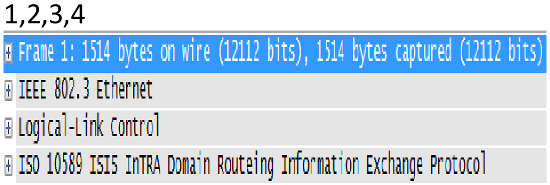
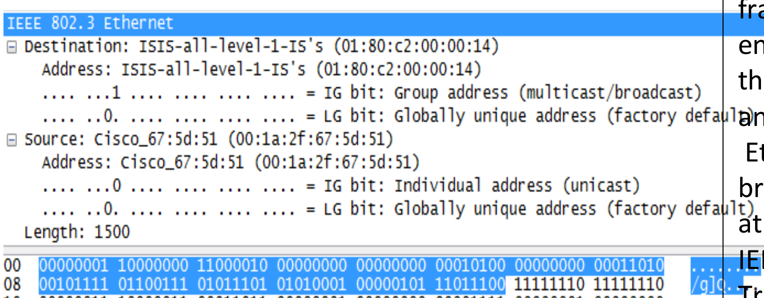
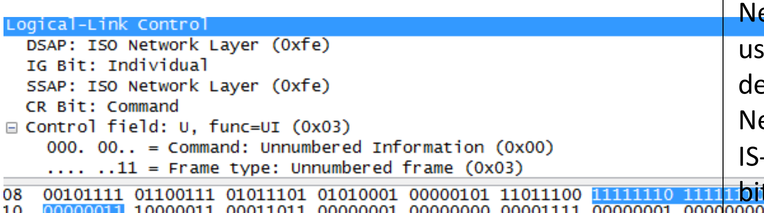

The file **R1R3onstartofisis.pcap** shows the stpes for adjacency establishment between routers R1 and R3 of the above network.

**Graphical representation of packets for file R1R3onstartofisis.pcap**






## R1R3onstartofisis.pcap description

| Packet No. | Description |
|---|---|
| 1,2,3,4<br><br><br> | These packets are alternate L1 and L2 Hello's by R1 since separate adjacency is established between each types of routers. The type is indicated in every 5th octet of Hello. Moreover the destination MAC address will also differentiate between L1 or L2 hello's. The IS_IS frame is of 1541 bytes in length and IS-IS packet is encapsulated in LLC layer and then is transferred over the Ethernet as an Ethernet frame. So IS-IS don't use IP and instead is directly encapsulated in layer 2.<br>Ethernet header is of 56 bits tells that the packet is broadcast from F0/1 interface of R1 for all level-1-IS's at MAC address 01-80-C2-00-00-13 which is used by IEEE 1905 under the standard IEEE Std 1905.1 for the Transmission of IEEE 1905.1 control packets.<br>Next comes the LLC header which indicates It will be used by the Network layer of both the source and destination and is unnumbered.<br>Next comes IS-IS packet which is of 1497 bytes long. All IS-IS packets begin with first 8 bit number where first bit indicates hex value )x83 corresponding to IS-IS and this PDU is 27 bytes long .the IS-IS version is 1 & this is a part of Hello Packet having binary 00001111. This interface is L1/L2 with the system ID 111.1111.1111 with default values of holding time and priority and it advertises itself as DR and 02 indicates it's a level 2 adjacency. Network Layer Protocol ID indicates the upper layer protocol used is IP having the interface address 192.168.0.150 and the associated IS-IS area of R1 is 49.0001. The Cisco NSF flag are 0 indicating not support for graceful restart. And at the last comes the padded bits which indicates the default padding is on so as to transmit full MTU. This is done for the early detection of transmission errors. |

<table>
<tr><td>ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol<br>Intra Domain Routing Protocol Discriminator: ISIS (0x83)<br>PDU Header Length: 27<br>Version (==1): 1<br>System ID Length: 0<br>PDU Type : L1 HELLO (R:000)<br>Version2 (==1): 1<br>Reserved (==0): 0<br>Max.AREAs: (0==3): 0<br>ISIS HELLO<br>Circuit type : Level 1 and 2, reserved(0x00 == 0)<br>System-ID {Sender of PDU} : 1111.1111.1111<br>Holding timer: 30<br>PDU length: 1497<br>Priority : 64, reserved(0x00 == 0)<br>System-ID {Designated IS} : 1111.1111.1111.02<br>Protocols Supported (1)<br>NLPID(s): IP (0xcc)<br>Area address(es) (4)<br>Area address (3): 49.0001<br>IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.250 (192.168.0.250)<br>Restart Signaling (3)<br>Restart Signaling Flags: 0x00<br>.... .0.. = Suppress Adjacency: False<br>.... ..0. = Restart Acknowledgment: False<br>.... ...0 = Restart Request: False<br>Padding (255)<br>Padding (255)<br>Padding (255)<br>Padding (255)<br>Padding (255)<br>Padding (163)</td><td></td></tr>
<tr><td>5</td><td>This is the hello packet generated by interface f0/0 of R3.R3 was configured as L2 router so its hello’s will have only one type i.e. L2 hello. It indicates system ID being 3333.3333.3333.02 and establishing L2 adjacency indicated by 02 at the end from area 49.0002. It also indicates F0/1 of R1 as neighbor resulting in 8 bytes less in padding</td></tr>
<tr><td>6</td><td>The Hello of R1 indicating R3’s interface as neighbor.</td></tr>
<tr><td>8<br>ISO 10589 ISIS Link State Protocol Data Unit<br>PDU length: 98<br>Remaining lifetime: 1199<br>LSP-ID: 1111.1111.1111.00-00<br>Sequence number: 0x00000002<br>Checksum: 0x5d58 [correct]<br>[Good Checksum: True]<br>[Bad Checksum: False]<br>Type block(0x03): Partition Repair:0, Attached bits:0, Overload bit:0, IS type:3<br>0... .... = Partition Repair: Not supported<br>.000 0... = Attachment: 0<br>.... .0.. = Overload bit: Not set<br>.... ..11 = Type of Intermediate System: Level 2 (3)<br>Area address(es) (4)<br>Area address (3): 49.0001<br>Protocols supported (1)<br>NLPID(s): IP (0xcc)<br>Hostname (2)<br>Hostname: R1<br>IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.241 (192.168.0.241)<br>IS Reachability (12)<br>Reserved value 0x00, must == 0<br>IS Neighbor: 1111.1111.1111.02<br>IP Internal reachability (36)<br>IPv4 prefix: 192.168.0.0/27<br>IPv4 prefix: 192.168.0.240/30<br>IPv4 prefix: 192.168.0.248/30</td><td>This is 115 bytes Link State PDU sent by R1 to R3 indicating its directly connected networks. Every LSP has its own ID and appropriate sequence number. In this it indicates that it is transferred between level2 from area 49.0001. It also indicate the name configured on the router i.e. R1 its interface address and also indicates that it is having L2 adjacency .<br>the metric associated for IS-IS becomes simply the hop count as of default vaues of parameters.</td></tr>
<tr><td>10<br>IS Reachability (23)<br>Reserved value 0x00, must == 0<br>IS Neighbor: 1111.1111.1111.00<br>IS Neighbor: 3333.3333.3333.00</td><td>R1 sends another type 3 i.e.L2 LSP indicating its adjacency with R3</td></tr>
<tr><td>12<br>Hostname (2)<br>Hostname: R3<br>IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.129 (192.168.0.129)<br>IS Reachability (12)<br>IP Internal reachability (36)<br>IPv4 prefix: 192.168.0.128/27<br>IPv4 prefix: 192.168.0.244/30<br>IPv4 prefix: 192.168.0.248/30</td><td>R3 send its directly connected networks and associated metrics indicating R1 as the neighbor it uses its loopback as a source for originating LSP’s.</td></tr>
<tr><td>14</td><td>R1 being elected as DR sends Complete Sequence</td></tr>
</table>

