An Efficient Approach of Converting an IPv4 Network to IPv6 Network through Dynamic Enhance Interior Gateway Routing Protocol

Submitted by
Md. Mazharul Haq Bhuiyan.
ID: 2013 – 2 – 96 – 008

Supervised by
Dr. Md. Nawab Yousuf Ali.
Associate Professor
Department of CSE

A Project Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science and Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

EAST WEST UNIVERSITY BANGLADESH

May 2015

ABSTRACT

Network dependent initiatives like cloud, 3G, virtualization and BYOD are rapidly consuming the last remaining IPv4 addresses. Organizations need to develop an IPv6 Network for that the project will going to establish an efficient approach to convert an IPv4 network to IPv6 Network where to optimum use of Bandwidth with EIGRP will be implementing. In this project we convert a existing IPv4 Network to IPv6 network thro our efficient Approach which is the sequential step of table to generate IPv4 to IPv6 topology and IPv4 Address to IPv6 Address and configure all the devices according to IPv6 topology and IPv6 address on Packet tracer Simulation .Here the theoretical analyses prove that the proposed approach works well in the simulation of EIGRP IPv6 network.

DECLARATION

I hereby, declare that all the work presented in this project is the outcome of the investigation and research performed by me under the supervision of Dr. Md. Nawab Yousuf Ali, Associate Professor, Department of Computer Science and Engineering, East West University, Dhaka, Bangladesh. I also declare that neither it nor part of it has been submitted for the requirement of any degree or diploma or for any other purposes.

Countersigned	Signature
… … … … … … … …	… … … … … … … … … …
(Dr. Md. Nawab Yousuf Ali) Associate Professor Department of CSE East West University Dhaka, Bangladesh **Supervisor**	Md. Mazharul Haq Bhuiyan candidate

LETTER OF ACCEPTANCE

The project entitled “An Efficient Approach of Converting an IPv4 Network to IPv6 Network through Enhanced Interior Gateway Routing Protocol: A Project” is submitted by Md. Mazharul haq Bhuiyan , Id: 2013 – 2 – 96 – 008 to the department of Computer Science and Engineering, East West University, Dhaka 1212, Bangladesh, is accepted by the Department for the partial fulfillment of the requirements for the degree of MS in Computer Science and Engineering.

Chairperson	**Supervisor**
Dr. Shamim H. Ripon	Dr. Md. Nawab Yousuf Ali
Associate Professor and Chairperson	Associate Professor
Department of CSE	Department of CSE
East West University	East West University
Dhaka, Bangladesh	Dhaka, Bangladesh

ACKNOWLEDGEMENT

I am truly grateful to Almighty Allah, whose blessings have always been enormous and who gave me the ability and strength to complete this project. I would like to dedicate my project to my parents, who enlightened me the value of education and always keep me on the right track. It is a great honor and pleasure for me to record this deep sense of gratitude and insightful indebtedness to my respected supervisor, Dr. Md. Nawab Yousuf Ali for his valuable contribution, constant guidance, intuitive advice, helpful criticism, valuable suggestions, commendable support, and also endless patience for the completion of this project work. I am very much grateful to him and feel proud to have worked with him because it was not possible for me to complete this work without his inspiring enthusiasm and encouragement.

ABBREVIATIONS AND ACRONYMS

3G	**T**hird **G**eneration
3GPP	**3rd G**eneration **P**artnership **P**roject
4G	**F**ourth **G**eneration
IPv4	**I**nternet **P**rotocol **V**ersion 4
IPv6	**I**nternet **P**rotocol **V**ersion **6**
BYOD	**B**ring **Y**our **O**wn **D**evice
IIG	**I**nternational **I**nternet **G**ateway
BC	**B**roadcast **C**hannel
BER	**B**it **E**rror **R**ate
ISP	**I**nternet **S**ervice **P**rovider
IIG	**I**nternational **I**nternet **G**etaway
IGW	**I**nternational **G**etaway
CDI	**C**hannel **D**irection **I**ndicator
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
IPsec	**I**nternet **P**rotocol **S**ecurity
QoS	**Q**uality **of S**ervice
PAN	**P**ersonal **A**rea **N**etwork
LAN	**L**ocal **A**rea **N**etwork
MAN	**M**etropolitan **A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork
DPC	**D**irty **P**aper **C**oding
eNB	**E**volve **N**ode **B**
FDD	**F**requency **D**ivision **D**uplex
SAN	**S**torage **A**rea **N**etwork
EPN	**E**nterprise **P**rivate **N**etwork
VPN	**V**irtual **P**rivate **N**etwork
DARPA	**D**efense **A**dvance **R**esearch **P**rojects **A**gency
IEEE	**I**nstitute **of E**lectrical **and E**lectronics **E**ngineers
IID	**I**ndependent **I**dentical **D**istributed
IP	**I**nternet **P**rotocol
DCAP	**D**ata **L**ink **S**witching **C**lient **A**ccess **P**rotocol
RIP	**R**outing **I**nformation **P**rotocol
RSVP	**R**esource **R**eSer **V**ation **S**etup **P**rotocol

MAC	**M**ultiple **A**ccess **C**hannel
VRRP	**V**irtual **R**outer **R**edundancy **P**rotocol
Mbps	**M**ega **B**it **P**er **S**econd
MBWA	**M**obile **B**roadband **W**ireless **A**ccess
MCW	**M**ultiple **C**ode **W**ord
MHz	**M**ega **H**ertz
RUDP	**R**eliable UDP
XOT	**X.25 over TCP**
IPDC	**IP D**evice **C**ontrol
IRC	**I**nternet **R**elay **C**hat **P**rotocol
POP3	**P**ost **O**ffice **P**rotocol Version **3**
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
TELNET	**TCP/IP T**erminal **E**mulation **P**rotocol
BGP	**B**order **G**ateway **P**rotocol
EGP	**E**xterior **G**ateway **P**rotocol
P to P	**P**oint **to P**oint
EIGRP	**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol
IGRP	**I**nterior **G**ateway **R**outing
OSPF	**O**pen **S**hortest **P**ath **F**irst
PPTP	**P**oint **to P**oint **T**unneling **P**rotocol
ARP	**A**ddress **R**esolution **P**rotocol
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
NAT	**N**etwork **A**ddress **T**ranslation
NDP	**N**eighbor **D**iscovery **P**rotocol
MLD	**M**ulticast **L**istener **D**iscovery
MTU	**M**aximum **T**ransmission **U**nit
EUI	**E**xtended **U**niversal **I**dentifier
DUAL	**D**iffusing **U**pdate **A**lgorithm
PDMs	**p**rotocol-**D**ependent **M**odules
ACK	**A**cknowledgment
SISO	**S**ingle **I**nput **S**ingle **O**utput
SO	**S**uccessive **O**ptimization
DNS	**D**omain **N**ame **S**erver

TDD	**T**ime **D**ivision **D**uplex
Tx	**T**ransmitter
UE	**U**ser **E**quipment
UL	**U**p **L**ink
WAN	**W**ide **A**rea **N**etwork
Wi – Fi	**W**ireless **F**idelity
WiMAX	**W**orldwide **I**nteroperability **for** **M**icrowave **A**ccess
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WPMC	**W**ireless **P**ersonal **M**ultimedia **C**ommunications

TABLE OF CONTENTS

Page

Chapter 3: Efficient Approach of converting an IPv4 Network To IPv6

Chapter 4: Application on a Real Scenario

Chapter 5: Configuration and Test

Chapter 6: Conclusion and Future Works

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Overview

Internet Protocol version 4 (IPv4) was developed in 1981; it provides a 32 bit addressing space containing 4.3billion unique Internet Protocol (IP) addresses [1]. Each Internet enabled device requires a unique IP address from this address space; however the rapid growth of the Internet has resulted in these addresses being exhausted; with the last of the address space allocated in February 2012 [2].Internet Protocol version 6 (IPv6) is designed to address the problem of limited address space by providing 128bits of addressing space, providing 128 IP addresses; a practically limitless addressing space for new internet enabled devices to utilize [3].IPv6 brings a number of improvements over IPv4 in addition to increased addressing space; IPv4 contains no security mechanisms: IPv4 relies upon higher level protocols to handle authentication and encryption of packets; this can lead to vulnerabilities when deploying IPv4 systems. This issue is addressed in IPv6 which increased security through the use of integrated Internet Protocol Security (IPsec) within the IPv6 protocol which provides authentication and encryption using cryptographic keys [4].IPv4 includes no quality of service mechanisms: IPv6 adds support for Quality of Service (QoS) mechanisms through the use of flow control bits; these will enable routers to priorities' packets based upon QoS considerations and economies storage by aggregating routing tables [5]. IPv4 headers have limited extensibility due to only containing a single options field within the header: IPv6 uses a fixed length header of 40 octets, but utilizes a separate extension header after the main protocol header which will enable the protocol to be extended with future developments [6]. Differences between IP version 4 and 6 packet layout mean that routing IPv6 traffic is not supported by existing IPv4 routing protocols [7]. Given the importance placed upon reliability and scalability in many networks, development of IPv6 dynamic routing protocols are essential for their operation.

Dynamic routing protocols provide increased scalability over static alternatives and the ability to automatically adjust to network topological changes such as a failed components; rerouting traffic through alternative paths automatically with minimal disruption. This is very important because of the current trend of network growth rate hence the need for the use of an appropriate routing protocol that will adjust to scale with this increasing growth [8].

1.2 Basic Concept of Network

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections (network links). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet[1].

Network computer devices that originate, route and terminate the data are called network nodes[1]. Nodes can include hosts such as personal omputers , phones , servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the transmission media.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications [9].

1.2.1 Types of Networks

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe[3].

Some of the different networks based on size are:

1)Personal area network, or PAN

2)Local area network, or LAN

3) Metropolitan area network, or MAN

4)Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

5)Storage area network, or SAN

6)Enterprise private network, or EPN

7)Virtual private network, or VPN

8)Bring your own device or BYOD

1.2.2 BYOD

BYOD (bring your own device) is the increasing trend toward employee-owned devices within a business. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace.BYOD is part of the larger trend of IT consumerization, in which consumer software and hardware are being brought into the enterprise. BYOT (bring your own technology) refers to the use of consumer devices and applications in the workplace. More specific variations on the term include bring your own computer (BYOC), bring your own laptop (BYOL), bring your own apps (BYOA) and bring your own PC (BYOPC)[23].

Employee-owned devices are sometimes sanctioned by the company and supported alongside devices that are owned by the business. In other cases, employee-owned devices are part of the parallel system known as shadow IT: hardware or software within an enterprise that is not supported by the organization’s central IT department.Whether employee-owned hardware and software are supported or not, they pose security risks to the organization if they connect to the corporate network or access corporate data. To minimize the risk and accommodate consumer technologies, many businesses are implementing BYOD policies[10].

1.2.3 Network Topology

The logical topology which defines how the media is accessed by the hosts. Logical topology refers also to how computers are being connected with each other.

The types of topologies:

1. BUS topology – uses a single backbone segment (length of cable) that all the hosts connect to directly. It is just like riding a bus. Like bus has only one driver and many passengers who are riding.

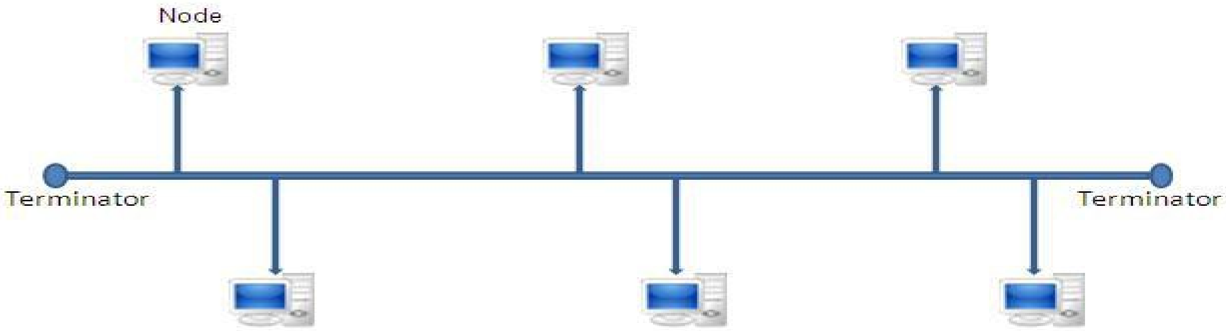


Fig 1.1 BUS TOPOLOGY

2. RING topology – connects one host to the next and the last host to the first. It creates a physical ring of cable.

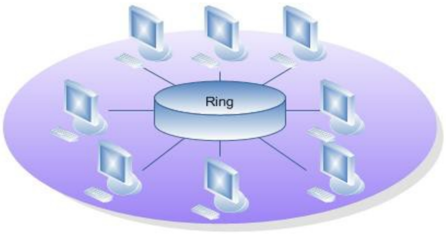


Fig 1.2 Ring Topology

3. STAR topology – connects all cables to a central point of concentration. The point is usually a hub or switch. Hub has a focal point where all the resources are there.

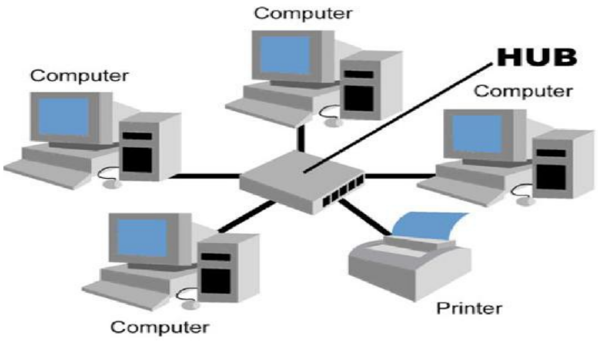


Fig 1.3 STAR TOPOLOGY

4. EXTENDED STAR topology – uses the star topology to be created. Star Topology links individual stars together by linking the hubs/ switches. It will extend the length of the network.

