Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Master's Thesis

IPv6 in Campus Network

Ibrahim Zeidan

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Ing. Ibrahim Zeidan

Informatics

Thesis title

IPv6 in Campus Network

Objectives of thesis

The main objective is to Plan and commit the transition from IPv4-only network infrastructure to hybrid IPv4/IPv6 infrastructure in a campus network.
The secondary objective is to create a risk map and establish a typical roadmap for similar situations in the desired business environment.

Methodology

Creating a literature review focused on IPv6 services transition, analysing protocols and applications currently available to support such transition. Prepare a risk map and offer possible solutions. Finalise the conclusion regarding the case study.

The proposed extent of the thesis

50-60

Keywords

OSI model, TCP/IP model, IPv4, IPv6, Routing and routed protocols

Recommended information sources

Ciprian P. Popoviciu, Deploying IPV6 Networks (2006)
David Malone, Niall Richard Murphy, IPv6 network administration (2005)
Tim Rooney, Michael Patrick Dooley, IPv6 deployment and management (2013)
Tom Coffeen, IPv6 Address Planning (2014)

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Eva Kánská, Ph.D.

Supervising department

Department of Information Technologies

Advisor of thesis

Ing. Tomáš Vokoun

Electronic approval: 13. 3. 2023	Electronic approval: 13. 3. 2023
doc. Ing. Jiří Vaněk, Ph.D.	**doc. Ing. Tomáš Šubrt, Ph.D.**
Head of department	Dean

Prague on 13. 03. 2023

Declaration

I declare that I have worked on my master's thesis titled "IPv6 in Campus Network" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 13.03.2023 ______________________________

Acknowledgement

I would like to thank Ing. Tomáš Vokoun, Ing. Eva Kánská, Ph.D., and my family, for their advice and support during my work on this thesis.

IPv6 In Campus Network

Abstract

With the rapid development of computer network, the construction of campus network is the inevitable choice of the development of information network. Internet Protocol version 4 (IPv4) addresses have been reported to be nearing exhaustion and the next generation Internet Protocol version 6 (IPv6) is gradually being deployed in the Internet. IPv6 provides a much larger address space, better address design and greater security, among other benefits.

For comitting the change from IPv4 to IPv6, three mechanisms will be used for a smooth transition from IPv4 to IPv6 with less effect on the network. These mechanisms are Tunnel, Dual-Stack and Translation.

This study shows the deployment of IPv6 in a campus network with network technology, network equipment selection, and so on, and gives the concrete network topology diagram and implementation of the campus area network and use manual transition strategies an automatic of IPv6 and also compare their performances to show how these transition strategies affects network behavior.

Keywords: IPV4, IPV6, DSTM, Tunnel, Transition, Campus.

Nasazení IPv6 v kampusové síti

Abstrakt

S rychlým rozvojem počítačové sítě, výstavbou kampusové sítě je nevyhnutelnou volbou rozvoje informační sítě. Bylo oznámeno, že adresy internetového protokolu verze 4 (IPv4) jsou téměř vyčerpány a na internet se postupně zavádí internetový protokol další generace verze 6 (IPv6). IPv6 kromě jiných výhod nabízí mnohem větší adresní prostor, lepší design adres a větší zabezpečení.
K ukončení přechodu z IPv4 na IPv6 budou použity tři mechanismy pro hladký přechod z IPv4 na IPv6 s menším vlivem na síť. Těmito mechanismy jsou Tunnel, Dual-Stack a Translation.

Tato studie ukazuje nasazení IPv6 v kampusové síti se síťovou technologií, výběrem síťového vybavení atd. A poskytuje konkrétní diagram topologie sítě a implementaci sítě areálových areálů a použití manuálních přechodových strategií automaticky IPv6 a také porovnává jejich představení, která ukazují, jak tyto přechodové strategie ovlivňují chování sítě.

Klíčová slova: IPV4, IPV6, DSTM, tunel, přechod, kampus.

Contents

List of pictures

List of tables

List of abbreviations

AAA	Authentication, Authorization, and Accounting
AAAA	Quad-A DNS Resource Record
API	Application Program Interfaces
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BIA	Bump in the API
BIS	Bump in the Stack
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol for IPv4
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DSTM	Dual Stack Transition Mechanism
HSRP	Hot Standby Routing Protocol
HTTP	Hypertext Transfer Protocol
ICMPv4	Internet Control Message Protocol for IPv4
ICMPv6	Internet Control Message Protocol for IPv6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

IPX Internetwork Packet Exchange
ISATAP Intra-Site Automatic Tunnel Addressing Protocol
IS-IS Intermediate System to Intermediate System
ISO International Organization for Standardization
ISP Internet Service Provider
IT Information Technology
MLS Multi-Layer Switch
MN Mobile Node
MPLS Multiprotocol Label Switching
NAT Network Address Translation
OSI Open Systems Interconnection
OSPF Open Shortest Path First
RTT Round-trip Time
SIIT Stateless IP/ICMP Translation Algorithm
STP Spanning Tree Protocol
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
TTL Time to Live
UDP User Datagram Protocol
URL Uniform Resource Locator
VLAN Virtual LAN
VoIP Voice over IP
VPN Virtual Private Network
VTP VLAN Trunking Protocol
WAN Wide Area Network

1 Introduction

It is a fact that the Internet has become a significant part of our lives, giving uncountable benefits in the way that people communicate, work, learn, and even play. And because of that, the number of connected devices has increased extremely in the past few years.

So, IP has become a scalable technology that responsible for addressing this massive number of connected devices with no limitation in the number of addresses and no restrictions on connectivity [1].

The current version of the Internet Protocol (IP) was developed 25 years ago at the beginning of the Internet. Intrinsically known as IPv4, although IPv4 has proven to be strong since its publication in 1981 (RFC 791) [1], but its initial design did not anticipate the Internet's explosive growth and exhaustion of IPv4 address space, so Network developers have made a large effort to make the transition to Internet Protocol version 6 (IPv6).

Today there are more than 1.2 billion users on the Internet who use IPv6 today [2].

As IPv6 is growing faster than IPv4 in terms of all metrics including the number of users, and the amount of traffic. So, the internet developers decided to invest it strategically and spread it widely to keep the internet growing. IETF has proposed many solutions to start deploying IPv6 alongside IPv4. The plan is to start integrating IPv4 with IPv6 until IPv6 is fully deployed.

2 Objectives and Methodology

2.1 Objectives

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 deploying IPv6 across the world, is Co-existence of IPv4 and IPv6. The complete transition of the Internet will be a huge task. The transition is expected to take several years. 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.

The goal of this research is planning and committing the transition from IPv4-only networks infrastructure to mixed IPv4/IPv6 infrastructure in campus networks.

Creating a risk map and establishing a typical roadmap for similar situations in the desired class of business environment.

2.2 Methodology

The work strategy is summarized as follows:

a) Theoretical study, which deals with the following:

- Creating a literature review focused on IPv6 service transition, analyzing protocols and applications currently available to support such a transition.

- Studying of deploying IPV6 in campus networks by an extensive study of the transition mechanisms.

b) Experimental Study and Simulation:

- Preparing the work environment by choosing and installing the appropriate simulator.

- Defining multiple scenarios with different transition techniques and performance measures used to evaluate network performance.

- Executing simulations and displaying results for different scenarios. And analysis the Network performance

c) Comparing the results and review the most important recommendations and future work of this work.

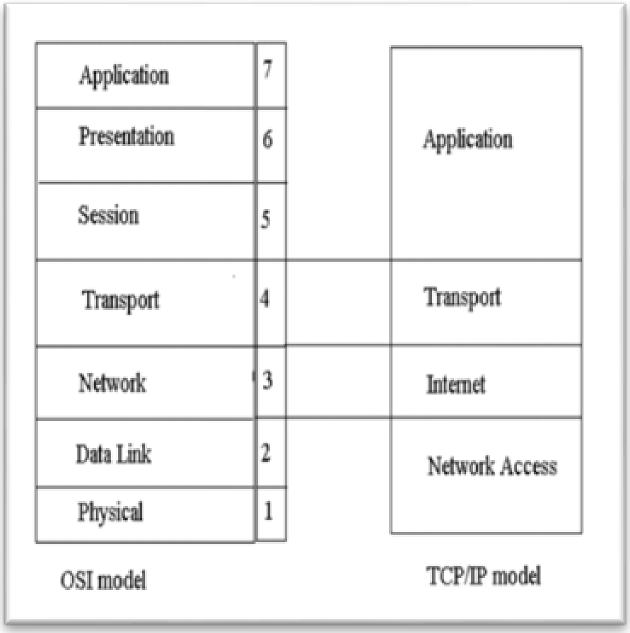
3 Literature Review

3.1 Introduction to Internet Protocol

In this chapter, we will provide a brief introduction to the Internet protocol in the fourth and sixth versions, with a review of the most important proposals to reduce the problems of IPv4, which prompted researchers to use IPv6, and then we will present in detail about the sixth administration of the Internet protocol and the most important advantages that it provided, after identifying the evidence of the IP header and in the paragraph Therefore, we will specialize in the strategies of moving from the infrastructure with ipv4 and deploying ipv6 and the most important protocols and mechanisms necessary to achieve this with the advantages and disadvantages of each of them, which is the focus of the topic of the presented research.

A network protocol is a set of rules that define the mechanism of data exchange and communication between network devices. There are two models for achieving this connection, the OSI model and the TCP/IP model.
The OSI model was proposed by ISO, as it consists of seven layers, each of which includes a set of protocols necessary to work: the physical layer, the data link layer, the network layer (IP, etc..), the transport layer (TCP, UDP, etc..), the session layer, the representation layer, and the application layer (DNS, HTTP, etc.) [3].

Picture (1) shows the structure and layers of the OSI model with their corresponding TCP/IP model.



Picture 1: OSI and TCP/IP Models [4]

In the TCP/IP model, protocols are divided into five layers: the physical layer, the data link layer, the Internet layer, transport layer, and application layer. where each of these layers adds a header to its data during the communication process between sending and receiving devices.
we can summarize the functions of each layer of the TCP/IP communication model as follows:

1- Application layer: It is the high-level user layer in the model, in which information to be transferred from one user's computer (the sender) to another computer (the receiver).
2- Transport layer: It is the second layer in the network model, it records the blocks of data, which are the outputs of the application layer, to be processed at the receiving device and then the header is added to make it called a segment. Transport layer protocols are responsible for controlling the transmission and reception of data through encapsulation, transmission.

3- Network layer: It is the most important layer in the model, its main job is routing. The network layer protocols define the rules for communication between different network devices.
The network layer receives the segments from the transport layer, and adds a header to it, and after that it will be called a Packet.
The most important and most common of these protocols is the Internet Protocol (IP).

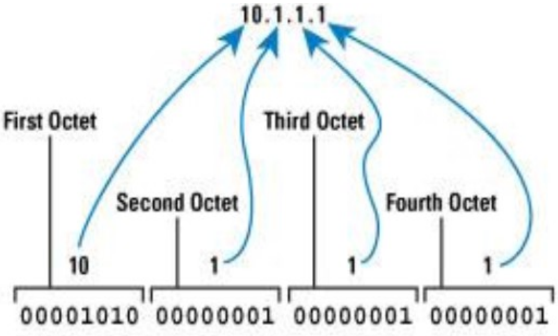
4- Data link layer: This layer provides multiple services such as framing and control of data and errors, here the packet becomes a frame.

5- The physical layer: Contains all the functions needed to carry the bit stream over a physical medium to another system.

3.1.1 IP Version 4 (IPv4)

The IPv4 protocol was defined in 1981 by the organization responsible for setting standards for Internet protocols IETF (Internet Engineering Task Force) and this version was widely used by connecting a small group of organizations. Although the number of devices connected to the Internet then was much less than it is now, IPv4 was the most widely used Internet protocol for device communication on the Internet and is still used for most Internet connections to this day [4].

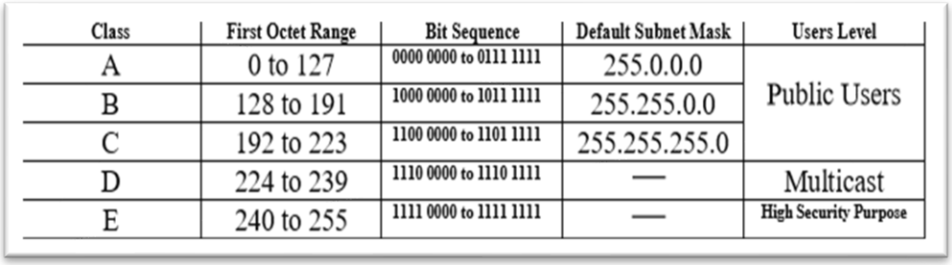
IPv4 uses a 32-bit address system and allows about 2^{32} addresses (over 4 billion addresses). These bits are separated into four groups of eight bits (octets).
The picture (2) shows this division, depending on the format used for IP, bits are represented as decimal numbers separated by dots in the decimal point system.



Picture 2 IPv4 Address Structure[5].

There are different types of addressing in IPv4. The picture (3) shows the classification of IPv4 addresses, the value used for each octet is within
range from 0 to 255 or 00000000 to11111111.

These octets are divided into five different classes of networks from A to E [6].



Class	First Octet Range	Bit Sequence	Default Subnet Mask	Users Level
A	0 to 127	0000 0000 to 0111 1111	255.0.0.0	Public Users
B	128 to 191	1000 0000 to 1011 1111	255.255.0.0	
C	192 to 223	1100 0000 to 1101 1111	255.255.255.0	
D	224 to 239	1110 0000 to 1110 1111	—	Multicast
E	240 to 255	1111 0000 to 1111 1111	—	High Security Purpose

Picture 3 IP address settings for the five IP address classes[6].

It can be noticed from the previous picture that Class A allows for fewer networks compared to other classes but with a larger number of hosts on each subnet.
The addresses of Classes A, B, C are used as public addresses for users, while addresses from Class D are used for multicast, i.e., to send data to a group of nodes on the same subnet.

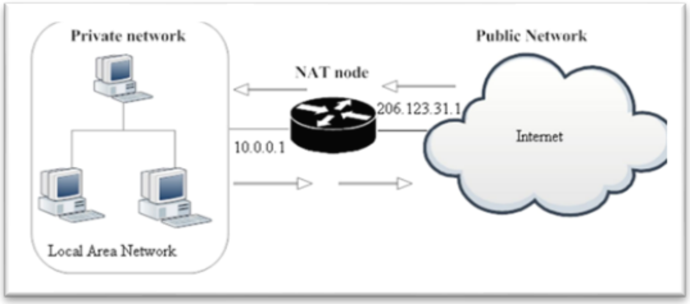
Because the original Internet architecture had fewer than 4.3 billion addresses available, depletion has been anticipated since the late 1980s, when the Internet started experiencing dramatic growth.
This depletion is one of the reasons in creating and adopting several new technologies, including network address translation (NAT), Classless Inter-Domain Routing (CIDR) in 1993, and IPv6 in 1998.

- Classless Inter-Domain Routing (CIDR) as specified in RFC 4632.
- Network Address Translation (NAT) as specified in RFC 3022.

1- Classless Inter-Domain Routing (CIDR):

The goal of proposing this technology is that multiple blocks of IPv4 addresses can be combined, or aggregated, to create the largest pool of classless IP addresses while allowing for more hosts. By using CIDR the addresses of the full class are reduced to less addresses of the classless class, thus better utilization of the address space is made.[7][2]

2- Network Address Translator (NAT) [RFC 1631]:
It is a mechanism used to bind a private internal address to an external public address. In a NAT services scenario, a single node acts as a proxy between the private network and the public network, which makes a single unique address representing a complete set of nodes in the network [1]. Picture (4) shows an example of NAT working in the network.

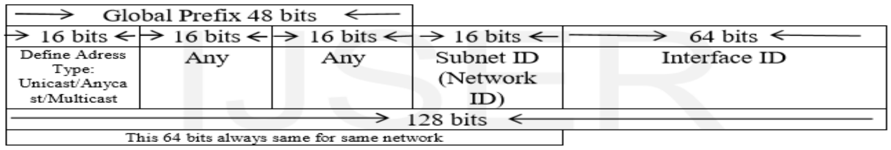


Picture 4 Network Address Translator (NAT) mechanism [4].

However, the CIDR and NAT mechanisms may not have the intrinsic support for solving the ipv4 problem, so it was necessary to publish the upgraded version 6 of the internet protocol, which will be reviewed in the next section.

3.1.2 IP Version 6 (IPv6)

IPv6 uses an IP address of 128 bits allowing a total of 2^{128} addresses. Picture (5) shows the new format for addressing [8].



→ Global Prefix 48 bits ←				
→ 16 bits ←	→ 16 bits ←	→ 16 bits ←	→ 16 bits ←	→ 64 bits ←
Define Adress Type: Unicast/Anycast/Multicast	Any	Any	Subnet ID (Network ID)	Interface ID
→ 128 bits ←				
This 64 bits always same for same network				

Picture 5 128 bits IPv6[6].

An IPv6 address is represented by hexadecimal numbers (digits) and 16 bytes in size, separated by a colon (":").

For example, the following address: 2001:abcd:120F:0000:0000:0001:876A:111B

Before starting in some details with this protocol, some terms used in the Internet protocol must be clarified.

- The network address: is used to find the location of a network and host.
- Prefix network: This is called the subnet mask in an IPv4 address and represents the high-order contiguous bits and expresses the length of the network portion of the address. It is a decimal value within the range 0-128, for example: 2001:abcd:120F:0000:0000:0001:876A:111B/64.