| | |
|---|---|
| ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit<br>PDU length: 83<br>Source-ID: 1111.1111.1111.00<br>Start LSP-ID: 0000.0000.0000.00-00<br>End LSP-ID: ffff.ffff.ffff.ff-ff<br>⊟ LSP entries (48)<br>⊟ LSP-ID: 1111.1111.1111.00-00, Sequence: 0x00000002, Lifetime: 1195s, Checksum: 0x5d58<br>LSP-ID: : 1111.1111.1111.00-00<br>LSP Sequence Number : 0x00000002<br>Remaining Lifetime : 1195s<br>LSP checksum : 0x5d58<br>⊟ LSP-ID: 1111.1111.1111.02-00, Sequence: 0x00000001, Lifetime: 1196s, Checksum: 0x4895<br>LSP-ID: : 1111.1111.1111.02-00<br>LSP Sequence Number : 0x00000001<br>Remaining Lifetime : 1196s<br>LSP checksum : 0x4895<br>⊟ LSP-ID: 3333.3333.3333.00-00, Sequence: 0x00000002, Lifetime: 1195s, Checksum: 0x4889<br>LSP-ID: : 3333.3333.3333.00-00<br>LSP Sequence Number : 0x00000002<br>Remaining Lifetime : 1195s<br>LSP checksum : 0x4889 | Number PDU(CSNP) describing its database so as to acknowledge all LSP's before this. |
| 17<br>ISO 10589 ISIS Link State Protocol Data Unit<br>PDU length: 109<br>Remaining lifetime: 1199<br>LSP-ID: 3333.3333.3333.00-00<br>Sequence number: 0x00000003<br>⊞ Checksum: 0xaac0 [correct]<br>⊞ Type block(0x03): Partition Repair:0, Attached bits:0, Overload bit:0, IS type:3<br>⊟ Area address(es) (4)<br>Area address (3): 49.0002<br>⊟ Protocols supported (1)<br>NLPID(s): IP (0xcc)<br>⊟ Hostname (2)<br>Hostname: R3<br>⊟ IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.129 (192.168.0.129)<br>⊟ IS Reachability (23)<br>Reserved value 0x00, must == 0<br>⊞ IS Neighbor: 1111.1111.1111.02<br>⊞ IS Neighbor: 2222.2222.2222.02<br>⊟ IP Internal reachability (36)<br>⊞ IPv4 prefix: 192.168.0.128/27<br>⊞ IPv4 prefix: 192.168.0.244/30<br>⊞ IPv4 prefix: 192.168.0.248/30 | This packet is same as that of 12 but in addition to its connected networks it also sends its neighbors with whom adjacency has been formed since it is the latest LSP so it has an incremented sequence number. |
| 20<br>Hostname (2)<br>Hostname: R2<br>IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.246 (192.168.0.246)<br>IS Reachability (12)<br>Reserved value 0x00, must == 0<br>⊞ IS Neighbor: 2222.2222.2222.02<br>IP Internal reachability (36)<br>⊞ IPv4 prefix: 192.168.0.64/27<br>⊞ IPv4 prefix: 192.168.0.240/30<br>⊞ IPv4 prefix: 192.168.0.244/30 | R3 has learned routes advertised by R2 is advertising newly learned routes and the system 2222.2222.2222.00including the area ID 49.0001 which is same as that of R1 |
| 21<br>ISO 10589 ISIS Link State Protocol Data Unit<br>PDU length: 52<br>Remaining lifetime: 1197<br>LSP-ID: 2222.2222.2222.02-00<br>Sequence number: 0x00000001<br>⊞ Checksum: 0xae62 [correct]<br>⊞ Type block(0x03): Partition Repair:0, Attached bits:0, Overload bit:0, IS type:3<br>⊟ IS Reachability (23)<br>Reserved value 0x00, must == 0<br>⊞ IS Neighbor: 2222.2222.2222.00<br>⊞ IS Neighbor: 3333.3333.3333.00 | R3 has established adjacency with R2 |
| 22<br>⊟ Area address(es) (4)<br>Area address (3): 49.0001<br>⊟ Protocols supported (1)<br>NLPID(s): IP (0xcc)<br>⊟ Hostname (2)<br>Hostname: R1<br>⊟ IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.241 (192.168.0.241)<br>⊟ IS Reachability (12)<br>Reserved value 0x00, must == 0<br>⊞ IS Neighbor: 1111.1111.1111.02<br>⊟ IP Internal reachability (60)<br>⊞ IPv4 prefix: 192.168.0.0/27<br>⊞ IPv4 prefix: 192.168.0.64/27<br>⊞ IPv4 prefix: 192.168.0.240/30<br>⊞ IPv4 prefix: 192.168.0.244/30<br>⊞ IPv4 prefix: 192.168.0.248/30 | R1 sends LSP indicating its newly learned networks from R2 |

| | |
|---|---|
| 24<br>Hostname (2)<br>Hostname: R2<br>IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.246 (192.168.0.246)<br>IS Reachability (12)<br>Reserved value 0x00, must == 0<br>⊞ IS Neighbor: 2222.2222.2222.02<br>IP Internal reachability (60)<br>⊞ IPv4 prefix: 192.168.0.0/27<br>⊞ IPv4 prefix: 192.168.0.64/27<br>⊞ IPv4 prefix: 192.168.0.240/30<br>⊞ IPv4 prefix: 192.168.0.244/30<br>⊞ IPv4 prefix: 192.168.0.248/30 | R3 send its routes learned from the other router . the router having hostname R2 and the sending interface of that router being 192.168.0.146 and is a neighbor as well. |
| 25, 31, 37,43 and 49<br>ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit<br>PDU length: 115<br>Source-ID: 1111.1111.1111.00<br>Start LSP-ID: 0000.0000.0000.00-00<br>End LSP-ID: ffff.ffff.ffff.ff-ff<br>⊟ LSP entries (80)<br>⊞ LSP-ID: 1111.1111.1111.00-00, Sequence: 0x00000003, Lifetime: 1162s, Checksum: 0xe1a9<br>⊞ LSP-ID: 1111.1111.1111.02-00, Sequence: 0x00000001, Lifetime: 1152s, Checksum: 0x4895<br>⊞ LSP-ID: 2222.2222.2222.00-00, Sequence: 0x00000003, Lifetime: 1160s, Checksum: 0x5464<br>⊞ LSP-ID: 2222.2222.2222.02-00, Sequence: 0x00000001, Lifetime: 1158s, Checksum: 0xae62<br>⊞ LSP-ID: 3333.3333.3333.00-00, Sequence: 0x00000003, Lifetime: 1159s, Checksum: 0xaac0 | These are the CSNP packets sent periodically (at an interval of 10 seconds) by the DR indicating the all connected networks and their life(decreasing with an interval of approximately 10 seconds) on he database until now advertised.It basically presents the database of DR. |

**isislinkchange.pcap**

A ping has been initialized from a PC connected to router R2. Because the source and destinations are within same area as well as because of the use of default metric and other parameters it can be said that the IS-IS metric simply gets limited to hop count. This information is indicated in IP Internal Reachability TLV as the Default Metric and the router with which the adjacency has been established is indicated as IPv4 interface.

