A NOVICE APPROACH ON TRANSITION FROM IPV4-IPV6 USING TUNNELING AND PROTOCOLS OF TUNNELING

Harjeet Singh Mehta[1], Dilip Kumar[2], Hemant Singhtth Rawat[3]

[1,2,3] Computer Science and Engineering Department,
Tulas Institute of Engineering and Management College, Dehradun, (India)

ABSTRACT

In this era of Internet evolution, the transition from IPv4 to IPv6 has become inevitable and fairly urgent. Internet Assigned Numbers Authority (IANA) has finally exhausted the IPv4 global address space, which leaves the community no choice but to push forward the IPv6 transition process. IPv4 and IPv6 networks both will exist during the transition period, while they were not compatible in nature with each other. Therefore it became necessary to maintain the availability, as well as to provide the inter-communication ability of IPv4 and IPv6. Years ago, a series of transition techniques were actually proposed. However because of some technical issues they failed to cover the solution space well. IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address. This paper reconsiders the key difficulties in IPv4-IPv6 transition and introduces the principles of tunneling and the tunneling protocol. This paper looks into the characteristics and transition requirements of practical ISP networks, and proposes the usage and deployment strategy of the transition mechanisms in both backbone and edge networks.

Keywords: Virtual Private Network (VPN), Packet buffer, Packet switching, Encapsulation, Sequenced Packet Protocol, frame-relay, interface, Open Shortest Path First (OSPF), Interior Gateway Protocol (IGP).

I. INTRODUCTION

In this we will be focusing more in IPv6. IPv4 is now completely exhausted. A similar issue would be if perhaps you want to connect to IPv6 internet, but your ISP is not ready to give you IPv6 address space. What happens is that we can end up with several sites running IPv6 “islands”, but those islands are connected via an IPv4 infrastructure. There are a few technologies that deal with how to connect IPv6 islands over an IPv4 network, and one of those technologies is IPv6 automatic 6to4 tunnels. We will be looking at that here.

Complete transition from IPv4 to IPv6 s not still there because IPv6 is not backward compatible. This results in a situation where either site is on IPv6 or it is not. To overcome this, we have fewer technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6 these are –

1. Tunneling
2. Dual Stack Router
3. NAT Protocol Translation (NAT-PT)

II. TUNNELING

Tunneling is a protocol that allows the secure movement of the data from ine network to another. This involves allowing private network communication to be sent across a public network, such as the Internet, through a process called Encapsulation. This encapsulation process allows the data packets to appear as though there nature is public to a public network whereas they are actually private data packets, allowing them to pass through unnoticed.

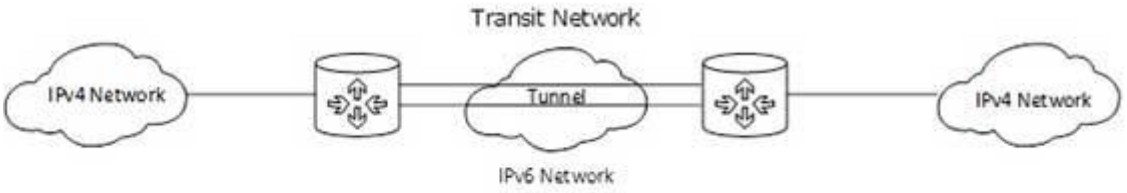
It is also called as PORT-FORWARDING.

There are various protocols that allow tunneling to occur, including

2.1 Point-to-Point Tunneling Protocol (PPTP): PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the "virtual" sense because it is actually being created in a tunneled environment.

