ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Evaluation of IpV4 and IpV6 Tunneling 66 Mechanisms and To Establish A Permanent Virtual Link between Two IpV6 Domains Over an IpV4 Backbone

Mohammad Firoz Alam[1], Ravinder Kumar[2]

Reaserch Scholar, Department of Electronics & Communication Engineering, AFSET, Al-Falah University, Fridabad, Haryana, India[1]

Assistant Professor, Department of Electronics & Communication Engineering, AFSET, Al-Falah University, Fridabad, Haryana, India[2]

ABSTRACT: The use of Internet Protocol (IP) based technologies is now a strategic element in the design, development and use of IP networks. As the use of IP-based networks, including the Internet, the Internet will continue to grow and the numbering system and the routing system will change to accommodate that growth. The most obvious change in going from IPv4 to IPv6 is the increase in the address space from 32 bits in IPv4 to 128 bits in IPv6. Internet Protocol version 6 (IPv6) is the new generation and the basic protocol of the Internet and every devices connected to the Internet must support it. The current version of IPv4 (IP version 4) has several shortcomings and in some cases present a barrier to the further development of the Internet. The coming IPv6 revolution should remove these barriers and provide a feature-rich environment for the future of global networking. To enable the integration of IPv6 into current networks, several transition mechanisms have been proposed by the IETF (Internet Engineering Task Force), namely Dual-stack techniques, Tunneling techniques and Translation techniques. This paper demonstrates and empirically evaluates one transition mechanism, namely IPv6 over IPv4 tunneling. The simulation is carried out using GNS3 to verify the presented approach.

KEYWORDS: Internet Protocol Ver.4 (IPv4), Internet Protocol Ver.6 (IPv6), TCP/IP protocol suite, IETF, ARPANET, NCP, GNS3, Dual Stack mechanism and Tunnel Mechanism.

I. INTRODUCTION

The IPv4 address structure is a 32-bits and It can manage up to 2^{32} is equal to 4.3 billion addresses only, but these much addresses are not sufficient for the whole population of the earth.The next-generation Internet Protocol known as Internet Protocol version 6 (IPv6) has been developed by the Internet Engineering Task Force (IETF) to replace the current Internet Protocol version 4 (IPv4).Transition from IPv4 to IPv6 in an instant is impossible due to huge size of the Internet and large number of IPv4 users. When both IPv4 and IPv6 are available and the users of Internet want to connect without any restrictions, a transition mechanism is required. To enable the integration of IPv6 into an existing IPv4 networks, several transition mechanisms have been proposed by the IETF like, Dual stack, Tunneling and Translation mechanism.When IPv6 or IPv6/IPv4 systems are separated from other similar systems with which they want to communicate to an existing IPv4 networks, IPv6 packets must be tunneled through the IPv4 network. IPv6 packets are tunneled over IPv4 very simply: The IPv6 packet is encapsulated in an IPv4 datagram, or in other words, a complete IPv4 header is added to the IPv6 packet. The presence of the IPv6 packet within the IPv4 datagram is indicated by a protocol value of 41 in the IPv4 header.This feature provides support for manually configured IPv6 over IPv4 tunnels. A manually configured tunnel is equivalent to a permanent virtual link between two IPv6 domains over an IPv4 backbone.

II. ARCHITECTURAL OVERVIEW OF THE TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite is so named for two of its most important protocols namely Transmission Control Protocol (TCP) and Internet Protocol (IP).Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry standard suite of protocols that is designed for large networks consisting of network segments that are connected by routers. The main design goal of TCP/IP was to build an interconnection of networks, referred to as an *Internetwork*, or *Internet*, that provided universal communication services over heterogeneous physical networks.The clear benefit of such an Internetwork is the enabling of communication between hosts on different networks, even separated by a large geographical area. In 1970, ARPANET hosts started to use Network Control Protocol (NCP), a preliminary form of what would become the Transmission Control Protocol (TCP). In 1974, the Transmission Control Protocol (TCP) was specified in detail. TCP replaced NCP and provided enhanced reliable communication services. In 1981, the Internet Protocol (IP) (also known as IP version 4 (IPv4) was specified in detail. IP provides addressing and routing functions for end-to-end delivery. In 1982, the Defense Communications Agency (DCA) and ARPA established the Transmission Control Protocol (TCP) and Internet Protocol (IP) as the TCP/IP protocol suite. In 1983, ARPANET switched from NCP to TCP/IP. In 1984, the Domain Name System (DNS) was introduced. DNS resolves domain names (such as www.google.com) to IP addresses (such as 192.168.5.18). In 1996, the first set of IP version 6 (IPv6) standards were published.TCP/IP is the entire suite of protocols defined for use on private networks and the Internet. TCP/IP includes both the IPv4 and IPv6 sets of protocols. IPv4 has a 20 byte header while IPv6 has a 40 byte header.

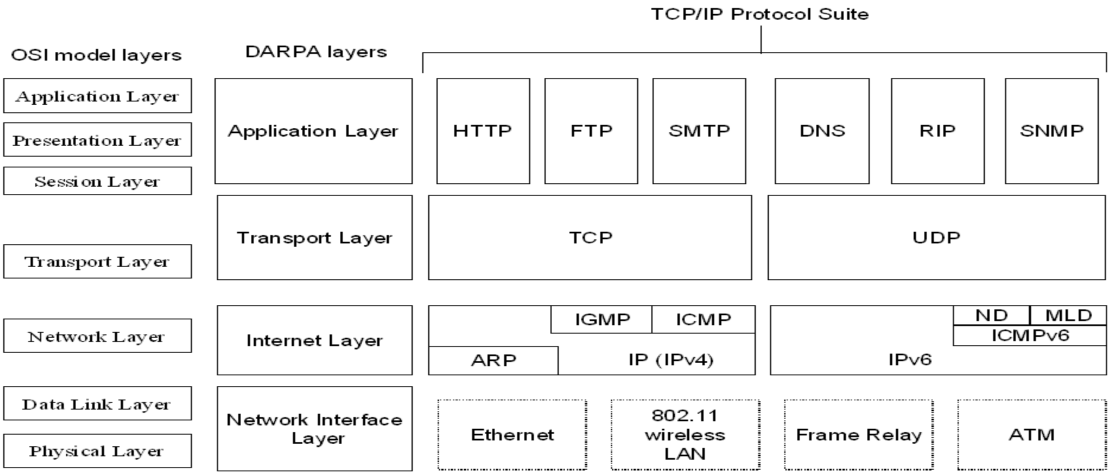


Figure 1 The architecture of the TCP/IP protocol suite

III. TRANSITION AND COEXISTENCE MECHANISMS OF IPv4 / IPv6

The designers of IPv6 recognized that the transition from IPv4 to IPv6 will take years and that there might be organizations or nodes within organizations that will continue to use IPv4 indefinitely. Therefore, although migration is the long-term goal, equal consideration must be given to the interim coexistence of IPv4 and IPv6 nodes.