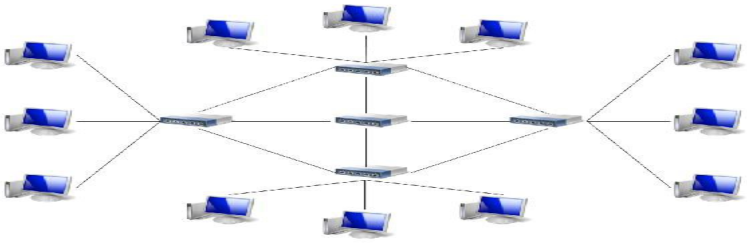


Fig 1.4 EXTENDED STAR TOPOLOGY

5. HIERARCHICAL topology - is created similar to an extended star but instead of linking the hubs/ switches together, system is linked to a computer which controls the traffic on the topology.

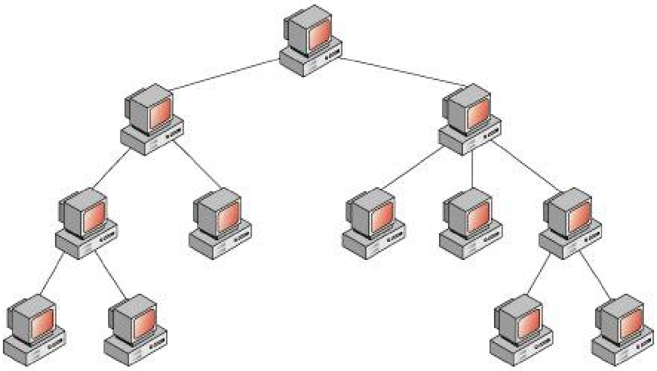


Fig 1.5 HIERARCHICAL TOPOLOGY

6. MESH topology – is used when there can be absolutely no break in communications. You can see in the graphic, every host has its connections to all other hosts. It also reflects the design of the internet which has multiple paths to any one location.

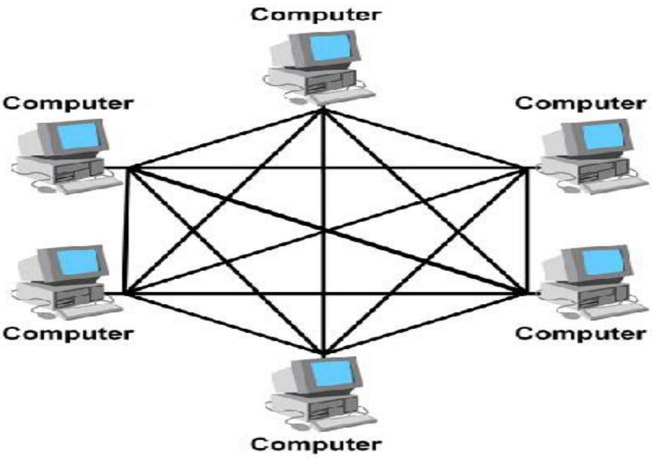


Fig 1.6 MESH TOPOLOGY

the logical topology which defines how the media is accessed by the hosts. Logical topology refers also to how computers are being connected with each other.

1.2.4 Network Protocols

The Defense Advance Research Projects Agency (DARPA) originally developed Transmission Control Protocol/Internet Protocol (TCP/IP) to interconnect various defense department computer networks. The Internet, an international Wide Area Network, uses TCP/IP to connect government and educational institutions across the world. TCP/IP is also in widespread use on commercial and private networks. The TCP/IP suite includes the following protocols [11].

Data Link Layer	
ARP/RARP	Address Resolution Protocol/Reverse Address
DCAP	Data Link Switching Client Access Protocol
Network Layer	
DHCP	Dynamic Host Configuration Protocol
DVMRP	Distance Vector Multicast Routing Protocol
ICMP/ICMPv6	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol version 4

IPv6	Internet Protocol version 6
MARS	Multicast Address Resolution Server
PIM	Protocol Independent Multicast-Sparse Mode (PIM-SM)
RIP2	Routing Information Protocol
RIPng for IPv6	Routing Information Protocol for IPv6
RSVP	Resource ReSerVation setup Protocol
VRRP	Virtual Router Redundancy Protocol
Transport Layer	
ISTP	
Mobile IP	Mobile IP Protocol
RUDP	Reliable UDP
TALI	Transport Adapter Layer Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
Van Jacobson	compressed TCP
XOT	X.25 over TCP
Session Layer	
BGMP	Border Gateway Multicast Protocol
Diameter	
DIS	Distributed Interactive Simulation
DNS	Domain Name Service
ISAKMP/IKE	Internet Security Association and Key Management Protocol and Internet Key Exchange Protocol
iSCSI	Small Computer Systems Interface

LDAP	Lightweight Directory Access Protocol
MZAP	Multicast-Scope Zone Announcement Protocol
NetBIOS/IP	NetBIOS/IP for TCP/IP Environment
Application Layer	
COPS	Common Open Policy Service
FANP	Flow Attribute Notification Protocol
Finger	User Information Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IMAP4	Internet Message Access Protocol rev 4
IMPPpre	Instant Messaging and Presence Protocols
IPDC	IP Device Control
IRC	Internet Relay Chat Protocol
ISAKMP	Internet Message Access Protocol version 4rev1
ISP	
NTP	Network Time Protocol
POP3	Post Office Protocol version 3
Radius	Remote Authentication Dial In User Service
RLOGIN	Remote Login
RTSP	Real-time Streaming Protocol
SCTP	Stream Control Transmision Protocol
S-HTTP	Secure Hypertext Transfer Protocol
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

SOCKS	Socket Secure (Server)
TACACS+	Terminal Access Controller Access Control System
TELNET	TCP/IP Terminal Emulation Protocol
TFTP	Trivial File Transfer Protocol
WCCP	Web Cache Coordination Protocol
X-Window	X Window
Routing	
BGP-4	Border Gateway Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
HSRP	Cisco Hot Standby Router Protocol
IGRP	Interior Gateway Routing
NARP	NBMA Address Resolution Protocol
NHRP	Next Hop Resolution Protocol
OSPF	Open Shortest Path First
TRIP	Telephony Routing over IP
Tunneling	
ATMP	Ascend Tunnel Management Protocol
L2F	The Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
PPTP	Point to Point Tunneling Protocol
Security	
AH	Authentication Header
ESP	Encapsulating Security Payload

TLS	Transport Layer Security Protocol

1.2.5 TCP/IP Protocol Architecture Model

The OSI model describes an idealized network communications protocol family. TCP/IP does not correspond to this model directly, as it either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Solaris implementation of TCP/IP, listed from topmost layer (application) to lowest (physical network).

Table I -TCP/IP Protocol Stack

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, Session, Presentation	Application	NFS, NIS+, DNS, `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data Link	Data Link	PPP, IEEE 802.2
1	Physical	Physical Network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

The table shows the TCP/IP protocol layers, their OSI Model equivalents, and examples of the protocols available at each level of the TCP/IP protocol stack. Each host involved in a communication transaction runs its own implementation of the protocol stack.

1.2.6 Network Devices

Computer networking devices are units that mediate data in a computer network and are also called network equipment. Units which are the last receiver or generate data are called hosts or data terminal equipment.

- **HUB**

Hubs connect computers together in a star topology network. Due to their design, they increase the chances for collisions. Hubs operate in the physical layer of the OSI model and have no intelligence. Hubs flood incoming packets to all ports all the time. For this reason, if a network is connected using hubs, the chances of a collision increases linearly with the number of computers (assuming equal bandwidth use). Hubs pose a security risk since all packets are flooded to all ports all the time. If a user has packet sniffing software, they can extract data from the network and potentially decode it and use it. Hubs make it easy to "spy" on users on the same LAN as you.

- **REPEATER**

A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation. Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the physical layer, the first layer of the OSI model. Repeaters are majorly employed in long distance transmission to reduce the effect of attenuation. It is important to note that repeaters do not amplify the original signal but simply regenerate it.

- **MODEM**

Modem (from modulator-demodulator) is a device that turns the digital 1s and 0s of a personal computer into sounds that can be transmitted over the telephone lines of Plain Old Telephone Systems (POTS), and once received on the other side, converts those sounds back into a form used by a USB, Ethernet, serial, or network connection. Modems are generally classified by the amount of data they can send in a given time, normally measured in bits per second, or "bps".

- **NIK**

A network interface card is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly. Most motherboards today come equipped with a network interface card in the form of a controller, with the hardware built into the board itself, eliminating the need for a standalone card[23].

- MEDIA CONVERTERS

Media converters are simple networking devices that make it possible to connect two dissimilar media types such as twisted pair with fiber optic cabling. They were introduced to the industry nearly two decades ago, and are important in interconnecting fiber optic cabling-based systems with existing copper-based, structured cabling systems. Media converters support many different data communication protocols including Ethernet, T1/E1, T3/E3, as well as multiple cabling types such as coaxial, twisted pair, multimode and single-modefiber optics. When expanding the reach of a Local Area Network to span multiple locations, media converters are useful in connecting multiple LANs to form one large "campus area network" that spans over a limited geographic area. As local networks are primarily copper-based, media converters can extend the reach of the LAN over single-mode fiber up to 130 kilometers with 1550 nm optics.

- SWITCH

Switches are often confused with bridges because they also operate at the data link layer of the OSI model. Similar to a hub, switches provide a central connection between two or more computers on a network, but with some intelligence. They provide traffic control for packets; rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected. They use a database of MAC addresses to determine where computers are located and very efficiently send packets only where they need to go. The database is created dynamically as computers communicate on the network. The switch simply watches the incoming packets and memorizes the MAC address and port a packet arrives on. If a packet arrives with a destination computer that the switch does not have an address for in its MAC address table, it will flood the packet out all connected ports. A switch creates separate collision domains for each physical connection. A switch will only create separate broadcast domains if separate VLANs(Virtual Local Area Networks) are assigned to different ports on the switch. Otherwise, a broadcast received on one port will be flooded out all ports except the one it came in on[23].

- WIRELESS ACCESS POINT

A wireless access point (WAP or AP) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

- ROUTER

Routers operate at the network layer of the OSI model and efficiently route information between Local Area Networks. Since routers operate in the third layer, the network layer, they must understand layer 3 addressing… such as TCP/IP. A router will divide a broadcast domain by not forwarding broadcasts on one connected network to another connected network. Routers operate in two different planes: the control plane, in which the router learns the outgoing interface that is most appropriate for forwarding specific packets to specific destinations, and the forwarding plane, which is responsible for the actual process of sending a packet received on a logical interface to an outbound logical interface.

- FIREWALL

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the Local Area Network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Without proper configuration, a firewall can often become worthless. Standard security practices dictate a "default-deny" firewall ruleset, in which the only network connections which are allowed are the ones that have been explicitly allowed[7].

1.3 Internet Protocol

Internet Protocol is part of the Internet suite of communications protocols that provides globally unique addresses in dotted quad notation, transmits data in packets and performs routing between IP based networks.This entire tutorial pertains to what is referred to as Internet Protocol version 4 (IPv4). There is also exists the next generation of Internet Protocol version 6 (IPv6 or IPng) that was created to fix some of the problems that weren't foreseen when IPv4 was created. Most Internet Service

Providers are capable of handling IPv6, but the vast majority of Internet users are still using IPv4.

1.3.1 Internet Protocol Version 4

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol (IP) used to facilitate communication over a network through an addressing system. It is currently the most popular Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 232 addresses (slightly over 4 billion addresses). Each device connecting to the Internet requires an IP address. That means that each device including cell phones, office phones, game consoles and computers each need their own IP address in order to connect and communicate over the Internet. With the ever-growing number of devices that need to connect to the Internet, it is no surprise that the amount of available IPv4 addresses will soon be exhausted. Already, there are more devices connected than there are routable IPv4 addresses. This is possible through a technology known as NAT (Network Address Translation) which allows multiple machines to appear as a single routable address. This comes with the cost of the complexity involved in supporting devices beployed behind a NAT device.

1.3.2 IPv4 Address Format

An IP address is a number used to identify the logical connection of a computer to a physical network is a 32-bit binary address, composed of four, 8-bit numbers. IP address are represented as four decimalnumbers between 0 and 255 separated by dots; (eg. 199.221.66.10). This is referred to as dotted-decimal notation. Anything attached to an IP network can be assigned an IP address. Note that this means that it is possible for a single host to have multiple IP addresses if it is running multiple network interfaces to support services such as DNS, Web or Mail server software. Addresses are always unique. Because IP addresses are software configured, it is easy to move hosts from one network to another simply by changing the IP address or the network mask. This process is called renumbering[Intendamono].

- **Network and Host Portion of an IP Address**

When looking at an IP address, the left-most portion of the address identifies which network the mahcine (host) belongs to. The right-most portion is used as the address of the host itself. A large number of addresses in use (but not all of them) look something like this:

VALUE	NETWORK			HOST
IN DECIMAL	199	232	66	10
IN BINARY	11000111	11101000	01000010	00001010

In the example above, the network address is 199.232.66 and the host portion of the address is 20, the complete IP address is 199.221.66.10. All the computers on the same local network would have the same network number in their address. Thus, two computers on the same network might be 199.221.66.10 and 199.221.66.44.When two hosts with IP addresses communicate, they send IP datagrams. IP datagrams contain the source and destination addresses of the hosts communicating. Only the addresses are recorded in the packet. There is no information stored in the packet to tell us which part of the address is network and which is host. If this is true, then how would we figure out which part of the address is the network portion, and which is the host portion First, you must remember that all hosts on the same network will have the same network address (the network portion of the IP address will be the same for all hosts). Only the host portion will be different and unique for each host on the network.