  In the above example, the IPv6 address has a prefix value (/64) and this represents the network address space 2001:abcd:120F:0000:0000:0001 The remainder of the address is represented as the host address in the example above.

There are 3 main types of Ipv6 addresses:

- **Unicast:** An address that specifies only one destination for data. IPv6 packets are sent to the interface specified by this address.
- **Anycast:** specifies a set of destinations (usually belonging to different nodes). A packet sent to an anycast address is delivered to one (any) of the destinations specified by that address (the closest as defined by routing protocols) [9].
- **Multicast:** A multicast address defines multiple interfaces for one-to-many communication. That is, the packet sent to the multicast address is delivered to all interfaces (usually belonging to different nodes) specified by the multicast address.

  In IPv4, the broadcast addresses are used to send traffic to all nodes on a subnet. While There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.

  In addition to providing an essential part of the IPv6 infrastructure, multicast applications include groupware, multimedia distribution, searching, routing, database replication, grid computing, and real-time information delivery. With IPv6, multicast addresses have scope ranging from a single interface or link to the global Internet. They can be permanently assigned and well-known, or they can be used transiently for specific purposes.

  Although multicast addresses are common in both IPv4 and IPv6, several important differences exist:

  Unlike IPv4, IPv6 does not have broadcast addresses. Instead, IPv6 uses optimizations like the Solicited Node multicast groups and all routers multicast addresses, which make better use of network resources than broadcast.

  In IPv6, multicast is used with ICMPv6 for infrastructure applications like neighbor discovery and autoconfiguration on local links.

  IPv6 multicast addresses have new capabilities such as scope and embedded unicast prefixes. In general, IPv6 extensions to multicast have been added to make multicast more useful over internets.

In addition to that, IPV6 provides various improvements in terms of security, routing, automatic address generation, mobility, QOS, etc. The important features and additions of the IPv6 protocol can be summarized as follows:

1- New header format: The IPv6 header has a new design. that is processed more efficiently by routers and at lower processing costs.

2- Large address range: Each IPv6 address contains 128 bits. Thus, the network can accommodate 2^{128} hosts, with other addresses available for future use, so we do not need address-saving technologies, such as NAT deployments.

3- Effective and Simple Routing Infrastructure: IPv6 addresses are designed to create an efficient and hierarchical routing infrastructure.

4- Stateful and stateless address generation: IPv6 supports both stateless and stateful address generation, stateful as address generation when there is a DHCP server and stateless address (address generation when there is no DHCP server). Where with stateful address generation, hosts are given IPv6 addresses automatically (called link-local addresses) and with addresses derived from prefixes declared by local routers. Also, even when there is no router, hosts on the same link can automatically generate link-local addresses and communicate without settings.

5- Built-in Security: IPsec is a suite of protocols for securing Internet Protocol (IP) communications by authenticating the sender and providing integrity protection plus optionally confidentiality for the transmitted data. Which provides this requirement for network security needs such as payload encryption and connection source authentication.

6- Provides better end-to-end support for real-time traffic: e.g., VoIP, voice and video.

7- Plug and Play: It is easy to connect the equipment to the network, this setting is done automatically.

8- QOS support, where new fields in the IPv6 address header define how traffic is handled. E.g., the Flow Label field in the IPv6 header of IPv6 routers helps identify and provide special handling for packets belonging to a particular packet stream between sender and receiver. QOS can also be supported when the packet payload is encrypted through IPsec.

9- Extensibility: IPv6 can be easily expanded for new features by adding additional headers after the ipv6 header.

10- Improved support for mobile networks: Mobile IPv6 means the ability to move with the same IP address from one place to another place far from the local Internet Service Provider, which allows customers the freedom to move and move flexibly Large and uninterrupted connection even if it is outside the scope of the service provider. Mobile IPv6 (MIPv6) is an enhanced protocol supporting roaming for a mobile node, so that it can move from one network to another without losing IP-layer connectivity as defined in RFC 3775, Mobility Support in IPv6.Therefore, (IPv6) gives the possibility to build mobile networks with high efficiency and low cost, as well as Internet connection services with high performance (Efficient Mobile Networks).

It is important to mention that IPv6 is not compatible with IPv4, so IPv4 systems cannot use IPv6 services or communicate with IPv6 hosts, therefore, the systems require interoperability between IPv4 and IPv6, so there are "transition mechanisms" which are compatible mechanisms that exist for the coexistence of IPv6 and IPv4 infrastructure. RFC 4294 defines the following types of nodes [15]:

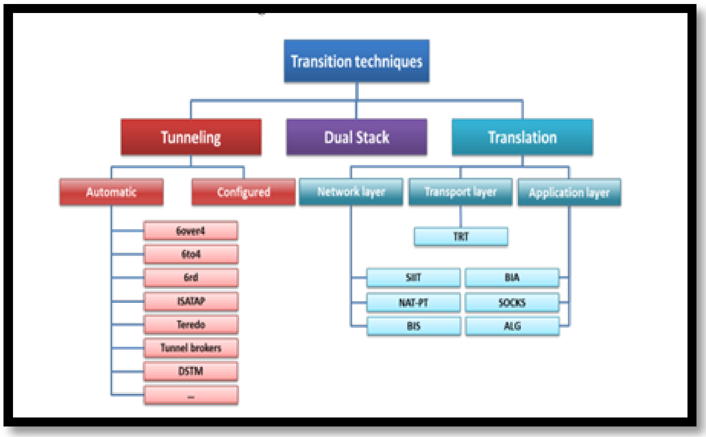
- A node is a device that owns an IP address.
- A router is a device that forwards IP packets to the destination nodes.
- A host is a node but not a router. It should be noted that in the transition environment.

Also, there are three different types of hosts:

A. IPv4 only A host that implements the IPv4 protocol inside it.
B. IPv6 only A host that uses the IPv6 protocol only.
C. Dual Stack IPv4 / IPv6 Host that uses both IPv6 and IPV4

3.1.3 Coexistence Strategies for Migrating to IPv6

The Internet Engineering Task Force (IETF) has identified a number of specific mechanisms for the IPv6 transition [15]. Which upgrades networks and increasingly deploys IPv6 with little or no disruption to IPv4 services. The appropriate transition mechanism is selected based on the client's capabilities, the particular transition strategy chosen, the time frame and phases of the transition. Initially, these mechanisms as shown in the picture (6) were mainly divided into Dual Stack, Tunnels, and Translation.

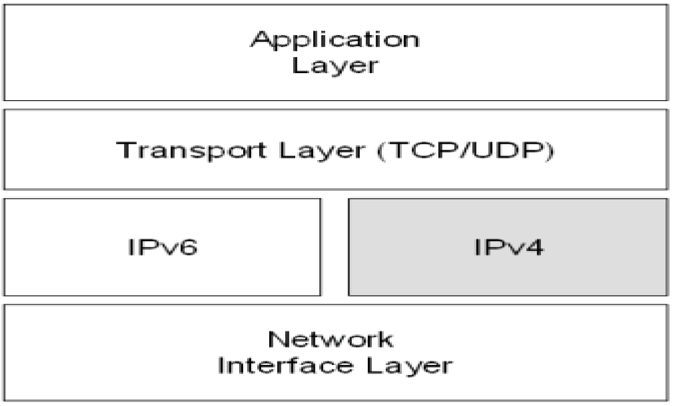


Picture 6 basic IPV6 transition techniques [16]

IPv6 deployment technologies have also been divided by network designers into four main types as follows [17]: Daul Stack technology that allows IPv4 and IPv6 applications to co-exist in a dual IP layer routing backbone, and IPv6 can be deployed via IPv4 tunneling technology. It uses so-called tunnels to encapsulate IPv6 traffic into IPv4 packets that includes many types such as manually-configured tunneling style, General Routing Encapsulation (GRE) tunnels, and semi-automated tunneling mechanisms such as tunnel broker services, and other mechanisms that are fully automated, such as 6to4 for a wide area network (WAN) and Intra-site Automated Tunneling Addressing Protocol (ISATAP).
For campus environments an IPv6 connection can be used with another IPv6 connection over other data links. Separate relay or Asynchronous Transfer Mode (ATM) with Permanent Virtual Circuits (PVC), but over the IPv4 MPLS backbone without modifying the underlying substructure.

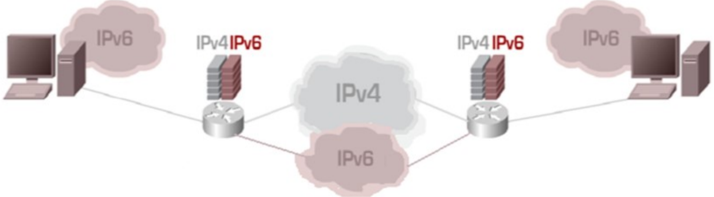
- **Dual Stack Transmission Mechanism (DSTM)**

The dual stack model is the simplest approach currently used as an option for the transition from IPv4 to IPv6 [18].
This transition allows the IP (IPv4 and IPv6) stacks to be run within a single node in parallel and thus allows the end node to use any of the protocols Routing protocols for both IP versions are selected and configured appropriately; For example, the Internal Gateway Protocol (IGP) is chosen (OSPFv2 for IPv4 and OSPFv3 for IPv6). IPv4 and IPv6 also share transport layer protocols such as TCP/IP. There are many clients and servers with different operating systems that support both protocol stacks. For example: Windows XP, Windows Server 2003, and Linux [19].
Picture (7) shows the TCP/IP model of a dual stack node.



Picture 7 Dual stack TCP/IP Architecture[4]

A node in a dual-stack network infrastructure must be able to understand and process both IP network protocols versions. But a dual stack node cannot decide randomly which IP stacks to use in communication but rather the routing protocol decides. Picture (8) shows the infrastructure of the dual stack model.

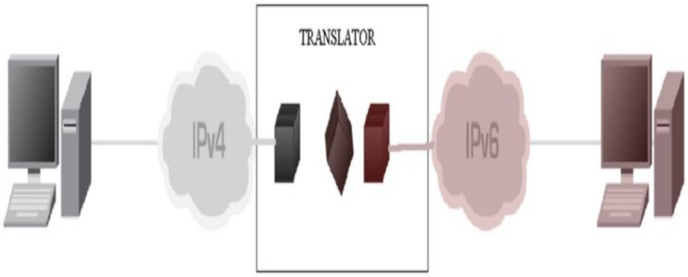


Picture 8 Dual Stack Infrastructure[4]

This technology needs to upgrade all routers in the network, so network administrators chosen for this approach must realize that all routers require dual addressing scheme selection and must be configured with enough memory for both the IPv4 and IPv6 routing tables.
Here, an application programming interface (API) is defined to support both IPv4 and IPv6 addresses and Domain Name Service (DNS) requests.
Currently, dual routing is a valid deployment strategy for a given network with a mix of IPv4 and IPv6 applications, for example, on a campus, which requires both protocols to be configured.

- **Translation Mechanism**

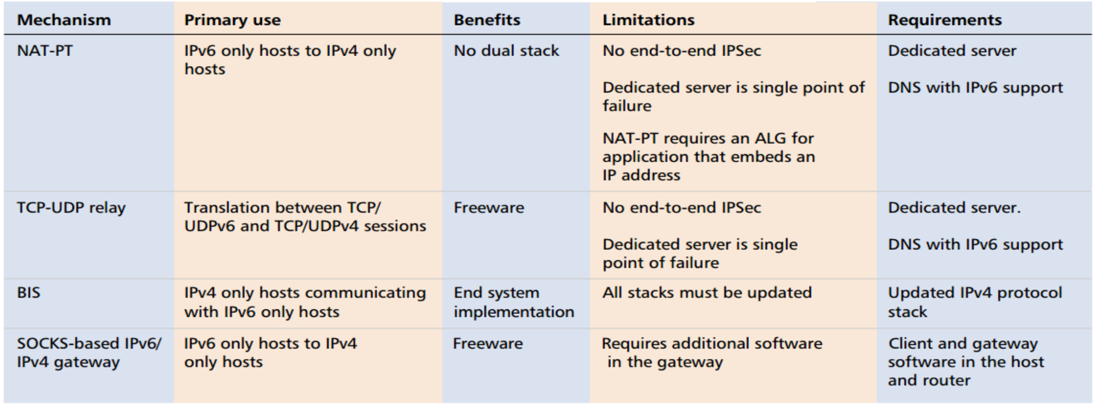
Some organizations or individuals may only install IPv6 in their nodes or networks but may not implement a dual stack. Under these circumstances, communication between IPv6 hosts only IPv4 hosts only require a certain level of translation between the IPv6 protocols and IPv4 host or router, or dual stack hosts, with an extension of an application-level understanding of which protocol should be used. For example, an IPv6-only network may still want to be able to access IPv4-only resources, such as IPv4-only web servers.
The translation mechanism can be defined as technique that allows an IPvX-only network to communicate directly with an IPvY-only network. It translates the IPvX packet to an IPvY packet to allow communication [20].
Figure (9) describes the translation approach. As translation mechanisms always need a translator that can translate a specific IPv4 address to a specific IPv6 address and convert both IPv4 and IPv6 header and payload according to their IP specifications.



Picture 9 Translation Mechanism Infrastructure[4].

There are a variety of IPv6-to-IPv4 translation mechanisms under study by the IETF working group, which fall into two categories [21]; Those that do not require any changes to IPv4 or IPv6 hosts.
An example is the TCP-UDP relay mechanism that runs on a dedicated server and sets up separate transport-level IPv4 and IPv6 hosts, then simply transfers information between the two. While for example that requires additional changes, BIS technology requires additional layers on the IPv4 protocol stack which be presented in the next chapter.

It should be noted that in addition to IPv6 propagation strategies within an IPv4 environment, the user also needs protocol translation mechanisms, such as NAT-PT, to allow communication between applications using IPv4 and those using IPv6 (for example, enabling only IPv6 web browsers to communicate with IPv4 web servers only or double stack). The SOCKS-based gateway technique relays two "terminal" IPv4 and IPv6 connections at the application layer, it consists of additional functions in both the end system (client) and a dual-stack router (gateway) to enable communication between IPv4 and IPv6 nodes.
These translation mechanisms may be useful as IPv6 deployment moves from testing to the actual use phase, and more relevant. Table (1) provides a comparison of translation mechanisms.



Mechanism	Primary use	Benefits	Limitations	Requirements
NAT-PT	IPv6 only hosts to IPv4 only hosts	No dual stack	No end-to-end IPSec Dedicated server is single point of failure NAT-PT requires an ALG for application that embeds an IP address	Dedicated server DNS with IPv6 support
TCP-UDP relay	Translation between TCP/UDPv6 and TCP/UDPv4 sessions	Freeware	No end-to-end IPSec Dedicated server is single point of failure	Dedicated server. DNS with IPv6 support
BIS	IPv4 only hosts communicating with IPv6 only hosts	End system implementation	All stacks must be updated	Updated IPv4 protocol stack
SOCKS-based IPv6/IPv4 gateway	IPv6 only hosts to IPv4 only hosts	Freeware	Requires additional software in the gateway	Client and gateway software in the host and router

Table 1 A comparison of protocol translation mechanisms[17].

We can divide Translation techniques into two approaches [22]:

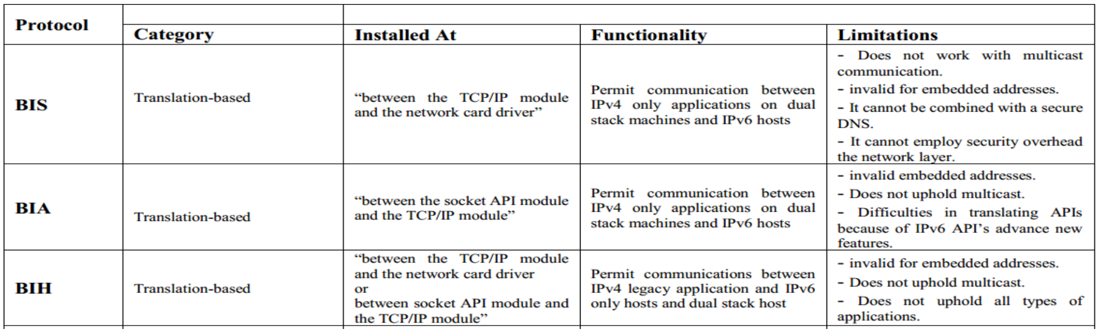
1- Host-Based Translation Approach:

This approach is used when translation is required and there is no match between the type of application that is running and the current host connection. Therefore, IPvX will be translated to communicate with IPvY and vice versa.
There are many mechanisms that have been proposed as a solution to guarantee dual connectivity between incompatible hosts. IETF has proposed mechanisms such as “Bump in The Stack (BIS)”, “Bump in the API (BIA)” and “Bump in The Host (BIH)”. Which will be reviewed in the next paragraph.

- **Bump in the Stack (BIS) [RFC2767]:** A protocol or technology that uses the SIIT algorithm to translate IPv4 packets (the header) to IPv6 and IPv6 packets to IPv4 by placing the translation module between the TCP/IPv4 module and the hardware card module [23].
  Translation is the transfer of data that passes through the two units, after translating the packets from IPv4 to IPv6 and vice versa. And the Domain Name System DNS server is responsible for assigning IP addresses, and it should be noted here that A Domain Name System (DNS) is needed for successful coexistence of IPv6 and IPv4 because of the prevalent use of names (rather than addresses) to refer to network resources. Upgrading the DNS infrastructure consists of populating the DNS servers with records to support IPv6 name-to-address and address-to-name resolutions. After the addresses are obtained using a DNS name query, the sending node must select which addresses are to be used for communication.

