Next Generation IP

1 INTRODUCTION

The IPv6 transition mechanism is a technology, which is designed to permit hosts on an IPv4 network to communicate with the hosts on an IPv6 network. With the exceptional expansion of Internet users in recent years, densely populated countries, for example China and India, are running out of IPv4 addressees. The TCP/IP has also played an important role in the global expansion of communications. More users joining the Internet results in spreading the knowledge in every field throughout the world. However, there is problem of the limited IP addresses while we are on IPv4. It has been estimated that IPv4 addressed would run out by 2011, so IPv6 was designed to solve the problem.

2 INTERNET PROTOCOL

Overview

On the Internet, every computer has a unique address. This address is called IP, which stands for Internet Protocol. It defines the format of packets and provides an addressing system, which has two functions: identifying hosts and providing a logical location service.

The dominant version of Internet Protocol is IPv4 and the next generation is Internet Protocol Version 6 (IPv6). Now, one may wonder where the IPv5 is. After the IPv4, IPv5 was introduced to overcome the obstacles or problems of IPv4. Mainly, it was designed to provide Quality of Service (Qos) for streaming services. It was envisioned to be the connection-oriented complement to IPv4 but was never introduced for public use. The next generation of Internet Protocol is IPv6, which is also called IPng or IP next generation.

IPV6

The Internet Engineering Task Force (IETF) is in charge for defining Internet Protocols standards. When they developed IPv4, many issues were not taken into consideration, such as address and security issues. Later on, in the early 1990s IETF decided that to overcome the issues related to IPv4, they needed new versions of IP and IPng was created which is now known as IPv6. IPv6 offers many functions, which were not introduced in IPv4. Some of the improvements were increased address size, integrity communications, built in security. With many of these new features, IPv4 is supposed to be replaced by IPv6 in every network without any limitations. At the end of 1998, IPv6 was fully standardized.

IPv6 header: -

<table>
<tr><td>Version</td><td>Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="2">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
</table>

Version – It specifies the Internet Protocol version 6.

Traffic Class – It holds two values consisting of six and two. Six-bit values are used for differentiated services to classify the packets. Two-bit values are used for explicit congestion notification (ECN).

Flow Label – The 20-bit flow label was created for giving real-time application. The flow label is used to detect spoofed packets.

Payload Length – The 16-bit payload length contains the length of the data fields in bits.

Next Header – The 8-bit selector specifies the transport layer protocol and specifies the type of next header.

Hop Limit – The 8-bit unassigned integer is decremented by 1, and when counter reaches 0 packet is discarded.

Source Address –The 128-bit source address indicates the originator.

Destination Address – The 128-bits source address indicates the recipient of the packet.

Features of IPv6

The features of IPv6 are listed below:

New Packet Format and Header – The new IPv6 packet format assists to minimize packet header processing by routers.

Larger Address Space – In comparison to IPv4, IPv6 uses four times more bits in the address. IPv4 uses 32 bits while IPv6 uses 128 bits

Auto Configuration – There are two types of auto configuration in IPv6. IPv6 supports both stateful and stateless auto configuration of every other host device.

Security – IPSec security is built in IPv6, which is difficult to add in IPv4.

COMPARISON OF IPV4 AND IPV6

Description	IPv4	IPv6
Address	32 bits long (4 bytes). For ex:- 192.168.255.255	128 bits long (16 bytes). For ex:- FE80:0000:0000:0000:0202:B3FF:FE1E:8329
Configuration	Need to be configured like IP address and routes.	Configuration is optional.
Domain Name System (DNS)	Support	Support

Dynamic Host Configuration Protocol (DHCP)	Used to dynamically obtain an IP address and other configuration information.	DHCP does not support.
File Transfer Protocol (FTP)	Allows transferring files across the networks.	FTP does not support.
Internet Group Management Protocol (IGMP)	Used to find the hosts which want traffic for particular multicast group,	MLD does what IGMP in IPv4, but uses ICMPv6 by adding a few MLD-specific ICMPv6 type values.
Internet Control Message Protocol (ICMP)	Used to communicate network information.	Similar is used while Internet Control Message Protocol Version 6 (ICMPv6) some new attributes.
IP header	Variable length of 20-60 bytes depending on IP options presents.	Fixed length of 40 bytes.
IP header options	More options might accompany an IP header.	No IP header options. IPv6 adds optional extension headers.
Layer Two Tunnel Protocol (L2TP)	Thought as virtual PPP and works over any supported	Does not support.