Different networks also have different network addresses. Network A would have a different address fromNetwork B. From the perspective of determining the correct network, the individual host address is irrelevant. We will need it later to find the host itself ON the network, but we don't need to look at it yet, since we need to find the correct network first. To find a particular host, you first find the network that host is on, then ask that network to find the host host . There are two solutions to handling this network vs. host address problem, and they are similar but separate addressing types: classful, and classless. Classful Addressing was the first addressing scheme developed. It helped manage the IP space and make organization of networks and hosts possible, but it could not support the growing complexity of theInternet, and wasted a lot of address space, so an new scheme was developed called Classless Addressing. Classless Addressing was more efficient by allowing the assignment of smaller blocks of addresses [24].

- **The Subnet Mask**

The Subnet Mask is a value that is stored in the configuration of a computer along with the IP address. The Subnet Mask gives the computer a simple way to figure out whether the IP address of anothercomputer is on the same local network, or on a different local network. Bear in mind that for this definition of a mask, a 'local network' is defined as a group of computers with IP addresses in a limited range [24].

Chapter 2

Implemented Network Technology

2.1 IPv6 Address

Internet Protocol Version 6 (IPv6) is the latest version of Internet Protocol. It has been under development since the early 1990s. Other benefits of IPv6 include:

- No need for NAT (Network Address Translation) because there are enough IPv6 addresses for each device to have it's own address
- Configuration can be automatic
- Eliminates the challenge of private address collisions
- Improved multicast routing
- A simplified packet header, which allows for more efficient forwarding
- Built-in authentication and privacy support through IPSec in the protocol.
- Flexible options and extensions to the header format[23].

IPv6 has 128-bit addresses compared to our 32-bit IPv4 addresses. IPv6 Address every additional bit doubles the number of IP addresses…so we go from 4 billion to 8 billion, 16,32, 64, etc. Keep doubling until you reach 128-bit. Just for fun I looked up how many IPv6 addresses this will give us:

340,282,366,920,938,463,463,374,607,431,768,211,456

Can we even pronounce this? Let's try this:

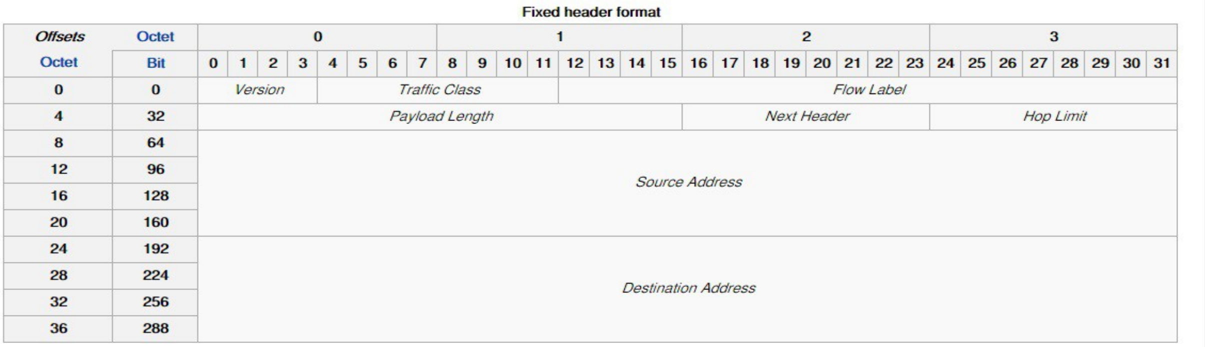
- 340- undecillion
- 282- decillion
- 366- nonillion
- 920- octillion
- 938- septillion
- 463- sextillion

- 463- quintillion
- 374- quadrillion
- 607- trillion
- 431- billion
- 768- million
- 211- thousand
- 456

2.1.1 IPv6 Header

The fixed header of an IPv6 packet consists of its first 40 octets (320 bits).[1] It has the following format:

Fixed header format



Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Version (4 bits)

The constant 6 (bit sequence 0110).

Traffic Class (8 bits)

The bits of this field hold two values. The 6 most-significant bits are used for differentiated services, which is used to classify packets.[2][3] The remaining two bits are used forECN;[4] priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.

Originally created for giving real-time applications special service.[1] The flow label when set to a non-zero value now serves as a hint to routers and switches with multiple outbound paths that these packets should stay on the same path so that they will not be reordered.[5][6] It has further been suggested that the flow label be used to help detect spoofed packets[7].

Payload Length (16 bits)

The size of the payload in octets, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo Payload option.[8]

Next Header (8 bits)

Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload. When extension headers are present in the packet this field indicates which extension header follows. The values are shared with those used for the IPv4 protocol field, as both fields have the same function (see List of IP protocol numbers).

2.1.2 IPv6 Address Look like

- X:X:X:X:X:X:X:X where X is a 16-bit hexadecimal field.
- Case-insensitive

No more decimal numbers like IPv4, we are using hexadecimal now.

- 2041:0000:140F:0000:0000:0000:875B:131B
- Original: 2041:0000:140F:0000:0000:0000:875B:131B
- Short: 2041:0000:140F::875B:131B
- Short: 2041:0000:140F::875B:131B
- Shorter: 2041:0:140F::875B:131B

There is one more thing we can do; We can make it even shorter! If We have a field with 4 zeroes you can remove them and leave only a single zero there.
Let summarize the rules:

- A string of zeroes can be removed leaving only a colon. (:)
- 4 zeroes can be removed leaving only a single zero.

We can’t remove all zeroes otherwise your IPv6 device has no idea where to fill in the zeroes to make it 128-bit again.

2.1.3 Types of IPv6

- **Unique local**
- **Link-local**
- **Global unicast**

- **Unique local**

Unique local is the equivalent of IPv4 private addresses. These are the addresses you should use for your own networks and not on the Internet. You can recognize them because the FD00::/8 address space is reserved for this. The IPv6 address space is so large however that organization will probably just use IPv6 global addresses for their internal networks[23].

- **Link-Local**

Link-local addresses are something new. Each IPv6 device will have a link-local address on the interface and it has a link-local scope. Packets send between link-local addresses will remain on the link and are not forwarded by routers to other subnets. What are they used for

- Used as the source address for RS (router solicitation) and RA (router advertisement). More on this later!

- Used for neighbor discovery (equivalent of ARP for IPv6).

- Used as the next-hop IPv6 address for IP routes.

Link-local IPv6 addresses are generated automatically by your IPv6 device for each interface. You can recognize them since they use the FE80::/10 range[23].

- **Global Unicast**

The global unicast addresses are used on the Internet and since the address space is so large this is probably what we will use for everything…even our internal networks. Instead of using NAT/PAT you'll have your own IPv6 address space to use. The address space we are using for global unicast is 2000::/3.The address space that was reserved for this is FEC0::/10.

There are two more IPv6 addresses that you might encounter:

• Unspecified • Loopback

The unspecified address will show up as ::/128 and is used when your host has no usable IPv6 address. The loopback is the same as IPv4's 127.0.0.1 but for IPv6 we use ::1/128.

2.1.4 Differences Between IPv4 and IPv6

IPv4	IPv6
IPv4 addresses are 32 bit length.	**IPv6 addresses** are 128 bit length.
IPv4 addresses are **binary numbers** represented in decimals.	**IPv6 addresses** are **binary numbers** represented in **hexadecimals**.
IPSec support is only optional.	Inbuilt **IPSec** support.
Fragmentation is done by sender and forwarding routers.	**Fragmentation** is done only by sender.
No packet flow identification.	Packet flow identification is available within the **IPv6 header** using the **Flow Label** field.
Checksum field is available in **IPv4 header**	No checksum field in **IPv6 header**.
Options fields are available in **IPv4 header**.	No option fields, but **IPv6 Extension headers** are available.
Address Resolution Protocol (ARP) is available to mapIPv4 addresses to MAC addresses.	**Address Resolution Protocol (ARP)** is replaced with a function of**Neighbor Discovery Protocol (NDP)**.
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	**Broadcast messages** are not available. Instead a link-local scope "All nodes" **multicast IPv6 address** (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of **IPv4 addresses** or DHCP (Dynamic configuration) is required to configure **IPv4 addresses**.	Auto-configuration of addresses is available.

2.1.5 Benefits of IPv6

With IPv6, everything from appliances to automobiles can be interconnected. But an increased number of IT addresses aren't the only advantage of IPv6 over IPv4. In honor of World IPv6 Day, here are six more good reasons to make sure your hardware, software, and services support IPv6.

More Efficient Routing IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of their customers' networks into a single prefix and announce this one prefix to the IPv6 Internet. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU)[23].

More Efficient Packet Processing IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection.

Directed Data Flows IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth. Disinterested hosts no longer must process broadcast packets. In addition, the IPv6 header has a new field, named Flow Label, that can identify packets belonging to the same flow.

Simplified Network Configuration Address auto-configuration (address assignment) is built in to IPv6. A router will send the prefix of the local link in its router advertisements. A host can generate its own IP address by appending its link-layer (MAC) address, converted into Extended Universal Identifier (EUI) 64-bit format, to the 64 bits of the local link prefix.

Support For New Services By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and services such as VoIP and Quality of Service (QoS) become more robust.

Security IPSec, which provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPSec can be applied to the ICMPv6 packets[23].

2.1.6 The Internet Authoritative Bodies

They belong to the group within the Internet community that is responsible for assigning unique classful networks. Everything started with the government-funded IANA, which is being commercially administered by Networks Solutions of Herndon, Virginia recently. On 25/11/1998, the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation managed by the US government, was officially recognized to perform administrative functions for the Internet, eg:

coordinating the assignment of protocol parameters, managing the domain name and root server systems, and allocating IP addresses. The growth of the Internet has led to regional organizations for the allocation of IP addresses. Regional Internet Registries (RIRs):

i) American Registry for Internet Numbers (ARIN, http://www.arin.net) serves North America, and parts of Caribbean.

ii) Réseaux IP Européens (RIPE, http://www.ripe.net) serves Europe, Middle East,and Central Asia.

iii) Latin American and Caribbean Internet Addresses Registry (LACNIC,

http://www.lacnic.net) serves Central and South America, and Caribbean.

iv) African Region Internet Registry (AfriNIC, http://www.afrinic.net) serves Africa.

v) Asia Pacific Network Information Center (APNIC, http://www.apnic.net) serves Asia, and Pacific Ocean regions.

Domain registration:

i) The Internet's Network Information Center (InterNIC, http://www.internic.net/)

2.2 EIGRP

EIGRP is a Cisco-proprietary hybrid routing protocol that contains features of distance vector and link-state routing protocols. Some of its features are:

i) Rapid convergence. EIGRP uses the Diffusing Update Algorithm (DUAL) to achieve rapid convergence. DUAL not only calculates the best loop-free routes, but also calculates backup routes in advanced before they are actually being needed.An EIGRP router stores all available backup routes for fast react upon network topology changes. If no backup route exists in the routing table, an EIGRP router will query its neighbors until an alternative route is found.

ii) Reduced bandwidth usage. EIGRP does not send periodic updates as with DV protocols.It sends partial updates upon the route information changes (eg: path, metric).Additionally, the update is propagated only to routers that require it, instead of all routers within an area as with LS routing protocols.

iii) Multiple routed protocols support. EIGRP has been extended from IGRP to be network-layer independent. It supports IP, IPX, and AppleTalk with protocol-dependent modules (PDMs), which are responsible for protocol requirements specific to the corresponding routed protocols. EIGRP offers superior performance and stability when implemented in IPX and AppleTalk networks. EIGRP maintains a neighbor table, a topology table, and a routing table for each running routed protocols (PDMs).

iv) Support all LAN and WAN data link protocols and topologies. EIGRP does not require special configuration across any L2 protocols. OSPF requires different configurations for different L2 protocols, eg: Ethernet and Frame Relay. EIGRP was designed to operate effectively in both LAN and WAN environments. EIGRP supports all multi-access networks, eg: Ethernet, Token Ring, FDDI, and all WAN topologies – leased lines, point-to-point links, and non-broadcast multiaccess (NBMA) topologies, eg: X.25, SMDS, ATM, and Frame Relay.

EIGRP has its roots as a distance-vector routing protocol (EIGRP is based on IGRP).It is considered an advanced DV routing protocol with traditional DV features,eg: auto summarization, easy configuration; and LS features, eg: dynamic neighbor discovery . Another distance-vector rule is that if a neighbor is advertising a destination, it must also be using that route to forward packets to the particular destination.

EIGRP (Enhanced IGRP) provides many enhancement features over IGRP, a traditional DV routing protocol, mainly in convergence properties and operating efficiency. Traditional DV routing protocols send periodic full routing updates, which consume unnecessary bandwidth.

EIGRP utilizes multicasts and unicasts only; broadcasts are not being used. As a result, end systems will not affected by the routing updates and queries.

EIGRP is a transport layer protocol that relies on IP packets to deliver its routing information. EIGRP packets are encapsulated in IP packets with the Protocol Number field value 88 (0x58) in the IP header. Some EIGRP packets are sent as multicasts (destination IP address 224.0.0.10),while others are sent as unicasts.A significant advantage of EIGRP (and IGRP) over other routing protocols is the support for **unequal-cost load balancing**.

EIGRP performs auto summarization by default, but this behavior can be disabled with the no auto-summary router subcommand.

