COMPARATIVE ANALYSIS BETWEEN LINK STATE PROTOCOLS OVER MPLS USING GNS 3

Research Proposal

By:

Saif-ur-Rehman (Roll # MSCS-F14-006)

MS (CS) / M.Phil

raajput007@gmail.com

Supervisor:

Mr. Engr. Waheed Aftab Khan

Department of Computer Science & Information Technologies

Superior University Lahore

In the name of Allah, the most Gracious, the most Merciful.

DECLARATION

I, Saif-ur-Rehman, Roll.#. MSCS-F14-006, student of MS (CS), certify that this thesis does not, to the best of my knowledge and belief:

- Contain any material previously or concurrently submitted / published.
- Contain any defamatory material.

Witnessed by:-

_____	_____
(Signature of Author)	**(Signature of Supervisor)**
Name : Saif-ur-Rehman	**Name :** Engr. Waheed Aftab Khan
Roll # : MSCS-F14-M006	**Date:**
Date:	

COMPARATIVE ANALYSIS BETWEEN LINK STATE PROTOCOLS OVER MPLS USING GNS 3

Submitted by

SAIF-UR-REHMAN

The undersigned certified that I have seen, verified and recommend this thesis for partial fulfillment of the requirement for Degree of Master of Science in Computer Science.

Signature: _____

Main Supervisor: Engr. Waheed Aftab Khan.

ACKNOWLEDGEMENTS

Firstly, I would like to say my deep thanks to Allah Almighty for his usual help, guidance, strength and endurance to complete this Dissertation work.

Foremost, I would like to express my sincere thanks to my advisor Engineer Waheed Aftab Khan, for his patience, motivation, enthusiasm and immense knowledge as well as guidance that helped me in all the times of research and writing of this thesis.

Further, I would also like to extend a very unfathomable thanks to my beloved family, parents, teachers, supervisors and bosom friends of Superior University who also helped me for successful completion of this thesis.

DEDICATION

I, dedicate my this dissertation work to my beloved Family and many amazing friends, who have been a constant source of support, guidance and encouragement during this challenging task. ‘Hasaan & Javeria’ my beloved kids, I am also truly thankful to you for having you in my life. This work is also dedicated to my beloved Parents, who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve.

Signature: _____

Saif-ur-Rehman

LIST OF ACRONYMS

ABR	Area Border Router
AD	Administrative Distance
ANSI	American National Standards Institute
APPN	Advanced Peer-to-Peer Networking
ASCII	American Standard Code for Information Interchange
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
AS	Autonomous System
AToM	Any Transport Over MPLS
BGP	Border Gateway Protocol
CE	Client Edge
CID	Cisco Internetwork Design
CIDR	Classless Inter-Domain Routing
CoS	Class of Service
CPU	Central Processing Unit
CSNP	Complete Sequence Number PDU
CSPF	Constraint Based Shortest Path First
DBD	Database Description
DIS	Designated IS
DLCI	Data Link Connection Identifier
DLS	Data Link Switching
DVR	Distance Vector Routing
DVRP	Distance Vector Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ELSR	Edge Label Switch Router
ESV	Encapsulated Postscript Vector
ES	End System
FIB	Forwarding Information Base
FDDI	Fiber Distributed Data Interface
FE	Fast Ethernet
FEC	Forwarding Equivalence Class

FR	Frame Relay
FTP	File Transfer Protocol
GNS	Graphical Network Simulator
GNU	General Public License
GUI	Graphical User Interface
HDLC	High Level Data Link Control
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
ICMP	Internet Control Message Protocol
IEC	International Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gate Protocol
IGRP	Interior Gateway Routing Protocol
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Standard Organization
ISP	Internet Service Provider
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Network
LDP	Label Distribution Protocol
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LLC	Logical Link Control
LS	Link State
LSA	Link State Advertisement
LSD	Link State Database
LSP	Label Switched Path
LSR	Link State Router/ Link State Request
LSU	Link State Update
MAC	Media Access Control

MAN	Metropolitan Area Network
MNET	Mobile Ad Hoc Network
Mbps	Million Bits Per Second
MLD	Multicast Listener Discovery
MPLS	Multiprotocol Label Switching
NA	Network Administrator
NAT	Network Address Translation
NBMA	Non-Broadcast Multiple Access
NDN	Named Data Network
NE	Network Engineer
NS	Network Simulator
NSAP	Network Service Access Point
NMS	Network Management System
NOC	Network Operation Center
OLSR	Optimized Link State Routing
OPNET	Optimized Network Engineering Tool
OSI	Open Source Interconnection
OSPF	Open Shortest Path First
PDU	Packet Datagram Unit
PE	Provider Edge
PHB	Per-Hop-Behavior
PHP	Penultimate Hop Popping
POC	Proof of Concept
POP	Point of Presence
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
P-to-P	Peer to Peer
PPTP	Point-to-Point Tunneling Protocol
RAM	Random Access Memory
RD	Router Distinguisher
RIB	Routing Information Base
RIP	Routing Information Protocol
RSVP	Resource reservation Protocol

RT	Route Target
SAGE	Semi-Automatic Ground Environment
SDLC	Synchronous Data Link Control
SDN	Software Defined Network
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SPF	Shortest Path First
SNA	Systems Network Architecture
SSH	Secure Shell
SSL	Secure Sockets Layer
SVG	Scalable Vector Graphics
TDP	Tag Distribution Protocol
TE	Traffic Engineering
TCP	Transportation Control Protocol
TLS	Transport Layer Security
TMN	Telecommunication Management Networks
TPID	Tag Protocol ID
TTL	Time to Live
TWCC	Two Way Connectivity Check
TVL	Type, Length, Value
QA	Quality Assurance
QLLC	Qualified Logical Link Control
QoS	Quality of Service
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Masking
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
W3C	World Wide Web Consortium
WAN	Wide Area Network
WYSIWYG	What You See is What You Get
W3C	World Wide Web Consortium
XRP	Ripple Payment Protocol

ABSTRACT

To govern the eminence of IP communication over any enterprise network/ ISP (Internet Service Provider) Link State Protocols, OSPF (*Open Shortest Path First*) & IS-IS (*Intermediate System to Intermediate System*) have the significant influence. Selection of best route between different recognized paths, calculate the lesser amount of routing traffic and convergence time are the key factors utilized by Link State Protocols for reaching to the desired destination. Although, IS-IS and OSPF are much more similar but IS-IS is the best choice and has better grip because of its good route convergence time, CPU utilization, scalability, minimum bandwidth requirement, better throughput and queuing delay and security as compared to OSPF. IS-IS works on layer 2 whereas OSPF transported by layer 3, MPLS (*Multiprotocol Label Switching*) hits between both of them and operates on layer 2.5. Thus the presence of MPLS including its applications and features strengthen the link state protocols and make the best choice for an ISP / Enterprise networks to implement. In this thesis, the comparative analysis of IS-IS and OSPF has been done over MPLS by using GNS3 (*Graphical Network Simulator Version 3*). As a matter of proof, different tests have been conducted, traffic generated, monitored and analyzed by using real time software and IOS i.e. CISCO IOS (*Internetwork Operating System*) for Routers' configuration and implementation in GNS, FileZilla for transferring the files, Wireshark for packet sniffing, data monitoring and analyzing, graph generating etc. Resultantly, it has been revealed which protocol in Link-State category is better choice for an ISP/ Enterprise network to implement that provides less link cost, better security, scalability and flexibility for a large network management operations.

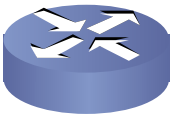
Keywords: Link State Protocol (LSP), OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System), MPLS (Multiprotocol Label Switching), GNS3 (Graphical Network Simulator 3), IOS (Internetwork Operating System), Architecture of MPLS, Difference between Link State Protocol, Comparative Analysis of OSPF and IS-IS.

TABLE OF CONTENTS

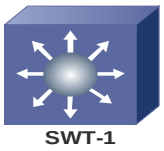
LIST OF FIGURES

LIST OF TABLES

ICONS USED IN THESIS



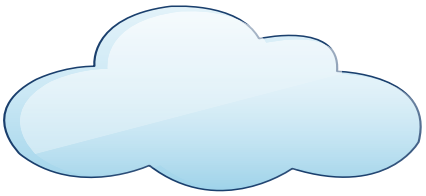
Router



Layer – III Devices

Layer – II Devices

Link Between Router



Cloud / Internet

End User Device

Figure 1: Icons Used in Thesis

Thesis Organization

Chapter # 1, comprising on the concise introduction of the topic. A glimpse over the subject matter, starting from basic protocol terminologies, discrepancies and its importance within the ISP / Enterprise Networks Environment has been delivered. Motivation for selection of this topic, problem statement and objectives have also been given.

Chapter # 2, focuses on the literature review. The core concepts i.e. routing protocols, their roles in any network topology & infrastructure, static & dynamic routing, structures of IPv4 & IPv6 and their minute comparison, difference between the LSP and DVP, similarities and dis-similarities of LSRP, their headers and updates, comparison of LSRP(s) with the help of tables and diagrams have been elaborated in this chapter. Further, a brief overview of MPLS domain, its header details & label operations, MPLS architecture has also been provided.

Chapter # 3, consist on the working and operations of the main network topology on which all the experimental test beds have been conducted. The detail of the devices, their interfaces, IP addressing scheme, topology transition tables has been given. Moreover, core portion of the running configuration of LSP(s), MPLS and BGP has also been provided in this chapter.

Chapter # 4, presents the details of all the software tools, IOS and practices i.e. *GNS3*, *EDraw Max Portable*, *File Zilla FTP Client Server*, *WireShark* etc. that have been utilized in the completion of this thesis. More importantly, the detailed reasons to choose and utilize these tools have also been provided in this chapter.

Chapter # 5, comprising on the experimental test beds. Results, monitoring and analysis along with the statistical tables, interactive graphs, WireShark captured snapshots have been presented in this chapter. Conclusion of the results derived from the experimental test beds have also been discussed in details.

Chapter # 6, covers the conclusion derived from the results and analysis obtain from experimental test beds. Detail future scope has also been described in this topic.

Chapter # 7, this chapter is equipped with all the reference papers which have been thoroughly read for the completion of this thesis.

CHAPTER # 1

1. INTRODUCTION

Internet communication has played vital and significant role in today's life. Almost everyone in this world is connected with each other via internet or networks infrastructure. The concept of modern world without the existence of the internet is impossible and indispensable. As the Network Infrastructures are the spinal cord of the Internet/ Cloud because networks all around the world make the 'Internet'. Therefore, the character of the ISP (Internet Service Provider) has been increased manifold. They are responsible for high speed connectivity & data rate, reliable, secure data connectivity and communication. Resultantly, the role of protocols i.e. routing & routed has also become more noteworthy and substantial. As in traditional WAN communication, there were low throughput, convergence, high delay and high error rates. But due to the exponential growth of the internet surfers all around the world, ISP (Internet Service Provider) are bound to provide the efficient, speedy, reliable, secure communication and connectivity from source to destination. In this scenario, here come the pivotal role of the routing protocols specially Link State Protocols along with MPLS (Multiprotocol Label Switching).

Keeping in view the current scenarios of ISP and Enterprise Networks, technologies and objects are vastly increasing and incapacitating its existing constraints and challenges rapidly. As there is not concept of the protocols without network connectivity and communication, the world is contributing more and more to make network connectivity and communication smooth, speedy, reliable and secure. Thus, the protocols for the selection of best paths/ routes in the network should be flawless to a large extent and having less discrepancies and constraints. Therefore, Link State Protocol implementation over MPLS [11] domain has been done with the help of real time Network Simulator called, GNS3 (Graphical Network Simulator 3). Long look of the concepts of Link State Protocols (OSPF – Open Shortest Path First and ISIS – Intermediate System to Intermediate System) has been taken and discussion has been made in length.

Starting from the basic but valuable and renowned concept of Protocol, IP and Routing concept, all the features and operations of Link State Protocol, their key processes, design, advantages and dis-advantages, key points, implementation criteria, architectures etc. various other protocols i.e. IP, HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), TCP

(Transmission Control Protocol), XRP (Ripple Payment Protocol), POP (Post Office Protocol), NTP (Network Time Protocol) have also been describe minutely. But keeping in view the boundary of our thesis, a comprehensive overview of OSPF and IS-IS and their implementation in MPLS Domain [11] has been delineated in detail.

In the thesis, comprehensive overview of LSP (Link State Protocols) has been given within the domain of MPLS (Multiprotocol Label Switching). Nowadays, MPLS is the core technology of ISP(s) all over the world because it forward the data packets on the base of Labels and the LSR (Label Switch Router) does not consult layer-3 for packet forwarding and the data packet is forwarded to switch unit called, data plane. Therefore, the performance of Link State Routing Protocols also get enhancement with the existence of MPLS domain [11] in an Enterprise Network / ISP.

Moreover, with the help and support of the tables, diagrams and structures of protocols, the difference between the static and dynamic routing has also been discussed in detail for better understanding of the major concepts. As the network are like roadways or airways for transmission of data via wires and wirelessly, the role of the ISP (Internet Service Provider) has also been expand, so the role of protocols too. The selection of the protocol is not a child's play within an Enterprise Network/ ISP(s), ones has to be very careful for the selection of the protocols in any Network Infrastructure. Any wrong choice can ruin the performance, speed and security of the Network Infrastructure. The finding of this thesis will help the Network Experts/ Professional to select the suitable protocols solution for their Enterprise Network Infrastructure.

It is not out of place to mention here that the outcome of this thesis is not for the beginner in the field of IT/ Networks but for the NA (Network Administrators) & NE (Network Engineers), professionals and experts who are working is ISP/ Enterprise Network Environment.

1.1.Motivation

Spending approximately 15 years in the field of Information Technology and having expertise in Enterprise Network Infrastructure Environment, it is my core liability to design and configure the network by implementing prevailed/ current standards and technologies to get the optimal performance of the Network Infrastructure. Speedy, reliable and secure data transmission over the network topology is one of the fundamental concern of any Network Professional so mine is. Definitely, I always try my best to adopt the new tools and techniques for the enhancement and betterment of the Network Infrastructure. I believe, nobody could perform his best without knowing the basic/ fundamentals / core concepts of any technology.

It is certainly valuable to added here that majority of ISP(s) in Pakistan have still not implemented the LSRP (Link State Routing Protocol) & MPLS (Multiprotocol Label Switching) and dependent on the traditional ancient methods of IP routing i.e. static routing, NOC setting etc. It is really surprising to learn that ISP(s) have also not implemented MPLS [11] in their Network Environment as it is the suitable technology that provides reliable, secure and speedy network services with TE (Traffic Engineering) and QoS (Quality of Services) [12]. They just provide the dedicated line to their Enterprise Customers from NOC (Network Operation Center) to destination by using static IP configuration and setting etc. This practice is some sort of manual setting rather than dynamic routing.

With the knowledge of my numerous certifications and experience in Network Field specially, Enterprise/ ISP level. I have observed that costly, efficient and high specs equipment are unable to provide optimal performance and security, if the soft level approach i.e. selection of protocols, configuration is not up to the mark. Hardware with the high-end specifications are also dependent of the design, configuration and implementation of software level approach.

Keeping in view the circumstances mentioned and performance of any Network Environment, I was longing for this to have the solid concepts and knowledge of what I am designing, configuring and implementing in the Network Infrastructure. It was also my dire need to implement these tech and techniques in my network environment too.

1.2.Problem Statement and Objectives

- Instead of ancient / traditional static IP routing, Link State Routing Protocols are better for Enterprise Networks / ISP. LSP(s) has encouraged the large Network Infrastructures by provide ease of administration, automatic convergence.

- Transmission of data in Hybrid Network Environment IP to MPLS domain and MPLS to IP domain with the help of LSP i.e. OSPF and IS-IS.

- Data Transmission with Network Topology having Hybrid Environment but the Speed, Reliability, Security of Data would not disturb.

- Comparative analysis of Link State Protocols over MPLS domain via using GNS, WireShark, FileZilla Server/ Client.

- Designing, Configuration and Implementation of OSPF with Area-0 over MPLS Domain and obtain the results in shape of XXXXXXX for comparative analysis.

- Configuration and Implementation of OSPF with Area 0-1 within MPLS Domain over personalized network topology (via using above stated software tools) and obtain results for comparative analysis.

- Configuration and Implementation of IS-IS with L-1 in MPLS Domain over customized network topology (via using above stated software tools) obtain results for comparative analysis.

- Configuration and Implementation of IS-IS with L-s in MPLS Domain over customized network topology (via using above stated software tools) obtain results for comparative analysis.

- Conclude the result obtain from the experimental test beds that which LSP is better than other and suitable for Enterprise Network Environment/ ISP.

CHAPTER # 2

2. LITERATURE REVIEW

Current chapter of this thesis emphasis on some important, valuable and renowned concepts of protocols. This chapter will prove very helpful for better and comprehensive understanding of the subject thesis. Starting from the emergence of the simple protocol technology till its current advancement, all the required terms, concepts have been elaborated for the better know-how and thorough understanding of the reader(s). It is very valuable to added here that without having understanding of the aforementioned concepts and ideas, it would be really hard to proceed further smoothly.

2.1. What is Protocol in Computer Science

In information technology age and computing, the term protocol or communication protocol is a specific set of invisible computer rules that govern how data would be transmitted between two devices/ computers. These could also be referred as programmatic rules that works in the back-ground. Simply we can say that protocol is an agreed format for transmission of data/ information between two or more digital devices and computers. Thus, the protocol determines that what part of conversation comes at which time, type of error checking to be used, data compression method, how the sender equipment will specify that the message sending has been finished and how the receiver equipment will specify that it has received a message. Further, these set of rules are universal in nature and all the computers and digital devices all over the networks in the whole world have to follow them. There are many type and variety of the standard protocols from which programmers and software engineers can choose. Each Protocol has its own particular advantages and disadvantages i.e. few are very simpler than others, some are more reliable and fast than other. Protocol could be implemented either in hardware from or in software form. There are many categories of protocols i.e. Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secured (HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Transmission Control Protocol (TCP), Ripple Payment Protocol (XRP), Internet Message Access Protocol (IMAP), Post Office Protocol (POP), Transmission Control Protocol (TCP), Network Time Protocol (NTP) etc.

It would be in the fitness of the things, if a brief discussion session regarding the types of the protocols may elaborate. Internet Protocol (IP) is the protocols that is liable for logical

addressing called ‘IP Address’ for routing the data and information within the network or between different networks. Hypertext Transfer Protocol Secured (HTTP / HTTPS) is utilized for sending and receiving Hypertext Markup Language (HTML) files and documents over the internet/ cloud. Simple Mail Transfer Protocol (SMTP) is used for transformation of electronic mails (e-mails) between computer devices over a network or internet. File Transfer Protocol (FTP) is utilized for shown off the files to be copied between different electronic devices. Transmission Control Protocol (TCP) make sure the delivery of data and information packets across the networks. Ripple Payment Protocol (XRP) is utilized for sending money over the internet. Network Time Protocol (NTP) performs the clock synchronization in computers or different devices. Post Office Protocol 3 (POP3) is most popular and common account type for personal e-mail. Internet Message Access Protocol (IMAP) ensures the e-mail storage and retrieval etc.

In today’s network world, Transmission Control Protocol/ Internet Protocol (TCP/ IP) suite is the most common, peculiar and powerful protocols suite, which ensure the transmission (delivery/ receiving) of data and information at the right place, without having any errors and omissions, what computer(s) will be used for accessing different server machines on a specific network as well as on world wide web. In reality, these two protocols are different in nature and procedures but often linked together. This linking is based on the common functions to carry out some complete task. The term TCP/ IP is normally utilized to refer the whole suite of protocols that carries out the basic operations of the web. It also used in many local area networks (LAN).

When an information or data is sent on the internet/ cloud, often it is broken into small billets, (pieces/ packets). These billets make rapid / speedy transmission and different portion of a message could be sent by different routes and reassembled at the destination. Due to this there is a minimum chances of losing data / information during the transmission. Simply, TCP creates the packets, put them back together in systematic order at the last and check to ensure that no packets/ billets are lost during the transmission process. If any errors and omission has been happened during this transmission then TCP will make request to resent the packet/ billets again.

Internet Protocol (IP) is the most common, renounce and best of the existing times protocol that is used for routing of the information to a specific address. Each computing devices / equipment over the internet has its unique address known as IP address. Each packet contains

an IP address (destination address), source address, number of routers before arrival at its final destination etc. It is also noted that internet protocol (IP) does not create any physical connections between two devices/ equipment but relies on TCP for the said operation. Internet Protocol (IP) is also utilized in conjunction with other protocols that create connections.

Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF) are the sub-domains of Internet Society which is the custodian and the competent authority who is responsible for maintaining and up-gradation of the TCP/ IP model and other similar protocols. Internet Society also support and co-operates closely with the other standards organizations and bodies such as World Wide Web Consortium (W3C) and International Standard Organization (ISO) / International Engineering Consortium (IEC).

2.2.Routing and IP Routing

Technically the term Routing refers the process of sending/ receiving data packets from one source to specific destination. In internetworking, routing is normally performed by a dedicated equipment/ device called a Router. It is the first and foremost operation of any network and the internet as it creates the messages to pass through from one specific computer device to another computer as well as reach the specific targeted computer machine. Furthermore, we can say that routing is the simple process to forwarding/ travelling the data packets (free of errors and faults) from one computer machine (source) to another computer machine (destination). To gain the effective results of data transmission, routing is done on some specific components i.e. network topology, setup of networking hardware, standard protocols and algorithms.

It is further elaborated that usually routing is performed by a specific / dedicated equipment called ‘Router’. Data packets are the more core and fundamental billets of information that transport in all the modern computer networks infrastructure. Each router in the network topology performs its own part and forward the data packets/ information to its next router, called ‘Hop’. It is not out of place to mention here that routing can also be performed by circuit switched networks, where a specific dedicated circuit is made for the duration of the transmission of each message. The best example of circuit switched network is the Public Switched Telephone Network (PSTN), which is also a worldwide collection of interconnected public telephone networks.

The term IP Routing is root stretch for the specific set of protocols that are used to determine the simple and shortest path for the transmission of information/ data from one source to another destination. Usually the information/ data is transmitted via series of routing devices as well as across multiple networks. Thus IP routing protocols enable routing devices to build up a forwarding table that correlates final destination with next hop addresses.

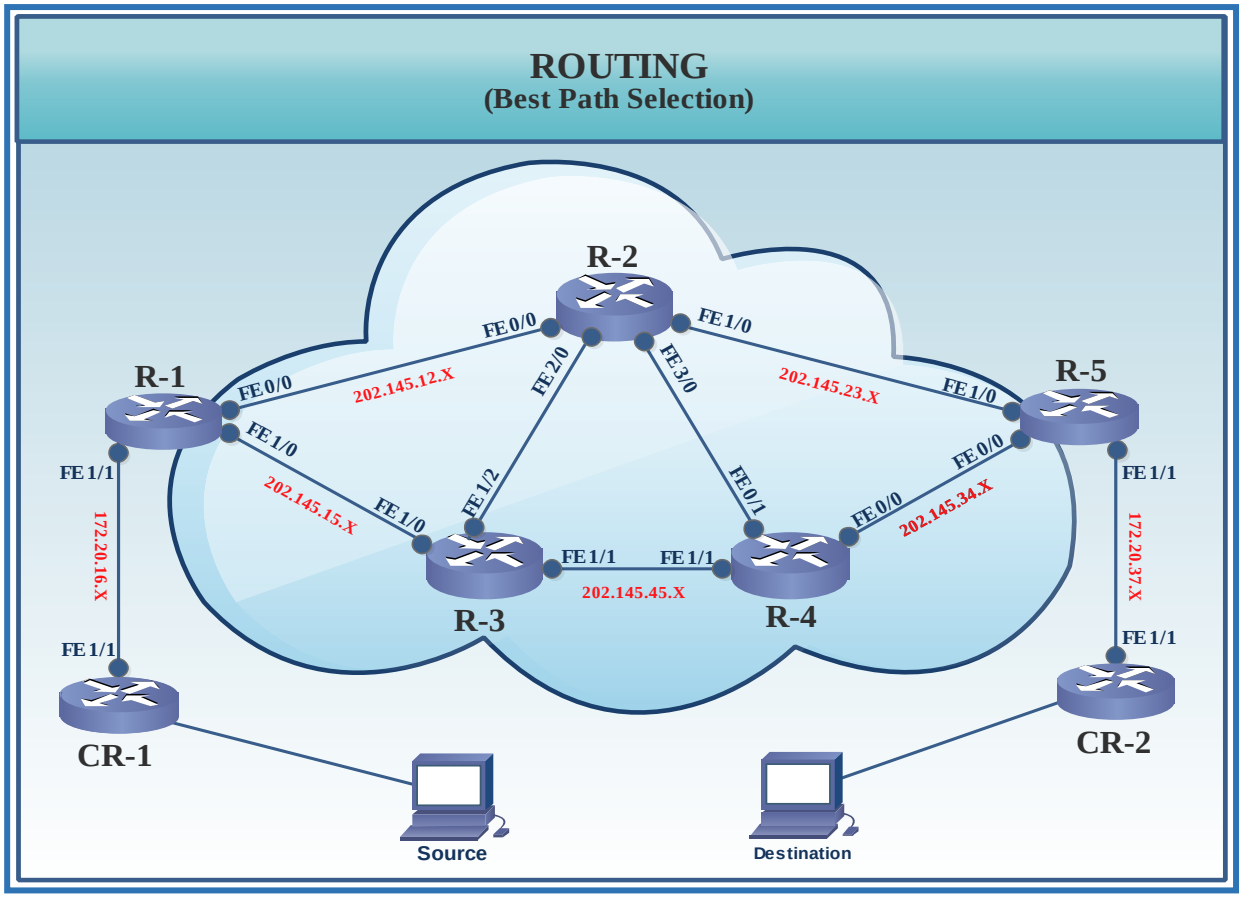


Figure 2. 1: Routing – Selection of Best Path

Technically speaking, an IP routing could also be defined as the process of transmission of data from point A (source) to another point, called B (destination) on a specific determine the route across one or more network. IP routing also perform one or more network devices on TCP/IP networks to connect with one another. In other words, IP routing specify the path for reaching the destination device.

2.3. What are Routing Protocols

Routing Protocols are the specific type of protocols that defines how routing equipment as well as layer III devices communicate with one another, disseminating or spreading information (usually called routing table) selection of the specific routes, shortest path, between the network infrastructure / topology. It is worth mentioning here that another major concepts regarding the classification of the routing protocols can be divided into many features. Here in this chapter, a brief glimpse on IP routing protocols will be provided. Routing protocols can be mainly classified into different groups according to their characteristics. It can be classified into different features due to the behavior purpose and operations of the routing protocols.

As far as the behavior of the routing protocols is concerned, there are its two types. Classless and Class-full Routing. Keeping in view the purpose of the routing protocols, it can be mainly classified into two categories, one is called IGP (Interior Gateway Protocol) or EGP (Exterior Gateway Protocols). As the operations of the routing protocols are concerned, distance vector protocols, link-state protocols and path vector protocols came into an account. This above mentioned paragraph can be summarized in the diagram placed on the very next page at Figure 2.2.