	line type.	
Netstat	Tool to look at the status of TCP/IP connections, interface or routes.	Same support for IPv6.
Network address translation (NAT)	Basic firewall functions integrated into TCP/IP.	Does not support as it solves the problem of shortage of address.
Packet filtering	It is the basic firewall functions, configured by the System i Navigator.	Does not support in IPv6.
Point to Point Protocol (PPP)	Supports dialup interface over various modem and line types.	PPP does not support IPv6.

TRANSITION FROM IPV4 TO IPV6

There is not complete transition from IPv4 to IPv6 because IPv6 is not backward compatible. However, there are some technologies, which can convert IPv4 to IPv6. The technologies that can convert IPv4 to IPv6 are described as below step by step.

Dual Stack

In this method, both IPV4 and IPv6 protocols are available in the same network node and that is why it can connect to remote servers with both technologies (IPv4, IPv6). This technology ensures that only IPv4 node is upgraded. This technology is based on name lookup and application selection.

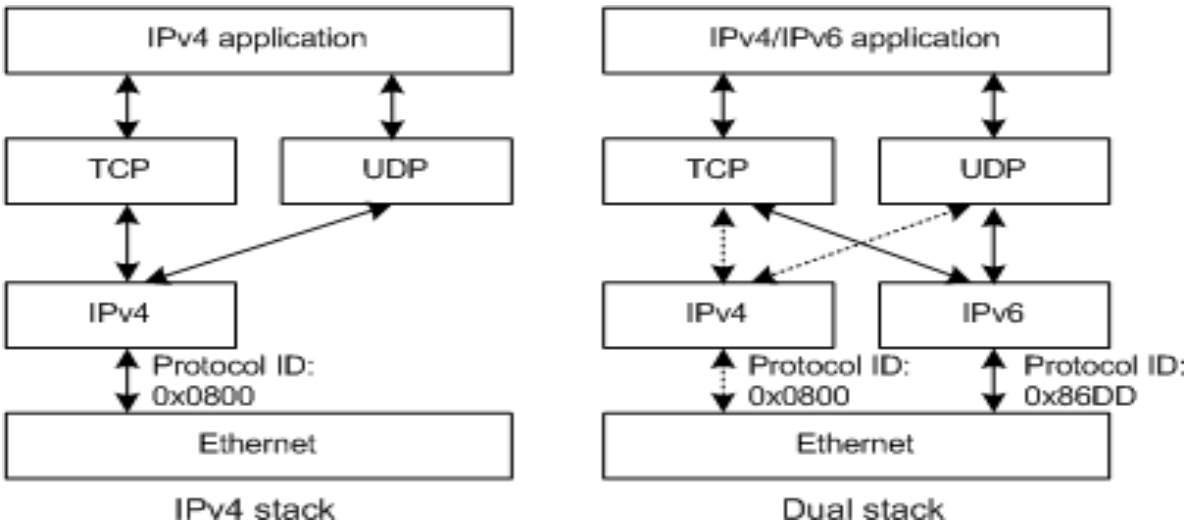

Figure . IPv4 application using the IPv4 stack /application using both IPv4 and IPv6 stacks

Challenges

Dual stack can connect with both IPv4 and IPv6 technologies. Challenges faced during the deployment of dual stack method are outlined as below:

- IPv4 and IPv6 have different software requirement to run. For example, IPv4 runs with OSPFv2 and IPv6 runs with OSPFv3.
- In Dual stack Exchange, the device is configured in only one stack and most forward to dual stack devices, for example, routers and then back to the same segment using the other stacks and this results in insufficient bandwidth. To implement dual stack, IPv6 needs to be activated in all network elements and this will cost on redesign of the existing networks.