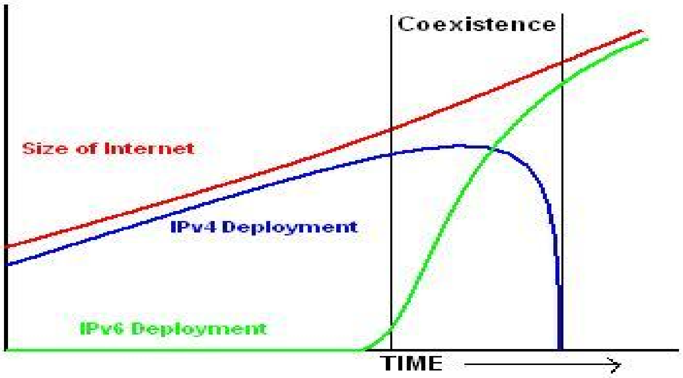


Figure 2 IPv4 and IPv6 Transition and coexistence mechanism

To coexist with an IPv4 infrastructure and to provide an eventual transition to an IPv6-only infrastructure, the following mechanisms are used:

- Dual stack (Using both IPv4 and IPv6 or dual IP layer architectures)
- Tunneling (IPv6 over IPv4 tunneling) techniques
- Translation (IPv6 and IPv4 traffic translation)

IV. TUNNELING MECHANISMS

Tunneling mechanisms can be used to deploy an IPv6 forwarding infrastructure while the overall IPv4 infrastructure is still the basis and either should not or cannot be modified or upgraded. Tunneling is also called *encapsulation*. With encapsulation, one protocol (in our case, IPv6) is encapsulated in the header of another protocol (in our case, IPv4) and forwarded over the infrastructure of the second protocol (IPv4). The process of encapsulation has three components:

- Encapsulation at the tunnel entry point
- Decapsulation at the tunnel exit point
- Tunnel management

So tunneling can be used to carry IPv6 traffic by encapsulating it in IPv4 header and tunneling it over the IPv4 routing infrastructure. In the IPv4 header, the Protocol field is set to 41.General tunneling techniques and the encapsulation of IPv6 packets in IPv4 packets are defined in several RFCs, such as RFC 2473.

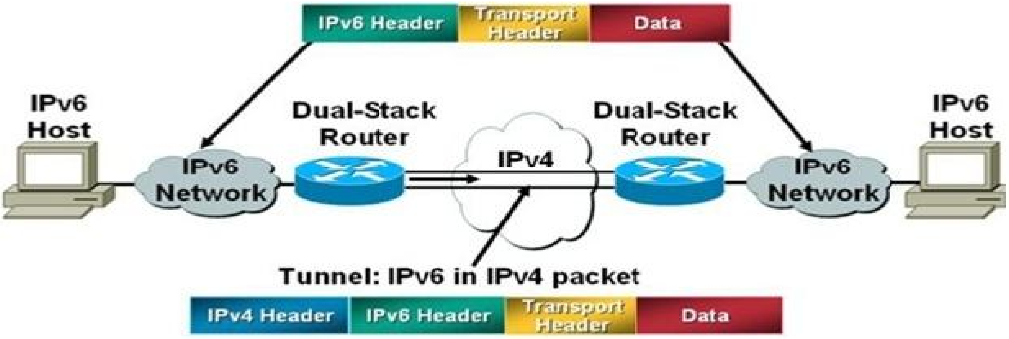


Figure 3 Encapsulation of IPv6 packets in IPv4 header

V. IPv6 OVER IPv4 TUNNELING

IPv6 over IPv4 tunneling is the encapsulation of IPv6 packets with an IPv4 header so that IPv6 packets can be sent over an IPv4 infrastructure. The Source and Destination fields are set to IPv4 addresses of the tunnel endpoints. The tunnel endpoints are either manually configured or are automatically derived from the sending tunnel interface and the next-hop address of the matching route for the destination IPv6 address in the tunneled packet.

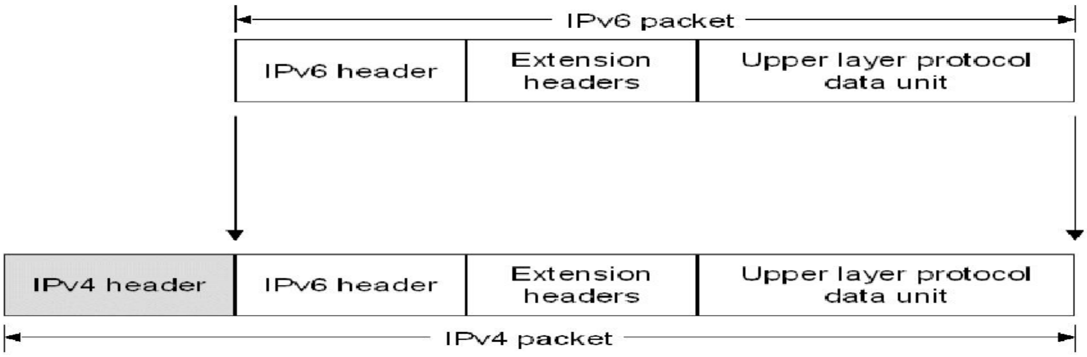


Figure 4 IPv6 over IPv4 tunneling

RFC 2893 defines the following tunneling configurations with which to tunnel IPv6 traffic between IPv6/IPv4 nodes over an IPv4 infrastructure:

•Router-To-Router

In the router-to-router tunneling configuration, two IPv6/IPv4 routers connect two IPv6-capable infrastructures over an IPv4 infrastructure. The tunnel endpoints span a logical link in the path between the source and destination. The IPv6 over IPv4 tunnel between the two routers acts as a single hop. Routes within each IPv6-capable infrastructure point to the IPv6/IPv4 router on the edge.

