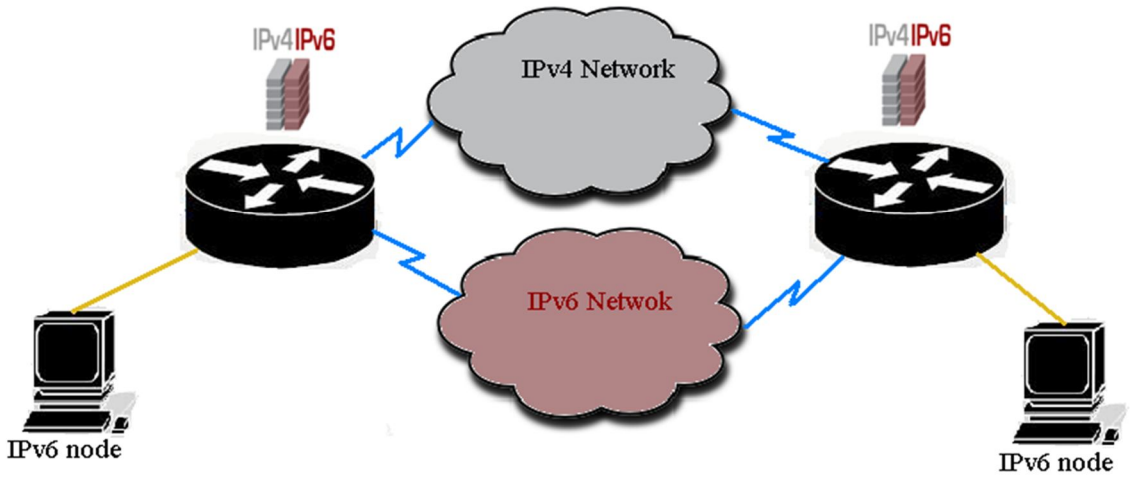
Technical report, May 2011

IPv4-IPv6 Transition Techniques

Bachelor's Thesis in Computer Communications

Lokesh Galla , Suyesh Regmi



School of Information Science, Computer and Electrical Engineering
Halmstad University

IPv4-IPv6 Transition Techniques

Bachelor's Thesis in Computer Communications

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

May 2011

Preface

We would like to express our sincere gratitude to our Halmstad University, Sweden.

Sincere thanks to every employee at Halmstad University, who help us directly or indirectly to finish our Bachelors in Computer Communications. We believed that, this is one of the mile stone in our life.

Personal thanks to:

Programme Director,

Nicolina Månsson.

Professor and Thesis Supervisor,

Malin Bornhager.

By,

Lokesh Galla.

Suyesh Regmi.

Abstract

When changing a network from IPv4 to IPv6, Internet networks will be hybrid by using both IPv4 networks and IPv6 networks. This thesis defines the essential information about compatibility between IPv4-IPv6 mechanisms. Dual Stack is one of the IPv4-IPv6 compatible mechanism by running both IPv4 stack and IPv6 stack in a single node. 6 to 4 tunneling mechanism encrypts IPv6 packets in IPv4 packets to make communications possible, from IPv6 network over IPv4 network. Dual Stack & Tunneling mechanisms were completely implemented later in this thesis work. This thesis examine transmission latency, throughput, jitter and delay from end to end, through empirical observations of both Dual Stack and tunneling mechanisms by using TCP/UDP as transport protocols in different scenarios. This thesis work contains some useful strategic point of view before trying to deploy IPv6 in a network.

Table of Contents

1. Introduction

A node or a computer needs an IP (Internet Protocol) address to communicate between peers. Internet Protocol Version 4 (IPv4) address exhaustion lead to another technology addressing protocol known as IP next generation (IPng) or Internet Protocol Version 6 (IPv6). The IPv6 was intended to design for sufficient address space for the present and future Internet network growth. IPv6 increases IP address scheme size from IPv4-32 bits to 128 bits [3]. IPv6 is an improved version of network layer protocol, designed to resolve problems with IPv4. In **CHAPTER 4** discussed much detailed about IPv4 and IPv6 address.IPv6 address scheme is compatible with IPv4 address scheme; this means IPv6 networks is able to co-existence with IPv4 networks for long-run future networks. The smooth running IPv4 in a network makes organization does not want to deploy IPv6 in their network. But, anyhow limitations of IPv4 does not support new upcoming network needs. The current IPv4 based Internet is huge and complex, so IPv4 could not be replaced by IPv6 ones overnight.

Migration from one technology to another technology is fairly complex, because of IPv4 and IPv6 uses different stacks for communication. But there are some mechanisms, those supports co-existence between IPv4 and IPv6 such as Dual Stack, Tunneling IPv6 packets over existing IPv4 networks, and IPv6 Only to IPv4 Only Transition Mechanisms. In **CHAPTER 6** discussed much detailed about IPv4-IPv6 Transition Mechanisms. IPv6 network and IPv4 network uses different routing protocols to send datagrams over the network. All Transition mechanisms are good in some cases and network scenarios, but every transition mechanism owns advantages and disadvantages in a particular scenario.

2. Motivation

The rapid growth of the Internet needs better IP address solutions. This headed to deployment of IPv6 in the Internet. As a first step towards deploy IPv6 across the world, is Co-existence of IPv4 and IPv6 [4]. The complete transition of the Internet will be a huge task. The transition is expected to take several years [1]. The best choice will be to use co-existence mechanisms. This thesis motivation is to make survey on different co-existence mechanisms to find better and cost-effective IPv6 deployment.

2.1 Problems analyze and approaching

Problems analyze and approaching is focused on both IPv4 and IPv6 implementation and routing functionalities. Below are stated some of the general enquires & problems.

- Could a node support IPv6
- Could a node support both IPv4 and IPv6
- Is co-existence a good mechanism

- How could we achieve routing between nodes with both IPv4 and IPv6?
- What are the smooth transition mechanisms?
- Etc…

3. Background

The IP protocol is used to connect various nodes in a network, so present Internet growth obsessively require global unique unicast IP addresses. IP considered as the common denominator to meet different application layers such as data, voice, video and audio. So these all devices demand IP addresses to inter connect all kind of IP appliances on the Internet.

The Internet Protocol version 4 (IPv4) is determined by its 32 bits address scheme. IPv4 is the fourth revision in the IP development. The limited space of IPv4 makes inconvenience for long-run growth of Internet. Furthermore, parts of the IPv4 classes' scheme, such as "Class D" and "Class E" are reserved for special uses. This decreases the number of globally unique unicast IPv4 addresses. The large blocks of globally unicast addresses were started assign to organizations across the globe in 1980s [1]. The present Internet is growing rapidly especially in Asia and Europe [1]. Some of Asian and African countries received one "Class C" address for the entire country; because of limitations in IPv4 and late arrives to the Internet.

The global Internet routing table is vast and still growing in the future. To support these vast routing tables, organizations are using despite mechanisms such as Classless interdomain routing *(CIDR)* and Network Address Translation *(NAT)* in IPv4 address scheme. Some studies predicted the exhaustion of the current IPv4 address between 2005 and 2011 [1]. Well people may have doubts. If CIDR & NAT mechanisms support substantially, what is the necessity of deploy IPv6? This thesis work tried to present some of the solutions.

3.1 Classless interdomain routing (*CIDR*)

Classless interdomain routing (*CIDR*) [RFC 1519, RFC 4632] mechanism was developed to prevent the problems of IPv4 exhaustion. Therefore IPv4 address space became much better effective. The theory behind CIDR is that blocks of IPv4 multiple class addresses can be combined, or aggregated, to create a larger classless set of IP address with more hosts allowed [2]. By employing CIDR breaks the Class-full addresses to Class-less addresses, to make better use of address space. However, it does not reference the issue of how to get additional public, registered globally unique IP address.

For example of CIDR Class B:-

Class-full: - n.n.0.0/16. Class-less: - n.n.x.0/18.

3.2 Network Address Translator (*NAT*)

The IP Network Address Translator (*NAT*) [RFC 1631] is a mechanism employed to map the internal private address to external public address. In a scenario of NAT services a single node act as agent between private network and public network. This makes a single unique IP address represents entire group of computers or nodes in a network. Figure 3.2-1 explains the NAT functionality,

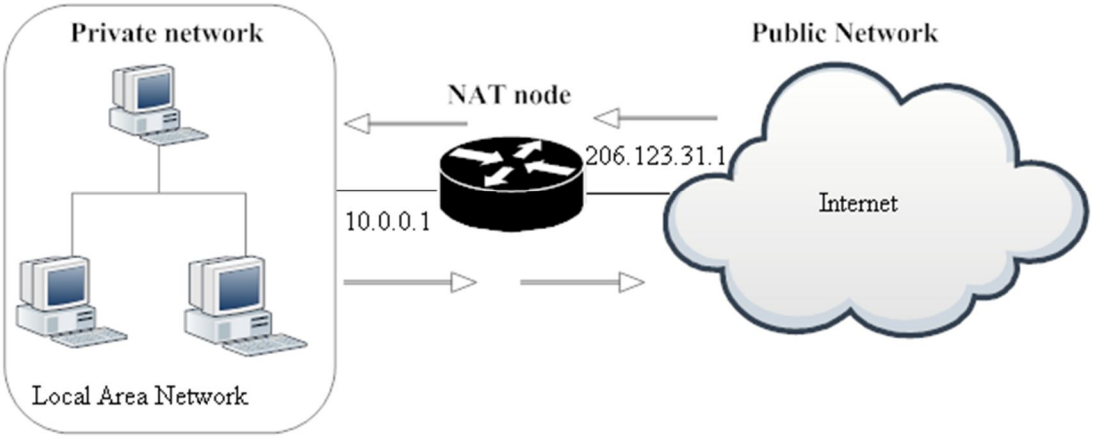


Figure 3.2-1 Network Address Translator (NAT) mechanism

NAT Functional Description:

A node from Local area network having IPv4 address 10.0.0.10 wants to communicate with a node in Internet having IPv4 address 206.123.31.10 in Figure 3.2-1.

The connection could be done like below,

	Node:10.0.0.10	NAT	Node:206.123.31.10
Source	10.0.0.10	10.0.0.10	206.123.31.1
Changed-Source	-	206.123.31.1	-
Destination	206.123.31.10	206.123.31.10	206.123.31.10

Table 3.2-1. NAT Functional description.

IP address original design was based on end to end model. Due to limited addresses of IPv4, NAT introduced as a temporary solution. NAT is a patch applied to

increase life span of IPv4 exhaustion. NAT usually breaks the end to end model to provide services. This imposes a number of limitations on the Internet such as:

Some of these limitations are documented in RFC [RFC 2775, RFC 2993] [1],

- NAT breaks IP's end to end model:

Design of IP has to handle network connection at only endpoints (hosts and servers), so NAT do not have to handle connections [1]. Break of IP's end to end impact on end to end services in a scenario.

- The necessity to keep the state of connections:

NAT need to keep the connections state and has to remember address translation and ports.

The necessity of keeping the connections state in NAT makes fast re-routing. In case of failure of a NAT device it is difficult to provide services. Networks use links and routes so redundancy can suffer problems [1].

If organizations deploy high-speed links such as Gigabit Ethernet, 10 Gigabit Ethernet into their network, NAT need additional processing because each connection state must be kept with NAT. Therefore NAT reduces network performance [1].

In a NAT infrastructure providers and organizations must keep state of all connections made by their end users for security reasons [1], Recording of NAT state tables become mandatory to trace back the source of problems [1].

- Applications problems with NAT:

The function of Network Address Translator (NAT) implies that many applications cannot be used effective in all instances.

Application such as multimedia applications videoconferencing, VoIP and Video-on demand/IPTV do not work smoothly through NAT devices [2].Multimedia applications uses Real-Time Transport protocol (RTP) and Real-Time Control Protocol (RCTP) as a transport protocol. These employs UDP with dynamic allocation of ports but NAT does not support this environment directly [2].

- Security problems with NAT:

- Keberos authentication needs the source address, and the source address in the IP header is mapped to another address by NAT devices. So this authentication cannot be done smoothly in NAT [2].

- IP-Sec is used extensively for data authentication, integrity and confidentiality. Due to NAT end to end IP address break makes impact on IP-Sec [2].

- Address space collision:

If two different organizations and networks use the same private addresses space and have to merge or connect to the Internet, this cause a collision of an address space in a network. Routing will be disables to reach the other network. However this problem could be solved by few techniques such as renumbering or twice the NAT. But these techniques are expensive and increase the complexness of NAT [1].

NAT has some more problems with routing, such as multicast routing requires complex configurations in a NAT environment [2].

4. Internet Protocol (*IP*)

The Internet Protocol enforces two basic operations; addressing and fragmentation. The Internet modules use the addresses carried in the Internet header to transmit datagrams towards their destinations [7]. An IP packet or a datagram has two fundamental components; IP header and payload [1]. Transmission control protocol (TCP) and the Internet protocol (IP) are the basic two protocols started function with IP. The TCP/IP Internet protocol derives from the Network layer in the OSI model.

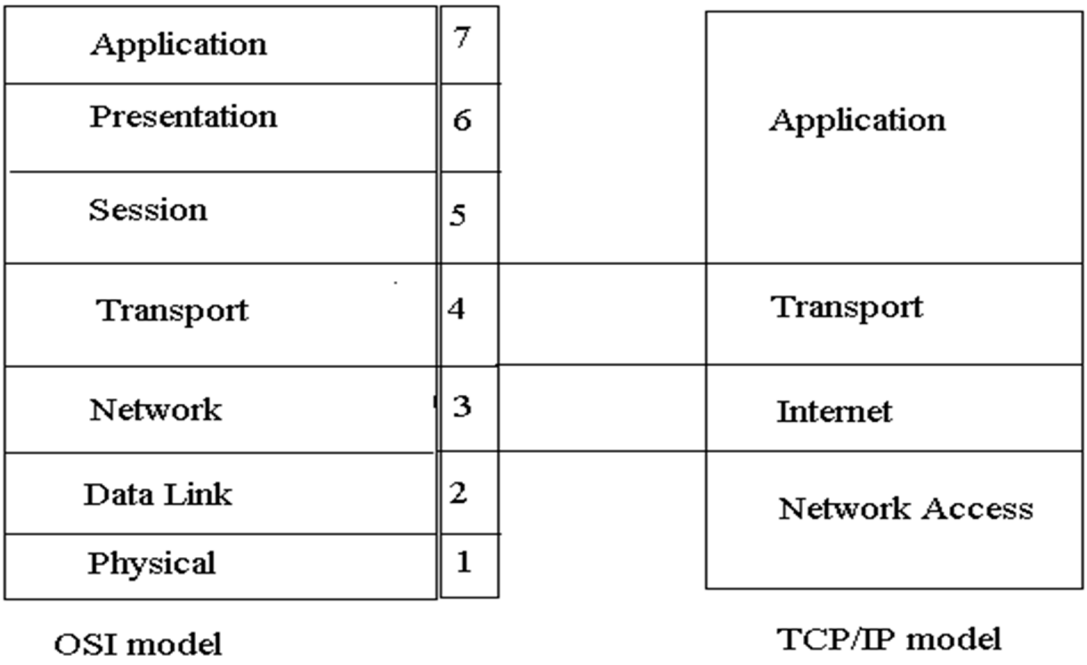


Figure 4.1 OSI – TCP/IP model

The choice of a path for transmitting datagrams is called routing. The Internet modules utilize fields in the Internet protocol header to fragment and reassemble datagrams for transmission through networks. For providing services on the Internet, the Internet protocol uses four fundamental mechanisms such as Type of Service, Time to Live, Options, and Header checksum [7] with Source and Destination address fields.

Present Internet has two well-known Internet protocols. Without these protocols present and the future Internet cannot exit. Those are,

- **Internet Protocol Version 4 (*IPv4*).**
- **Internet Protocol Version 6 (*IPv6*).**

4.1 Internet protocol version 4

An IPv4 address is a 32 bit numeric address to a node in a network. Internet protocol utilizes IP addresses to make a communication with a particular node in the network. An IPv4 address carries two sort of information such as “Network address” and “Host Address”. The network address is used to find location of a network and host address is utilized to reach particular destination within a network.

4.1.1 IPv4 header classification

<table>
<tr><td>Version</td><td>IHL</td><td>Type-of-Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td>Time To Live</td><td colspan="2">Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options (padding)</td></tr>
<tr><td colspan="5">Data(Variable)</td></tr>
</table>

Table 4.1-1 IPv4 Header

Version:

The version of the IPv4 header is for version information. It is 4-bits IP version information embedded in an IPv4 header.

Header Length:

Header length is 4-bit in octets of the header size and is up to payload field.

Types of Service (ToS):

Length of ToS is 8-bit.Types of Service are applied to indicate the quality of the service (QoS) desired [7].This field also be constructed as Differentiated service code point (DSCP) [1].

Total Length:

The size of Total Length is 16-bit IP packet in octets. It includes header and payload. The maximum size of an Ipv4 packet is 65,535 octets [1].