2.4.Dynamic Routing Protocols – Categories

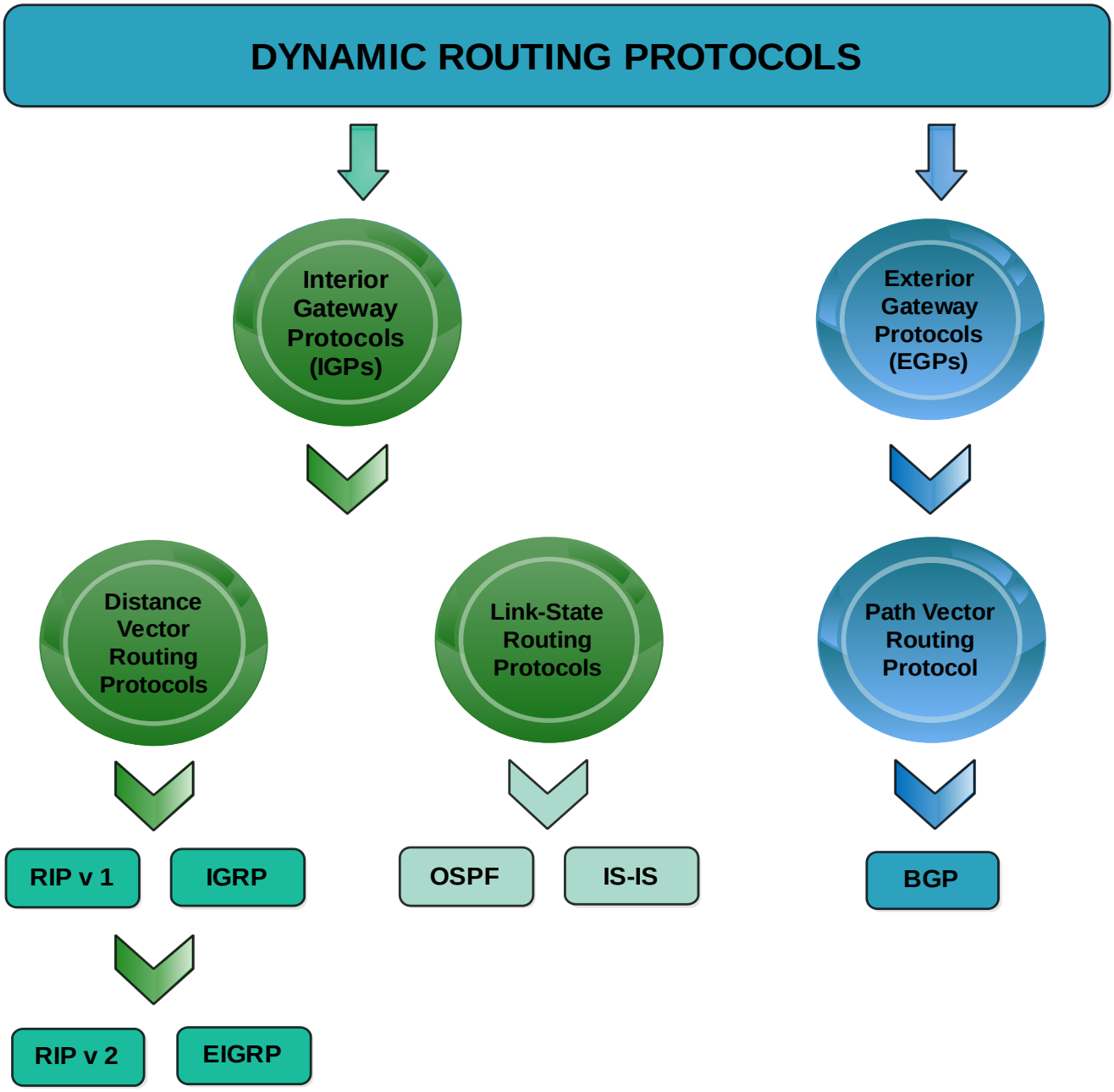


Figure 2. 2: Classification of Dynamic Routing Protocols

Keeping in view the earlier stated diagram, a minute overview on the routing protocols is elaborated here. RIPv1 is distance vector in nature, Classful proprietary by Cisco, covers under Interior Gateway Protocol. Its enhanced version is RIPv2 which is classless protocol. IGRP is another proprietary of Cisco Inc. is distance vector, Classful protocol that covers under the domain of Interior Gateway Protocol. Its advanced version is called EIGRP which is classless and developed by Cisco Inc. OSPF [1] and IS-IS are link-state in nature, classless protocols comes under the repository of IGPs. Border Gateway Protocol is Exterior Gateway Protocol in nature, classless and specifically path vector.

In classless routing the protocols disseminate the subnet mask with their updates. Thus, the Variable Length Subnet Masks (VLSMs) is also used in case of classless routing. The prominent examples of the classless routing protocols are RIPv2 (Routing Information Protocol version 2), EIGRP (Enhanced Interior Gateway Routing Protocol) [5], OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System).

Classful routing protocols are RIPv1 (Routing Information Protocol Version 1) and IGRP (Interior Gateway Routing Protocol). Classful networks are the networks where the addressing design or architecture used in the internet.

2.5.Structure of Different Protocols

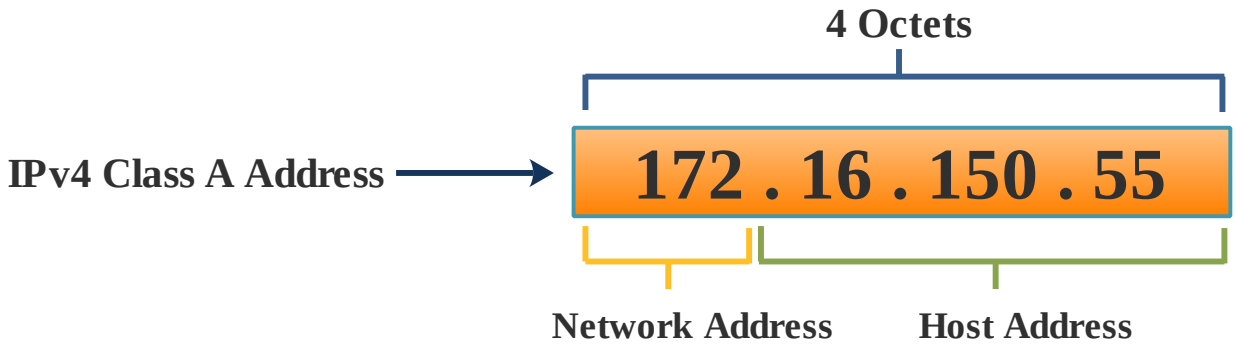


Figure 2. 3: Structure of IPv4 Address

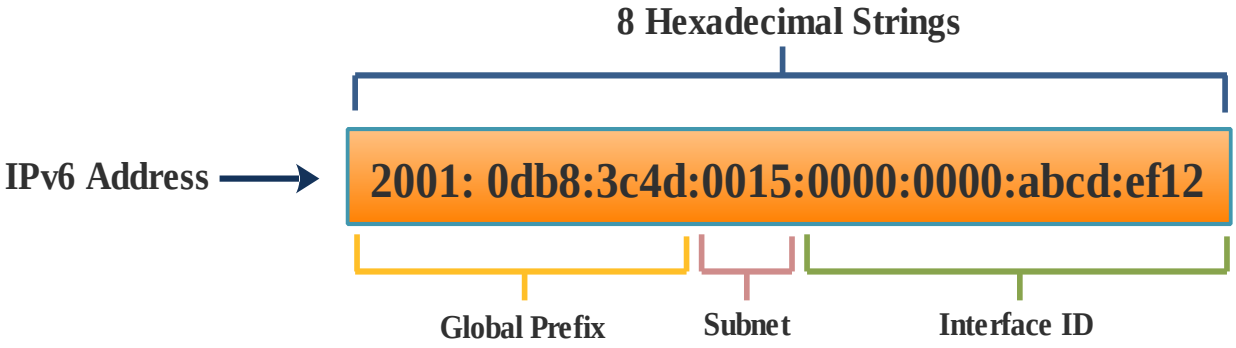


Figure 2. 4: Structure of IPv6 Address

Figure 2.4 contains the information regarding IPv6 Protocol Header. IPv6 (Internet Protocol Version 6) is latest protocol tech which has been designed to be the new generation of the IP Protocol, followed by IPv4 [18]. Surprisingly, the missing number 5 (IPv5), has already been assigned to another internet protocol, the Internet Stream Protocol version II, defined in RFC 1190 but unfortunately it could not be popularized much. Another reason of its unpopularity is the non-utilization / less access to the general public.

IPv6 has its broader view than IPv4, having bigger scope as well as flexibility that is direly required for the bigger network (internet) due to the day-to-day growing surfers/ users. As the internet has become a bigger source of global connectivity, nobody can say for sure that how large the internet will grow. Due to the 32 bits address space limits of IPv4 against the number of growing internet users, the authorities worked on IPv6 that can maintain enough address space limit up-to several upcoming years or couple of decades.

IPv6 address is much big as there are enough addresses space for large number of increasing hosts globally. The address space size has been increased to 128 bits. Majorly, IPv6 contains 8 hexadecimal strings, 03 strings are for Global Prefix, 01 is for subnet(s), 04 are for interface ID. Now ISPs can assign a huge ranges of space addresses to its clients. IPv6 is much flexible, scalable, secure and easy to configure as it can also work through DHCP (Dynamic Host Configuration Protocol). Furthermore, it is very easy to migrate from IPv4 to IPv6 [17].

IPv6 is now an approved specification standard. RFC(s) have specified enough for IPv6 i.e. 2373 (IP version 6 Architecture and Global Unicast Address Froamt), 2460 to 2463 defines the IPv6 Specification, Neighbour Discovery, Stateless Address Auto configurable, ICMPv6 (Internet Control Message Protocol) specification etc. RFC(s) for DNS Extension Support, Path MTU Discovery, BGP-4 Multiprotocol Extension for Inter Domain Routing, Transmission over IPv4 Domains, RIP Ping for IPv6, Unicast Address Allocation, Packet Tunneling, Reserved IPv6 Subnet Any-cast, MLD (Multicast Listener Discovery), OSFP for IPv6 have been also approved and standardized.

2.6. Difference between IPv4 and IPv6

Point of Differences	IPv4	IPv6
Address Format/ Length	32 Bits	64 Bits
Address Type	Unicast, Multicast, Broadcast	Unicast, Multicast, Anycast
Address Representation	4 Decimal Numbers from 0 to 255 Separated by Periods Notation.	8 Groups of 4 Hexadecimal Digits Separated by Colon Signs.
Configuration	Manual or DHCP	Auto Configuration of Addresses Available
Packet Header	20 Bytes	40 Bytes Long
IPSec Support	Optional	Built-in

Table 2. 1: Difference between IPv4 & IPv6

A detailed overview regarding the difference between both of the protocols i.e. IPv4 and IPv6 has been expressed at Table 2.1. It is pertinent to mention here that IPv6 also having more vendor support than IPv4. RIPv6 [17], Traffic Filtering, BGP-4 for IPv6, Automatic and Static Tunnels, Dual Stack Support for Telnet, Neighbor Discovery, EUI-64 Addressing, IPv6 Over Ethernet, FDDI, Cisco HDLC and ATM PVCs, DNS and TFTP, ICMPv6 and Ping, Traceroute and Debug Commands etc.

2.7.Difference between IGP and EGP

Interior Gateway Protocols (IGP) are the protocols that are utilized for routing within an AS (Autonomous System). An Autonomous System is called a collection of routing devices under common/ same administrative control or domain such as an ISP (Internet Services Provider), firm, company, organization, institute etc. Autonomous System is also known as a routing domain/ single administrative control. Interior Gateway Protocols are also known as Intra-Autonomous System routing. Various network/ internet services providers use IGPs in their network infrastructure. RIP (Version 1 and 2), EIGRP, OSPF and IS-IS are the Interior Gateway Protocols.

Exterior Gateway Protocol are normally used for the routing within two or more different Autonomous Systems. It is also known as Inter-Autonomous System Routing. Large group of companies, services providers normally used EGP (Exterior Gateway Protocol) for interconnectivity. BGP (Border Gateway Protocol) is one and only available EGP nowadays for official routing over the internet.

2.8. Difference between Distance Vector and Link-State Protocols

A glimpse regarding the difference between Distance Vector and Link State Protocols may please be perused below. Keeping view of only the major differences with regards to protocols' types, operations, features, components etc. within the DV and LS protocols, the following Table 2.2 has been created.

Point of Differences	Distance Vector Protocols	Link State Protocols
Convergence	Slow Convergence	Fast Convergence
Routing Information	Sends Complete Routing Table	Sends Only LS (Link-State) Information/ Periodic Updates
Broadcast/ Multicast	Sometimes Updates Sent Using Broadcast	Always Uses Multicast for Routing Updates.
Bandwidth Utilization	Consumes a Lot of BW (Bandwidth)	Consumes Less (BW) Bandwidth
Configuration/ Administration	Configuration and Administration is Simple	Configuration and Administration is Quite Harder than DV
Routing Loops	More Chances/ Susceptible to Routing Loops	Less Chances/ Susceptible to Routing Loops
Network Topology	Unaware of Network Topology / Infrastructure	Aware/ Knows the Entire Network Topology/ Infrastructure
Path Access	Copies Routing Table to its Neighbors	Uses Shortest Path

Table 2. 2: Difference between Distance Vector and Link State

2.9.Distance Vector

For a clear understanding of Distance Vector Protocol, two terms are very much important to understand, one is ‘Distance’ and other one is ‘Vector’. In any network infrastructure, the Distance Vector protocols identify the distance from source node to destination node. The whole mechanism is based on the measuring rod called ‘metric’. The metric is such as hop count, bandwidth, cost, delay etc. As far as the vector is concerned, is specify the direction of the next-hop/ device i.e. router or exit interface to reach to the destination node.

Using distance vector protocol, any routing device has no detail or information (including entire path detail) about the exact path to the destination. Routing devices/ equipment are used as a sign posts/ milestones to reach its destination address. The only information or detail that a routing device knows the metric or an interface name to get to the destination. Distance Vector routing protocols having no specific idea or actual map of the network topology.

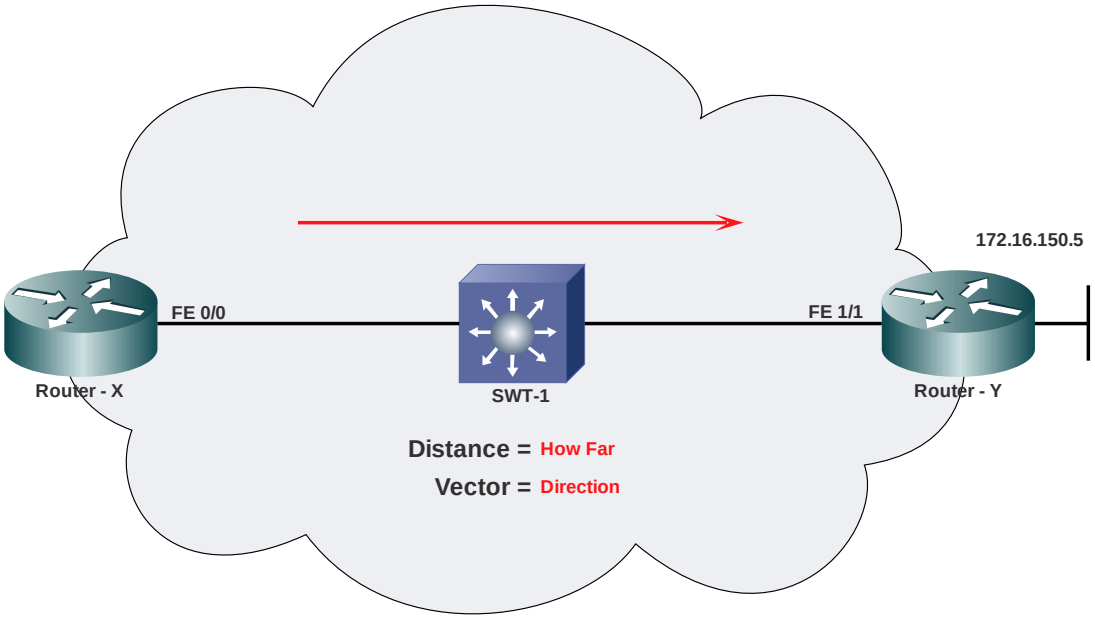


Figure 2. 5: How Does Distance Vector Protocol Work

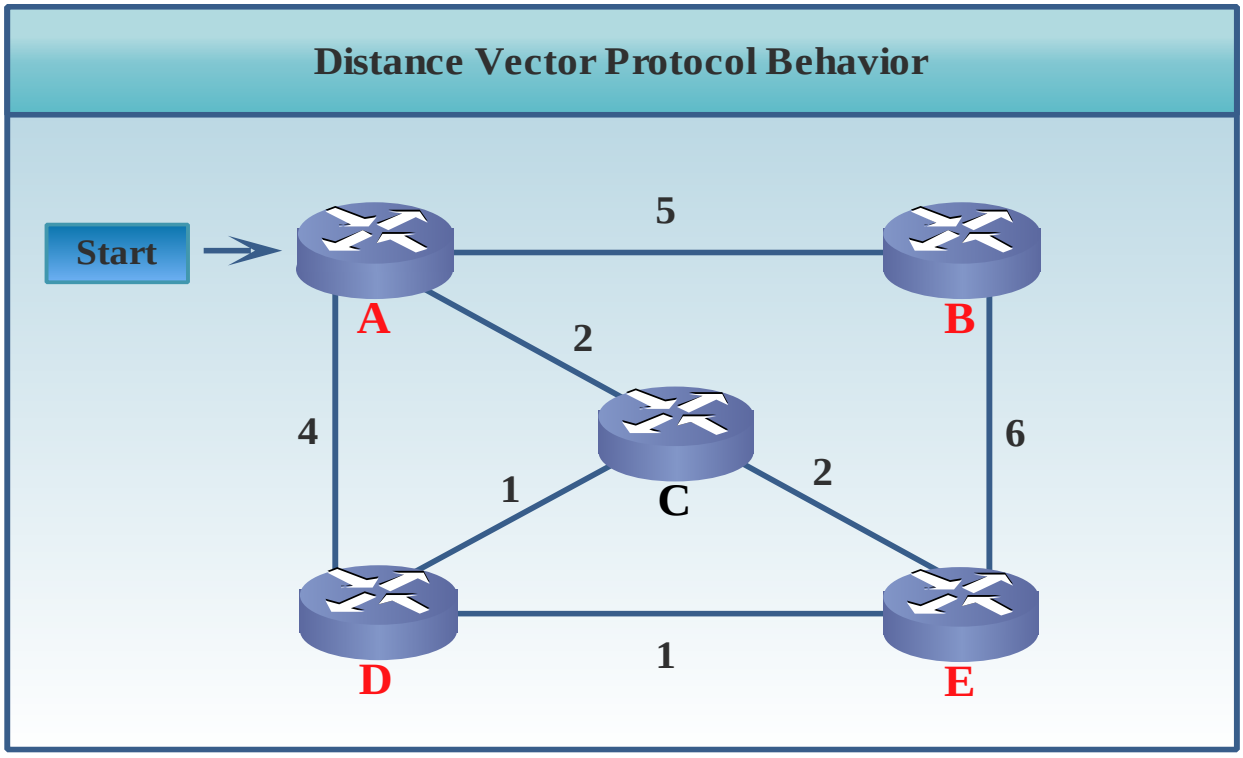


Figure 2. 6: Behavior of Distance Vector Protocol

x_o

Router	Cost	Predecessor	Status
A	0	0	P
B	X	0	T
C	X	0	T
D	X	0	T
E	X	0	T

x_1

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	4	A	T
E	X	0	T

x_2

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	1	C	P
E	2	C	T

x_3

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	1	C	P
E	1	D	P

x_4

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	P
C	2	A	P
D	1	C	P
E	1	D	P

Table 2. 3: Behavioral Transition of Distance Vector Protocol

2.10. Link State Protocol

The devices enabled with the LSRP (Link State Routing Protocol) have the full information or clear road maps of the network. Every router in the topology with LRSP contain the information about its neighbors, directly connected links and the state of those who are linked with each other. The said information within the topology is sent to all the routing devices through a multicast message. LSR always maintain the complete network topology by updating itself incrementally when a change is occurred in the network. Every routing devices within the network topology keep as copy of the said information without making any change. After gather the full and complete picture of the network topology, every routing device calculates independently its own best path(s) to reach to the desired destination within the network.

It is further added here that the LSP (Lint State Protocol) have the base of SPF (Shortest Path First) algorithm to find the best path to reach to the destination. This algorithm is also popular as “Dijkstra”, since it was conceptualized by Dijkstra. In this algorithm, whenever a changes is occurred on a link of the routing device, a routing update called a LSA (Link State Advertisement) is exchanged between the routing devices. Whenever a routing device receives LSA routing update, the Link State Algorithm recalculate the shortest path to affected destinations. Every routing device again constructs a map of the complete network topology. The famous types of Link State Protocols are OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System).

In short, the LSA (Link State Advertisement) a packet contains routing information of the network topology is sent to all the routing devices within the network. The topological database is collected from LSA. The SPF (Shortest Path First – Dijkstra Algorithm) perform the calculation on the database resulting in the SPF Tree. Here in Link State Protocol, a list of the known paths and interfaces are stored in the Routing Tables.

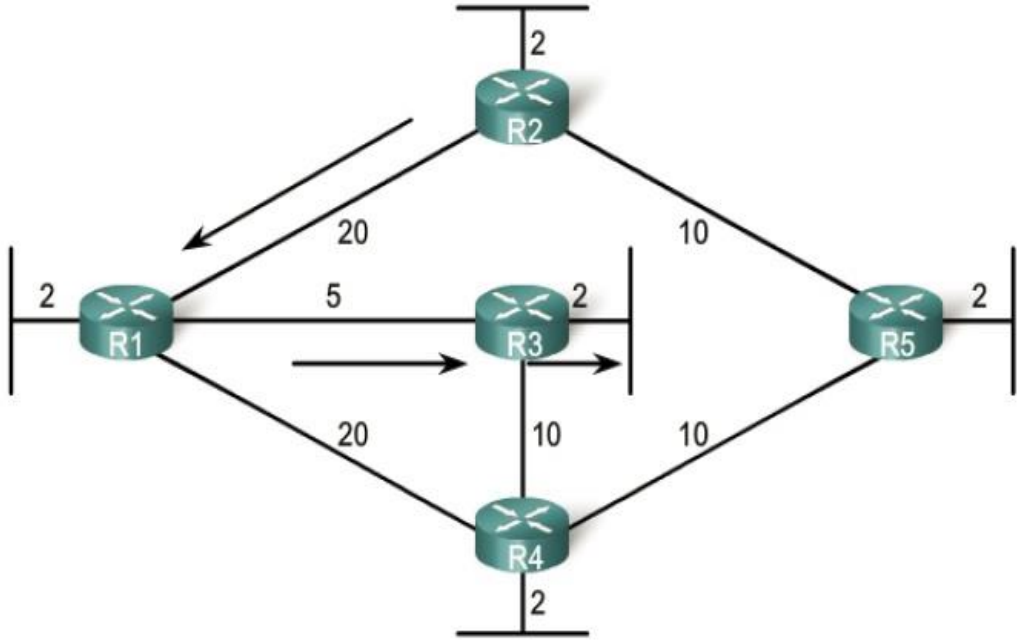


Figure 2. 7: Dijkstra Algorithm Behavior

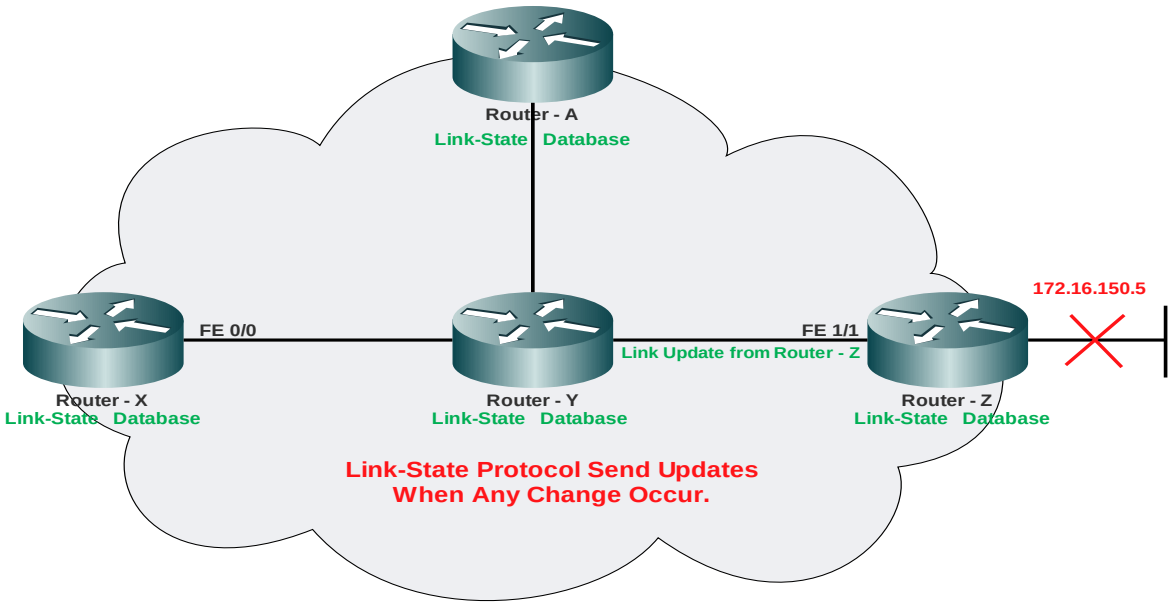


Figure 2. 8: How Does Link State Protocol Work

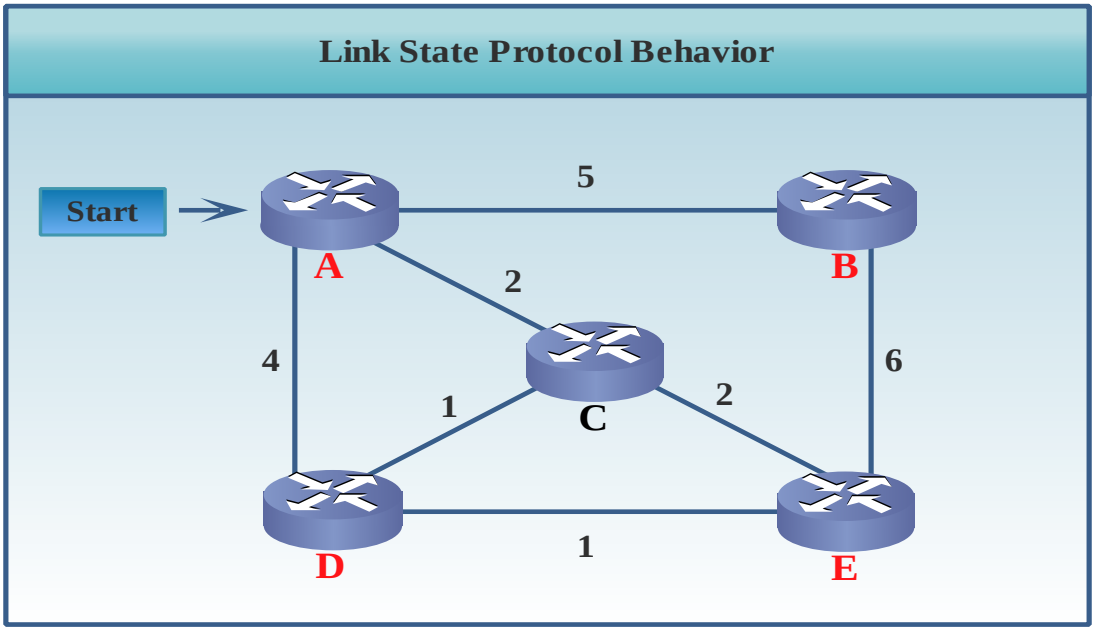


Figure 2. 9: Behavior of Link State Routing Protocol

x_o

Router	Cost	Predecessor	Status
A	0	0	P
B	X	0	T
C	X	0	T
D	X	0	T
E	X	0	T

x_1

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	4	A	T
E	X	0	T

x_2

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	3	C	P
E	4	C	T

x_3

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	T
C	2	A	P
D	3	C	P
E	4	C	P

x_4

Router	Cost	Predecessor	Status
A	0	0	P
B	5	A	P
C	2	A	P
D	3	C	P
E	4	C	P

Table 2. 4: Behavioral Transition of Link State Protocol

2.11. Analysis of OSPF Links-State Update

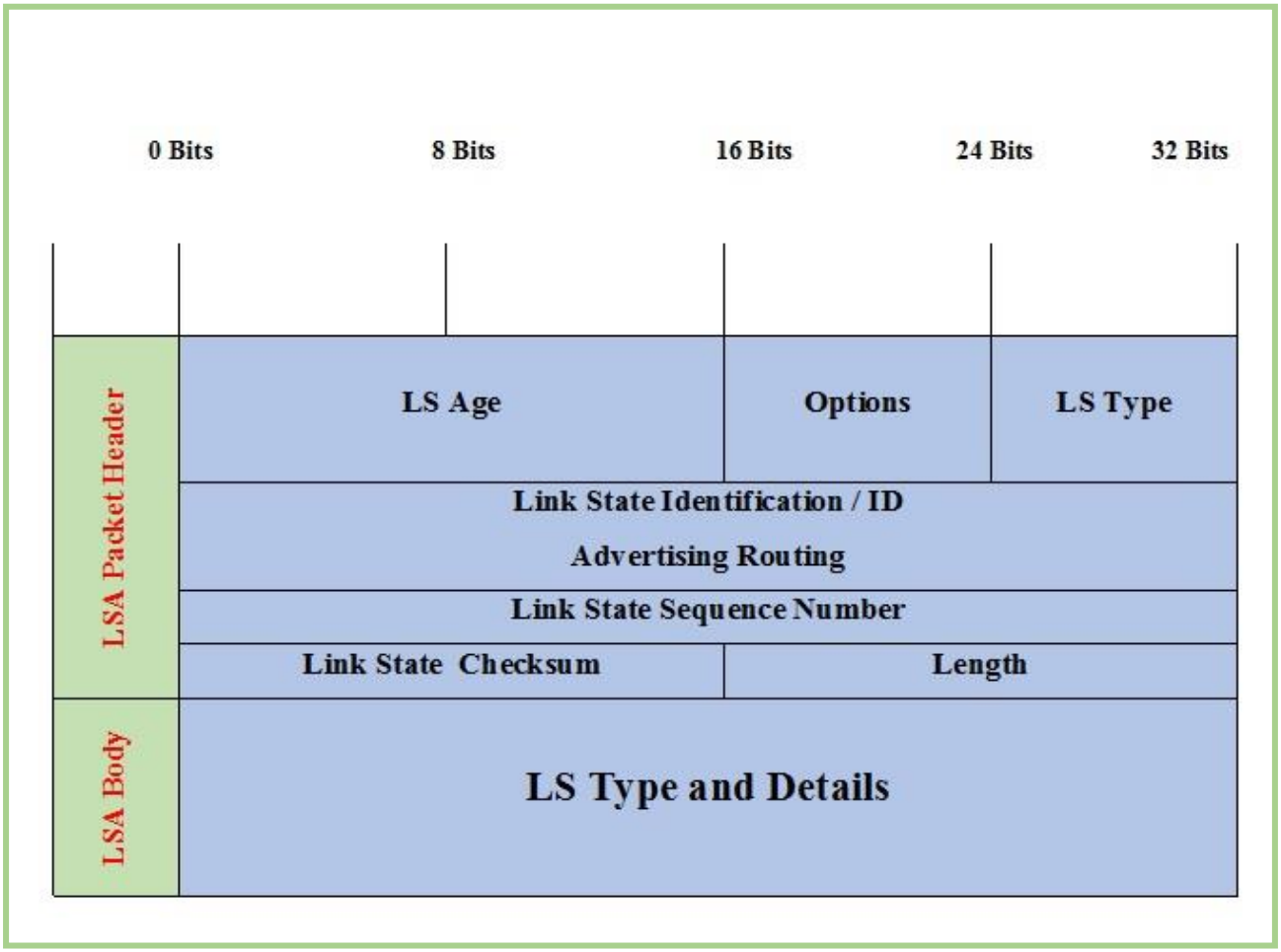


Figure 2. 10: LSA Body and Packet Header Detail

Figure 2.10 contains the thorough pictorial analysis of LSA (Link State Advertisement). LSA have 32 bits Packet Header, first 16 bits contain LS age, 08 bits are reserved for Options and further 8 bits utilized at LS Type. Second layer/ portion of the header contain LS Identification that is advertised to other Routing Device. Third part have the Link State Sequence Number. Fourth portion of the LSA Packet Header (16 bits) are reserved for Link State Checksum and Further 16 bits are earmarked for the Length.