- **Bump in the API (BIA) [RFC3338:** is a technique used to translate functions of IPv4 socket API to IPv6 socket API and vice versa [24].
  This protocol defines the functions of the IPv4 socket API and calls the equivalent IPv6 socket API IPv6 functions, so the entire IP header is not translated. Different from BIS, it places an API interpreter between the socket API and the TCP/IP module on dual stack hosts.

- **Bump in the Host (BIH):** It is a host-based technology that integrates both BIS and BIA technologies together and translates from IPv4 to IPv6. The BIH protocol is achieved by two applications, which are interpreted in a socket API that is placed between the TCP/IP module and the TCP/IP module [25].
  Table (2) shows a brief comparison of the different technologies listed under the Host-Based Translation category.



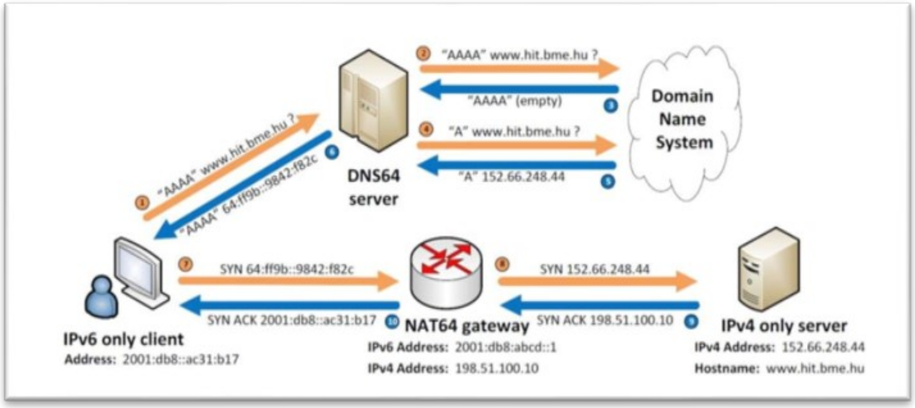
Protocol	Category	Installed At	Functionality	Limitations
BIS	Translation-based	"between the TCP/IP module and the network card driver"	Permit communication between IPv4 only applications on dual stack machines and IPv6 hosts	- Does not work with multicast communication. - invalid for embedded addresses. - It cannot be combined with a secure DNS. - It cannot employ security overhead the network layer.
BIA	Translation-based	"between the socket API module and the TCP/IP module"	Permit communication between IPv4 only applications on dual stack machines and IPv6 hosts	- invalid embedded addresses. - Does not uphold multicast. - Difficulties in translating APIs because of IPv6 API's advance new features.
BIH	Translation-based	"between the TCP/IP module and the network card driver or between socket API module and the TCP/IP module"	Permit communications between IPv4 legacy application and IPv6 only hosts and dual stack host	- invalid for embedded addresses. - Does not uphold multicast. - Does not uphold all types of applications.

Table 2 Comparison between the previously presented transition techniques [47] .

2- Network-based Translation Approach:

In this model, the IP header for each packet is translated. This is to provide communication between networks with an IPv4 architecture only and networks with an IPv6 architecture only and vice versa. An example of network-based translators is Stateless IP/ICMP Translation (SIIT) [26], and Stateful Address and Protocol Translation from IPv6 Client to IPv4 Servers (NAT64) [27].

- **Stated NAT64 with DNS64:** The goal of this mechanism is to enable only IPv6 clients to connect to only IPv4 servers. To illustrate the working principle of this mechanism [27], picture (10) shows an example of a scenario using this protocol where an IPv6 client only wants to connect to an IPv4 server only. It first sends a request to the DNS64 server asking for an IPv6 address (e.g an AAAA record for the web server www.hit.bme.hu.) and then the DNS64 server asks the DNS for this address. Since the DNS system has no such record it responds with the corresponding IPv4 address (such as an A record), which in this case is 152.66.248.44. The DNS64 server uses the well-known NAT64 prefix 64:ff9b::/96 to assemble a so-called IPv4-embedded IPv6 address by adding the 32-bit IPv4 address of the receiver (i.e. 152.66.2 .44 It responds to the customer with this compound address. Then the IPv6 client just starts a TCP session and assigns the IPv6 address included in the receiving IPv4 (64:ff9b::9842:f82c) as the target address of the IPv6 packet where the last 32-bit "x9842f82c" represents the IPv4 address 152.66.248.44)) All packets are destined to the pre-address 64:ff9b::/96 to the NAT64 gateway. Thus, this NAT64 gateway receives a packet over its IPv6 interface, and then creates an IPv4 packet using the last 32 bits of the address (152.66.248.44) as the IPv4 target address and its IPv4 interface address as the source address of the IPv4 packet, records the connection in the connection tracing table, and then sends the IPv4 packet to the IPv4 web server only. The server responds to a NAT64 gateway. The NAT64 gateway receives an IPv4 reply packet from the server, creates an IPv6 packet from the information recorded in the state table, and sends this IPv6 packet to the IPv6 client only.



Picture 10 NAT64 and DNS64 scenario server [28].

- **Stateless Internet Protocol/Internet Control Messaging Protocol Translation(SIIT) [RFC 2765]:**

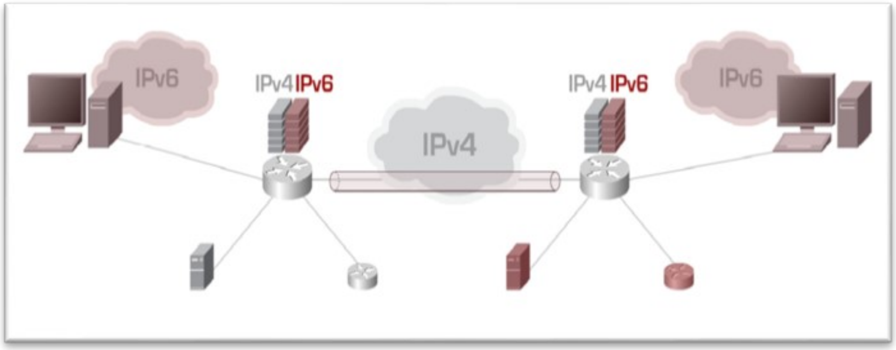
Is a stateless translation technology, which translates IPv4 packet headers into IPv6 (including ICMP headers) and vice versa by implementing the address binding algorithm and depending on the compiler's settings and the information of the compiled packet. In addition, the translator does not maintain any dynamic session or binding state.

Therefore, packets in a single session or stream can pass more than one interpreter instead of a single interpreter as state compilers do [2].

- **Tunnelling Mechanism**

One of the major deployment strategies for both service providers and organizations during the period of IPv4 and IPv6 coexistence, is used in networks that do not have the infrastructure where they are not able to provide IPv6 functions. This technology is also called "encapsulation".
It is the process of encapsulating the information of one protocol into another protocol packet which allows the encapsulated data to be transmitted over the encapsulation protocol [29].

Any redirection in the tunnel is encapsulated in an IPv6 packet into an IPv4 packet and is processed according to the normal IPv4 routing scheme and is unwrapped at the other end of the tunnel. That is, a tunnel connection provides a way to carry IPv6 data over an existing IPv4 infrastructure, an example of an infrastructure is shown in picture (11) for tunnels. Several tunneling mechanisms are available to carry IPv6 traffic over IPv4 networks and require having tunnel endpoints operate in double stack mode.
These mechanisms include manually created tunnels such as IPv6 over IPv4 GRE tunnels, semi-automated tunneling mechanisms such as those used by tunnel brokerage services, and fully automated tunneling mechanisms such as ISATAP and 6to4 tunnels.



Picture 11 Tunneling Mechanism infrastructure[4]

Not all migration strategies will be applicable to all networks, most clients may be interested in tunneling IPv6 over existing IPv4 networks tunnel,
It is possible to clarify different scenarios for tunnels, which are as follows:

1- **Manual tunnels**
Also called explicit tunnels, the basic idea of this type of tunneling technique is that when IPv6 hosts/sites are linked together over an IPv4 infrastructure the IPv6 traffic is encapsulated in IPv4 packets at one of the two endpoints of the tunnel Then encapsulation is done at the end point of the tunnel at the other end. The value of the Protocol Type field in IPv4 packets in this case, IPv4 header should be 41, and the

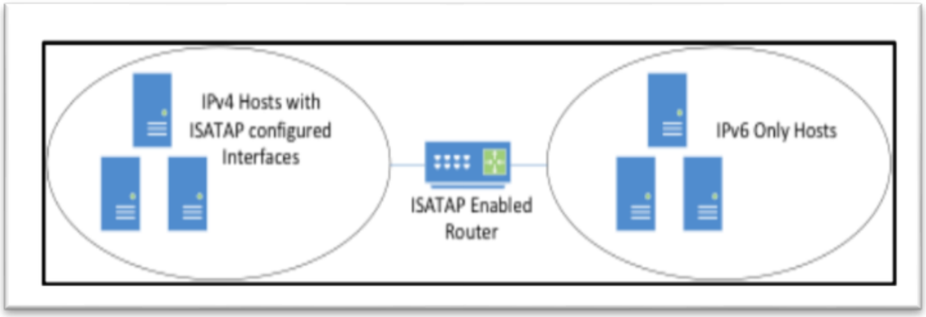
network administrator must set the settings manually and the two endpoints (router or host) are of Dual Stack type (ipv4, ipv6 stacks) [30].
Thus, this type requires additional administrative efforts to adjust the settings (point to point).

2- **Generic Routing Encapsulation (GRE)**
When GRE IPv6 tunnels are configured, the source and target tunnel ends are assigned IPv6 addresses. The tunnel interface can contain specific IPv4 or IPv6 addresses. So, the host or router at the end of each tunnel must support dual stack (IPv4 and IPv6 protocol packets) [30].

3- **Automatic GRE Tunnel**
The routing infrastructure in this type of tunnel automatically determines the endpoint of the tunnel. That is, one tunnel endpoint can find the other end without prior configuration. One way to tunnel IPv6 over IPv4 is achieved by including IPv4 addresses in IPv6 addresses. These tunnels were suitable for use in the early stages of IPv6 migration. Some of the most important automatic tunneling mechanisms are: 6 to4 Tunneling, IPv6 domains connection over IPv4 Clouds - router to router, Intra-site Tunneling ISATAP and the use of a Tunnel Broker.

a) 6 to4 Tunneling (RFC 3056)
RFC 3056 recommends this type of automatic tunneling as it overcomes the problems of 4in 6 manual tunneling by allowing IPv6 hosts/sites, which have at least one public IPv4 address, to communicate with each of them over an IPv4 network without explicit tunneling setup [31]. It also supports communication between IPv6 hosts/sites and native IPv6 domains via relay routers. It is a system that allows IPv6 packets to be transmitted over an IPv4 backbone without the need to physically configure explicit tunnels. It works as follows: it allocates a block of IPv6 address space to any host or network that has a public IPv4 address (which includes 4 to 6 prefix (2002::/16) to distinguish its packets over the public IPv4 network) and then encapsulates the IPv6 packets into IPv4 packets for transmission over the IPv4 network using 4 in 6 from which the traffic is routed between 4 to 6 networks and the “native” IPv6 networks.

b) Intra-site Automatic Tunnel Addressing protocol (ISATAP)
The Intra-site Automatic Addressing Protocol (ISATAP) is designed [32] Mainly for dual-stack nodes communication with IPv6 nodes over IPv4 networks. The ISATAP host forms an IPv6 address format from a predefined 64-bit prefix obtained from the ISATAP server, followed by a reserved interface identifier (::5efe) and ending with a 32-bit IPv4 address. This address is then used to communicate over the ISATAP network.



Picture 12. ISATAP Tunneling mechanism [30]

Although the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as the IPv6 6to4 tunnel, ISATAP is designed to transport IPv6 packets within a site, not between sites.

4- Tunnel Broker

Tunnel Broker is not a technology per itself, but a way to manage IPv4 tunnels for IPv6 hosts/sites by deploying dedicated servers for automatic processing of tunnel requests coming from IPv6 hosts/sites and is defined as a service that provides a network tunnel [33]. These tunnels provide the encapsulation to connect through existing infrastructure to other infrastructure. IPv6 tunnel brokers secure IPv6 connectivity to IPv4/IPv6 dual-stack nodes on IPv4 networks without port administrative support for a large site.

It is therefore intended to stimulate an increase in the number of interconnected IPv6 host s and to allow IPv6 network providers to provide easy access to their IPv6 networks.

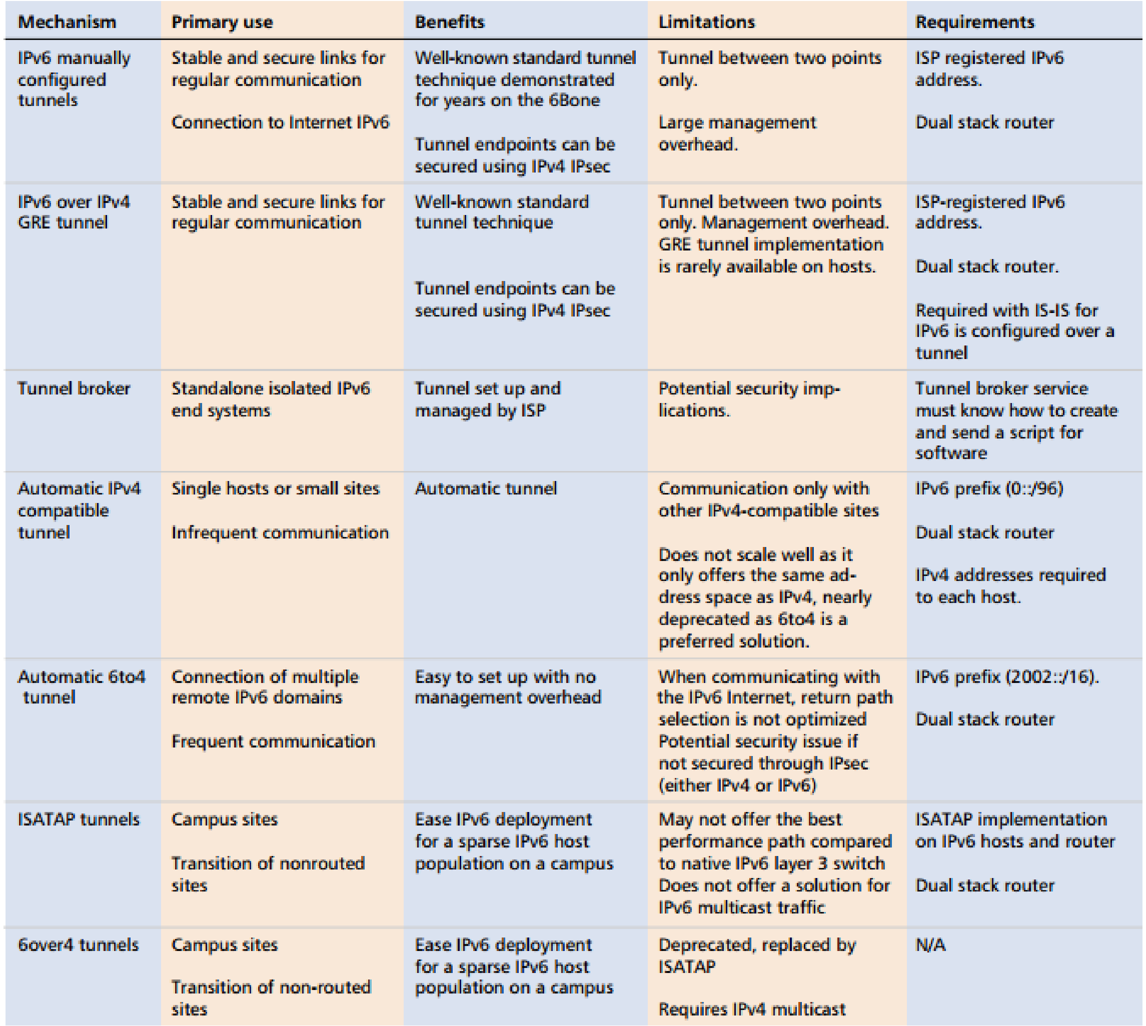
5- Teredo

Enables IPv4 hosts that do not have a public IPv4 address, to connect to IPv6 nodes by tunneling IPv6 packets over UDP. To accomplish this task, Teredo deploys two types of devices: Teredo Server

and Teredo relay, where the Teredo server is responsible for configuring the Teredo tunnel while the Teredo relay acts as an IPv6 router and is responsible for redirecting traffic to/from Teredo clients.

Each Teredo host is assigned an IPv6 address that starts with a special service prefix (2001:0000:/32) [34][41].

The table (3) shows a comparison of different IPv6 tunneling technologies as it presents the pros and cons of the above mechanisms [17]. We note that even without manual configuration, we can run IPv6 end stations and campuses across an IPv4 cloud using the tunneling mechanisms mentioned above. To achieve IPv6 security over IPv4 tunneling, network administrators can configure IPsec for either IPv4 or IPv6 on edge routers.