Identification; Flags; and Fragment Offset:

The size of each field in IPv4 header is 16-bit, 3-bit, and 13-bit respectively. These fields are related to packet fragmentations by routers. The Maximum Transmission Unit (MTU) along path is smaller than the sender's MTU size; these fields in IP header attend fragmentation of an IP packet. For Ethernet the MTU is 1500 octets [1].

Time to Live:

Time to live is 8-bit IPv4 packet life time information embedded in IPv4 packet. This field is decremented each time the packet passes through the router. When field becomes value 0, The IPv4 packet is destroyed and error message sent to the source node through Internet Control Message Protocol (ICMP).

Protocol Number:

Protocol Number with size of 8-bit specifies the upper-layer protocol used in packet payload [1]. Upper-layer protocols information such as TCP, UDP, or ICMP, etc...

Header checksum:

Header Checksum is 8-bit of the IP header; this is used for error checking.

Source Address:

Source address is a 32-bit numeric value of source or sender node's IPv4 address.

Destination Address:

Destination is a 32-bit numeric value of receiver or destination node's IPv4 address.

Options:

Options field is variable in size and it increases the length of the header when used [1].

Padding:

Padding is used to assure that the packet ends on 32-bit boundary [1].

Payload or Data:

It represents the data to be delivered to a destination. Payload is not a field of basic IPv4 header.

4.1.2 IPv4 Address classification

IPv4 is made up of 32 binary bits and is divided into two portions, such as network portion and host portion with the help of a subnet mask. The 32 binary bits are separated into four octets, each octet is 8 bits and divided with the symbol dot (“.”). The value used for each octet is in the range 0 to 255 or decimal notation 00000000 to 11111111. IPv4 is a dotted decimal format, for example: 192.169.22.101.

IPv4 address octets are broken down to provide an addressing scheme that can adapt large and small networks [14]. These octets separated into five different classes of networks from A to E. These classes were used for allocation of IPv4 addresses in different locations in the Internet. IPv4 address classes were divided as follows:

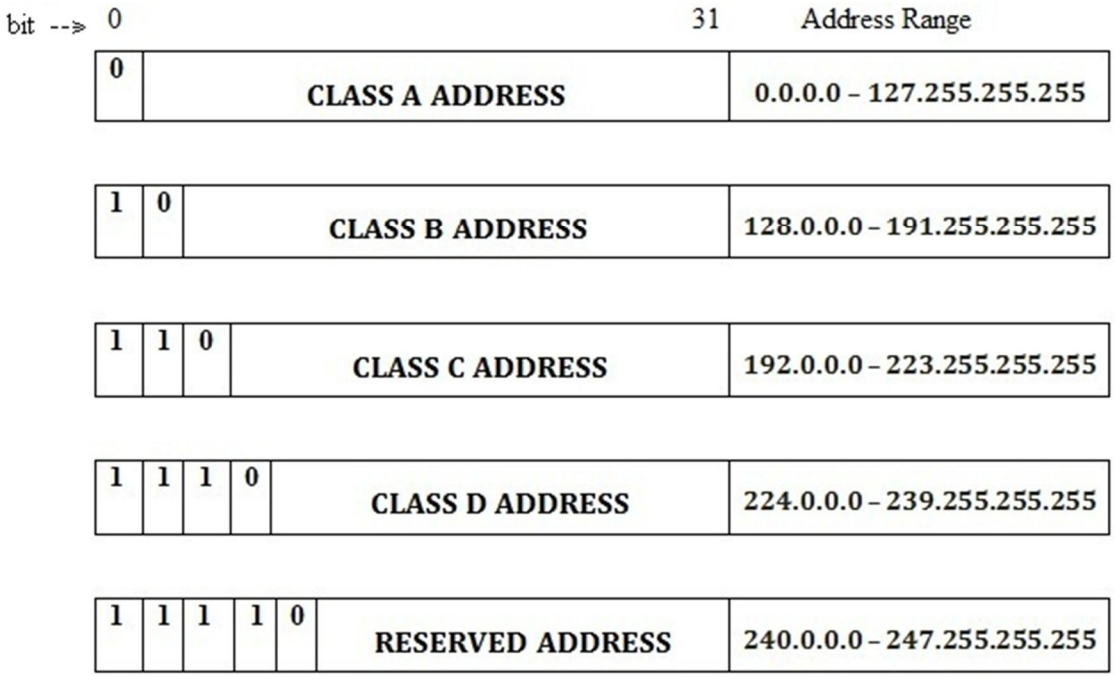


Figure 4.1.1-1 IPv4 Classes Ranges

4.2 Internet Protocol version 6

The Internet Engineering Task Force (IETF) designed the IPv6 Address scheme [16]. The IPv6 protocol represents an upgrade of the IPv4 [1]. IPv6 is designed not only to solve the IP addresses shortage problems, but also improves and enhances prominent features over IPv4.

IPv6 prominent features [16][1][2]:

- Scalability enhances routing and addressing capabilities.
- Simplifies the IP header.
- Capable of provide globally unique addresses for all of the present and future IP devices in the Internet.
- Multihoming with preservation of route aggregation is possible.
- ARP broadcast is replaced by multicast use on the local link.
- Security features such as payload encryption and authentication of the source of the communication.
- Provides better support from end to end networks for real time traffic, example VoIP, Voice and Video.
- Plug and Play: This facilitates the connection of equipment to the network. This configuration is automatic.
- Freedom from NAT breaks.

General differences between IPv4 – IPv6,

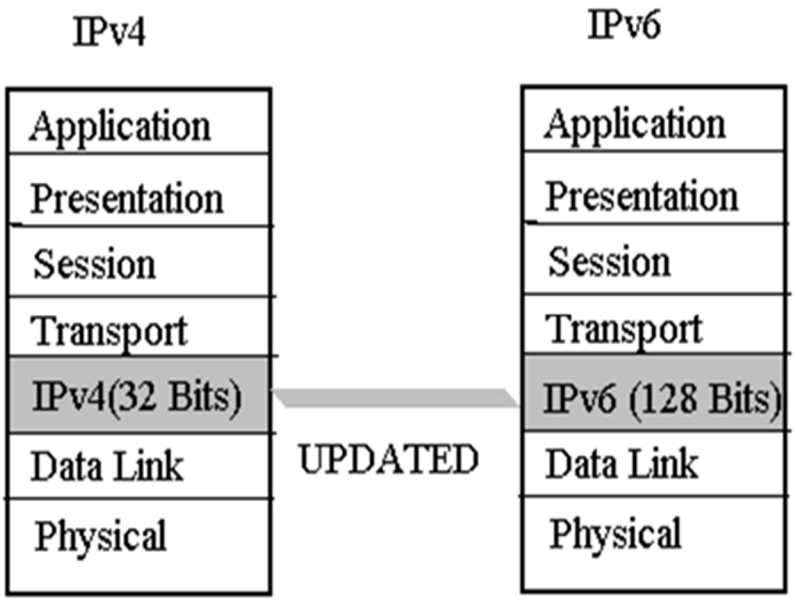


Figure 4.2-1 scope of IPv4 and IPv6 with OSI

4.2.1 IPv6 header classification

The IPv6 header is simpler than IPv4 packet header [1]. Six fields from IPv4 header were removed in IPv6 packet header. Options and Padding fields has 14 fields, and the IPv6 header has eight fields. The basic size of IPv6 header is fixed length, but in IPv4 header with options field may have variable length [1].

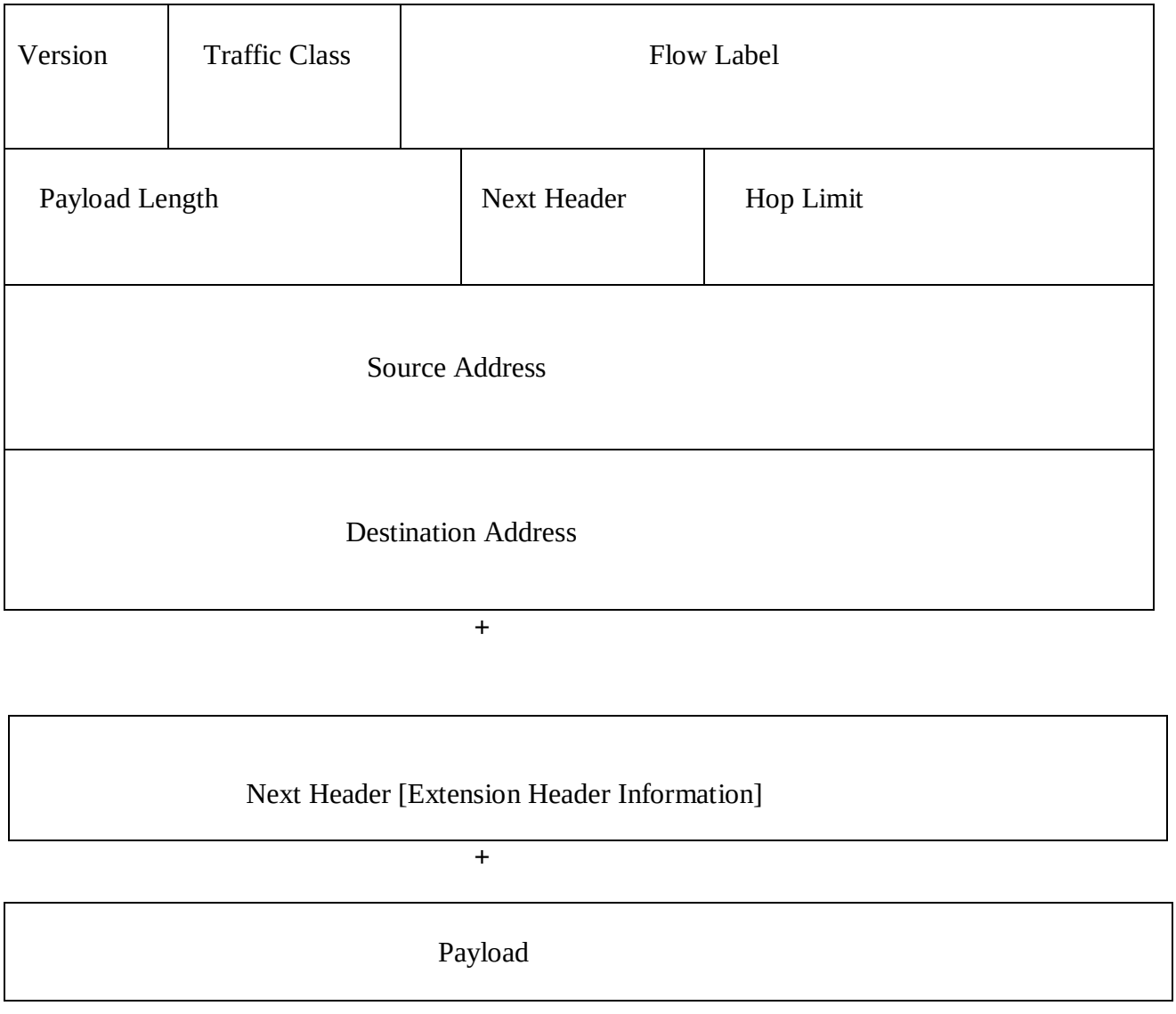


Table 4.2-1 IPv6 Header

Version:

The 4-bit version of IPv6 header format identifies the version number of Internet Protocol , which is used to generate the packets.

Traffic Class:

The 8-bit Traffic Class field replaces the Type of Services field in IPv4 header format and defines the traffic priority of the packet.

Flow Label:

The 20-bit Flow Label field provides additional support for Quality of Services (QoS) and real time datagram delivery.

Payload Length:

The 16-bit Pay Load field replaces the Total Length field from IPv4 header format and it contains the number of bytes of the Payload.

Next Header:

The 8-bit Next Header field identifies the type of header that follows the next IPv6 header. This field replaces the IPv4 Protocol field and uses the same value.

Hop Limit:

The 8-bit Hop Limit field replaces the Time to live field in IPv4 header format. Hop Limit is used to prevent the packets from endlessly circulating in IPv6 network. When the Hop Limit is zero packet will discard.

Source Address:

The 128-bit Source Address field identifies the IP address of the original source of the IPv6 Packet.

Destination Address:

The 128-bit Destination Address field identifies the IP address of the final destination of the IPv6 Packet.

Payload:

IPv6 can send packets more than 65,535 octets network with large MTU value [1] [RFC 2675]. These packets are called IPv6 Jumbograms [1].Payload is data sending from source to destination.

IPv6 Extension headers [1]:

Except Main Header Format IPv6 consist of separate optional Extension Headers that are located between the IPv6 Header and the Upper Layer Header in a packet. An IPv6 packet may contain none, one or more than one Extension Headers. Most of the Extension Headers are not processed by the router until the packet arrives to the final destination. There are different kinds of Extension Headers such as:

Hop By Hop Options:

This header is used to carry optional information that must be examined by every node along a packet delivery path.

Routing header:

This header defines a method that allows a source to specify the route of the packet.

Fragmentation header:

This header is included when a packet contains only a fragment of original message.

Encapsulating Security Payload header (ESP):

This header carries encrypted data for the secure communication.

Authentication Header (AH):

This header carries information used to verify the authentication of the encrypted data.

Destination Options:

This header is used to carry additional information that is processed only by the destination node on a routing path of packet.

4.2.2 IPv6 address classification

IPv6 is a 128-bit hexadecimal IP address for an IP device. An IPv6 Address contains 16-byte hexadecimal number fields divided by colons (":"). An example of IPv6 Address: 2001:abcd:120F:0000:0000:0001:876A:111B.

IPv6 uses a compressed form to make IPv6 address easier to represent. Methods that are used to compress are as follows:

- **Example 1:-**

  The compressed form of "0000" in 16-byte hexadecimal number is "0".
  An IPv6 address 2001:abcd:120F:**0000**:**0000**:0001:876A:111B
  compressed as 2001:abcd:120F:**0**:**0**:0001:876A:111B

- **Example 2:-**

  "0001" 16-byte hexadecimal compressed form is "1".

  Ex: - 2001:abcd:120F:0:0:**0001**:876A:111B
  compressed form is 2001:abcd:120F:0:0:**1**:876A:111B.

- **Example 3:-**

  Continuous zeros of 16-byte hexadecimal could be compressed by a pair of colons (":"). However, the pair of colons is allowed just once in a valid IPv6 address compressed form [16].

  Ex:- 2001:abcd:120F:**0000:0000**:0001:876A:111B
  Valid compressed form is 2001:abcd:120F**::**1:876A:111B

Network Prefix

Network prefix is used to identify network length in an IPv6 address. Network Prefix is known as subnet mask in IPv4. The IPv6 prefix is made up of left most bits acts as network identifies [16]. The prefix-length is a decimal value used in the range of 0-128 high-order contiguous bits indicates the length of network portion of the address.

For Example: - 2001:abcd:120F:0000:0000:0001:876A:111B/64

In the above example IPv6 address has prefix value **(/64)** this represents the network address space [**2001:abcd:120F:0000**] and reaming of the address [0000:0001:876A:111B] acts as host address in the above example.

4.2.3 IPv6 address types [16][1][2][15]

An IPv4 host typically uses one IP address; but an IPv6 host can have more than one IP address [16].

There are three major types of IPv6 address:

1) Unicast
2) Anycast
3) Multicast

Unicast:

Unicast is an address that identifies a single interface. An IPv6 packet that is sent to a unicast address is delivered to the interface identified by that unicast address. Unicast addresses are divided into following types,

- **Aggregatable global unicast address:** Aggregatable global unicast addresses are globally routable and globally reachable on the Internet [2].
- **Link local Address:** Link local address is utilized by nodes when communicating with neighboring nodes on the same link [2].
- **Site-local address:** Site-local address is utilized between site to site links in the same organization.

- **Special addresses:** Such as unspecified and loopback addresses.
- **Compatibility addresses:** Compatibility address is 6to4 address

Anycast:

An Anycast address identifies a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface as defined by the routing protocols [16]. For example mail group distribution [2].

Multicast:

A Multicast address identifies multiple interfaces for one-to-many communication. A packet sent to a multicast address is delivered to all interfaces identified by the multicast address [16].