2.1 Layer Two Tunneling Protocol (L2TP): This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.

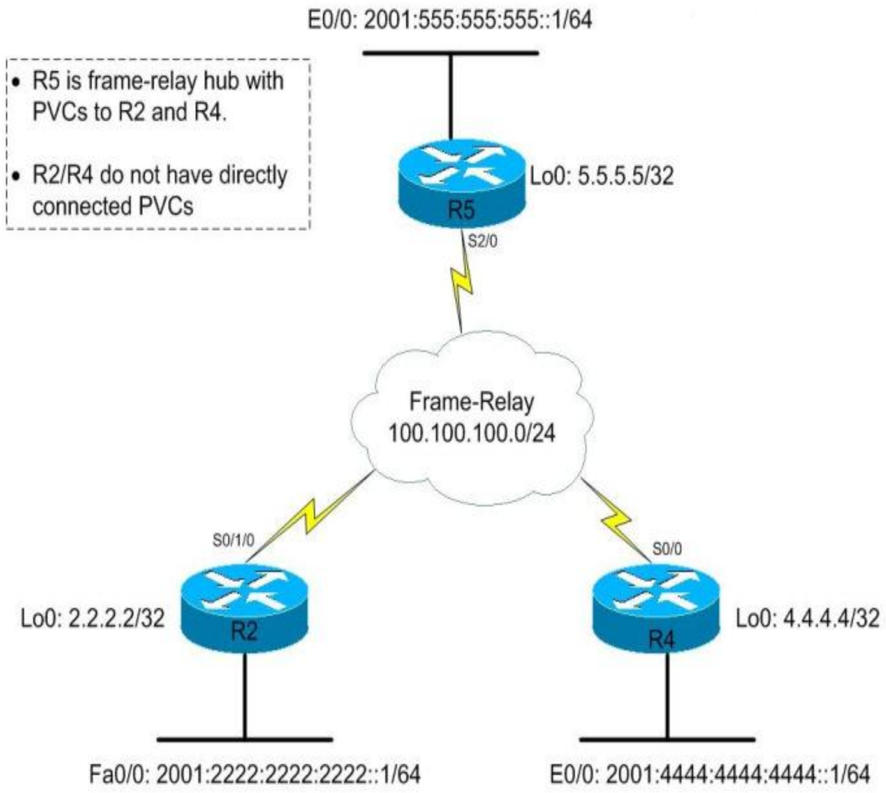
The scenario where different IP versions exist on intermediate path or transit networks, tunneling provides an enhanced solution where the data of the user can pass through a non-supported IP version.



III. TUNNELING

The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the intermediate network is on IPv6 and vice versa is also possible.

Here we will be with a corporate network. Our network has three major sites connected over a Wide Area Network (WAN) in a hub and spoke topology. R5 is our HQ site and is the hub. R2 and R4 are spoke sites. R5 has frame relay Permanent Virtual Circuits (PVCs) directly to R2 and R4 whereas R2 and R4 donot talk directly with each other, only through the hub. Our corporate company is interested in IPv6 but wants to pilot it between the three major sites before committing to go fully IPv6 in the future. Unfortunately, Internet Service Provider (ISP) is still only running on IPv4 and so we have three IPv6 island networks connected through a IPv4 backbone. Let's checkout through a diagram


E0/0: 2001:555:555:555::1/64
• R5 is frame-relay hub with PVCs to R2 and R4.
• R2/R4 do not have directly connected PVCs
Lo0: 5.5.5.5/32
R5
S2/0
Frame-Relay
100.100.100.0/24
S0/1/0
S0/0
Lo0: 2.2.2.2/32
R2
R4
Lo0: 4.4.4.4/32
Fa0/0: 2001:2222:2222:2222::1/64
E0/0: 2001:4444:4444:4444::1/64

IV. INITIAL CONFIGURATIONS

Let's look at the initial configurations without any IPv6. We will be running Open Shortest Path First (OSPF) as our Interior Gateway Protocol (IGP) over frame-relay. Each site will advertise its loopback address into OSPF. After we look at the frame-relay and OSPF configuration on each router we will verify OSPF adjacencies and make sure we can ping the other loopback addresses to ensure we have full IPv4 reachability between our routers.

R2

```
interface Serial0/1/0
 ip address 100.100.100.2 255.255.255.0
 encapsulation frame-relay
 ip ospf priority 0
 frame-relay map ip 100.100.100.2 205
 frame-relay map ip 100.100.100.5 205
 frame-relay map ip 100.100.100.4 205 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
router ospf 1
```

```
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 100.100.100.0 0.0.0.255 area 0
R2#sh ip ospf neigh
Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5         255   FULL/DR         00:01:58    100.100.100.5   Serial0/1/0
R2#ping 4.4.4.4 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/114/116 ms
R2#ping 5.5.5.5 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
```

R4

```
interface Serial0/0
 ip address 100.100.100.4 255.255.255.0
 encapsulation frame-relay
 ip ospf priority 0
 frame-relay map ip 100.100.100.2 405 broadcast
 frame-relay map ip 100.100.100.4 405
 frame-relay map ip 100.100.100.5 405
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 100.100.100.0 0.0.0.255 area 0
R4#sh ip ospf neigh
Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5         255   FULL/DR         00:01:37    100.100.100.5   Serial0/0
R4#ping 2.2.2.2 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
```

```
Packet sent with a source address of 4.4.4.4
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/115/116 ms
R4#ping 5.5.5.5 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/60 ms
```