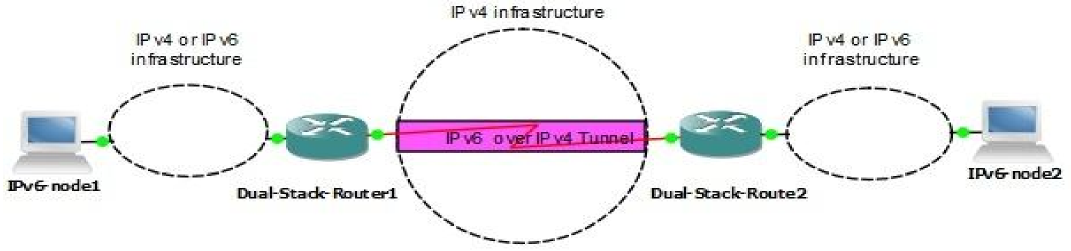


Figure 5 Router-to-Router tunneling

•Host To Router or Router To Host

In the host-to-router tunneling configuration, an IPv6/IPv4 node that resides within an IPv4 infrastructure creates an IPv6 over IPv4 tunnel to reach an IPv6/IPv4 router. The tunnel endpoints span the first segment of the path between the source and destination nodes. The IPv6 over IPv4 tunnel between the IPv6/IPv4 node and the IPv6/IPv4 router acts as a single hop. In the router-to-host tunneling configuration, an IPv6/IPv4 router creates an IPv6 over IPv4 tunnel across an IPv4 infrastructure to reach an IPv6/IPv4 node. The tunnel endpoints span the last segment of the path between the source node and destination node. The IPv6 over IPv4 tunnel between the IPv6/IPv4 router and the IPv6/IPv4 node acts as a single hop.

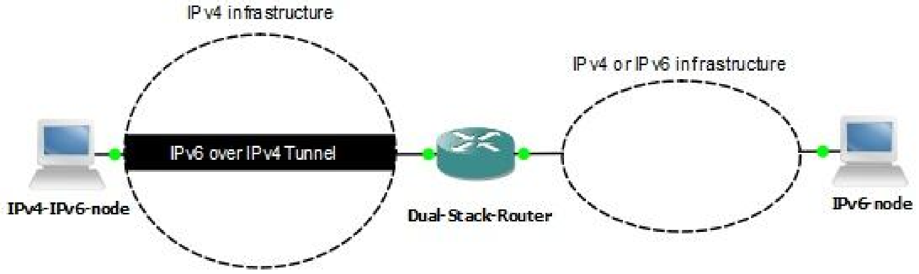


Figure 6 Host-to-Router or Router-to-Host tunneling

•Host To Host

In the host-to-host tunneling configuration, an IPv6/IPv4 node that resides within an IPv4 infrastructure creates an IPv6 over IPv4 tunnel to reach another IPv6/IPv4 node that resides within the same IPv4 infrastructure. The tunnel endpoints span the entire path between the source and destination nodes. The IPv6 over IPv4 tunnel between the IPv6/IPv4 nodes acts as a single hop. On each IPv6/IPv4 node, an interface representing the IPv6 over IPv4 tunnel is created. IPv6 routes are added that use the tunnel interface. Based on the sending tunnel interface, the route, and the destination address, the sending node tunnels the IP v6 traffic to the next hop or to the destination. The IPv4 address of the tunnel endpoint can be manually configured or automatically determined from the next-hop address for the destination and the tunnel interface.

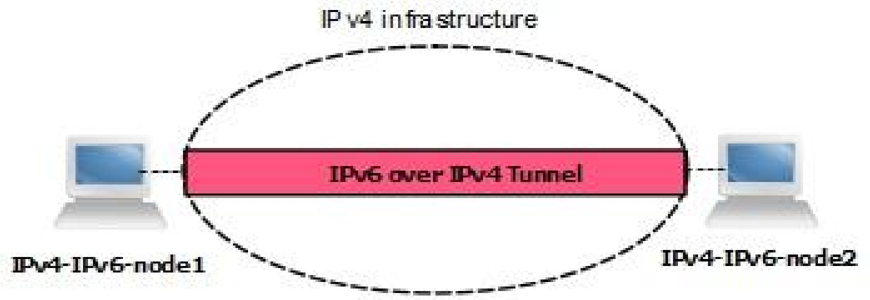


Figure 7 Host to host tunneling

VI. TYPES OF TUNNELS

RFC 2893 defines the following types of tunnels:

•Manually configured tunneling of IPv6 over IPv4

IPv6 packets are encapsulated in IPv4 packets to be carried over IPv4 routing infrastructures. These are point-to-point tunnels that need to be configured manually.

•Automatic tunneling of IPv6 over IPv4

An automatic tunnel is a tunnel that does not require manual configuration. Tunnel endpoints are determined by the use of logical tunnel interfaces, routes, and destination IPv6 addresses. IPv6 nodes can use different types of addresses, such as 6to4, 6rd, or ISATAP addresses, to dynamically tunnel IPv6 packets over an IPv4 routing infrastructure. These special IPv6 unicast addresses carry an IPv4 address in some parts of the IPv6 address fields, which can be used to determine the IPv4 address of the destination or the tunnel endpoint, respectively.

VII. DEVICES USED AND EXPERIMENTAL PROCEDURES

In this experiment we evaluate one transition mechanism namely “Tunneling mechanism” using GNS3. It was configured a set up of hardware and software to achieve the desired results.The hardware include two Cisco routers of C3600 series with running Cisco IOS Software, RJ-45 connectors, UTP straight cables (cat5/cat6/cat6e), two Ethernet switches and two end-workstations C1 and C2 running windows 7 in two different sites. The entire testing process was carried out within the GNS3 Emulation Environment using a virtual topology. We explore the impact of this approach on end to end user application using "ping or tracert" command.The prime benefit of tunneling in the scenario is helping to understand the encapsulation of IPv6 packet in IPv4 header.The prime aim of this approach is to forward IPv6 packets of IPv6 network through IPv4 networks also. Configured tunneling is IPv6-over-IPv4 tunneling where the IPv4 tunnel endpoint addresses are determined by configuration information on the tunnel endpoints. All tunnels are assumed to be bidirectional. The tunnel provides a virtual point-to-point link to the IPv6 layer using the configured IPv4 addresses as the lower layer endpoint addresses. The administrative work to manage configured tunnels is higher than with automatic tunnels, but for security reasons it may be desirable, as it provides more possibilities to control the forwarding path of IPv6 packets.Typically, router-to-router tunneling configurations are manually configured.