Ping has been initialized from PC connected to 192.168.0.2 whose command prompt output is :

C:\Users\ABC>ping 192.168.0.66 -t

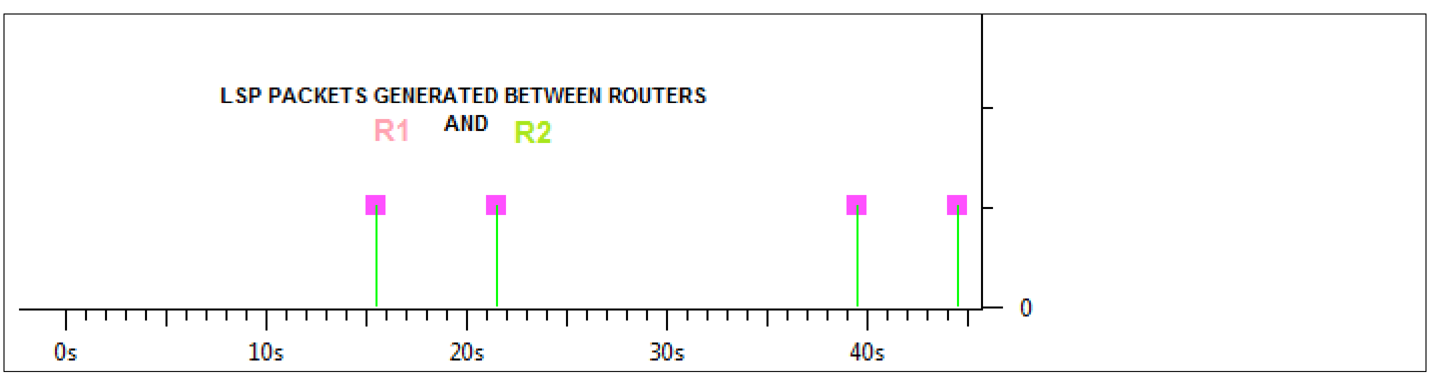
Pinging 192.168.0.66 with 32 bytes of data:

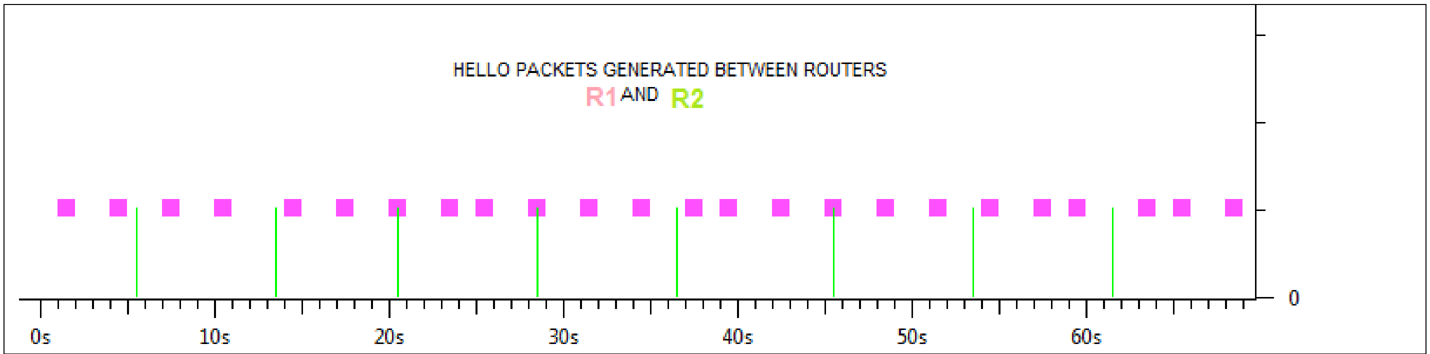
1. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
2. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
3. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
4. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
5. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
6. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
7. Request timed out.
8. Reply from 192.168.0.1: Destination host unreachable.
9. Request timed out.
10. Reply from 192.168.0.66: bytes=32 time=1ms TTL=125
11. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
12. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
13. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
14. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
15. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
16. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
17. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
18. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
19. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
20. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125

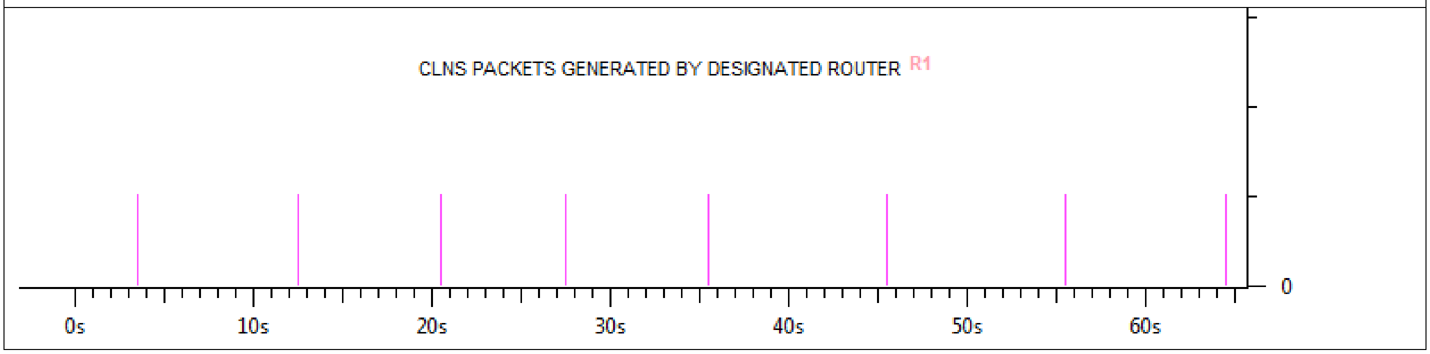
21. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
22. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
23. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
24. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
25. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
26. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
27. Reply from 192.168.0.66: bytes=32 time<1ms TTL=125
28. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
29. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
30. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
31. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
32. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
33. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
34. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
35. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
36. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
37. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
38. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
39. Reply from 192.168.0.66: bytes=32 time=18ms TTL=126
40. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
41. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
42. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126
43. Reply from 192.168.0.66: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.0.66:
Packets: Sent = 43, Received = 41, Lost = 2 (4% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 18ms, Average = 9ms

The packets were following the path PC1-R2-R1-PC2 within the same area. After 6$^{th}$ packet the link R2-R1 gets down and there occurred a loss of 3 packets out of which one is a reply by R2 as "Destination Unreachable". The ping packets sent was having TTL value of 128 from both PC's(request from PC1 and reply from PC2) the received ping reply indicates the path traversed was composed of 2 routers for packets 1-6 after a loss of 3 packets. The packets traverse PC1-R2-R3-R1-PC2 path and the presence of 3 routers is indicated by TTL value change to 125. After that the link R2-R1 becomes up and the routers start forwarding packets again via the initial path. The routers behavior has been captured in file **isislinkchange.pcap** which is captured from link R3-R1 with the help of a switch. The various packets flow are graphically shown below:






Out of 3 types of packets generated in this case Hello's are not of much concern because of a different link. The IP internal reachibilty TLV in packets 12,13,19,20,33,34,37,38 variation indicates the state change of R2-R1 link.

12

```
  IPv4 interface address: 192.168.0.250 (192.168.0.250)
IS Reachability (12)
IP Internal reachability (60)
⊟ IPv4 prefix: 192.168.0.0/27
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.64/27
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.240/30
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.244/30
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.248/30
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
```

13

```
  IPv4 interface address: 192.168.0.246 (192.168.0.246)
IS Reachability (12)
IP Internal reachability (60)
⊟ IPv4 prefix: 192.168.0.0/27
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.64/27
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.240/30
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.244/30
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.248/30
    Default Metric: 20, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
```

19

```
IP Interface address(es) (4)
  IPv4 interface address: 192.168.0.250 (192.168.0.250)
IS Reachability (12)
IP Internal reachability (24)
⊟ IPv4 prefix: 192.168.0.0/27
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.248/30
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
```

20

```
  IPv4 interface address: 192.168.0.246 (192.168.0.246)
IS Reachability (12)
IP Internal reachability (24)
⊟ IPv4 prefix: 192.168.0.64/27
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
⊟ IPv4 prefix: 192.168.0.244/30
    Default Metric: 10, Internal, Distribution: up
    Delay Metric:   Not supported
    Expense Metric: Not supported
    Error Metric:   Not supported
```