Mechanism	Primary use	Benefits	Limitations	Requirements
IPv6 manually configured tunnels	Stable and secure links for regular communication Connection to Internet IPv6	Well-known standard tunnel technique demonstrated for years on the 6Bone Tunnel endpoints can be secured using IPv4 IPsec	Tunnel between two points only. Large management overhead.	ISP registered IPv6 address. Dual stack router
IPv6 over IPv4 GRE tunnel	Stable and secure links for regular communication	Well-known standard tunnel technique Tunnel endpoints can be secured using IPv4 IPsec	Tunnel between two points only. Management overhead. GRE tunnel implementation is rarely available on hosts.	ISP-registered IPv6 address. Dual stack router. Required with IS-IS for IPv6 is configured over a tunnel
Tunnel broker	Standalone isolated IPv6 end systems	Tunnel set up and managed by ISP	Potential security implications.	Tunnel broker service must know how to create and send a script for software
Automatic IPv4 compatible tunnel	Single hosts or small sites Infrequent communication	Automatic tunnel	Communication only with other IPv4-compatible sites Does not scale well as it only offers the same address space as IPv4, nearly deprecated as 6to4 is a preferred solution.	IPv6 prefix (0::/96) Dual stack router IPv4 addresses required to each host.
Automatic 6to4 tunnel	Connection of multiple remote IPv6 domains Frequent communication	Easy to set up with no management overhead	When communicating with the IPv6 Internet, return path selection is not optimized Potential security issue if not secured through IPsec (either IPv4 or IPv6)	IPv6 prefix (2002::/16). Dual stack router
ISATAP tunnels	Campus sites Transition of nonrouted sites	Ease IPv6 deployment for a sparse IPv6 host population on a campus	May not offer the best performance path compared to native IPv6 layer 3 switch Does not offer a solution for IPv6 multicast traffic	ISATAP implementation on IPv6 hosts and router Dual stack router
6over4 tunnels	Campus sites Transition of non-routed sites	Ease IPv6 deployment for a sparse IPv6 host population on a campus	Deprecated, replaced by ISATAP Requires IPv4 multicast	N/A

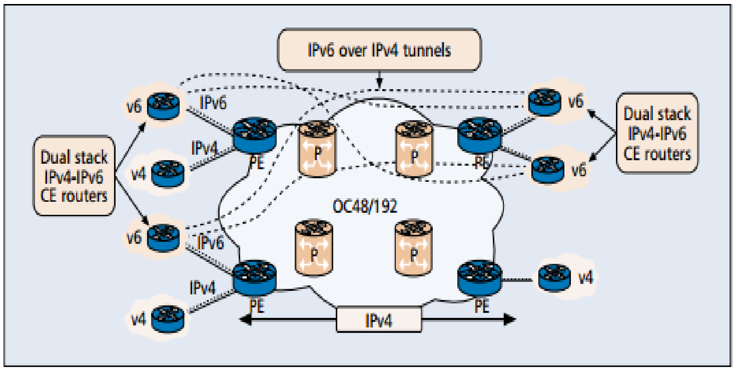
Table 3 Comparison of various tunneling mechanisms[17]

3.1.4 Deploying IPv6 over MPLS Backbone

This technology allows for IPv6 domains Communicate with each other over IPv4 MPLS network core. This requires much less basic infrastructure than an upgrade with no need to reset the core routers, because forwarding is done based on labels rather than the IP address header itself, offering a cost-effective way to propagate IPv6. VPN and Traffic Engineering (TE) are available within an MPLS environment that allows IPv6 networks to be federated into VPNs. There are many different ipv6 deployment strategies that fall under this type of deployment, as follows [17]:

1- IPv6 tunnels at the edge of client routers (CE)

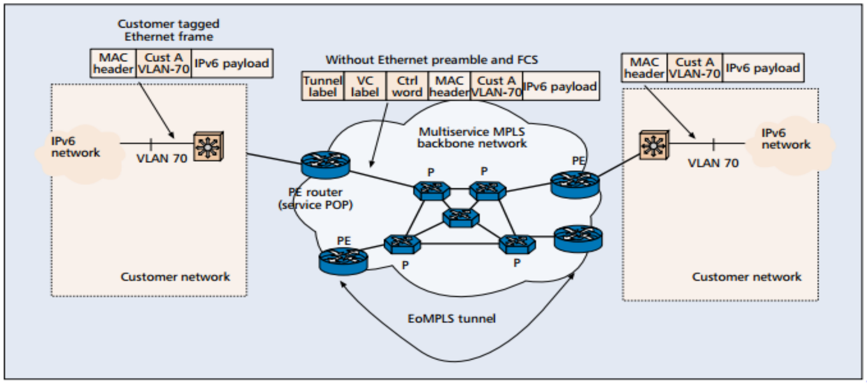
As shown in picture (13), the first of these strategies does not require any changes to the MPLS core component of Provider (P) and PE routers. Where IPv4 tunnels are used on dual-stack CE routers, IPv6 traffic is encapsulated, and thus appears as IPv4 traffic within the MPLS network.



Picture 13:IPv6 deployment using tunnels on the CE routers[17]

2- Layer 2 transport circuit via MPLS

Here, there is no change to the underlying routing mechanisms as PE routers (to support one Layer 2 circuit transport over MPLS mechanisms) connected to clients. Communications between remote IPv6 domains run native IPv6 protocols over a dedicated link, IPv6 traffic is tunneled using either Transport over MPLS (AToM) or Ethernet over MPLS (EoMPLS) [35], with IPv6 routers connected through an ATM interface or Ethernet, respectively. Picture (14): shows an example of IPv6 propagation via an MPLS circuit transport method.



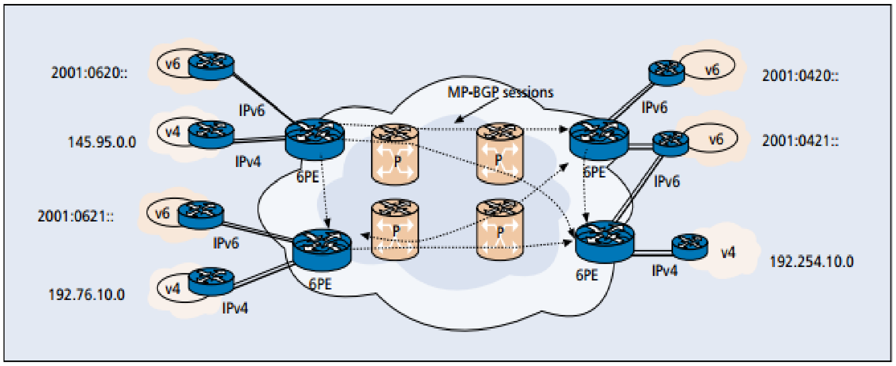
Picture 14. IPv6 over "Ethernet over MPLS."[17].

3- IPv6 at the edge of 6PE (6VPE) provider routers

Is another deployment strategy for configuring IPv6 on MPLS PE routers [36] that maintains the benefits of existing IPv4 MPLS features (e.g., MPLS-TE or VPNs), while securing a native IPv6 service for enterprise customers using IPv6 prefixes that it provides.

Picture (15) shows an example of IPv6 propagation on PE routers. Each PE router must be upgraded to be a dual stack to become a 6PE router) and the settings are configured to run MPLS on interfaces connected to P-core routers. The 6PE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, depending on the connection, diverting IPv4 and IPv6 traffic over native IPv4 and IPv6 interfaces and not by implementing MPLS. The 6PE router exchanges accessibility information with other 6PE routers in the MPLS domain using the Multiple Border Gateway Protocol (BGP), and shares the IPv4 routing protocol, such as the Open Shortest

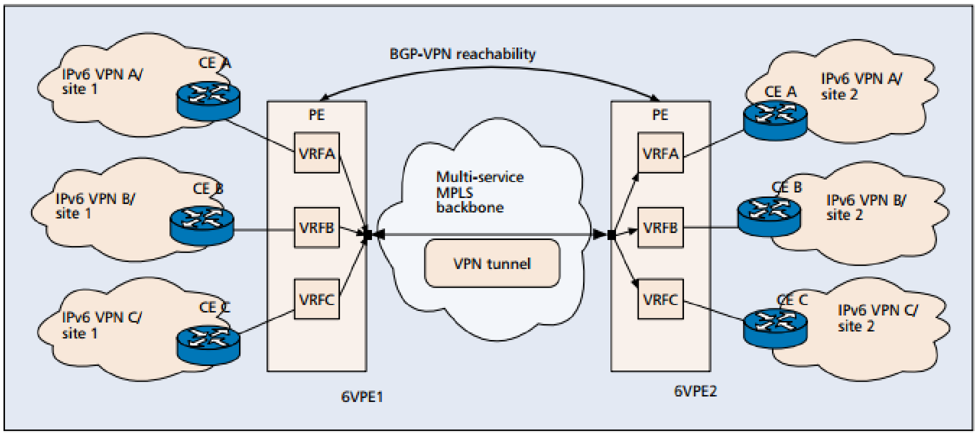
Path First (OSPF), with the other P and PE devices in the field. 6PE routers encapsulate IPv6 traffic using two levels of MPLS labels. The top label is distributed by the Label Distribution Protocol (LDP) or TDP file used by devices in the core to carry the packet to the 6PE destination using IPv4 routing information. The second is assigned with the IPv6 address prefix to the target through the BGP-4 multiprotocol, allowing load balancing to be performed.



Picture 15: IPv6 on provider edge routers [17].

4- Adding IPv6 MPLS VPNs to 6PE (6VPE)

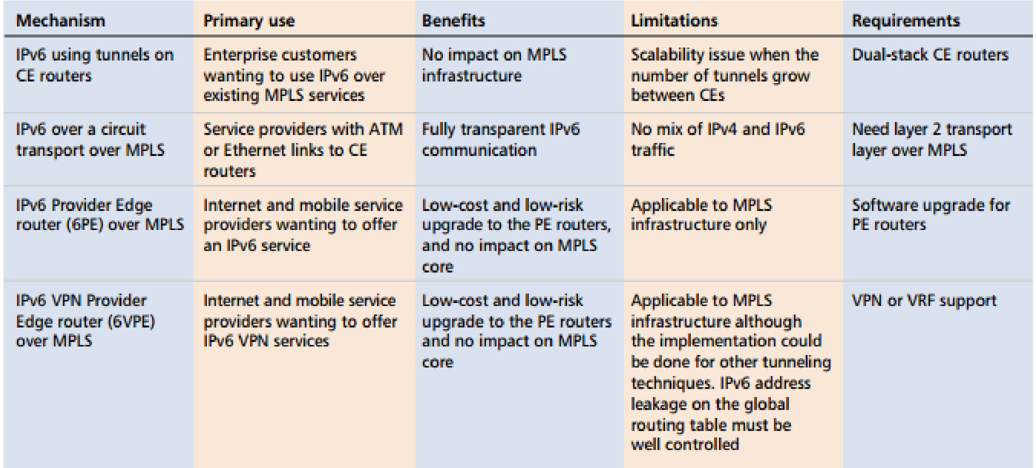
A VPN is said to be IPv6 VPN [37] when a CE router runs native IPv6 over an interface or sub-interface of the PE router. And by adding IPv6 VPN capability to a 6PE router, it's called 6VPE for IPv6 VPN Provider Edge Router over MPLS, an option that enables the ISP to offer similar services to IPv4. Similar to IPv4 VPN Routes Distribution, BGP and its extensions are used to distribute routes from an IPv6 VPN site to all other 6VPE routers connected to the same IPv6 VPN site. Product experts use VPN routing and forwarding tables (VRFs) to separately maintain accessibility and forwarding information The information of each IPv6 VPN, as shown in the following picture.



Picture 16 :IPv6 MPLS VPN architecture[17]

Also, the latter strategy requires a complete network upgrade of all P and PE routers, with dual control planes for IPv4 IPv6. It represents the core IPv6 MPLS native.

Table (4) shows a comparison of these strategies for IPv6 transport over the MPLS backbone.



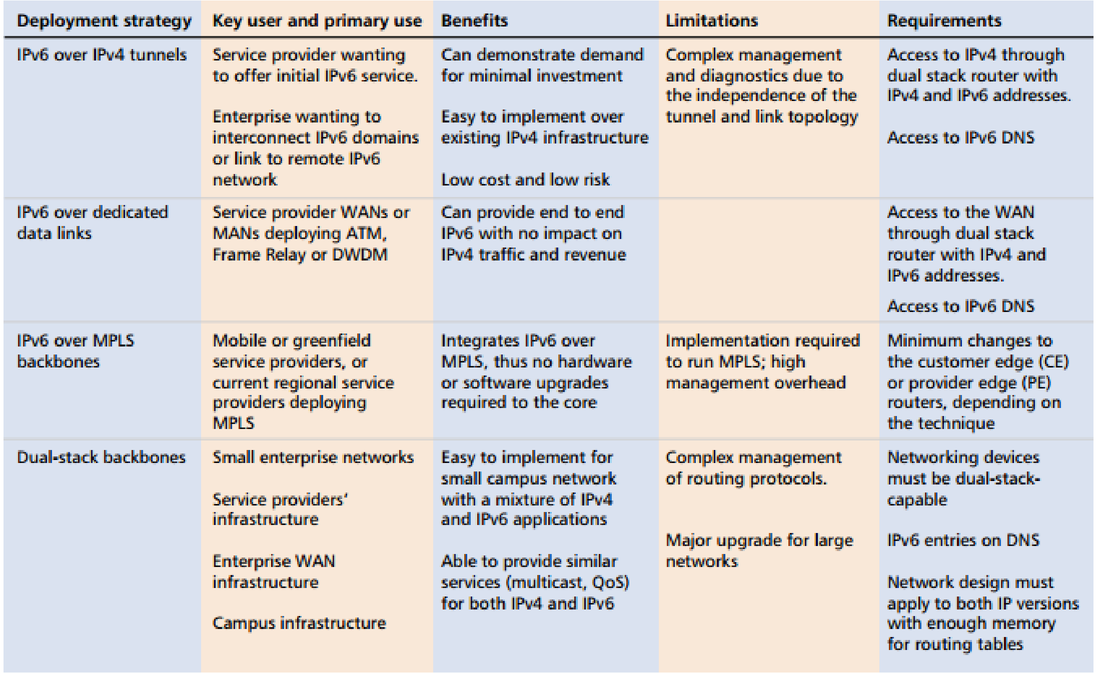
Mechanism	Primary use	Benefits	Limitations	Requirements
IPv6 using tunnels on CE routers	Enterprise customers wanting to use IPv6 over existing MPLS services	No impact on MPLS infrastructure	Scalability issue when the number of tunnels grow between CEs	Dual-stack CE routers
IPv6 over a circuit transport over MPLS	Service providers with ATM or Ethernet links to CE routers	Fully transparent IPv6 communication	No mix of IPv4 and IPv6 traffic	Need layer 2 transport layer over MPLS
IPv6 Provider Edge router (6PE) over MPLS	Internet and mobile service providers wanting to offer an IPv6 service	Low-cost and low-risk upgrade to the PE routers, and no impact on MPLS core	Applicable to MPLS infrastructure only	Software upgrade for PE routers
IPv6 VPN Provider Edge router (6VPE) over MPLS	Internet and mobile service providers wanting to offer IPv6 VPN services	Low-cost and low-risk upgrade to the PE routers and no impact on MPLS core	Applicable to MPLS infrastructure although the implementation could be done for other tunneling techniques. IPv6 address leakage on the global routing table must be well controlled	VPN or VRF support

Table 4 A comparison of all deployment or transition mechanisms[17].

3.1.5 Design Requirements & Establishing Roadmap for IPv6 Deployment

when network designers prefer an IPv6 integration strategy to begin from the edges of the network and moving to the core, this allows control of deployment cost and focus on the needs of the applications, rather than a complete full upgrade to the original IPv6 network.

Various deployment strategies allow the early stages of the transition to IPv6 to happen now, whether it is piloting IPv6 capabilities or controlling early stages of major IPv6 network applications. Table (5) compares the different deployment strategies in terms of the primary use, benefits, limitations and requirements of each strategy.



Deployment strategy	Key user and primary use	Benefits	Limitations	Requirements
IPv6 over IPv4 tunnels	Service provider wanting to offer initial IPv6 service. Enterprise wanting to interconnect IPv6 domains or link to remote IPv6 network	Can demonstrate demand for minimal investment Easy to implement over existing IPv4 infrastructure Low cost and low risk	Complex management and diagnostics due to the independence of the tunnel and link topology	Access to IPv4 through dual stack router with IPv4 and IPv6 addresses. Access to IPv6 DNS
IPv6 over dedicated data links	Service provider WANs or MANs deploying ATM, Frame Relay or DWDM	Can provide end to end IPv6 with no impact on IPv4 traffic and revenue		Access to the WAN through dual stack router with IPv4 and IPv6 addresses. Access to IPv6 DNS
IPv6 over MPLS backbones	Mobile or greenfield service providers, or current regional service providers deploying MPLS	Integrates IPv6 over MPLS, thus no hardware or software upgrades required to the core	Implementation required to run MPLS; high management overhead	Minimum changes to the customer edge (CE) or provider edge (PE) routers, depending on the technique
Dual-stack backbones	Small enterprise networks Service providers' infrastructure Enterprise WAN infrastructure Campus infrastructure	Easy to implement for small campus network with a mixture of IPv4 and IPv6 applications Able to provide similar services (multicast, QoS) for both IPv4 and IPv6	Complex management of routing protocols. Major upgrade for large networks	Networking devices must be dual-stack-capable IPv6 entries on DNS Network design must apply to both IP versions with enough memory for routing tables

Table 5 A comparison of all deployment or transition mechanisms[17].

For Establishing a customized roadmap, we can present a basic adoption approach look like this [38]:

Phase 1 Start with Internet-facing services: This phase uses dual-stack to maintain full IPv4 functionality, while establishing an IPv6 Internet presence.The implementation ought to start with external-facing connectivity addressing Internet connectivity; reach to users, partners and mobileendpoints. The capability for IPv6 isbrought into data centres and hosted sites. The impact focuses on security,impacting firewalls, web servers,router ISP .