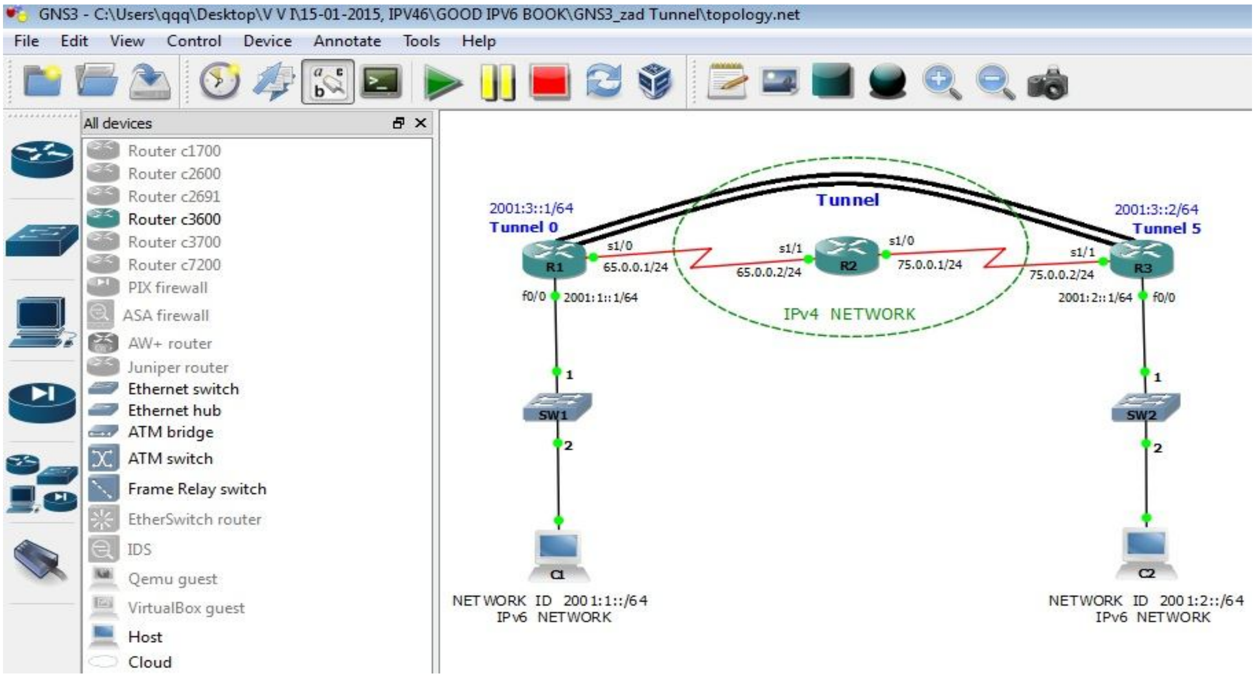


Figure 8 Network with Tunnel over IPv4 infrastructure

VIII. ASSIGNING IP ADDRESSES AND PORTS TO THE NETWORKING DEVICES

Router	Interface	IP address	Tunnel Interface	IP address
R1	f0/0	2001:1::1/64	Tunnel 0	2001:3::1/64
	s1/0	65.0.0.1/24		
R2	s1/1	65.0.0.2/24	Tunnel 5	2001:3::2/64
	s1/0	75.0.0.1/24		
R3	s1/1	75.0.0.2/24		
	f0/0	2001:2::1/64		

Workstation (VPC)	Local port	Remote port	IP address
C1	30000	20000	IPv6 – 2001:1::2/64
C2	30001	20001	IPv6 – 2001:2::2/64

8.1 Configuration of Router R1, Cisco IOS commands are:

```
R1#configure terminal
R1(config)# interface fastethernet 0/0
R1(config-if)# ipv6 address 2001:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 1/0
R1(config-if)#ip address 65.0.0.1  255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#encapsulation hdlc
R1(config-if)#clockrate 64000
R1(config-if)#exit
R1(config)#
```

8.2 Configuration of Router R2, Cisco IOS commands are:

```
R2#configure terminal
R2(config)#interface serial 1/1
R2(config-if)#ip address 65.0.0.2  255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#encapsulation hdlc
R2(config-if)#clockrate 64000
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ip address 75.0.0.1  255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#encapsulation hdlc
R2(config-if)#clockrate 64000
R2(config-if)#exit
```

8.3 Configuration of Router R3, Cisco IOS commands are:

```
R3#configure terminal
R3(config)# interface fastethernet 0/0
R3(config-if)# ipv6 address 2001:2::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface serial 1/1
R3(config-if)#ip address 75.0.0.2  255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#encapsulation hdlc
R3(config-if)#clockrate 64000
R3(config-if)#exit
R3(config)#
```

8.4 Tunnel 0 end configuration, Cisco IOS commands are:

```
R2#configure terminal
R2(config)#no ip routing
R2(config)# ip routing
R1#configure terminal
R1(config)#no ip routing
R1(config)# ip routing
R1(config)#no ipv6 unicast-routing
R1(config)# ipv6 unicast-routing
```