33

34

| | |
|---|---|
| IP Interface address(es) (4)<br>IPv4 interface address: 192.168.0.241 (192.168.0.241)<br>IS Reachability (12)<br>IP Internal reachability (36)<br>⊟ IPv4 prefix: 192.168.0.0/27<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.240/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.248/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported | IPv4 interface address: 192.168.0.246 (192.168.0.246)<br>IS Reachability (12)<br>IP Internal reachability (36)<br>⊟ IPv4 prefix: 192.168.0.64/27<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.240/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.244/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported |
| 37<br>IPv4 interface address: 192.168.0.241 (192.168.0.241)<br>IS Reachability (12)<br>IP Internal reachability (60)<br>⊟ IPv4 prefix: 192.168.0.0/27<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.64/27<br>Default Metric: 20, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.240/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.244/30<br>Default Metric: 20, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.248/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported | 38<br>IPv4 interface address: 192.168.0.246 (192.168.0.246)<br>IS Reachability (12)<br>IP Internal reachability (60)<br>⊟ IPv4 prefix: 192.168.0.0/27<br>Default Metric: 20, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.64/27<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.240/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.244/30<br>Default Metric: 10, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported<br>⊟ IPv4 prefix: 192.168.0.248/30<br>Default Metric: 20, Internal, Distribution: up<br>Delay Metric: Not supported<br>Expense Metric: Not supported<br>Error Metric: Not supported |

t

R3 had formed different adjacencies with R1 and R2 resulting in two DR's one being R1 on R1-R3 link and other being R2 on R2-R3 so it is having 2 different types of metric value advertised by R1 and R3 monitored interfaces. There occurs a loss of networks in LSU 19-20 advertising only directly connected interfaces. The ipv4 interface address shown indicates the source via which the R3 and R1 has learned routes. So as it can be seen from the output of file isisping@2 that there occurs an approximate of 10 seconds loss of connectivity which is approximately the time interval between 19$^{th}$ and 33$^{rd}$ packet. The LSU's 33-34 indicate the interface R2-R1 coming up .After that in packets 37-38 the newly established metrics via area 1 are shown.

# BGPv4 (BORDER GATEWAY PROTOCOL VERSION 4)

BGP is an inter Autonomous System routing protocol that runs from the transport layer using TCP port 179 and can be used for loop free inter-domain routing. The BGP speaking routers form an adjacency using TCP connection at port 179 and they exchange their full routes once after that the kepalive messages are used for the sole purpose of link state monitoring and when there occurs a change in any network updates are sent so that the routers can modify their routing information. Two BGP speaking routers are called peers or neighbors. When BGP runs within a same Autonomous System it is called iBGP having AD equal to 200 and when it runs within AS's it is called eBGP having AD value of 20. So the routes learned via eBGP are preferred over iBGP.
BGP uses four types of messages namely open , update, notification of keepalive. Every BGP message begin with a header called BGP header which is composed of 4 components:

1. Marker : this is a 16 byte sequence of all1's and is sent so as to check the synchronization between transmitter and receiver
2. Length : This 2 byte sequence which indicates the length of the BGP meaasage in octets when converted into decimal.
3. Type : The 1 byte field indicates the type of the message i.e. update, keepalive etc. The RFC 1771 specify only 4 message types as shown in table

| Type field value(in decimal) | Meaning |
|---|---|
| 1 | Open |
| 2 | Update |
| 3 | Notification |
| 4 | Keepalive |

4. Actual Message this is a variable length field varying from 0 to 4077 bytes in length.

Various message types are :
***Open Message*** establishes a peering session contains the following information:

| version | My AS | Hold Time | Identifier | Par Length | Optional Parameters |
|---|---|---|---|---|---|

**Version** this is a 4 bytes field which is set to four i.e. current version of BGP
**My AS** is the autonomous sytem of the sender and this field is 2 bytes in length
**Hold Time** a 2 bytes field which indicates the time after which TCP session is to be torn down if no message is received
**Identifier** is a 4 bytes long field conaits the ip address of the router advertising BGP
**Par Length** is 1 byte long field indicates the length of the optional parameters if included
**Optional Parameters** this value coud be 0 to 255 bytes in lengh and tells about the presence of additional features such as authentication

***Update Message send***
Used to transfer route information

| UR length | Withdrawn Routes | Path attribute length | Path Attributes | Network Layer Reachability Information |
|---|---|---|---|---|

The update message begins with 2 bytes UR length field which is unfeasible routes length which corresponds to the next field which is withdrawn field
**PA length** indicates the total length in octets of path attributes it's a 2 byte field

**Path Attributes** it's a variable length field indicates the path attributes contained and every path attribute begins with 2 bytes out of which first is attribute flag byte and the second is attribute type

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Optional Bit | Transitive Bit | Partial Bit | Extended Bit | unused | unused | unused | unused |

Optional bit indicates whether the attributes are well known(0) or optional ones(1)
Transitive Bit is used to control the scope of community i.e transitive(1) or non-transitive(0)
Partial Bit tells us that if the attribute is patial(1) or complete (0)
Extended Bit when 0 indicates attribute flag is one byte and when 1 indicates attribute flag is two bytes
Next 4 bits are not used
Attribute Type is used to select optimum route in case of existence of multiple routes

| Type code | Meaning |
|---|---|
| 1 | origin |
| 2 | AS path |
| 3 | Next hop |
| 4 | Multi Exit Discriminator |
| 5 | Local preference |

Next come the **NLRI** field which includes the paths to be advertised as reachable

***Notification Message***

| | | |
|---|---|---|
| Error Code (1 byte) | Error Sub-code (1 byte) | Error Data (variable in length ) |

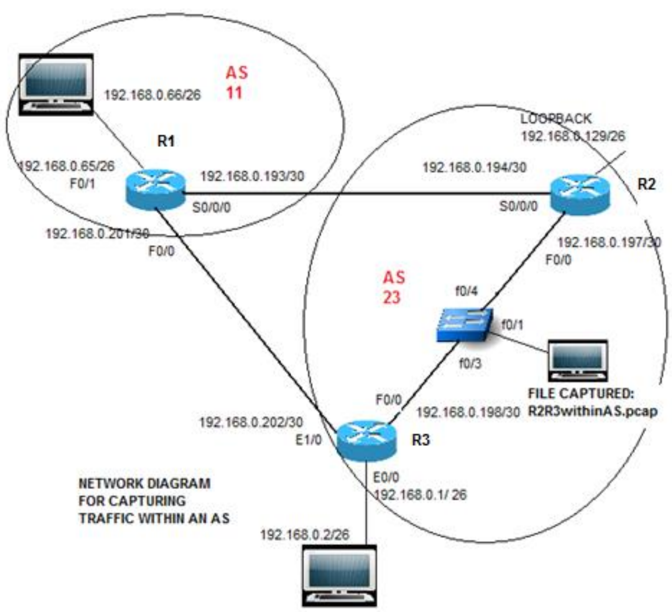
Error code indicates the type of error
Error subcode indicates whether the aerror is related to message header, Update message etc.
Error data contains the actual erroneous message

***Keepalive Message***

Keepalive messages are sent between peer routers so as to validate the connectivity it is a 19 octets long message and contains BGP message header

| | | |
|---|---|---|
| Marker(16 Bytes) | Length(2 Bytes) | Type(1 Byte) |

**R2R3withinAS.pcap**



The message exchanged between two routers upon startup of BGP within an AS has been captured in file R2R3withinAS.pcap.Every BGP message id having PSH control bit set whereas TCP does not. Moreover the TTL value is 255 for all packets exchanged within AS. Also the source and destination ports from which router communicate with BGP TCP port 179 is always same on both end routers/neighbors. Because of use of TCP the sequence numbers must be properly handled for successful communication .The description of which is below:

```
 Sequence number: 0    (relative sequence number)
 Header length: 24 bytes
 Flags: 0x02 (SYN)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR):
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...0 .... = Acknowledgement: Not set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
 ⊞ .... .... ..1. = Syn: Set
Sequence number: 0    (relative sequence number)
Acknowledgement number: 1    (relative ack number)
Header length: 24 bytes
Flags: 0x12 (SYN, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR)
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgement: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
⊞ .... .... ..1. = Syn: Set
Sequence number: 1    (relative sequence number)
Acknowledgement number: 1    (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR):
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgement: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
Sequence number: 1    (relative sequence number)
[Next sequence number: 46    (relative sequence number)]
Acknowledgement number: 1    (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgement: Set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
Window size value: 16384
[Calculated window size: 16384]
[Window size scaling factor: -2 (no window scaling used)]
```

The packets 1, 2 and 3 establish a TCP connection indicating 3-way handshake. The first packet is a simple connection initiation by R2 indicating the Source Port used is 62513 and the destination port being 179 (the BGP port) at R3. The SYN flag is set so as to make synchronization between initial connection establishment packets. The initial sequence numbers shown is 0(for simplicity Wireshark don't shows the default because of preference setting for TCP). In second packet R3 acknowledges the first packet indicating acknowledgement number of 1. Also the ACK bit is set.