2.12. OSPF Area 0 (Backbone)

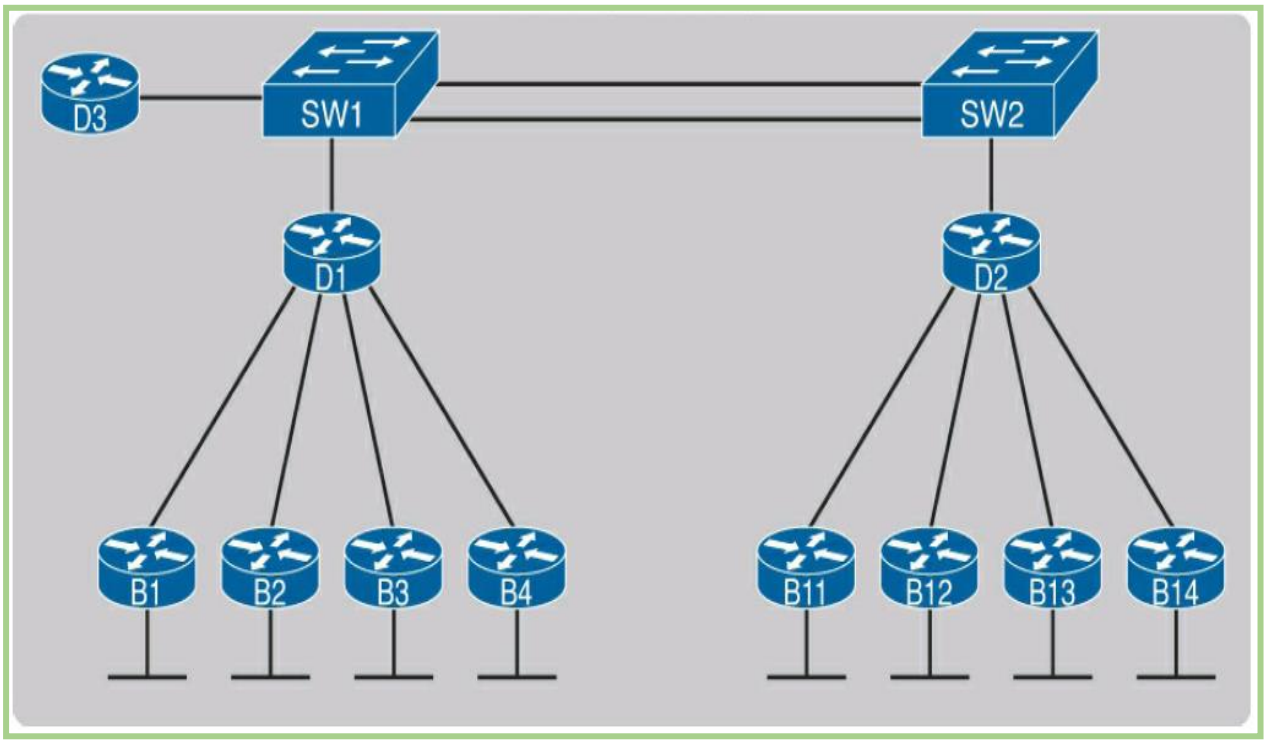


Figure 2. 11: Single Area OSPF

Before proceeding further in the topic, it is really necessary to have the thorough concept of Area, especially Single Area of OSPF (Open Shortest Path First). It has been delineated in the Figure XX, OSPF version 2 suffer in large networks with single area design implementation. CPU time to execute the SPF algorithm on all the devices within the topology data takes mush time. Consequently, the convergence time (the time required to react to make changes in the network topology) in OSPF [1] version 2 could be slow. The devices within the topology may run low on memory as well. Another few more discrepancies in the larger topology is the requirement of more memory on each routing device. Changing in the status of even a single interface of the routing device in the whole network topology can slower the performance.

2.13. OSPF with Different Areas

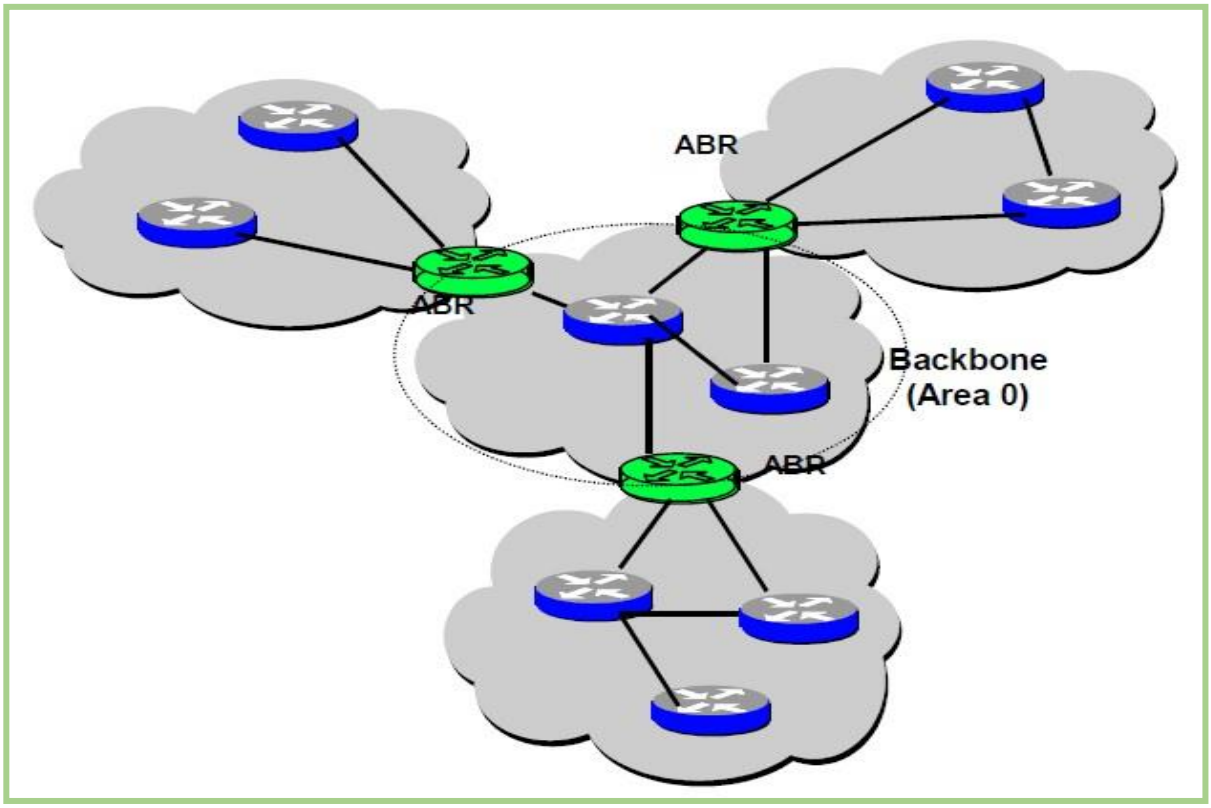


Figure 2. 12: OSPF with Different Areas

Figure 2.12, express the logical connectivity of different areas is OSPF (Open Shortest Path First). As per the logics of OSPF, it is direly necessary that all the configured areas in OSPF must be connected with Area-0. The Routing Devices that connected different areas in OSPF are called ABR (Area Border Router) which have been shown in Light Green color in above positioned Figure XX whereas all other router existed within their respective Areas are delineated in Blue color.

2.14. Similarities and Dis-Similarities of LSP

OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) are also some points of differences which may be elaborated and perused in the following Table 2.5.

Similarities/ Dissimilarities	OSPF	IS-IS
Routing Device Convention	Router/ Host	End System (ES)
	Designated Router	Designated IS
	Back-up Designated Router	N/A
	Area Border Router (ABR)	L1/ L2 Router
Link Detail Algorithm	Link Dijkstra SPF	Circuit Dijkstra SPF
Advertisement Known	Link State Advertisement (LSA)	Link State PDU (LSP)
Packet Called	Hello Packet	Hello IS/ IIH PDU
Boundary Information	Area	Sub Domain
	Non-Backbone Area Backbone Area	Level 1 Area Level 2 Sub Domain
DB Description	Database Description (DBD)	Complete Sequence Number PDU (CSNP)
Tramsport	Uses IP 89 as Transport	Encapsulated in Layer 2
Support	CIDR, VLSM	CIDR, VLSM

Table 2. 5: Similarities & Dis-Similarities of LSP

Although, both are containing with some points of difference but these are also equipped with some most common features as well. As both fall in the category of Interior Gateway Protocol (IGP) that distribute internal reachability details between the routing devices belonging to the same / single AS (Autonomous System). Both of the protocols also support IPv4, IPv6 [17], Authentication Processes, CIDR (Classless Inter Domain Routing), Multi-Path Access, Un-Numbered Links, VLSM (Variable Subnet Length Masking) etc.

2.15. IS-IS (Intermediate System to Intermediate System)

Another type of link state routing protocol is ISIS (*Intermediate System to Intermediate System*), is a not a new routing protocol, it is the chronicle one. Here the term 'Intermediate System' notify a Router, therefore, it is also called "Router to Router Protocol".

"Intermediate System to Intermediate System (IS-IS) routing protocol was developed / designed to transport (transmit/ receive) information in an efficient way within a network infrastructure. It accomplish the said task by determine the best path selection for datagrams via a packet switched network.

Before going further, it little history should be in mind for sure, in early 1980's, it was the age of CLNS (*Connection Less Network Services*) and CLNP (*Connection Less Network Protocol*). IS-IS (*Intermediate System to Intermediate System*) was developed by DecNet (*Digital Equipment Corporation Network*) for routing of CLNS and CLNP. Implementation of IP routing [16] was also spreading side-by-side. So keeping in view the dire need of exited technology ISO (International Standard Organization) redefined IS-IS, called Dual / Integrated IS-IS. Exiting IS-IS is fully equipped with the support to CLNS, CLNP and IP as well. Moreover, It is not the proprietary in nature as IGRP & EIGRP are. It is fully supported by all the vendors of the world who are dealing in network related equipment. It is predominantly used in ISP (*Internet Service Providers*) nowadays.

IS-IS is IGP (*Interior Gateway Protocol*) as OSPF (*Open Shortest Path First*) that disseminated routing information between two routing devices belonging to the same AS (*Autonomous System*). Furthermore, it also covers under CIDR (*Classless Inter-Domain Routing*), VLSM (*Variable Subnet Length Masking*), Authentication, Support Multi-path and IP Unnumbered Links etc. As far as its format is concerned, it is directly encapsulated in the layer II.

Figure 2. 13: IS-IS Header

IS-IS is less widely implemented and used on the Routing platforms. Main IS-IS implementations are more tunable than equivalent to OSPF [1] Implementations.

2.16. Comparison of OSPF and IS-IS

IS – IS & OSPF COMPARISON		
	IS-IS	**OSPF**
Interior / Exterior	Interior	Interior
Type	Link – State	Link – State
Default Metric	Cost	Cost
Administrative Distance	115	110
Hop Count Limit	None	None
Convergence	Fast	Fast
Update Timers	Only When Changes Occurs	Only When Changes Occurs (*LSA Table Refreshed Every 30 Minutes*)
Updates	Only Changes	Only Changes
Classless	Yes	Yes
Supports VLSM	Yes	Yes
Algorithm	Dijkstra	Dijkstra
Update Address	-	224.0.0.5 (All SPF Routers) 224.0.0.6 (DRs and BDRs)
Protocol and Port	-	IP Protocol 89

Table 2. 6: Comparison of OSPF & IS-IS

As far as the theoretical configuration of integrated/ dual IS-IS is concerned, there are very few step that are taken systematically. Firstly, we define different areas as per requirement, prepare an address plan for the routing device (include it NETs), then determine the interface on which IS-IS will run. Second step is to enable the IS-IS as an IP routing protocol on the routing devices and assign the tags to different processes (in case of requirement). We configure NETs on the routing devices afterwards. Lastly, on the proper / concerned interfaces of the router (routing device), we enable integrated IS-IS.

In case of the physical configuration on the routing device (router), we just have to configure integrated IS-IS within three commands. Moreover, the optional tag (s) could be used for identifying different / multi IS-IS processes by giving a meaningful name for a routing process. If it is not specified, a null tag (0) is assumed and the process is references with a null tag. The said name should be unique amount all the IP routing devices processes for a given router.

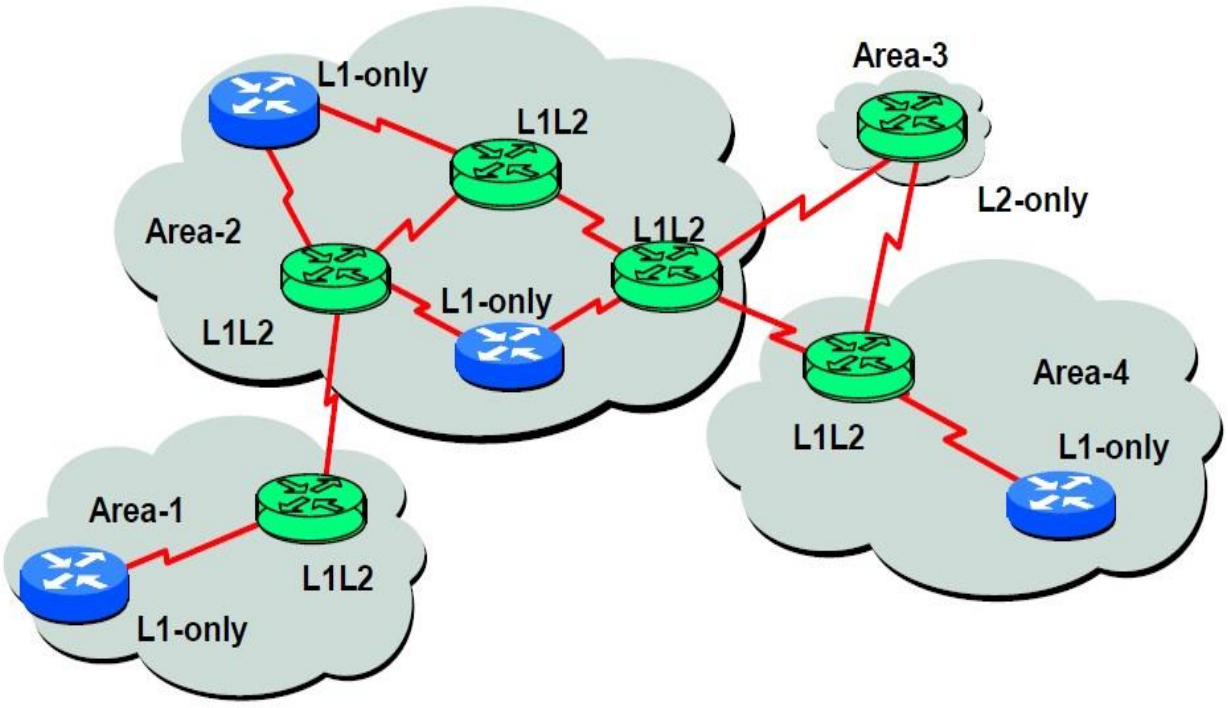


Figure 2. 14: IS-IS in Different Levels

2.17. MPLS Header

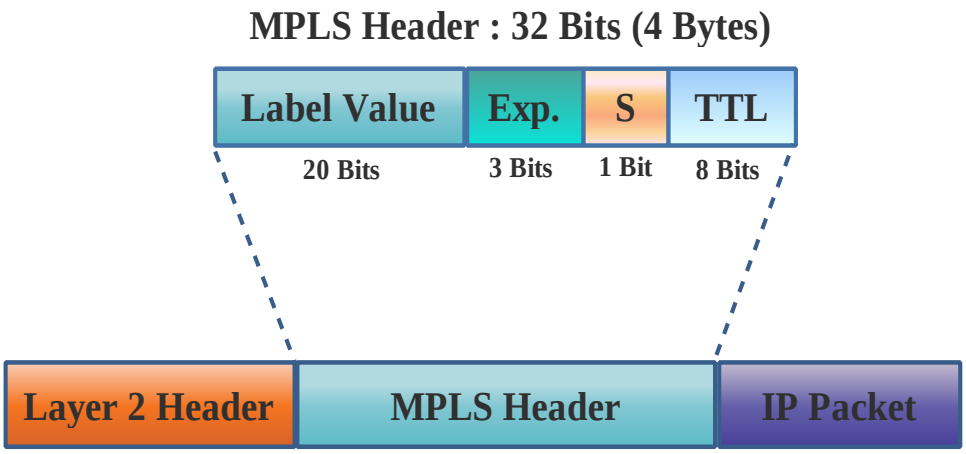


Figure 2. 15: MPLS Header

Figure 2.15 showing mainly contains on two different parts. First portion of the diagrams shows its header detail whereas second part of the figure represents the placement of MPLS Header in layer model. Initially the header of MPLS would be discussed in detail then placement in ISO Layer model.

MPLS header contains 32 bits (4 bytes) as shown in above figure. First 20 bits are called "Label Value". Actually these value represents the total number of labels that can assign or utilized for an IP packet that comes under the domain of MPLS [15]. It also identify the part of LSP (Label Switched Path). Further 03 bits are called experimental bits. These 03 bits are also known as CoS (Class of Service) field, used for QoS marking and no longer used for experimental purposes. Third portion of the MPLS header comprises on 01 bit which is called as 'Stack' field that supports the hierarchical label stack. Clearly it means that Flag, which when set to 1. The last part of MPLS header having 08 bits of TTL (Time to Live) that provides the usual or conventional IP TTL functionality.

Second part of the above mentioned figure represents the placement of MPLS header in OSI Layer Model. MPLS basically called layer 2.5 technology because it comes within the center of layer 2 (Data Link Layer) and layer 3 (Network Layer). Frankly, we may say that MPLS works with the features / functionality of Layer 3 & Layer 2 which are ATM, Frame Relay, PPP, Ethernet (Layer-2) and IPv4, IPv6, IPX, Apple Talk (Layer-3).

Equipped with the technology of layer 2.5 (MPLS) we are capable enough to gain the advantages of Simplified Improved Forwarding of Packets, Efficient Explicit Routing with QoS (Quality of Services) , Mapping from IP packet to FEC (Forwarding Equivalence Class), Traffic Engineering & Shaping, Common Operation Over Packet & Cell Media, Partitioning of Functionality, Integration of IP and ATM in the same Network, Building of Interoperable Networks, Scalability of Network etc.

MPLS [15] supports the single as well as converged network infrastructure for both new and legacy services. QoS (Quality of Services) are guaranteed to be delivered in the presence of MPLS technology. It reduces the router's processing to a large extent since the router simply forward the packets that are based on fixed labels. Very best of its approach is to provide the better scaled VPNs rather than customer based VPNs. Last but not least it also provide the best and appropriate level of security which is necessarily required for any network infrastructure domain. One more of its best advantage is the provision of secured, scalable, flexible and automate VPN tunnels. With the presence of MPLS, it is certainly possible to have the forwarding of data through the desired path. The priority to send/ receive the data can be prioritize from lower to high and wise versa. Different sort of Traffic Engineering could be done for sensitive voice, video packets over a high priority/ lesser utilized/ shorter path. As the MPLS [15] is a connected oriented network unlike connection less network like IP, therefore, it is much more reliable.

Dynamic bandwidth allocation is another of its advantage as it can be utilized to provide the bandwidth as per demand of the user/ client. Furthermore, Data Rate Limiting and other bandwidth management parameters can also be setting-up on the demand or desire of the client/ user. These bandwidth management parameters allow a certain bandwidth to be dedicate for the mission critical applications as well.

2.18. MPLS Label Operations

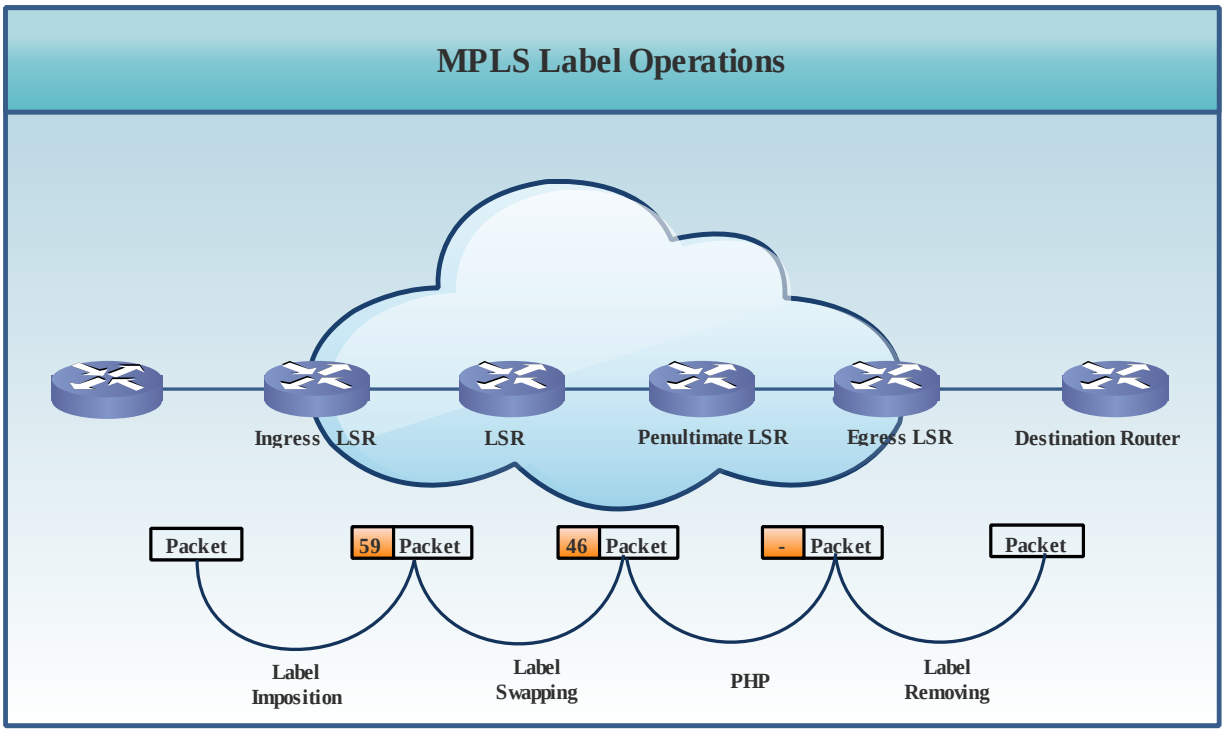


Figure 2. 16: MPLS Label Operations

Above is the diagram or network topology at Figure 2.16 that represents the different label operations in MPLS Domain. As the ingress LSR (*First Router of the MPLS Domain*) receive the IP packet in MPLS domain [11], it embosses the label on the packet received from an IP domain. Here in this example the packet label has been stamped i.e. 59. On another LSR (Second Router of the MPLS Domain) in the same MPLS domain the label is swapped with the new label i.e. 46. Label swapping process continuous till second last router of MPLS domain [12]. The second last router of MPLS domain is called Penultimate LSR that stamped Null to the label and sent it to Egress LSR [15] which is the last router of MPLS domain. Egress LSR removes the label from the packet and forward the same in IP domain. More elaboration of the label's operations has been made in shaped of Table 2.7 below.

MPLS LABEL OPERATIONS		
SR. #.	**OPERATIONS**	**DETAIL**
1.	**PUSH**	Insertion/ assigning process of a label to an IP packet is known as "Push". Further, the process of add a level to an incoming IP packet that is received on an ingress Router is called the "Push Operation. Label imposition is also refer this concept.
2.	**Swap**	In MPLS Domain, the swapping of different labels is called "Swap Operation". As a LSR receive a label, LFIB examine the same and a assign a new label keeping in view the destination.
3.	**POP**	Removing of the label from an outgoing packet is called the "POP Operation". As the implicit Null is received from LSR then the last/ previous label will be removed and IP packet will only be forward further. This process is also know a label disposition.