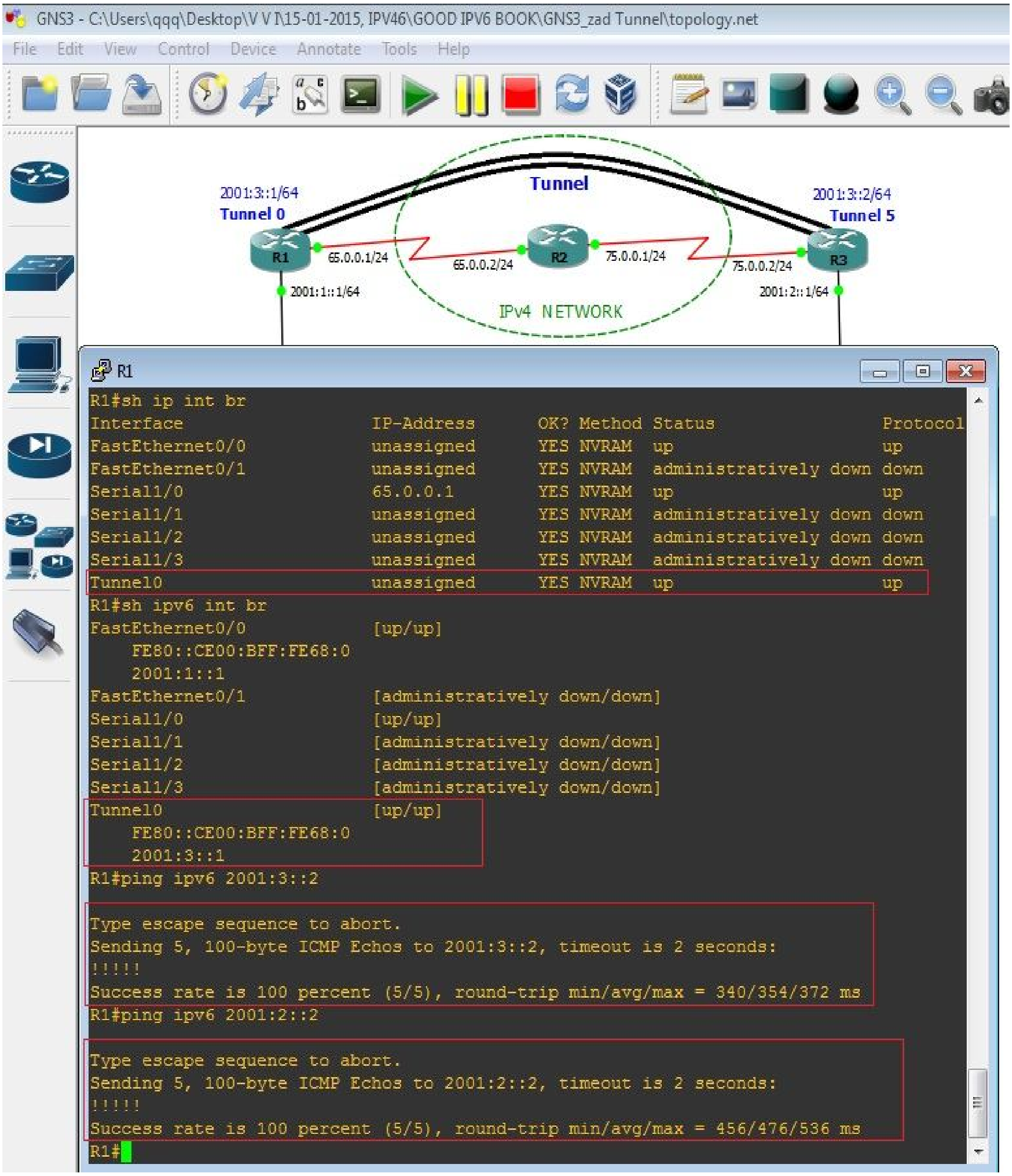
```
R1(config)# int tunnel 0
R1(config)#ipv6 address 2001:3::1/64
R1(config)#no shutdown
R1(config)#tunnel source s1/0
R1(config)#tunnel destination 75.0.0.2
R1(config)#tunnel  mode  ipv6ip
R1(config)#ip route 0.0.0.0  0.0.0.0 s1/0
R1(config)#ipv6 route 2001:2::/64 tunnel 0
R1(config)#exit
```

8.5 Tunnel 5 end Configuration, Cisco IOS commands are:

```
R3#configure terminal
R3(config)#no ip routing
R3(config)# ip routing
R3(config)#no ipv6 unicast-routing
R3(config)# ipv6 unicast-routing
R3(config)# int tunnel 5
R3(config)#ipv6 address 2001:3::2/64
R3(config)#no shutdown
R3(config)#tunnel source s1/1
R3(config)#tunnel destination 65.0.0.1
R3(config)#tunnel  mode  ipv6ip
R3(config)#ip route 0.0.0.0  0.0.0.0 s1/1
R3(config)#ipv6 route 2001:1::/64 tunnel 5
R3(config)#exit
```

IX. SIMULATION RESULTS

The result of the configured tunnel is given below.The communication among all the devices within the network through the virtual link (Tunnel) will take place only if the status of the configured tunnel is up. Now the communication between IPv6 domains over an IPv4 infrastructure will exist through the permanent virtual link (Tunnel). The communication between Router to Router, Router to the end Workstation and end to end Workstation of different sites through the tunnel is checked , verified and the output is given below.