Phase 2: Enables users to access IPv6 Internet Once IPv6 has been enabled externally, the next step would be to deploy it internally, allowing internal users to access IPv6 on more endpoints and talk inside the network. Tunneling mechanisms or Proxy servers are options to for IPv4 users on the privatenetwork to access the IPv6 network.

Phase 3: Migration of WAN to dual-stack,where IPv6 support is extended to remote locations which is the final phase in the approach. Private internal networks become IPv6 capable, including MPLS/VPN,routers and private lines. Mobility and unified communication applicationsare moved to dual-stack. Depending on their specific needs, companies can choose to remain in this phase for some time, fully enabled on both protocols.

Phase 4: Application migration) impacts the applications and screens, such as reporting tools. All internal application and network management tools will be migrated to a purely IPv6 protocol.

3.1.6 Security Issues in IPv6 Protocol

The Communications through any public medium such as the Internet are usually unprotected and vulnerable to hacking by unauthorized persons, so a research team The Internet (IETF) has adopted a security protocol called IPsec (Internet Protocol Security
In IP version VI, IPsec provides integrated point-to-point security protection Receiving (Point-to-Point) is the confidentiality, privacy, and reliability of data and without any impact on the adequacy of the communication protocol, as it usually uses several encryption algorithms such as DES, AES or 3DES algorithm, for the purpose of protecting important and confidential data being transmitted Through the Internet and using IPv6 (.)

3.1.6.1. IPv6 Security Risks

The security issue became one of the most common topics in IPv6, we summarize them as follows [39]:

- Tracking the identity of the user.
- IPv6 address spoofing i.e., changing the MAC address spoofing IPv6.
- Weakness in the large address space (space vulnerability).
- Weakness in the process of giving multiple addresses vulnerability
- The security gap in the multicast (Multicast security) vulnerability
- Extension vulnerability in packet start size (header vulnerability)
- The vulnerability in the packet fragmentation process
- The security gap in the process of discovering and petitioning the neighbour in connection with this, many international companies have begun to perform extensive tests on the sixth version of the protocol.

3.1.6.2. Comparison of IPv4 and IPv6 Security Weaknesses

When moving from IPv4 to IPv6 the network layer of the OSI model (layer 3) changes. Hence, all security weaknesses that attack the layers below or above the network layer remain the same, e.g. cross-site scripting attacks in a web application. Little differences are in attacks against the local area network that use the Neighbor DiscoveryProtocol (NDP) instead of the Address Resolution Protocol (ARP). The classical ARP spoof is now called Neighbor Advertisement spoof, but the impact to the local network is the same. Amplification attacks now use the concept of multicast instead of broadcast, and rogue DHCPv6 serverschange their protocol from DHCPv4.
Security threats that are new to IPv6 are related to multicast, extension headers, an ICMPv6.

An advantage even for security reasons is the vast address space of IPv6. It is now possible to divide the infrastructure into small subnets in order to enforce security already on the network layer with appropriate firewalls. Finally, due to the returned end-to-end communication model, IPsec can be used for securing channels betweensingle hosts, which adds more security options for communicating over the Internet.
In summary, IPv6 security is in many ways the same as IPv4 security" but since IPv6 is new to many network administrators and security specialists who have not experienced

IPv6indetail yet, it is more likely that an attacker can exploit some vulnerabilities due to misconfigured IPv6 nodes in a network.

3.1.6.3. Attacks against the Transition Methods

Unless IPv6 connectivity is not offered by all ISPs around the world, whether for big companies or for small office/home office DSL connections, This section covers security issues that arise with the usage of different transition mechanismThe concept of dual-stack is a full operating IPv6 stack as well as a full operating IPv4 stack on each node on the network, which are completely independent of each other. This means that both protocols must be fully supported by all security devices and applications.but , All IPv6 tunnel methods do not have any built-in security methods such as authentication, integrity or confidentiality. Thereby all tunnel mechanisms are applicable for the following securityattacks, [40]:

• Tunnel Sniffing: If an attacker sits in the IPv4 routing path he has full control over the IPv6 tunnel and can sniff the tunnel or even execute man-in-the-middle attacks.

• Tunnel Injection: The attacker can spoof the source IPv4 address of one tunnel endpoint and inject packets into the IPv6 network of the other tunnel endpoint. We note that the primary security problem with NAT64 is that it cannot be used with IPsec since it breaksthe end-to-end communication model. The protocol translation technique itself is vulnerable to a denial of service attack in which an inside IPv6 attacker initiates many outbound requests in order to deplete the IPv4 address .

3.1.6.4. Decreasing IPv6 Security Risks

Before deploying IPv6, we must be aware of the following security aspects [39]:

- Protection of the vulnerability in the automatic address assignment process.
- Preventing fake IPv6 routers.
- IPv6 packet protection.
- Protection of host computers from attacks.
- Controlling traffic over the Internet.
- Controlling packet traffic when performing the exchange process with the Internet.

There are many IPv6 Security Tools such as:

- **IP Stack Integrity Checker (ISIC):** For **testing the implementation** of a proposed
  standard a \fuzzer" tool can be used.
- **Nmap:** Nmap is a **network mapper** tool which discovers hosts on the network and open ports (services) on hosts.
- **Scapy:** In order to **create any type of packet** with forged values, Scapy is the appropriateprogram

3.2 IPv6 Deployment in Campus Networks

The IPv6 requirements in Campus networks differs from requirements in a WAN/branch environment, the main reason of this difference is that IPv6 must be forwarded using hardware which support high-performance needs[2].

There are many deployments models for IPv6 in Campus networks, the most used ones are the following:

1- Dual Stack Model (DSM):

This model is the most preferred model, and it is totally based on Dual-Stack transition mechanism, and both versions IPv4 and IPv6 are deployed simultaneously on the same device interface, but of course, simultaneous deployment for the two protocols will lead to extra expenses because everything will be doubled, such as addressing, management, routing protocols, and access control lists (ACL) [2].

It is very important to make sure that the network devices (such as switches) in the campus network support IPv6.

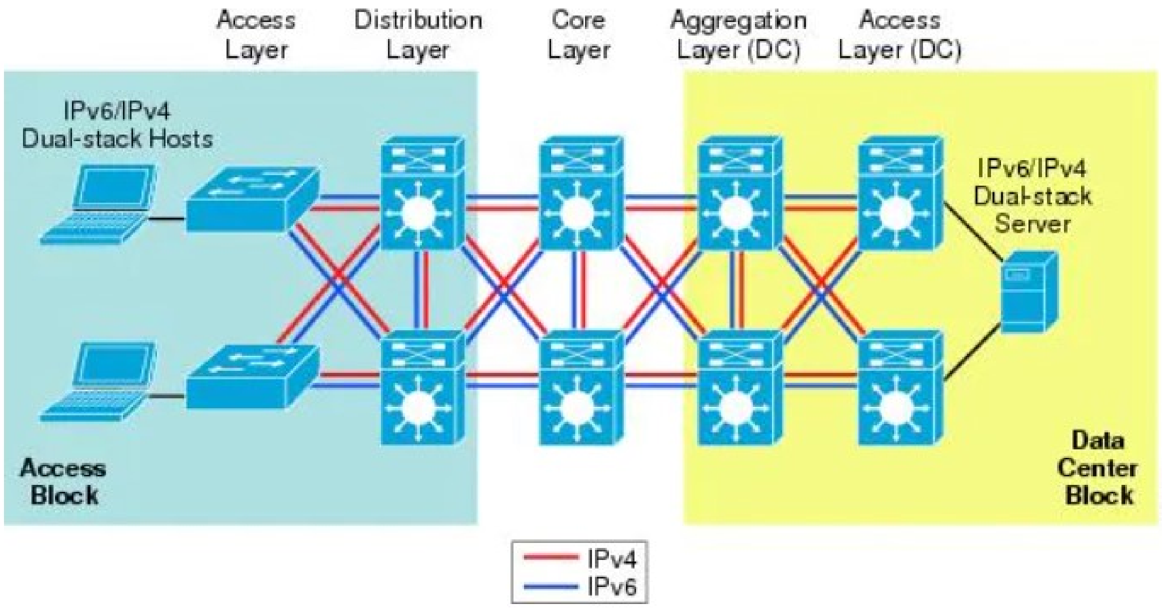
In dual-stack model IPv6 and IPv4 work independently in term of network services, such as routing, quality of service (QOS), high availability (HA), multicast policies, and security services.

Dual-stack model provides higher performance in packet processing, because the packets in this model are forwarded without the need for extra processes such as encapsulation and lookup processes.

Dual-Stack Model Network Topology:

The used environment in DSM is the classical campus three-tier design, which consists of the access, distribution, and core layer.

All the network devices interfaces are designed and configured to enable both IPv4 and IPv6 addresses, which make it a pure dual-stack model.



Picture 17 Dual-stack Model Topology[45].

2- Hybred Model (HM)

The word hybrid in HM refers to employing two or more independent transition mechanisms.

This model uses a tunneling mechanisms based on host devices, these mechanisms encapsulate the IPv6 addresses in IPv4 addresses when the need occurs and uses the dual-stack mechanism everywhere else.

The HM uses the three main IPv6 transition mechanisms:

- **Dual-stack:** Deployment of two protocols IPv4 and IPv6.

- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP):** A mechanism uses a Host-to-router tunnel and depends on an existing IPv4 infrastructure.

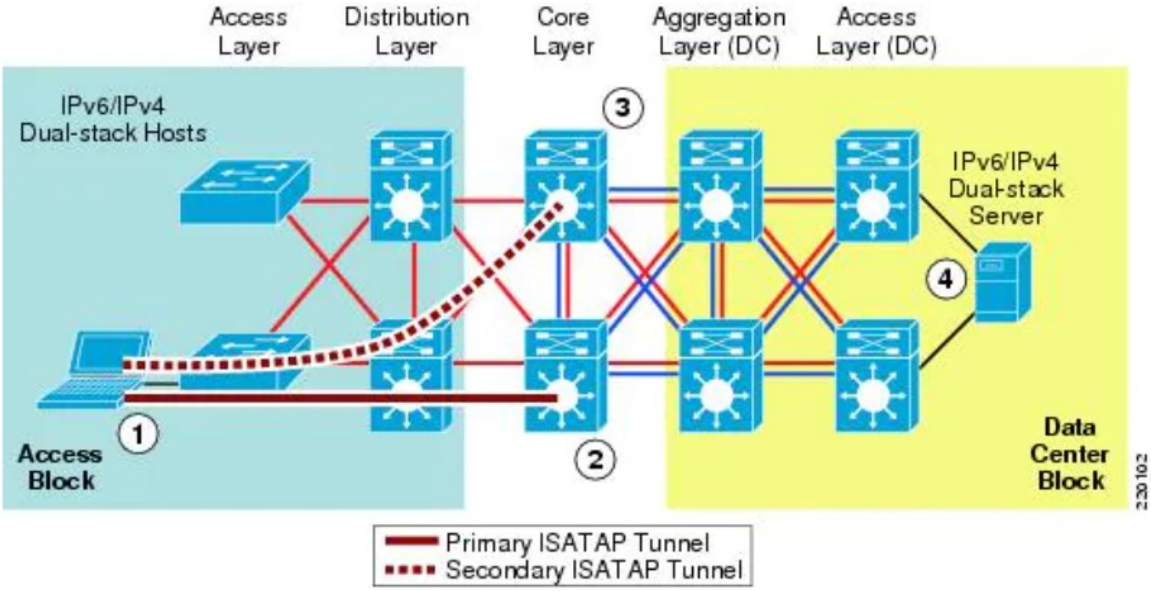
- **Manually configured tunnels:** A mechanism uses a router-to-router tunnel and depends on an existing IPv4 infrastructure as well.

The main benefit of hybrid model is making the hosts located in the access layer of campus network able to use IPv6 services when the distribution layer is not IPv6 enabled.

The distribution layer switch is most commonly the first Layer 3 gateway for these devices (hosts and switches) which are located in the access layer.

If distribution layer switches don't have IPv6 enabled, the hosts won't be able to get their addresses from the DHCPv6 which had to be served from their gateway, and they won't be able as well to get the routing information, and subsequently won't be able to access the rest of the IPv6-enabled network.

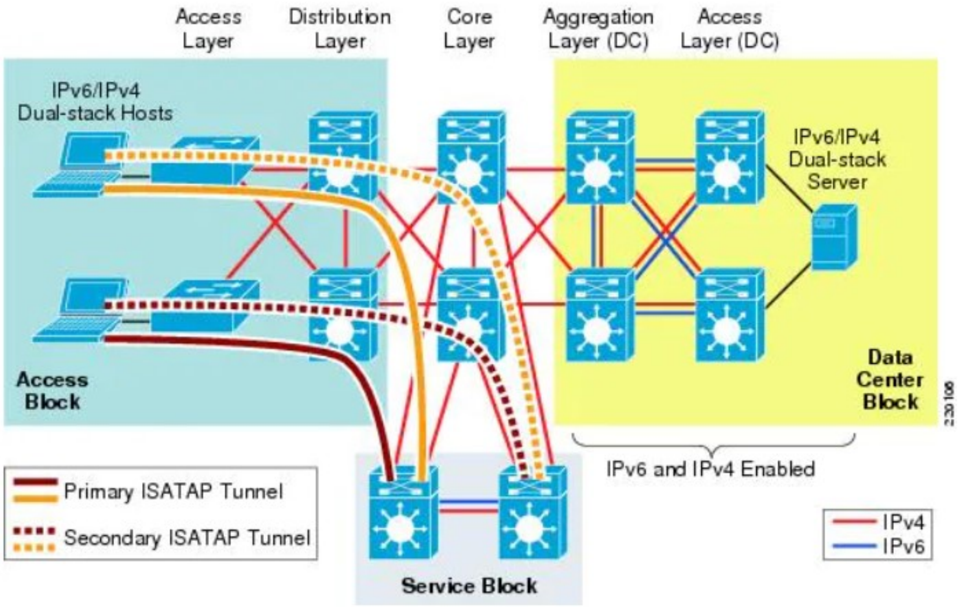
To solve this problem, the HM model establishes an ISATAP tunnel between the IPv6-enabled hosts and the core layer switches to provide the access to IPv6 services from the core switches.



Picture 18 HM using ISATAP tunnel to provide hosts with IPv6 services[45].

3- Service Block Model (SBM)

SBM is very different compared to other campus models. It is unique in that it can be deployed without any impact on the existing IPv4 network, and is fully centralized.When the current campus network becomes IPv6 capable, SBM can become decentralized. The connections in the SBM are changed from tunneling (ISATAP and/or manually configured) to dual stack connections. When all campus layers are capable of double-stacking, the SBM can be disassembled and redesigned for other uses.
The key to maintaining a scalable, multi-need configuration in SBM is to ensure that a high-performance, admin switch and modules are used to handle the ISATAP load, manually configured tunnels, and stacked duplex connections for the entire campus network.



Picture 19 Campus Service Block Model Example [45].

It is similar to the hybrid model in that it offers the same flexibility options and allows for the deployment of different transmission mechanisms based on application requirements, location, performance, and scalability.

However, in the hybrid model, existing network infrastructure devices are used to terminate the tunnel; But with the block model, all the transition mechanisms end in the newly created service block.

While the hybrid campus design uses the network design as it exists today, the service block model designer adds a new network layer (or block) to the existing network design used only for IPv6 and its various transmission mechanisms. In this way, it provides the ability to quickly deploy IPv6 services without modifying the existing network [44].

An important advantage of the service block design model is that with hardware upgrade, tunnels can be replaced by double stack links, eventually freeing up service block resources for other purposes, for example, an application hosted in a data center, an IPv6 capable application with hosts at the access layer to campus and who need access to this app.

ISATAP tunnels can be used from hosts, manually configured tunnels can be used from the data center aggregation layer, and both terminate on service block switches. As a network, components such as core layer switches become double-stack, and tunnels can be replaced by double-stack links. In the end, the entire service group can be removed and network equipment redirected.

We analyze various architectures for providing IPv6 services in campus networks.

Table (6) summarizes the benefits and challenges with each of the models.

Model	Benefit	Challenge
Dual-stack model (DSM)	No tunneling required No dependency on IPv4 (routing, QoS, HA, multicast, security, and management are separated) Superior performance and highest availability for IPv6 unicast and multicast Scalable	Requires IPv6 hardware-enabled campus switching equipment Operational challenges with supporting dual protocols—Training/management tools
Hybrid Model (HM)	Most of the existing IPv4-only campus equipment can be used (access and distribution layer) Provides high-availability for IPv6 access over ISATAP tunnels	Tunneling is required; massive increase in operations and management IPv6 multicast is not supported Causes core layer to become an access layer for IPv6 tunnels Requires IPv6-enabled hosts with ISATAP configuration
Service block model(SBM)	Highly reduced time-to-delivery for IPv6-enabled services Requires no changes to existing campus infrastructure Provides high-availability for IPv6 access over ISATAP tunnels Provides high-availability for IPv6 connectivity over configured tunnels	New IPv6 hardware capable, campus switches are required Tunneling is required (extensively) IPv6 multicast is not supported on the ISATAP tunnels Requires IPv6-enabled hosts & ISATAP configuration

Table 6 benefits and challenges of transtion cisco models

4 Practical Part

For practical part, various scenarios were implemented using GNS3 (2.2.19) network simulator which is one of the most accurate, agile, vendor-agnostic software and it has also got copious networking components. Moreover, it provides a great GUI which any complex topologies can be implemented easily. All the analysis of the topologies has been carried out using Wireshark packet analyser.