Table 2. 7: MPLS Label Operations

2.19. MPLS Architecture

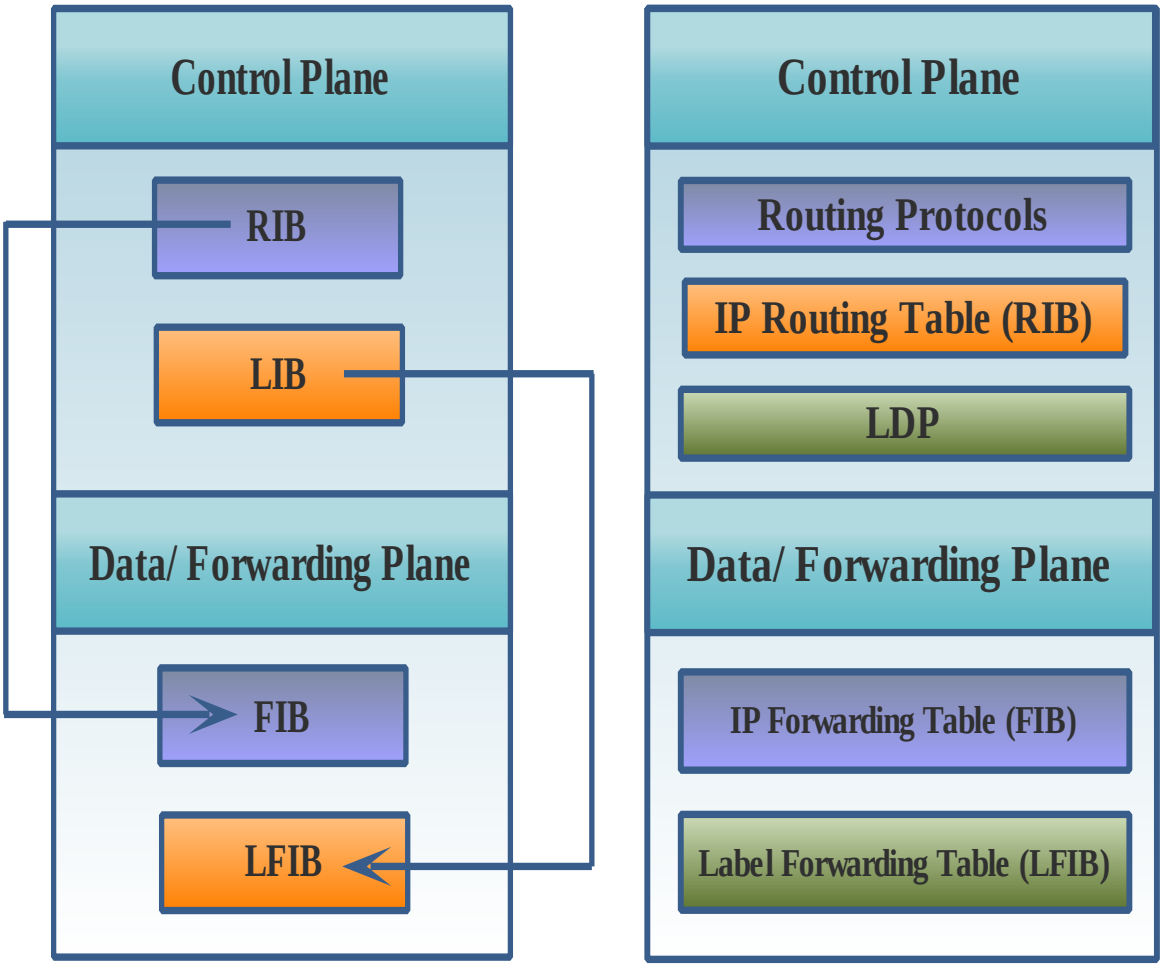


Figure 2. 17: MPLS Control Plane

2.19.1. Control Plane

Software based part of the MPLS [11] architecture is called Control Plane. Further, it contains two more parts, RIB (Routing Information Base) and LIB (Label Information Base). The responsibility of the RIB is to handle and maintain the routing information through routing protocols e.g. IS-IS, OSPF, EIGRP , RIP, BGP etc. Moreover, RIB is responsible to build the routing table. Whereas the FIB (Forwarding Information Base) is a portion in the Data Plane is generated by the RIB [15].

2.19.2. Label Information Base (LIB)

LIB is responsible to exchange the labels between neighbor device within the MPLS domain. Above action is performed by LIB via using two protocols e.g. LDP (Label Distribution Protocol) and TDP (Tag Distribution Protocol). TDP is the proprietary protocol of Cisco. Where the LDP is standardized by IEEE. The said protocols performed labels exchanging and binding learned through routing tables [16].

2.19.3. Data/ Forwarding Plane

Hardware base forwarding engine is called Data/ Forwarding Plane. There are its two components; one is called FIB (Forwarding Information Base) and other is called LFIB (Label Forwarding Information Base). FIB is generated by RIB (Routing Information Base).

FIB further contains three parts the Pre-build cache, adjacency table and label information. LFIB is the second part of the Data Plane, build by Label Information Base (LIB). It is comprising of the labels information. FIB is consulted when an IP packet is received whereas LFIB is consulted when a label packet is received.

CHAPTER # 3

3. MAIN TOPOLOGY

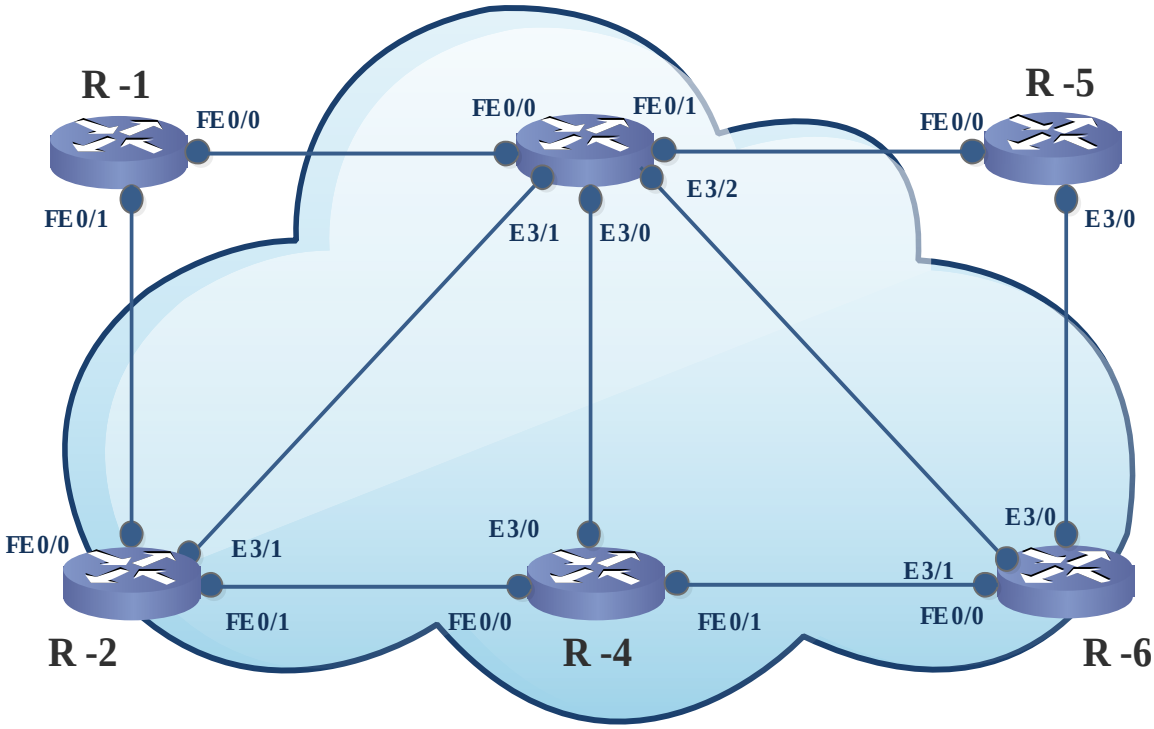


Figure 3. 1: Main Topology – Devices Interfaces

At Figure 3.1, Logical glimpse of the main Network Topology has been placed as above. Six (06) numbers of Routers / Routing devices have been used for conducting the proposed analysis and results. These routing devices have been connected with each other by using Fast Ethernet interfaces. As it has been demonstrated in the above mentioned topology that the main load is on R-3 which is also performing the leading role as an intermediate routing device. Five (05) of its Fast Ethernet interfaces are being utilized.

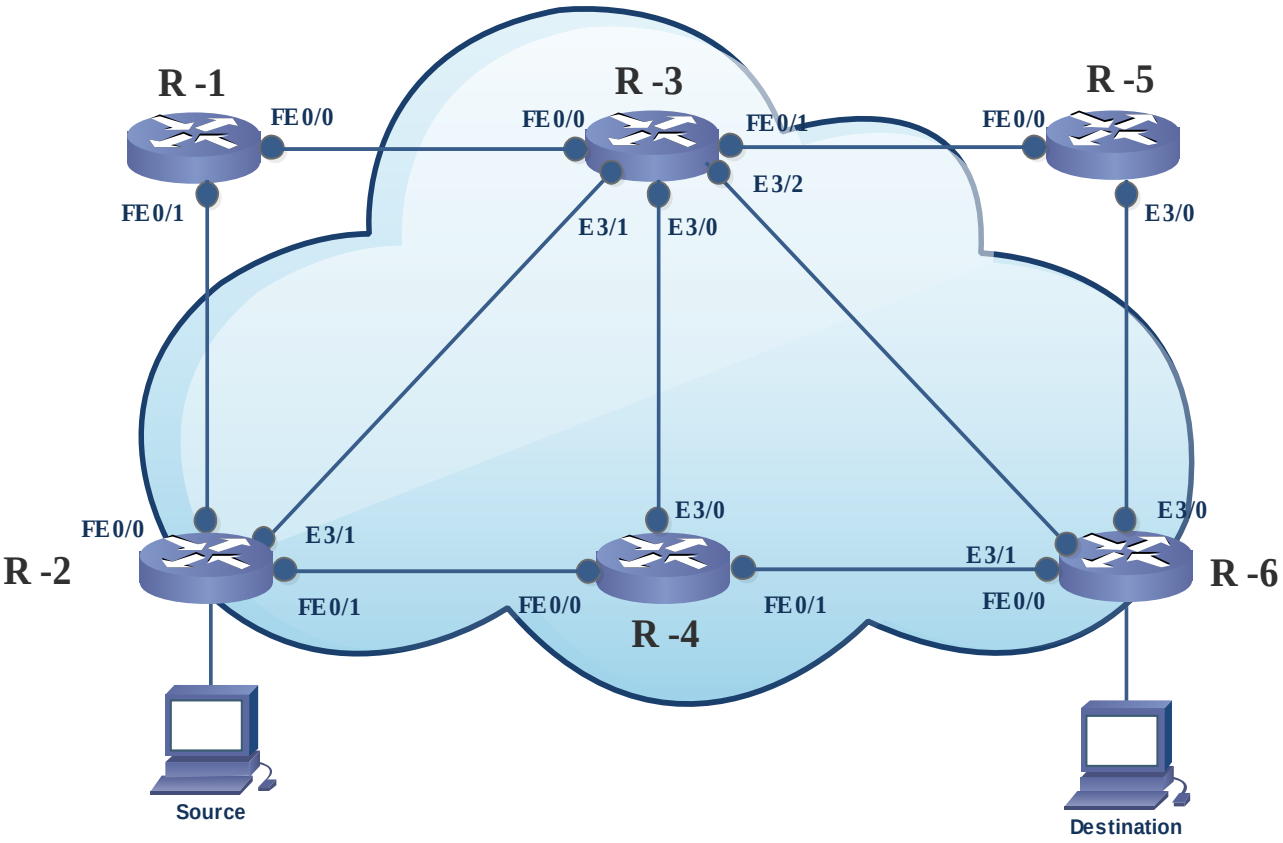


Figure 3. 2: Main Topology – Client Users Attachments

All the six (06) numbers of Routers are connected with each other via Fast Ethernet interfaces. These are also logically connected with each other through the internet / cloud. For conducted the results and analysis purpose, one source (end-user device) and one destination (end-user device) have been attached. Source (end-user) device is attached with Router-2 whereas destination (end-user) device is attached with Router-6 which is placed far away from Router-2.

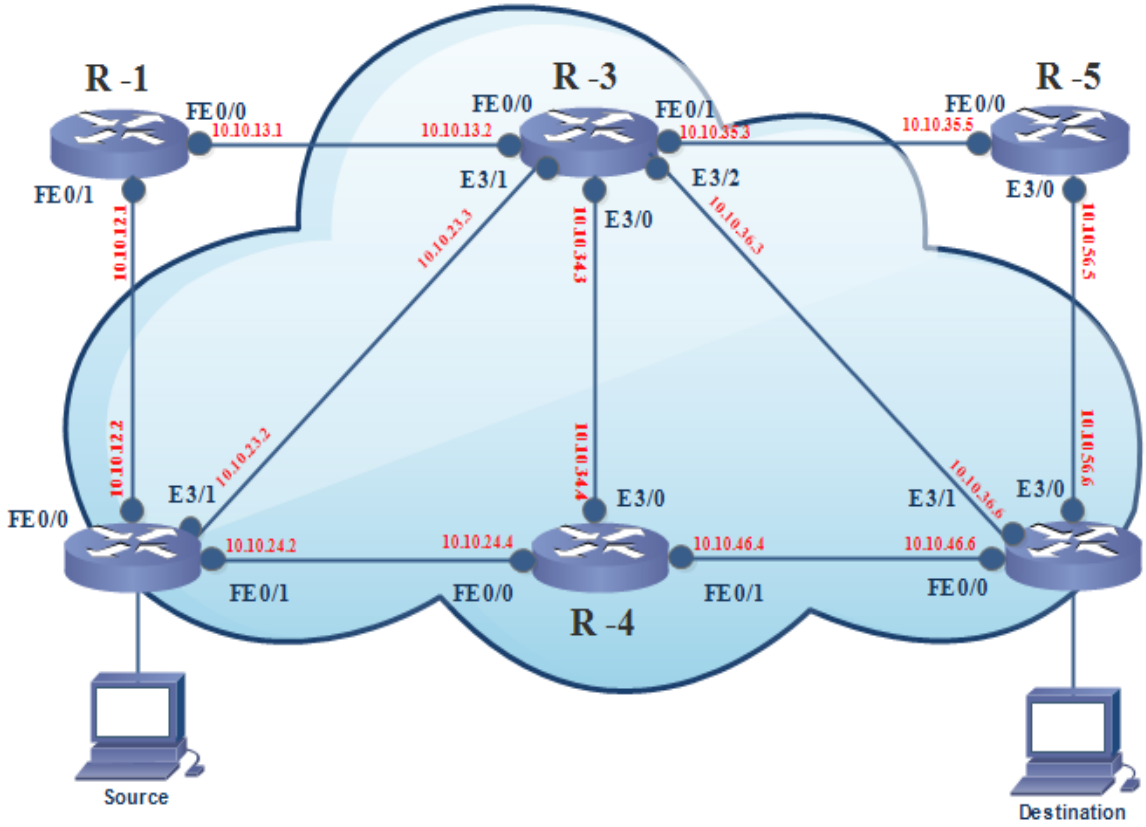


Figure 3. 3: Main Topology – Assigning the IP Schemes

In the above mentioned Figure 3.3, main Network Topology, the 10.10.X.X scheme of IP subnets have been awarded on each Fast Ethernet interface of every Router. IP(s) for each Fast Ethernet interface have been assigned with a simple logic i.e. the IP of the link between Router-1 and Router-2 is 10.10.12.1 & 2. Primarily two octets of this IP Scheme represents the IP class, third octet shows the routers ID which are directly connected with each other and forth octet truly represents the management IP of the every device. All the IP(s) have been assigned with the same logic as mentioned above. Furthermore, loop back of each router is also delineated as 10.10.0.X, here X represents ID of the router i.e.10.10.0.1 is the loop back address of Router-1.

3.1. Topology Transition Table – Main Topology

TOPOLOGY TRANSITION TABLE				
Sr. #.	**Router Name (Source Router)**	**Connected With (Destination Router)**	**Via Interface**	**Via Interface**
1.	R - 1	R – 3	Fast Ethernet 0/0	10.10.13.1
2.	R – 1	R – 2	Fast Ethernet 0/1	10.10.12.1
3.	R – 2	R - 1	Fast Ethernet 0/0	10.10.12.2
4.	R – 2	R - 4	Fast Ethernet 0/1	10.10.24.2
5.	R – 2	R - 3	Fast Ethernet 3/1	10.10.23.2
6.	R - 3	R - 1	Fast Ethernet 0/0	10.10.13.3
7.	R - 3	R – 5	Fast Ethernet 0/1	10.10.35.3
8.	R - 3	R – 4	Fast Ethernet 3/0	10.10.34.3
9.	R - 3	R – 2	Fast Ethernet 3/1	10.10.23.3
10.	R - 3	R – 6	Fast Ethernet 3/2	10.10.36.3
11.	R – 4	R – 2	Fast Ethernet 0/0	10.10.24.4
12.	R – 4	R – 6	Fast Ethernet 0/1	10.10.46.4
13.	R – 4	R – 3	Fast Ethernet 3/0	10.10.34.4
14.	R – 5	R – 3	Fast Ethernet 0/0	10.10.35.5
15.	R – 5	R – 6	Fast Ethernet 3/0	10.10.56.5
16.	R – 6	R – 4	Fast Ethernet 0/0	10.10.46.6
17.	R – 6	R – 3	Fast Ethernet 3/0	10.10.36.6
18.	R – 6	R – 5	Fast Ethernet 3/1	10.10.56.6

Table 3. 1: Main Topology – Transition Table

To facilitate and better understanding of the given topology, a transition Table 3.1 has also been prepared. This table has been prepared or designed by taking the Router(s) description, connection with other Router, interface detail through which the device is connected and lastly IP address of the link. With the help of the table, we can also create the topology manually as well as initial routing table.

It is not out of place to adhesive here the major section of the actual configuration performed on the Router in the main network topology. An instance configuration of Router-1 and Router-3 has been pasted here.

3.2.Running Configuration of the Devices

3.2.1. Router – 1 : Running Configuration

```
interface Loopback0
 ip address 10.10.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.10.13.1 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 10.10.12.1 255.255.255.0
 speed auto
 duplex auto
!
```

3.2.2. Configuration for OSPF Area - 0:

```
!
router ospf 1
 log-adjacency-changes
 network 10.10.0.1 0.0.0.0 area 0
 network 10.10.12.1 0.0.0.0 area 0
 network 10.10.13.1 0.0.0.0 area 0
 network 0.0.0.0 255.255.255.255 area 0
!
```

3.2.3. Configuration for IS-IS Level 2:

```
!
router isis
 net 47.0109.0000.0000.1010.00
 net 47.0119.0000.0000.1010.00
 is-type level-2-only
 metric-style wide
!
```

3.2.4. Router – 3 Running Configuration

// Assigning IP Address on the different interfaces of the Router.

```
!
interface Loopback0
 ip address 10.10.0.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.10.13.3 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 10.10.35.3 255.255.255.0
 speed auto
 duplex auto
!
```

3.2.5. Configuration for OSPF Area 0:

```
!
router ospf 1
 log-adjacency-changes
 network 10.10.0.3 0.0.0.0 area 0
 network 10.10.13.3 0.0.0.0 area 0
 network 10.10.23.3 0.0.0.0 area 0
 network 10.10.34.3 0.0.0.0 area 0
 network 10.10.35.3 0.0.0.0 area 0
 network 10.10.36.3 0.0.0.0 area 0
!
```

3.2.6. Configuration for OSPF Area 0 - 1:-

```
!
router ospf 1
 log-adjacency-changes
 network 10.10.0.3 0.0.0.0 area 0
 network 10.10.13.3 0.0.0.0 area 0
 network 10.10.23.3 0.0.0.0 area 0
 network 10.10.34.3 0.0.0.0 area 1
 network 10.10.35.3 0.0.0.0 area 1
 network 10.10.36.3 0.0.0.0 area 1
!
```

3.2.7. Configuration for IS-IS Level 2:

```
!
router isis
 net 47.0109.0000.0000.1012.00
 net 47.0139.0000.0000.1012.00
 is-type level-2-only
 metric-style wide
!
```

3.2.8. MPLS Configuration on Router's Interface:

```
!
interface FastEthernet0/0.13
 encapsulation dot1Q 13
 ip address 10.10.12.1 255.255.255.0
 mpls ip
!
```

3.2.9. MPLS Configuration – Step Further

```
!
multilink bundle-name authenticated
mpls label protocol ldp
call rsvp-sync
!
```

3.2.10. BGP Neighbour Configuration On Router

```
!
router bgp 10
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.10.0.2 remote-as 10
 neighbor 10.10.0.2 update-source Loopback0
 neighbor 10.10.0.3 remote-as 10
 neighbor 10.10.0.3 update-source Loopback0
 neighbor 10.10.0.4 remote-as 10
 neighbor 10.10.0.4 update-source Loopback0
 neighbor 10.10.0.5 remote-as 10
 neighbor 10.10.0.5 update-source Loopback0
 neighbor 10.10.0.6 remote-as 10
 neighbor 10.10.0.6 update-source Loopback0

 !
```

3.2.11. BGP Neighbor Configuration – Step Further

```
 address-family ipv4
  no synchronization
  network  10.10.0.1 mask 255.255.255.255
  neighbor 10.10.0.2 activate
  neighbor 10.10.0.2 send-community
  neighbor 10.10.0.2 route-reflector-client
  neighbor 10.10.0.3 activate
  neighbor 10.10.0.3 send-community
  neighbor 10.10.0.3 route-reflector-client
  neighbor 10.10.0.4 activate
  neighbor 10.10.0.4 send-community
  neighbor 10.10.0.4 route-reflector-client
  neighbor 10.10.0.5 send-community
  neighbor 10.10.0.5 route-reflector-client
  neighbor 10.10.0.6 send-community
  neighbor 10.10.0.6 route-reflector-client

  no auto-summary
 exit-address-family
!
```

CHAPTER # 4

4. DESIGNING & IMPLEMENTATION

4.1. Why Use GNS Version 3

Graphical Network Simulator-3 (GNS-3) is a prevalent open source graphical network simulator under the terms and condition of General Public Licensing. It is exorbitantly worldwide utilized network simulation that's supports real-life IOS of different network devices. GNS3 [20] also allows the collaboration of real-life devices and virtual devices used for simulating the complex network infrastructures and topologies.

GNS3 also helps to design and create a thorough and very comprehensive network infrastructure topology that must be tested in a risk free virtual [20] network environment. A network topology infrastructure could be designed including hundreds of equipment/ devices and implemented without any further requirement of network / IT hardware. Furthermore, GNS3 [19] also provide the support for creation / designing of network diagram for troubleshooting and proof of concept (POC) testing.

4.1.1. System Requirement for GNS3

SYSTEM REQUIREMENTS FOR GNS3	
1.	02 Logical Core Processors or More
2.	04 GB RAM (Memory) for Efficient Working
3.	01 GB Hard Disk Space

Table 4. 1: System Requirements for GNS3

GNS3 could be installed on a desktop system with lower specification but to obtain the maximum efficiency and performance the above mentioned requirements mentioned in the table are necessarily needed. The requirement i.e. RAM, can be decreased from 4 GB to 2 GB at least, hard disk space can also be reduced from 1 GB to 750 MB. It could be installed over multifarious operating systems i.e. Microsoft Windows 7 or later [20].

4.1.2. GNS 3 Important Features

Few of its main feature of GNS3 are as follows;

i. Open Source
ii. Public Domain/ Freeware
iii. Easily Downloadable and Accessible
iv. Built-in Packet Capturing
v. ASA, PIX Firewalls and Other Security Devices Support Available
vi. Connect with VMS
vii. Less Hardware and Software Requirements
viii. Work on Real IOS
ix. Integration with Real Life Network & Devices
x. Layer-II Switching Support
xi. Provide Support for Juniper Devices
xii. Support Bigger Network Topology

Although, there are many other simulators [22] and emulators are also available in the world market but there is no comparison of GNS3 with them. GNS3 is one & only best choice among all. This choice has not only been made on any myth or hypothetical base. There are many other solid reasons and basis for using the GNS3.

Packet Tracer, NetSim, Marionnet, Mininet, OpenStack, PSimulator2 are also existed simulator and emulators available in the market. But few are very expensive (not free as GNS3), Few does not support for real life devices, some are command line and having not GUI display, several simulators/ emulators does not equipped with pedagogy features, certain same type of software are very complex to install and configure, some of them are not compatible with Windows Operating Systems and only supports Linux or Mac Book, few are very big that requires huge computer resources consumption.

Keeping in view the hurdles and discrepancies as mentioned above regarding different simulators [22] and emulators, GNS3 [19] was the best choice and selection for the completion of this project/ thesis. You can now easily observe that how flexible, scalable, efficient, speedy and reliable the GNS3 is [21].

4.1.3. Simulators - Comparison

COMPARISON OF SIMULATOR			
SR. #.	**COMPARISON CRITERIA**	**GNS3**	**PACKET TRACER**
1.	**Real-Life Devices Support**	YES	NO
2.	**Support of Configuration Commands**	As per version of IOS - Fully Support.	Very Limited
3.	**Connectivity with Real World Network.**	YES	NO
4.	**Types of Equipment Support**	Router, Switch (L-2 & 3), IDS, IPS, Qemu, Firewall,Cloud, Virtual Box, Host Machine OS.	Router, Switch (L-2 & 3) with limited support of commands, IP Phones, PC, Tablet PC, Printers, Servers etc.
5.	**Availability**	Open Source, however, IOS are not included with Software.	Free - only for Cisco Environment.
6.	**OS Support**	Windows, Linux, MAC	Windows and Linux
7.	**Quality of Configuration Response**	Provide more detail of realistic configuration respond.	Suppress Configuration response.
8.	**Computer Resource Consumption**	Consume high level processing of computer, depends upon topology and number of devices.	Consume less computer processing.

Table 4. 2: Comparison of Simulators

4.2.SYSTEM SPECIFICATION – TEST PERFORMED

In the field of Information Technology, hardware resources really matter especially at the time of designing, implementing, monitoring and analyzing the different performance related parameters of any research.

Keeping in view the limited budget for this research, few basic and intermediate level desktop computer machines were prepared and checked. Finally, the desktop system machine with the specification mentioned in the table below was selected. The hardware resources specification mentioned in the table below are usual routine life desktop computer machine. Although, the specification of the selected desktop system is not very high but it fulfills the purpose and the main goal of this research is not been ignored. Better hardware resources support definitely matters a lot in any field of IT infrastructure but less specification of hardware resources does not matter even to a little extent. Table below contains the specification of hardware and software resources used for the demonstration of the project.

All the software(s) used form the preparation to finalization of this thesis were installed on the said desktop computer machine. The software(s) for designing & preparation of Network Topology, Maps, Comparison Table, Figures & Templates, Results Conduction, Monitoring and Comparative Analysis etc. were installed on the computer system which specification have been mentioned below at Table 4.3.

SPECIFICATION OF DESKTOP SYSTEM FOR TESTS		
Desktop System Specifications	**Hardware Name**	**Description**
	Processor	3.0 GHz (3rd Generation)
	RAM (DDR3)	4 GB
	Hard Drive	1 GB SATA
	Cache	3 MB
	ChipSet	Intel H61 or Intel Q75 Express or Above
	Operating System 32-Bit	Windows 8 (Professional)

Table 4. 3: Specification of System for Experimental Test Beds

4.3.EDRAW MAX PORTABLE

Designing chapter has an exorbitant impact of any research thesis or bookish work. Keeping in view the sensitivity and important of this chapter, graphical representation has been done with very flexible, rich GUI and best designing tools. Different diagrams, layouts, topology, site plans and graphical representations have been made by using E-Draw 7 and Microsoft Visio Software. These are the best and very powerful tools that are currently available in the market for making vector graphics, organization diagrams, flow charts, roadmaps, layout etc.