Neighbor table lists the directly connected adjacent EIGRP routers to ensure bidirectional communication with the neighbors. It is similar to the neighborship database in LS routing protocols. It maintains information such as address, hold time, and interface which an adjacent router connected to. An EIGRP router keeps a neighbor table for each running routed protocol. EIGRP routers must form neighbor relationships before exchanging EIGRP updates.

Topology table maintains all advertised routes to all destinations, along with the advertising neighbors and advertised metric for each destination. The term "topology table" is confusingly named, as it does not actually store the complete network topology, but rather the routing tables from the directly connected neighbors. All successors and feasible successors to all destinations will be maintained in this table.

The best routes to a destination will be selected from the EIGRP topology table and placed into the routing table. An EIGRP router maintains 1 routing table for each running routed protocol. It contains all best routes selected from the EIGRP topology table and other routing processes. Successors and feasible successors (when unequal-cost load balancing is enabled with the variance router subcommand) will be selected from the topology table and stored in this table.

The show ip eigrp neighbors, show ip eigrp topology, and show ip route EXEC commands display the EIGRP neighbor table, EIGRP topology table, and routing table.

Successor is the lowest-metric best path to reach a destination. EIGRP successor routes will be placed into the routing table.

Feasible Successor (FS) is the best alternative loop-free backup path to reach a destination. Because it is not the least-cost or lowest-metric path, therefore it is not being selected as the primary path to forward packets and not being inserted into the routing table. Feasible successors are important as they allow an EIGRP router to recover immediately upon network failures and hence reduce the number of DUAL computations and therefore increase performance. The convergence time upon a successor failure with a feasible successor exists is in the range of 2 to 4 seconds (1 ping drop). Feasible successor routes are maintained in the topology table only.

2.2.1 EIGRP Packet Format

EIGRP sends out the following 5 types of packets:

Hello Used to discovery neighbor before establishing adjacency. EIGRP Hellos are sent as multicasts and contain an acknowledgment number of 0. EIGRP routers must form neighbor relationships before exchanging EIGRP updates.

Update Used to communicate the routes that a particular router has used to converge. EIGRP Updates are sent as multicasts when a new route is discovered or when convergence is completed ; and are sent as unicasts when synchronizing topology tables with neighbors upon the EIGRP startup. They are sent reliably between EIGRP routers.

Query Used to query other EIGRP neighbors for a feasible successor when DUAL is Re -computing a route in which the router does not have a feasible successor.EIGRP Queries are sent reliably as multicasts.

Reply Sent as the response to an EIGRP Query packet. EIGRP Replies are sent reliably as unicasts.

Acknowledge Used to acknowledge EIGRP Updates, Queries, and Replies; Hello and ACK packets do not require acknowledgment. ACKs are Hello packets that contain no data and a non-zero acknowledgment number and are sent as unicasts. An EIGRP router sends Hello packets out all EIGRP-enabled interfaces. The EIGRP multicast address is 224.0.0.10. An EIGRP router only establishes neighbor relationships (adjacencies) with other routers within the same autonomous system.EIGRP Hello packets are sent every 5 seconds on LANs (eg: Ethernet, Token Ring, and FDDI) and point-to-point links (eg: PPP, HDLC, Frame Relay and ATM point-to-point sub interfaces, and multipoint circuits with bandwidth greater than T1 (eg: ISDN PRI, ATM, and Frame Relay),and 60 seconds on T1 or low-speed interfaces (eg: ISDN BRI, X.25, ATM, and Frame Relay). The ip hello-interval eigrp {as-num} {sec} interface subcommand configures the Hello interval for an EIGRP routing process running upon an interface. The EIGRP neighbor table also maintains the hold time – the amount of time a router considers a neighbor is up without receiving a Hello or any EIGRP packet from the particular neighbor. The ip hold-time eigrp {as-num} {sec} interface subcommand configures the hold time interval for an EIGRP routing process. The hold time interval is recommended to be at least 3 times the Hello interval. In fact, the hold time interval is 3 times the Hello interval by default. The hold time interval is not automatically adjusted upon the change of the Hello interval. Once the Hello interval is changed, the hold time interval must be manually configured according to the new Hello interval[6].

2.2.2 EIGRP Metric Computation

EIGRP supports the following types of routes: Internal Routes that are originated within an EIGRP autonomous system. External Routes that are learnt from another routing protocol or another EIGRP AS. Summary Routes that encompass multiple subnets. EIGRP summary routes have an administrative distance value of 5 (better than any dynamically learned route)[23].

AD values are locally significant and hence are not propagated to other routers. EIGRP uses Diffusing Update Algorithm (DUAL) to calculate and select loop-free primary and backup routes to a destination. When the primary routes fails, EIGRP can immediately uses a backup route without the need for hold down, and hence results in fast convergence. The EIGRP composite metric calculation can use up to 5 variables, but only the following 2 are used by default (K1 and K3):

K1 – Bandwidth The minimum or lowest bandwidth between the source and destination.

K3 – Delay the cumulative interface delay values along the path. The following variables are not commonly used, as they often cause frequent recalculation ofthe topology table.

K2 – Load

Utilization

The worst load on a link between the source and destination based on the packet rate and the configured interface bandwidth.

K4 – **Reliability** The worst reliability between the source and destination.

K5 – **Maximum**

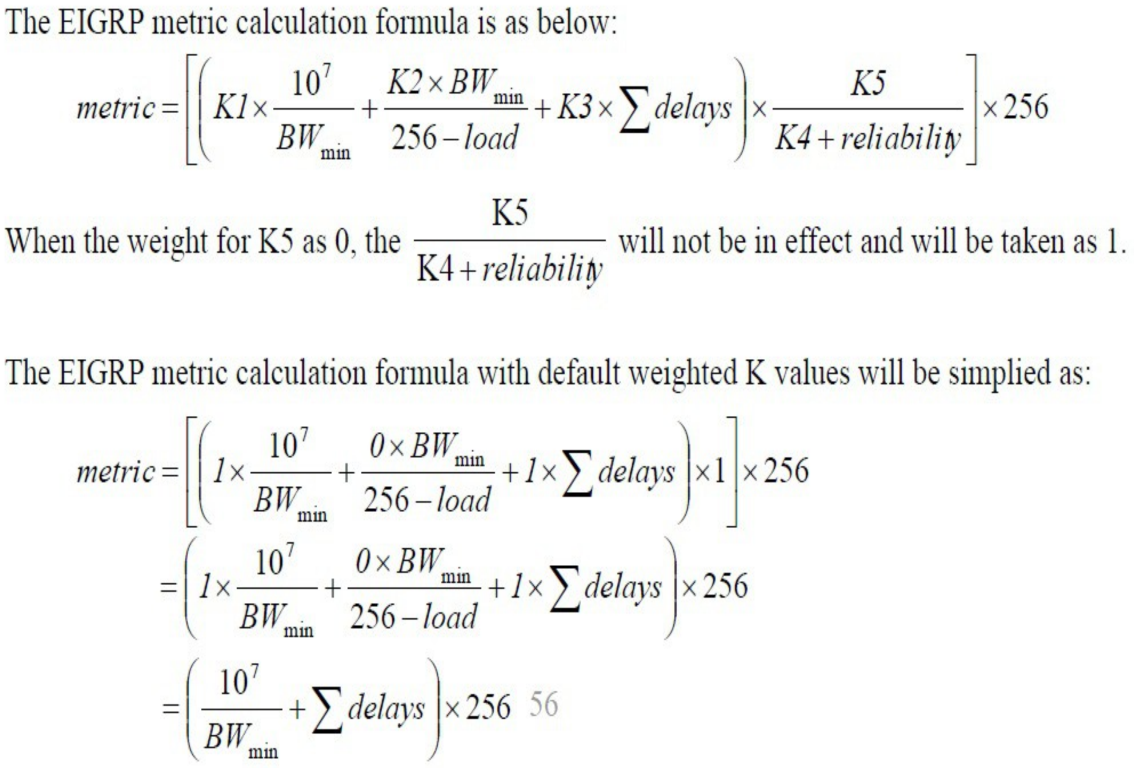
Transmission Unit

The smallest MTU along a path. MTU is included in the EIGRP Update packets but was never included in the formula used for metric calculation. EIGRP calculates the metric to a network by adding weighted values for variables of the links. Below shows the weights attributed to the K variables:

i) K1 = Bandwidth (1)
ii) K2 = Load Utilization (0)
iii) K3 = Delay (1)
iv) K4 = Reliability (0)
v) K5 = MTU (0)

The EIGRP metric calculation formula is as below:

When the weight for K5 as 0, the will not be in effect and will be taken as 1.The EIGRP metric calculation formula with default weighted K values will be simplied as:



The EIGRP metric calculation formula is as below:

$$metric = \left[\left(K1 \times \frac{10^7}{BW_{\min}} + \frac{K2 \times BW_{\min}}{256 - load} + K3 \times \sum delays \right) \times \frac{K5}{K4 + reliability} \right] \times 256$$

When the weight for K5 as 0, the $\frac{\mathrm{K5}}{\mathrm{K4} + reliability}$ will not be in effect and will be taken as 1.

The EIGRP metric calculation formula with default weighted K values will be simplied as:

$$metric = \left[\left(1 \times \frac{10^7}{BW_{\min}} + \frac{0 \times BW_{\min}}{256 - load} + 1 \times \sum delays \right) \times 1 \right] \times 256$$

$$= \left(1 \times \frac{10^7}{BW_{\min}} + \frac{0 \times BW_{\min}}{256 - load} + 1 \times \sum delays \right) \times 256$$

$$= \left(\frac{10^7}{BW_{\min}} + \sum delays \right) \times 256$$

56

2.2.3 EIGRP DUAL – Diffusing Update Algorithm

EIGRP uses the DUAL finite-state machine to tracks all routes advertised by all neighbors with the topology table, performs route computation on all routes to select an efficient and loop-free path to all destinations, and inserts the lowest metric route into the routing table. EIGRP uses the advertised distance and feasible distance to determine the successor (best route) and feasible successor (backup route) to a destination network.

Advertised Distance The EIGRP metric for a next-hop EIGRP neighboring router to reach a destination network. Also known as Reported Distance.

Feasible Distance The EIGRP metric for the local router to reach a destination network. Theoretically it is the sum of the advertise distance of an EIGRP neighbor and the metric to reach the neighbor, but actually the local router would recalculate the EIGRP metric to the destination network. The xxx and yyy in the via A.B.C.D (xxx/yyy), interface entry in the show ip eigrp topology EXEC command represent feasible distance and advertised distance respectively.

2.2.4 EIGRP Reliability

EIGRP reliability mechanism ensures the delivery of important routing information – Update, Query, and Reply packets, to neighboring routers in order to maintain a loop-free topology.

A sequence number is assigned to every packet and requires an explicit acknowledgment for the sequence number. Acknowledgments are not necessary sent via ACK packets, as the ACK field in any RTP unicast packet is sufficient to acknowledge the received EIGRP packets. For efficiency purpose, only certain EIGRP packets are being transmitted reliably.

Reliable Transport Protocol (RTP) is responsible for guaranteed and ordered delivery of EIGRP packets with the use of sequence and acknowledge numbers, but without any fancy windowing or congestion control mechanism (because only one packet will be sent at a time).

It supports transmission of both multicast and unicast packets. Sending Hello packets to all neighbors individually is inefficient on a multi-access networks that provide multicast capabilities (eg: Ethernet), therefore Hello packets do not require acknowledgement are sent as unreliable multicasts. All packets that carry routing information

Update, Query, and Reply packets are sent reliably and require explicit acknowledgment. Note: Hello and ACK packets which are not being transmitted reliably have no sequence number. RTP ensures ongoing communication is maintained between neighboring routers by maintaining/a retransmission list for each neighbor. The list is used to track all the reliable packets that were sent but not acknowledged within the Retransmission Time Out (RTO). If the RTO timer expires before an ACK packet is received, EIGRP will transmit another copy of the reliable packet until the hold timer expires and terminate the neighbor relationship.

The use of reliable multicast packets is efficient. However, delays are potential to exist on multi-access media with multiple neighbors, as a reliable multicast packet cannot be transmitted until all peers have acknowledged the previous multicast packet. If a router is slow to respond, it would delay the transmission of next packet and affects all other routers. RTP is designed to handle such situation – neighbors that respond slow to multicasts would have the unacknowledged multicast packets retransmitted as unicasts when the RTO timer expires. This allows the reliable multicast operation to proceed without delaying communications with others and ensure low convergence time in the environments with variable-speed links.

The multicast flow timer determines how long to wait for an ACK packet before switching from multicast to unicast; while the RTO determines how long to wait between subsequent unicasts. The EIGRP process for each neighbor calculates both the multicast flow timer and RTO timer based on the Smooth Round-Trip Time (SRTT). The formulas for the SRTT, RTO,and multicast flow timer are Cisco-proprietary.

RTO is a dynamically adjusted over time. It is based on the SRTT, which specifies the average time in milliseconds between the transmission of a packet and the receipt of an acknowledgment. As more unacknowledged updates are sent, the SRTT would get higher and higher, which causes the RTO to increase exponentially. The maximum RTO value is 5000 ms (5 seconds).

In a steady-state network where no routes are flapping, EIGRP waits for the specified hold-time interval to expire before determining that an EIGRP neighbor adjacency is down. By default, EIGRP waits up to 15 seconds for high-speed links and up to 180 seconds for low-speed links. When EIGRP determines that a neighbor is down and the router cannot reestablish the adjacency, the router will remove all reachable networks through that neighbor from the routing table. The router will attempt to find alternative paths to those networks when the convergence.