Tunneling

For minimizing the transitions, all the routers on the way between the two IPv6 nodes do need to support IPv6. This method of transition is called tunneling. Primarily IPv6 packets are placed inside IPv4 packets then the packets are routed through the IPv4 routers.

One of the objections to integrating IPv6 into the current IPv4 networks is the ability to transport IPv6 packets over IPv4 –only networks. Tunneling or in IPv6 known as overlay tunnel can be used. IPv6 packets are encapsulated through the overlay tunnel in IPv4 packets for delivery across IPv4 infrastructure. The main disadvantage of tunneling is that it does not let communication between users of new protocols and old protocols without dual stack hosts.

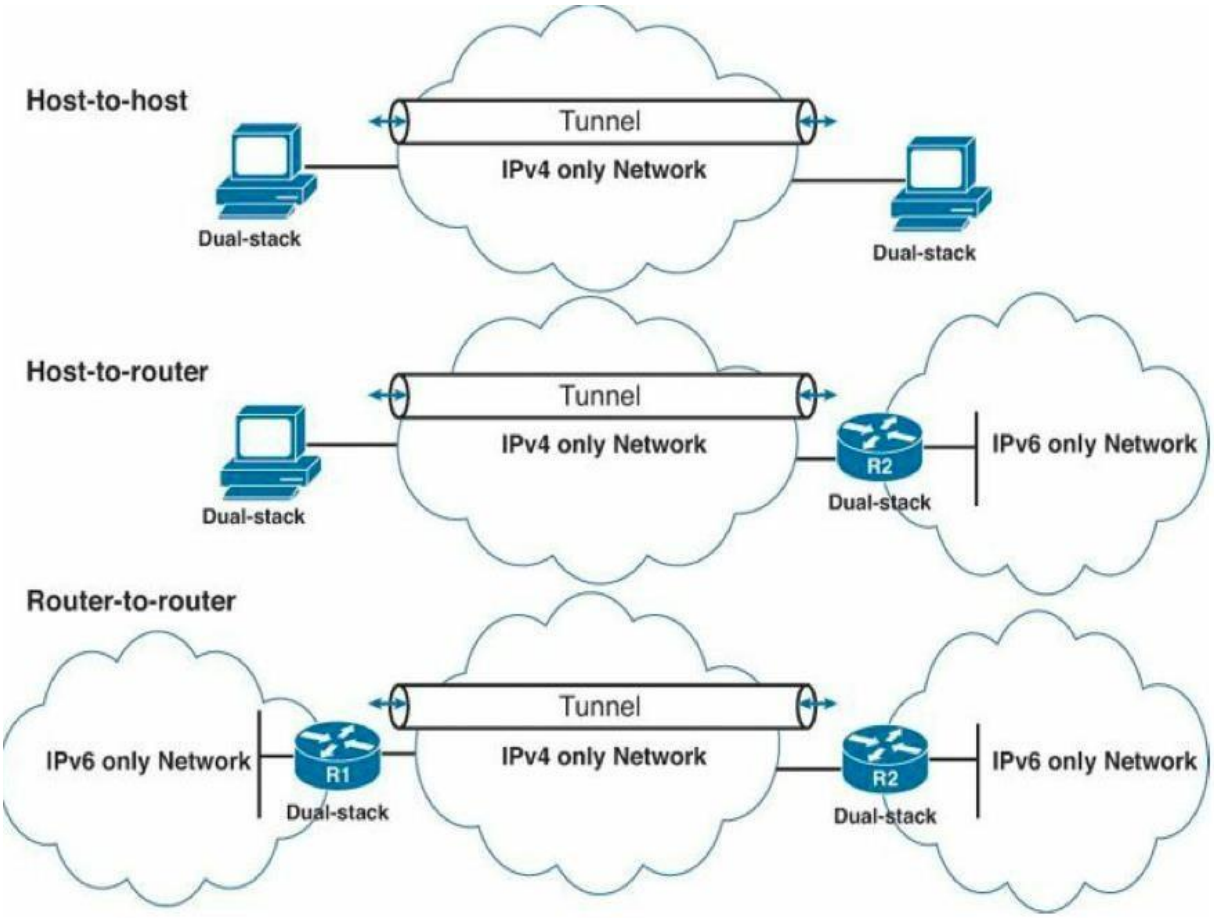

Figure . IPv6 tunneling involving different scenarios

Tunneling can involve any combinations of routers depending upon the end-points (entry and exit points) of the tunnels. There are three scenarios: - host-to-host, host-to-router and router-to-router which are shown in Figure 6.

