Democratic and Popular Algerian Republic

Ministry of Higher Education and Scientific Research

University SAAD DAHLEB Blida 1

DEPARTMENT: Aeronautics and Space Studies

Thesis of project of end of studies

For obtaining the Master's degree in space telecommunication

Theme

"Study and Analysis of Network System Performance using the OSPF Routing Protocol"

Presented by:

HAOUARI Selma **MAZA Walid**

Supervised by:

Mr. KRIM Mohamed

Promotion 2023/2024

We extend our sincerest appreciation to all those who have stood by us during this academic endeavor.

We are especially grateful to our mentor, **M.KRIM**, for their consistent guidance, support, and constructive criticism. Their expertise and motivation have been instrumental in the successful completion of this thesis.

Furthermore, we are thankful to our parents for their unwavering love, encouragement, and belief in our capabilities. Your unwavering support has given us the strength and determination to overcome obstacles.

Lastly, we express our gratitude to our friends for their continuous encouragement and understanding. Your companionship and support have made this journey more bearable and fulfilling.

We are truly thankful for all the help and encouragement we have received

We dedicate this thesis to our beloved parents and dear friend with heartfelt gratitude and love. Your support, encouragement, and sacrifices have been crucial in our academic and personal growth.

The love, patience, and belief from our parents have given us the courage to chase our dreams and the strength to face challenges. To my friend, your friendship, encouragement, and support have made tough times easier and good times even better.

Thank you for being my sources of strength and motivation.

With love and deepest appreciation.

Abstract

This thesis addresses the optimization of OSPF within network infrastructures, focusing on a specific network's challenges. It proposes enhancements to reduce latency, optimize routing efficiency, and lower OSPF operational costs. Using Cisco Packet Tracer, a new network layout is designed and evaluated to align with OSPF best practices, demonstrating improved performance and reliability in Internet Exchange Point (IXP) environments.

Keywords: network systems, OSPF protocol, OSPF optimization, Cisco Packet Tracer.

ملخص

تتناول هذه الأطروحة تحسين بروتوكول التوجيه الأقصر المفتوح أولاً داخل البنية التحتية للشبكات، مع التركيز على تحديات شبكة معينة. تقترح تحسينات لتقليل زمن الانتقال، وتحسين كفاءة التوجيه، وخفض تكاليف التشغيل للبروتوكول. باستخدام برنامج تتبع الحزم، تم تصميم وتقييم تخطيط جديد للشبكة ليتماشى مع أفضل ممارسات البروتوكول، مما يظهر أداءً وموثوقية محسنة في بيئات نقاط تبادل الإنترنت.

الكلمات المفتاحية: أنظمة الشبكات، بروتوكول التوجيه الأقصر المفتوح أولاً، تحسين بروتوكول التوجيه الأقصر المفتوح أولاً، برنامج تتبع الحزم.

Résumé

Cette thèse aborde l'optimisation d'OSPF au sein des infrastructures réseau, en se concentrant sur les défis d'un réseau spécifique. Elle propose des améliorations pour réduire la latence, optimiser l'efficacité du routage et réduire les coûts opérationnels OSPF. En utilisant Cisco Packet Tracer, une nouvelle disposition de réseau est conçue et évaluée pour s'aligner avec les meilleures pratiques OSPF, démontrant des performances et une fiabilité améliorées dans les environnements IXP (Internet Exchange Point).

Mots Clés : systèmes réseaux, Protocole OSPF, OSPF optimisation, Cisco Packet Tracer.