The 180-second hold time interval for low-speed links seems excessive, but it accommodates the links which are generally connected to less-critical remote sites. Additionally, 15 seconds is considered too long for some networks with high-speed links and serving mission-critical and time-sensitive applications. Always remember that there are situations and reasons in which modifying the default hold time interval is necessary in order to achieve faster convergence.

When a local router sends an update packet to a remote router and the remote router does not acknowledge the packet, the router would retransmit the update every time the RTO expires for up to 16 times, or until the hold timer expires, whichever is longer, and eventually terminate the neighbor relationship; not as claimed by some sources that the neighbor relationship will be terminated after 16 retransmissions rather than wait until the hold timer expires! EIGRP packets are only being generated at the moment of transmission. The transmit queues contain small and fixed-size structures that indicate which parts of the topology table to include in an EIGRP packet. As a result, the queues do not consume large amounts of memory and only the latest information will be transmitted. Ex: If a route changes state several times, only the last state is transmitted in the packet. This approach reduces bandwidth utilization.

2.2.5 Network Routing protocol

In computer networks, the routing protocol specifies how routers communicate to select the routes for in formation or data transfer for that, the routing algorithm is more important [7]. First, the routing protocol informs or shares the information with their associative neighbors and then throughout the network, in which topology is determined [5] – [10]. Different types of routing protocols are as follows,

OSPF & IS-IS-> Interior gateway routing using link state routing protocol RIP & EIGRP -> Interior gateway routing using Distance vector routing protocol BGP -> Exterior gateway routing using path vector routing protoco

- **Routing Information Protocol (RIP)**

RIP stands for Routing Information Protocol in which distance vector routing protocol is used for data/packet transmission. In Routing Information protocol (RIP), the maximum number of Hop is 15, because it prevents routing loops from source to destination. Mechanism like split horizon, route poisoning and hold own are used to prevent from incorrect or wrong routing information. Sally Floyd and Van Jacobson [1994] suggest that, without slight randomization of the timer, the timers are synchronized overtime [8]. Compared to other routing protocol, RIP (Routing Information Protocol) is poor and limit size i.e. small network. The main advantage of using RIP is it uses the UDP (User Datagram Protocol) and reserved port is 520 [12] .

- **Enhanced Interior Gateway Protocol (EIGRP)**

EIGRP stands for Enhanced Interior Gateway Protocol which allows router to share information to the neighboring routers which are within the same area. Instead of sending the entire information to the neighboring router, the information which is needed are shared which reduces the workload and amount of data needs to be transmitted. EIGRP (Enhanced Interior Gateway Protocol) designed by CISCO system which can be used onlyin CISCO routers, but in 2013 it became open source, so it can be used in other routers [5] – [7]. Neighbor table and Topology table are maintained by the EIGRP (Enhanced Interior Gateway Protocol) [12].

- **Open Shortest Path First (OSPF)**

OSPF stands for Open Shortest Path First which uses link-state routing algorithm. Using the link stateinformation which is available in routers, it constructs the topology in which the topology determines the routingtable for routing decisions [7]. It supports both variable-length subnet masking and classless inter-domainrouting addressing models.Since it uses Dijkstra's algorithm , it computes the shortest path tree for each route.The main advantages of the OSPF (Open Shortest Path first) is that it handles the error detection by itself and ituses multicast addressing for routing in a broadcast domain [10].

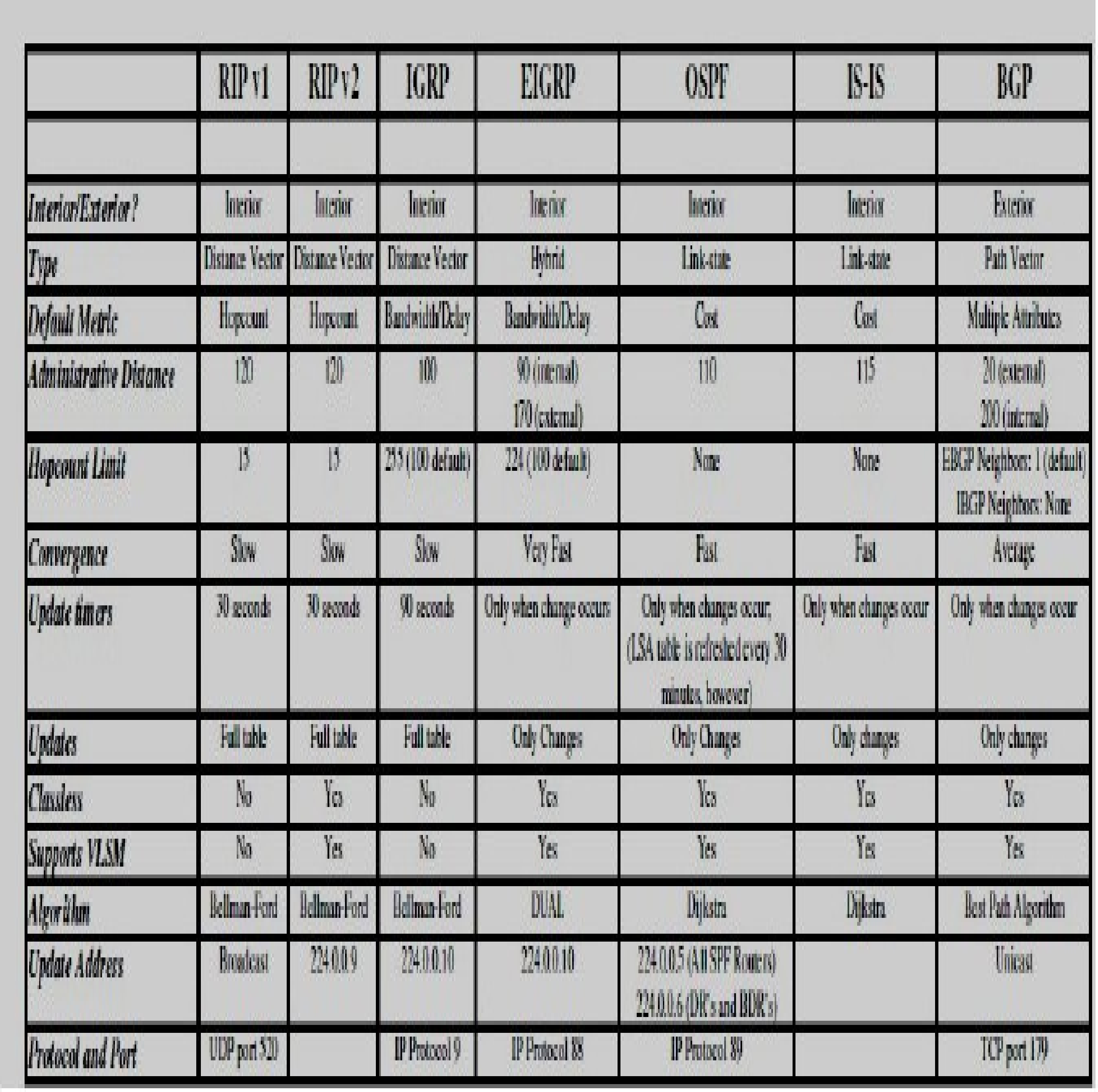
- **Intermediate-System to Intermediate - System (IS- IS)**

IS-IS stands for Intermediate-system to Intermediate - system which uses link-state routing algorithmfor high speed data transmission. IS-IS (Intermediate-system to Intermediate system) uses Dijkstra's algorithm in which independent database built by each IS-IS router for computing the best path for transmission in anetwork. It is standardized by ISO, but later IETF (Internet Engineering Task Force) standardized as the InternetStandard in RFC 1142 [5], [6], [15].

- **Interior Gateway Routing Protocol (IGRP)**

IGRP stands for Interior Gateway Routing protocol which uses distance vector protocol (interior) toexchange data within a system [9]. It supports multiple metrics for each node which includes delay, load and bandwidth, in order to compare the 2 routes which are combined into single metrics. The port number for IGRPis 9 which are used for communication and by default every 90 seconds it updates the routing information [18].

2.2.6 Comparison of Routing Protocols



	RIP v1	RIP v2	IGRP	EIGRP	OSPF	IS-IS	BGP
Interior/Exterior?	Interior	Interior	Interior	Interior	Interior	Interior	Exterior
Type	Distance Vector	Distance Vector	Distance Vector	Hybrid	Link-state	Link-state	Path Vector
Default Metric	Hopcount	Hopcount	Bandwidth/Delay	Bandwidth/Delay	Cost	Cost	Multiple Attributes
Administrative Distance	120	120	100	90 (internal) 170 (external)	110	115	20 (external) 200 (internal)
Hopcount Limit	15	15	255 (100 default)	224 (100 default)	None	None	EBGP Neighbors: 1 (default) IBGP Neighbors: None
Convergence	Slow	Slow	Slow	Very Fast	Fast	Fast	Average
Update timers	30 seconds	30 seconds	90 seconds	Only when change occurs	Only when changes occur, (LSA table is refreshed every 30 minutes, however)	Only when changes occur	Only when changes occur
Updates	Full table	Full table	Full table	Only Changes	Only Changes	Only changes	Only changes
Classless	No	Yes	No	Yes	Yes	Yes	Yes
Supports VLSM	No	Yes	No	Yes	Yes	Yes	Yes
Algorithm	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra	Dijkstra	Best Path Algorithm
Update Address	Broadcast	224.0.0.9	224.0.0.10	224.0.0.10	224.0.0.5 (All SPF Routers) 224.0.0.6 (DR's and BDR's)		Unicast
Protocol and Port	UDP port 520		IP Protocol 9	IP Protocol 88	IP Protocol 89		TCP port 179

Table II-Routing Protocol Deference

2.2.7 Configaration

In this project we need configure two types of device network device and computer or Host device .

- **Computer IPv6 configuration**

Unlike IPv6 in Windows XP and Windows Server 2003, the IPv6 protocol in Windows Server 2008 and Windows Vista is installed and enabled by default. The IPv6 protocol for Windows Server 2008 and Windows Vista is designed to be auto configuring. For example, it automatically configures link-local addresses for communication between nodes on a link. If there is an IPv6 router on the host's subnet or an ISATAP router, the host uses received router advertisements to automatically configure additional addresses, a default router, and other configuration parameters. You can manually configure IPv6 addresses and other parameters in Windows Vista using the following:

a) Form LAN card properties.   b)From command prompt.

We can configure IPv4 settings through the properties of the Internet Protocol Version 4 (TCP/IPv4) component in the Network Connections folder, We can now configure IPv6 settings through the properties of the Internet Protocol Version 6 (TCP/IPv6) component. The set of dialog boxes for IPv6 configuration is very similar to the corresponding dialog boxes for IPv4. However, the properties of the Internet Protocol Version 6 (TCP/IPv6) component provide only basic configuration of IPv6.We can in Windows XP and Windows Server 2003, you can configure IPv6 settings for Windows Server 2008 or Windows Vista from the interface ipv6 context of the **Netsh.exe** tool. Although typical IPv6 hosts do not need to be manually configured, IPv6 routers must be manually configured.

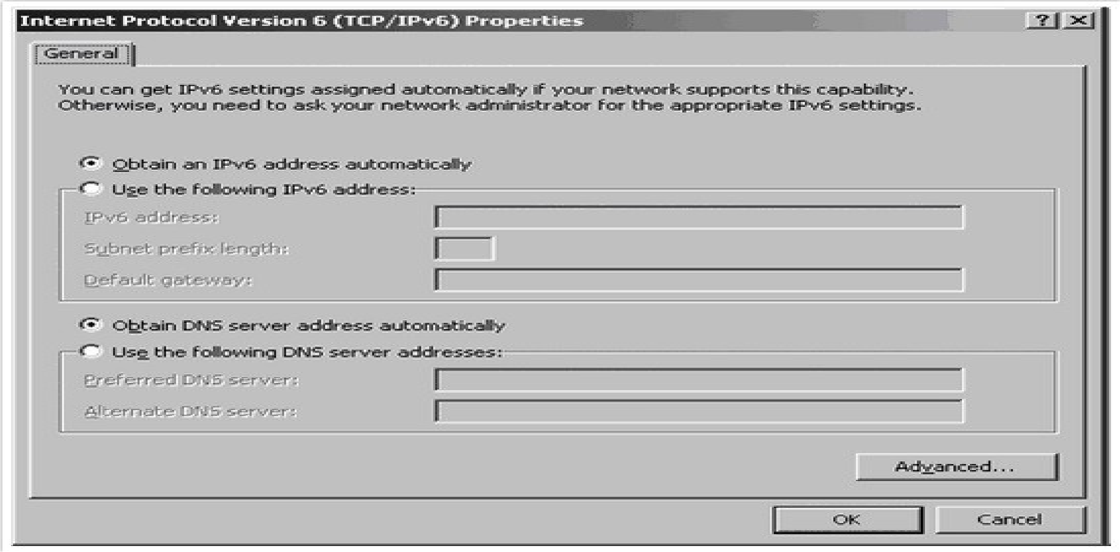
Configuring IPv6 Through the Properties of (TCP/IPv6)

To manually configure IPv6 settings through the Network Connections folder, We need to do the following:

1) From the Network Connections folder, right-click the connection or adapter on which you want to manually configure IPv6, and then click Properties.

2) On the Networking tab for the properties of the connection or adapter, under This Connection Uses The Following Items, double-click Internet Protocol Version 6 (TCP/IPv6) in the list.