In the third packet R2 acknowledges the R3's packet indicated by change in sequence number and acknowledgement number field

Since the TCP connection has been established successfully so R2 send an open message indicating its sequence number and next sequence number expected. Moreover the ACK and PSH is set so as to send the data immediately and no window scaling has been used.

```
Border Gateway Protocol
⊟ OPEN Message
    Marker: 16 bytes
    Length: 45 bytes
    Type: OPEN Message (1)
    Version: 4
    My AS: 33
    Hold time: 180
    BGP identifier: 192.168.0.129
    Optional parameters length: 16 bytes
  ⊟ Optional parameters
    ⊟ Capabilities Advertisement (8 bytes)
        Parameter type: Capabilities (2)
        Parameter length: 6 bytes
      ⊟ Multiprotocol extensions capability (6 bytes)
          Capability code: Multiprotocol extensions capability (1)
          Capability length: 4 bytes
        ⊟ Capability value
            Address family identifier: IPv4 (1)
            Reserved: 1 byte
            Subsequent address family identifier: Unicast (1)
    ⊟ Capabilities Advertisement (4 bytes)
        Parameter type: Capabilities (2)
        Parameter length: 2 bytes
      ⊟ Route refresh capability (2 bytes)
          Capability code: Route refresh capability (128)
          Capability length: 0 bytes
    ⊟ Capabilities Advertisement (4 bytes)
        Parameter type: Capabilities (2)
        Parameter length: 2 bytes
      ⊟ Route refresh capability (2 bytes)
          Capability code: Route refresh capability (2)
          Capability length: 0 bytes
```

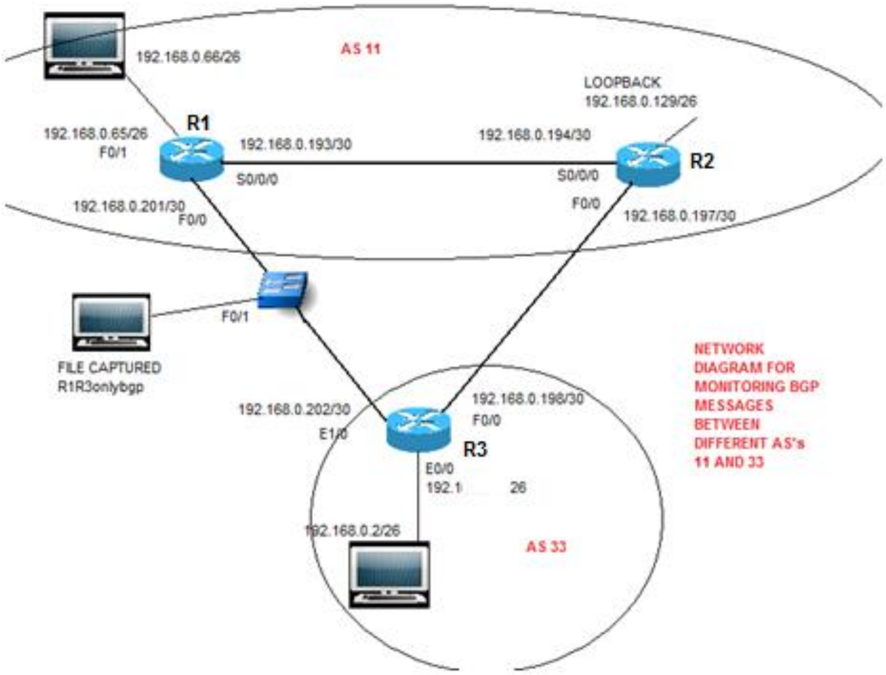
$4^{th}$ packet is BGPv4 open packet which is used to establish a peering session and the router advertises its capabilities as well. The packet indicates that the loopback is used for advertising the BGP indicated in BGP identifier field and it is originated from AS number 33 and hold time is 180second. The advertising router supports multiprotocol extensions and route refreshing. The PSH and ACK are set for OPEN message as well. Also there occurs a change in sequence number and acknowledgement numbers relatively and the window size also varies as per data.

| | |
|---|---|
| Type: OPEN Message (1)<br>Version: 4<br>My AS: 33<br>Hold time: 180<br>BGP identifier: 192.168.0.202<br>Optional parameters length: 16 bytes<br>⊟ Optional parameters<br>⊟ Capabilities Advertisement (8 bytes)<br>Parameter type: Capabilities (2)<br>Parameter length: 6 bytes<br>⊟ Multiprotocol extensions capability (6 bytes)<br>Capability code: Multiprotocol extensions capability<br>Capability length: 4 bytes<br>⊟ Capability value<br>Address family identifier: IPv4 (1)<br>Reserved: 1 byte<br>Subsequent address family identifier: Unicast (1)<br>⊟ Capabilities Advertisement (4 bytes)<br>Parameter type: Capabilities (2)<br>Parameter length: 2 bytes<br>⊟ Route refresh capability (2 bytes)<br>Capability code: Route refresh capability (128)<br>Capability length: 0 bytes<br>⊟ Capabilities Advertisement (4 bytes)<br>Parameter type: Capabilities (2)<br>Parameter length: 2 bytes<br>⊟ Route refresh capability (2 bytes)<br>Capability code: Route refresh capability (2)<br>Capability length: 0 bytes<br>⊟ Border Gateway Protocol<br>⊟ KEEPALIVE Message<br>Marker: 16 bytes<br>Length: 19 bytes<br>Type: KEEPALIVE Message (4) | in 5th packet R3 sends its own Open message besides acknowledging previous OPEN message received. Also it contains a keepalive message in that.It tells us that this router is also in same AS 33 and is advertising using its interface 192.168.0.202.<br>It advertises its own capabilities which are same as that of R2.<br>At the end there is attached a keepalive packet which is basically the BGP header. |
| 6-7, 8-9 and 10-11 | These are the normal keepalive and acknowledgement pairs of BGP and TCP messages |
| 12<br>Path attributes<br>⊟ ORIGIN: IGP (4 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: ORIGIN (1)<br>Length: 1 byte<br>Origin: IGP (0)<br>⊟ AS_PATH: empty (3 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: AS_PATH (2)<br>Length: 0 bytes<br>AS path: empty<br>⊟ NEXT_HOP: 192.168.0.197 (7 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: NEXT_HOP (3)<br>Length: 4 bytes<br>Next hop: 192.168.0.197 (192.168.0.197)<br>⊟ MULTI_EXIT_DISC: 0 (7 bytes)<br>⊞ Flags: 0x80 (Optional, Non-transitive, Complete)<br>Type code: MULTI_EXIT_DISC (4)<br>Length: 4 bytes<br>Multiple exit discriminator: 0<br>⊟ LOCAL_PREF: 100 (7 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: LOCAL_PREF (5)<br>Length: 4 bytes<br>Local preference: 100<br>Network layer reachability information: 15 bytes<br>⊞ 192.168.0.196/30<br>⊞ 192.168.0.192/30<br>⊞ 192.168.0.128/26 | R2 sends Update message specifying its directly connected routes and associated address masks as well as advertises 5 path attributes AS_PATH, NEXT_HOP, MULTI_EXIT_DISC and LOCAL_PREFERENCE that are used for route selection criteria by BGP. The origin code value is 0 indicating the routes are learned via iBGP.T he next hop attribute conveys that the interface having IPv4 address of 192.168.0.197 has been used to reach the destination router . Local preference is the default value of 100. |
| in 13th packet R3 acknowledges packet 12. 14 and 15 are the normal keepalive messages and 16 is again a TCP acknowledgement by R3 | |
| 17 R3 sends its own update message to R2 and it contains a keepalive as well. | It contains three directly connected networks and the next hop of 192.168.0.198 and the routes are being learned by using IGP having the default preference of 100. At the end is appended a keepalive message. |