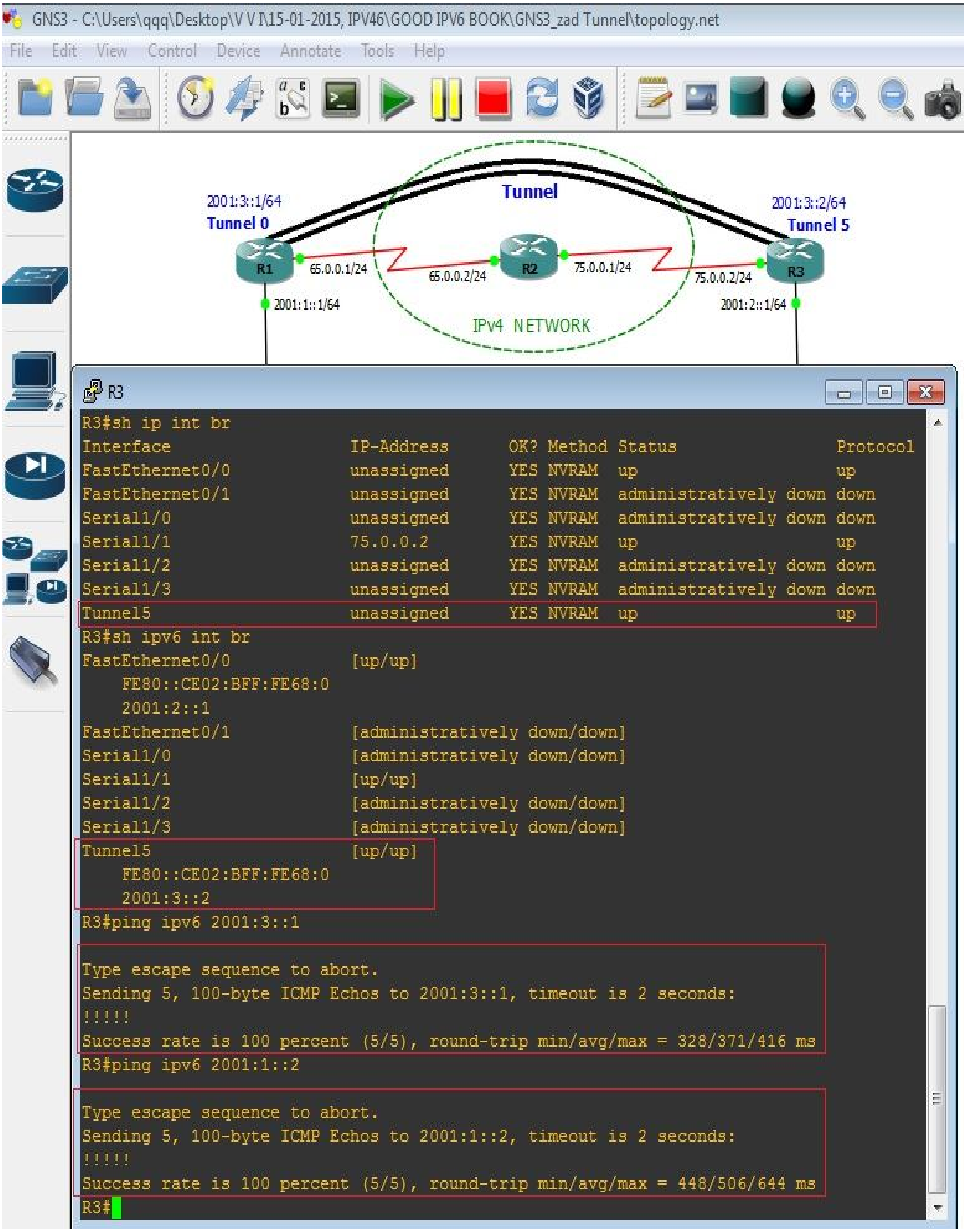

GNS3 - C:\Users\qqq\Desktop\V V I\15-01-2015, IPV46\GOOD IPV6 BOOK\GNS3_zad Tunnel\topology.net
File Edit View Control Device Annotate Tools Help
2001:3::1/64
Tunnel 0
Tunnel
2001:3::2/64
Tunnel 5
R1
65.0.0.1/24
65.0.0.2/24
R2
75.0.0.1/24
75.0.0.2/24
R3
2001:1::1/64
2001:2::1/64
IPv4 NETWORK
R1

```
R1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial1/0                  65.0.0.1        YES NVRAM  up                    up
Serial1/1                  unassigned      YES NVRAM  administratively down down
Serial1/2                  unassigned      YES NVRAM  administratively down down
Serial1/3                  unassigned      YES NVRAM  administratively down down
Tunnel0                    unassigned      YES NVRAM  up                    up
R1#sh ipv6 int br
FastEthernet0/0            [up/up]
    FE80::CE00:BFF:FE68:0
    2001:1::1
FastEthernet0/1            [administratively down/down]
Serial1/0                  [up/up]
Serial1/1                  [administratively down/down]
Serial1/2                  [administratively down/down]
Serial1/3                  [administratively down/down]
Tunnel0                    [up/up]
    FE80::CE00:BFF:FE68:0
    2001:3::1
R1#ping ipv6 2001:3::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 340/354/372 ms
R1#ping ipv6 2001:2::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 456/476/536 ms
R1#
```

Figure 9 Communication between Router R1 to Router R3 to end Workstation



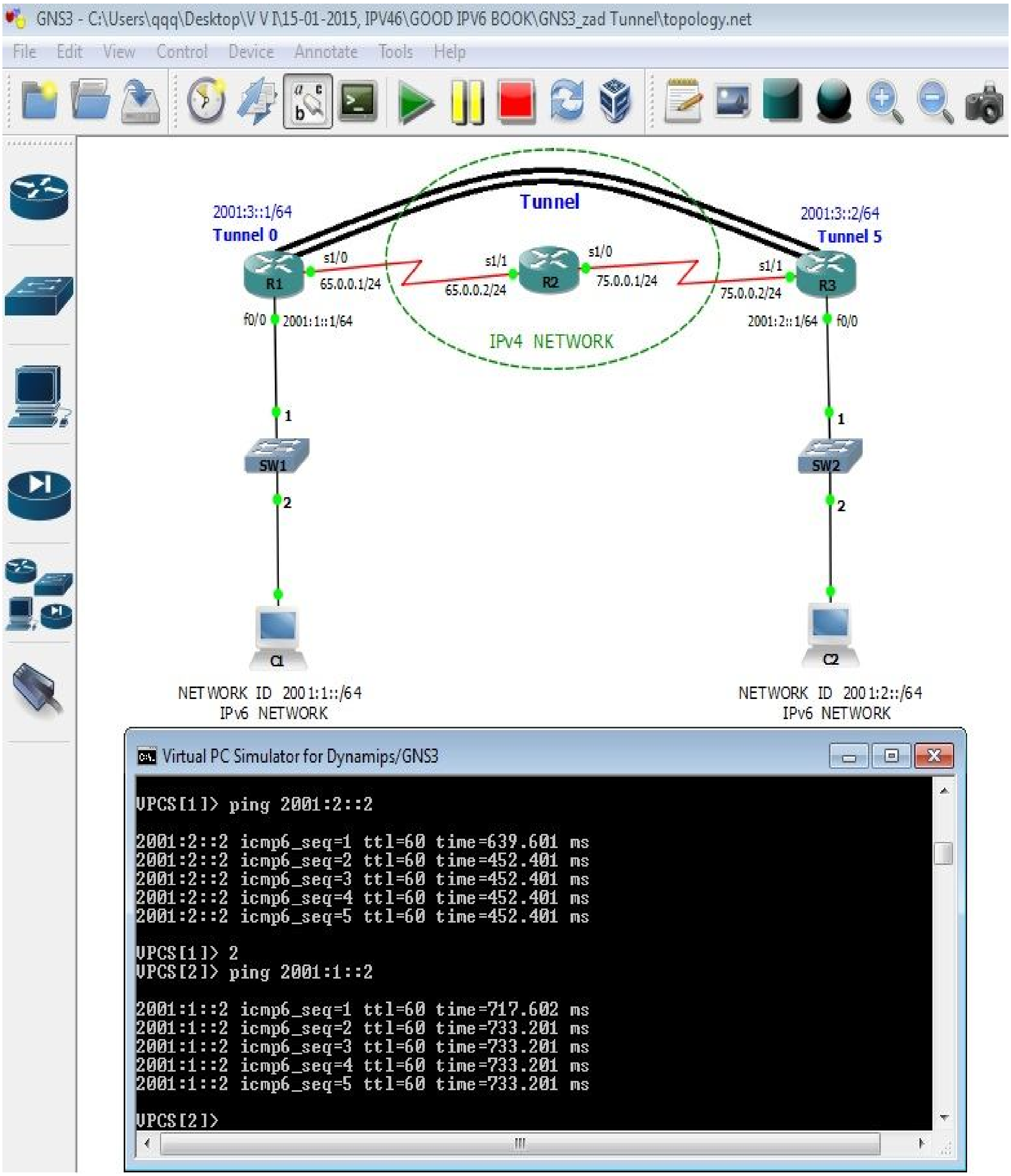
```
R3#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial1/0                  unassigned      YES NVRAM  administratively down down
Serial1/1                  75.0.0.2        YES NVRAM  up                    up
Serial1/2                  unassigned      YES NVRAM  administratively down down
Serial1/3                  unassigned      YES NVRAM  administratively down down
Tunnel5                    unassigned      YES NVRAM  up                    up
R3#sh ipv6 int br
FastEthernet0/0            [up/up]
    FE80::CE02:BFF:FE68:0
    2001:2::1
FastEthernet0/1            [administratively down/down]
Serial1/0                  [administratively down/down]
Serial1/1                  [up/up]
Serial1/2                  [administratively down/down]
Serial1/3                  [administratively down/down]
Tunnel5                    [up/up]
    FE80::CE02:BFF:FE68:0
    2001:3::2
R3#ping ipv6 2001:3::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:3::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 328/371/416 ms
R3#ping ipv6 2001:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 448/506/644 ms
R3#
```