The Internet Protocol Version 6 (TCP/IPv6) Properties dialog box



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability.
Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Fig 2.1 internet protocol version 6 dialog box

On the General tab of the Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, you can configure the following:

a) Obtain an IPv6 address automatically Specifies that IPv6 addresses for this connection or adapter are automatically determined by stateful or stateless address autoconfiguration.

b) Use the following IPv6 address< Specifies that an IPv6 address and default gateway for this connection or adapter are manually configured.

c) IPv6 address Provides a space for you to type an IPv6 unicast address. You can specify additional IPv6 addresses from the Advanced TCP/IP Settings dialog box.

d) Subnet prefix length Provides a space for you to type the subnet prefix length for the IPv6 address. For typical IPv6 unicast addresses, this value should be set to 64, its default value.

e) Default gateway Provides a space for you to type the IPv6 unicast address of the default gateway.

f) Obtain DNS server address automatically Specifies that the IPv6 addresses for DNS servers are automatically determined by stateful address autoconfiguration (DHCPv6).

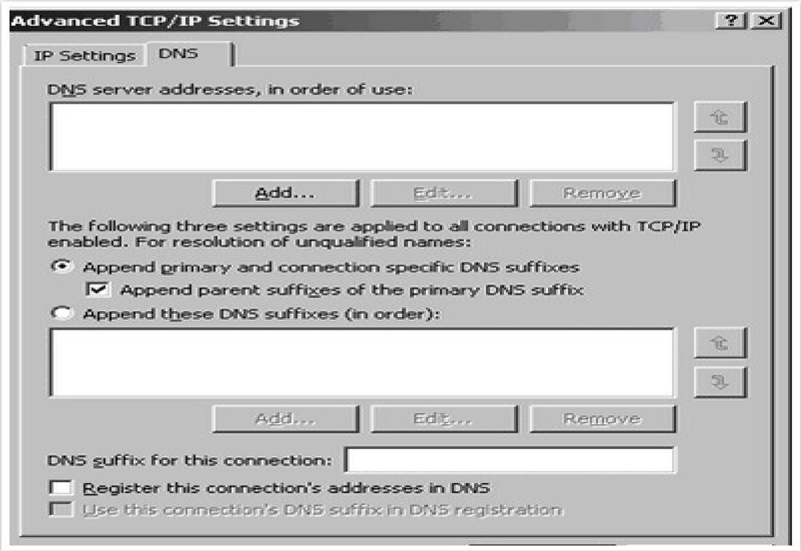
g) Use the following DNS server addresses Specifies that the IPv6 addresses of the preferred and alternate DNS servers for this connection or adapter are manually configured.

h) Preferred DNS server Provides a space for you to type the IPv6 unicast address of the preferred DNS server.

i) Alternate DNS server Provides a space for you to type the IPv6 unicast address of the alternate DNS server. You can specify additional DNS servers from the Advanced TCP/IP Settings dialog box.

• Advanced TCP/IP Settings

From the General tab, you can click Advanced to access the Advanced TCP/IP Settings dialog box. This dialog box is very similar to the Advanced TCP/IP Settings dialog box for the Internet Protocol Version 4 (TCP/IPv4) component except there is no WINS tab (IPv6 does not use NetBIOS and the Windows Internet Name Service [WINS]) or Options tab (TCP/IP filtering is defined only for IPv4 traffic). For IPv6, the Advanced TCP/IP Settings dialog box has IP Settings and DNS tabs.



DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

□ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

Fig 2.2Advance tcp/ip setting Dialogbox

- **The IP Settings tab**

From the IP Settings tab, you can configure the following:

a) Multiple IPv6 addresses (by clicking Add under IP Addresses) For each unicast IPv6 address, you must specify an IPv6 address and a subnet prefix length. The Add button is available only if Use The Following Ipv6 Address has been selected on the General tab of the Internet Protocol Version 6 (TCP/IPv6) Properties dialog box.

b) Multiple default gateways (by clicking Add under Default Gateways) For each default gateway, you must specify the IPv6 address of the gateway and whether you want the metric for the default route associated with this default gateway to be manually specified or based on the speed of the connection or adapter.

c) Route metrics You can also specify whether to use a specific metric for the routes associated with the configuration of IPv6 addresses or default gateways or a metric determined by the speed of the connection or adapter.

- **The DNS tab**

From the DNS tab, you can configure the following:

a) The IPv6 addresses of DNS servers, in order of use (by clicking Add under DNS Server Addresses, In Order Of Use).

b) Primary and connection-specific DNS suffix and name registration and devolution behavior. These settings are the same as for IPv4.

Chapter 03

Efficient Approach of converting an IPv4 Network To IPv6

3.1 Introduction

In Bangladesh IIG And ISP Company are rapidly increases, Due to their reseller Global IP requirement are exponential with various technology as cloud, BYOD, virtualization. By taking this issue the solution could be a conversion there existing network from IPv4 to IPv6 network with the Enhance intrigued Gateway routing Protocol for proper utilize of network bandwidth ,This Project will going to brief discretion on an efficient approach to convert an IPv4 network to IPv6 Network . This efficient approach that allows discovering IPv4 and IPv6 network assets, plan and model, IPv6 addressing scheme and map your IPv6 network onto existing IPv4 resources. We hope that our approach enables you to make the conversion easier From any IPv4 to IPv6 network.

3.2 Basic Planning

On this project our object is converting any IPv4 Network to IPv6 network .According to our view to implement this here we introducing a sequence of steps (three steps).There are

A) Network Assets Management.

B) IP Address management Technology.

C) Configuration with low cost Routing protocol.

3.2.1 Network Assets Management

After collection of Existing IPv4 network topology Network Assets Management system start it's works .

First it list out all the devices of existing network according the network types thro propose Table

Table III Device Identification table

SL NO	Network Type	Device Name	Host Name
1	LAN	Server,Switch,PC and others access Devices	WEB Server(e.g)
2	WAN	Router ,Firewall,	BoderRouter(e.g)
3	Border Network	Border Router ,Border Firewall ,Proxy Server	DC Firewall(e.g)

- **LAN Device**

With the definition sense of LAN all the Access devices and related switch and hub are the element of this category.

- **WAN Device**

With the definition sense of WAN all the Router, Layer Three Switch,Firewell are the element of this category .

- **Border Router**

Exit and enter point device of an autonomous system are the element of this category . After completing the device identification Table Network Assets Management system start to identification link of devices with physical interface according to Propose Table.

Table IV Interconnected Interface table

Interconnected Interface with Host name	Network Types
Border Router Se0/0/0 to BDR Se0/0/0(e.g)	WAN
PC Nic to LAN Switch FE0/0(e.g)	LAN

- **Interconnected Interface Table**

Here we can identify the inter related interface link and also can assigned network type which is help as to allocated ipv6 address according to network types. Easy techniques of assigned network types of Interface link is router to router link is Wan and Router to switch and Switch to PC or others host is LAN Network .

3.2.2 IP Address Management Technology

After collect the IPv6 IP range we apply variable length subnetting for WAN and LAN Network separately under tabular format called LAN Subneting Table and WAN Subnetting .

- **WAN IPv6 Address**

Table V WAN IPv6 Address Table

Given Range	1st Range	2nd Range	3rd Range	Smallest Range
::/32	::/64	::/96	::/112	::/124
2^96	2^64	429,49,67,296	65536	15 Host
			One of them will Given for LAN	WAN

According to the table WAN Interface pare port will get Smallest /124 subnet IPv6.

- **LAN IPv6 Address**

Table VI -LAN IPv6 Address Table

Given Range from LAN IPv6 Address ::/112	Range For Lan ::/120(Variable)
e.g 2404:b00:0:3:0:7::/112	2404:b00:0:3:0:7:1::/120

After choosing an IPv6 address Rang we split it /120 subnet than we cane use it for LAN Side .

3.2.3 Configuration with low cost Routing protocol

According to the IP address Table we need to configure all router and others Network device with CLI command and set IP to computer or host device . Here we used Cisco command line interface language [2.2.7] .

CLI Command

- ### Configuring Passwords

This command works on both routers and switches

Router(config)#enable password test	Sets enable password to **test**
Router(config)#enable secret vinita	Sets enable secret password to **vinita**
Router(config)#line console 0	Enters console line mode
Router(config-line)#password console	Sets console line mode password to **console**
Router(config-line)#login	Enables password checking at login
Router(config)#line vty 0 4	Enters vty line mode for all five vty lines
Router(config-line)#password telnet	Sets vty password to **telnet**
Router(config-line)#login	Enables password checking at login
Router(config)#line aux 0	Enters auxiliary line mode
Router(config-line)#password aux	Sets auxiliary line mode password to **aux**
Router(config-line)#login	Enables password checking at login

- Configuring a Fast Ethernet Interface

Router(config)#interface fastethernet 0/0	Moves to Fast Ethernet 0/0 interface configuration mode
Router(config-if)#description Student Lab LAN	Optional descriptor of the link is locally significant
Router(config-if)#ip address 192.168.20.1 255.255.255.0	Assigns address and subnet mask to interface
Router(config-if)#no shutdown	Turns interface on

- **Creating a Message of the Day Banner**

```
Router(config)#banner motd # Next Schedule metting with manager is Postponed   #
```

- Saving and erasing configurations

Router(config)#exit	Bring you back in Privilege exec mode
Router#copy running-config startup-config	Saves the running configuration to local NVRAM
Router#copy running-config tftp	Saves the running configuration remotely to a TFTP server
Router#erase startup-config	Deletes the startup configuration file from NVRAM

