Department of Electronics and communication
Engineering

PESIT, Bangalore South Campus

HOSUR ROAD, BANGALORE-560100

IPV4 TO IPV6 MIGRATION AND PERFORMANCE ANALYSIS

USING GNS3 AND WIRESHARK

Subject: COMPUTER COMMUNICATION NETWORKS

Sub Code: UE20EC301

ABSTRACT

The internet is a system of various interconnected networks accessible worldwide. IPv4, a layer 3 protocol enables two or more computers to share the data among them. Previously, all the IPv4 address space was exhausted and now we are going for IPv6. Migration techniques have been proposed in this project, to migrate to the IPv6 network. Manual tunneling transition technique is used to transmit an IPv6 packet through an IPv4 network. These transition techniques have been simulated using Graphical Network Simulator (GNS3). Wireshark has been used to capture a live packet on the wire and to analyze the packet header. We investigate migration techniques performance in terms of success rate and the minimum, average and maximum round – trip time and latency and throughput.

INTRODUCTION

Internet Protocol (IP) is the best-known Layer 3 or Network layer protocol. Presently two versions of IP are assigned by Internet Assigned Number Authority (IANA) . The designers of IPv4 did not envision the explosive growth of its use. 4.3 billion addresses seemed more than enough. The IPv4 protocol is not particularly efficient in its use of the available space, with many addresses being wasted. The internet authorities started to predict address exhaustion in the late 1980s and IPv6 was developed in the 1990s as the long-term solution. There is not a seamless migration from IPv4 to IPv6 due to IPv6 being incompatible with IPv4. The demand for transition techniques will go on until and unless a complete transition from IPv4 to IPv6 is completed. The transition to IPv6 from IPv4 can be divided into 3 phases as follows: Phase I, IPv6 network is an island in an IPv4 ocean, where IPv4 continues to dominate on global networking. Phase II, after a few years, IPv4 will become an island while IPv6 will be an ocean. At this stage, IPv6 is much bigger than IPv4. Phase III, the final phase, in this phase most of the networks are in IPv6 native . IPv6 was delivered with migration techniques to cover every conceivable IPv4 upgrade case, with many being rejected by the networking community. Here we investigate IPv6 transition by Tunnelling process. We will simulate the topologies using GNS3 and then present the simulations result of these transition techniques in terms of success rate and the minimum, average and maximum round – trip time and latency and throughput. These performances considered will affect their scalability and quality of service (QoS). In addition to the larger address space, IPv6 was designed to support built-in security and host mobility. IPv6 uses a 128-bit address compared to IPv4's 32-bit address. IPv6 provides more than 7.9*1028 times as many addresses as IPv4. In addition to the larger address space, IPv6 also needed to overcome the limitations that existed with IPv4, more latency, less address space, and less security.

THEORY

Graphical Network Simulator (GNS3):

GNS3 is a network software emulator used to simulate complex networks by allowing the combination of virtual and real devices. We use GNS3 to make topologies for both Dual-Stack and Tunneling Transition techniques.

Wireshark :

Wireshark is a packet-sniffing open source software used to analyze and troubleshoots a network. We use Wireshark to capture the packet during the tunneling transition and analyze its header .

Routing Protocols:

If a router receives traffic for a network, which is not directly connected to, it needs to know to get there in order to forward the traffic. An administrator can manually add a static route to the destination, or the router can learn it via a routing protocol.

1) Static Routing: In this type of routing, the routing entries remain unchanged. The routes are added manually by entering the desired commands in command line interface (CLI). Routes can be viewed in the routing table using 'show ip route' command in 'privileged exec mode'. Routes configured using static routing need to be manually configured if any change occurs in the network topology.

2) Dynamic Routing: Routing protocols, which allow routers to advertise their best paths to known networks to each other. Routers use this information to find out their own best path to the known destinations. Routing protocols are more scalable than administrator defined static routes. If a subnet is added or removed, the routers will automatically discover that and update their routing tables. If the best path to a subnet goes down routers automatically discover that and will find a new best path if one is available.

3) OSPF: We have used the Open Shortest Path First (OSPF) protocol to design our topologies for dynamic routing. OSPF is an open standard protocol and thereby supported on all vendors equipment. OSPF is a link state routing protocol and is a part of interior gateway routing protocols (IGPs). It has a very fast convergence time and supports large networks. In link-state routing protocols, each router describes itself and its interface to its directly connected neighbors.

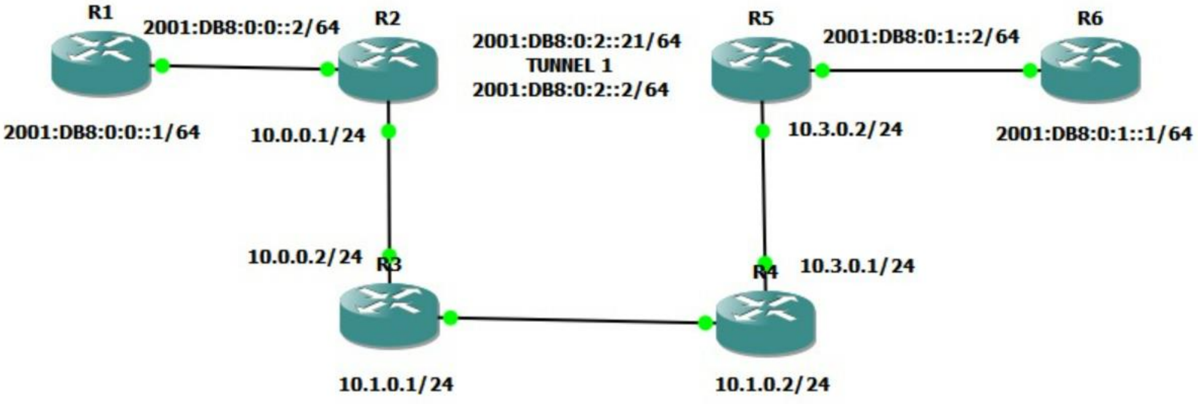
Performance parameters:

1) **Latency:** The delay before a transfer of data begins following instruction for its transfer from the client.
   Latency = (Average Round trip time for Packet / 2) ms
2) **Throughput:** Also referred to as network throughput, it is the rate of successful packet delivery over a communication channel.
   Throughput = (Packet Size / Latency) Mbps

Tunneling Process:

Tunneling transition is used for the secure transmission of data. Tunneling allows private network data packets to be transmitted across a public network through the encapsulation process. Tunneling provides a secure path for data transmission through an open or untrusted network. Here, we have configured manual tunneling. A virtual tunnel is created between two routers and packets are sent through the tunnel. Manual tunneling provides a stable connection between two routers, for providing connections to remote IPv6 networks over the IPv4 network.

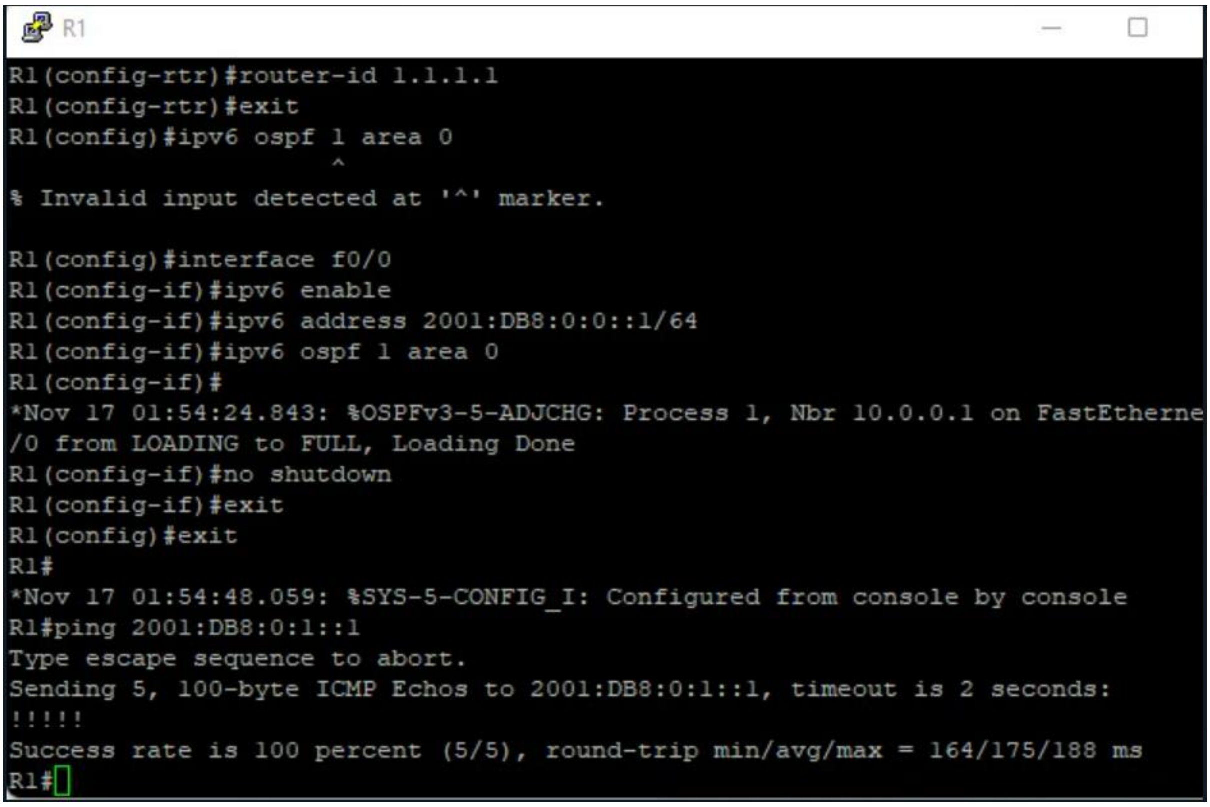
Tunneling Topology:



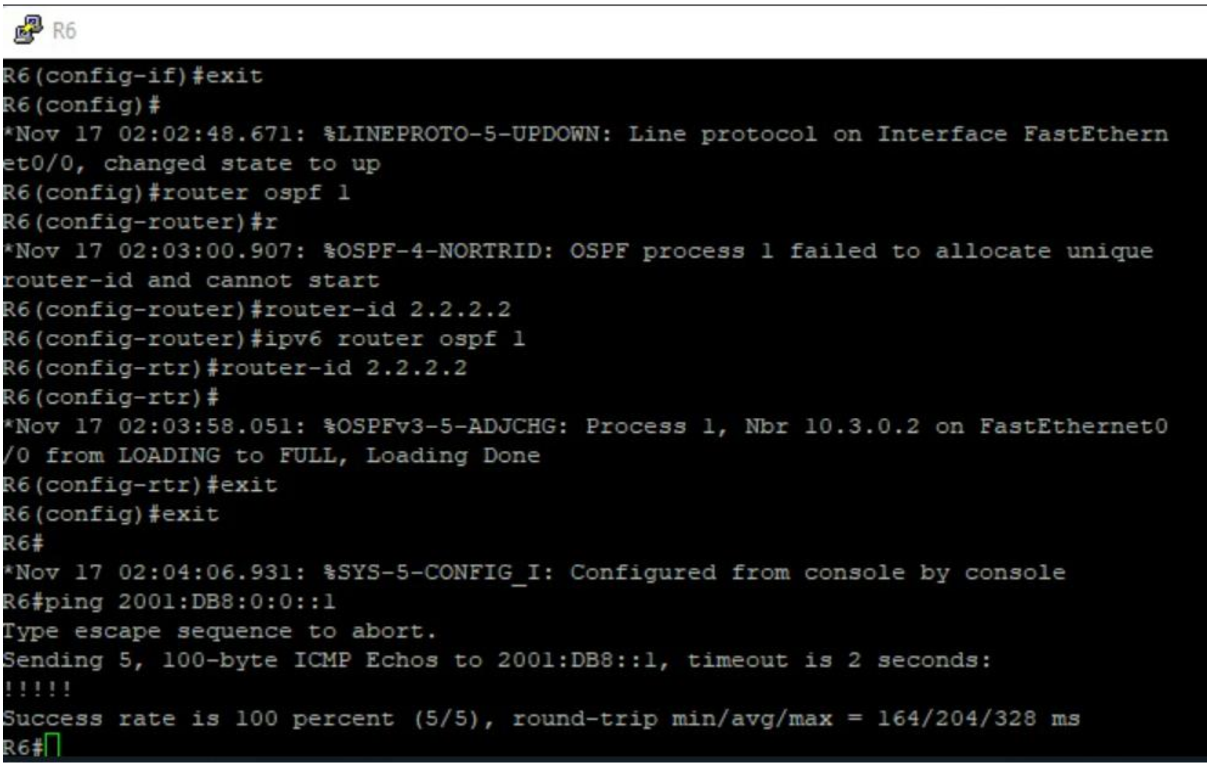
CONFIGURATION :

Designing of tunneling transition technique is done to transfer the data packets from an IPv6 network on router R1 to another IPv6 network on router R6 through Routers R3 and R4 that make up the IPv4 network. The designing of this manual tunneling is done using the OSPF protocol. Routers R2 and R5 are the edge routers having one of their interface connected to an IPv6 network and the other interface to IPv4 network. These routers R2 and R5 are called dual-stack routers. When the data is sent to R1 from R6 (or vice-versa) as it reaches the dual stack router R5, the router attaches an IPv4 header with the IPv6 packet, thereby allowing the packet to tunnel across the IPv4 network and arriving at the other dual stack router R2 where the IPv4 header is removed from the IPv6 packet and the packet is forwarded to the IPv6 network.

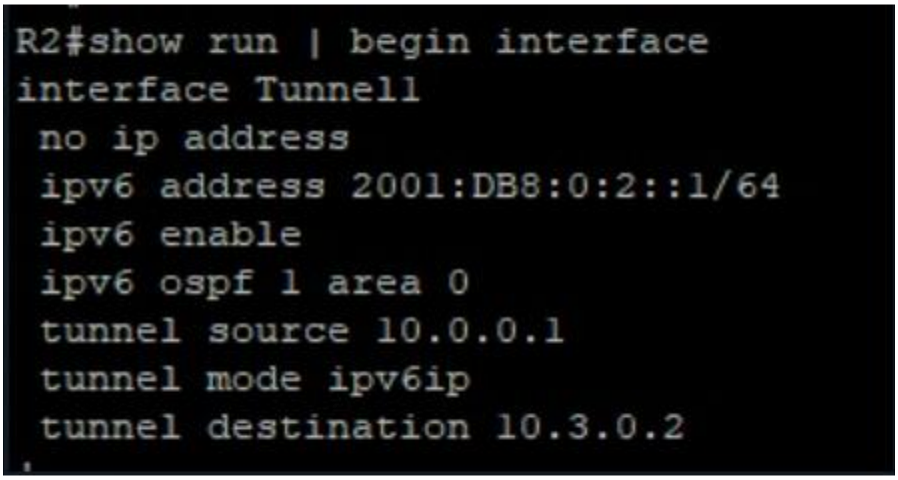
STIMULATION RESULTS:



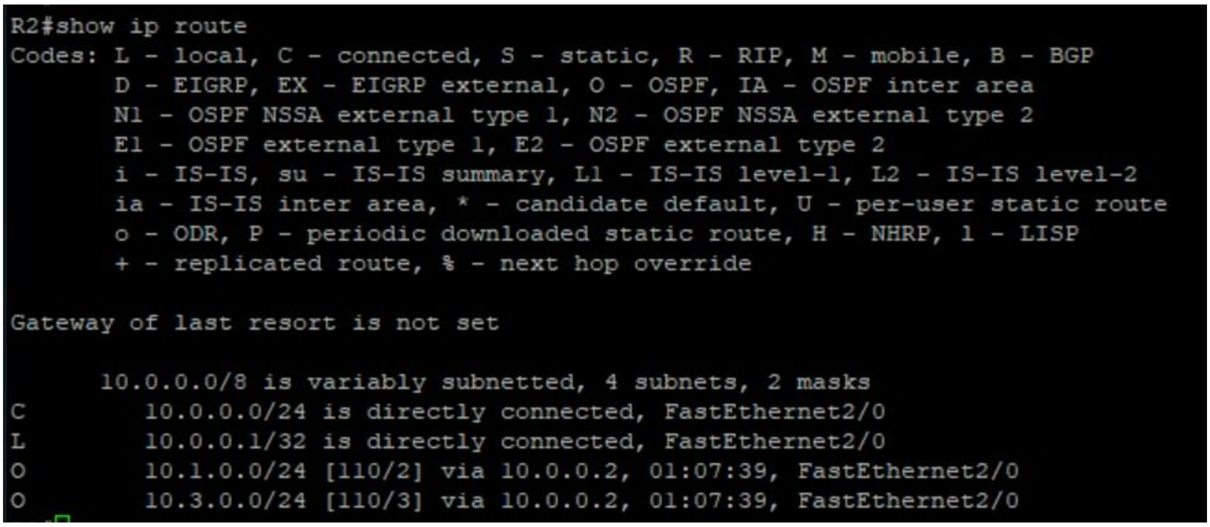
```
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#ipv6 ospf 1 area 0
                     ^
% Invalid input detected at '^' marker.

R1(config)#interface f0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:0:0::1/64
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#
*Nov 17 01:54:24.843: %OSPFv3-5-ADJCHG: Process 1, Nbr 10.0.0.1 on FastEtherne
/0 from LOADING to FULL, Loading Done
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
*Nov 17 01:54:48.059: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 2001:DB8:0:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 164/175/188 ms
R1#
```



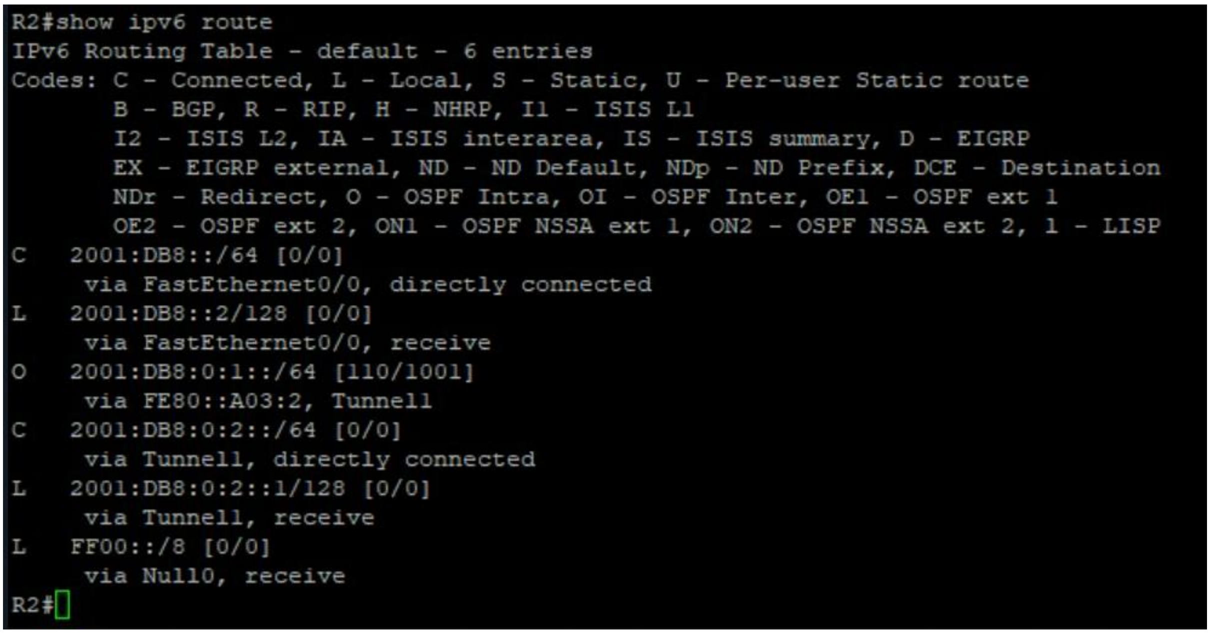
```
R6(config-if)#exit
R6(config)#
*Nov 17 02:02:48.671: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R6(config)#router ospf 1
R6(config-router)#r
*Nov 17 02:03:00.907: %OSPF-4-NORTRID: OSPF process 1 failed to allocate unique
router-id and cannot start
R6(config-router)#router-id 2.2.2.2
R6(config-router)#ipv6 router ospf 1
R6(config-rtr)#router-id 2.2.2.2
R6(config-rtr)#
*Nov 17 02:03:58.051: %OSPFv3-5-ADJCHG: Process 1, Nbr 10.3.0.2 on FastEthernet0
/0 from LOADING to FULL, Loading Done
R6(config-rtr)#exit
R6(config)#exit
R6#
*Nov 17 02:04:06.931: %SYS-5-CONFIG_I: Configured from console by console
R6#ping 2001:DB8:0:0::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 164/204/328 ms
R6#
```