Detailed picture of IPv6 Address types and ranges,

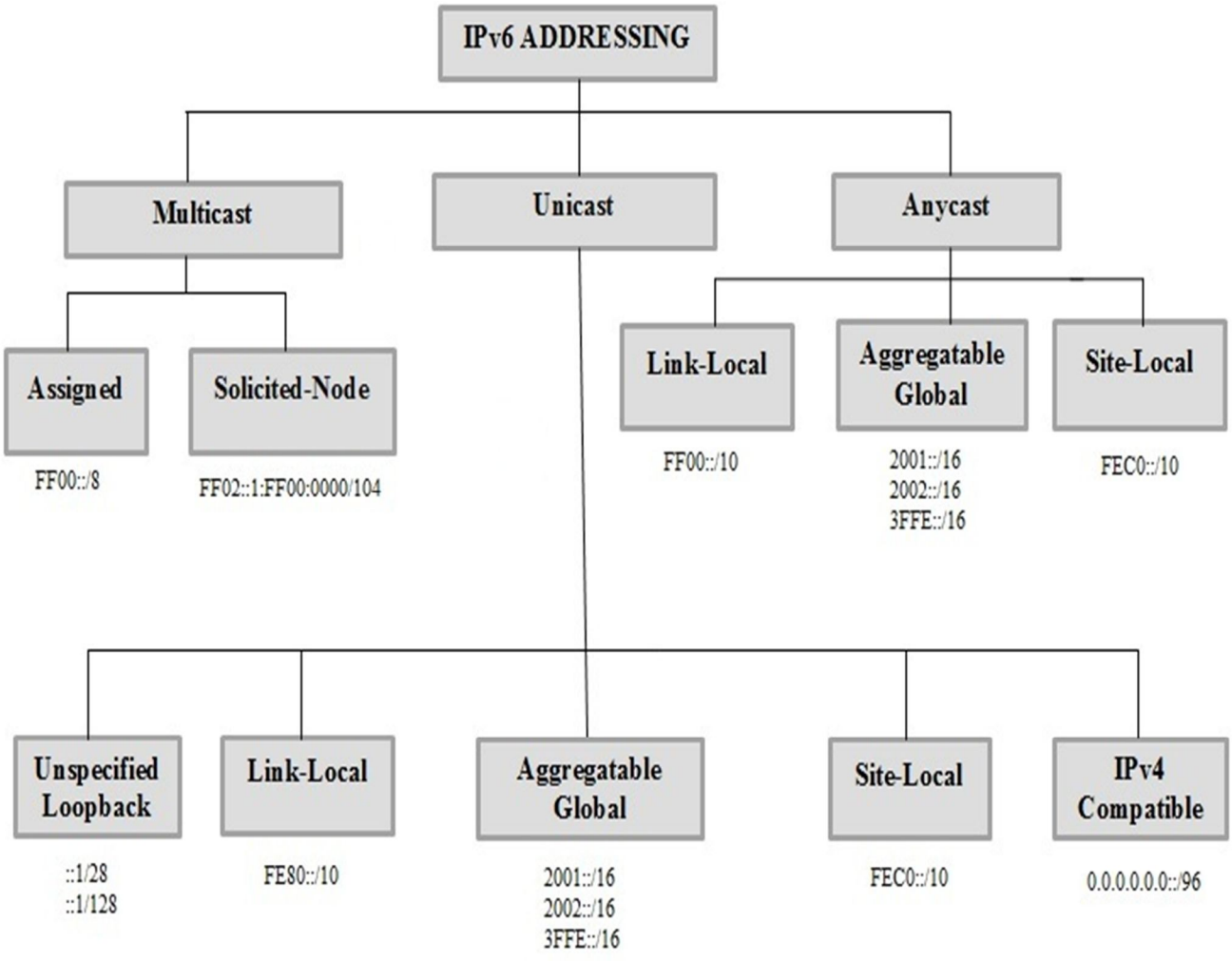


Figure 4.2.2-1 IPv6 Address types [1]

5. Routing protocols

The selection of a path for transmitting datagrams is called routing. The important task of a router in a network is to determine the best path during the packet forwarding process. The routing process need a router to use routing table and the routing table contains entries information of different paths through the routing protocols. The IPv6 uses the similar kind of routing protocols with IPv4 but with some modifications. However, IPv6 is a new version of protocol and different from IPv4. The routing table is also managed separately from IPv4 routing table when both protocols were enabled on a router.

5.1 Exterior Gateway Protocols

Exterior gateways protocols are used to exchange routing information among different Autonomous Systems (AS).

- Example of an EGP:-
  - Border Gateway Protocol (BGP4+).
  - Exterior Gateway Protocol (EGP).

5.1.1 BGP4+

The most common exterior gateway routing protocol for IPv6, is a new version of Border Gateway Protocol 4 (BGP4+), known as multiprotocol BGP or BGP4+. BGP4+ is a path vector routing protocol that uses Transmission Control Protocol (TCP) to enable connections with other BGP neighbours. BGP4+ is a multiprotocol BGP, so it can carry routing information for IPv6 as well as other protocol such as IPv4. BGP4+ can support the same features and functionality as IPv4 BGP.

5.2 Interior Gateway Protocols

Interior gateway protocols are used to handle routing information within Autonomous Systems (AS).The most common interior gateway routing protocols are two kinds, such as Distance vector protocols and link state protocols.

- Distance vector protocols
  - RIP (Routing information Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - IGRP (Interior Gateway Routing Protocol)
- Link state protocols
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System-to-Intermediate System)

The new and extended version of interior gateway routing protocols for IPv6 are RIPng, OSPFv3, IS-IS for IPv6 and EIGRP for IPv6.

5.2.1 RIPng

RIPng is an interior gateway routing protocol for IPv6 and also called Routing Information Protocol next generation. It is based on RIPv2 for IPv6 and defined in [RFC 2080]. It has the same features and capabilities as RIPv2. RIPng allow routers to exchange information for computing routes through an IPv6 network [9]. RIPng is a distance vector protocol and like RIP, it is also limited to radius of maximum 15-hops. User Datagram Protocol is used to send and receive routing information by RIPng. For IPv6 RIPng has been updated some extra features such as IPv6 prefix of the destination, IPv6 address of the next router along with path to the destination (next-hop address), Transport (RIPng messages are sent over IPv6 packets), UDP port number of 521 used to send and receive information between RIPng routers, and Link-local address FE80:: /10 use as the source address for RIPng updates sent to adjacent routers.

5.2.2 EIGRP for IPv6

EIGRP is an Enhanced version of IGRP developed by Cisco, uses the same distance vector algorithm and distance information as IGRP [10]. IPv6 supportive EIGRP is known as EIGRP for IPv6 and is similar to EIGRP used with IPv4. EIGRP provide features such as increased network width of 224 hops in compare to 15 hops of RIP and simple hello mechanism for neighbour discovery. EIGRP provide fast convergence, which allows quick routing information and EIGRP can scales to large network. EIGRP for IPv6 provides route filtering, and also has a protocol-dependent module for IPv4, IPv6 [11].

- Drawback of EIGRP runs only Cisco nodes.

5.2.3 OSPFv3

OSPFv3 is an interior gateway routing protocol for IPv6 defined in RFC 2740 and it is based on OSPFv2. Most of the functions provide by OSPFv3 is similar to OSPFv2 such as both uses same 5 packet type hello, database description (DDP), link state request (LSR), link state update (LSU) and link state acknowledgement (LSA), similar mechanism for neighbour discovery. However to handle the large address space some changes have been made in OSPFv3 such as OSPFv3 runs over a link instead of IPv4 behaviour of per-subnet [12]. OSPFv3 uses the IPv6 Link-Local address to identify neighbours. OSPFv3 uses IPsec Authentication Headers and IPsec Encapsulating Security Payload for security

purposes. LSA (Link-state acknowledgement) format have been changed in OSPFv3 and the new Link-LSA and Intra-Area-Prefix-LSA have been added. OSPFv3 allows IPv6-over-IPv4 tunnel configuration by sending OSPFv3 messages over IPv6 packet. OSPFv3 can support the ability to run multiple OSPF protocol instances on a single link [12].

In a Dual-Stack environment, for running OSPF need both OSPFv2 (IPv4) and OSPFv3 (IPv6) is needed because OSPFv3 is an IPv6-only protocol.

5.2.4 IS-IS for IPv6

Intermediate system to Intermediate system (IS-IS) is an Interior routing protocol for connectionless Network Service (CLNS) traffic. IS-IS routing protocol is based on the OSI model, which used as an Interior gateway Protocol to support TCP/IP as well as OSI. This allows IS-IS to support pure IP environments, OSI environment and dual environments [13].

The IETF have updated the IS-IS with two new Type Length Values (TLVs), those are **IPv6 Reachability** and **IPv6 Interface Address** to carry information related to IPv6 routing. The IPv6 Reachability defines about routing prefix, metric information and the IPv6 Interface Address contains 128 bit IPv6 Interface address.

Since IS-IS is a Link-State protocol has to enable both IPv6 & IPv4 protocols on all adjacency IS-IS routers. The IS-IS protocol must be enabled with both protocols on all adjacency routers at same time otherwise the IS-IS routers drop adjacencies with all their IS-IS routers [1].

6. Transition Mechanisms

The deployment of IPv6 is happening gradually on the Internet. Initially deployment of IPv6 should be happened within isolated islands, and then these islands should interconnect with other islands over existing IPv4 Infrastructures. To connect these islands “Transition mechanisms” are needed and these are compatible mechanisms employed for Co-existence of IPv6 and IPv4 infrastructure.

A number of transition mechanisms have been defined to support co-existence [2]. There is an additional need for a node to support IPv6. RFC (request for comments) defines the following types of nodes [2][RFC 4294].

- A node is device that has IP implements in it.
- A router is a device that forwards IP packets towards destination.
- A host is a node but not a router.

Types of node:

- **IPv4-only node:** A host or router that implements only IPv4 protocol in it.
- **IPv6/IPv4 node:** A host or router that implements both IPv6 and IPv4 protocol in it.
- **IPv6-only node:** A host or router that implements only IPv6 protocol in it.

The Internet Engineering Task Force (*IETF*) has defined a number of specific mechanisms to assist transition of IPv6 [2]. These mechanisms are basically divided as follows:

- Dual Stack
- Translation
- Tunneling

6.1 Dual Stack Transition Mechanism (DSTM) [18][2]

Dual-stack transition mechanism enables to run both IP stacks (IPv4 and IPv6) in a single node. Dual stack nodes maintains both IP protocol stacks that operates parallel and thus allow the end node to use either protocols [2]. The Dual stack node is capable of handling both kinds of IP (IPv4&IPv6) routing. Flow or routing decisions in the node are based on IP header version's field [2]. Both IPv4 and IPv6 shares common transport layer protocols such as TCP/IP. Many of client and server operating systems provide dual IP-protocol stacks [2].

For example: Windows XP, Vista, 7, Windows server 2003, Linux, Mac OS x [19][2].

TCP/IP model for dual stack node is as follows:

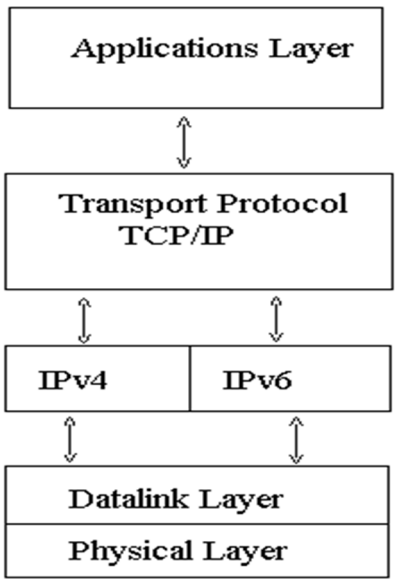


Figure 6.1-1 Dual stack TCP/IP model

Dual stack networking deploys IPv4 and IPv6 in the same infrastructure. If a node that support dual stack network, should be able to understand and process both IP protocols network. The dual stack node itself cannot decide at randomly, which IP stacks to use to communicate so the routing protocol decides, which stack to use. Example of Dual Stack infrastructure as follows:

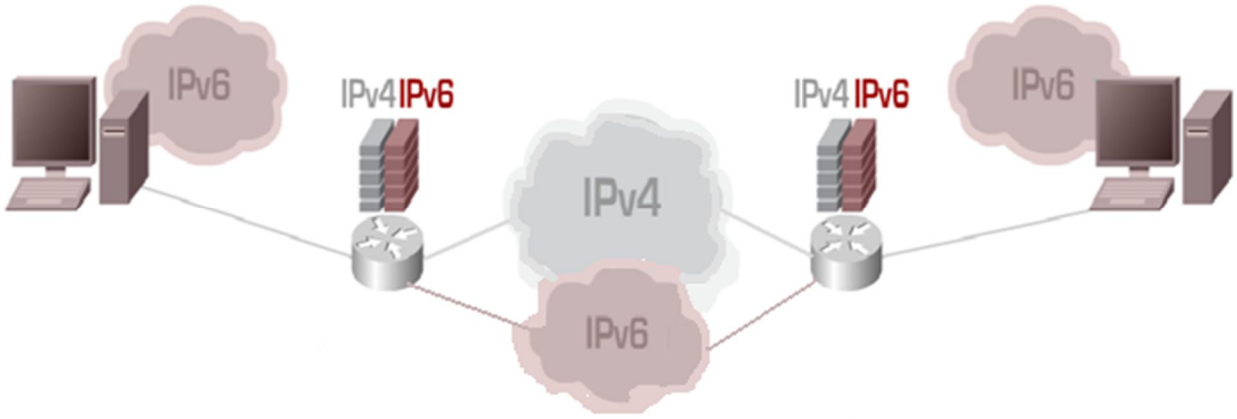


Figure 6.1-2 Dual Stack Infrastructure

6.2 Translation Mechanisms

Translation mechanism refers the direct conversion of IP protocols [2]. Translation mechanism may include transformation of both IPv4 and IPv6 protocol's header and payload according to their IP specifications. Some of the translation mechanisms are as follows:

- Stateless Internet Protocol/Internet Control Messaging Protocol Translation (SIIT) [RFC 2765][2].
- Bump in the Stack (BIS)[RFC2767][2].
- Bump in the API (BIA) [RFC3338][2].
- Network Address Translation - Protocol Translation (NAT-PT)[RFC2766][2].
- Transport Relay Translator [2].

Translation mechanisms always need translators that can translate particular IPv4 address to particular IPv6 address. This makes break in end to end network as NAT; this would not be a good choice.

Example of Translation Infrastructure:

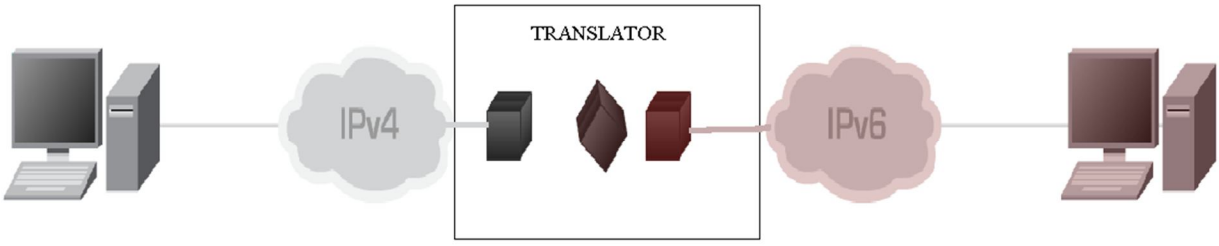


Figure 6.2-1 Translation Mechanism Infrastructure

6.3 Tunneling Mechanism

Tunneling, also known as encapsulation is a transition mechanism often used, where the networks infrastructure is not capable of offering IPv6 functionality so IPv6 traffic has to cross the existing IPv4 networks via tunnels [20]. Tunneling is a process where information of one protocol is encapsulated inside the packet of another protocol this allows the transport of the encapsulated data across the encapsulating protocol's network. The processes of packet forwarding in a tunnel, is IPv6 packet encapsulated in IPv4 packet and proceeds over normal IPv4 routing system and decapsulated at the other end of a tunnel. Tunneling provides a way for an existing IPv4 infrastructure to carry IPv6 traffic. There are several kinds of tunneling method for carrying IPv6 traffic over IPv4 networks. Tunnels can be done in different scenarios.

Some of them are as follows:

- Static Tunneling [2]
- Automatic Tunneling using IPv4-compatible Addresses[2]
- 6over4 Transition Mechanism [2]
- 6to4 Transition Mechanism [2]
- Intrasite Automatic Tunnel Addressing protocol (ISATAP)[2]
- Teredo [2]

Example of a tunneling infrastructure:

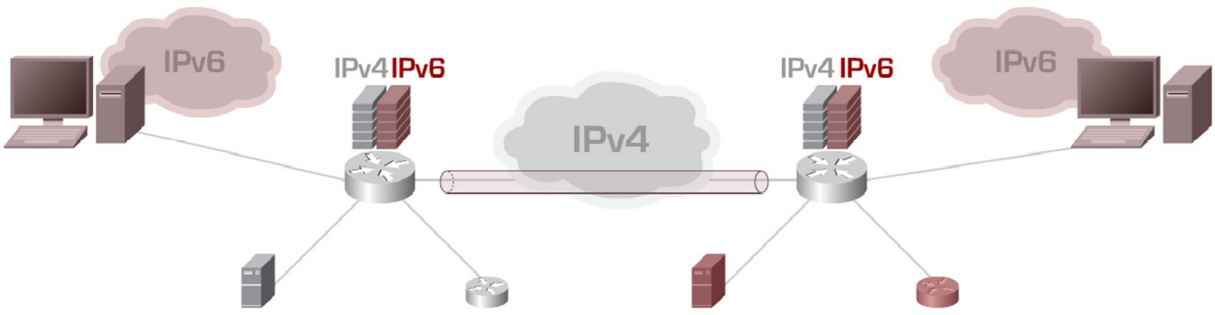


Figure 6.3-1 Tunneling Mechanism infrastructure

7. Implementation

The implementation setup has been done between “headquarters” and “branch office” of a company over public network (Internet Service Provider). Two sample models were experimented in a lab environment to evaluate the complexity and pros and cons of each method. Implementation work is done in two scenarios by implementing two methods such as 6to4 manual tunnel and Dual stack.