Chapter I Introduction to Network Fundamental

Chapter II Understanding Routing: Key Protocols and Concepts

Chapter III OSPF Fundamentals and Applications

Chapter IV OSPF Optimization: Strategies for Improved Network Routing

PAN	Personal Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
OSI	Open Systems Interconnection
ISO	International Organization for Standardization
MAC	Media Access Control Address
LLC	Logical Link Control
DLL	Data Link Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
DAPRA	Defense Advanced Research Projects Agency
IP	Internet Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
OSPF	Open Shortest Path First
IGMP	Internet Group Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SMTP	Simple Mail Transfer Protocol
FTP	File Transfer Protocol
SSH	Secure Shell
HTTP	The Hypertext Transfer Protocol
DOD	Department of Defense
IGP	Interior Gateway Protocol
EGP	Exterior Gateway Protocol
RIP	Routing Information Protocol
AS	An Autonomous System

OSPF	Open Shortest Path First protocol
BGP	Border Gateway Protocol
IRP	Interior Routing Protocol
IS IS	Intermediate System to Intermediate System
AD	Administrative Distance
VLSM	variable length subnet masks
LSA	link-state advertisement
LSDB	link state database
SPF	Shortest Path First
IETF	Internet Engineering Task Force
RFC	Request for Comments.
BDR	Backup Designated Router
ID	Identifier
P2P	Point To Point
RID	Router Identifier
RFID	Radio Frequency Identification
P2MP	Point to Multipoint
ECMP	Equal cost multipath
DR	Designated Router
IR	Internal Router
ABR	Area Border Router
ASBR	Autonomous System Boundary Router
NSSA	Not So Stubby Areas

LSR	Link State Request
LSU	Link State Update
DBD	Database Description
LSA ck	Link-State Acknowledgment
BMA	Broadcast Multi Access
DR	Designated router
NBMA	Non-Broadcast Multi Access
NAT	Network Address Translation
ISP	Internet Service Provider
IXP	Internet Exchange Point
CPU	Central Processing Unit
IOS	Inter network Operating System
EIGRP	Enhanced Interior Gateway Routing Protocol
MD5	Message Digest Algorithm 5
PING	Packet Internet Groper
TTL	Time to Live
I/O	Input/output
NSFNET	National Science Foundation Network
ARPANET	Advanced Research Projects Agency Network
MTU	Maximum Transmission Unit

In the rapidly evolving world of digital communication, understanding the intricacies of network structures and protocols is paramount. This thesis aims to explore and optimize network performance through a detailed examination of network fundamentals, routing mechanisms, and the Open Shortest Path First (OSPF) protocol.

To begin, networks are defined as interconnected devices, each possessing a unique address. These networks are categorized based on their geographical scope into Personal Area Networks (PANs), Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs). Various network topologies, such as mesh, star, bus, and ring, along with key devices like routers, switches, hubs, and gateways, will be discussed to provide a foundational understanding.

An overview of layered network architectures, specifically the OSI and TCP/IP models, offers a framework for understanding how networks facilitate communication. Routing, a critical concept within network communication, involves determining optimal paths for data packets. This thesis covers the types of routing and the roles of Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs), examining key elements such as routing tables and convergence. Prominent routing protocols, including Distance Vector protocols (e.g., RIP) and Link State protocols (e.g., OSPF), are analyzed.

The focus then shifts to OSPF (Open Shortest Path First), a pivotal protocol in network communication. Detailed insights into OSPF's characteristics, including its metric system and zone segmentation, enhance understanding of network administration. OSPF's capabilities for quick network convergence and robust security measures to protect against unauthorized access are highlighted. Evaluating the advantages and disadvantages of OSPF aids in informed decision-making for network configuration.

This exploration concludes with a practical aspect of network enhancement through the revamp of an existing structure to optimize OSPF performance. Identifying challenges in the initial network setup, a new layout is presented aimed at reducing latency, streamlining routing, and lowering OSPF costs. Comprehensive evaluation demonstrates that the new layout adheres to OSPF best practices and significantly improves network efficiency.

Together, these elements provide a thorough understanding of network fundamentals, routing mechanisms, the intricacies of OSPF, and practical strategies for network optimization. This knowledge is essential for professionals and enthusiasts aiming to enhance their network infrastructure and ensure efficient and secure data communication.