E-Draw 7 is the updated version that is currently available in the market for designing and graphical works. The things which were not covered in Microsoft Vision, the E-Draw 7 has been used. There are various plus point of this software, as this colossal software is equipped with splendid build-in templates i.e. Arrows Diagrams, Flow, Marketing and Organization Charts, Brainstorming Diagram, Business, Relationship and Six Sigma Matrix, Cause and Effects (Fish Bone Diagram), Circle Spoken Diagram, Fault Analysis Diagram, TQM, Value Chain, Work Flow Diagram, Value Stream Mapping and Venn Diagrams etc.

The above mentioned templates are contained rich graphics which have been used to make / design most of the diagrams and templates of this thesis. Edraw is an all in one software that is used to create professional graphical and designing work in a corporate environment. It

covers approximately all area of working life, as human resources need to be able to design organization charts, software engineer need to work on UML diagrams, Network Experts are required to design network topologies, diagram and layouts. 6200 plus rich graphical designs for Graphic Designers etc. Another of its beauty is to conversion in almost all the graphical formats i.e. PDF (Portable Document Format), SVG (Scalable Vector Graphics), EPS (Encapsulated Postscript Vector), WYSIWYG (What you see is what you get – way of designing / crating the electronic documents) support.

There are many other useable and magnificent features of E-Draw 7 are UI, color themes and features, fonts and effects, real time preview, templates galleries, drawing objects, quick layouts and styles, shape and texts are easy to apply even in other software and applications like Microsoft Word, Excel, Power Point, Paint etc. Furthermore, E-draw is equally famous within students, teachers, businessmen professional, IT experts and almost every person who uses the computer and specially involve in some sort of graphical and designing field.

Hardware and software requirement for the installation and utilization of this exorbitantly valuable software is not very high. Only normal hardware resource and space area is required. The detail of the resources for installation of E-Draw is as follows at Table 4.4..

4.3.1. System Specification of EDraw Portable Max

DETAIL OF BASIC RESOUCES FOR INSTALLATION OF E-DRAW		
Desktop System Specifications	**Hardware Name**	**Description**
	Processor	750 MHz 3.3
	RAM	512 GB
	Hard Drive	300 MB (Without Full Library)
		700 MB (With Full Library)
	Preferred Resolution	1024 x 768
	Operating System	Windows 200, XP, 2003, Vista, 7, 8, 8.1 (All Editions – Either 32 / 64 Bits)

Table 4. 4: Resources Detail for Installation of EDraw

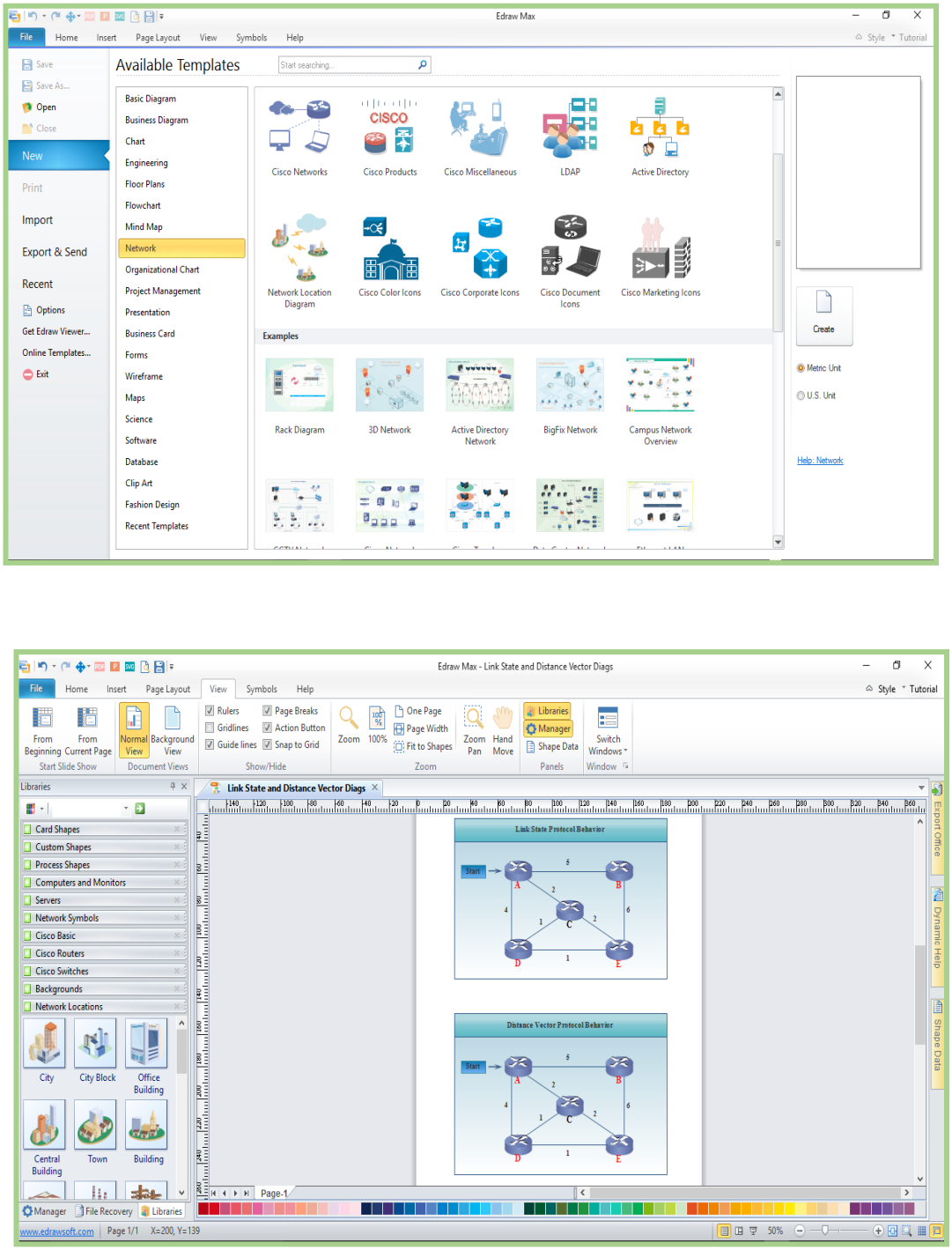
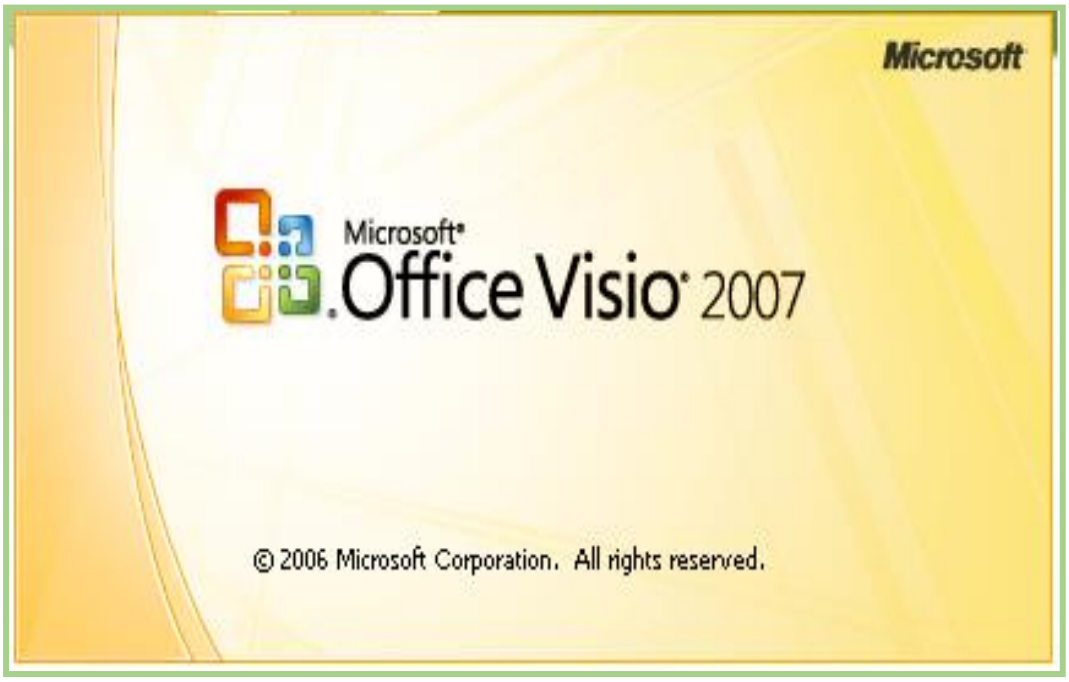


Figure 4. 1: Snapshots of EDraw Max Portable

4.4.MS VISIO



Microsoft Visio is another splendid graphical tool which has been used for the finalization of graphical and designing documentations of this thesis'. It also offers a vast variety of built-in templates, shapes, stencils and different graphical objects. In my point of view, this is the best existing graphical and designing tool for the creation of stencils and objects. By using this a user can creates his own shapes and rich graphical templates. A couple of hundreds of standardized templates, shapes, objects and layouts of different day life categories are available for use in Microsoft Visio.

It is valuable to mention here that Microsoft Visio is primarily clientele have been enterprise users at the corporate culture. The approach of this software is slightly be different E-Draw 7, it is equipped with templates as well as a large library of different categories. The detail of the available items in the library and built-in templates i.e. Alarm and Access Control, Appliances, Bath and Kitchen Plan, Building Core, Cabinets, Cubicles, Electrical and Telecom, Furniture, Garden Accessories, HVAC Controls and Equipment, Initiation and Annunciation, Irrigation, Office Accessories, Equipment and Furniture, Parking and Roads, Pipes and Valves, Planting, Plumbing, Points of Interest, Registers, Grills and Diffusers, Resources, Shop Floor, Machines and Equipment, Vehicles, Video Surveillance, Walls,

Doors and Windows, Shell and Structure, Warehouse, Shipping and Receiving and many more others.

Different file formats that normally covers by the Microsoft Visio are VSD (Visio Extension- Simple Drawing), VSS (For Stencil), VST (For Template), VSW (For Web Drawing), VDX (For XML Drawing), VSDX (For OPC/ XML Drawing, Macro Enabled), VSL (For Specially Add On) etc. These all are the special and proprietary file extensions which are supported only by Microsoft Visio. The beauty of the file format/ extension is that these are compressed as well. These format taken a very light weight to carry them.

The requirement for the installation of Microsoft Visio is slightly high as compared to E-Draw 7. But it does not mean that high side hardware and software resources are required for the installation of the same. Down here at Table 4.5, the detail of the resources for the installation of Microsoft Visio.

4.4.1. System Specification for MS Visio

DETAIL OF BASIC RESOUCES FOR INSTALLATION OF MS VISIO		
Desktop System Specifications	**Hardware Name**	**Description**
	Processor	1 GHz
	RAM	1 GB
	Hard Drive	3 GB Available
	Display	1024 x 576 *(DiretX is also Required for Acceleration of Graphics Hardware)*
	Operating System	Windows 7, 8, 8.1, 10 Windows Server 2008, 2012

Table 4. 5: Resources Detail for Installation of MS Visio

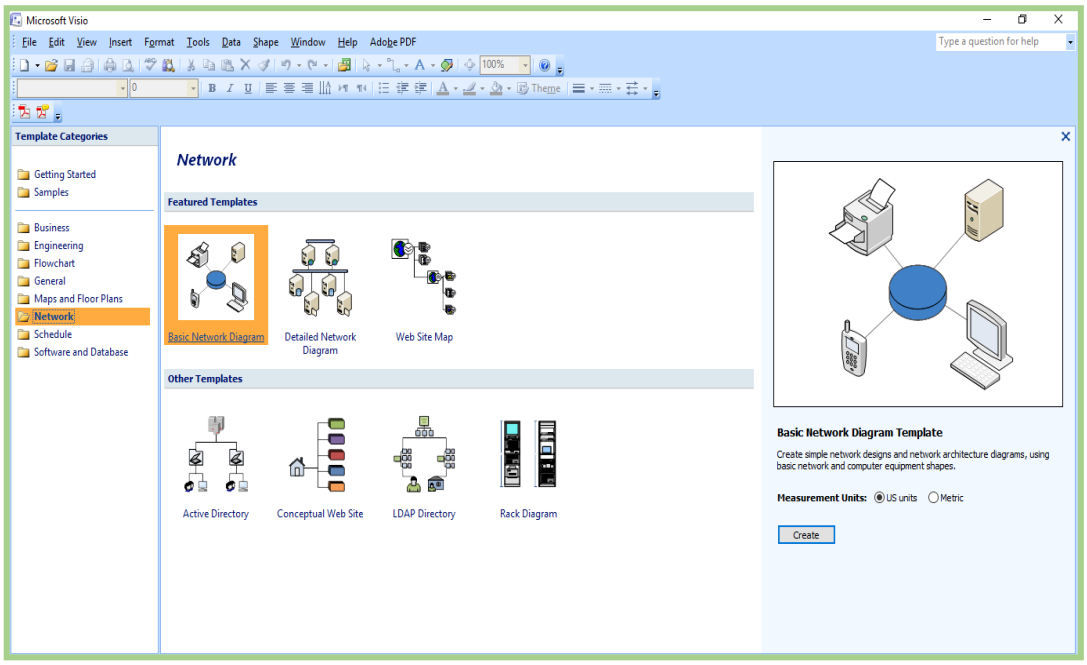
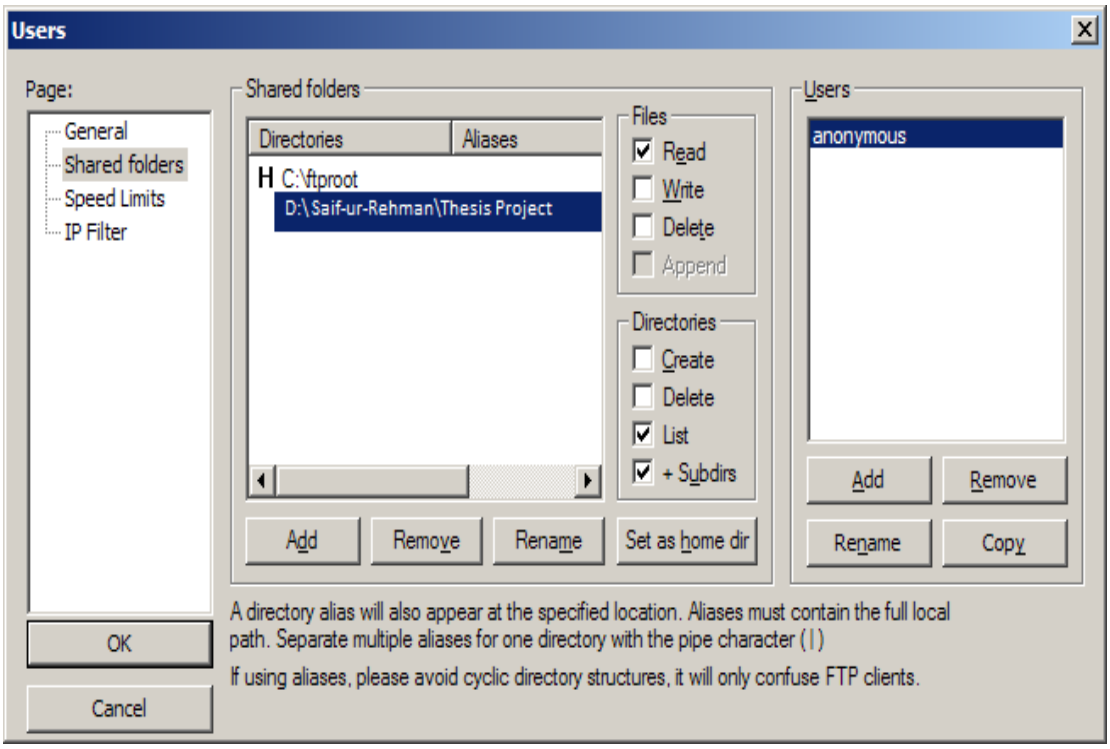


Figure 4. 2: Snapshots of MS Visio

4.5.FILE ZILLA SERVER



Protection and security of data over a network or internet is much important during any transaction of information. Here in this thesis, secure and encrypted connectivity to the server has been made through File Zilla Client Server application software. It is an open source FTP server under the terms and condition of the GNU (General Public License) that's source code is also available over different internet sites.

File Zilla Server application is the software base server that provide full support for FTP (File Transfer Protocol). FTP on TLS (Transport Layer Security – cryptographic protocol for secure communication) and SSL (Secure Sockets Layer – Protocol which creates a secure connection between server machine and client machine) provides the guaranteed encrypted and highly secured connectivity to a server machines. File Zilla application server also support TLS. It uses the same level of data security and encryption as the usual web browser uses to secure and protect your data transmission.

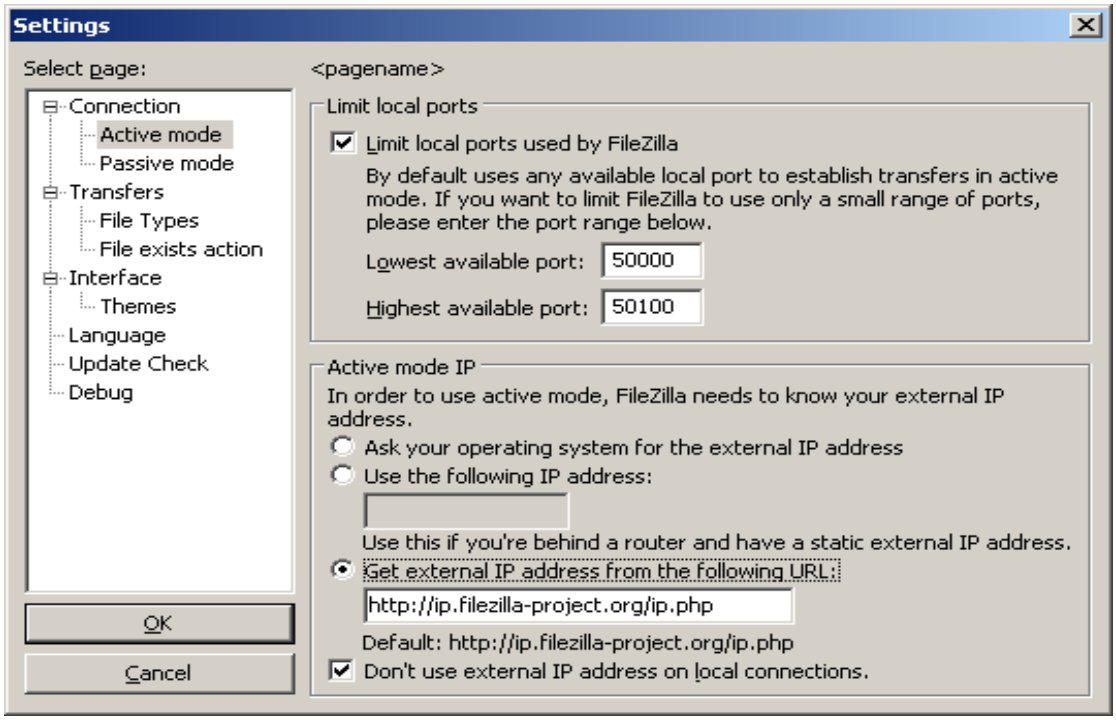


Figure 4. 3: Snapshot of FileZilla Client Server

Heavy hardware resources are not required for the installation of File Zilla Server, only few software level setting are necessarily required to run it smoothly. Exact of its port number, some share directories settings, user accounts are needed to setting it up. A glimpse of the hardware requirement is placed below at Table 4.6.

4.5.1. System Requirement for FileZilla Server

BASIC RESOUCES FOR INSTALLATION OF FILE ZILLA SERVER		
Desktop System Specifications	**Hardware Name**	**Description**
	Processor	7.33 MHz / Pentium III Processor.
	RAM	256 MB or Above
	Hard Drive	500 MB is Much More
	Operating System	Windows 7, 8, 8.1, 10 Windows Server 2008, 2012

Table 4. 6: Resources Detail for Installation of FileZilla Server

4.6. WIRESHARK

Packets capturing were required for the analysis and perusal of the results obtained. To perform this task another freeware open source packet analyzer software was use 'Wireshark'. It is also further used for real life network monitoring, analysis and troubleshooting. Its old name was "Etheral" that renamed "Wireshark" in 2006 due to some trademark matters.

Wireshark actually captures the packets send/ received on a specific interface of the network device. It also supports the wireless network devices like if you want to capture a packet/ data on a wireless device so the promiscuous mode must be enabled. Wireshark captures the data packets in a human readable format/ mode. It is equipped with the various brilliant features like filter, color coding schemes to let you dig deep into the real life network traffic.As far as the packets capturing of this project is concerned, Wireshark was used. All the graphs and calculated graphs of chapter number 5 have been summarized with the help of Wireshark packet capturing software. As it has been mentioned above that it helps you to dig deep in real network to analyze the network traffic and inspection each and individual data packet. The beauty of this software is to distinguish the different data packets into different color code scheme i.e. green represents the TCP traffic, dark blue presents DNS traffic, light blue is for UDP traffic and black identify TCP packets with problems. Table 4.7 contains the specs;

4.6.1. System Specification for WireShark

RESOUCES FOR INSTALLATION OF WIRESHARK		
Desktop System Specifications	**Hardware Name**	**Description**
	Processor	7.33 MHz / Pentium III Processor.
	RAM	512 MB or Above
	Hard Drive	1 GB
	Operating System	Windows 7, 8, 8.1, 10 Windows Server 2008, 2012

Table 4. 7: Resources Detail for Installation of WireShark

CHAPTER # 5

5. TEST BEDS

5.1. TEST BED # 01: MPLS over OSPF Area 0

Experimental test beds has conducted to implement MPLS over OSPF Area - 0 (Backbone Area) using GNS3 (Graphical Network Simulator Version 3). File of 4000000 (in byte) has transferred for multiple times using FileZilla server and client Software. The traffic generated has monitored by using Wire-shark Packet Analyzer tool. Tabular demonstration has presented via using Wireshark results.

MPLS OVER OSPF AREA 0	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3129
Bytes	4000000
Average Packet Size	1278.5
Average Transfer Time	737.599 Sec
Average Transfer Rate (Bytes/s)	5423
Average Megabits/s	0.43

Table 5. 1: MPLS over OSPF Area 0

5.1.1. Average Data Transfer Time

Statistical table at 5.1 express the analysis of MPLS over OSPF Area-0 (Backbone Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. The Average Transfer Time (in seconds) is 737.599/ second.

5.1.2. Average Data Transfer Rate

Statistical table at 5.1, displays the analysis of MPLS over OSPF Area-0 (Backbone Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. Average Transfer Rate (Bytes/ seconds) is 5423.

5.1.3. Average Bandwidth Utilization:

Statistical table at 5.1, shows the analysis of MPLS over OSPF Area-0 (Backbone Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. An Average bandwidth utilization (in megabits/ seconds) 0.43%.

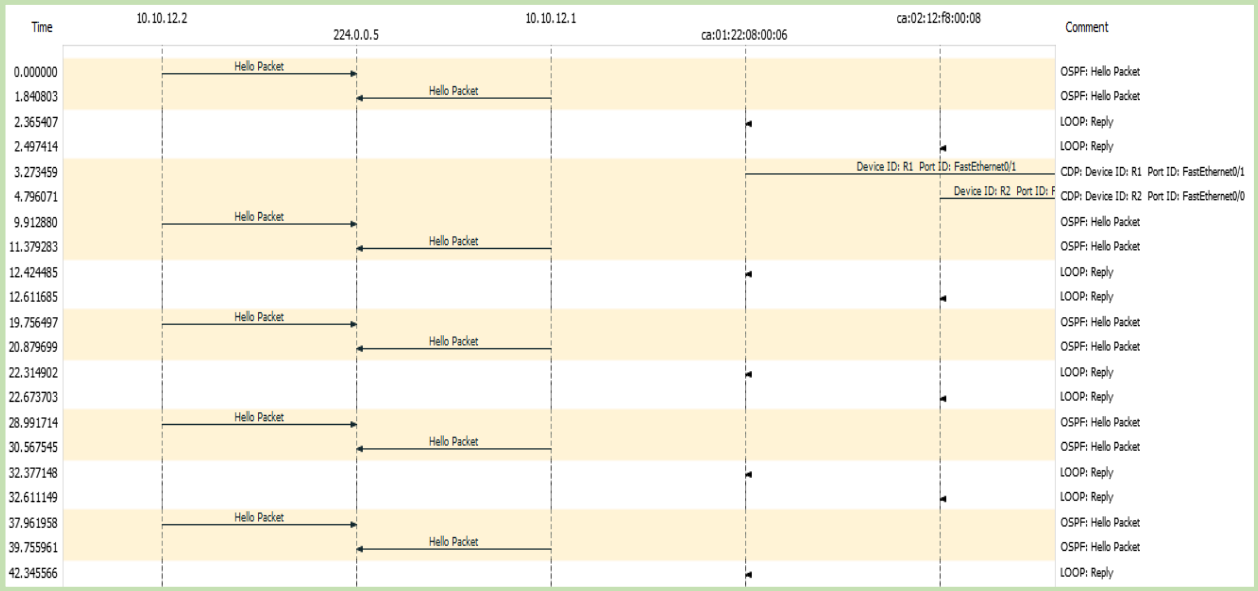


Figure 5. 1: MPLS over OSPF Area 0 - Exchanges of Hello Packets

Figure 5.1, demonstrate the exchanges of the 'Hello' are being exchanged between 10.10.12.2 and 10.10.12.1. The multicast address is 224.0.0.5 which has also been shown in above located figure.

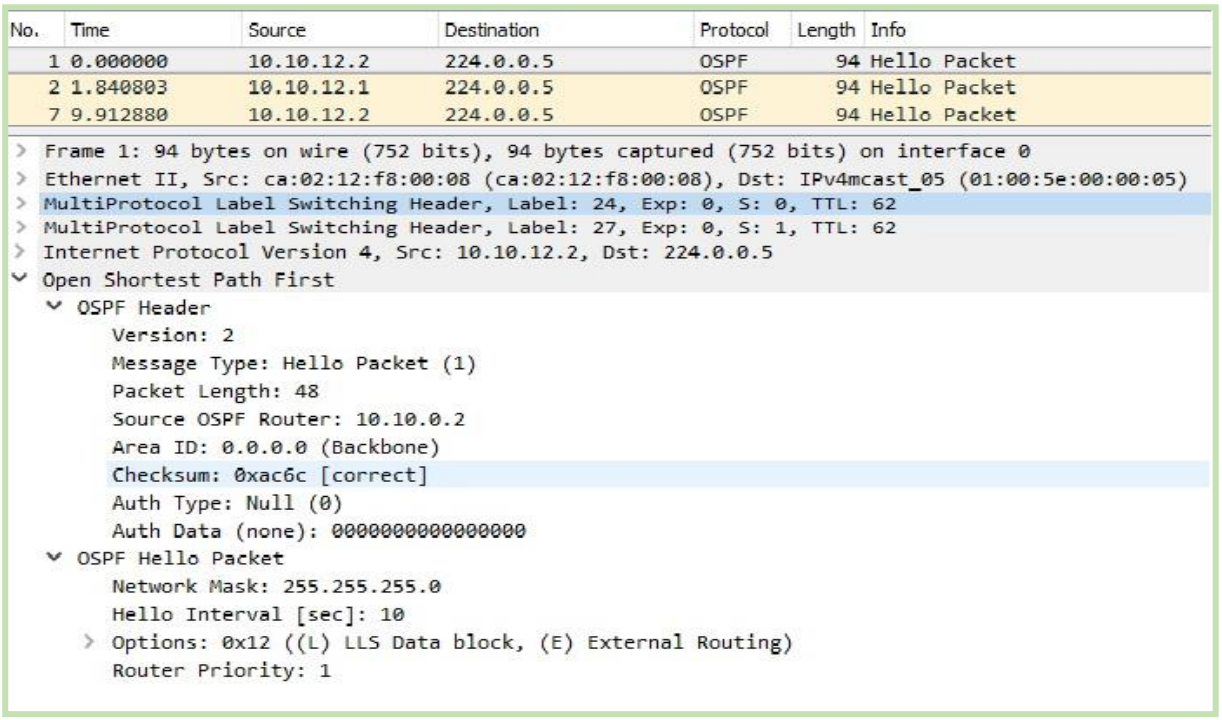


Figure 5. 2: MPLS over OSPF Area 0 – Header Detail

A Frame of MPLs over OSPF Area-0 has captured via Wireshark. Detail of OSPF header has been shown at Figure 5.2 as its Version (2), Message Type (Hello Packet), Packet Length (48), Source OSPF Router (10.10.0.2) and Area ID (Backbone Area). Moreover, the first frame 94 bytes (752 bits) on wire has captured on Interface 0. MPLS header has also been highlighted.