| | |
|---|---|
| Border Gateway Protocol<br>⊟ UPDATE Message<br>Marker: 16 bytes<br>Length: 66 bytes<br>Type: UPDATE Message (2)<br>Unfeasible routes length: 0 bytes<br>Total path attribute length: 28 bytes<br>⊟ Path attributes<br>⊟ ORIGIN: IGP (4 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: ORIGIN (1)<br>Length: 1 byte<br>Origin: IGP (0)<br>⊞ AS_PATH: empty (3 bytes)<br>⊟ NEXT_HOP: 192.168.0.198 (7 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: NEXT_HOP (3)<br>Length: 4 bytes<br>Next hop: 192.168.0.198 (192.168.0.198)<br>⊞ MULTI_EXIT_DISC: 0 (7 bytes)<br>⊟ LOCAL_PREF: 100 (7 bytes)<br>⊞ Flags: 0x40 (Well-known, Transitive, Complete)<br>Type code: LOCAL_PREF (5)<br>Length: 4 bytes<br>Local preference: 100<br>⊟ Network layer reachability information: 15 bytes<br>⊞ 192.168.0.0/26<br>⊞ 192.168.0.196/30<br>⊞ 192.168.0.200/30<br>Border Gateway Protocol<br>⊟ KEEPALIVE Message<br>Marker: 16 bytes<br>Length: 19 bytes<br>Type: KEEPALIVE Message (4) | |
| after that 18th and 21st are both TCP acknowledgement by R2 and R3 respectively as well as 19-20 are the keep alive messages. | |

Next is the file diff AS R1R3onlybgp.pcap which indicates the behavior of two BGP running routers R1 and R3 in different Autonomous Systems 11 and 33 respectively (the wireshark coloring scheme shows the different AS router packets in RED colour by default so as to differentiate it from iBGP packets).

The first 3 packets cause 3 way handshake to occur and a successful connection has been established. After that Both routers send their OPEN message so as to form peer adjacencies. The main difference between the previously discussed packets and these ones is the change in AS number values to mentioned above. Also the TTL values of all packets except the 2nd in three-way handshake (which is acknowledgement is 1 have TTL=255 indicating it can travel more than one hops) within two different AS's. Moreover different coloring scheme has been used by wireshark for indicating different AS packets (red colored)




<table>
<tr>
<td>Border Gateway Protocol<br>⊟ UPDATE Message<br>Marker: 16 bytes<br>Length: 63 bytes<br>Type: UPDATE Message (2)<br>Unfeasible routes length: 0 bytes<br>Total path attribute length: 25 bytes<br>⊟ Path attributes<br>⊞ ORIGIN: IGP (4 bytes)<br>⊞ AS_PATH: 11 (7 bytes)<br>⊞ NEXT_HOP: 192.168.0.201 (7 bytes)<br>⊞ MULTI_EXIT_DISC: 0 (7 bytes)<br>⊟ Network layer reachability information: 15 bytes<br>⊞ 192.168.0.200/30<br>⊞ 192.168.0.192/30<br>⊞ 192.168.0.64/26<br>R1 sends its update in 12th packet Indicating the AS , Next hop used to advertise and the routes advertised with subnet mask. It also indicates these routes are learned via IGP.</td>
<td>Border Gateway Protocol<br>⊟ UPDATE Message<br>Marker: 16 bytes<br>Length: 63 bytes<br>Type: UPDATE Message (2)<br>Unfeasible routes length: 0 bytes<br>Total path attribute length: 25 bytes<br>⊟ Path attributes<br>⊞ ORIGIN: IGP (4 bytes)<br>⊞ AS_PATH: 33 (7 bytes)<br>⊞ NEXT_HOP: 192.168.0.202 (7 bytes)<br>⊞ MULTI_EXIT_DISC: 0 (7 bytes)<br>⊟ Network layer reachability information: 15 bytes<br>⊞ 192.168.0.0/26<br>⊞ 192.168.0.196/30<br>⊞ 192.168.0.200/30<br>Border Gateway Protocol<br>⊟ KEEPALIVE Message<br>Marker: 16 bytes<br>Length: 19 bytes<br>Type: KEEPALIVE Message (4)<br>In 17th packet R3 sends its UPDATE message for R1 as well as includes a keep alive message. It is clear that AS is different from R1 and is 33.</td>
</tr>
</table>

The rest of the packets are normal keepalives and TCP acknowledgements.
Next is verified the behavior of network for R1-R3 link state change. First the preferred path was PC1-R3-R1-PC2 then the link R1-R3 gets down and the traffic starts flowing alternate path PC1-R3-R2-R1-PC2 this change of path by R3 has been captured in file bgppingR3R2.pcap and is explained below.(The first Network Diagram has been used for capturing traffic)
For packets 1 to 6 there were no ICMP traffic on the link as the other link was up but after 6th packet the link R1-R3 goes down and this change can be seen on link R3-R2 from the update packet no. 7 sent by R3 to R2 indicating the removed routes that become unavailable after link state change on R3-R1 and the message sent by R2 to R3

| update from R3 to R2 | update from R2 to R3 |
|---|---|

**update from R3 to R2**

```
Border Gateway Protocol
⊟ UPDATE Message
    Marker: 16 bytes
    Length: 43 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 20 bytes
  ⊟ Withdrawn routes:
    ⊞ 192.168.0.64/26
    ⊞ 192.168.0.128/26
    ⊞ 192.168.0.192/30
    ⊞ 192.168.0.200/30
    Total path attribute length: 0 bytes
```

**update from R2 to R3**

```
Border Gateway Protocol
⊟ UPDATE Message
    Marker: 16 bytes
    Length: 28 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 5 bytes
  ⊟ Withdrawn routes:
    ⊞ 192.168.0.200/30
    Total path attribute length: 0 bytes
```

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 60.001034 | 192.168.0.197 | 192.168.0.198 | BGP | 73 | KEEPALIVE Message |
| 6 | 60.200460 | 192.168.0.198 | 192.168.0.197 | TCP | 60 | bgp > 13461 [ACK] Seq=39 Ack=39 Win=16054 Len=0 |
| 7 | 61.435854 | 192.168.0.198 | 192.168.0.197 | BGP | 97 | UPDATE Message |
| 8 | 61.634311 | 192.168.0.197 | 192.168.0.198 | TCP | 60 | 13461 > bgp [ACK] Seq=39 Ack=82 Win=16037 Len=0 |
| 9 | 62.176128 | 192.168.0.2 | 192.168.0.66 | ICMP | 74 | Echo (ping) request id=0x0001, seq=491/60161, ttl=127 |
| 10 | 64.568847 | 192.168.0.197 | 192.168.0.198 | BGP | 82 | UPDATE Message |
| 11 | 64.768100 | 192.168.0.198 | 192.168.0.197 | TCP | 60 | bgp > 13461 [ACK] Seq=82 Ack=67 Win=16026 Len=0 |
| 12 | 67.183956 | 192.168.0.2 | 192.168.0.66 | ICMP | 74 | Echo (ping) request id=0x0001, seq=492/60417, ttl=127 |
| 13 | 67.201717 | 192.168.0.66 | 192.168.0.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=492/60417, ttl=126 |
| 14 | 68.182382 | 192.168.0.2 | 192.168.0.66 | ICMP | 74 | Echo (ping) request id=0x0001, seq=493/60673, ttl=127 |
| 15 | 68.200186 | 192.168.0.66 | 192.168.0.2 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=493/60673, ttl=126 |