R5

```
interface Serial2/0
 ip address 100.100.100.5 255.255.255.0
 encapsulation frame-relay
 ip ospf priority 255
 serial restart-delay 0
 frame-relay map ip 100.100.100.2 502 broadcast
 frame-relay map ip 100.100.100.4 504 broadcast
 frame-relay map ip 100.100.100.5 504
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
router ospf 1
 router-id 5.5.5.5
 log-adjacency-changes
 network 5.5.5.5 0.0.0.0 area 0
 network 100.100.100.0 0.0.0.255 area 0
 neighbor 100.100.100.2
 neighbor 100.100.100.4
R5#sh ip ospf neigh
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/DROTHER    00:01:49    100.100.100.2   Serial2/0
4.4.4.4           0   FULL/DROTHER    00:01:46    100.100.100.4   Serial2/0
R5#ping 2.2.2.2 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
R5#ping 4.4.4.4 so lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/59/60 ms
```

Basic IPv6 Configurations

R2

```
ipv6 unicast-routing
interface FastEthernet0/0
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2001:2222:2222:2222::1/64
```

R4

```
ipv6 unicast-routing
interface Ethernet0/0
 no ip address
 ipv6 address FE80::4 link-local
 ipv6 address 2001:4444:4444:4444::1/64
```

R5

```
ipv6 unicast-routing
interface Ethernet0/0
 no ip address
 ipv6 address FE80::5 link-local
 ipv6 address 2001:5555:5555:5555::1/64
```

V. HOW IPV6 6TO4 TUNNELING WORK

Here we will know how tunneling is actually going to work. We have three separate IPv6 islands now, yet we are connected via an IPv4 infrastructure. Essentially what a 6to4 tunnel does is it encapsulates IPv6 traffic into IPv4 packets. The IPv4 packet will have a source address of its loopback interface and a destination address of the destination router’s loopback interface. The IPv4 packet on the “outside” will carry IP protocol 41 and on the “inside” will be our IPv6 packet with header and payload. Up until now, this sounds a lot like a simple ipv6ip tunnel, so what’s the difference? In an ipv6ip tunnel you specify an IPv4 source and an IPv4 destination manually on the tunnel. It is strictly point-to-point. With IPv6 6to4 tunnels, you don’t actually manually specify a tunnel destination, and the technology is multipoint. On each router we will only need a single 6to4 tunnel interface.

The IPv6 prefix 2002::/16 is reserved specifically for the 6to4 tunneling technology. Your 6to4 tunnel interface will use an address from this range. Built into the address is an encoding scheme that takes your IPv4 address and encodes it into part of the IPv6 address. This works by encoding the IPv4 address into the IPv6 prefix so that your IPv6 prefix looks something like this: 2002:AABB:CCDD::/48. AABB:CCDD would be your IPv4 address. Once you have your /48 prefix you can utilize a /64 or whatever for your actual tunnel IPv6 address.

When routers need to send packets to any address in the 2002::/16 range they will actually look at the 32 bits following 2002, convert them into an IPv4 address and thus figure out themselves the destination of the tunnel.

VI. ENTITIES INVOLVED IN THIS TECHNOLOGY

Mobile Node: The device that needs IPv6 mobility.

Home Link: This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.

Home Address: This is the address which the Mobile Node acquires from the Home Link. This is the permanent address of the Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities take place as usual.

Home Agent: This is a router that acts as a registrar for Mobile Nodes.

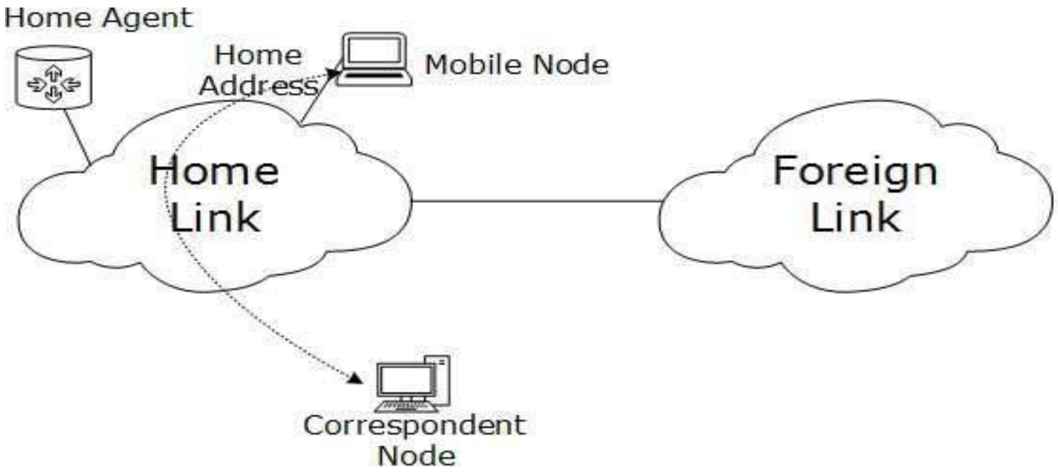
Foreign Link: Any other Link that is not Mobile Node's Home Link.