- **Scenario 1 method: 6to4 manual tunnel.**
- **Scenario 2 method: Dual stack.**

Behind selection of these particular two methods are easy to implement in existed equipment in an organization instead of spending budget on new equipment and accessories. Basic topology was established with three routers named as headquarters (HQ), Internet service provider (ISP 1) and Branch office (Br) .With that two Clients were used named as Host1 and Host2. Detailed process of connectivity has been explained in each of the scenarios. In both scenarios the connectivity was same.

Equipment used:-

- **Routers:** Cisco 2800 series with Cisco IOS version 12.4(4) T8.
- **Client:** Windows XP with IP dual stack installed.

IPv6 Installation on Host (Windows XP)

- To find out either node supports IPv6 address or not?

Find information about the node in the documentation and use the below commands on the end node computer and it shows the network interfaces installed in the node.

C:\> ipconfig.

If the node does not have IPv6 interface, install it by following steps. IPv6 Installation in windows machine is easy and it takes few steps to configure. Process of installation as follows: Open command prompt from windows start and follow below steps,

C:\> ipv6 install
C:\> netsh
netsh> interface
nestsh interface > ipv6
netsh interface ipv6 > add address “Local Area Connection” FEC0:78:1::2
netsh interfaceipv6> add route ::/0 “Local Area Connection”FECO:78:1::1
netsh interfaceipv6> add dns “Local Area Connection” [IPv6 add] [index]

For delete an IPv6 address use **delete** instead of **add** in configurations.

To determine the configuration use below command,

C:\> ipconfig .

7.1 Scenario 1 (6to4 manual tunnel)

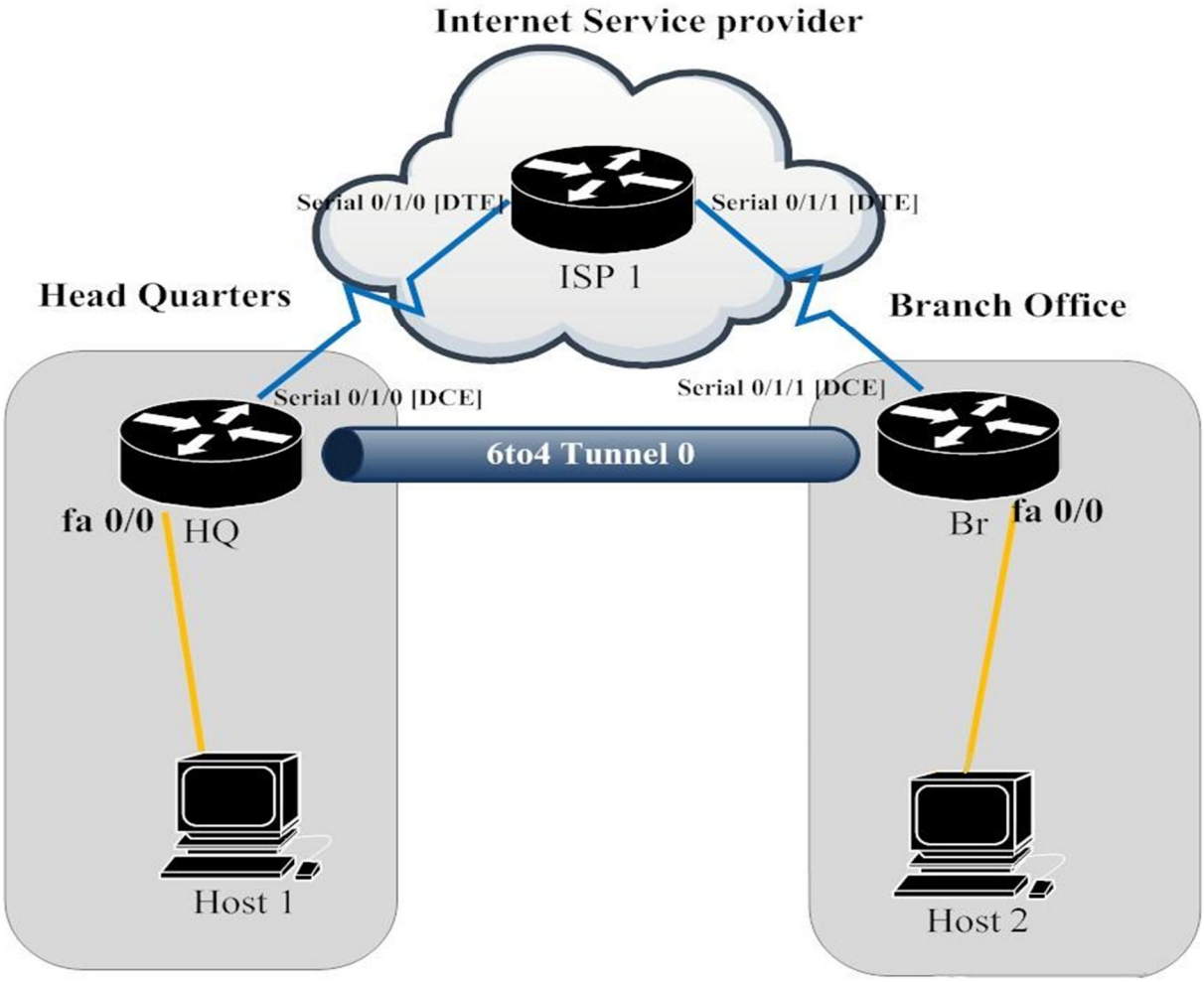


Figure 7.1-1 6to4 tunnel network topology

7.1.1 Physical Connections:

A network has been established between headquarters (HQ) and branch office (Br) over the Internet service provider (ISP1) as shown in the figure 7.1-1. In Scenario 1 to setup a network, three routers and two clients were used. From the figure 7.1-1 Host 1 is connected to HQ interface fa0/0 with an Ethernet cable. HQ interface serial 0/1/0[DCE] was connected to ISP1 interface serial 0/1/0[DTE] with a serial cable. ISP1 interface serial 0/1/1[DTE] was connected to Br interface serial 0/1/1[DCE] with a serial cable. Br interface fa0/0 was connected to Host2 with an Ethernet cable. This fulfill physical connectivity between headquarter to branch office.

7.1.2 IP Address Scheme:

Host 1:

IPv6 address	FEC0:78:1:1::2/64
IPv6 Gateway address	FEC0:78:1:1::1/64

Table 7.1.2-1 Host 1 IP addresses

Host 2:

IPv6 address	FEC0:78:1:2::2/64
IPv6 Gateway address	FEC0:78:1:2::1/64

Table 7.1.2-2 Host 2 IP addresses

Headquarter:

Interface	IPv4 address	IPv6 address
Fast Ethernet 0/0	--	FEC0:78:1:1::1/64
Serial 0/1/0	190.168.10.1/24	--
Loopback 0	192.168.1.1/24	FEC0::1:1/112
Tunnel 0	--	FEC0::2:1/112

Table 7.1.2-3 Headquarters' IP addresses

ISP 1:

Interface	IPv4 address	IPv6 address
Loopback 0	192.168.2.1/24	--
Serial 0/1/0	190.168.10.2/24	--
Serial 0/1/1	190.168.20.1/24	--

Table 7.1.2-4 ISP 1 IP addresses

Branch:

Interface	IPv4 address	IPv6 address

Loopback 0	192.168.3.1/24	FEC0::3:1/112
Serial 0/1/1	190.168.20.2/24	--
Fast Ethernet 0/0	--	FEC0:78:1:2::1/64
Tunnel 0	--	FEC0::2:2/112

Table 7.1.2-5 Branch IP addresses

7.1.3 Establish routing:

To make communication possible from Host1 to Host2, routing protocols must be established in all routers. To achieve these, two kinds of protocols were employed in a network. Those are, BGP as an Exterior gateway protocol (EGP) for public network such as Internet service provider network and Interior gateway protocol (IGP) is OSPFv3 for private network such as local connections. In particular selection of these protocols is, OSPFv3 is a link state protocol makes faster network routes merging and maintains copies of routing tables especially supports IPv6 routing. BGP is a path vector routing protocol, present widely using as EGP protocol in the Internet. Two IP protocols were employed in this scenario such as IPv4 for public networks and IPv6 for private networks. Public network was used between HQ to ISP1 and ISP1 to Br in **Figure 7.1-1**. IP addresses used for communication were in this scenario explained in above exercise (7.1.2).Private network was used to connect between HQ to Host1 & Br to Host2. In router HQ, OSPFv3 configured for IPv6 network and BGP for IPv4 network. Router ISP1 is in public network so BGP was configured. In router Br, OSPFv3 configured for IPv6 network and BGP for IPv4 network. Routing protocols were established in all routers but the incompatibility of IPv4 and IPv6 does not make communication possible from Host1 to Host2. So in this situation a smooth transition mechanism is needed to make this communication possible.

Well, **what mechanism can make this possible and how?**

As explained in **chapter 6** above 6to4 manual tunnel is one of the tunneling mechanisms. It used for encapsulate IPv6 packets into IPv4 packets in a dual stack enabled router and send over normal IPv4 routing to the end of the tunnel, node at the tunnel end is also a dual stack enabled router decapsulate IPv6 packets from IPv4 packets and delivered to according destination.

6to4 manual tunnel Process:

In Scenario1 an IPv6 packet from Host1 generated to the destination as Host2, and sent to HQ. Router HQ is a tunnel starting point that encapsulate IPv6 packet in IPv4, and sent through ISP1 over normal IPv4 routing to the end of tunnel. End of the tunnel is a router BR decapsulate the IPv6 packet from the IPv4 packet and delivered to Host2.

For configurations see **Appendix A**.

7.2 Scenario 2 (Dual Stack)

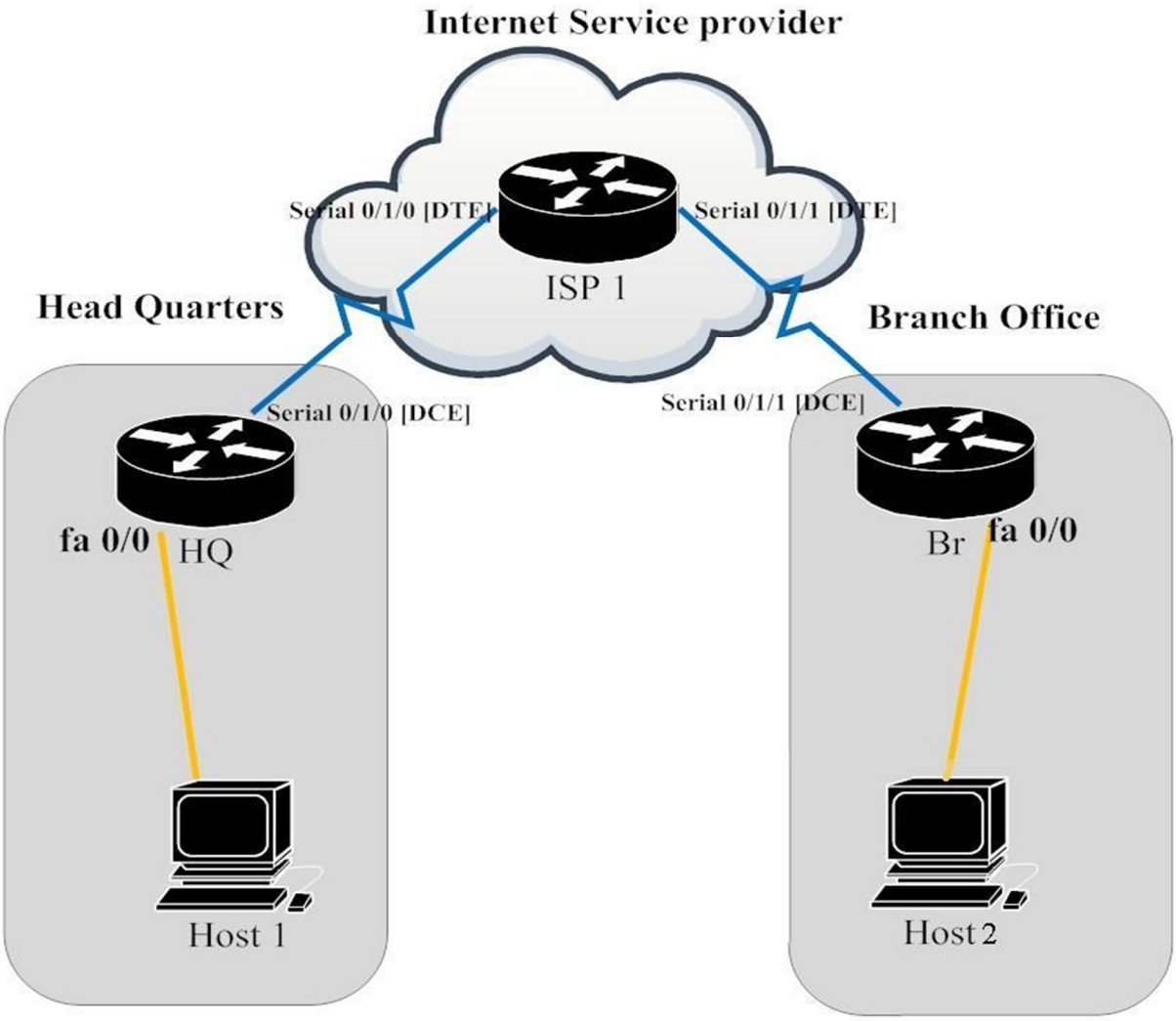


Figure 7.2-1 Dual stack network topology

7.2.1 Physical Connections:

The physical setup for Scenario 2 was done in the same way as Scenario 1.But the transition mechanism was changed.

A network has been established between headquarters (HQ) and branch office (Br) over the Internet service provider (ISP1) as shown in the figure 7.1-1. In Scenario 1 to setup a network, three routers and two clients were used. From the figure 7.1-1 Host 1 is connected to HQ interface fa0/0 with an Ethernet cable. HQ interface serial 0/1/0[DCE] was connected to ISP1 interface serial 0/1/0[DTE] with a serial cable. ISP1 interface serial 0/1/1[DTE] was connected to Br interface serial 0/1/1[DCE] with a serial cable. Br

interface fa0/0 was connected to Host2 with an Ethernet cable. This fulfill physical connectivity between headquarter to branch office.

7.2.2 IP Address Scheme:

Host 1:

	IPv4 address	IPv6 address
Ethernet	192.168.10.10/24	FEC0:78:1:1::2/64
Gateway address	192.168.10.1/24	FEC0:78:1:1::1/64

Table 7.2.2-1 Host 1 IP addresses

Host 2:

	IPv4 address	IPv6 address
Ethernet	192.168.20.20/24	FEC0:78:1:2::2/64
Gateway address	192.168.20.1/24	FEC0:78:1:2::1/64

Table 7.2.2-2 Host 2 IP addresses

Headquarter:

Interface	IPv4 address	IPv6 address
Fast Ethernet 0/0	192.168.10.1/24	FEC0:78:1:1::1/64
Serial 0/1/0	190.168.10.1/24	2001:22:1::1/48
Loopback 0	192.168.1.1/24	FEC0::1:1/112

Table 7.2.2-3 Headquarters' IP addresses

ISP 1:

Interface	IPv4 address	IPv6 address
Loopback 0	192.168.2.1/24	FEC0::2:1/112
Serial 0/1/0	190.168.10.2/24	2001:22:1::2/48
Serial 0/1/1	190.168.20.1/24	2001:22:2::1/48

Table 7.2.2-4 ISP 1 IP addresses

Branch:

Interface	IPv4 address	IPv6 address
Loopback 0	192.168.3.1/24	FEC0::3:1/112
Serial 0/1/1	190.168.20.2/24	2001:22:2::2/48
Fast Ethernet 0/0	192.168.20.1/24	FEC0:78:1:2::1/64

Table 7.2.2-5 Branch IP addresses

7.2.3 Establish routing:

In Scenario2 employed two versions of IP protocols in each router. This means in each router two protocols (IPv4 & IPv6) are running simultaneously, so each router need to have two routing protocols to support this infrastructure. Routing protocol OSPFv3 is capable of support both IPv4 and IPv6 in a single node but it classifies into two routing tables in each node. IP addresses scheme were used in this scenario explained in above exercise (7.2.2). OSPFv3 was configured in all routers (HQ, ISP1, and Br) for both IPv4 and IPv6 addresses. This enabled Dual Stack routing between nodes. Dual Stack transition mechanism was employed to support both IP protocols in the network. Dual Stack node is capable of deliver and communicates with both IPv4 & IPv6 traffic at the same time.