Figure 5. 3: MPLS over OSPF Area 0 – Wireshark IO Graph

The statistics derivative from the experimental test beds from MPLS over OSPF Area-0 (Backbone Area) has been expressed in Figure 5.3 in form of Graph. On X- axis, an Average Time with the interval of 20 seconds have been showed whereas on Y-axis, packets/seconds has been shown with the interval of 6 packets/seconds.

5.2. TEST BED # 02 : MPLS over IS-IS Level - 1

Experimental test beds has conducted with the implementation of MPLS over IS-IS Level-1 using GNS3. A file of 4000000 (in byte) has transferred for multiple times using FileZilla server and client Software. The traffic generated has monitored by using Wire-shark Packet Analyzer tool. Tabular demonstration has presented via using Wireshark results.

MPLS OVER IS-IS LEVEL - 1	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3085
Bytes	4000000
Average Packet Size	1296.5
Average Transfer Time	668.561 Sec
Average Transfer Rate (Bytes/s)	5983
Average Megabits/s	0.48

Table 5. 2: MPLS over IS-IS Level-1

5.2.1. Average Data Transfer Time

Statistical table at 5.2 express the analysis of MPLS over IS-IS Level – 1. A file of 4000000 (in byte) has been transferred for Twenty Five times. The Average Transfer Time (in seconds) is 668.561/ second.

5.2.2. Average Data Transfer Rate

Statistical table at 5.2, displays the analysis of MPLS over IS-IS Level – 1. A file of 4000000 (in byte) has been transferred for Twenty Five times. An average Transfer Rate (Bytes/ seconds) is 5983.

5.2.3. Average Bandwidth Utilization

Statistical table at 5.2, shows the analysis of MPLS over IS-IS Level – 1. File of 4000000 (in byte) has been transferred for Twenty Five times. An Average bandwidth utilization (in Megabits/ seconds) 0.48%.

Figure 5. 4: MPLS over IS-IS Level - 1 - Exchanges of Hello Packets

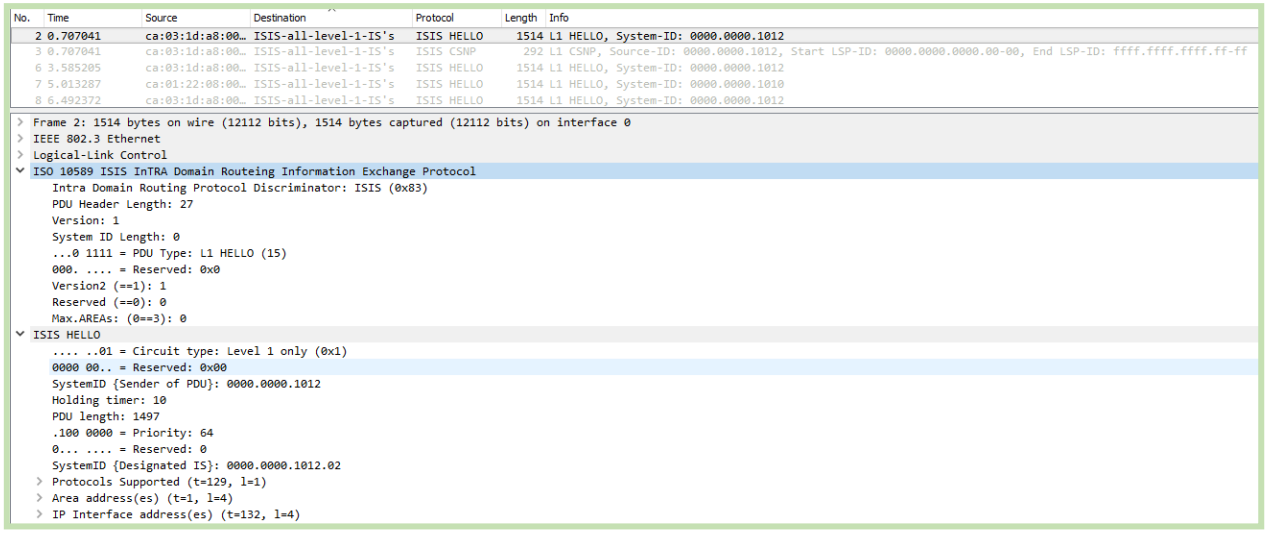


Figure 5. 5: MPLS over IS-IS Level - 1 – Header Detail

A Frame has been captured of MPLs over IS-IS Level-1 via Wireshark. As the frame 2 on wire on interface 0 has been captured and having 1514 bytes. Further, intra domain routing of IS-IS, Version, circuit type and header of the ‘Hello’ packet has been shown in Figure 5.5.

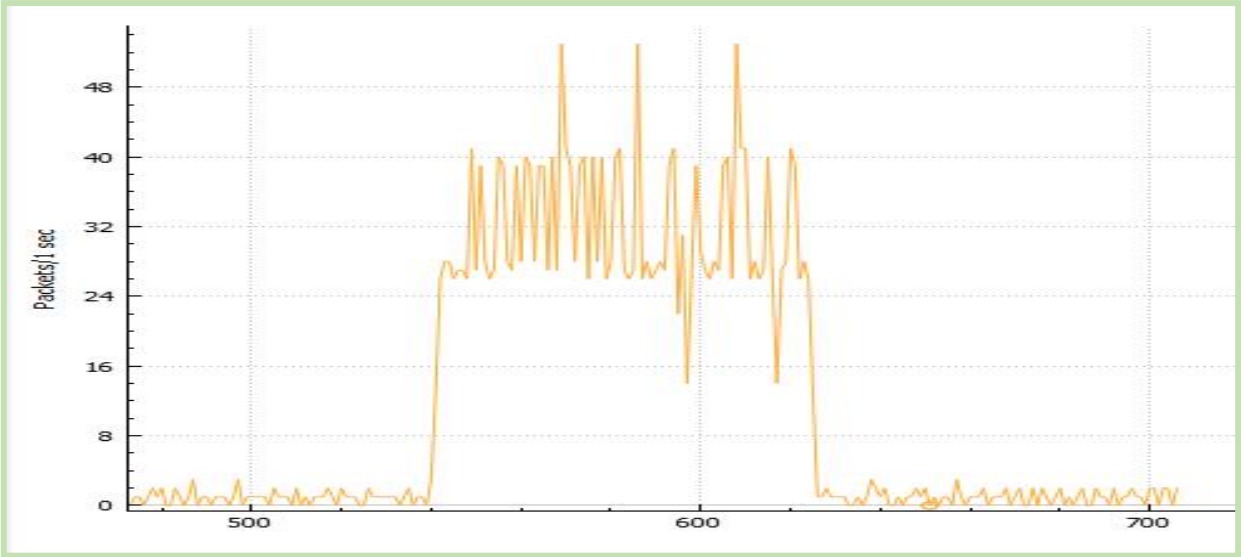


Figure 5. 6: MPLS over IS-IS Level - 1 - Wireshark IO Graph

The statistics derived from the experimental test bed # 02, MPLS over IS-IS Level-1 has been expressed in Figure 5.6 in form of Graph taken from Wireshark. On X- axis, an Average Time with the interval of 20 seconds have been showed whereas on Y-axis, packets/seconds has been shown with the interval of 8 packets/seconds.

5.3. TEST BED # 03: MPLS over OSPF Normal Area

Experimental test beds has steered to implement MPLS over OSPF Area 0 - 1 (Normal Area) using GNS3 (Graphical Network Simulator Version 3). File of 4000000 (in byte) has transferred for multiple times using FileZilla server and client Software. The traffic generated has monitored by using Wire-shark Packet Analyzer tool. Tabular demonstration has presented via using Wireshark results.

MPLS OVER OSPF NORMAL AREA 0 - 1	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3573
Bytes	4000000
Average Packet Size	1119.5 Bytes
Average Transfer Time	1784.12 Sec
Average Transfer Rate (Bytes/s)	2242
Average Megabits/s	0.18

Table 5. 3: MPLS over OSPF Area 0 – 1 (Normal Area)

5.3.1. Average Data Transfer Time

Statistical table at 5.3 shows the analysis of MPLS over OSPF Area 0 – 1 (Normal Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. The Average Transfer Time (in seconds) is 1784.12/ second.

5.3.2. Average Data Transfer Rate

Statistical table at 5.3, demonstrate the analysis of MPLS over OSPF Area 0 - 1 (Normal Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. Average Transfer Rate (Bytes/ seconds) is 2242.

5.3.3. Average Bandwidth Utilization

Statistical table at 5.3, shows the analysis of MPLS over OSPF Area 0 - 1 (Normal Area). A file of 4000000 (in byte) has been transferred for Twenty Five times. An Average bandwidth utilization (in Megabits/ seconds) 0.18%.

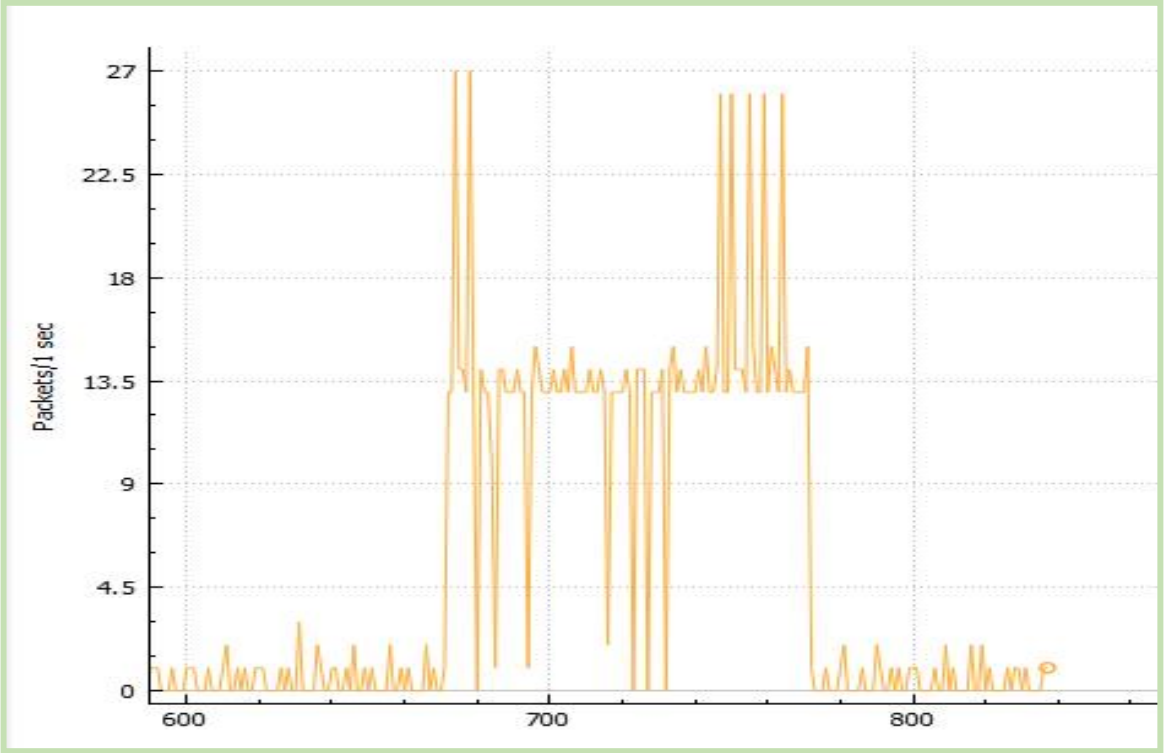


Figure 5. 7: MPLS over OSPF Area 0 - 1 - Wireshark IO Graph

At Figure 5.7, the statistics taken from the experimental test bed # 03, MPLS over OSPF Area 0 - 1 (Normal Area) has been expressed in form of Graph. On X- axis, an Average Time with the interval of 20 seconds have been showed whereas on Y-axis, packets/seconds has been shown with the interval of 4.5 packets/seconds.

5.4.TEST BED # 04: MPLS over IS-IS Level - 2

Experimental test beds has conducted with the implementation of MPLS over IS-IS Level - 2 using GNS3. A file of 4000000 (in byte) has transferred for multiple times using FileZilla server and client Software. The traffic generated has monitored by using Wire-shark Packet Analyzer tool. Tabular demonstration has presented via using Wireshark results.

MPLS OVER IS-IS LEVEL-2	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3002
Bytes	4000000
Average Packet Size	1332.5
Average Transfer Time	483.092 Sec
Average Transfer Rate (Bytes/s)	8280
Average Megabits/s	0.66

Table 5. 4: MPLS over IS-IS Level - 2

5.4.1. Average Data Transfer Time

Statistical table at 5.4 express the analysis of MPLS over IS-IS Level – 2. A file of 4000000 (in byte) has been transferred for Twenty Five times. The Average Transfer Time (in seconds) is 483.092/ second.

5.4.2. Average Data Transfer Rate

Statistical table at 5.4, displays the analysis of MPLS over IS-IS Level – 2. A file of 4000000 (in byte) has been transferred for Twenty Five times. An average Transfer Rate (Bytes/ seconds) is 8280.

5.4.3. Average Bandwidth Utilization

Statistical table at 5.4, shows the analysis of MPLS over IS-IS Level – 2. File of 4000000 (in byte) has been transferred for Twenty Five times. An Average bandwidth utilization (in Megabits/ seconds) 0.66%.

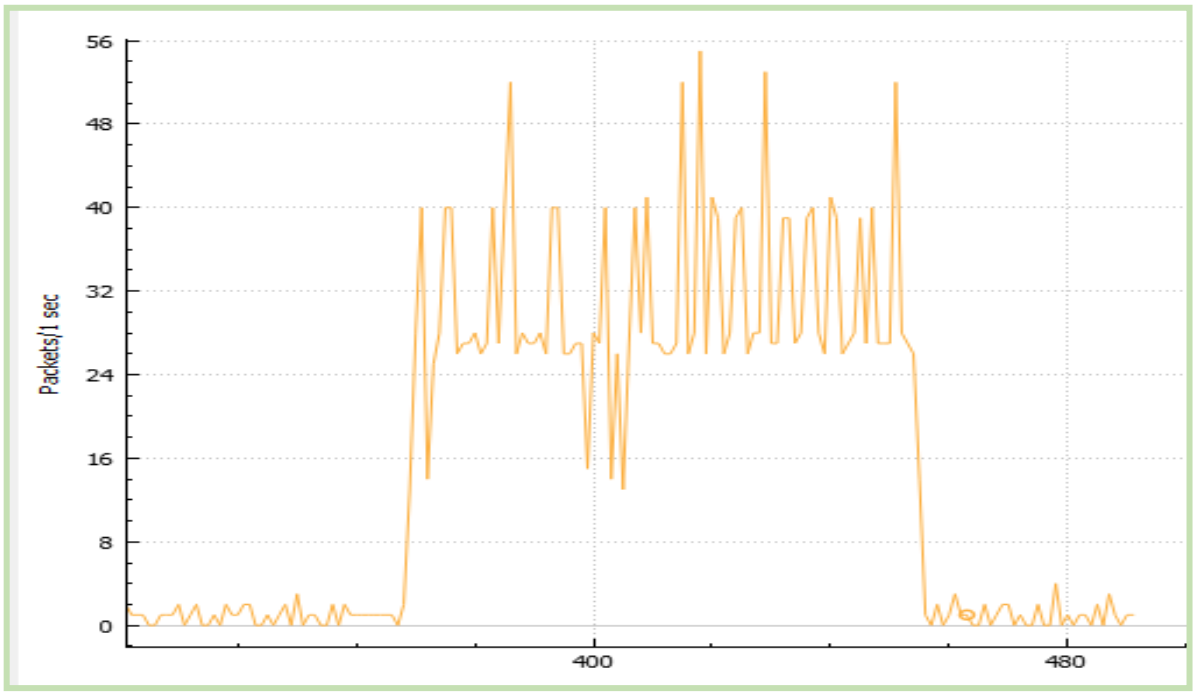


Figure 5. 8: MPLS over IS-IS Level - 2 - Wireshark IO Graph

The statistics obtained from the experimental test beds from MPLS over IS-IS Level - 2 has been reflected in Figure 5.8 in form of Graph. On X- axis, an Average Time with the interval of 20 seconds have been showed whereas on Y-axis, packets/seconds has been shown with the interval of 8 packets/seconds.

5.5. TEST BED # 05: Comparative Analysis

COMPARATIVE ANALYSIS IN TABULAR FORM

MPLS OVER OSPF AREA 0	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3129
Bytes	4000000
Average Packet Size	1278.5
Average Transfer Time	737.599 Sec
Average Transfer Rate (Bytes/s)	5423
Average Megabits/s	0.43

MPLS OVER IS-IS LEVEL-1	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3085
Bytes	4000000
Average Packet Size	1296.5
Average Transfer Time	668.561 Sec
Average Transfer Rate (Bytes/s)	5983
Average Megabits/s	0.48

MPLS OVER OSPF AREA 0 - 1	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3573
Bytes	4000000
Average Packet Size	1119.5 Bytes
Average Transfer Time	1784.12 Sec
Average Transfer Rate (Bytes/s)	2242
Average Megabits/s	0.18

MPLS OVER IS-IS LEVEL-2	
Encapsulation	Ethernet
Packet Size Limit	65535 bytes
Packets	3002
Bytes	4000000
Average Packet Size	1332.5
Average Transfer Time	483.092 Sec
Average Transfer Rate (Bytes/s)	8280
Average Megabits/s	0.66

Table 5. 5: Overall Comparative Analysis Table

5.5.1. COMPARATIVE ANALYSIS – Average Transfer Time

COMPARISON AVERAGE TRANSFER TIME				
Test Beds	**OSPF Area-0**	**OSPF Area 0-1**	**IS-IS Level-1**	**IS-IS Level-2**
Result Obtain	**737.599**	**1784.12**	**668.561**	**483.092**

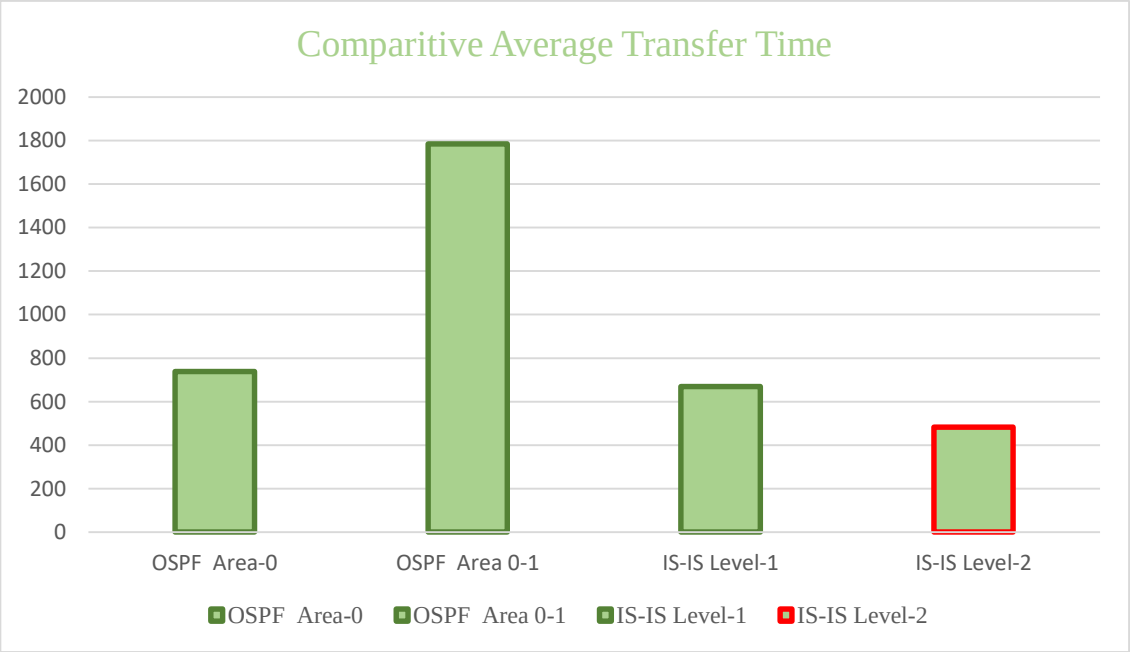


Figure 5. 9: Comparative Analysis - Average Transfer Time

Figure 5.9 demonstrated the overall comparison of OSPF Area 0 & Area 0-1, IS-IS Level-1 & Level-2 with regard to the Average Transfer Time/ Second. After conducting a comprehensive results, it has been found that IS-IS Level – 2 (483.092/Sec) required lesser time than all of the remaining i.e. OSPF with Area 0 – 737.599, OSPF with Area 0 – 1, 1784.12 and IS-IS Level-1, 668.567. It is valuable to added there the IS-IS Level-2 is also slightly less than OSPF.

5.5.2. COMPARATIVE ANALYSIS – Average Transfer Rate

COMPARISON AVERAGE TRANSFER RATE				
Test Beds	**OSPF Area-0**	**OSPF Area 0-1**	**IS-IS Level-1**	**IS-IS Level-2**
Result Obtain	**5423**	**2242**	**5983**	**8280**

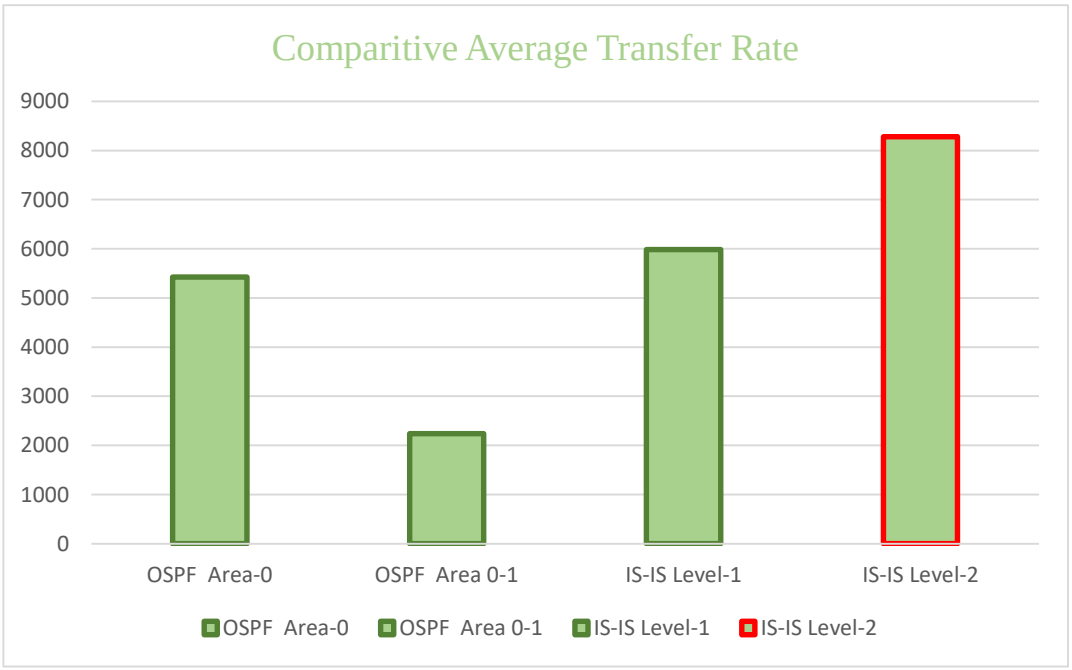


Figure 5. 10: Comparative Analysis - Average Transfer Rate

Figure 5.10 expressed the overall comparative analysis of OSPF Area 0 & Area 0-1, IS-IS Level-1 & Level-2 with regard to the Average Transfer Rate/ Second. After conducting results in this regard, it has been observed that IS-IS with Level – 2 contains high Average Data Transfer Rate (8280/Sec) than others i.e. OSPF with Area 0 (5423), OSPF with Area 0 – 1, (2242) and IS-IS Level-1 (5983). IS-IS with Level-1 hold the second place in this context.

5.5.3. COMPARATIVE ANALYSIS – Average Bandwidth Utilization in %

COMPARISON AVERAGE TRANSFER RATE				
Test Beds	**OSPF Area-0**	**OSPF Area 0-1**	**IS-IS Level-1**	**IS-IS Level-2**
Result Obtain %	**0.43**	**0.18**	**0.48**	**0.66**

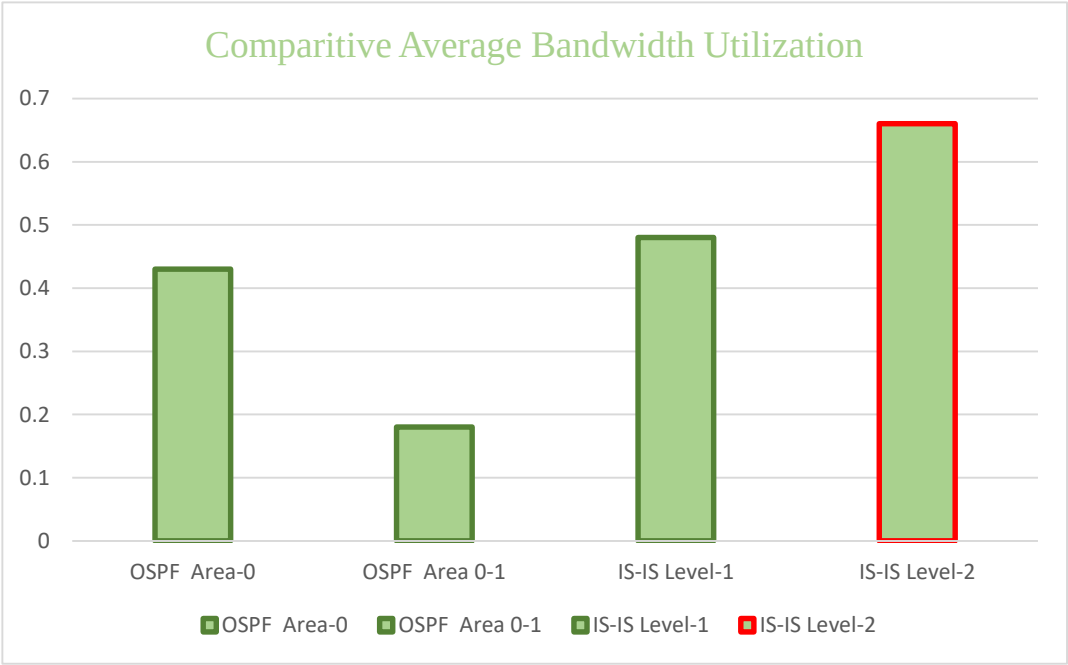


Figure 5. 11: Comparative Analysis – Average Bandwidth Utilization in %

Figure 5.11 demonstrated overall comparison of the results of OSPF Area 0 & Area 0-1, IS-IS Level-1 & Level-2 with regard to an Average Bandwidth Utilization in Percentage (%). The analysis shown that the percentage of an Average Bandwidth Utilization of IS-IS Level – 2 (0.66 %) is higher than the others i.e. OSPF Area 0 (0.43 %), OSPF with Area 0 – 1 (0.18 %) and IS-IS Level-1 (0.48 %). IS-IS with Level-1 having the second position again in this case.