Chapter I:

Introduction to Network Fundamentals

I. Introduction

A network is created when a group of devices communicate with each other using interconnected links. Each device, known as a host, has its own unique address. In the initial chapter, we delve into networks from a theoretical perspective, categorizing them based on their scope and geographical area as PANs, LANs, MANs, and WANs. In order to understand how the network functions, we delve into the various network topologies (mesh, star, bus, and ring configurations) and highlight the crucial role played by network devices such as routers, switches, hubs, and gateways in their implementation.

Networks employ layered architectures like the OSI and TCP/IP models to facilitate communication. In the following chapter, we offer a comprehensive explanation of the role played by each layer and protocol, finally comparing the two models.

I.1 Network Definition

A network is nothing more than two or more nodes connected by a cable or by a wireless radio connection, a node can be a computer, printer or any other device that can send and receive data from other nodes on the network.

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security. **[1]**

I.2 Types of Networks

The size, scope, and number of machines (or devices) in a network are key factors in determining the category it falls into.

The following Figure I-1 presents the various types of networks

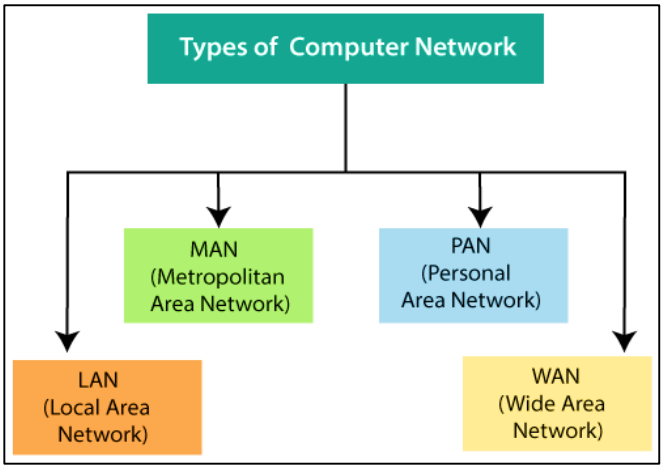

Figure I-1Types of Networks

I.2.1 Personal Area Network

Let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals .PANs can be built with technologies that communicate over short ranges, such as RFID on smartcards, library books, and Bluetooth. **[2]**

I.2.2 Local Area Network

The coverage area of a LAN is limited to a few hundred meters to a kilometer at most, such as home, office, or school, etc. It used to connect computers and other devices to share resources like printers, files, and services. LANs can be considered private networks if their access is restricted.

I.2.3 Metropolitan Area Network

A network that covers a larger geographical area (several km to 10 km) it used to connect local area networks (LANs) and offer fast networking services. Educational Institutions, large corporations, and services to exchange communication and data sharing processes utilize MANs.

I.2.4 Wide Area Network

Wide-area networks can cover great geographical distances (several km to 100 km or more). They are designed to connect devices and different local networks in different cities, regions, states, or countries using high-speed solutions or telephone lines.

I.3 Categories of Topologies

Network topology shows how computer units are connected in a network. It includes nodes (devices) and links (connections). There are four fundamental topologies that can be employed: mesh, bus, star and ring.

I.3.1 Mesh Topology

The mesh topology is a highly interconnected network where all the devices are linked to one another by point-to-point connections.

This topology ensures reliability, robustness, redundancy, parallel communication, and easy fault identification and isolation, making it ideal for long-distance communication scenarios where reliability and performance are crucial. It also provides security by preventing physical boundaries from allowing access to messages. Mesh topologies have disadvantages due to the high cabling and I/O ports, which make installation and reconnection difficult and require space that is more physical and prohibitively expensive hardware.

Figure I-2 represents a structure of mesh topology where devices are interconnected with multiple redundant paths between them:

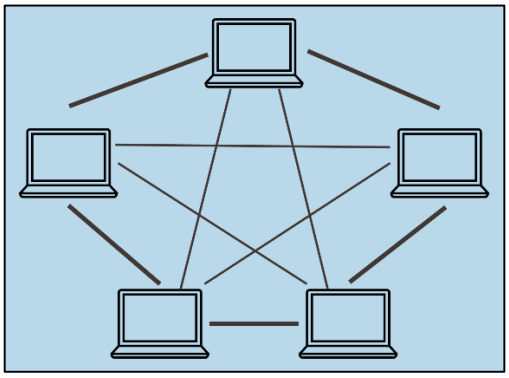

Figure I-2 Mesh Topology

I.3.2 Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called hub **[1].** A star topology is less expensive than the mesh topology due to its single link and I/O port for each device, making it easy to install, reconfigure, and handle

additions, moves, and deletions. The hub's robustness allows for easy fault identification and isolation.