For configurations see **Appendix B**.

8. Results

Results are discussed about both pros and cons of Scenario 1 & 2. In implementation and also solutions for the problems analysed in the beginning, peculiar transition mechanisms were chosen such as 6to4 manual tunneling and Dual stack. Behind selection of these methods were cost-effective, smooth transition techniques between IPv4-IPv6 and easy to maintain. Both methods are possible to implement in existing network with a Dual Stack enabled node at the end. But deployment of IPv6 in the network is more beneficial.

Comparison between Scenarios 1 & 2 derives in two ways; those are Empiric results and Theoretic findings. Empiric results were explained by utilized tool name **iperf.** Results have been evaluated from both network scenarios, but did not configure any other parameters to the network such as QoS, Security, etc…

Comparison between two networks would be depending on an organisation necessity. But basic comparison between two IP network parameters for an organisation as follows:

- **Response Time:** Response Time or latency is a round trip time taken by an IP packet of data from sender to destination to sender.

- **Available bandwidth:** The available bandwidth is transferring bytes of data per second from sender to destination over network.
- **Streaming media:** Streaming media applications such are voice, video, VoIP, and IPTV encapsulates into IP packets uses UDP protocol as a transporter over network. These packets are accumulated into a jitter and jitter buffer at the receiving end.
- **Jitter:** Jitter is a time variation between packets arriving over network.

8.1 Tool "iperf" [23]

Tool iperf was developed by NLANR/DAST for measuring TCP/UDP bandwidth performance [23]. This tool reports bandwidth, delay, jitter, and datagram loss from end to end IP network scenario. License for iperf is open source [24]. The Java based Graphical user interface (GUI) for **iperf** is called **jperf** version **2.0.2.**

Functionality of jperf

Jperf is used on one endpoint with Server mode and another endpoint Client mode. The IP address (IPv4/IPv6) used to connect the Server to Client; there are several parameters to measure different kinds of traffic behaviour of TCP/UDP traffic. These were explained later in this chapter.

The quality of the connection tested as follows: [25]

- Latency : Measured with ping command (response time or RTT).
- Jitter : Measured with an iperf UDP test (latency variation).
- Datagram loss : Measured with an iperf UDP test.
- Bandwidth : Measured through TCP tests.

TCP (Transmission Control Protocol) is mostly using layer 4 protocol for network applications like HTTP, FTP and SMTP. To test TCP network performance, following options were used in jperf tool.

- **Buffer Length**: Memory allocated for send and receives traffic flow.
- **Window size**: Packets that are sent before receiving any acknowledgement. For example bits, Bytes, Kbits, Kbytes, Mbytes.
- **Max segment size (MSS)**: Quantity of data that sent in each packet. For example bits, Bytes, Kbits and Kbytes.

UDP (User Datagram Protocol) provides a process for an application program to send messages to another program. UDP is a stateless protocol used as inherent IP protocol. Common network applications DNS (Domain name server), VoIP (Voice over IP), Media application, TFTP (Trivial File Transfer Protocol) are using UDP as a transport protocol. The UDP protocol used to find jitter and datagrams loss in implemented scenarios. To test UDP network performance, following options were used in jperf tool.

- **UDP bandwidth,**
- **UDP buffer size,**
- **UDP packets size.**

8.2 Empirical results

This chapter is an explanation of empiric observations derived from Scenario 1 & 2. Basic comparisons of TCP/UDP protocols behaviour in both scenarios results have been demonstrated.

8.2.1 Ping test:

Ping is a command used for connection test between two nodes in a network. By using ping command latency between two nodes would explicate. In both scenarios ping test has been made between Host1 to Host2 for more than 100 packets. Observed results as follows:

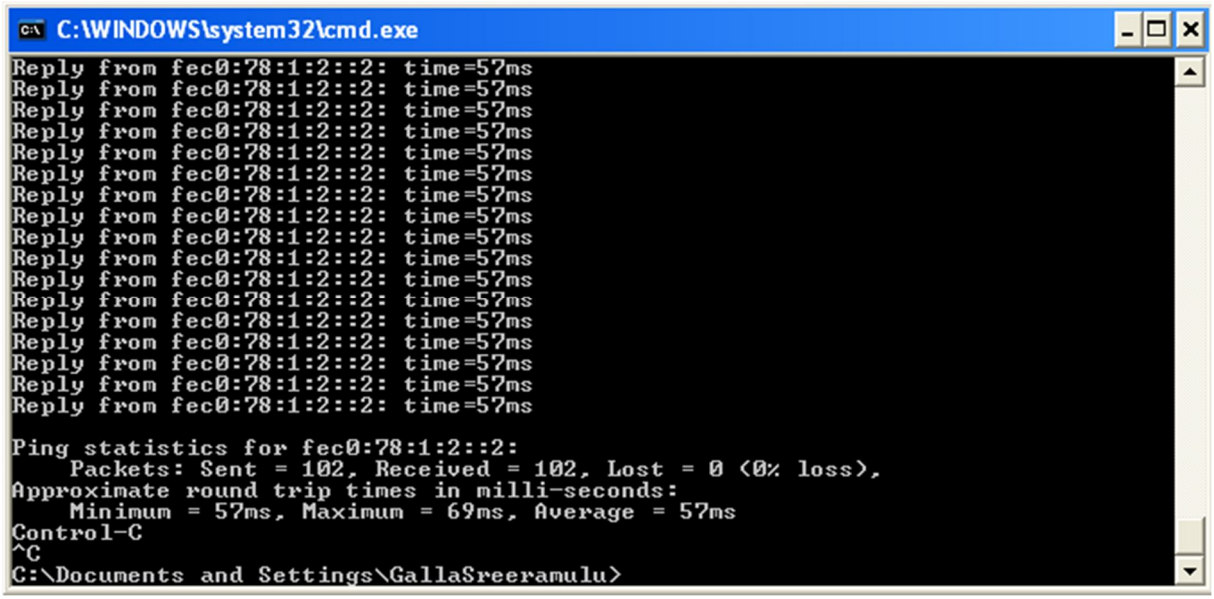


Figure 8.2.1-1 Scenario 1 ping test results.

From figure 8.2.1-1 ping test has been made in Scenario 1 between Host1 (IPv6: FEC0:78:1::2) to Host2 (IPv6: FEC0:78:2::2) to find out latency and packet loss.

Results from Scenario 1 ping test:

Source IPv6 add: FEC0:78:1::2	Destination IPv6 add: FEC0:78:2::2
Packets Sent	102
Packets Received	102
Loss	0

Table 8.2.1-1 Ping test results for Scenario 1

Latency Scenario 1 ping test:

	Latency in milliseconds
Minimum	57
Maximum	69
Average	57

Table 8.2.1-2 Latency test results for Scenario 1

Below figure 8.2.1-2 illustrate ping test in Scenario 2 between Host1 (IPv6: FEC0:78:1::2) to Host2 (IPv6: FEC0:78:2::2) to find out latency and packet loss. Ping test has been made for more than 100 packets.

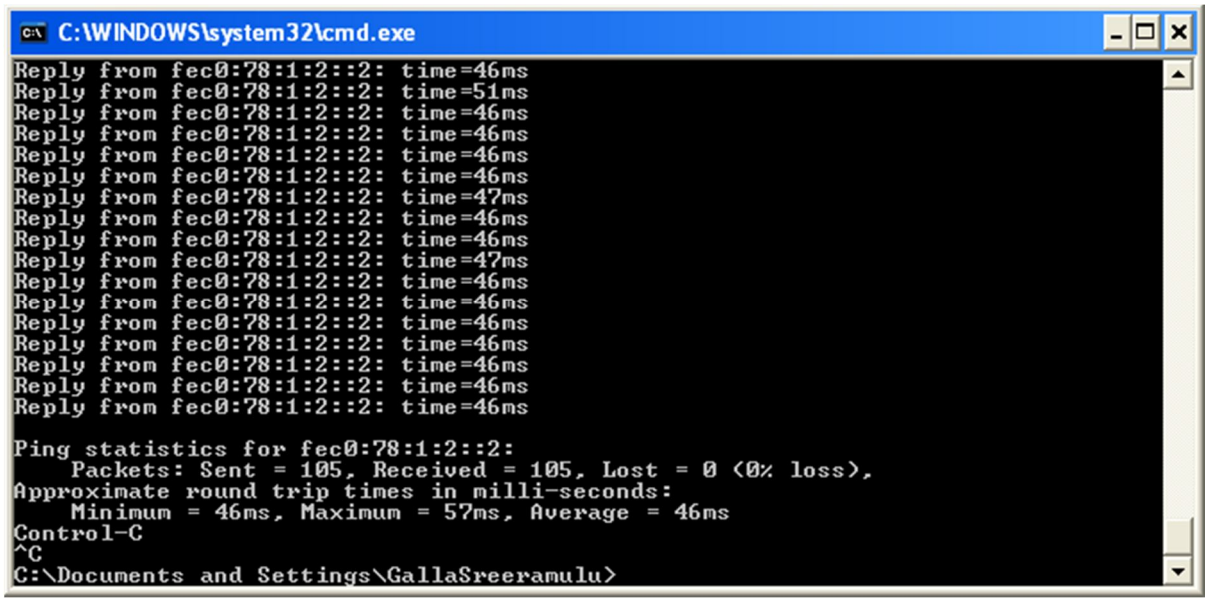


Figure 8.2.1-2 Scenario 2 ping test results.

Results from Scenario 2 ping test:

Source IPv6 add: FEC0:78:1::2	Destination IPv6 add: FEC0:78:2::2
Packets Sent	105
Packets Received	105
Loss	0

Table 8.2.1-3 Ping test results for Scenario 2

Latency Scenario 2 ping test:

	Latency in milliseconds
Minimum	46
Maximum	57

Average	46

Table 8.2.1-4 Latency test results for Scenario 2

8.2.2 Bandwidth test with TCP:

Bandwidth test was made with assistance of tool **jperf** in both Scenario 1 & 2**.** Tests have been made for TCP protocol behavior in both scenarios. General TCP window size was considered as 128 Kilobytes. In both scenarios Host1 was treated as server and Host2 was treated as client. In tool **jperf,** client generated TCP/UDP traffic and sent to server over a network. Results have been observed and illustrated below,

Scenario 1 TCP bandwidth test results

First test was made for TCP bandwidth behavior in Scenario 1. Host2 as a client and Host1 as a server listen to client by using tool **jperf**, client generates TCP traffic by using follow command in the tool jperf,

bin/iperf.exe -c FEC0:78:1:1::2 -P 1 -i 1 -p 5001 -w 128.0K -V -f k -t 10

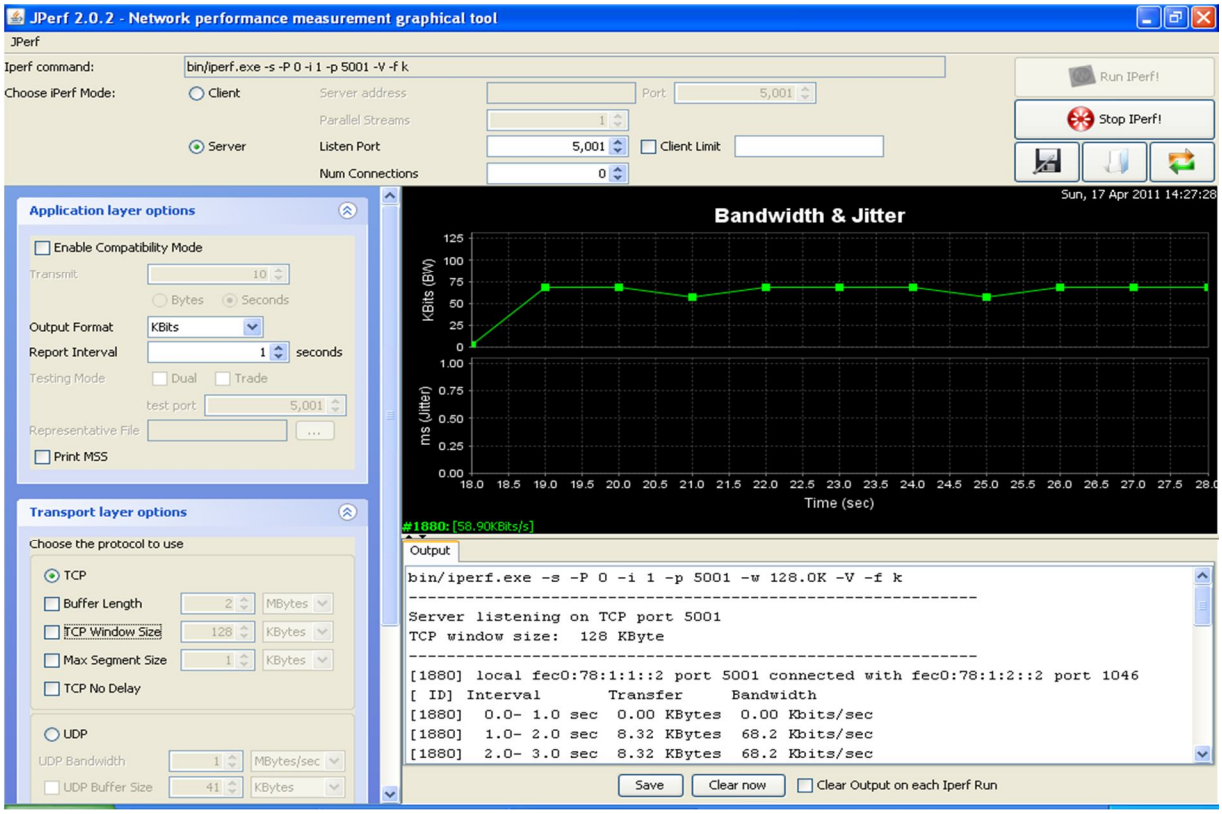


Figure 8.2.2-1 Scenario 1 TCP bandwidth test.

Server listening on TCP port 5001
TCP window size: 128 Kbyte

[1880] local fec0:78:1:1::2 port 5001 connected with fec0:78:1:2::2 port 1046

[ID] Interval Transfer Bandwidth

[1880] 0.0-28.9 sec   208 Kbytes 58.9 Kbits/sec

From the above TCP test in Scenario 1, average bandwidth received in server by the client was 58.9 Kbits/sec in between 0.0-28.9 seconds over Fast Ethernet link.

Scenario 2 TCP bandwidth test results

Test was made for TCP bandwidth behavior in Scenario 2. Host2 as a client and Host1 as a server listen to client by using tool jperf, client generates TCP traffic by using the following command in jperf,

bin/iperf.exe -c FEC0:78:1:1::2 -P 1 -i 1 -p 5001 -w 128.0K -V -f k -t 10

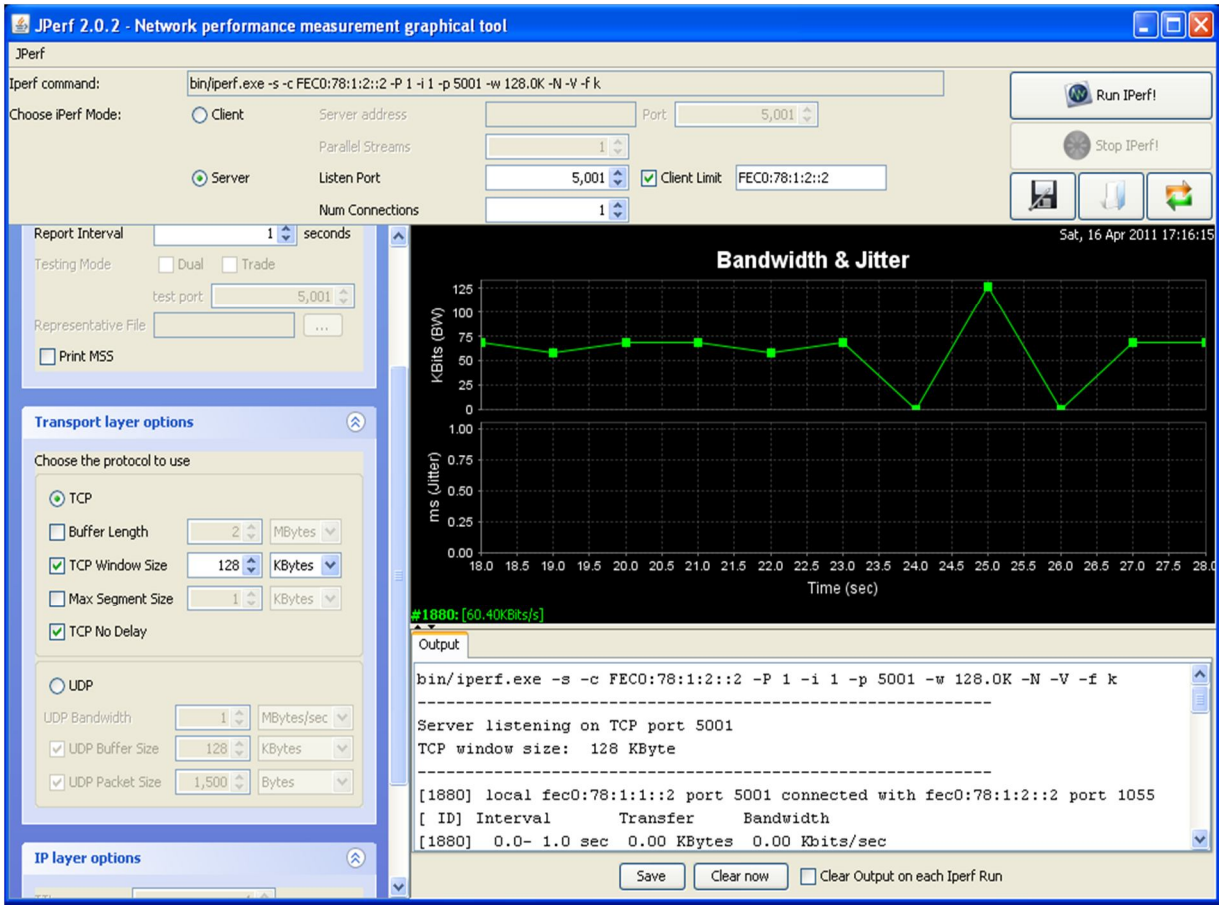


Figure 8.2.2-2 Scenario 2 TCP bandwidth test

Server listening on TCP port 5001
TCP window size: 128 Kbyte

[1880] local fec0:78:1:1::2 port 5001 connected with fec0:78:1:2::2 port 1055
[ID] Interval Transfer Bandwidth
[1880] 0.0-28.2 sec 208 Kbytes 60.4 Kbits/sec

Above table demonstrated in Scenario 2, average bandwidth received in server by the client was 60.4 Kbits/sec in between 0.0-28.2 seconds.