CHAPTER # 6

6. CONCLUSION

After conducting a thorough experimental test beds, it has been observed that IS-IS (Intermediate System to Intermediate System) is the best choice within the category of link state protocols over the MPLS domain. As IS-IS runs over layer-2 and OSPF works on layer-3 therefore the performance of IS-IS is better than OSPF with respect to Encapsulation and Fragmentation. Moreover, OSPF relies on IP fragmentation for large LSAs whereas IS-IS runs directly over L-2. Both of the Link State Protocols i.e. OSPF and IS-IS support two level hierarchy of the areas but OSPF's area falls within the router whereas IS-IS area exists on links. Routers calculate the SPF (Shortest Path First) per area in case of OSPF whereas IS-IS does not perform the same. Due to these facts the processing of CPU is less required for IS-IS instead of OSPF. Open Shortest Path First utilizes multistate process to synchronize database among its neighbors where IS-IS uses its regular flooding techniques to synchronize its neighbors. Furthermore, LSP update in IS-IS put into a single container and sent to its neighbor which also make it more efficient over OSPF.

6.1.FUTURE WORK

Integration with the features and applications of MPLS, Link State Protocols like IS-IS (Intermediate System to Intermediate System) and OSPF (Open Shortest Path First) are much strengthen and preferred to be the best option for ISP (Internet Service Provider) or Enterprise Network Infrastructure to govern the eminence of communication from source to destination. In MPLS Domain LSP (Link State Protocols) could also be utilized in SDN (Software Defined Network) which is an emerging and today's technology of any Network Infrastructure Environment. As per the Cisco publishing, IoT (Internet of Things), network nodes and objects would be raised exorbitantly high till the end of 2019. LSP (Link State Protocols) would be used to enhance the performance of enterprise network communications.

CHAPTER # 7

7. REFERENCES

[1] - J. Lv, X. Wang, M. Huang, F. Li, K. Li and H. Cheng, "Accomplishing Information Consistency under OSPF in General Networks," 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Wuhan, 2016, pp. 278-285.

[2] - P. Anu and S. Vimala, "Optimization of OSPF LSA flooding process using clustering technique," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-5.

[3] - S. R. Javid and S. K. Dubey, "Implementing OSPFv3 in IPv6 network," 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, 2016, pp. 580-584.

[4] - V.Vetriselvan, Pravin R.Patil, M.Mahendran, "Survey on the RIP, OSPF, EIGRP Routing Protocols", IJCSIT Vol. 5, No. 2, pp 1058-1065, 2014.

[5] - Z. Luo and C. Suh, "An analytical model for evaluating spanning tree based layer 2 routing schemes," 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, 2016, pp. 527-531.

[6] - Y. Zhao, Y. Liu, C. Hai and R. Sa, "Research on the Conformance Testing of the IS-IS Routing Protocol On TTCN-3," 2009 International Conference on Computational Intelligence and Software Engineering, Wuhan, 2009, pp. 1-4.

[7] - Mijeong Yang, Jinho Hahm, Youngsun Kim and Sangha Kim, "Design and implementation of the IS-IS routing protocol with traffic engineering," 9th Asia-Pacific Conference on Communications (IEEE Cat. No.03EX732), 2003, pp. 1102-1105 Vol.3.

[8] - B. Fortz and M. Thorup. Optimizing OSPF/IS-IS weights in a changing world. IEEE Journal on Selected Areas in Communications, 20(4):756– 767, 2002.

[9] - Tran Cong Hung; Le Quoc Cuong; Tran Thi Thuy Mai, "A study on Any transport over MPLS (AToM)," Advanced Communication Technology (ICACT), 2010 The 12th International Conference on, vol.1, no., pp.64, 70, 7-10 Feb. 2010.

[10] - Rick Gallaher, “MPLS Training Guide: Building Multi-Protocol Label Switching Networks,” Syngress Publishing, 2003.

[11] - Lancy Lobo, Umesh Lakshman, “MPLS Configuration on Cisco IOS,” Cisco Press, 2005.

[12] - H. H. Liu, S. Kandula, R. Mahajan, M. Zhang, and D. Gelernter. Traffic engineering with forward fault correction. In Proceedings of the 2014 ACM Conference on SIGCOMM, SIGCOMM ’14, pages 527–538, New York, NY, USA, 2014. ACM.

[13] - Muhammad Adeel, Saquib Javed, Ahsan A.Chaudhry, M.H.Zaidi, Waqar Mahmood, Ahmad A.Iqbal, NUST Institute of Information Technology, A Comparative analysis of Routing Protocols in GMPLS Pakistan, IEEE 2005

[14] - Badran, H.F., "Service provider networking infrastructures with MPLS," Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on, vol., no., pp.312, 318, 2001.

[15] - Xipeng Xiao, Lionel Ni, Reducing Routing Table Computation Cost in OSPF, IEEE 1999

[16] - Franck Le and Joao Luis Sobrinho, Interconnecting Routing Instances, IEEE/ACM Transactions on Networking, April 2014

[17] - Chandra Wijaya, Indonesia, Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPV4 and IPv6 Network, 2011 First International Conference on Informatics and Computational Intelligence

[18] - Liangxu Sun, Jiansheng Wu, Yujun Zhang and Hang Yin, 'Comparison between physical devices and simulator software for Cisco network technology teaching', 2013 8th International Conference on Computer Science & Education, 2013.

[19] - R. Emiliano and M. Antunes, "Automatic network configuration in virtualized environment using GNS3," 2015 10th International Conference on Computer Science & Education (ICCSE), Cambridge, 2015, pp. 25-30.

[20] - P. Gil, G. Garcia, A. Delgado, R. Medina, A. Calderon and P. Marti, 'Computer networks virtualization with GNS3: Evaluating a solution to optimize resources and achieve a distance learning', 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, 2014.

[21] - Cisco, 'Cisco', 2016. [Online]. Available: http://www.cisco.com. [Accessed: 17- Oct- 2016].

[22] - Sllame and M. Jafaray, 'Using Simulation and Modeling Tools in Teaching Computer Network Courses', 2013 International Conference on IT Convergence and Security (ICITCS), 2013.

[23] - GNS3, 'Download GNS3', 2016. [Online]. Available: https://www.gns3.com/software/download/. [Accessed: 17- Oct- 2016].

CHAPTER # 8

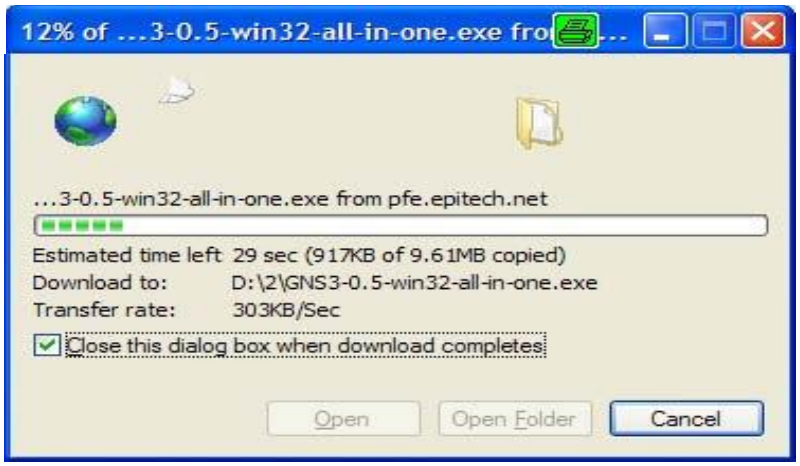
APPENDIX

A - GNS3 Quick Installation for Windows

Step 1:- Download GNS3

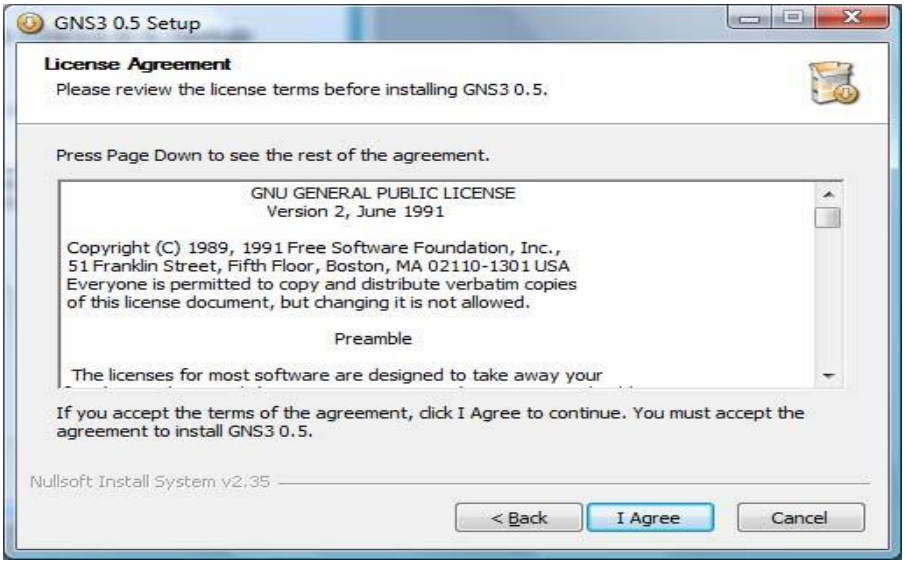
Click Save Button to Download the exe File.

Download will begin after couple of seconds, depending upon the speed of your internet device.

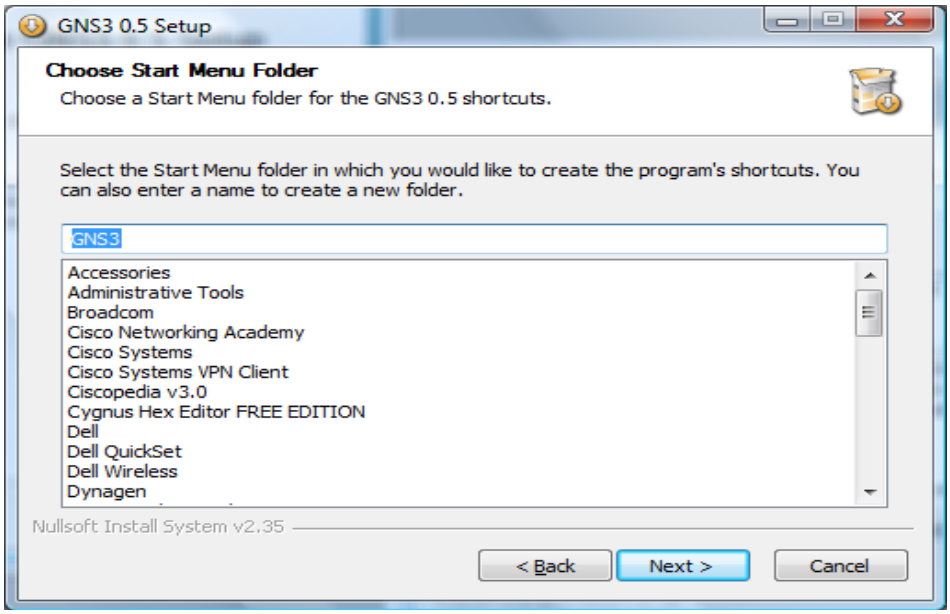


Find the downloaded file and double click on it to begin installation of GNS3. The GNS3 setup wizard will begin. Click the Next Button

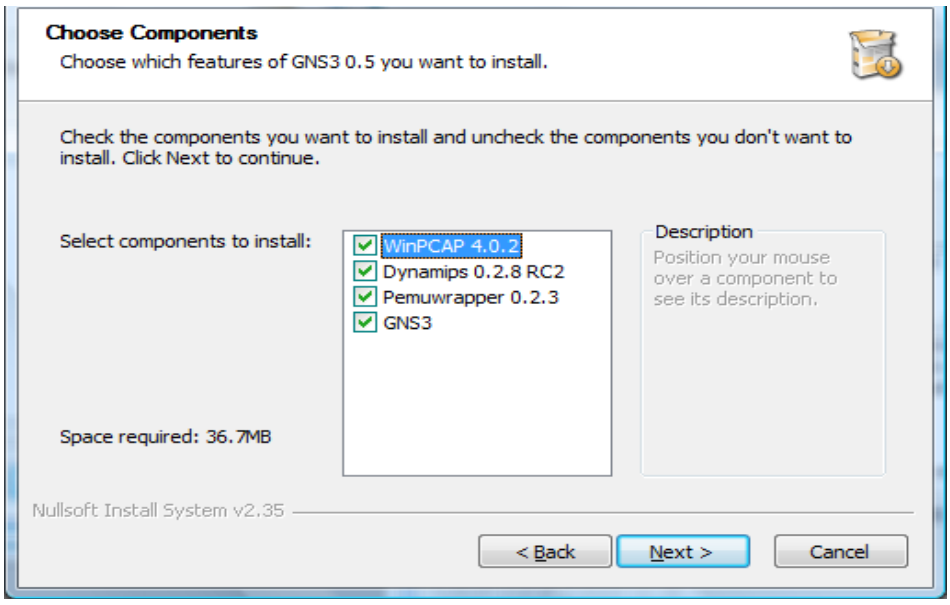
Clink I Agree Button to Continue Installation of GNS3.



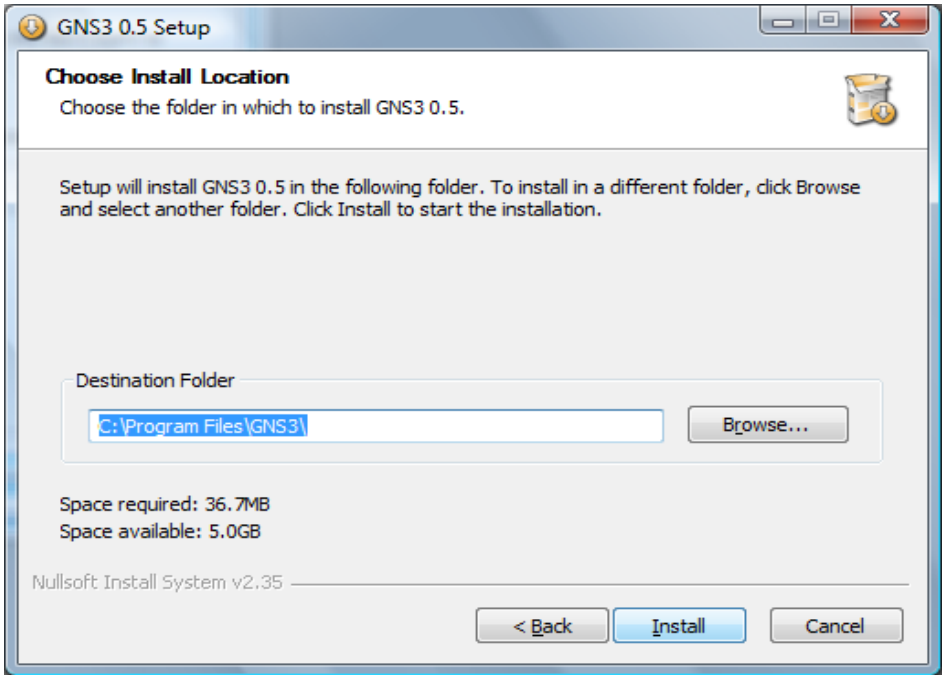
Allow GNS3 to create a Start Menu folder with the default name GNS3 by clicking the *Next* button.



These components along with GNS3 are all chosen by default for installation, so just click the *Next* button to continue.

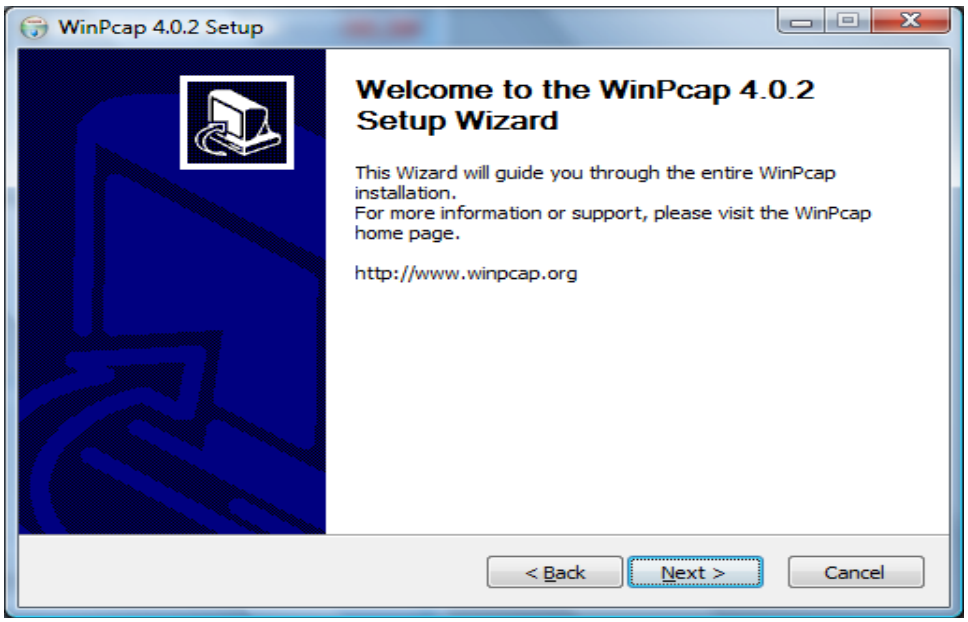


A default location is chosen for GNS3. Click the *Install* button to accept the default location and to begin the actual installation of files.

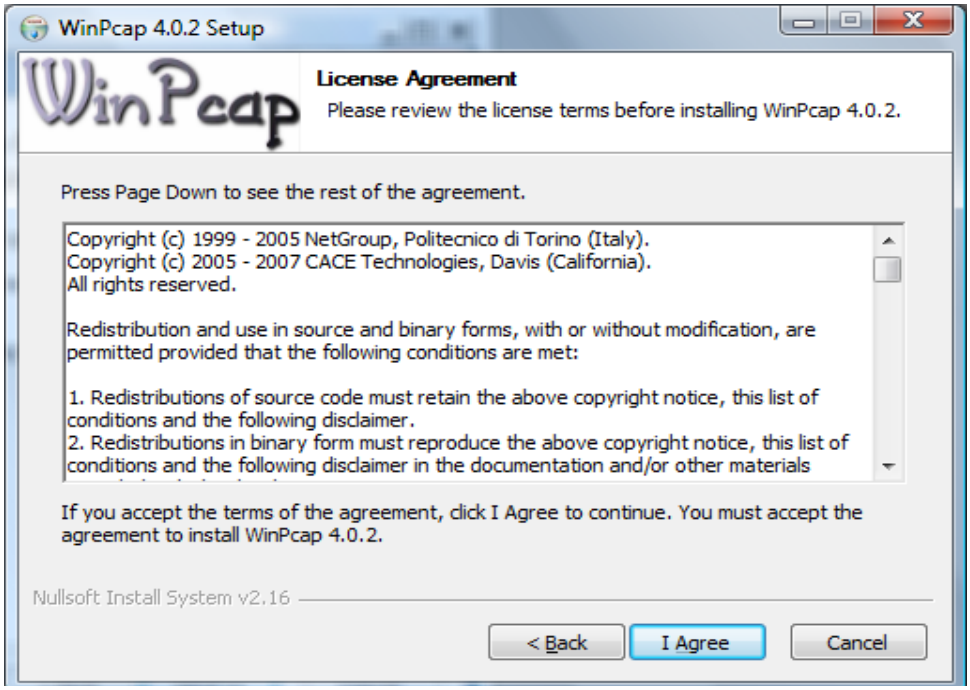


The first dependency for GNS3 is WinPcap. Click the *Next* button to begin the WinPcap Setup Wizard.

Click *I Agree* to accept the License

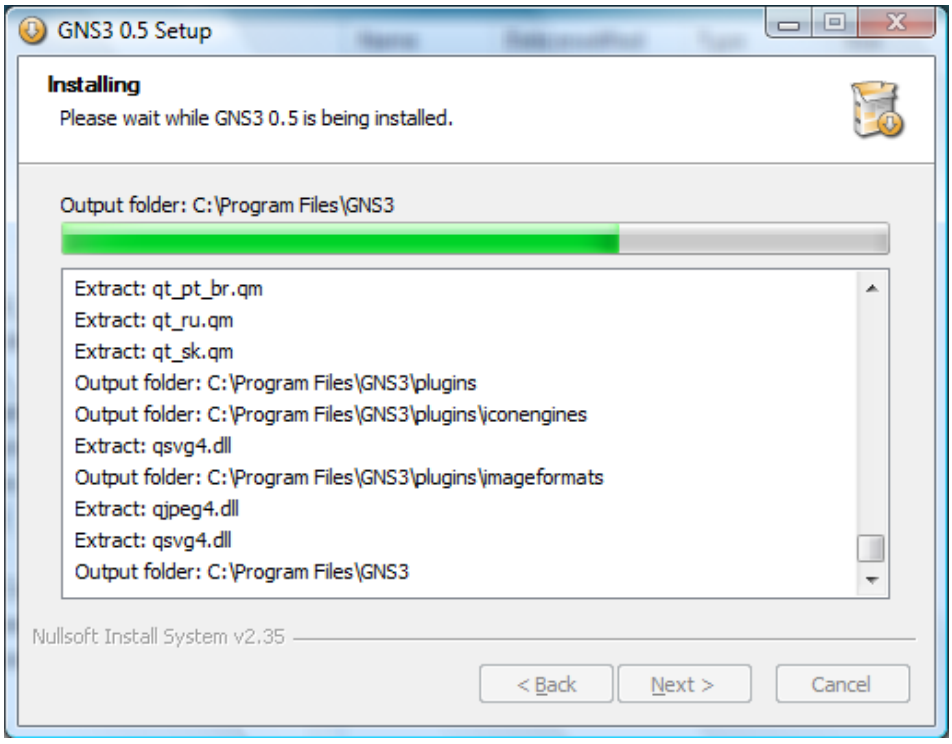


Agreement for WinPcap.

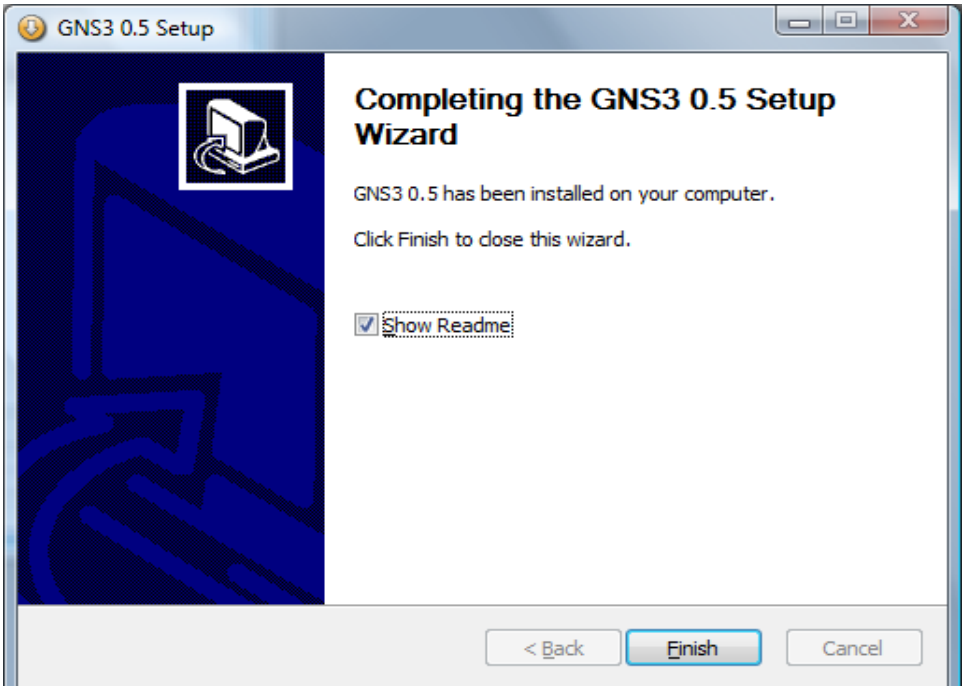


After WinPcap is installed, the GNS3 Setup Wizard returns to installing GNS3.

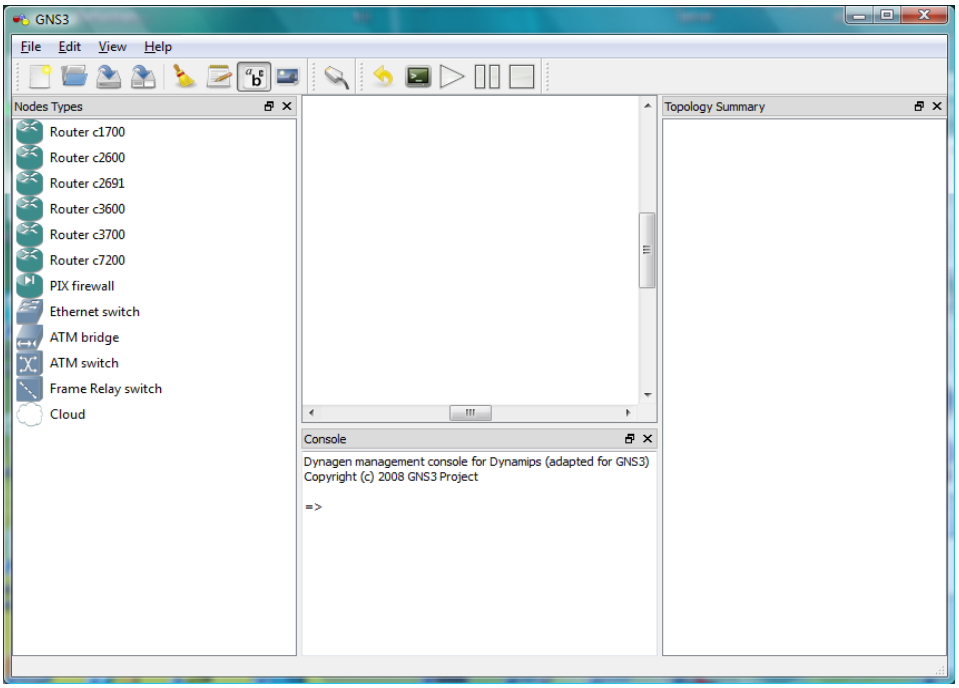
When the wizard finishes, you may



uncheck *Show Readme* and then click the *Finish* button.



You have now completed the installation of GNS3.



As mentioned earlier, you must provide your own Cisco IOS to use with GNS3 due to licensing

issues. GNS3 is meant to be used in a lab environment for testing and learning. Once you have obtained your own copy of a Cisco IOS for one of the supported platforms, you are ready to continue. Current platforms supported include:

B - Detail of Devices' IOS

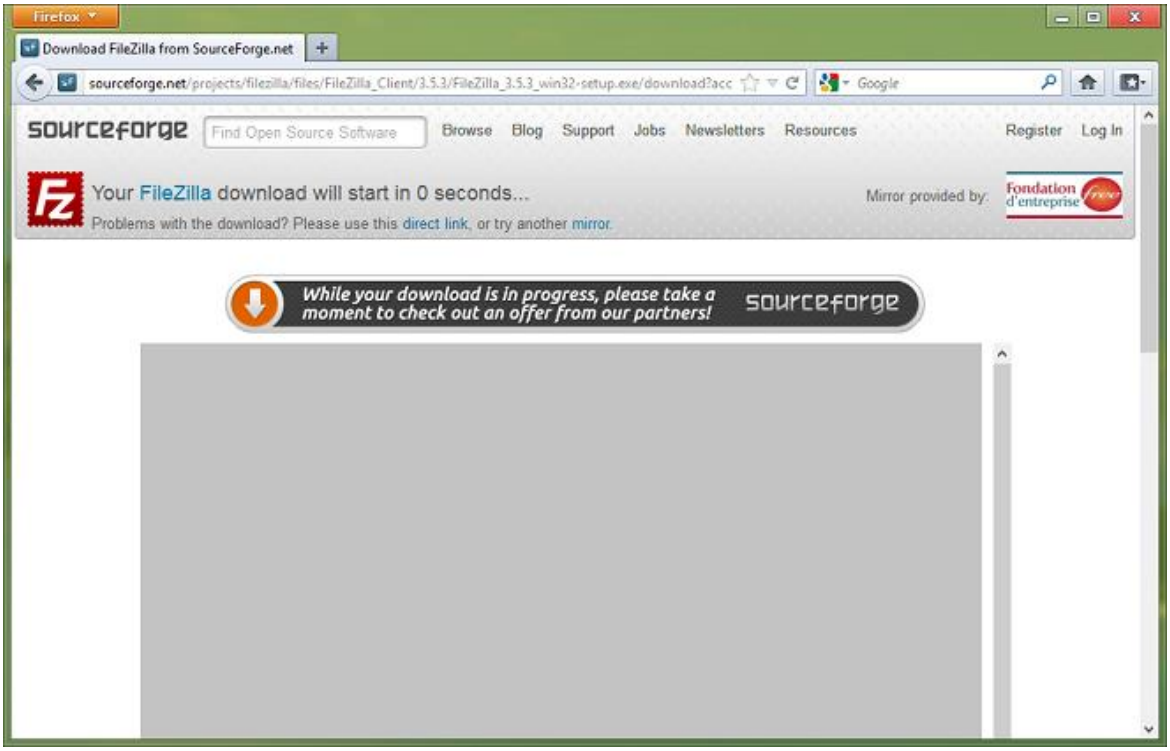
- 1710
- 1720
- 1721
- 1750
- 1751
- 1760
- 2610
- 2610XM
- 2611
- 2611XM
- 2620
- 2620XM
- 2621
- 2621XM
- 2650XM
- 2651XM
- 2691
- 3620
- 3640
- 3660
- 3725
- 3745
- 7200

In this thesis, 7200 series of routers have been used. The configuration has also been made on the same devices' ISO.