Figure 10 Communication between Router R3 to Router R1 to end Workstation

DOI: 10.15680/ijircce.2015. 0307066



```
VPCS[1]> ping 2001:2::2

2001:2::2 icmp6_seq=1 ttl=60 time=639.601 ms
2001:2::2 icmp6_seq=2 ttl=60 time=452.401 ms
2001:2::2 icmp6_seq=3 ttl=60 time=452.401 ms
2001:2::2 icmp6_seq=4 ttl=60 time=452.401 ms
2001:2::2 icmp6_seq=5 ttl=60 time=452.401 ms

VPCS[1]> 2
VPCS[2]> ping 2001:1::2

2001:1::2 icmp6_seq=1 ttl=60 time=717.602 ms
2001:1::2 icmp6_seq=2 ttl=60 time=733.201 ms
2001:1::2 icmp6_seq=3 ttl=60 time=733.201 ms
2001:1::2 icmp6_seq=4 ttl=60 time=733.201 ms
2001:1::2 icmp6_seq=5 ttl=60 time=733.201 ms

VPCS[2]>
```

Figure 11 Communication between end Workstations C1 and C2

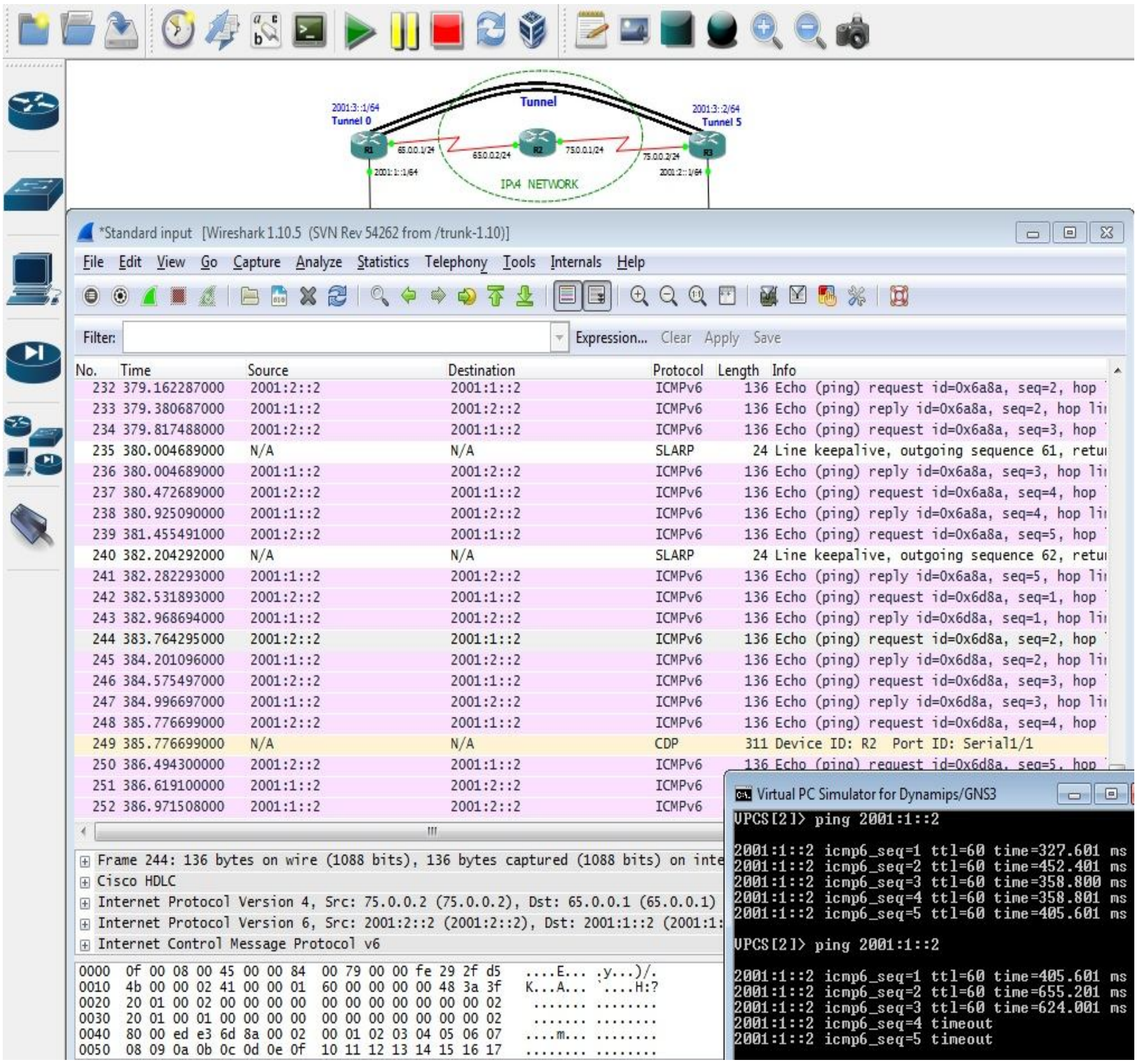
Packets are captured at the serial or ethernet interface of a router.The router accept both IPv4 and IPv6 packets.The result is given below.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015