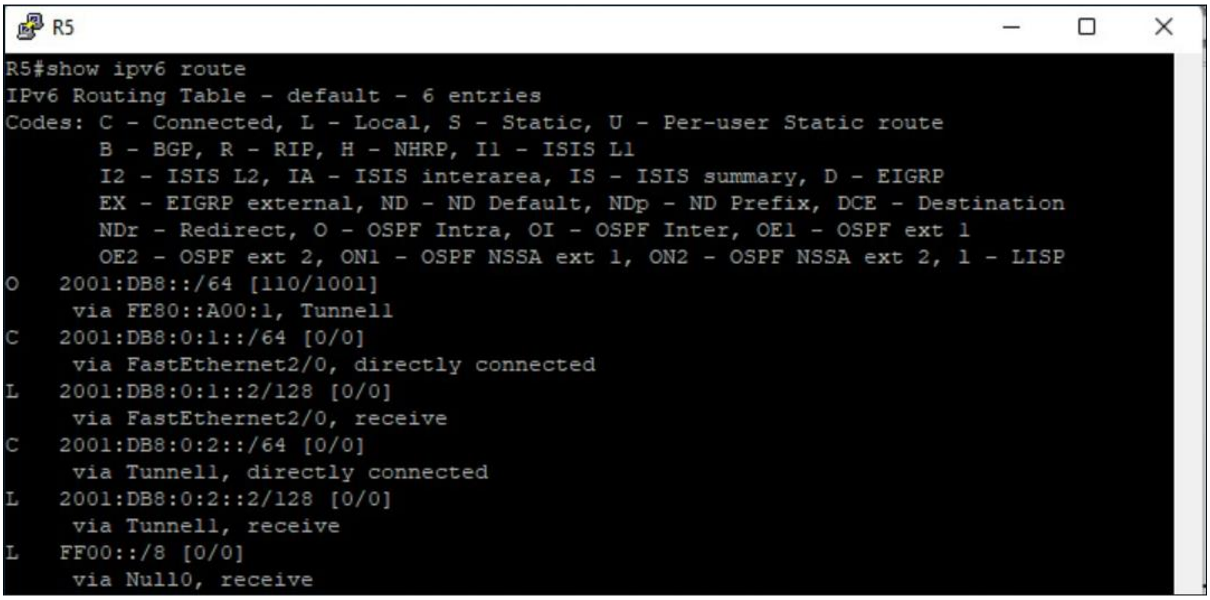
```
R2#show run | begin interface
interface Tunnel1
 no ip address
 ipv6 address 2001:DB8:0:2::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source 10.0.0.1
 tunnel mode ipv6ip
 tunnel destination 10.3.0.2
```



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

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, FastEthernet2/0
L        10.0.0.1/32 is directly connected, FastEthernet2/0
O        10.1.0.0/24 [110/2] via 10.0.0.2, 01:07:39, FastEthernet2/0
O        10.3.0.0/24 [110/3] via 10.0.0.2, 01:07:39, FastEthernet2/0
```

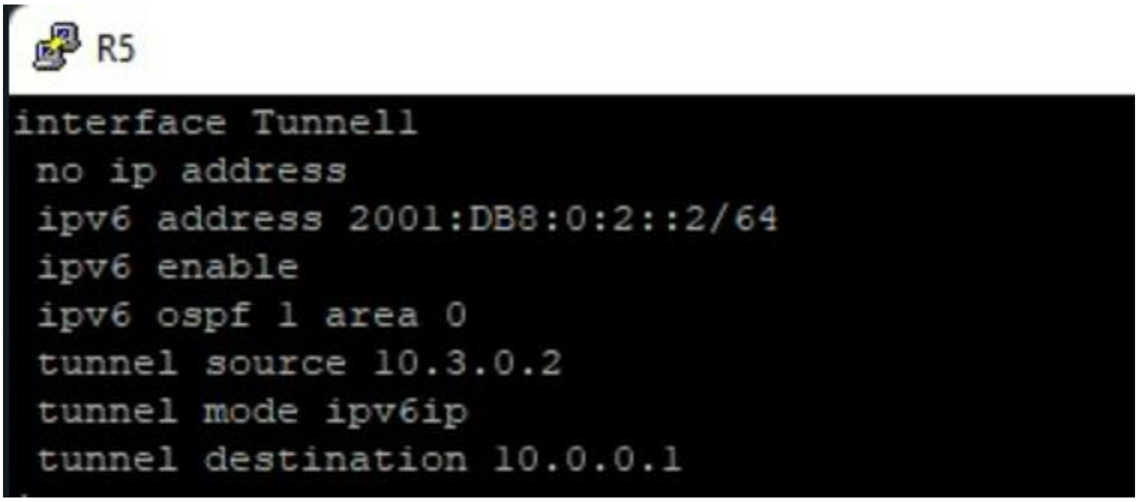