Care-of Address: When a Mobile Node gets attached to a Foreign Link, it acquires a new IP address of that Foreign Link subnet. Home Agent maintains the information of both Home Address and Care-of Address. Multiple Care-of addresses can be assigned to a Mobile Node, but at any instance, only one Care-of Address could get bind with the Home Address.

Correspondent Node: Any IPv6 enabled device that intends to have communication with Mobile Node.

VII. MOBILITY OPERATION

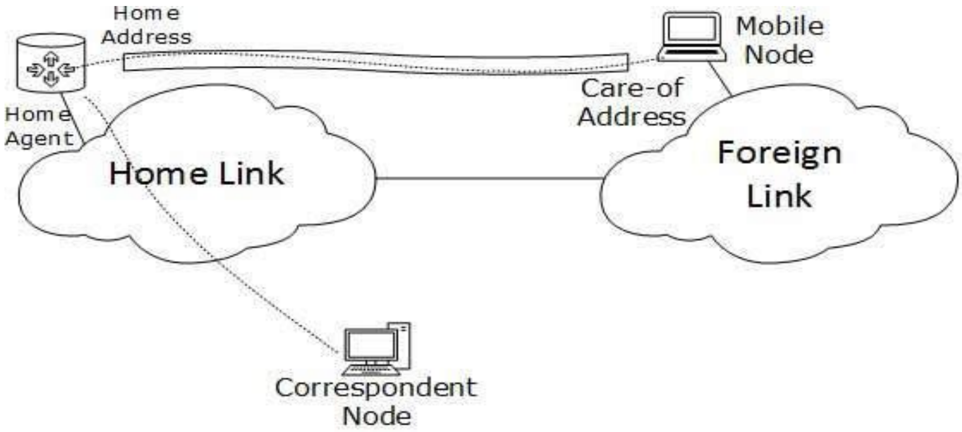
When Mobile Node stays in its Home Link, all communications take place on its Home Address as depicted in the figure below:



VIII. MOBILE NODE CONNECTED TO THE HOME LINK

When a Mobile Node leaves its Home Link and is connected to some Foreign Link, the Mobility feature of IPv6 comes into play. After getting connected to a Foreign Link, the Mobile Node acquires an IPv6 address from the Foreign Link. This address is called Care-of Address. The Mobile Node sends a binding request to its Home Agent with the new Care-of Address. The Home Agent binds the Mobile Node's Home Address with the Care-of Address, establishing a Tunnel between both.

Whenever a Correspondent Node wanted to establish a connection with the Mobile Node, the Home Agent intercepts the packet and forwards to Mobile Node's Care-of Address over the Tunnel which has already been established.



Mobile Node Connected To Foreign Link

IX. PROPOSED WORK

Through tunneling the transition from IPv4-IPv6 the transition takes place through certain protocols pf tunneling which ultimately is increasing the time-complexity. It would be better if the transition occurs without tunneling which reduces the complexity of time.

X. CONCLUSION

This document discusses ways to provide a seamless Internet experience to user accessing IPv4 internet services though completely new IPv6-ip. We have discussed over the difference between the IPv6 and IPv6-ip. We have seen the need of transition from IPv4 to IPv6. We should also keep in mind the security for this we have discussed certain protocols of tunneling. It also describes how established content providers and content enablers can transparently provide existing or new services to IPv6 Internet users by deploying Network Address Translation IPv6 to IPv4 (NAT64) technology with little or no change in their existing network infrastructure, thus maintaining business continuity.

XI. ACKNOWLEDGEMENT

We thank Dr. Pramod Kumar Jain (Director, Tulas Institute Dehradun). We would also like to thanks Mrs. Mitali Chugh (HOD of CSE Department, Tulas Institute) for her assistance and comments that greatly improved our manuscript.

We would also like to show our gratitude to Mrs. Shuchi Jain (Assistant Professor CSE Department, Tulas Institute) for sharing their pearls of wisdom with us during the course of this research. Although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1]. http://www.webopedia.com/TERM/T/tunneling.html

[2]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6380492

[3]. http://www.tutorialspoint.com/ipv6/ipv6_ipv4_to_ipv6.htm

[4]. https://www.techopedia.com/definition/5402/tunneling

[5]. http://profmattstrassler.com/articles-and-posts/particle-physics-basics/tunneling-a-quantum-process/

[6]. https://rfcbasher.wordpress.com/2011/11/25/ipv6-tunneling-mechanism-demystified-6-to-4-tunnel/