C - FileZilla Installation for Windows

Downloading the file

You will now get to a new page which should look something like the picture below:



If the download does not start automatically after a few seconds, click on the link labeled **direct link**. Sometimes the mirror chosen for the download is unavailable. You can select a different mirror by clicking on **Select a different mirror**.

Saving and running

Depending on which browser you are using you will (normally) see a window where you can decide what to do with the file you are downloading. The easiest way is just to hit run or open and the file will download and then be run. As FileZilla does not contain a software signature/certificate, you might get some warning messages telling you that you are running a potentially dangerous file downloaded from the Internet, but let me assure you, Sourceforge is a reliable download source and it shouldn't be any problem. If you are familiar with how to save the file and would like to do that, go ahead. Just remember to save it where you can easily find it afterwards and then open it from there :) On Windows Vista, 7 or 8, you might need to confirm an additional UAC prompt to start the installer.

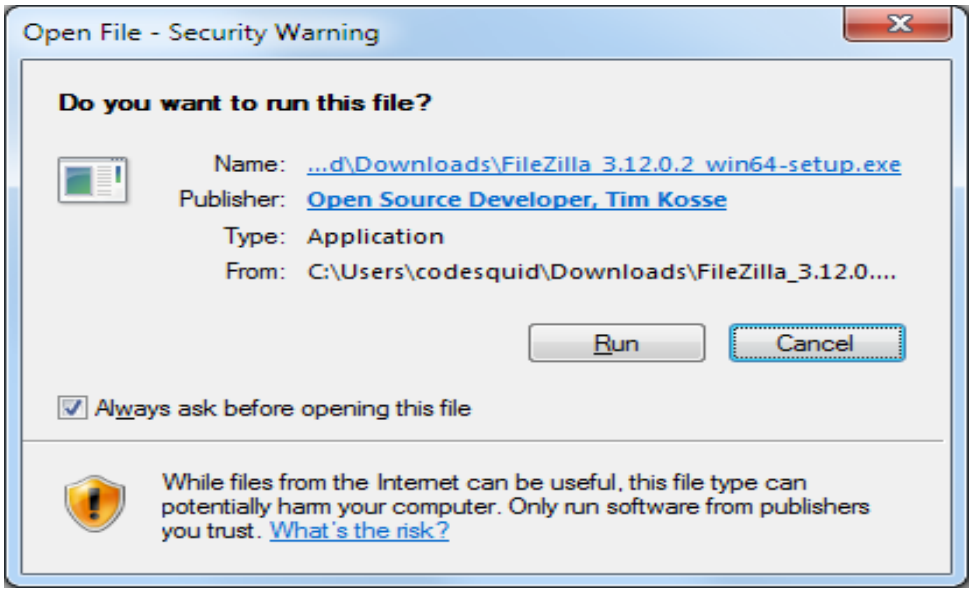
Hopefully after the file downloads you will have started the FileZilla installer if you went for the installer version or opened the zip file in a zip program for any other version. In the next section I'll help you through the installation process.

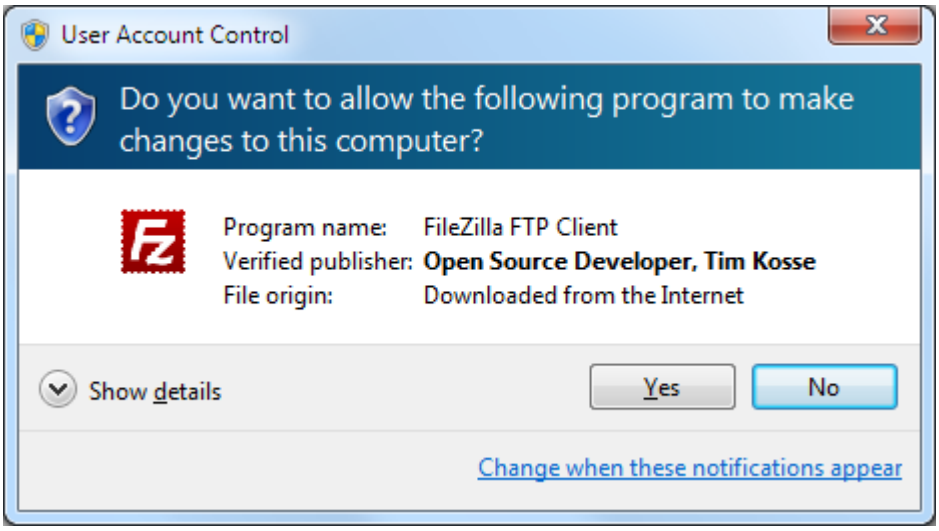
Installing on Windows with installer version

Please note: All screenshots are from Windows 8. Yours may look different, but the functionality is the same. Make sure that the user account which is being used for the installation has administrative rights that allow the installation of software.

Possible Confirmation prompts

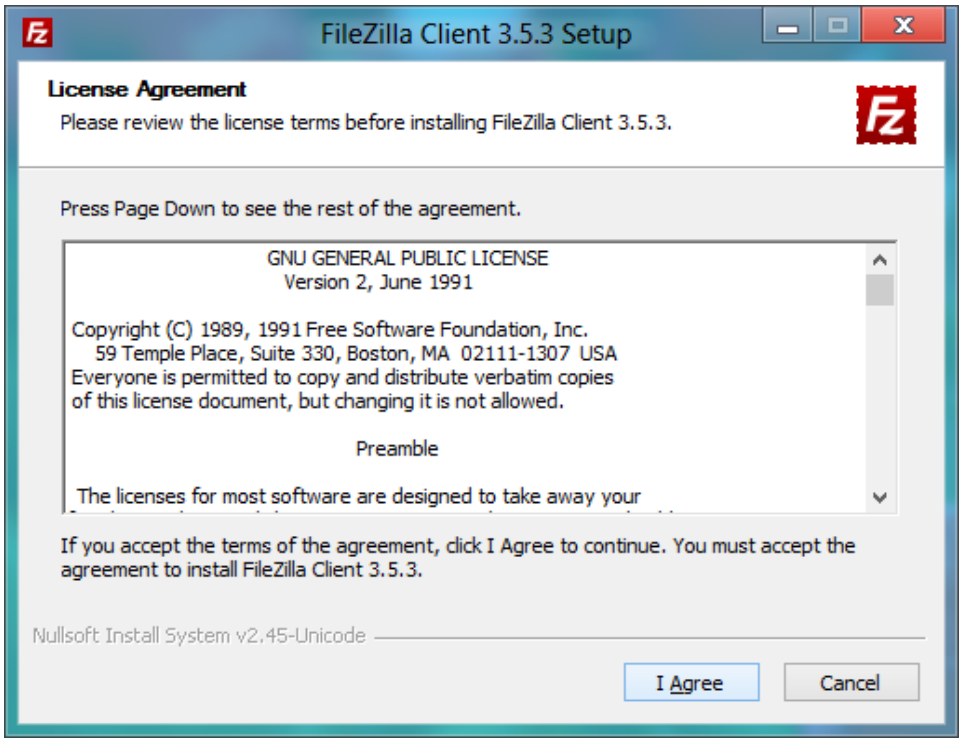
Depending on OS settings and version, it is possible that one or both of the following confirmation prompts appear:


Open File - Security Warning
Do you want to run this file?
Name: ...d\Downloads\FileZilla_3.12.0.2_win64-setup.exe
Publisher: Open Source Developer, Tim Kosse
Type: Application
From: C:\Users\codesquid\Downloads\FileZilla_3.12.0....
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?



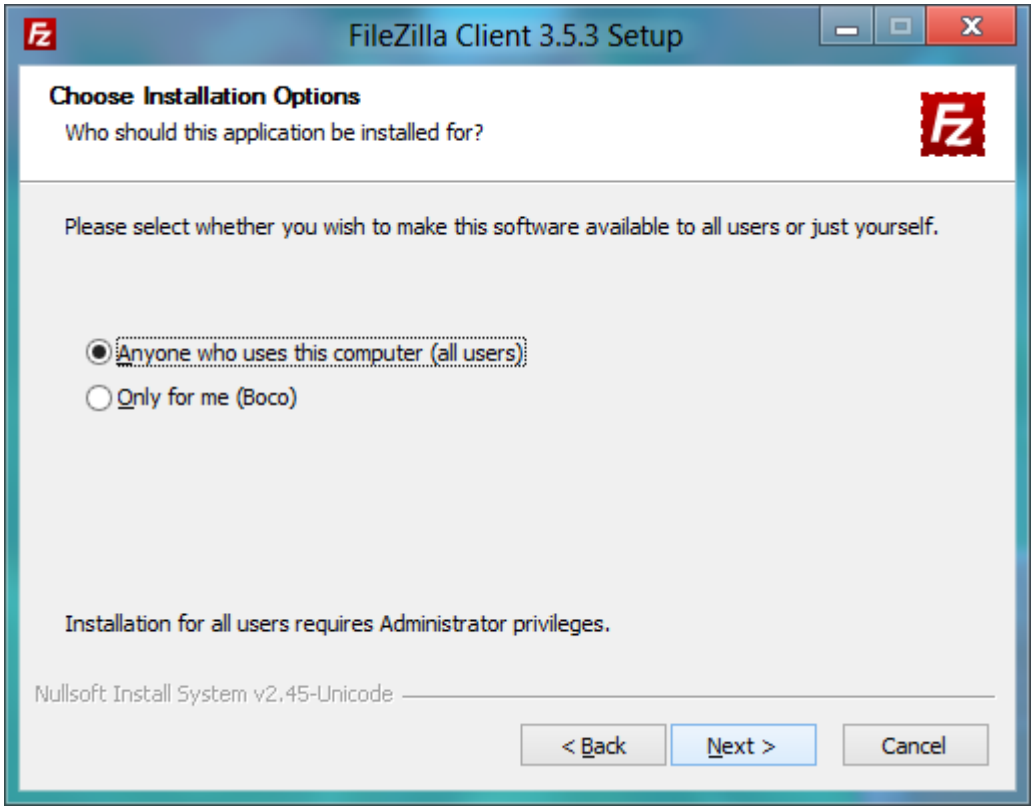
License agreement

Hopefully you should now see the following window where you will have to accept the terms of the license agreement to continue. Read through it and click "I Agree" if you do.



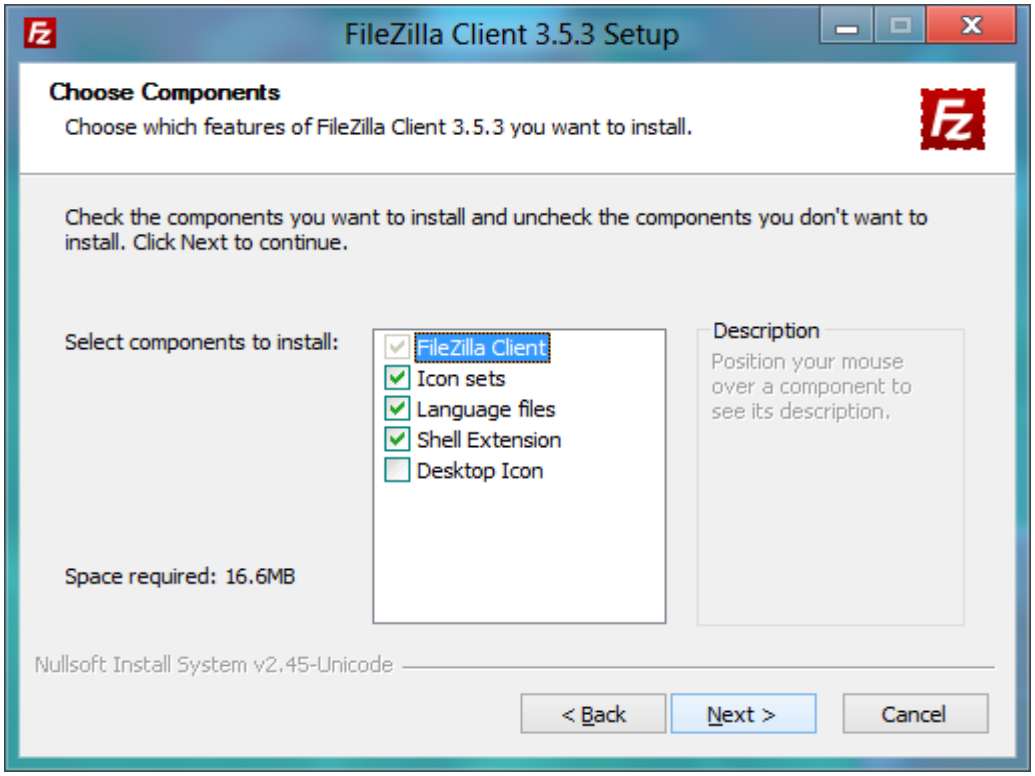
Installing for me or all users?

You will now have to decide if you want to install only for your user account or if FileZilla should be accessible by every user on the machine. This mainly affects where the Start Menu icons are placed. Installing for all users needs administrative privileges, and every user will have his/her own settings.



Choosing components

Next you need to choose which parts of the FileZilla client you want to install. If you hover your mouse over a choice, FileZilla will show you a description of the item. Here is the window:



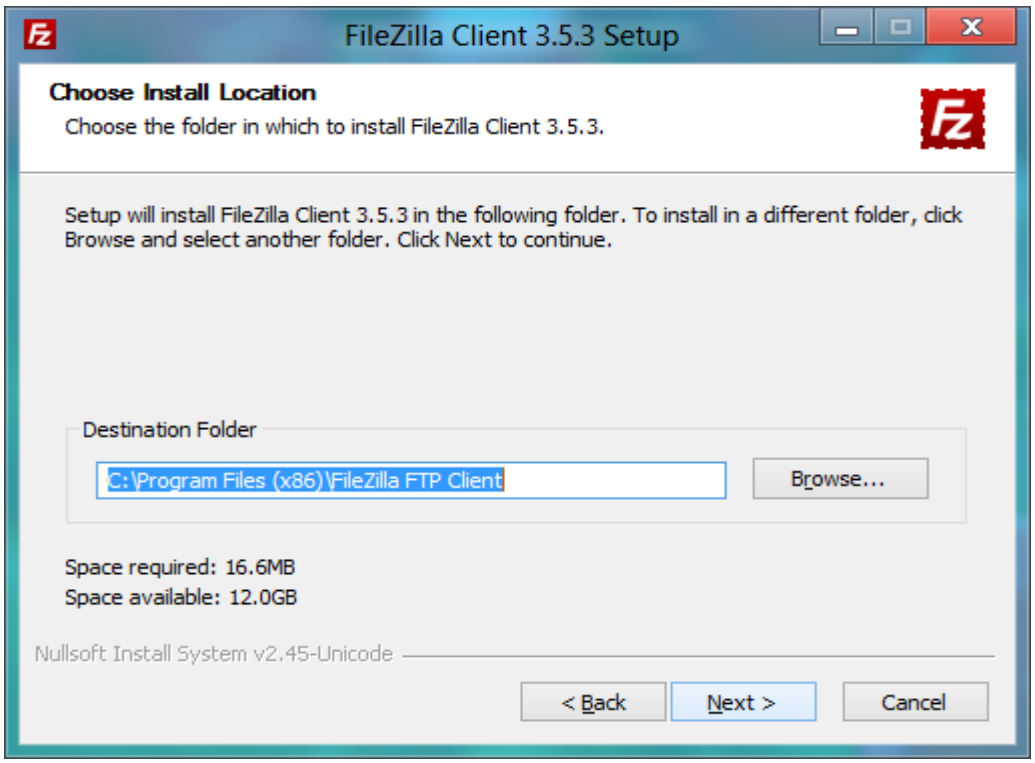
Go through all of them and just check/uncheck the stuff you want. Select additional languages if you want FileZilla in another language than English. Icon sets let you choose different looks for FileZilla's icons (they are partly user contributed). The shell extension integrates FileZilla into the Windows Explorer. Most users will go with what's selected by default here. When you're all finished, click Next.

Two small notes regarding the shell extension:

1. Installing or removing requires full administrative privileges.
2. Though FileZilla for Windows is only available as 32bit build, it contains a shell extension for both the 32bit and 64bit shell.

Install location

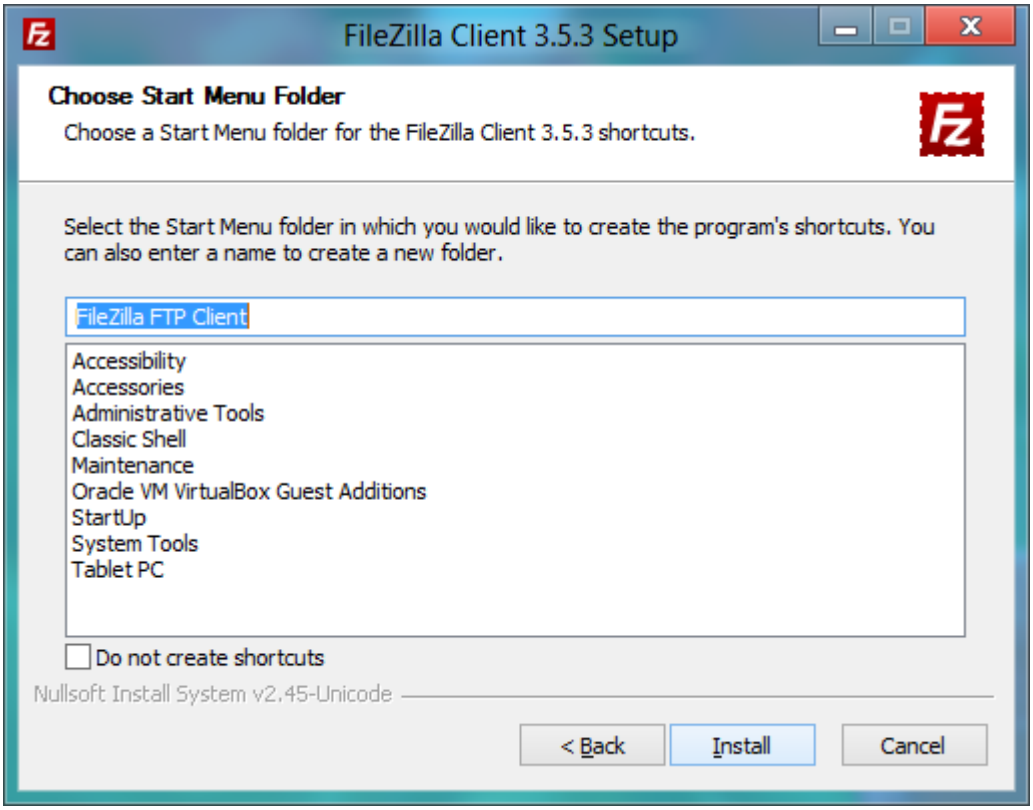
The next window will ask you where to install the program. If you don't have any special needs, click Next.



The default path is to install into your "Program Files" directory on 32bit Windows, and into "Program Files (x86)" on 64bit Windows. Please, if you are migrating from FileZilla 2, do NEVER, EVER install into the same directory as FileZilla 2! FileZilla 3 is not an upgrade to FileZilla 2, and merging both directories creates a mess.

Start menu shortcuts

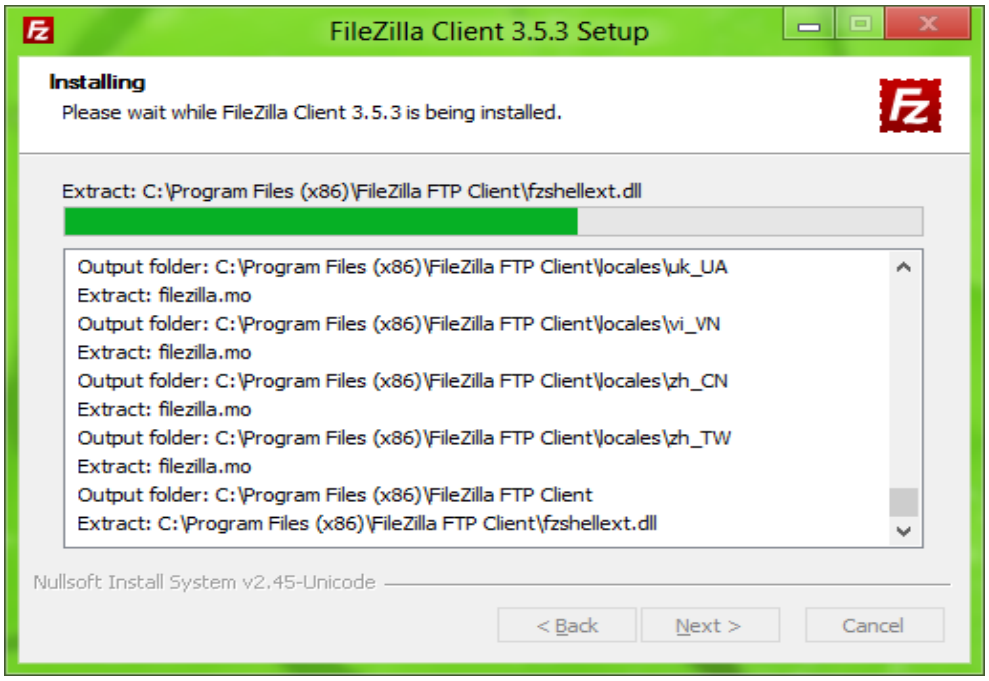
Here, you will be asked what you want to name the folder with the shortcuts to FileZilla inside. The default name "FileZilla FTP Client" should be good for most people. You can also choose not to install these shortcuts.



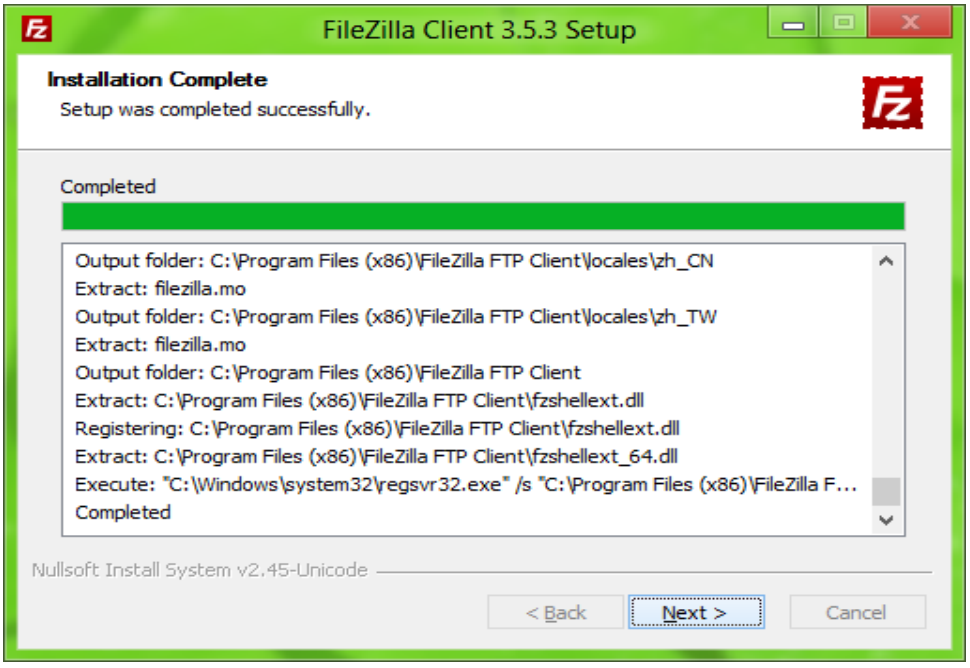
Note to Windows 8 users: In Windows 8, MS has removed the Start Menu, but if you install the one from ClassicShell you will get your Start menu icons back.

Finishing installation

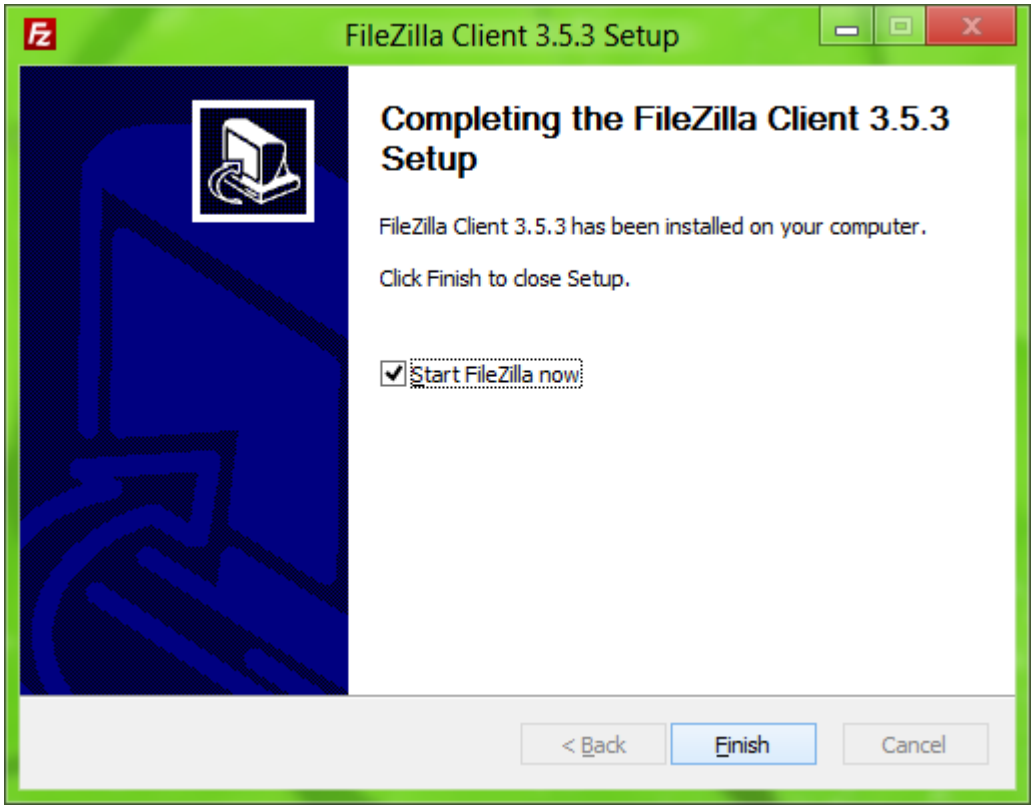
When you click Install, FileZilla will get installed.



If no errors occur it should complete in some seconds.



When it's done, click Next to finish the installation.



Congratulations, you've now successfully installed the FileZilla Client and can now move on to running!