- **Configuration Example: Basic Router Configuration**

```
    --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface fastethernet 0/0
R1(config-if)#description Student Lab LAN
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state toup
R1(config-if)#exit
```

```
R1(config)#banner motd # Next Schedule metting with is postponed #
R1(config)#banner login # Unauthorized access is prohibited !
 Enter you user name and password #
R1(config)#ip host Lucknow 172.16.1.1
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#password consloe
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password telnet
R1(config-line)#login
R1(config-line)#exit
% Unrecognized command
R1(config)#enable password test
R1(config)#enable secret vinita
R1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Chapter 04

Application on a Real Scenario

4.1 Real scenario

In this chapter we will apply our approach to converting an IPv4 conventional network to an IPv6 Network with EIGRP Routing Protocol on a collected IPv4 network topology .This real topology collected from an renown running Nation wide ISP company which customer number are increasing day by day .

4.1.1 Collected Existing Topology

To implement our An efficient approach of converting an IPv4 Network to IPv6 Network through dynamic Enhance intrigued Gateway routing Protocol we collect a topology from a Large renown ISP Company the topology are below

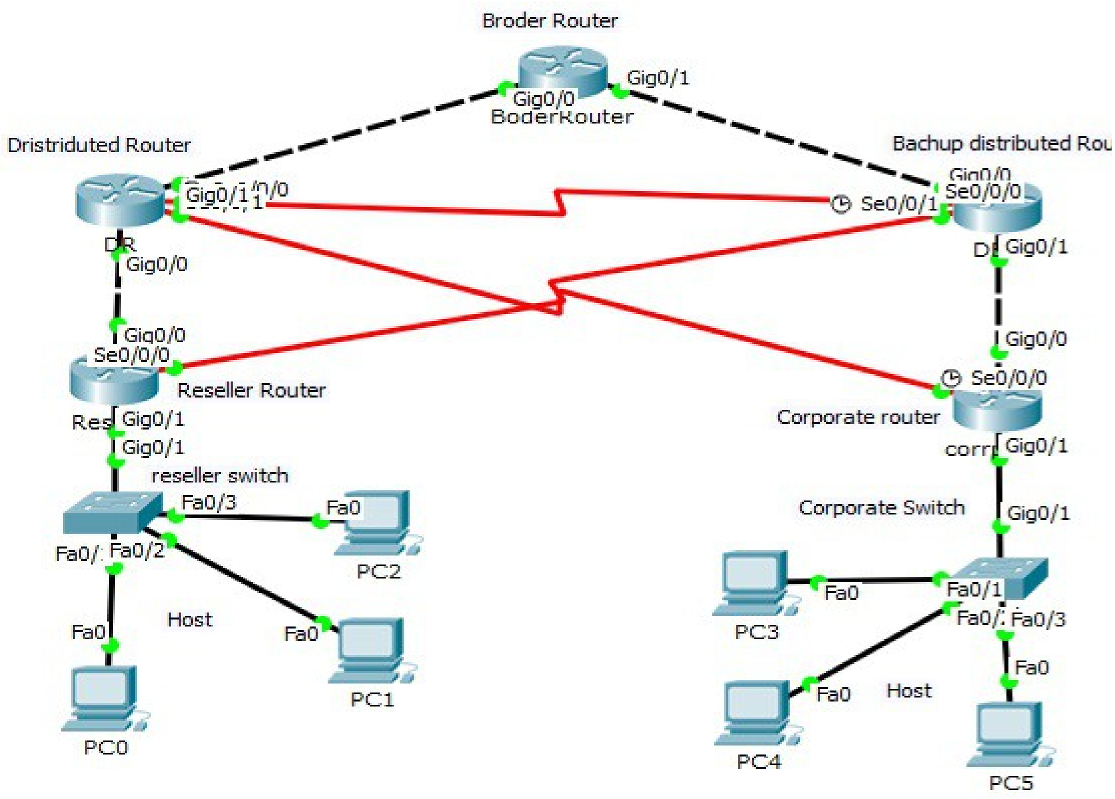


Fig 3.1: Existing ISP Topology

4.1.2 Basic Configuration details of Existing Topology

- **Border Router**

In this topology They use a Border router to connect up link as like Mango or Ammar Technology with any BGP routing protocol and static route company assign ip to down link for won network thro two giga ether port .

- **DR**

Distributed Router is used for Distributed IP address to ISP won Devices according to sequence and serial Ip subnet with /30 series

- **BDR**

Backup Distributed Router is used for Distributed IP address to ISP won Devices according to sequence and serial IP subnet with /30 series on behalf of DR throw Serial link with Secondary IP Address .

- **Reseller**

This router use to distribute IP to IPS who get connection from this ISP as Mother Company or Uplink.

- **Corporate**

This router use to distribute IP to Corporate who get connection from this ISP as Mother Company or Uplink.

- **Reseller Switch**

This switch is a layer two Manageable switch which is use for each ISP UP link thro it's each gi/fa port .

- **Corporate Switch**

This switch is a layer two Manageable switch which is use for each Corporate client UP link thro it's each gi/fa port . They configure Broder router uplink with BGP routing Topology according to there uplink company and all others device configure Static IP according small last subnet /30 for each link and also two Router named Reseller and Corrporet to distribute and allocated IP for there operations .Two Switch use for district them from each other with there specific VLan .

4.1.3 Device Identification table creation

Table VII Device Identification Drive Table

SL NO	Network Type	Device Name	Host Name
1	LAN	Server,Switch, PC and others access Devi	Reseller Switc,Corporate Switch. Host Pc
2	WAN	Router ,	DR,BDR.ResellerRouter,CorporateRouter
3	Border Network	Border Router ,	Border Router

According to the table number III we can identify all devices with Network type .Here we find all router except broder Router are WAN device and only border router is Border Network device .All switch and Pc are Lan Device .

4.1.4 Interconnected Interface table creation

Table VIII Interconnected Interface Drive Table

Interconnected Interface with Host name	Network Types

Border Router LoopBack 0	WAN
Border Router LoopBack 1 Mango	WAN
Border Router LoopBack 2 AAmra	WAN
Border Router Gig0/0/0 to DR Gig 0/0	WAN
Border Router Gig0/0/1 to BDR Gig 0/0	WAN
DR Serial 0/0/0 to BDR Serial 0/0/0	WAN
DR Se0/0/1 to Corporate Router Se0/0/0	WAN
BDR Se0/0/1 to Reseller Router Se0/0/0	WAN
Reseller Router Gig0/1 to Reseller Sw Gig0/1	LAN
Corporate Router Gig0/1 to Corporate Sw Gig0/1	LAN
Reseller Switch to PC or client	LAN

According to the table number 4 from there topology we find the inter connected interfere fro assigning IPv6 address . Here Broder router contain three LoopBack interface .A loopback interface is an virtual live interface it always run as active. Loopback 0 for Google HTTP interface .Loopback 1 for Mango up link and Loopbook 2 for AAmra Up link. Border Router Gig0/0/0 to DR Gig 0/0 interface interconnected WAN network . Border Router Gig0/0/1 to BDR Gig 0/0 interface interconnected WAN network. DR Serial 0/0/0 to BDR Serial 0/0/0 Backup interconnected WAN Network. DR Se0/0/1 to Corporate Router Se0/0/0 it work as Reseller router backup path and BDR Se0/0/1 to Reseller Router Se0/0/0 it work for Corporate router backup path as WAN Network . Reseller Router Gig0/1 to Reseller Sw Gig0/1 interface provide LAN Network and also can distributed SUBNET for reseller . Corporate Router Gig0/1 to Corporate Sw Gig0/1 1 interface provide LAN Network and also can distributed SUBNET for corporate .Host are single client computer and here act as test device .

4.2 Implementation of IP Address Management Technology.

After completing the Table 3 and 4 now we can create IPv6 address for WAN and LAN according to the table 5 and 6 WAN IPv6 Address and LAN IPv6 Address .

4.2.1 Implementation of WAN IPv6 Address

Table V WAN IPv6 Address Table

Given Range	1st Range	2nd Range	3rd Range	Smallest Range
::/32	::/64	::/96	::/112	::/124
2^96	2^64	429,49,67,296	65536	15 Host

			Given for LAN	WAN

This table show that what will be structure of our IPv6 IP Address if we gate ::/32 subnetted IP we should start from given range column if we get less according to the table that column is the given range .from 3rd range which sub net we will chose except it from here any one we can chose for LAN .The ISP company give me the 2404:b00::/32 series for IPv6 so the WAN IPv6 Address table looks like below

Table IX WAN IPv6 Address Table Damo

Given Range	1st Range	2nd Range	3rd Range	Smallest Range
::/32	::/64	::/96	::/112	::/124
2^96	2^64	429,49,67,296	65536	15 Host
2404:b00::	2404:b00::/64	2404:b00:0:3::/96	2404:b00:0:3:0:1::/112	2404:b00:0:3:0:8:a:0/124
2404:b00::	2404:b00::/64	2404:b00:0:3::/96	2404:b00:0:3:0:2::/112	2404:b00:0:3:0:2:a:0/124
			Given for LAN	WAN

According to the table 2404:b00:0:3:0:8:a:0/124 we can use for any WAN Interface link and 2404:b00:0:3:0:2:: For LAN so the full IPv6 WAN IP Address extended full table are shown on next page

Table X WAN IPv6 Address Extended Table

Ggiven Rang	**1st Range**	**2nd Range**	**3rd Range**	**Smallest (15 Host per Net)**
::/32	**::/64**	**::/96**	**::/112**	**::/124**
2^96	**2^64**	**429,49,67,296**	**65536**	**15 Host**
2404:b00::/32			**2404:b00:0:3:0:8:0::/112**	**2404:b00:0:3:0:8:a:0/124**
			2404:b00:0:3:0:8:1::/112	**2404:b00:0:3:0:8:a:10/124**
		2404:b00:0:3:0::/96	**2404:b00:0:3:0:8:2::/112**	**2404:b00:0:3:0:8:a:20/124**
		2404:b00:0:3:0:1::/96	**2404:b00:0:3:0:8:3::/112**	**2404:b00:0:3:0:8:a:30/124**
		2404:b00:0:3:0:2::/96	**2404:b00:0:3:0:8:4::/112**	**2404:b00:0:3:0:8:a:40/124**
		2404:b00:0:3:0:3::/96	**2404:b00:0:3:0:8:5::/112**	**2404:b00:0:3:0:8:a:50/124**
		2404:b00:0:3:0:4::/96	**2404:b00:0:3:0:8:6::/112**	**2404:b00:0:3:0:8:a:60/124**
	2404:b00::/64	**2404:b00:0:3:0:5::/96**	**2404:b00:0:3:0:8:7::/112**	**2404:b00:0:3:0:8:a:70/124**
	2404:b00:01::/64	**2404:b00:0:3:0:6::/96**	**2404:b00:0:3:0:8:8::/112**	**2404:b00:0:3:0:8:a:80/124**
	2404:b00:02::/64	**2404:b00:0:3:0:7::/96**	**2404:b00:0:3:0:8:9::/112**	**2404:b00:0:3:0:8:a:90/124**
	2404:b00:03::/64	**2404:b00:0:3:0:8::/96**	**2404:b00:0:3:0:8:a::/112**	**2404:b00:0:3:0:8:a:a0/124**
	2404:b00:04::/64	**2404:b00:0:3:0:9::/96**	**2404:b00:0:3:0:8:b::/112**	**2404:b00:0:3:0:8:a:b0/124**
	2404:b00:05::/64	**2404:b00:0:3:0:a::/96**	**2404:b00:0:3:0:8:c::/112**	**2404:b00:0:3:0:8:a:c0/124**

	2404:b00:f::/64	2404:b00:0:3:0:b::/96	2404:b00:0:3:0:8:d::/112	2404:b00:0:3:0:8:a:d0/124
		2404:b00:0:3:0:c::/96	2404:b00:0:3:0:8:e::/112	2404:b00:0:3:0:8:a:e0/124
		2404:b00:0:3:0:e::/96	2404:b00:0:3:0:8:f::/112	2404:b00:0:3:0:8:a:f0/124
		2404:b00:0:3:0:f::/96	2404:b00:0:3:0:8:10::/112	2404:b00:0:3:0:8:a:100/124
			2404:b00:0:3:0:8:11::/112	2404:b00:0:3:0:8:a:110/124
			2404:b00:0:3:0:8:12::/112	2404:b00:0:3:0:8:a:120/124
			2404:b00:0:3:0:8:13::/112	
			2404:b00:0:3:0:8:14::/112	
			2404:b00:0:3:0:8:15::/112	
			2404:b00:0:3:0:8:1f::/112	
			For LAN	**WAN**

4.2.2 Implementation of LAN IPv6 Address Table

Table XI -LAN IPv6 Address Table

Given Range from LAN IPv6 Address ::/112	Range For Lan ::/120(Variable) Host 256
2404:b00:0:3:0:7:1::/112	2404:b00:0:3:0:7:1:0:/120 - 2404:b00:0:3:0:7:1:FF:/120
	2404:b00:0:3:0:7:1:100:/120 - 2404:b00:0:3:0:7:1:1FF:/120

Now according to the XI LAN IPv6 Address table we can assign lan Network tyape IP addres

4.3 New Network Topology

After creating table TABLE VII Device Identification Drive Table and VIII Interconnected Interface Drive Table we can design the new IPv6 Topology without IPv6 Address which looks like below

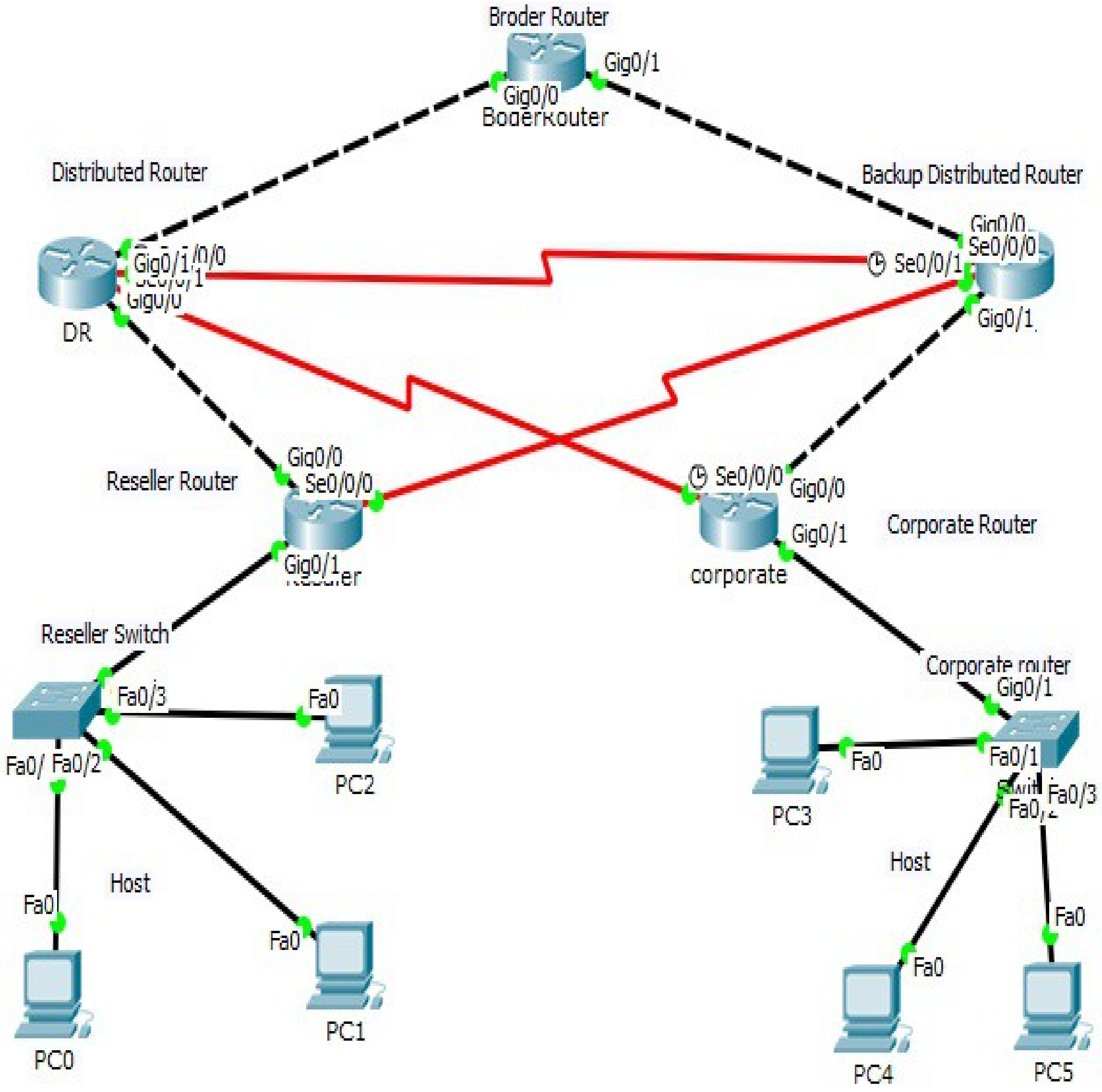


Fig 4.1: Converted IPV6 Topology without IPV6 Address

4.4 IPv6 New Network Topology

After creating table TABLE X WAN IPv6 Address Extended Table and TABLE XI -LAN IPv6 Address Table we can design the new IPv6 Topology with IPv6 Address which looks like below

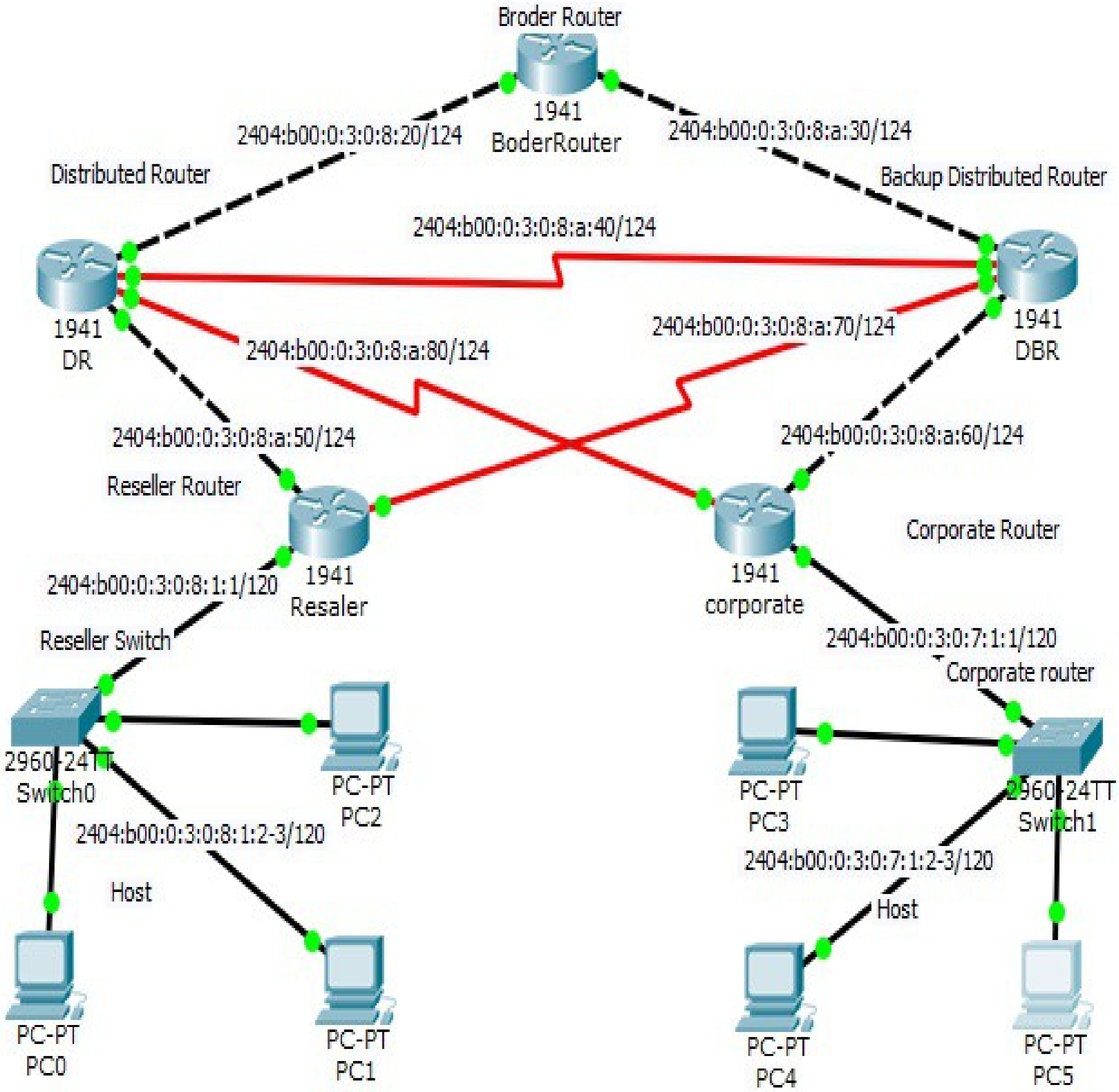


Fig 4.2 : Converted IPV6 Topology with IPV6 Address

In this topology Border router are connected to DR with 2404:b00:0:3:0:8:a:20/124 and Border Router are connected to BDR with 2404:b00:0:3:0:8:a:30/124 and also a serial path back up plan was exist if main path is cut over or disconnected data will be pass thro serial link those serial link are Dr to BDR with 2404:b00:0:3:0:8:a:40/124 and BR to corporate router with 2404:b00:0:3:0:8:a:50/124 and BDR to Reseller Router with 2404:b00:0:3:0:8:a:60/124. Reseller to reseller switch with 2404:b00:0:3:0:8:1:0/120 and corporate to corporate switch with 2404:b00:0:3:0:7:0/120 and the host are get 2,3,4 on there won subnet .

4.5 IPv6 New Network Topology IPv6 address Assigning

Table XII – ALL Interface IPv6 Address Table

Interconnected Interface with Host name	Network Types	IPv6Address
Border Router LoopBack 11	WAN	8:8:8:8:8:8:8:8
Border Router LoopBack 12 Mango	WAN	7:7:7:7:7:7:7:7
Border Router LoopBack 13 AAmra	WAN	6:6:6:6:6:6:6:6
Border Router Gig0/0/0 to DR Gig 0/0	WAN	2404:b00:0:3:0:8:a:20/124
Border Router Gig0/0/1 to BDR Gig 0/0	WAN	2404:b00:0:3:0:8:a:30/124
DR Serial 0/0/0 to BDR Serial 0/0/0	WAN	2404:b00:0:3:0:8:a:40/124
DR Se0/0/1 to Corporate Router Se0/0/0	WAN	2404:b00:0:3:0:8:a:80/124
BDR Se0/0/1 to Reseller Router Se0/0/0	WAN	2404:b00:0:3:0:8:a:70/124
DR Gig0/0 to Reseller Gigo/o	WAN	2404:b00:0:3:0:8:a:50/124
BDR Gig0/0 to Corporate Gig0/0	WAN	2404:b00:0:3:0:8:a:60/124
Reseller Router Gig0/1 to Reseller Sw Gig0/1	LAN	2404:b00:0:3:0:8:1:1/120
Corporate Router Gig0/1 to Corporate Sw Gig0/1	LAN	2404:b00:0:3:0:7:1:1/120
Reseller Switch to PC or client	LAN	PC0-2404:b00:0:3:0:8:1:2/120
		PC1-2404:b00:0:3:0:8:1:3/120
		PC2-2404:b00:0:3:0:8:1:4/120
Corporate Switch to PC or client	LAN	PC0-2404:b00:0:3:0:7:1:2/120
		PC1-2404:b00:0:3:0:7:1:3/120
		PC2-2404:b00:0:3:0:7:1:4/120

According to this table we can convert IPv4 Topology to IPv6 Network Topology.

Chapter 5

Configuration and Test

5.1 Configuration

In this chapter according to the CLI Language and our approach now we going to show how to configure various device in real life of new IPv6 Topology to use Packet tracer simulation .Thro the packet tracer we can create router ,switch pc and others network devices and can test .

5.1.1 Packet Tracer

Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask “what if” questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts.

Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving. Packet Tracer complements the Networking Academy curricula, allowing instructors to easily teach and demonstrate complex technical concepts and networking systems design.

5.2 Device configuration

Here now we will going to show specific configuration for each device and issues . There are some basic configuration as like host name ,logging ,password telnet , consol, banner and other management configuration and also has some technical configuration. Configuration are below with sub title .

5.2.1 Device Access command