```
R2#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
C   2001:DB8::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:DB8::2/128 [0/0]
     via FastEthernet0/0, receive
O   2001:DB8:0:1::/64 [110/1001]
     via FE80::A03:2, Tunnel1
C   2001:DB8:0:2::/64 [0/0]
     via Tunnel1, directly connected
L   2001:DB8:0:2::1/128 [0/0]
     via Tunnel1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R2#
```

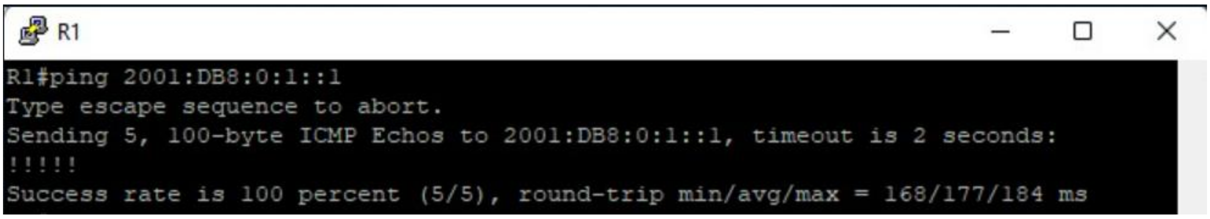


R5

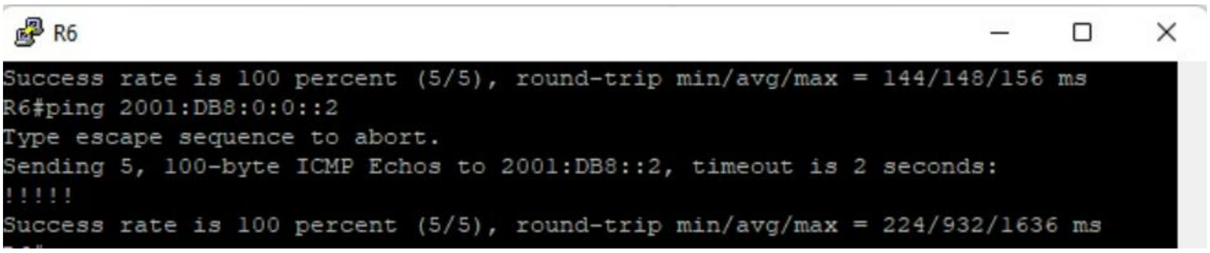
```
R5#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
O   2001:DB8::/64 [110/1001]
     via FE80::A00:1, Tunnel1
C   2001:DB8:0:1::/64 [0/0]
     via FastEthernet2/0, directly connected
L   2001:DB8:0:1::2/128 [0/0]
     via FastEthernet2/0, receive
C   2001:DB8:0:2::/64 [0/0]
     via Tunnel1, directly connected
L   2001:DB8:0:2::2/128 [0/0]
     via Tunnel1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```



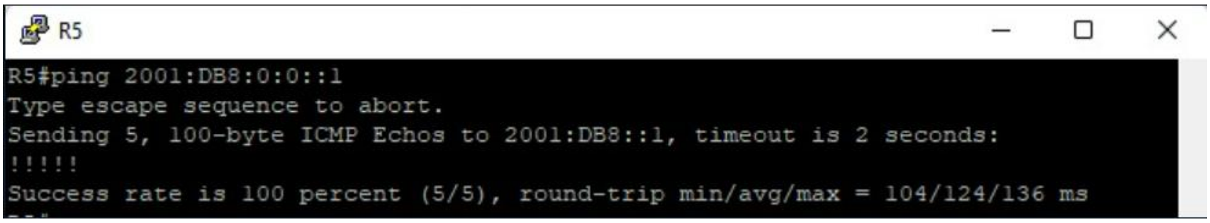
```
interface Tunnel1
 no ip address
 ipv6 address 2001:DB8:0:2::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source 10.3.0.2
 tunnel mode ipv6ip
 tunnel destination 10.0.0.1
```



```
R1#ping 2001:DB8:0:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/177/184 ms
```



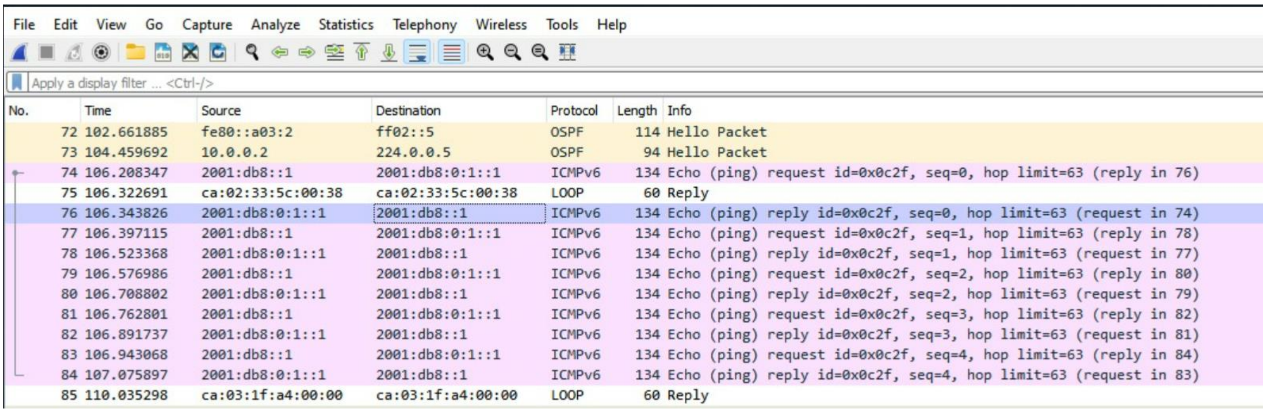
```
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/148/156 ms
R6#ping 2001:DB8:0:0::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 224/932/1636 ms
```



```
R5#ping 2001:DB8:0:0::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/124/136 ms
```