2001:3::1/64
Tunnel 0
Tunnel
2001:3::2/64
Tunnel 5
R1
65.0.0.1/24
65.0.0.2/24
R2
75.0.0.1/24
75.0.0.2/24
R3
2001:1::1/64
2001:2::1/64
IPv4 NETWORK
*Standard input [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Virtual PC Simulator for Dynamips/GNS3

```
No.  Time           Source       Destination  Protocol  Length  Info
 232 379.162287000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6a8a, seq=2, hop
 233 379.380687000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6a8a, seq=2, hop li
 234 379.817488000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6a8a, seq=3, hop
 235 380.004689000  N/A          N/A          SLARP       24 Line keepalive, outgoing sequence 61, retu
 236 380.004689000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6a8a, seq=3, hop li
 237 380.472689000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6a8a, seq=4, hop
 238 380.925090000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6a8a, seq=4, hop li
 239 381.455491000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6a8a, seq=5, hop
 240 382.204292000  N/A          N/A          SLARP       24 Line keepalive, outgoing sequence 62, retu
 241 382.282293000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6a8a, seq=5, hop li
 242 382.531893000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6d8a, seq=1, hop
 243 382.968694000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6d8a, seq=1, hop li
 244 383.764295000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6d8a, seq=2, hop
 245 384.201096000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6d8a, seq=2, hop li
 246 384.575497000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6d8a, seq=3, hop
 247 384.996697000  2001:1::2    2001:2::2    ICMPv6     136 Echo (ping) reply id=0x6d8a, seq=3, hop li
 248 385.776699000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6d8a, seq=4, hop
 249 385.776699000  N/A          N/A          CDP        311 Device ID: R2  Port ID: Serial1/1
 250 386.494300000  2001:2::2    2001:1::2    ICMPv6     136 Echo (ping) request id=0x6d8a, seq=5, hop
 251 386.619100000  2001:1::2    2001:2::2    ICMPv6
 252 386.971508000  2001:1::2    2001:2::2    ICMPv6
```

```
⊞ Frame 244: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on inte
⊞ Cisco HDLC
⊞ Internet Protocol Version 4, Src: 75.0.0.2 (75.0.0.2), Dst: 65.0.0.1 (65.0.0.1)
⊞ Internet Protocol Version 6, Src: 2001:2::2 (2001:2::2), Dst: 2001:1::2 (2001:1:
⊞ Internet Control Message Protocol v6
```

```
0000  0f 00 08 00 45 00 00 84  00 79 00 00 fe 29 2f d5   ....E... .y...)/.
0010  4b 00 00 02 41 00 00 01  60 00 00 00 00 48 3a 3f   K...A... `....H:?
0020  20 01 00 02 00 00 00 00  00 00 00 00 00 00 00 02    ....... ........
0030  20 01 00 01 00 00 00 00  00 00 00 00 00 00 00 02    ....... ........
0040  80 00 ed e3 6d 8a 00 02  00 01 02 03 04 05 06 07   ....m... ........
0050  08 09 0a 0b 0c 0d 0e 0f  10 11 12 13 14 15 16 17   ........ ........
```

```
VPCS[2]> ping 2001:1::2

2001:1::2 icmp6_seq=1 ttl=60 time=327.601 ms
2001:1::2 icmp6_seq=2 ttl=60 time=452.401 ms
2001:1::2 icmp6_seq=3 ttl=60 time=358.800 ms
2001:1::2 icmp6_seq=4 ttl=60 time=358.801 ms
2001:1::2 icmp6_seq=5 ttl=60 time=405.601 ms

VPCS[2]> ping 2001:1::2

2001:1::2 icmp6_seq=1 ttl=60 time=405.601 ms
2001:1::2 icmp6_seq=2 ttl=60 time=655.201 ms
2001:1::2 icmp6_seq=3 ttl=60 time=624.001 ms
2001:1::2 icmp6_seq=4 timeout
2001:1::2 icmp6_seq=5 timeout
```

Figure 12 Packet capturing at Router interface

X. CONCLUSION

Configured tunnels are best employed when providing external IPv6 connectivity to a whole network. This approach permits the IPv6 traffic to be encapsulated in an IPv4 packet and forwarded, creating an IPv6 tunnel over the IPv4 infrastructure. A tunnel may be created as a solution for transporting IPv6 traffic from source IPv6 node to the destination IPv6 node over the IPv4 network only. A "virtual link" is created in between the two established IPv6 nodes that acts as a point-to-point link. IPv6 over IPv4 tunneling only describes an encapsulation of IPv6 packets with an IPv4 header so that IPv6 nodes are reachable across an IPv4 infrastructure. Network devices are required two processes of encapsulation and de-capsulation at tunnel endpoints. As a result, these two steps always increase requirements for processing and packet delay. This approach is used to transfer data between compatible networking nodes over incompatible networks and IPv6 over IPv4 tunneling does not provide security for tunneled IPv6 packets. Up to date, there exist different Tunneling methods such as 6to4, ISATAP, Teredo, DSTM, and 6over4.

REFERENCES

1. Martin Dunmore,(An IPv6 Deployment Guide), The 6NET Consortium, September 2005.
2. Understanding IPv6 by Joseph Devies, Microsoft 3rd Edition.
3. Cisco.com IPv6 information at http://www.cisco.com/ipv6
4. Cisco Certified Network Associated by Richard Deal,Tata Mcgraw-Hill Edition, 2010
5. ICND2 Official Exam Certification Guide by Wendell Odom. 2E, Cisco Press
6 .IPv6 Essentials, Third Edition by Silvia Hagen
7. Cisco, Introduction to IPv6 by Villayat Muhammad, Service Provider Solution Architect
8. Prepare today for tomorrow's IPv6 world sustaining business continuity in a dual-protocol environment, Business white paper.
9. Transmission of IPv6 Packets over IPv4 Domains without Explicit Tunnels" ("6over4"), RFC 2529 at http://www.ietf.org/rfc/rfc2529.txt
10. IPv4 & IPv6 Integration and Transition / **Mohd.Firoz Alam*** , Jai Singh and Ravinder Kumar / VSRD International Journal of Electrical, Electronis & Communication Engineering, Vol. V Issue June 2015 e-ISSN:2231-3346, p-ISSN:2319-2232@ www.vsrdjournals.com
11. Establishing Link between IPv6 Networks Using IPv4 Clouds / Junaid Qayyum, Fayyaz Gul / International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 11 No: 03
12. CCNP ROUTE 642-902 Official Certification Guide by Cisco.
13. TRANSITION FROM IPv4 TO IPv6/ LAHTI UNIVERSITY OF APPLIED SCIENCES / Degree Programme in Business Information Technology/ Thesis, Spring 2012 / Nguyen, Phu Minh Nguyen / Nguyen, Quynh Anh.