```
BoderRouter>en
BoderRouter>enable
Password:
BoderRouter#sho
BoderRouter#show run
BoderRouter#show running-config
Building configuration...
Current configuration : 1674 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

5.2.2 Device Basic configuration

```
!
hostname BoderRouter
!
enable password ewu
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX15245489
!
spanning-tree mode pvst
```

5.2.3 Device IPv6 Active configuration

To act with IPv6 Address router and switch need to be active thro command like below

5.2.4 Device IPv6 Enable Configuration

```
!
no ip cef
ipv6 unicast-routing
!
```

5.2.5 Device Interface IPv6 Enable Configuration

```
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 enable
!
```

5.2.6 Device Inter face IPv6 Address Configuration

```
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2404:B00:0:3:0:8:A:31/124
ipv6 enable
!
interface FastEthernet0/0/1
switchport mode trunk
shutdown
!
interface FastEthernet0/0/2
switchport mode access
shutdown
!
interface FastEthernet0/0/3
switchport mode access
shutdown
!
interface Serial0/1/0
clock rate 2000000
shutdown
!
```

5.2.7 Device Router Id Configuration

```
!
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
no shutdown
!
```

5.2.8 IPv6 EIGRP Configuration

In IPv6 Address configuration no need to configure network for EIGRP only interface are need to allocated as EIGRP as like below

```
!
ipv6 router eigrp 1
eigrp router-id 1.1.1.1
no shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2404:B00:0:3:0:8:A:31/124
ipv6 eigrp 1
ipv6 enable
!
```

5.3 Ping Test

Packet Tracer simulating is visually capable to show PING Packet pass as Envelops from one device to others and only pc need to show at CLI Mode PING command.

Chapter 5

Conclusion and Future Works

5.1 Summary of the Efficient approach

This literature provides a approach called An efficient approach of converting an IPv4 Network to IPv6 Network through dynamic Enhance Interior Gateway routing Protocol to make the IPv4 to IPv6 conversion easy and quick. The detailed of IPv6, EIGRP and CLI command and the tabular technical of Our approach are discussed theoretically in here. Where the IPv6 and the EIGRP approach provides good performance and it can be applicable in a ISP Topology models. The higher complexity IPv6 enable on Router FastEthernet interface also achieves better performance by CLI Advance command which feature is very suitable for research and education network and ISP, IIG, IGW network. In the DUAL feature of EIGRP provide manageable Optimum dynamic path for routing. On the other hand, the IPv6 increase the IP address for unique identification of large number of global devices or node. The serial back up techniques also reduce the possibility of live device down and backup link alive.

Undoubtedly the successful application of efficient approach of converting an IPv4 Network to IPv6 Network to ISP network will considerably enhance the efficient of the operating ISP, IIG, IGW. Effectively, Efficient approach of converting an IPv4 Network to IPv6 Network give the potion to provide large number of IP to there customer . This success is limited because here we only use manual subnetting on Unicast addresses and **Multicast addresses. Anycast addresses** which need to be addressed in future research.

REFERENCES

[1] ISIUSC, "DARPA internet program protocol specification,"Information Sciences Institute University of Southern California,1981

[2] S. Jian and Y. Y. Fang. "Research and implement of Ospfv3 in Ipv6 network," in Proc. of Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, Harbin, China, July 26-30, 2011, pp.743-746.

[3] M. Cooper and D. C. Yen. "IPv6: business applications and implementation concerns," Computer Standards and Interfaces,vol.28, no. 1, pp. 27–41. July 2005.

[4] X. Wen, C. Xu, J. Guan, W. Su, and H. Zhang, "Performance investigation of IPsec protocol over IPv6 network," in Proc. Of Artificial Intelligence Applications & Innovations, Larnaca, Cyprus,October 6-7, 2010, pp. 174-177.

[5] O. J. S. Parra, A. P. Rios, and G. L. Rubio, "IPV6 and IPV4 QoS mechanisms," in Proc. of International Organization for Information Integration and Web-based Application and Services, 2011, pp.463-466.

[6] R. M. Hinden, "IP next generation overview," Communications of the ACM, June 1996, vol. 39, no. 6, pp. 61-71.

[7] D. Genkov, "An approach for finding proper packet size in IPv6 networks," in Proc. of 12th International Conference on Computer Systems and Technologies, Vienna, Austria, 2011, pp. 442-447.

[8] A. Balchunas. (2007). Static vs. dynamic routing. [Online]. Available: http://www.routeralley.

[9] http://en.wikipedia.org/wiki/Computer_network

[10] http://whatis.techtarget.com/definition/BYOD-bring-your-own-device

[11] http://www.protocols.com/pbook/tcpip1]

[12] http://docs.oracle.com/cd/E19455-01/806-0916/6ja85398k/index.html

[13] S. Shah, et al.,“Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation,” Proceedings of the NationalConference on Mobile and Pervasive Computing (CoMPC-2008), Chennai, India, August 2008.

[14] K. Gorantala, “Routing Protocols in Mobile Ad Hoc Networks, ” Master Thesis, Department of Computing Science, UmeøaUniversity, Sweden, June 2006.

[15] Z. Bojković, M. Stojanović, and B. Milovanović, “Current Developments towards the 4G Wireless System,” Proceedings of International Conference TELSIKS, N iš, Serbia, September 2005, pp. 229-232.

[16] S. Barakovićand J. Baraković, “Comparative Performance Evaluation of Mobile Ad Hoc Routing Protocols,”Proceedings of the 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2010),Opatija, Croatia, May 2010.[5] Nurul I. Sarkar & Wilford G.

[17] Lol “A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility” 978 -1-4244-7755-5/10/$26.00 ©2010 IEEE Page no. 515-520

[18] Vasudha Arora & C. Rama Krishna “Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions” 2010 2nd International Conference on Computer Engineering and Technology [Volume 6] 978 -1-4244-6349-7/10/$26.00 c 2010 IEEE

[19] Patel, B.; Srivastava, S.;, "Performance analysis of zone routing protocols in Mobile Ad Hoc Networks," Communications (NCC),2010 National Conference on, vol.,pp.1-5, 29-31 Jan. 2010.

[20] J. Wang, F. Xu, F. Sun.“Benchmarkinng of Routing Protocols for Layered Satellite Networks”. In Proceedings of Multiconference on Computational Engineering in Systems Applications, pp. 1087-1094, vol. 2, Oct 2006.

[21] Lachhman,S., Asad, Y.,Malkani “Performance analysis of WLAN standards for video conferencing applicati ons” , InternationalJournal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 6, December 2011[10] Rajan, R., Shipra, S. “WLAN Performance Improvisation by Fine Tuning IEEE 802.11 Parameters”, International Journal ofComputer Applications, April 2012.

[22] 1. D. Gesbert, M. Shafi, D. – S. Shiu, P. J. Smith, and A. Naguib, “From theory to practice: An overview of MIMO space – time coded wireless systems,” IEEE Journal on Selected Ares In Communications, vol. 21, no. 3, pp. 281 – 302, April 2003.

[23] How To Master of NP , C 2002-2011 by René Molenaar.

[24] Intendamono , B C Fuga 2002- 2004