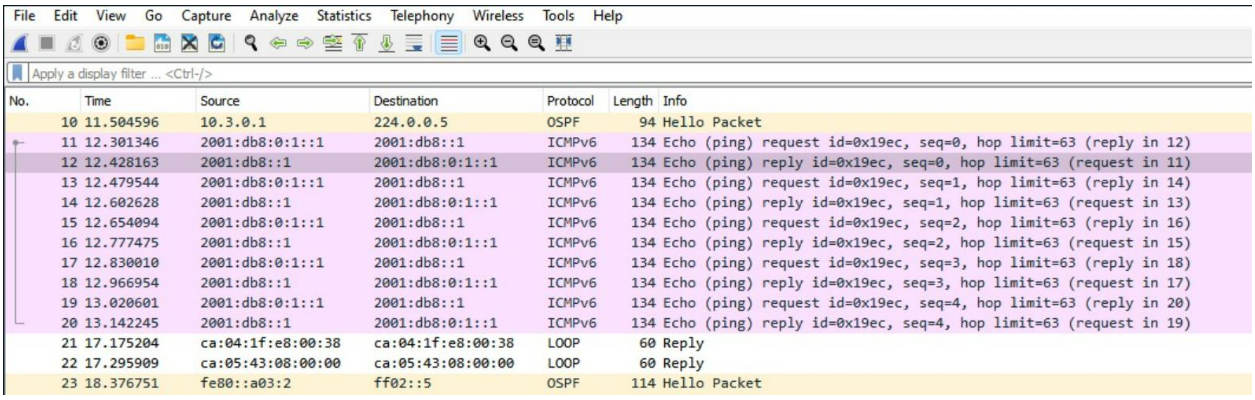
WIRESHARK CAPTURE:

R1 TO R6:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

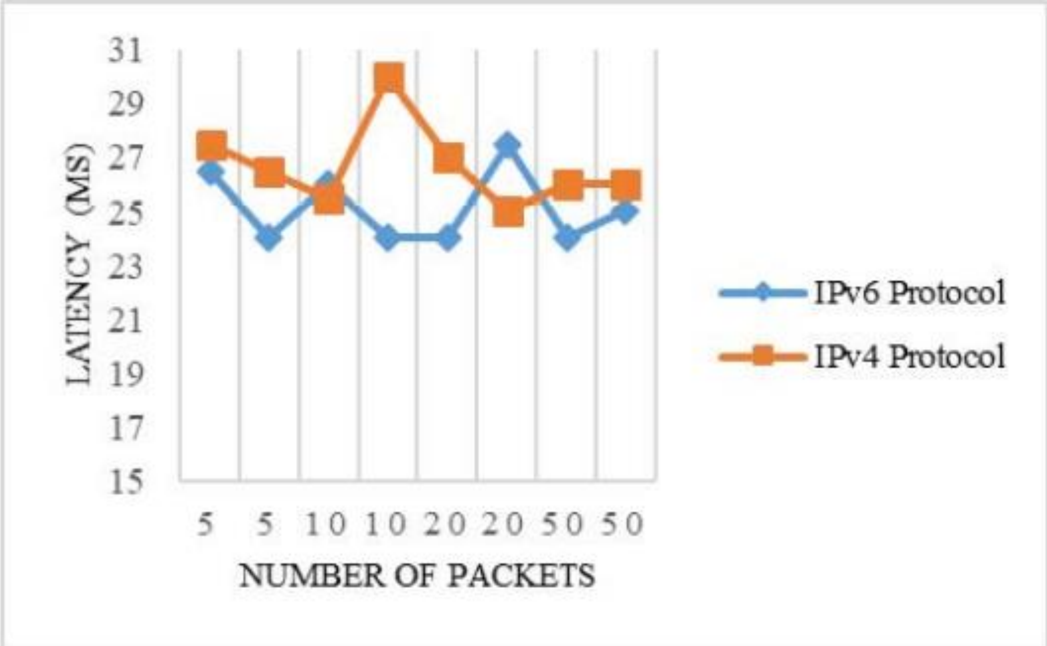
```
No.   Time        Source              Destination         Protocol  Length Info
   72 102.661885  fe80::a03:2         ff02::5             OSPF      114 Hello Packet
   73 104.459692  10.0.0.2            224.0.0.5           OSPF       94 Hello Packet
   74 106.208347  2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) request id=0x0c2f, seq=0, hop limit=63 (reply in 76)
   75 106.322691  ca:02:33:5c:00:38   ca:02:33:5c:00:38   LOOP       60 Reply
   76 106.343826  2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) reply id=0x0c2f, seq=0, hop limit=63 (request in 74)
   77 106.397115  2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) request id=0x0c2f, seq=1, hop limit=63 (reply in 78)
   78 106.523368  2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) reply id=0x0c2f, seq=1, hop limit=63 (request in 77)
   79 106.576986  2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) request id=0x0c2f, seq=2, hop limit=63 (reply in 80)
   80 106.708802  2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) reply id=0x0c2f, seq=2, hop limit=63 (request in 79)
   81 106.762801  2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) request id=0x0c2f, seq=3, hop limit=63 (reply in 82)
   82 106.891737  2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) reply id=0x0c2f, seq=3, hop limit=63 (request in 81)
   83 106.943068  2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) request id=0x0c2f, seq=4, hop limit=63 (reply in 84)
   84 107.075897  2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) reply id=0x0c2f, seq=4, hop limit=63 (request in 83)
   85 110.035298  ca:03:1f:a4:00:00   ca:03:1f:a4:00:00   LOOP       60 Reply
```