Wireshark is an open source, free and user-friendly packet analyser software which is generally used for troubleshooting, protocol development and analysis of data.

Similar topologies are built for Dual stack and tunnelling transition techniques.

To implement campus network, network for organization has many different departments, Finance, IT, HR and Sale has been proposed.

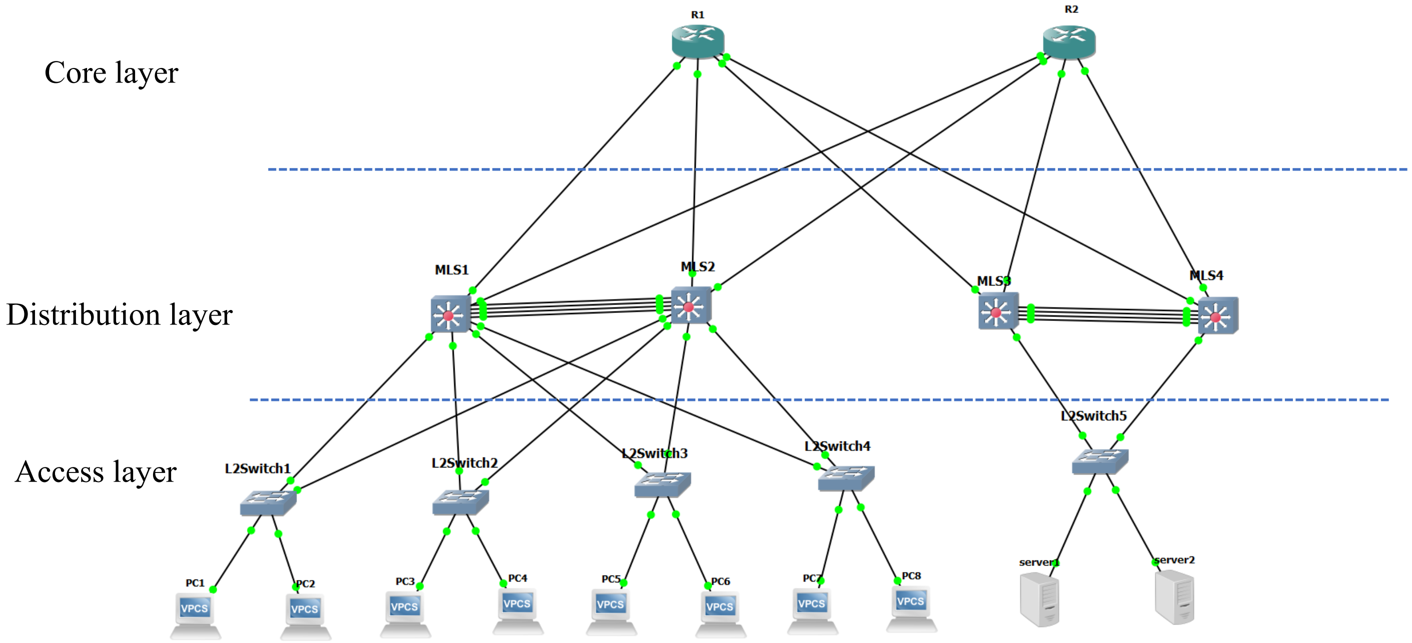
4.1 Campus network design

Hierarchical network design is used in campus network that involves dividing the network into discrete layers. Each layer in the hierarchy provides specific functions that define its role within the overall network. This helps to optimize and select the right network hardware, software and features to perform specific role for that network layer.

LAN campus network design includes the following three layer:

- **Access layer**: Provides workgroup access to the network.
- **Distribution layer:** Provides policy-based connectivity and control the boundary between the access and core layer.
- **Core layer:** Provides fast transport between distribution switches within enterprise campus.

Picture 20 shows Hierarchical network design of campus.



Picture 20 Hierarchical network design of campus.

The ***access layer*** incorporates five Layer 2 switches and access points providing connectivity between workstations and servers.

The ***distribution layer*** aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. In picture the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

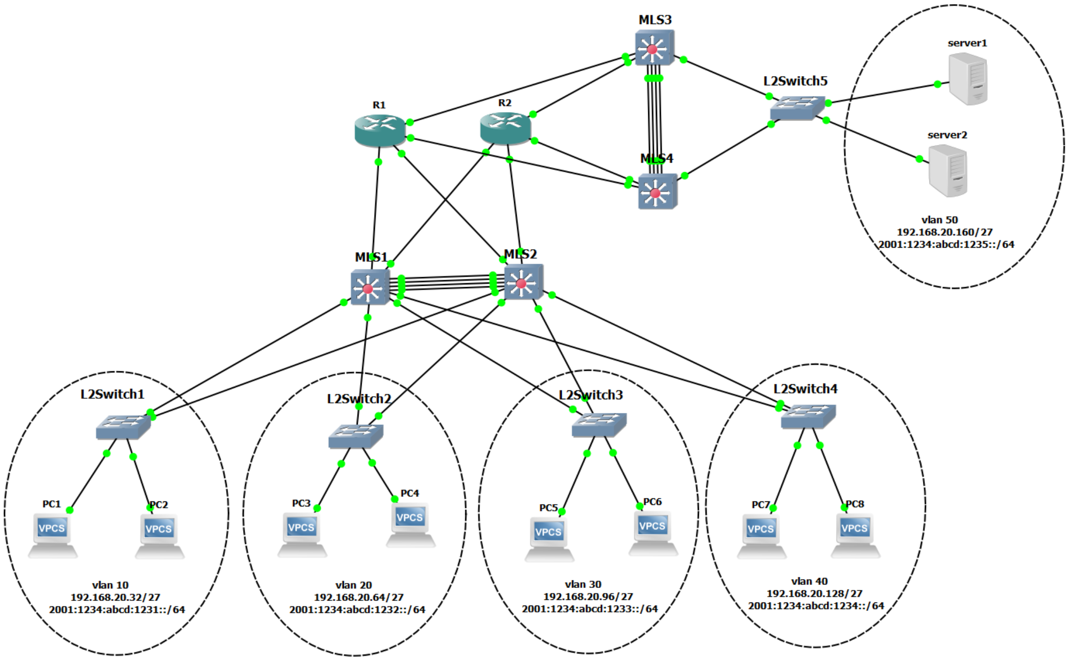
The ***core layer*** is also referred to as the network backbone. The core layer consists of high-speed network devices. These are designed to switch packets as fast as possible and interconnect multiple campus components, such as distribution modules, service modules, and the data center.

Core layer can be used later to connect distribution WAN and Internet Edge.

As shown in picture additional instance of network devices and lines of communication were added to help ensure network availability and decrease the risk of failure along the critical data path.

4.2 Dual Stack mechanism

All of network devices in Picture 21 are configured with IPv4 and IPv6 i.e., all used devices in this network are dual stack/ dual IP configured devices.



Picture 21 Dual stack topology

To implement campus network, the following steps were followed:

- Assigning IPv4 and IPv6 addresses for all interfaces. class C IPv4 address that is 192.168.20.0/24 dividing into eight subnets was used, six of them were used and the rest of them were reversed for future scalability.

  Subnet 192.168.20.0/27 is subnetted to /30 for all distribution connections to the core.

  Subnet 192.168.20.32/27 is used for IT department, Subnet 192.168.20.64/27 is used for Sale department, Subnet 192.168.20.96/27 is used for IT department, Subnet 192.168.20.128/27 is used for IT department and Subnet 192.168.20.160/27 is used for IT department.

For IPv6 addressing, network address 2001:1234:abcd:1231::/64 is used for VLAN 10, network address 2001:1234:abcd:1232::/64 is used for VLAN 20, network address 2001:1234:abcd:1233::/64 is used for VLAN 30, network address 2001:1234:abcd:1234::/64 is used for VLAN 40 and network address 2001:1234:abcd:1235::/64 is used for VLAN 50.

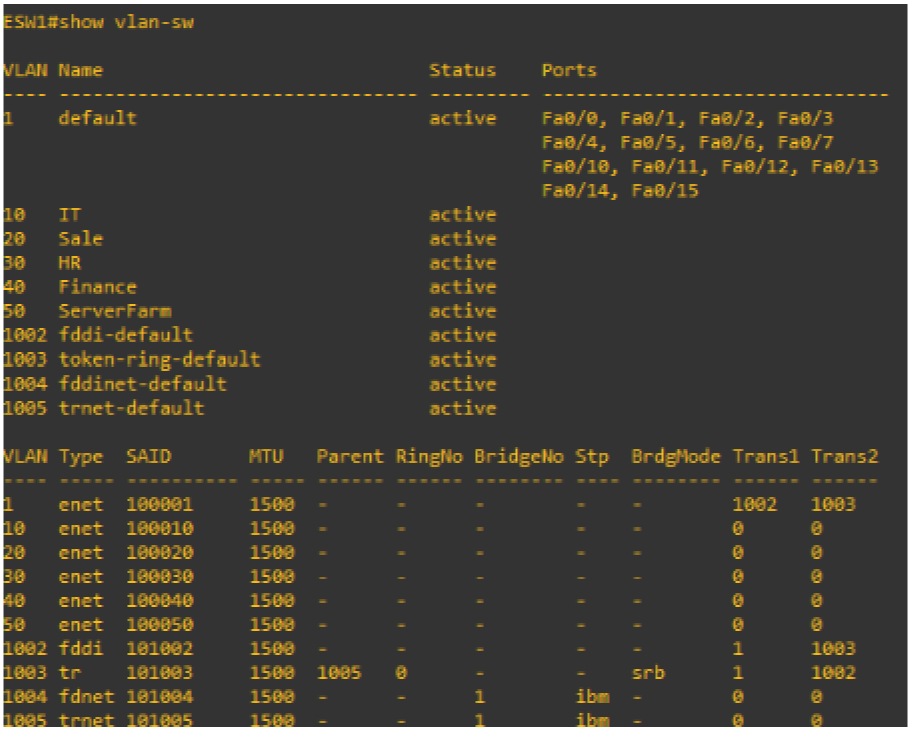
- Creating VLANs (vlan 10 name IT, vlan 20 name Sale, vlan 30 name HR, vlan 40 name Finance and vlan 50 name ServerFarm).

  VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

  VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other.

  VLANs tend to be flexible because they are based on logical connection, rather than physical.

  Picture 22 shows show vlan-sw command in multilayer switch MLS1:



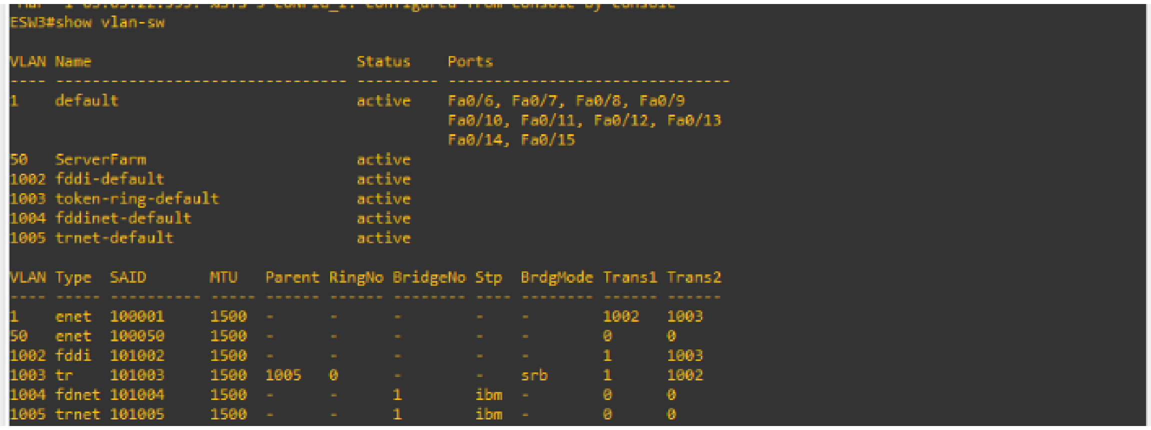
```
ESW1#show vlan-sw

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/0, Fa0/1, Fa0/2, Fa0/3
                                                Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15
10   IT                               active
20   Sale                             active
30   HR                               active
40   Finance                          active
50   ServerFarm                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Picture 22 show vlan-sw command in MLS1

Picture 23 shows show vlan-sw command in multilayer switch MLS2:



```
ESW3#show vlan-sw

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15
50   ServerFarm                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
50   enet  100050     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

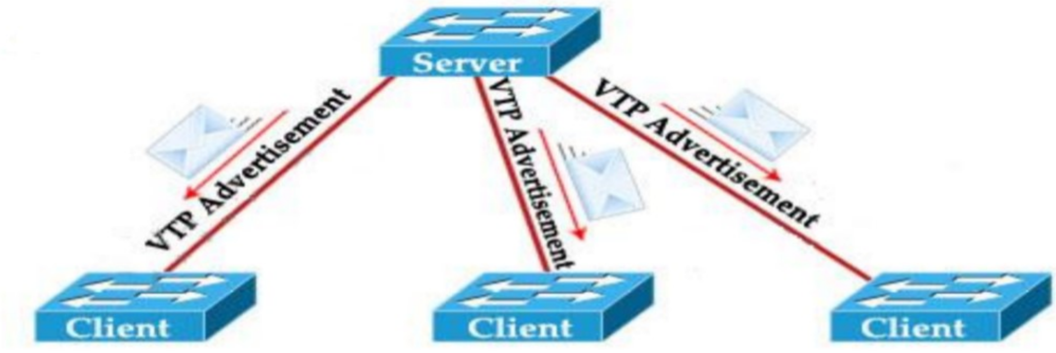
Picture 23 show vlan-sw command in MLS3

- Configuring a Cisco-priority protocol VTP that is available in most of the Cisco Catalyst series products, is used to reduce administration in switched network; When a new VLAN on one VTP server is configured, this VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

switches can be configured in three modes: server, client or transparent using VTP.

VTP server help to advertise the VTP domain VLAN information also VTP client enables to store the VLAN information for the entire domain when the switch is on.

VTP advertisements mechanism is showed in picture 21:



Picture 24 VTP advertisement mechanism

MLS1, MLS2, MLS3 and MLS4 which are multilayer switch were configured as VTP server and L2switch1, L2switch2, L2switch3, L2switch4 and L2switch5 were configured as VTP client.

They all were configured in the same VTP domain (campus.com) so they can share their VLANs information.

VLAN 10, VLAN 20, VLAN 30 and VLAN 40 were created on MLS1. VLAN 50 was created on multilayer switch MLS3.

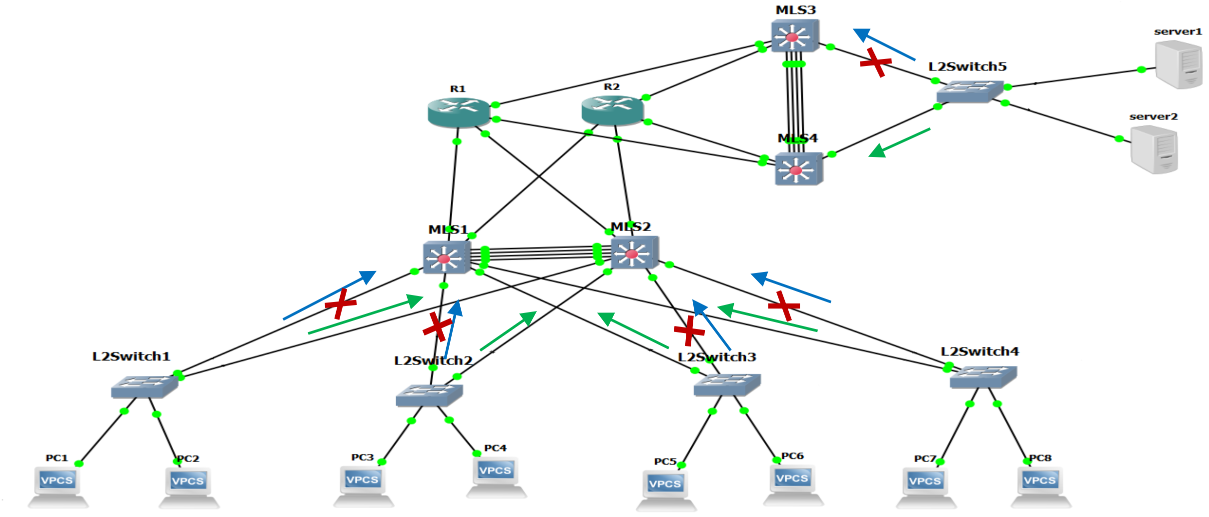
then multilayer switches advertise VLAN information through trunk links and layer 2 switches store VLANs information that is advertised.

- Configuring Spanning Tree Protocol (STP) which is a layer 2 protocol that runs on bridges and switches. The main purpose of STP is to ensure that we do not create any loop when we have redundant paths in the network.

  Network is configured with redundant paths because redundancy can help protect against disaster, it can also lead to switch looping. Looping occurs when data travels from a source to destination along redundant paths and data begins to circle around the same paths, becoming amplified and resulting in a broadcast storm.

  MLS1 was configured as a primary root of VLAN 10 and VLAN 20, MLS2 was configured as primary root of VLAN 30 and VLAN 40 and MLS3 was configured as primary root of VLAN 50.

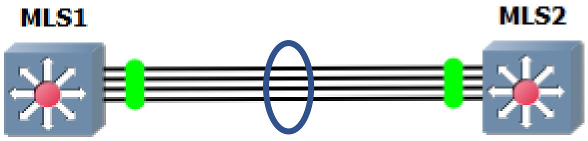
  In the picture 25 shown below, the access switches have redundant paths if the paths shown in blue fails as shown by the red X, the frames would take the new path shown by the green arrow.