The trace above shows the moment while the alternate path is being established with the help of start of a ping reply after the one didn't get .The corresponding section of command prompt window is : Pinging 192.168.0.66 with 32 bytes of data:

Reply from 192.168.0.66: bytes=32 time=2ms TTL=126
Reply from 192.168.0.66: bytes=32 time<1ms TTL=126
Reply from 192.168.0.66: bytes=32 time<1ms TTL=126
Reply from 192.168.0.66: bytes=32 time<1ms TTL=126
Request timed out.
Request timed out.
Reply from 192.168.0.66: bytes=32 time=18ms TTL=125
Reply from 192.168.0.66: bytes=32 time=18ms TTL=125

Out of which one might get lost on the down link .

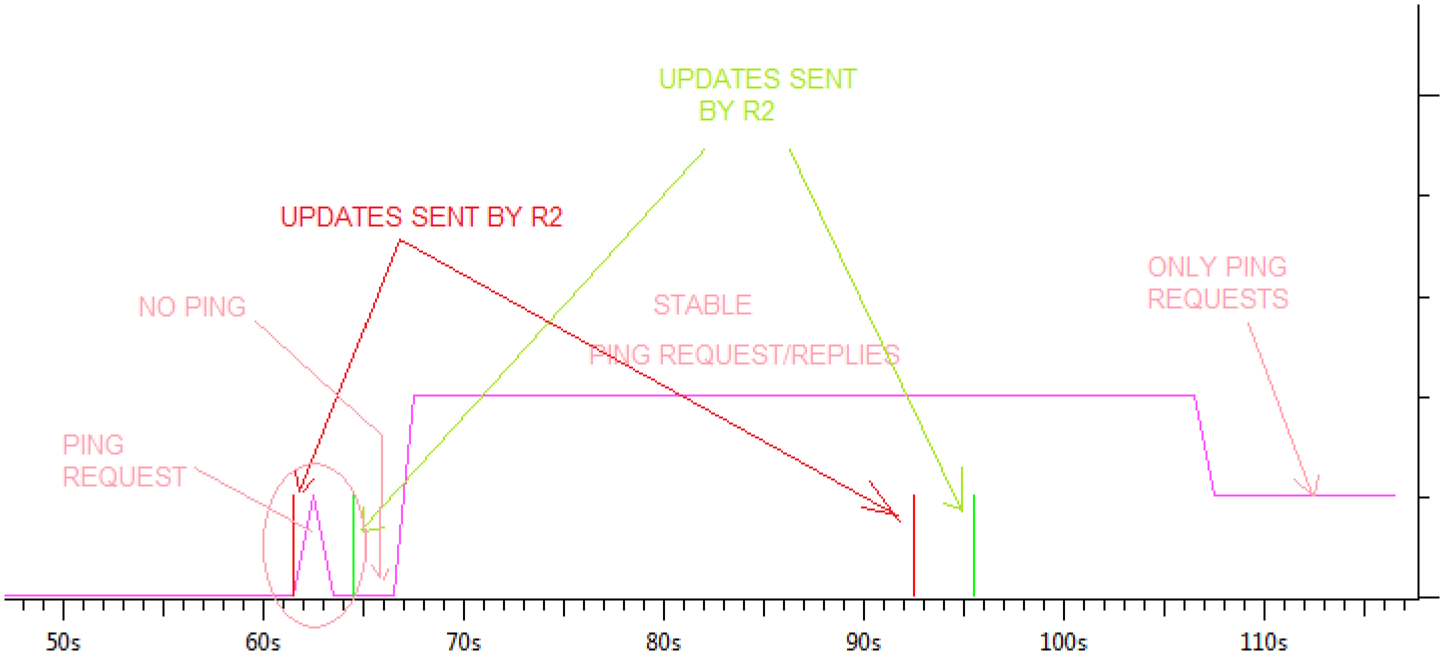
After that upto packet no. 63 pings are getting reply and the the link R3-R1 gets up as shown in packet 64 below

```
Border Gateway Protocol
⊟ UPDATE Message
    Marker: 16 bytes
    Length: 53 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 25 bytes
  ⊟ Path attributes
    ⊞ ORIGIN: IGP (4 bytes)
    ⊞ AS_PATH: 33 (7 bytes)
    ⊞ NEXT_HOP: 192.168.0.198 (7 bytes)
    ⊞ MULTI_EXIT_DISC: 0 (7 bytes)
  ⊟ Network layer reachability information: 5 bytes
    ⊞ 192.168.0.200/30
```

This has been confirmed by R2 in packet 72 as

```
Border Gateway Protocol
⊟ UPDATE Message
    Marker: 16 bytes
    Length: 46 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 18 bytes
  ⊟ Path attributes
    ⊞ ORIGIN: IGP (4 bytes)
    ⊞ AS_PATH: 11 (7 bytes)
    ⊞ NEXT_HOP: 192.168.0.197 (7 bytes)
  ⊟ Network layer reachability information: 5 bytes
    ⊞ 192.168.0.200/30
```

After that packet no. 74to 95 use the already established route and after packet 96 -105 didn't get ant reply indicating the path change .