R6 TO R1:

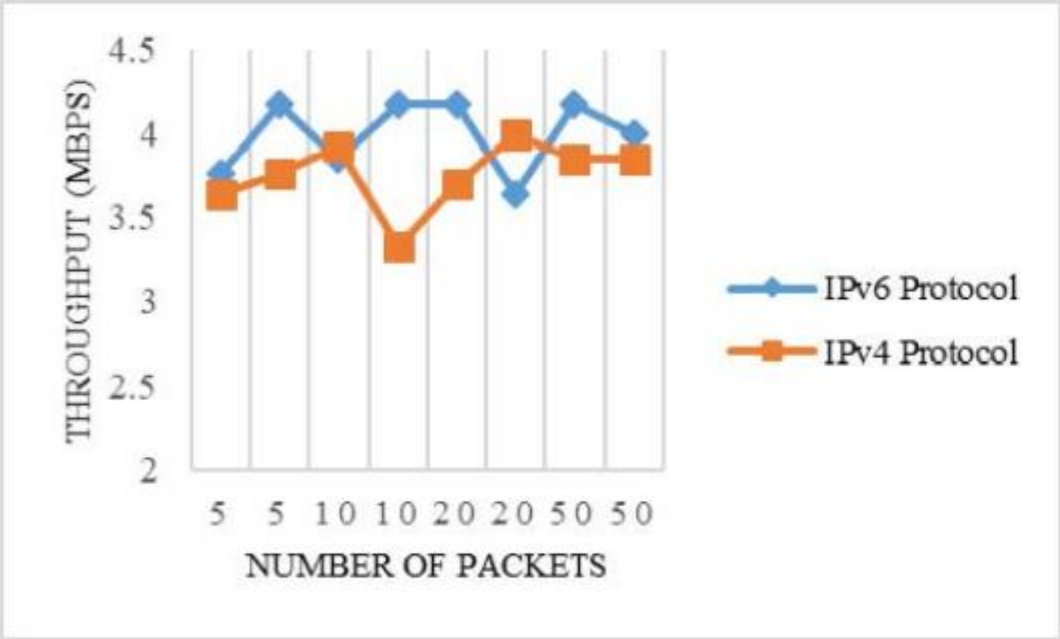

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination         Protocol  Length Info
   10 11.504596   10.3.0.1            224.0.0.5           OSPF       94 Hello Packet
   11 12.301346   2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) request id=0x19ec, seq=0, hop limit=63 (reply in 12)
   12 12.428163   2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) reply id=0x19ec, seq=0, hop limit=63 (request in 11)
   13 12.479544   2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) request id=0x19ec, seq=1, hop limit=63 (reply in 14)
   14 12.602628   2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) reply id=0x19ec, seq=1, hop limit=63 (request in 13)
   15 12.654094   2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) request id=0x19ec, seq=2, hop limit=63 (reply in 16)
   16 12.777475   2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) reply id=0x19ec, seq=2, hop limit=63 (request in 15)
   17 12.830010   2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) request id=0x19ec, seq=3, hop limit=63 (reply in 18)
   18 12.966954   2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) reply id=0x19ec, seq=3, hop limit=63 (request in 17)
   19 13.020601   2001:db8:0:1::1     2001:db8::1         ICMPv6    134 Echo (ping) request id=0x19ec, seq=4, hop limit=63 (reply in 20)
   20 13.142245   2001:db8::1         2001:db8:0:1::1     ICMPv6    134 Echo (ping) reply id=0x19ec, seq=4, hop limit=63 (request in 19)
   21 17.175204   ca:04:1f:e8:00:38   ca:04:1f:e8:00:38   LOOP       60 Reply
   22 17.295909   ca:05:43:08:00:00   ca:05:43:08:00:00   LOOP       60 Reply
   23 18.376751   fe80::a03:2         ff02::5             OSPF      114 Hello Packet
```

LATENCY COMPARISION:



THROUGHPUT COMPARISION:



CONCLUSION

The application of Tunneling transition technique for migration to the IPv6 network from the IPv4 network has been studied. The transfer of a different number of packets across the network has been studied. Round trip time has been analyzed in the transition techniques and by using these value latency and throughput has been calculated. We conclude that IPv6 protocol along with providing much wider address space also provides less latency and better throughput than the IPv4 protocol.