There are two types of protocols in a tunnel, namely transport protocol and passenger protocol.

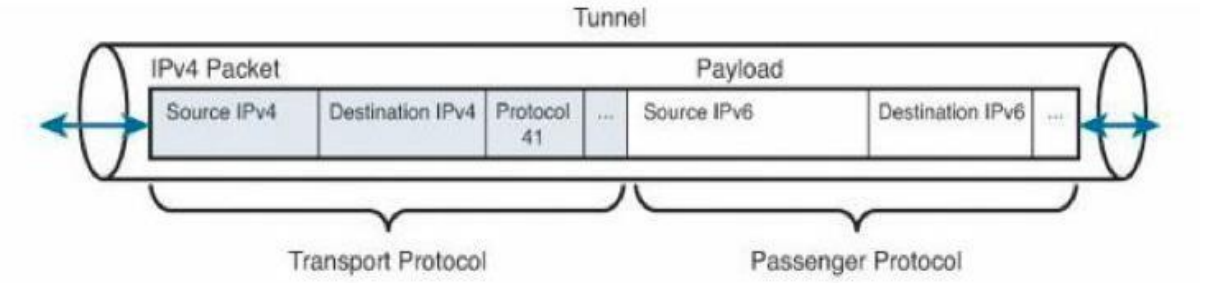

Figure . Tunnel consisting of protocols [10]

Transport Protocol: IPv4 is the transport protocol where the tunnel is created. In the IPv4 header, protocol 41 shows that the encapsulated data portion is an IPv6 packet. Passenger Protocol: IPv6 is the passenger protocol. Protocols are encapsulated in the tunnel and carried over the tunnel.