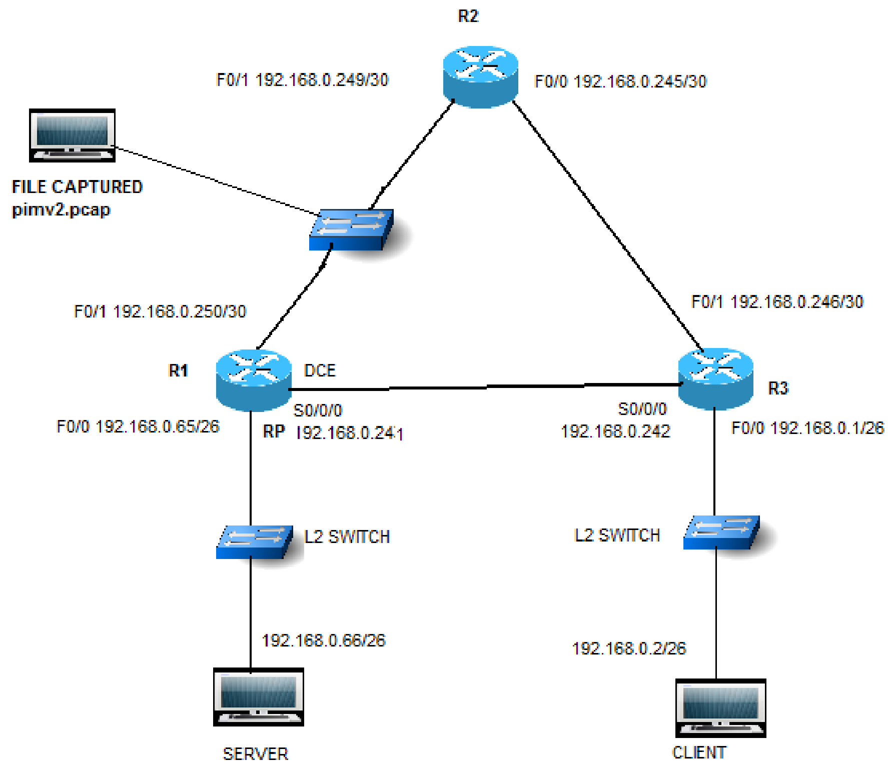

**GRAPHICAL LINK STATE CHANGE ILLUSTRATION**

## PIMv2(Protocol Independent Multicast Version 2)

IP multicasting is the way of sending IP data to a group of hosts. The multicast group address range is Class D 224.0.0.0 to 239.255.255.255 out of which the addresses 239.0.0.0 to 239.255.255.255 are administratively scoped addresses and are used privately. Multicast is different from broadcast in the sense that data is not transmitted to all hosts on network but only to hosts belonging to particular group(s). Clients which are interested in listening to multicast traffic transmit's their queries to join/leave via IGMP to routers and routers communicate between each other using PIM so as to fulfill the request of joining/leaving via PIM. PIM is the widely used multicast routing protocol. PIM version 2 is identified by protocol number 103 and the packets are directly encapsulated in IP with a TTL value of 1. PIM can operate in 3 modes namely Sparse Mode, Dense Mode and Sparse Dense Mode. PIM DM uses flood and prune approach in which first the routers transmit the data on all interfaces and then prune as per response acquired back so it is basically called source based multicast tree whereas in PIM SM the router interface(s) near to the multicast source is either statically selected or dynamically selected and is called Rendezvous Point (RP) and Reverse Path Forwarding is the method adopted for constructing Shortest Path Forwarding Tree based on the core or RP. When configured for Sparse Dense Mode the PIM will use SM when RP is defined otherwise DM is used. So as to prevent multicast routing loops the mechanism used is Reverse Path Forwarding. RPF is just like normal loop avidance mechanism used in unicast routing so as not to forward the packet on the interface on which the message has ben received , it relies on unicast routing table.

All PIM messages contain 32 bit long header and the type specific information as well.

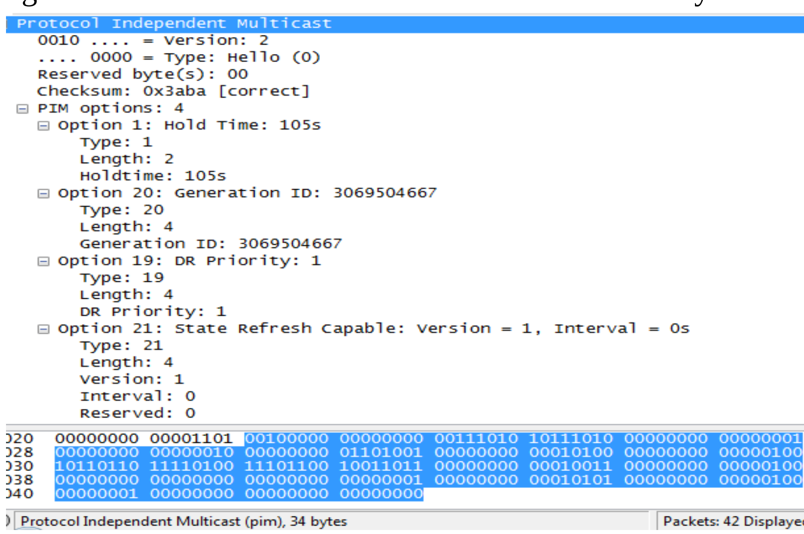
```
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 1
  Protocol: PIM (103)
⊞ Header checksum: 0x142b [correct]
  Source: 192.168.0.249 (192.168.0.249)
  Destination: 224.0.0.13 (224.0.0.13)
Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0000 = Type: Hello (0)
  Reserved byte(s): 00
  Checksum: 0x3aba [correct]
⊞ PIM options: 4
```




NETWORK DIAGRAM FOR PIM ANALYSIS

The file captured is pimv2.pcap. The activity captured is the joining and leaving of client and the moment of chane of path while server is multicasting data stream.
Two types of PIMv2 messages are seen first is Hello Packet which is sent by the router with a time interval of approximately 10 seconds. The PIM encapsulation is in IP and then IP is in Ethernet frame as
`[Protocols in frame: eth:ip:pim]`

The first two messages are the hellos generated between two routers R1 and R2 which only differ by the




checksum value and generation ID. This hello packet contains 34 bytes out of which first 4 bits are version which is 2 and next 4 are the type of PIM message as it is hello Type 0. Next 8 bits are reserved and are always set to zero .After the checksum comes the 4 PIM options. The hold time tells the receiver about the time the established adjacency between them will expire. The generation ID which is a random number generated during PIM forwarding. DR priority is used for SM for the election IGMPv1 querier since the priority is one it indicates the operation of PIM SM underneath. State refresh interval if configured is used by DM routers for refreshing the state with the help of State Refresh Messages so as to conserve the bandwidth by not flooding multicast periodically and then pruning back.

```
Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0x9852 [correct]
⊟ PIM options
    Upstream-neighbor: 192.168.0.250
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210s
  ⊟ Group 0: 239.255.1.1/32
    ⊟ Num Joins: 2
        IP address: 192.168.0.65/32 (SWR)
        IP address: 192.168.0.66/32 (S)
      Num Prunes: 0
```

At 3rd packet the client joins the group indicated by Type 3 message as the router was not having the entry for the host so it send this message to its directly connected neighbor so as to forward it above the tree this packet is shown when it comes to R2 from R1 and is having the Next-Hop towards core router R1. Num Groups parameter tells about the number of multicast groups contained an dthe respective value of hold time. The group ID joined is 239.255.1.1.Then comes the number of joined source which are RP 192.168.0.65 and source 192.168.0.66 and there is no pruning because of only direct link R1R2R3

After that with normal Hello messages there starts coming Join/Pruning messages which are generated by routers so as to transfer the multicast stream where needed. and this indicates that R2 has been elected as DR. These messages keep the adjacency established. At packet 16 the client leaves the group so it is indicated by pruning of source and RP as

```
Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0x9852 [correct]
⊟ PIM options
    Upstream-neighbor: 192.168.0.250
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210s
  ⊟ Group 0: 239.255.1.1/32
      Num Joins: 0
    ⊟ Num Prunes: 2
        IP address: 192.168.0.66/32 (S)
        IP address: 192.168.0.65/32 (SWR)
```

17th packet indicates rejoining of client with the same parameters. After the normal join/prune messges indicating the established connectivity the serial link S0/0/0 was turned on because of use of static routing for unicast data the stream was forced to change the route and it results in pruning via link R2 via the same message as above.

After that normal hellos are transfer between routers continues.

## References:


Wireshark Network Analsis by Laura Chappell
http://www.comm.utoronto.ca/~jorg/teaching/itlab/pdf/Ch10_v1.pdf
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00801e1e2b.shtml
http://www.itechtalk.com/thread219.html
http://standards.ieee.org/develop/regauth/grpmac/public.html
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps6629/prod_presentation0900aecd80310f6d.pdf
http://www.workrobot.com/sysadmin/routing/ospf_facts.html
http://cisco.iphelp.ru/faq/5/ch08lev1sec1.html
EIGRP network design solutions [electronic resource] Pepelnjak, Ivan.
Integrated IS-IS Routing Protocol Concepts By Abe Martey.
Jeff Doyle, TCP/IP routing Volume-1
CCNP Building Scalble Internetworks LabPortfolio By: David Kotfila, Joshua Moorhouse, Ross G. Wolfson
http://pcvr.nl/tcpip/arp_addr.htm
http://sites.google.com/site/amitsciscozone/home/is-is/
http://www.workrobot.com/sysadmin/routing/ospf_facts.html
http://tools.ietf.org/id/draft-ietf-ospf-oob-resync-01.txt
http://www.itechtalk.com/thread219.html
http://www.rhyshaden.com/isis.htm
http://fengnet.com/book/OSPFandISIS/ch09lev1sec2.html
http://www.netcraftsmen.net
http://technet.microsoft.com/en-us/library/default.aspx