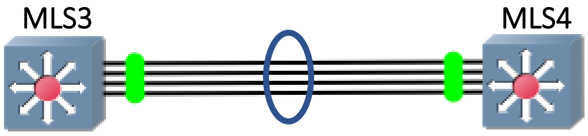
Picture 25 STP protocol effect

- Configuring EtherChannel which is a link aggregation technology used primarily on cisco switches. EtherChannel enables bundling of multiple physical Ethernet links to create one logical Ethernet link which provides high throughput and resilient links.

  EtherChannel between two multilayer switches (MLS1 and MLS2) was configured, and another one was configured between the multilayer switches MLS3 and MLS4 as the pictures shown below.



Picture 26 Etherchannel between MLS1 and MLS2



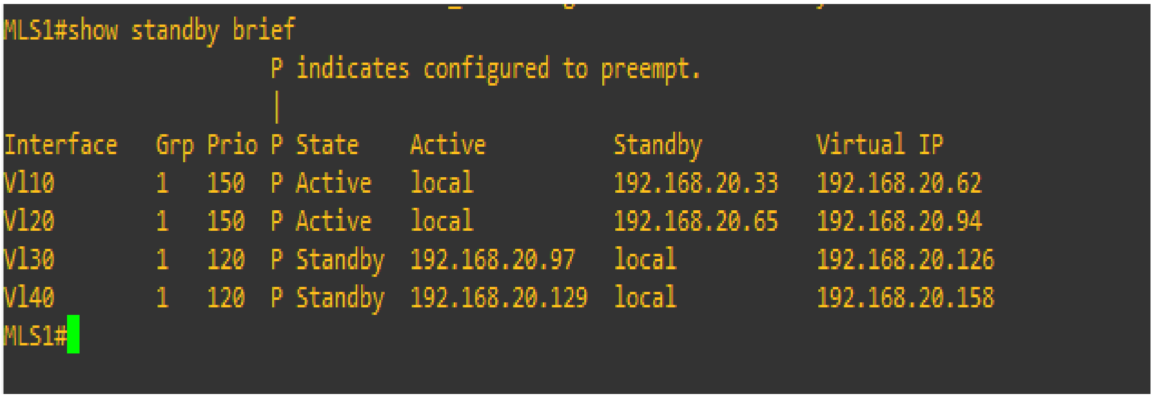
Picture 27 Etherchannel between MLS3 and MLS4

- Configuring Hot Standby Routing Protocol HSRP which allows to configure two or more routers as standby routers and only a single router as an active router at a time. All the routers in a single HSRP group shares a single MAC address and IP address, which acts as a default gateway to the local network. The *Active router* is responsible for forwarding the traffic. If it fails, the *Standby router* takes up all the responsibilities of the active router and forwards the traffic.

  Priority 150 was given to interface VLAN 10 and VLAN 20 and priority 120 was given to interface VLAN 30 and interface VLAN 40 in multilayer switch MLS1.

  Priority 150 was given to interface VLAN 30 and VLAN 40 and priority 120 was given to interface VLAN 10 and interface VLAN 20 in multilayer switch MLS2.

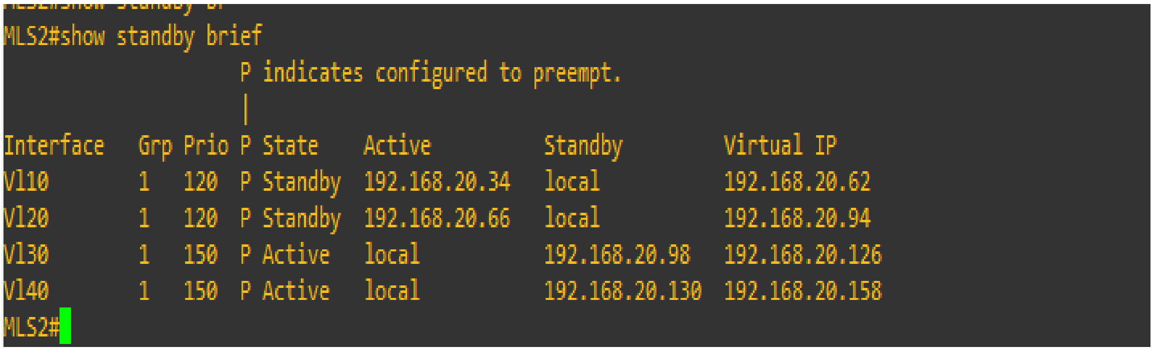
  So MLS1 works as standby for VLAN 10 and VLAN 20, and active for VLAN 30 and VLAN 40.



```
MLS1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        1   150  P Active   local           192.168.20.33   192.168.20.62
Vl20        1   150  P Active   local           192.168.20.65   192.168.20.94
Vl30        1   120  P Standby  192.168.20.97   local           192.168.20.126
Vl40        1   120  P Standby  192.168.20.129  local           192.168.20.158
MLS1#
```

Picture 28 show standby brief command in MLS1

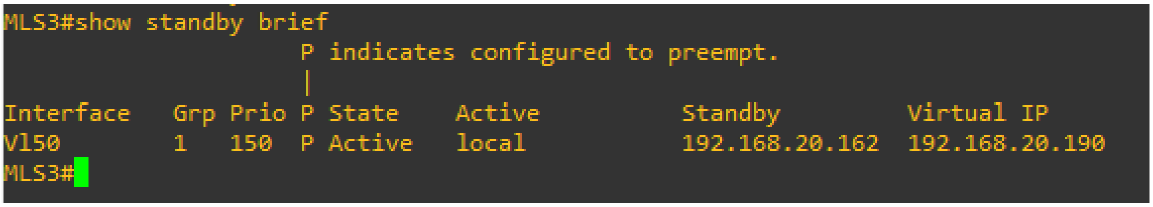
MLS2 works as standby for VLAN 30 and VLAN 40, and active for VLAN 10 and VLAN 20.



```
MLS2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl10        1   120  P Standby  192.168.20.34   local           192.168.20.62
Vl20        1   120  P Standby  192.168.20.66   local           192.168.20.94
Vl30        1   150  P Active   local           192.168.20.98   192.168.20.126
Vl40        1   150  P Active   local           192.168.20.130  192.168.20.158
MLS2#
```

Picture 29 show standby brief command in MLS2

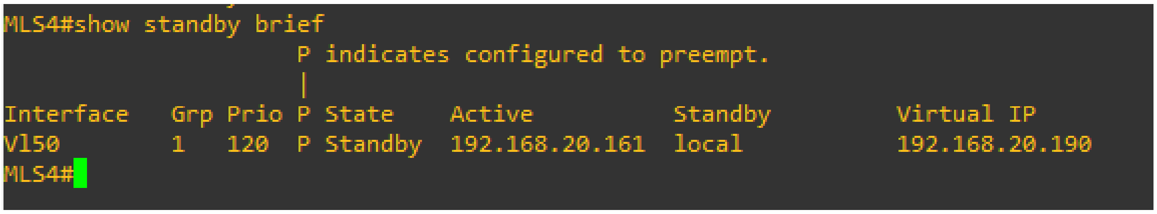
MLS3 works as active for VLAN 50.



```
MLS3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Vl50        1    150  P Active   local           192.168.20.162  192.168.20.190
MLS3#
```

Picture 30 show standby brief command in MLS3

MLS4 works as standby for VLAN 50.



```
MLS4#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Vl50        1    120  P Standby  192.168.20.161  local           192.168.20.190
MLS4#
```

Picture 31 show standby brief command in MLS4

- Configuring routing protocol. OSPF for IPv4 and OSPFv3 for IPv6.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the Autonomous System, so that every router within the AS has a complete picture of the topology of the Autonomous System. This picture is then used to calculate end-to-end paths through the Autonomous System, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra- and inter-area, and AS external routes and virtual links. It differs from its IPv4 counterpoint in a number of respects, including the following: Peering is done through link-local addresses and the protocol is link based rather than network based. Point-to-point links are also supported in order to enable operation over tunnels. It is possible to enable OSPF and OSPFv3 at the same time. OSPF works with IPv4, and OSPFv3 works with IPv6.

4.3 ISATAP tunnelling mechanism

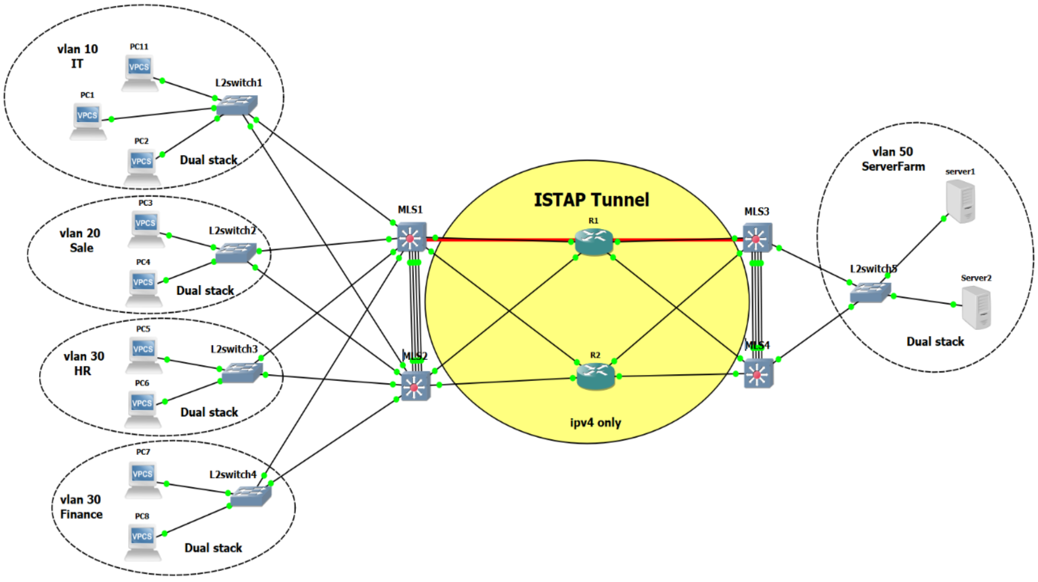
For ISATAP tunnel scenario that is simillar to the previous one, was proposed but in this network, core layer works with IPv4 only and the rest of it works with IPv4 and IPv6.

When configuring ISATAP tunneling, there are 2 modes involved.

- **ISATAP router** (it can be a router or server like Windows Server) which has the IPv6 capabilities enabled and it advertise the network which nodes can use to configure the IPv6 address when connected to the Ethernet interface.
- **ISATAP Client** establishes a static tunnel to the server and requests for IPv6 address. Usually end hosts will be ISATAP clients such as Windows PC with IPv6 enabled initiates the tunnel with ISATAP router.

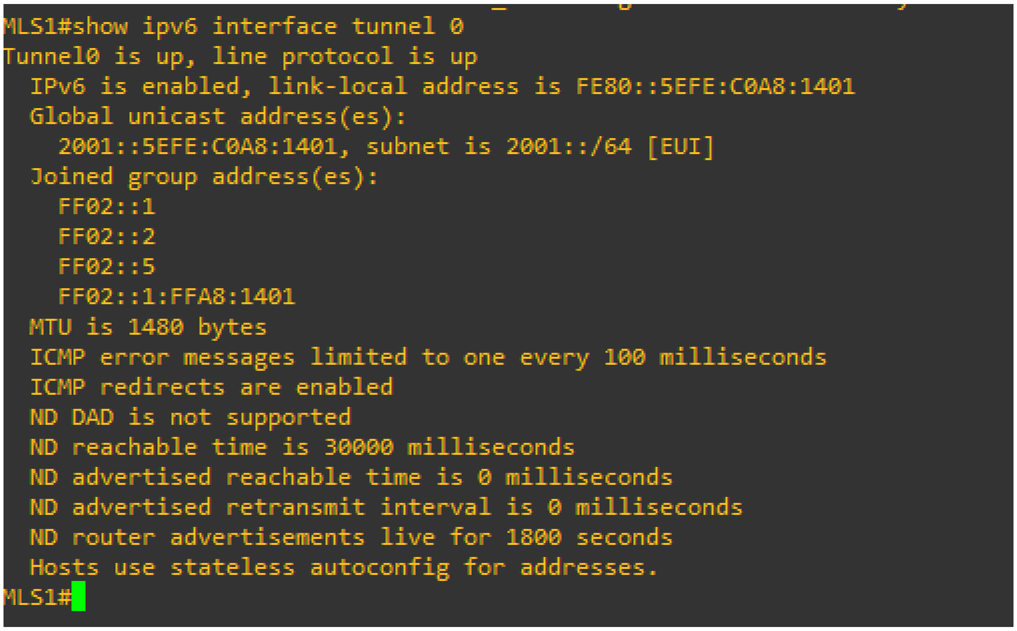
The ISATAP router/server uses unicast addresses that include a 64-bit IPv6 prefix and a 64-bit interface identifier. The interface identifier is created in modified EUI-64 format in which the first 32 bits contain the value **000:5EFE** to indicate that the address is an **IPv6 ISATAP address.**

MLS1 was supposed as ISATAP server and MLS3 as ISATAP client so any pc can ping any server in vlan 50. network topology is shown in picture 32.



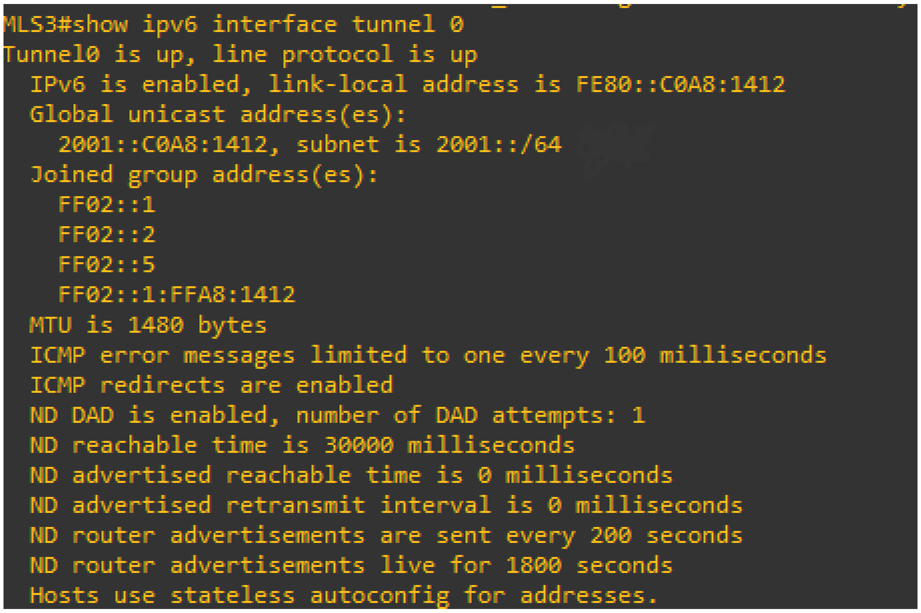
Picture 32 ISATAP topology

In the follwing picture 33 and picture 34 show the ISATAP tunnel in the side of server and on the side of client.



```
MLS1#show ipv6 interface tunnel 0
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::5EFE:C0A8:1401
  Global unicast address(es):
    2001::5EFE:C0A8:1401, subnet is 2001::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FFA8:1401
  MTU is 1480 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is not supported
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
MLS1#
```

Picture 33 ISATAP server configurations



```
MLS3#show ipv6 interface tunnel 0
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C0A8:1412
  Global unicast address(es):
    2001::C0A8:1412, subnet is 2001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::1:FFA8:1412
  MTU is 1480 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Picture 34 ISATAP client configurations

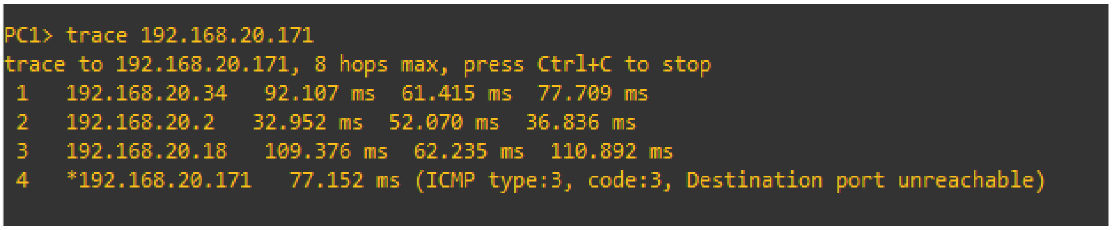
5 Results and Discussion

5.1 Network Latency

The Trace Route helps to find different routes the data-packet takes to reach the destination. It also finds the RTT (Round-trip time) of a data-packet to hit all intermediate routers. RTT is time taken for the packet to be sent from the source to that particular host and get acknowledgement from the host to source.

5.1.1 Network latency using Dual Stack Mechanism:

The picture 35 gives the detail about ICMPv4 sent from PC1 in vlan 10 to server1 in vlan 50. Trace Route command sends three datagrams at a time and so in the picture 35 three different times are seen. Each time period represents the time taken by particular datagram to reach the particular host.

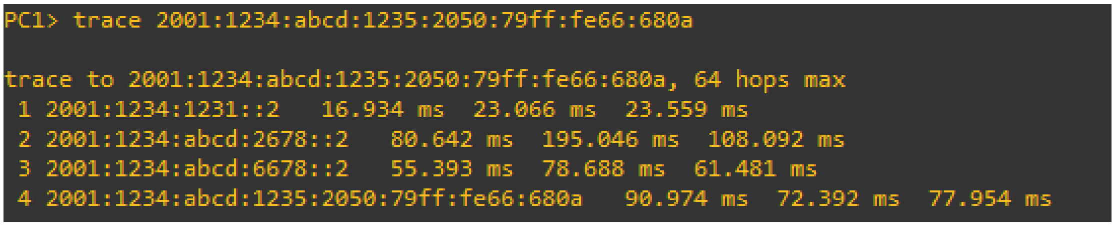


```
PC1> trace 192.168.20.171
trace to 192.168.20.171, 8 hops max, press Ctrl+C to stop
 1   192.168.20.34   92.107 ms  61.415 ms  77.709 ms
 2   192.168.20.2   32.952 ms  52.070 ms  36.836 ms
 3   192.168.20.18   109.376 ms  62.235 ms  110.892 ms
 4   *192.168.20.171   77.152 ms (ICMP type:3, code:3, Destination port unreachable)
```

Picture 35 Trace route Ipv4 ping from pc1 to server1 using dual stack mechanism

In most cases, RTT is treated as latency. So, latency of IPv4 packet to reach server1 from PC1 is 77.152 ms.

Picture 36 displays Trace route IPv6 ping from PC1 to server1 which has latency about 80.44 ms (avg).