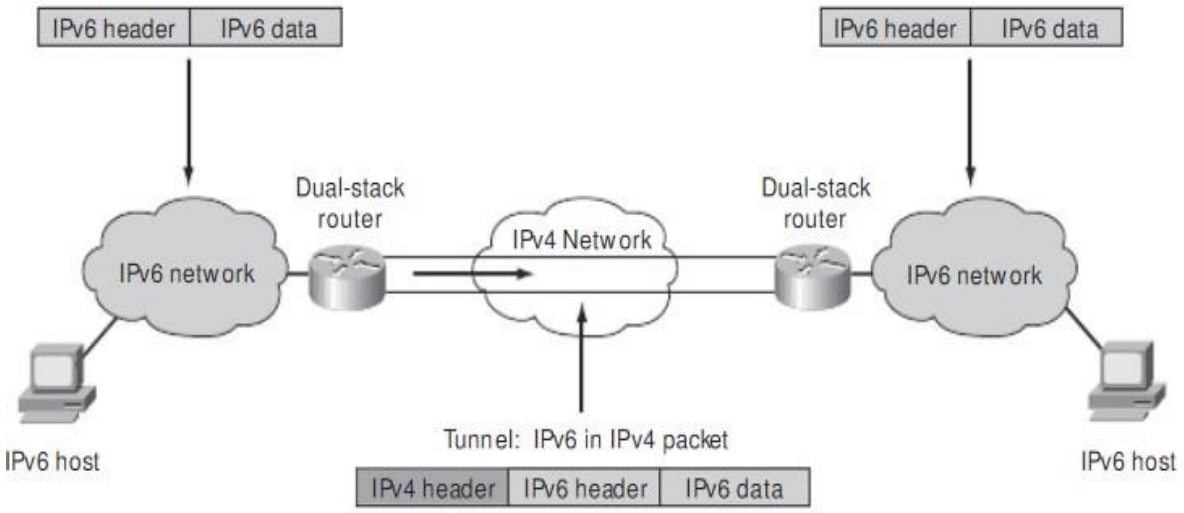

Figure . Use of IPv6 over IPv4 tunnels

ADVANTAGES AND DISADVATAGES OF PRACTICAL TRANSITION OF IPV6 OVER IPV4

ISPs and big companies need to take steps to ensure service continuity with transparency for their customers at all the times during transition and co-existence. It is most important that the transition to IPv6 is stable and non-interruptive to exiting services. The operators should have clear ideas how they will transition to IPv6 and know the risks and challenges ahead before they start the transition. Some operators may focus on green design while other may focus on IPv4 and IPv6 co-existence. Operators should have list of strategies and concepts what they are seeking for. IETF has been developing tools for more than a decade for transitioning to IPv6 but many operators have not yet begun yet. The reason behind that could be lacking IPv6 development in applications, hosts, CPEs, network equipment, and contents. Another reason could be lack of knowledge in applying technologies and techniques in the network without causing interruption in service. The transition problem faced by the providers include the following areas: Network, Connectivity, Applications, and network Management and Operation.

a) Network problems

Address Architecture

IPv6 has much larger address space in comparison with IPv4. Due to the large IPv6 address space, special attention is needed when designing the IPv6 network since it differs from the fragmented and smaller IPv4 address design. Providers will need to plan in advance for IPv6 unlike IPv4, will provide them with an enormous address space, which needs cautious architectural consideration.

Connectivity

While starting transition to IPv6, the systems engineers should design a network to provide continuity of service to the customers. For this, dual stack is the natural approach but due to the depletion of IPv4 address and cost, providers may consider to upgrade part of their network to IPv6-only.

High Availability

High Availability (HA) is the major requirement for every service and network service. Providers have huge experience in running high availability in IPv4 using mature protocols, such as VRRP and OSPF Graceful Restart. Compared to IPv4, HA for IPv6 is less known. An application running on IPv6 may need to failover to IPv4 network due to network failure during transitioning. Some work needs to be done in this area to fix this problem. Besides, the new transition techniques require new HA models. If HA is supported, providers will normally deploy a transition method. [16]

b) Application Problems

During the transition process, IPv4 and IPv6 application will coexist in the network. Regardless of what technology providers choose to use, services should be provided to the customers. Providers should find out the best techniques for the transition without affecting the services they provide.

c) Network Management and Operation Problems

In paper, organizing an IPv6 network should be similar to organizing an IPv4 network. For example, SNMP works over IPv6 without modification. New technologies and techniques may be introduced during the transition process. These new technologies and techniques require new operation models.

The growth of Internet users has led to the shortage of usable IPv4 in the nearer future. Giant communication companies, like China Telecom, are practical examples for encouragement of IPv6, because of consequences caused due to the limited IPv4 addresses. Few technical issues arise due to the change of platform from IPv4 to IPv6 and these are outlined as follows: -

1. Limited availability of IPv4 addresses to China Telecom gave rise to the need to find a new way of identifying Internet gateways. This led to the transition to IPv6. [17]
2. Newly used IPv6 is uncommon in Internet websites and very few Internet Content Provider (ICP) look for the option of IPv6 when

expanding proprietary services because of the enormous code change and increasing manpower. Many business websites are always linking each other and creating a complex structure, which leads to many problems when one website migrates to IPv6 only. Content Provider/Service Providers (CP/SP) do not realize how urgent it is to migrate to IPv6, which is the main reason why ICP migration lacking motivation. [17]

3. Some specific terminals (for example, set top box) do not support IPv6 while the main operating systems do. [17]
4. China Telecom has two key problems while IPv6 transition, large-scale network and large number of subscribers. The transition involves multiples level and broad scope, which lead to huge costs in modification as with the large-scale network and various service platforms. [17]
5. The use of IPv6 becomes a reliable solution for companies like China Telecom and Internet-based companies for expanding the volume of subscribers.