8.2.3 Bandwidth & Jitter test with UDP

Bandwidth & Jitter test was made with assistance of tool jperf in both Scenarios 1 & 2. Tests have been made for UDP protocol behaviour in both scenarios. General UDP window size was considered as 128 Kilobytes. In both scenarios Host1 was treated as server and Host2 was treated as client. In tool jperf, client generated TCP/UDP traffic and sent to server over a network. Results have been observed and illustrated below,

Scenario 1 UDP bandwidth & Jitter test results

For UDP traffic behavior connection was setup same way like TCP made. The results have been captured by server in the scenario. But client uses following command to generate UDP traffic,

bin/iperf.exe -c FEC0:78:1:1::2 -u -P 1 -i 1 -p 5001 -w 128.0K -V -f k -t 10

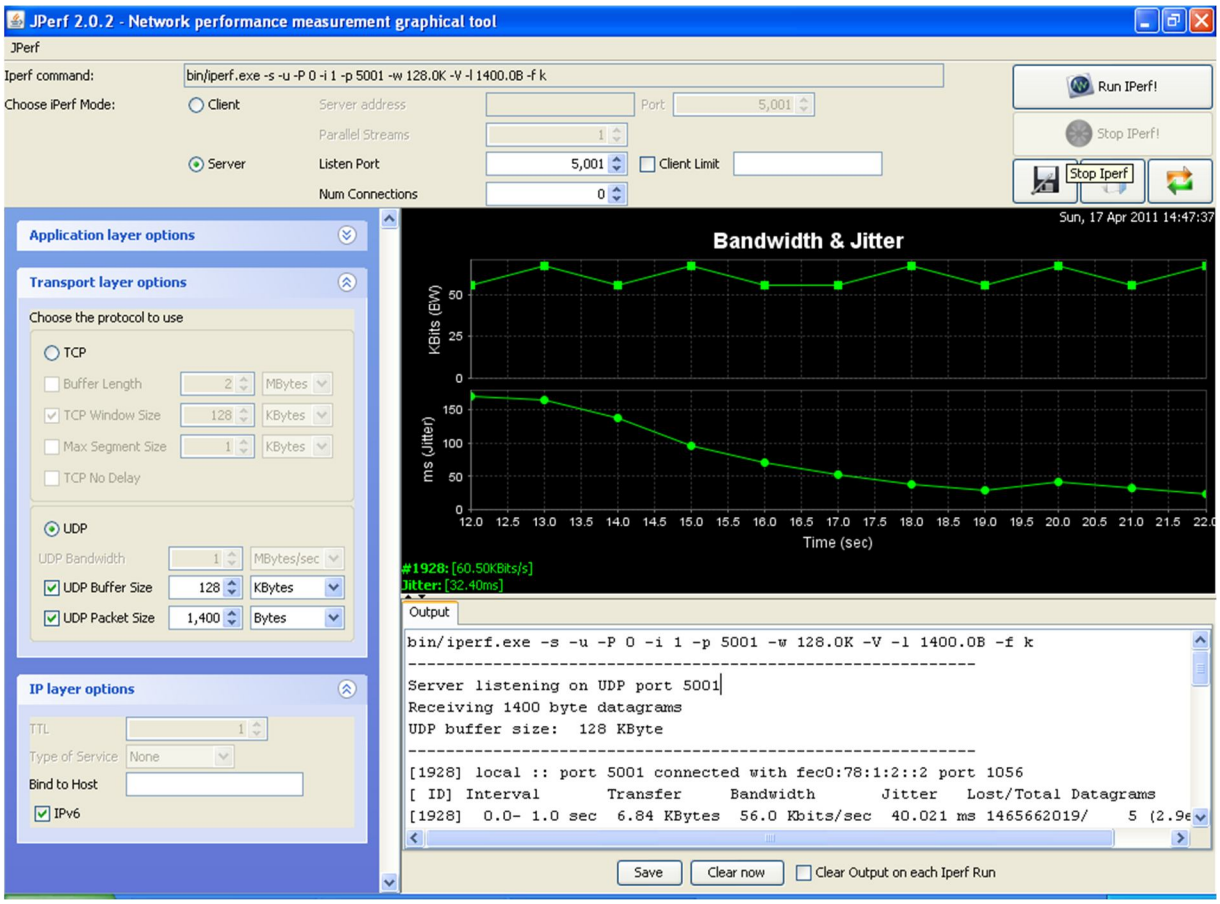


Figure 8.2.3-1 Scenario 1 UDP bandwidth & jitter test

Server listening on UDP port 5001
Receiving 1400 byte datagrams
UDP buffer size: 128 Kbyte

[1928] local :: port 5001 connected with fec0:78:1:2::2 port 1056
[ID] Interval Transfer Bandwidth Jitter
[1928] 0.0-22.2 sec 164 Kbytes 60.5 Kbits/sec 32.401 ms

From the above UDP test in Scenario 1, average bandwidth was 60.5 Kbits/sec and jitter was 32.401 ms were received in server by the client in between 0.0-22.2 seconds over Fast Ethernet link.

Scenario 2 UDP bandwidth & Jitter test results

Test was made for UDP bandwidth behavior in Scenario 2. Host2 as a client and Host1 as a server listen to client by using tool jperf, client generates UDP traffic by using the following command in jperf,

bin/iperf.exe -c FEC0:78:1:1::2 -P 1 -i 1 -p 5001 -w 128.0K -V -f k -t 10

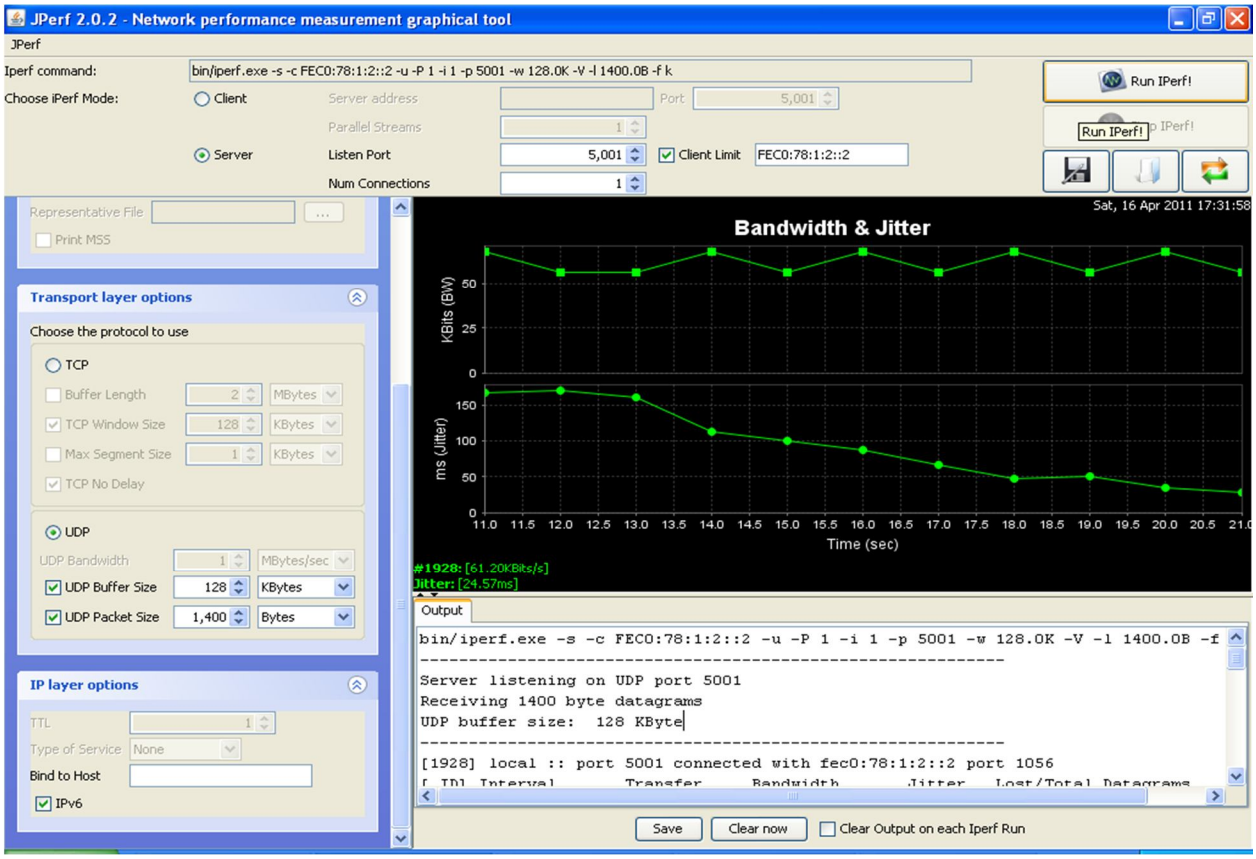


Figure 8.2.3-1 Scenario 1 UDP bandwidth & jitter test

```
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1400 byte datagrams
UDP buffer size:  128 Kbyte
------------------------------------------------------------
[1928] local :: port 5001 connected with fec0:78:1:2::2 port 1056
[ ID]      Interval          Transfer          Bandwidth          Jitter
[1928]  0.0-22.0 sec        164 Kbytes        61.2 Kbits/sec     24.574 ms
```

Above table demonstrated in Scenario 2, average bandwidth 61.2 Kbits and jitter 24.574 ms were received in server by the client in between 0.0-22.0 seconds.

8.3 Theoretic findings

Theoretic findings are about some pros and cons of both transition mechanisms such are Dual Stack and 6to4 manual tunneling. In this section basic security issues also expressed.

Pros & cons of Dual stack mechanism: [27(a)][27(b)]

Advantages:

- Native Dual Stack does not require any tunneling mechanism on internal network.
- Both IPv4 and IPv6 run independent of each other.
- This mechanism is easy to use and can be implemented in both end system of network node.

Disadvantages: [27(b)]

- Both ends routers must support dual stack protocols.
- Dual stack node need additional CPU power and memory, because of two separate protocol stacks run in the same node.
- All the tables are kept twice because of one per protocol stack.
- Routing protocol must deal with both IPv4 and IPv6.

Pros & cons of 6to4 manual tunneling mechanism: [28]

Advantages:

- Manual tunneling is simple and stable.
- Manual tunnels are secured than other tunneling mechanisms.

Disadvantages:

- Tunnels have to configure both source and destination addresses of tunnel manually.
- Routers at both end of tunnel must support dual stack protocols.
- Communication could be possible between two edge nodes.

- This type of tunnels are not very scalable so only suitable for permanent link.
- Tunnels carry IPv6 packets only.

8.3.1 Security Issues:

Security Issues on Dual Stack: [29(a)]

An organization may have to tackle the vulnerabilities of IPv6 and IPv4 protocols that run Dual Stack. As well as others security problems if security policies are not created for both protocols for example if a firewall is not configured to IPv6 and IPv4 packets, the firewall may let pass IPv6 through to dual stack hosts within the network, potentially exposing them to attack. When using dual-stack techniques, make sure that there is firewall in place that protect not only IPv4 network but also IPv6 network, and needs separate security concepts and firewall rules for each protocol.

Security Issues on Manual Tunneling:

A manually configured tunnel is most stable because of administrator configured tunnel manually to the particular point, and more secured because of encapsulation of IP packets over the network. But packet spoofing and encapsulates a malware into IP packet send over network are problems may face by tunneling network.

8.3.2 IPv6 Security Consideration: [30(a)][30(b)]

The IPv6 protocol solved some security problems found in IPv4. For example IPsec is mandatory in IPv6 but still there are other security problems that must be able to handle for secure networks. When deploying IPv6 in a network administrator must concerns about following threats.

Authorization for automatically assigned address and configurations:

To prevent unauthorized computers from communicating on private networks we can use IEEE 802.1X authentication at the link layer so that the computers can’t send any traffic until they have authenticated themselves.

Protection of IP packets:

IPsec is used to prevent IP packets from tampering and provide security from end-to-end communications at the network layer. IPsec prevent the IP packets by providing data origin authentication, access control, data integrity and confidentiality.

Control of traffic Exchange with Network:

Firewalls were used to prevent unwanted and unauthorized traffic in IPv6 network.

IP Spoofing in IPv6 Network:

IP spoofing is the creation of IP packets with a fake (spoofed) source IP address. IP

spoofing is frequently used in Denial-of-Service (DoS) attack. A host using IPv6 have multiple addresses and IPv6 and IPv4 interconnections network will likely face spoofing problems.
Solution: Packet filtering prevents an outside attacker against spoofing the source address.

IPv6 Routing Attacks:

The purpose of routing attack is to corrupt routing information in order to cause DoS attack.
Solution: In case of BGP, EIGRP and IS-IS use protocol authentication keyed MD5 digest. For OSPFv3 and RIPng configure IPsec.

Application Layer Attacks:

This is the common attack against computer system at layer 7. To prevent this type of attack operators must update their systems.

Denial of Service (DoS) Attacks:

Flooding attacks are same as between IPv4 and IPv6 and preventing from this attack requires DoS detection tools, which can analyse IPv6 communication flows. If the communication is authenticated by IPsec the DoS packets are not delivered to final destination.

8.4 Possible scenarios between two transition mechanisms

Below table demonstrates possible scenarios of stake holders between two transition mechanisms, those are Dual Stack and manual tunneling.

Stake holders	**Manual Tunnel**	**Dual Stack**
Home users	**No**	**Yes**
Enterprise Networks	**Yes**	**Yes**
Web hosting providers	**Yes**	**Yes**
Data centres	**Yes**	**Yes**
Internet Service Provider	**Yes**	**Yes**

Table 8.4-1 demonstrating possible scenarios

9. IT-Strategic Consideration

The strategic consideration of IPv6 plays a significant role for an organization that is considering to the deployment of IPv6. For a small organization transition to IPv6 may not be a big problem but for larger organizations it can be complex

and difficult task so various kind of issues should be consider in the preparation. It must be well planned before implement the transition method for successful deployment of IPv6 and to maximize the return of investment (ROI). A strategic plan and following issues are useful for an organization to implement IPv6.

Strategic issues: [22(a)][22(b)]

- Before implementing the transition mechanism an organization must investigate how IPv6 would affect their services including new applications.
- An organization has to identify the strategic advantages of deploying IPv6 as well as its benefits, risks and implementation costs.
- Inventory of the equipment and application that support IPv6 or not. If the equipment does not support must be upgrade.
- Understand and develop an addressing plan and requirements.
- An organization must understand about IPv6 routing infrastructure for example what changes are requires to add in current routing infrastructure to support IPv6.
- Well plan that how their organization interconnects with other organizations.
- Understand about different kinds of transition mechanisms and select the mechanism that support and run smoothly on their network infrastructure.
- An organization must plan about security policy and threats that may exist.
- Train an employee about IPv6 in an organization to make better utilization of IPv6 services and error handling methods.
- An organization has to consider about the goals, path and timeline for the reliable and scalable infrastructure.