```
PC1> trace 2001:1234:abcd:1235:2050:79ff:fe66:680a

trace to 2001:1234:abcd:1235:2050:79ff:fe66:680a, 64 hops max
 1 2001:1234:1231::2   16.934 ms  23.066 ms  23.559 ms
 2 2001:1234:abcd:2678::2   80.642 ms  195.046 ms  108.092 ms
 3 2001:1234:abcd:6678::2   55.393 ms  78.688 ms  61.481 ms
 4 2001:1234:abcd:1235:2050:79ff:fe66:680a   90.974 ms  72.392 ms  77.954 ms
```

Picture 36 Trace route Ipv6 ping from pc1 to server1 using dual stack mechanism

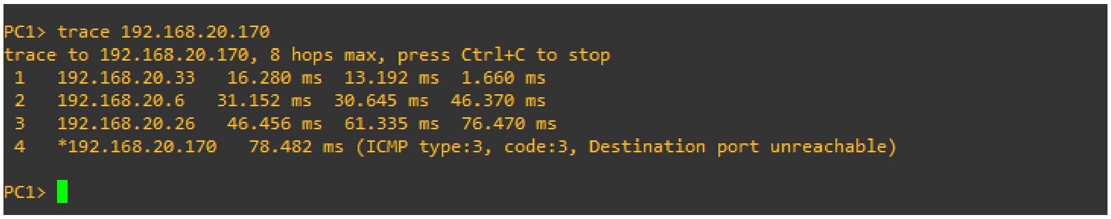
The following table results was obtained from several tests with different packet sizes were made:

Packet Size | Bytes	Latency Avg | ms (IPv4)	Latency Avg | ms (IPv6)
200	93.72	86.67
400	136.2	102.32
800	142.72	105.98

Table 7 Latency average for different packet sizes in IPv4 and IPv6 using Dual Stack Mechanism

5.1.2 Network latency using ISATAP Tunnelling Mechanism:

Picture 37 displays Trace route IPv4 ping from PC1 to server1 which has latency about 78.482 ms (avg).

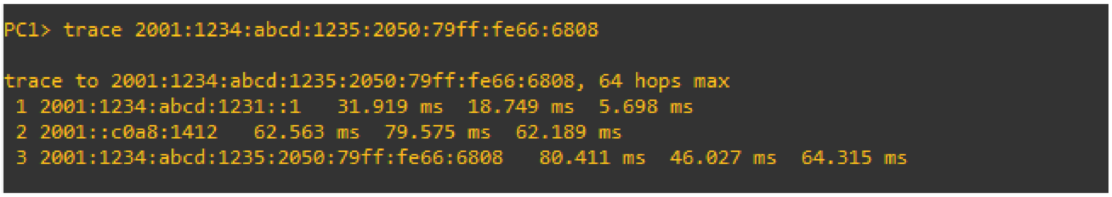


```
PC1> trace 192.168.20.170
trace to 192.168.20.170, 8 hops max, press Ctrl+C to stop
 1   192.168.20.33   16.280 ms  13.192 ms  1.660 ms
 2   192.168.20.6   31.152 ms  30.645 ms  46.370 ms
 3   192.168.20.26   46.456 ms  61.335 ms  76.470 ms
 4   *192.168.20.170   78.482 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Picture 37 Trace route Ipv4 ping from pc1 to server1 using ISATAP tunnel mechanism

Picture 38 displays Trace route IPv6 ping from PC1 to server1 which has latency about 63.584 ms (avg).



```
PC1> trace 2001:1234:abcd:1235:2050:79ff:fe66:6808

trace to 2001:1234:abcd:1235:2050:79ff:fe66:6808, 64 hops max
 1 2001:1234:abcd:1231::1   31.919 ms  18.749 ms  5.698 ms
 2 2001::c0a8:1412   62.563 ms  79.575 ms  62.189 ms
 3 2001:1234:abcd:1235:2050:79ff:fe66:6808   80.411 ms  46.027 ms  64.315 ms
```

Picture 38 Trace route Ipv6 ping from pc1 to server1 using ISATAP tunnel mechanism

The following results were obtained from several tests with different packet sizes were made:

Packet Size | Bytes	Latency Avg | ms (IPv4)	Latency Avg | ms (IPv6)
200	72.87	84.55
400	83.57	92.787
800	110.9	104.16

Table 8 Latency average for different packet sizes in IPv4 and IPv6 using ISATAB Tunneling Mechanism

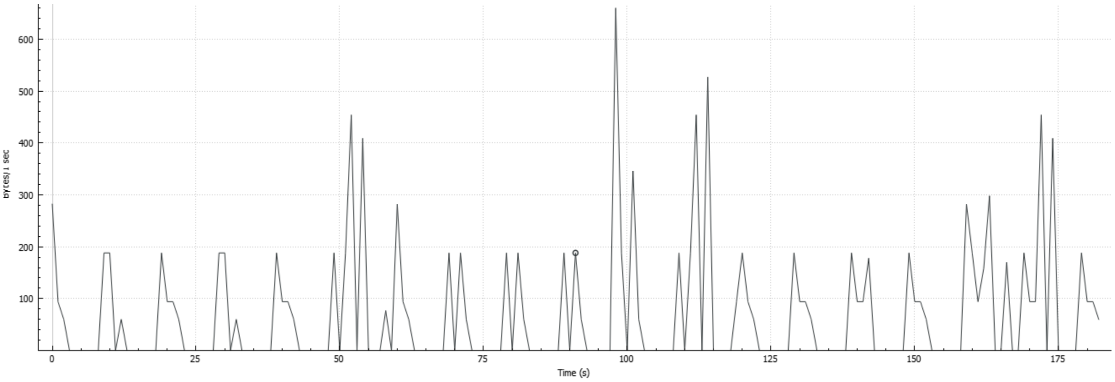
5.2 Network throughput

For the analysis in the topology, data passing the interface fa0/0 of R1 was captured using Wireshark packet analyzer.

In networking, throughput is defined as the amount of data transferred from one node to another in a specific time.

5.2.1 Network throughput using dual stack mechanism

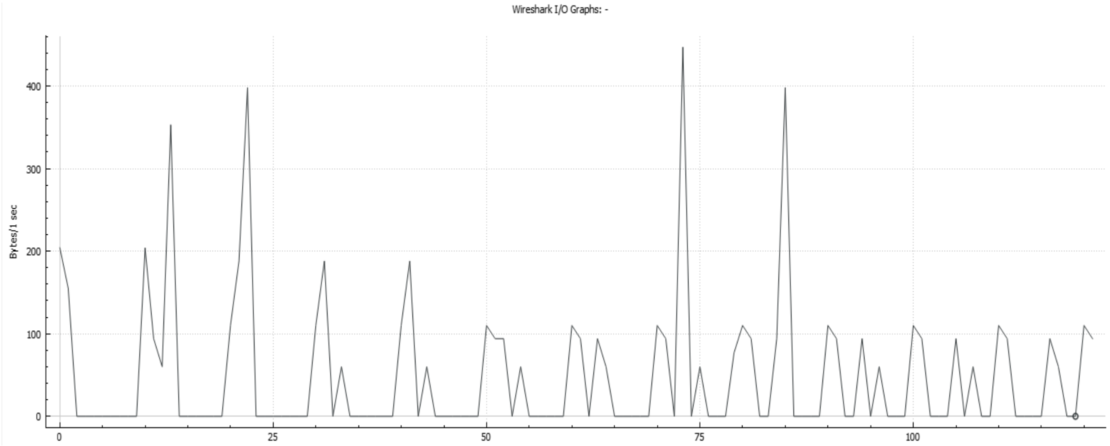
picture 51 provides network throughput in the network over time.



Picture 51 network trhouput analysis in dual stack mechanism

5.2.2 Network throughput using ISATAP tunnel mechanism

Picture 52 provides network throughput in the network over time.



Picture 52 network throughput analysis in ISATAP tunnel mechanism

6 Conclusion

In the past, IPv4 has proven its ability in terms of reliability, security and quick data transfer. But IPv4 uses 32-bit addresses allowing for a total of 4294967296 (2^{32}) addresses. That is a big problem with continuing to use IPv4.

To solve this problem, new techniques like NAT and IPv6 have been existed. But transition from IPv4 to IPv6 takes time. So, there is utmost necessity for transition techniques to play their role to establish smooth communication between both IP versions.

In the previous study, two techniques for transition from IPv4 to IPv6 in campus network were proposed which are dual stack and ISATAP tunnelling. Then network topologies were analysed with Wireshark packet analyser.

When two techniques were compared, the RTT or latency in Dual Stack was found higher than RTT in ISATAP tunnelling mechanism because of complexity involved in router.

On the other hand, after the comparison between network throughputs, the results shown that the Dual Stack is absolutely better than ISATAP tunnelling.

7 References

1- J. Postel, RFC 791: Internet Protocol (Internet Engineering Task Force), September 1981. [Online] http://www.ietf.org/rfc/rfc791.txt

2- Sophia A ,S,IPv6 Best Practices, Benefits,Transition Challenges and the Way Forward, ETSI ,White Paper No. 35, First ed August 2020 ISBN No. 979-10-92620-31-1.p71

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

4- Galla.l , Regmi.s, IPv4-IPv6 Transition Techniques, Bachelor's Thesis in Computer Communications, Technical report, School of Information Science, Computer and Electrical Engineering,Halmstad University ,May 2011

5- R. White, Working with IP Addresses (Cisco), March 2006. [Online] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/

6- Bosu1,R; Mondal,K; Talukdar.K.S; Md. Abu Zahed, Overview of IPv4, IPv6, Networking and Designing a Network Based on IPv4 in Shariatpur Polytechnic Institute's Campus, International Journal of Scientific & Engineering Research, Volume 7, Issue 9, September-2016 ISSN 2229-5518,p1426-1441

7- V. Fuller, T. Li and J.Yu, RFC 1519: Classless Inter-Domain Routing (CIDR: anAddress Assignment and Aggregation Strategy (Internet Engineering Task Force),September 1993.

8- S. Deering and R. Hinden, RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (Internet Engineering Task Force), December 1998. [Online] https://www.ietf.org/rfc/rfc2460.txt

9- "IPv6addressing",[Online]//www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/BN_Enterprise_IPv6_Addressing_Guide_H2CY10.pdf

10- Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6), Edited by: RegisDesmeules.

11- C. Partridge, Using the Flow Label Field in IPv6 (Internet Engineering Task Force), June 1995.

12- "IPv6Headers", [Online] //www.cu.ipv6tf.org/literatura/chap3.pDf, chapter 3, pp. 40-55, Des 12 1997

13- TR-101 Issue 2 Migration to Ethernet-Based DSL Aggregation BBF 2006.

14- TR-242 ,IPv6 Transition Mechanisms for Broadband Networks
Issue: 2

15- John J. Amoss & Daniel Minoli, Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporate Networks.

16- Hermann,S and Fabian .B, A Comparison of Internet Protocol (IPv6) Security Guidelines. Future Internet 6, 2014,p1-60; doi:10.3390/fi6010001

17- Tatipamula ,M& Grossetete,P. IPv6 Integration and Coexistence Strategies for Next-Generation Networks. IEEE Communications Magazine • ,January 2004,P88-96.

18- By Eun-Young Park, Jae-Hwoon Lee and Byoung-Gu Choe , an IPv4-to-IPv6 Dual StackTransition Mechanism Supporting Transparent Connections between IPv6Hosts and IPv4Hosts in Integrated IPv6/IPv4 Network 013132656;.

19- IPv6 supporting Operating systems. [Online] http://ipv6int.net/systems/index.html

20- M. Georgescu, L. Pislaru, G. Lencse, Benchmarking ethodology for IPv6transition technologies, IETF RFC 8219 (2017).doi: https://doi.org/10.17487/RFC8219.

21- D. G. Waddington and F. Chang, “Realizing the Transition to IPv6,” IEEE Commun. Mag., June 2002.

22- A. Hamarsheh, M. Goossens, “A Review: Breaking the Deadlocks forA. Hamarsheh et al. / Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 1, 336-341 (2021) [online]
www.astesj.com

23- K. Tsuchiya, H. Higuchi and Y. Atarashi, “Dual Stack Hosts using the "BumpIn-the-Stack" Technique (BIS),” California, USA: Internet Engineering Task Force RFC 2767, 2000.

24- S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand, “Dual Stack Hosts Using "Bump-in-the-API" (BIA),” California, USA: Internet Engineering Task Force RFC 3338, 2002.

25- B. Huang, H. Deng, T. Savolainen, “Dual-Stack Hosts Using "Bump-in-theHost" (BIH),” California, USA: Internet Engineering Task Force RFC 6535,2012.

26- X. Li, C. Bao, F. Baker, “IP/ICMP Translation Algorithm,” California, USA:Internet Engineering Task Force RFC 6145, 2011.

27- M. Bagnulo, P. Matthews, I. van Beijnum, “Stateful NAT64: NetworkAddress and Protocol Translation from IPv6 Clients to IPv4 Servers,” California, USA: Internet Engineering Task Force RFC 6146, 2011

28- G. Lencse, A. Soós, Design, implementation and testing of a tiny multithreaded DNS64 server, International Journal of Advances inTelecommunications, Electrotechnics, Signals and Systems 5 (2) (2016) pp.68–78.doi: http://doi.org/10.11601/ijates.v5i2.129

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

30- (MCMC)MCMC Tower 1 Selangor Darul Ehsan15,CODE OFs PRACTICE FOR THE DEPLOYMENT OF INTERNET PROTOCOL VERSION 6 (IPv6), , Malaysian Communications and Multimedia Commission Issue Date: February 2015.

31- B. Carpenter, K. Moore, Connection of IPv6 domains via IPv4 clouds, IETF RFC 3056 (2001).doi: https://doi.org/10.17487/RFC3056

32- F. Templin, T. Gleeson, D. Thaler, Intra-site automatic tunnel addressing protocol (ISATAP), IETF RFC 5214 (2008).doi: https://doi.org/10.17487/RFC5214

33- C. Huitema, Teredo: Tunneling IPv6 over UDP through network address translations (NATs), IETF RFC 4380 (2006) doi: https://doi.org/10.17487/RFC4380

34- A. Durand, P. Fasano et al., IPv6 tunnel broker, IETF RFC 3053 (2001).doi: https://doi.org/10.17487/RFC305

35- L. Martini et al., “Transport of Layer 2 Frames over MPLS,” IETF draft, draft-martini-l2circuit-trans-mpls-11.txt, work in progress, Apr. 2003.

36- J. De Clercq et al., “Connecting IPv6 Islands across IPv4 Clouds with BGP,” IETF draft, draft-ooms-v6ops-bgptunnel-00.txt, work in progress, Oct. 2002.

37- J. De Clercq et al., “BGP-MPLS VPN extension for IPv6 VPN,” IETF draft, draft-ietf-l3vpn-bgp-ipv6-01.txt, work in progress, Aug. 2003.

38- Tom Siracusa,5 Phases for IPv6 Adoption, [online] (2011), http://www.govtech.com/newsletters/5-Phases-for-IPv6-Adoption .html

39- Daaoud.I,H. Minimize IP security risks Sixth Version (IPV6), The Arab International Journal of Informatics, Volume 3, Issue 7, 2015 AD,P39-48.

40- Johannes Weber, IPv6 Security Test Laboratory, Ruhr-University Bochum, Germany, Master Thesis,p189.

41- 4294book.fm, September 26, 2003 .

42- Juniper Networks, Inc., Campus Networks refereNCe arChiteCture ,8030007-001-EN Apr 2009

43- R. White, IPv6: How to Get Started (Cisco), 2010 p1-5

44- R. White Federal Agencies and the Transition to IPv6 (Cisco), 2007. p1-7. http://www.cisco.com/ipv6.

45- MCFARLAND ,SH. *Deploying IPv6 in Campus Networks* Last Updated: Corporate Headquarters: Cisco Systems, February 27, 2012.

46- Tim Chown, IPv6 Campus Transition Experiences, Southampton SO17 1BJ, United Kingdom ,tjc@ecs.soton.ac.uk.

47- A. Al-hamadani1, G. Lencse1. *A survey on the performance analysis of IPv6 transition technologies*, Acta Technica Jaurinensis, Vol. 14, No. 2, pp. 186-211, 2021