Conclusion

IPv6 overcomes many of the limitations over IPv4 with new features and functionalities. It has been designed to support smooth transition with IPv4. The combination of CIDR and NAT mechanisms has assisted to reduce IPv4 address exhaustion time; However NAT breaks the end to end IP model so it has many limitations for protocols. IPv6 larger address space provides more unique globally unicast addresses for the present and future Internet growth. Fully deployment of IPv6 needs upgrading of applications, hosts, routers and DNS to support IPv6, might be expensive and deployment takes many years. At this situation transition mechanisms are one of the best solutions, so this makes IPv6 & IPv4 networks run in the same infrastructure. IPv4 to IPv6 several transition mechanisms have been developed for according to different organization needs. This report discussed and compared between Dual Stack and 6to4 manually tunneling mechanisms. Both mechanisms have their own advantages and disadvantages in different Infrastructure. Dual Stack transition mechanism is the most common and straightforward way for IPv6 & IPv4 nodes to communicates with IPv6 & IPv4 nodes independently without changing the network. Dual stack is suitable for Internet Service Providers (ISPs), Enterprises networks as well as Home users. On the other hand manual tunnels are configured between two IPv6 networks over IPv4 network infrastructure, Manual tunnel is a secure mechanism in compared to other transition mechanisms. This mechanism is suitable for ISPs, Enterprises networks, Data center but not for Home users. Based on report we concluded that the transition mechanisms fulfill the problems of future Internet growth but selection of transition mechanism is depends on infrastructure, security issues, budget, advantages and disadvantages of the mechanism to an organization.

References

[1] Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6), Edited by: Regis Desmeules.

[2] Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporate Networks, By John J. Amoss & Daniel Minoli.

[3]Internet Protocol Version 6 (IPv6) specifications, RFC2460 by S.Deering & R.Hinden

[4]IPv6 Deployment around the World, source: http://ipv6.com/articles/deployment/IPv6-Deployment-Status.htm by Kausik das Accessed on 5/2011.

[5] Classless interdomain routing (CIDR), source: http://tools.ietf.org/html/rfc4632

by V.Fuller and T.Li.

[6] Network Address Translator (NAT), source: http://www.ietf.org/rfc/rfc1631.txt By K.Egevang and P.Fransis.

[7] Internet protocol version 4 source: http://www.faqs.org/rfcs/rfc791.html by

Wilson Defense Advanced Research Projects Agency, Virginia.

And

Information Sciences Institute University of Southern California, California.

[8] IPv4 Header ; source : http://www.cisco.com/web/about/security/intelligence/ttl-expiry.html

[9] RIPng, source: http://tools.ietf.org/html/rfc2080

[10] EIGRP for IPv6 source: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp.html

[11] EIGRP for IPv6 source: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80260051.pdf

[12] OSPFv3 source: http://tools.ietf.org/html/rfc2740

[13] IS-IS source: http://tools.ietf.org/html/rfc1195

[14] IPv4 addressing, source:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml

[15] IPv6 Addressing, source: http://tools.ietf.org/pdf/rfc4291.pdf

[16] IPv6 addressing, source
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/BN_Enterprise_IPv6_Addressing_Guide_H2CY10.pdf

[17] Types of nodes with respect to IPv6 ;

source: https://www.ietf.org/rfc/rfc4294.txt

[18] Dual Stack transition mechanism: source: IEEE an IPv4-to-IPv6 Dual Stack Transition Mechanism Supporting Transparent Connections between IPv6Hosts and IPv4 Hosts in Integrated IPv6/IPv4 Network 013132656;

By Eun-Young Park, Jae-Hwoon Lee and Byoung-Gu Choe.

[19] IPv6 supporting Operating systems ;source http://ipv6int.net/systems/index.html

[20] Tunneling mechanism (IPv6 Deployment Guide); source:
http://www.6net.org/book/deployment-guide.pdf

[21] Deploy IPv6 (A great tutorials for basic information about IPv6)
http://www.6deploy.org/e-learning/english/

[22]IT-strategy of deploying IPv6, source,
a) http://www.commandinformation.com/research/ipv6_top10.html
b) http://www.cisco.com/web/partners/pr67/pr41/docs/C11-439724-00_PlanningandAccomplishingtheIPv6Integration_v2.pdf
[23] ipref tool , Source : http://code.google.com/p/iperf/

[24] Open Source Initiative OSI – The BSD licensing, Source:
http://www.opensource.org/licenses/bsd-license.php

[25] jperf tool, source : http://openmaniak.com/iperf.php

[26] IPv6 installation on windows machine, source:

a) http://msdn.microsoft.com/en-us/windows/hardware/gg463251.aspx

b) http://msdn.microsoft.com/en-us/library/bb736546(v=vs.85).aspx

[27] Pros & cons of Dual Stack, source:
a)http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/at_a_glance_c45-625859.pdf

b) http://e-articles.info/e/a/title/IPv4-vs-IPv6:-Comparison/

[28] Pros & cons of 6to4 manual tunnels, source:

http://www.ipv6vsipv4.com/manual.html
[29] Security issues of tunneling mechanisms, source:

a) http://www.brucert.org.bn/files/IPv6-to IPv4%20Transition%20&%20Security%20Issues.pdf

[30] IPv6 Security considerations, Source:

a) http://www.6net.org/book/deployment-guide.pdf (IPv6 Deployment Guide)

b) http://technet.microsoft.com/en-us/library/bb726956.aspx

Appendix A: -

It is a reference configuration of Scenario 1 6to4 tunneling method.

Router HQ

HQ#*showrun*

hostname HQ

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

resource policy

!

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

ip subnet-zero

!

!

ipv6 unicast-routing

```
!
voice-card 0
!
!
!
interface Tunnel0
 no ip address
 ipv6 address FEC0::2:1/112
 ipv6 ospf 64512 area 0
 tunnel source Serial0/1/0
 tunnel destination 190.168.20.2
 tunnel mode ipv6ip
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FEC0::1:1/112
 ipv6 ospf 64512 area 0
!
interface FastEthernet0/0
 no ip address
 duplex auto
ipv6 address FEC0:78:1:1::1/64
 ipv6 ospf 64512 area 1
!
interface FastEthernet0/1
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 190.168.10.1 255.255.255.0
 clock rate 64000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router bgp 64000
 bgp log-neighbor-changes
 neighbor 190.168.10.2 remote-as 64000
 !
 address-family ipv4
 neighbor 190.168.10.2 activate
 no auto-summary
 no synchronization
 network 190.168.10.0 mask 255.255.255.0
 exit-address-family
!
ip classless
!
!
ip http server
```

```
no ip http secure-server
!
ipv6 router ospf 64512
 log-adjacency-changes
 area 0 range FEC0::/64
 area 1 range FEC0:78:1:1::/64
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces details

HQ#*show ip interface brief*

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/1/0	190.168.10.1	YES	manual	up	up
Serial0/1/1	unassigned	YES	manual	administratively down	down
Loopback0	192.168.1.1	YES	manual	up	up
Tunnel0	unassigned	YES	manual	up	up

IPv6 Interfaces details

HQ#*show ipv6 interface brief*

FastEthernet0/0 [up/up]

FE80::224:C4FF:FE46:F556

FEC0:78:1:1::1

FastEthernet0/1 [administratively down/down]

Serial0/1/0 [up/up]

Serial0/1/1 [administratively down/down]

Loopback0 [up/up]

FE80::224:C4FF:FE46:F556

FEC0::1:1

Tunnel0 [up/up]

FE80::224:C4FF:FE46:F556

FEC0::2:1

IPv4 Routing Details:

HQ#sh ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

B 190.168.20.0 [200/0] via 190.168.10.2, 01:23:41

C 190.168.10.0 is directly connected, Serial0/1/0

C 192.168.1.0/24 is directly connected, Loopback0

IPv6 Routing Details:

HQ#sh ipv6 route

IPv6 Routing Table - 11 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

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 FE80::/10 [0/0]

via ::, Null0

O FEC0::/64 [110/0]

via ::, Null0

C FEC0::1:0/112 [0/0]

via ::, Loopback0

L FEC0::1:1/128 [0/0]

via ::, Loopback0

C FEC0::2:0/112 [0/0]

via ::, Tunnel0

L FEC0::2:1/128 [0/0]

via ::, Tunnel0

O FEC0::3:1/128 [110/11111]

via FE80::BEA8:1402, Tunnel0

C FEC0:78:1:1::/64 [0/0]

via ::, FastEthernet0/0

L   FEC0:78:1:1::1/128 [0/0]

via ::, FastEthernet0/0

OI FEC0:78:1:2::/64 [110/11112]

    via FE80::BEA8:1402, Tunnel0

L   FF00::/8 [0/0]

    via ::, Null0

Router ISP1

ISP1#*showrun*

hostname ISP1

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

resource policy

!

memory-size iomem 5

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

ip subnet-zero

ip cef

```
!
voice-card 0
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 190.168.10.2 255.255.255.0
!
interface Serial0/1/1
ip address 190.168.20.1 255.255.255.0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 network 190.168.10.0 mask 255.255.255.0
 network 190.168.20.0 mask 255.255.255.0
```

```
 network 192.168.10.0
 network 192.168.20.0
 neighbor 190.168.10.1 remote-as 64000
 neighbor 190.168.20.2 remote-as 64000
 no auto-summary
!
ip classless
!
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces details

```
HQ#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/1/0            190.168.10.2    YES manual up                    up
Serial0/1/1            190.168.20.1    YES manual up                    up
```

IPv6 Interfaces details

HQ#show ipv6 interface brief

FastEthernet0/0 [administratively down/down]

FastEthernet0/1 [administratively down/down]

Serial0/1/0 [up/up]

Serial0/1/1 [up/up]

ISP1#show ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

C 190.168.20.0 is directly connected, Serial0/1/1

C 190.168.10.0 is directly connected, Serial0/1/0IPv4 Routing Details

IPv6 Routing Details

ISP1#show ipv6 route

IPv6 Routing Table - 0 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

Router Br

Br#*showrun*

hostname Br

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

resource policy

!

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

ip subnet-zero

ip cef

!

ipv6 unicast-routing

!

voice-card 0

!

```
interface Tunnel0
 no ip address
 ipv6 address FEC0::2:2/112
 ipv6 ospf 64513 area 0
 tunnel source Serial0/1/1
 tunnel destination 190.168.10.1
 tunnel mode ipv6ip
!
interface Loopback0
 ip address 192.168.3.1 255.255.255.0
 ipv6 address FEC0::3:1/112
 ipv6 ospf 64513 area 0
!
interface FastEthernet0/0
 no ip address
 duplex auto
speed auto
 ipv6 address FEC0:78:1:2::1/64
 ipv6 ospf 64513 area 1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
```

```
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/1/1
 ip address 190.168.20.2 255.255.255.0
 clock rate 64000
!
router bgp 64000
 bgp log-neighbor-changes
 neighbor 190.168.20.1 remote-as 64000
address-family ipv4
 neighbor 190.168.20.1 activate
 no auto-summary
 no synchronization
 network 190.168.20.0
 network 192.168.10.0
 exit-address-family
!
ip classless
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 64513
```

```
 log-adjacency-changes
 area 0 range FEC0::/64
 area 1 range FEC0:78:1:2::/64
!
ipv6 router ospf 64512
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces details

```
Br#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/1/0            unassigned      YES manual administratively down down
Serial0/1/1            190.168.20.2    YES manual up                    up
Loopback0              192.168.3.1     YES manual up                    up
Tunnel0                unassigned      YES manual up                    up
```

IPv6 Interfaces details

```
Br#show ipv6 interface brief
FastEthernet0/0        [up/up]
```

FE80::224:C4FF:FE62:7246

FEC0:78:1:2::1

FastEthernet0/1 [administratively down/down]

Serial0/1/0 [administratively down/down]

Serial0/1/1 [up/up]

Loopback0 [up/up]

FE80::224:C4FF:FE62:7246

FEC0::3:1

Tunnel0 [up/up]

FE80::BEA8:1402

FEC0::2:2

IPv4 Routing Details

Br#show ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

C 190.168.20.0 is directly connected, Serial0/1/1

B 190.168.10.0 [200/0] via 190.168.20.1, 01:28:02

C 192.168.3.0/24 is directly connected, Loopback0

IPv6 Routing Details

Br#show ipv6 route

IPv6 Routing Table - 11 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

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 FE80::/10 [0/0]

via ::, Null0

O FEC0::/64 [110/0]

via ::, Null0

O FEC0::1:1/128 [110/11111]

via FE80::224:C4FF:FE46:F556, Tunnel0

C FEC0::2:0/112 [0/0]

via ::, Tunnel0

L FEC0::2:2/128 [0/0]

via ::, Tunnel0

C FEC0::3:0/112 [0/0]

via ::, Loopback0

L FEC0::3:1/128 [0/0]

via ::, Loopback0

OI FEC0:78:1:1::/64 [110/11112]

via FE80::224:C4FF:FE46:F556, Tunnel0

C FEC0:78:1:2::/64 [0/0]

via ::, FastEthernet0/0

L FEC0:78:1:2::1/128 [0/0]

via ::, FastEthernet0/0

L FF00::/8 [0/0]

via ::, Null0

Host 1

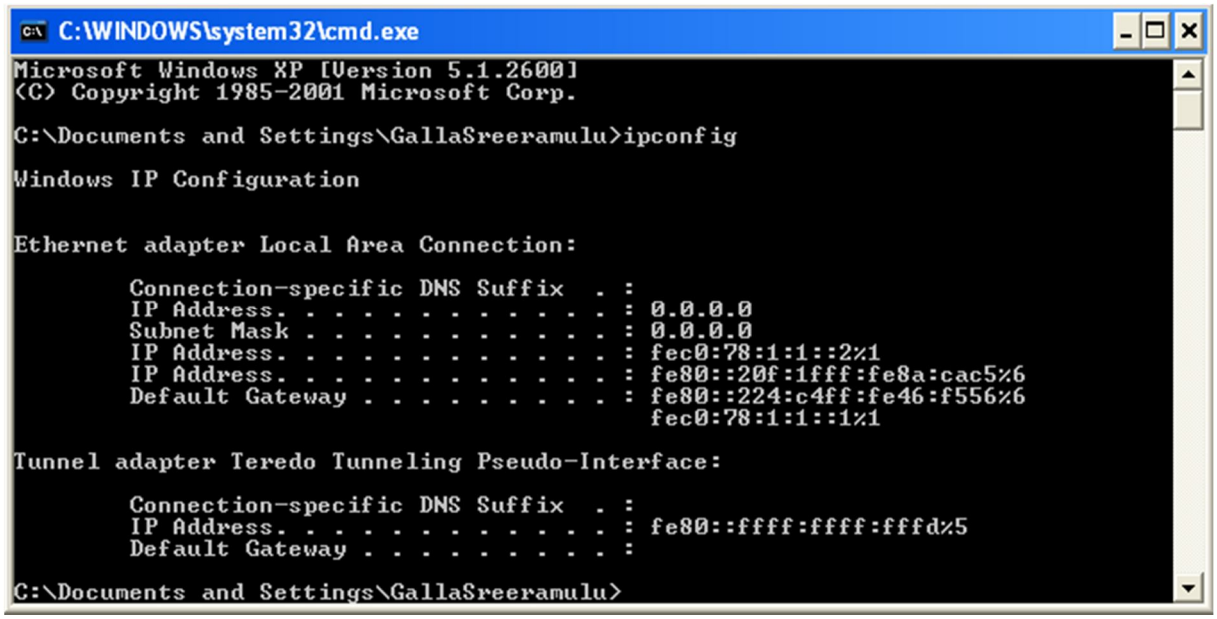


Figure 1.1-A Host 1 IP Address

Host 2

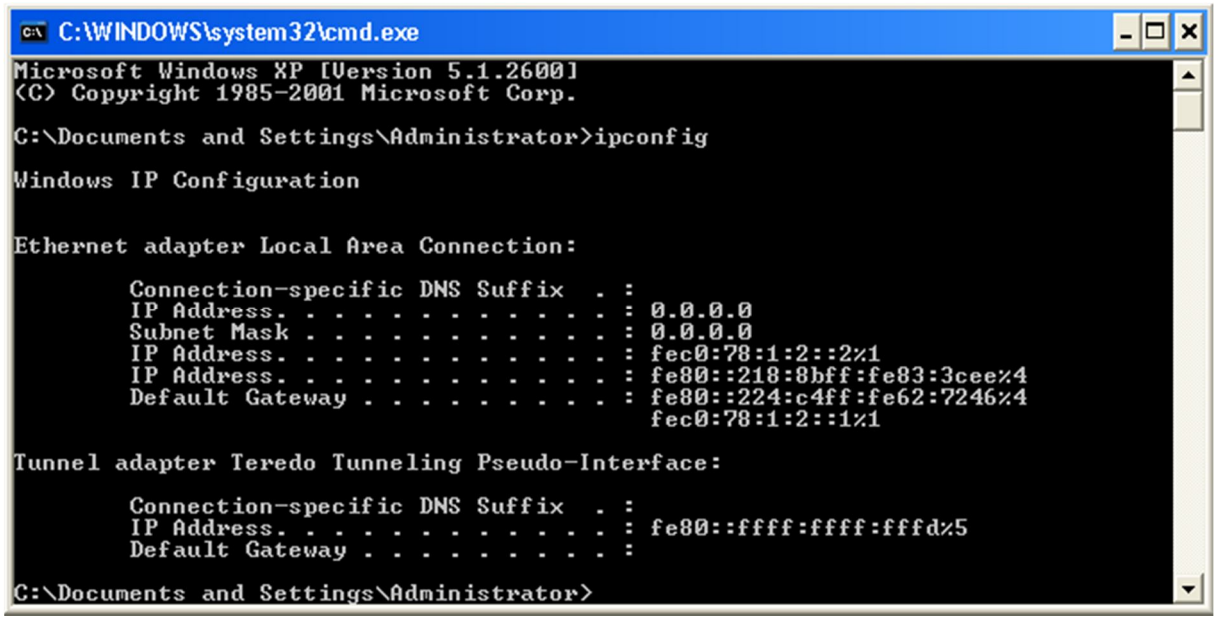


Figure 1.2-A Host 1 IP Address

Appendix B: -

It is a reference configuration of Scenario 2 Dual stack method.

Router HQ

HQ#showrun

hostname HQ

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

resource policy

!

mmi polling-interval 60

```
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
 ip cef
!
ipv6 unicast-routing
!
voice-card 0
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FEC0::1:1/112
 ipv6 ospf 64512 area 0
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FEC0:78:1:1::1/64
 ipv6 ospf 64512 area 1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial0/1/0
 ip address 190.168.10.1 255.255.255.0
 ipv6 address 2001:22:1::1/48
 ipv6 ospf 64512 area 0
 clock rate 64000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 64512
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 190.168.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 1
!
ip classless
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 64512
 log-adjacency-changes
```

```
 area 0 range 2001:22:1::/48
 area 0 range FEC0::/112
 area 1 range FEC0:78:1:1::/64
 passive-interface FastEthernet0/0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces Details:

```
HQ#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/1/0            190.168.10.1    YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Loopback0              192.168.1.1     YES manual up                    up
```

IPv6 Interfaces Details:

```
HQ#show ipv6 int brief
FastEthernet0/0        [up/up]
    FE80::224:C4FF:FE46:F556
    FEC0:78:1:1::1
```

FastEthernet0/1 [administratively down/down]

Serial0/1/0 [up/up]

FE80::224:C4FF:FE46:F556

2001:22:1::1

Serial0/1/1 [administratively down/down]

Loopback0 [up/up]

FE80::224:C4FF:FE46:F556

FEC0::1:1

IPv4 Routing Details:

HQ#show ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

O 190.168.20.0 [110/845] via 190.168.10.2, 03:26:05, Serial0/1/0

C 190.168.10.0 is directly connected, Serial0/1/0

C 192.168.10.0/24 is directly connected, FastEthernet0/0

O IA 192.168.20.0/24 [110/846] via 190.168.10.2, 03:26:05, Serial0/1/0

C 192.168.1.0/24 is directly connected, Loopback0

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/65] via 190.168.10.2, 03:26:05, Serial0/1/0

192.168.3.0/32 is subnetted, 1 subnets

O 192.168.3.1 [110/846] via 190.168.10.2, 03:26:05, Serial0/1/0

IPv6 Routing Details:

HQ#show ipv6 route

IPv6 Routing Table - 13 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

C 2001:22:1::/48 [0/0]

via ::, Serial0/1/0

L 2001:22:1::1/128 [0/0]

via ::, Serial0/1/0

O 2001:22:2::/48 [110/845]

via FE80::224:C4FF:FE46:F358, Serial0/1/0

O 2001:22:2::/64 [110/909]

via FE80::224:C4FF:FE46:F358, Serial0/1/0

L FE80::/10 [0/0]

via ::, Null0

C FEC0::1:0/112 [0/0]

via ::, Loopback0

L   FEC0::1:1/128 [0/0]

    via ::, Loopback0

O   FEC0::3:1/128 [110/845]

    via FE80::224:C4FF:FE46:F358, Serial0/1/0

O   FEC0::4:1/128 [110/64]

   via FE80::224:C4FF:FE46:F358, Serial0/1/0

C   FEC0:78:1:1::/64 [0/0]

    via ::, FastEthernet0/0

L   FEC0:78:1:1::1/128 [0/0]

    via ::, FastEthernet0/0

OI FEC0:78:1:2::/64 [110/846]

    via FE80::224:C4FF:FE46:F358, Serial0/1/0

L   FF00::/8 [0/0]

    via ::, Null0

Router ISP1

ISP1#*showrun*

hostname ISP1

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

```
resource policy
!
memory-size iomem 5
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
ipv6 unicast-routing
!
voice-card 0
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address FEC0::4:1/112
 ipv6 ospf 64000 area 0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
speed auto
!
interface Serial0/1/0
 ip address 190.168.10.2 255.255.255.0
 ipv6 address 2001:22:1::2/48
 ipv6 ospf 64000 area 0
!
interface Serial0/1/1
 ip address 190.168.20.1 255.255.255.0
 ipv6 address 2001:22:2::1/48
 ipv6 ospf 64000 area 0
!
router ospf 64000
 log-adjacency-changes
 network 190.168.10.0 0.0.0.255 area 0
 network 190.168.20.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
ip classless
!
!
ip http server
no ip http secure-server
ipv6 router ospf 64000
 log-adjacency-changes
```

```
 area 0 range 2001:22:1::/48
 area 0 range 2001:22:2::/48
 area 0 range FEC0::/112
!
control-plane

!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces Details:

```
ISP1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/1/0            190.168.10.2    YES manual up                    up
Serial0/1/1            190.168.20.1    YES manual up                    up
Loopback0              192.168.2.1     YES manual up                    up
```

IPv6 Interfaces Details:

```
ISP1#show ipv6 interface brief
FastEthernet0/0        [administratively down/down]
FastEthernet0/1        [administratively down/down]
```

Serial0/1/0 [up/up]

FE80::224:C4FF:FE46:F358

2001:22:1::2

Serial0/1/1 [up/up]

FE80::224:C4FF:FE46:F358

2001:22:2::1

Loopback0 [up/up]

FE80::224:C4FF:FE46:F358

FEC0::4:1

IPv4 Routing Details:

ISP1#show ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

C 190.168.20.0 is directly connected, Serial0/1/1

C 190.168.10.0 is directly connected, Serial0/1/0

O IA 192.168.10.0/24 [110/782] via 190.168.10.1, 03:31:30, Serial0/1/0

O IA 192.168.20.0/24 [110/782] via 190.168.20.2, 03:31:30, Serial0/1/1

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/782] via 190.168.10.1, 03:31:30, Serial0/1/0

C 192.168.2.0/24 is directly connected, Loopback0

192.168.3.0/32 is subnetted, 1 subnets

O 192.168.3.1 [110/782] via 190.168.20.2, 03:31:30, Serial0/1/1

IPv6 Routing Details:

ISP1#show ipv6 route

IPv6 Routing Table - 13 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

C 2001:22:1::/48 [0/0]

via ::, Serial0/1/0

L 2001:22:1::2/128 [0/0]

via ::, Serial0/1/0

C 2001:22:2::/48 [0/0]

via ::, Serial0/1/1

O 2001:22:2::/64 [110/845]

via FE80::224:C4FF:FE62:7246, Serial0/1/1

L 2001:22:2::1/128 [0/0]

via ::, Serial0/1/1

L FE80::/10 [0/0]

via ::, Null0

O FEC0::1:1/128 [110/781]

via FE80::224:C4FF:FE46:F556, Serial0/1/0

O FEC0::3:1/128 [110/781]

via FE80::224:C4FF:FE62:7246, Serial0/1/1

C FEC0::4:0/112 [0/0]

via ::, Loopback0

L FEC0::4:1/128 [0/0]

via ::, Loopback0

OI FEC0:78:1:1::/64 [110/782]

via FE80::224:C4FF:FE46:F556, Serial0/1/0

OI FEC0:78:1:2::/64 [110/782]

via FE80::224:C4FF:FE62:7246, Serial0/1/1

L FF00::/8 [0/0]

via ::, Null0

Router Br

Br#*showrun*

hostname Br

!

boot-start-marker

boot-end-marker

!

```
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
ipv6 unicast-routing
!
voice-card 0
!
!
interface Loopback0
 ip address 192.168.3.1 255.255.255.0
 ipv6 address FEC0::3:1/112
 ipv6 ospf 64513 area 0
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FEC0:78:1:2::1/64
```

```
 ipv6 ospf 64513 area 1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/1/1
 ip address 190.168.20.2 255.255.255.0
 ipv6 address 2001:22:2::2/64
 ipv6 ospf 64513 area 0
 clock rate 64000
!
router ospf 64513
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 190.168.20.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 1
!
```

```
ip classless
!
ip http server
no ip http secure-server
!
ipv6 router ospf 64513
 log-adjacency-changes
 area 0 range 2001:22:2::/48
 area 0 range FEC0::/112
 area 1 range FEC0:78:1:2::/64
 passive-interface FastEthernet0/0
!

control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

IPv4 Interfaces Details:

```
Br#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.20.1    YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/1/0                unassigned      YES unset  administratively down down
```

Serial0/1/1 190.168.20.2 YES manual up up

Loopback0 192.168.3.1 YES manual up up

IPv6 Interfaces Details:

Br#show ipv6 interface brief

FastEthernet0/0 [up/up]

FE80::224:C4FF:FE62:7246

FEC0:78:1:2::1

FastEthernet0/1 [administratively down/down]

Serial0/1/0 [administratively down/down]

Serial0/1/1 [up/up]

FE80::224:C4FF:FE62:7246

2001:22:2::2

Loopback0 [up/up]

FE80::224:C4FF:FE62:7246

FEC0::3:1

IPv4 Routing Details:

Br#show ip route

Codes: 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

Gateway of last resort is not set

190.168.0.0/24 is subnetted, 2 subnets

C 190.168.20.0 is directly connected, Serial0/1/1

O 190.168.10.0 [110/845] via 190.168.20.1, 03:16:04, Serial0/1/1

O IA 192.168.10.0/24 [110/846] via 190.168.20.1, 03:16:04, Serial0/1/1

C 192.168.20.0/24 is directly connected, FastEthernet0/0

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/846] via 190.168.20.1, 03:16:04, Serial0/1/1

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/65] via 190.168.20.1, 03:16:04, Serial0/1/1

C 192.168.3.0/24 is directly connected, Loopback0

IPv6 Routing Details:

Br#show ipv6 route

IPv6 Routing Table - 13 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

O 2001:22:1::/48 [110/845]

via FE80::224:C4FF:FE46:F358, Serial0/1/1

O 2001:22:2::/48 [110/845]

via FE80::224:C4FF:FE46:F358, Serial0/1/1

C 2001:22:2::/64 [0/0]

via ::, Serial0/1/1

L 2001:22:2::2/128 [0/0]

via ::, Serial0/1/1

L FE80::/10 [0/0]

via ::, Null0

O FEC0::1:1/128 [110/845]

via FE80::224:C4FF:FE46:F358, Serial0/1/1

C FEC0::3:0/112 [0/0]

via ::, Loopback0

L FEC0::3:1/128 [0/0]

via ::, Loopback0

O FEC0::4:1/128 [110/64]

via FE80::224:C4FF:FE46:F358, Serial0/1/1

OI FEC0:78:1:1::/64 [110/846]

via FE80::224:C4FF:FE46:F358, Serial0/1/1

C FEC0:78:1:2::/64 [0/0]

via ::, FastEthernet0/0

L FEC0:78:1:2::1/128 [0/0]

via ::, FastEthernet0/0

L FF00::/8 [0/0]

via ::, Null0

Host 1

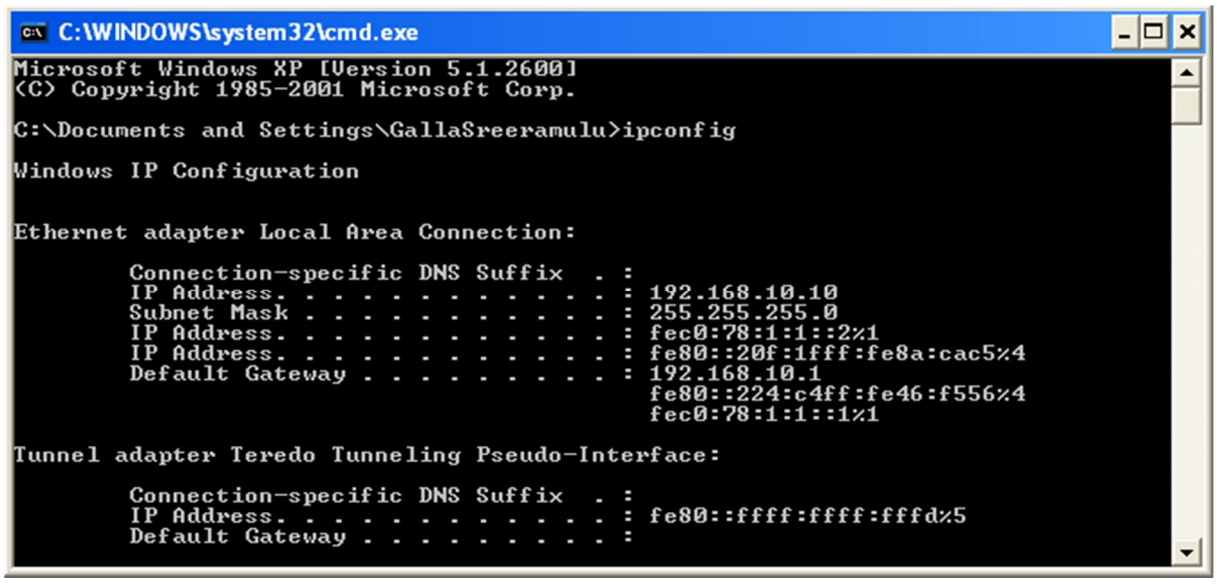


Figure 2.1-B Host 1 IP address

Host 2

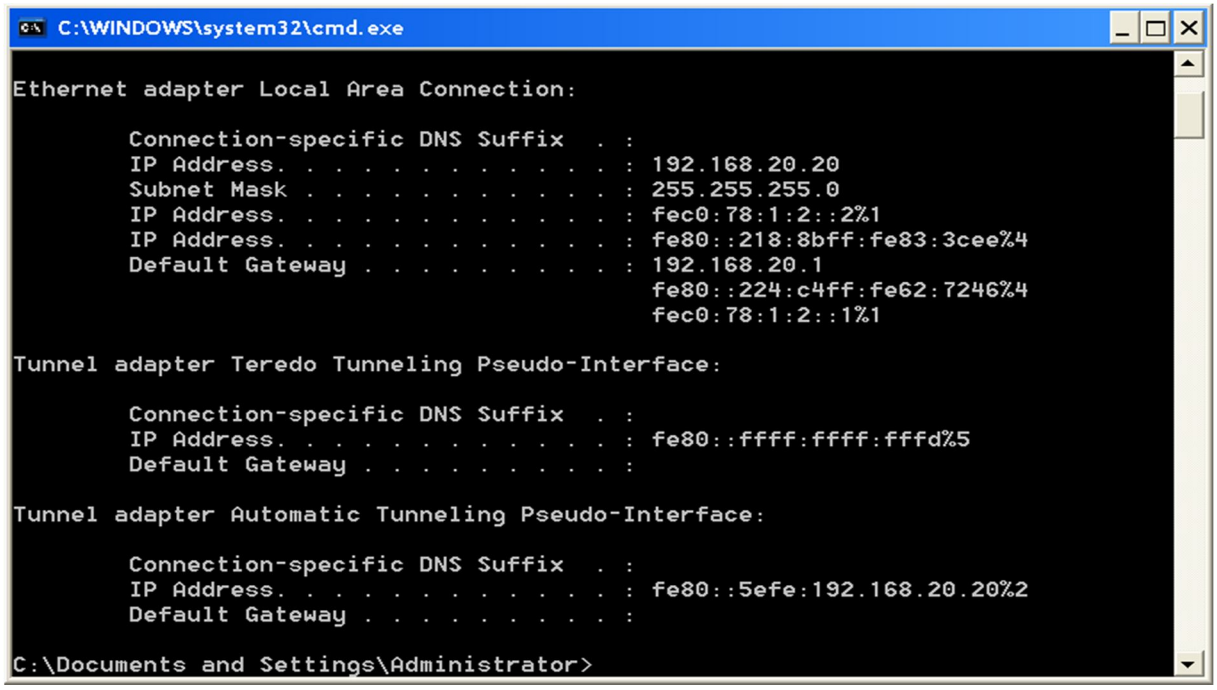


Figure 2.2-B Host 2 IP address