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead**. [1]**

The following figure represent a centralized structure of star topology:

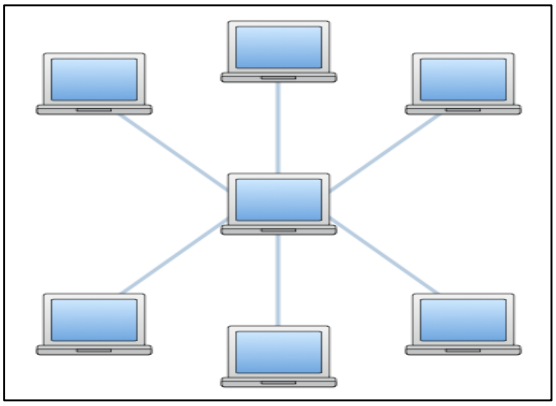

Figure I-3 Star Topology

I.3.3 Ring Topology

In ring networks, two other devices connect each device to form a circular configuration. The signal moves in a single direction through this ring, passing through every device on the way to its destination. It allows for fault isolation and communication, with a maximum ring length and number of devices.

Devices are interconnected with their immediate neighbors in a ring network, whenever any device fails, an alarm goes off. On the other hand, unidirectional traffic can have some disadvantages as a break in a simple ring can disable the entire network, which can be addressed by using a dual ring or switch

The Figure I-4 represent an example of ring topology where the 6 devices are connected in a circular manner:

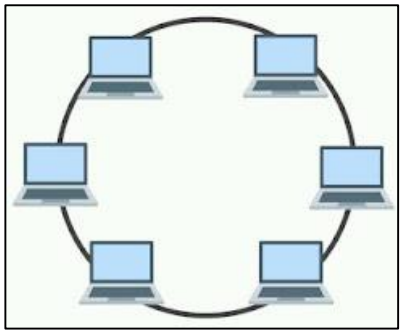

Figure I-4 Ring Topology

I.3.4 Bus Topology

Alternatively called line topology, is a network setup where each computer and network device is connected to a single cable or backbone. It being less complex than other topologies, it is also useful in labs or classrooms for teaching students new to networking**. [3]**

With its easy installation process, this system uses less cable by requiring a shorter length than both star and ring topologies, which eliminate redundancy as backbone cables can be laid efficiently and connected to nodes through drop lines of various lengths.

Disadvantages of bus systems include difficulty in reconnection and fault isolation; if the main cable is damaged, the entire network will fail; and potential degradation in quality due to signal reflection at taps, which can be controlled by limiting device spacing.

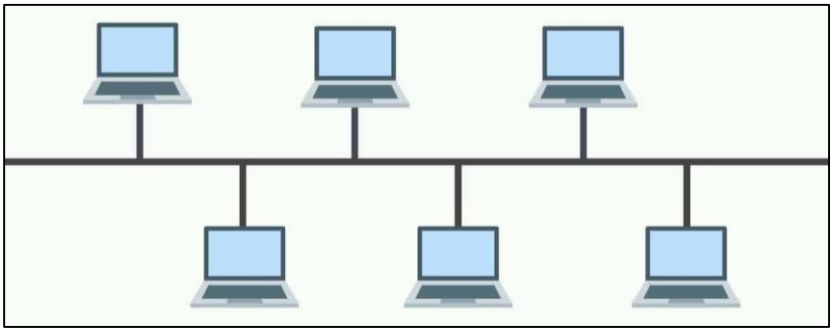

Figure I-5 Bus Topology

I.4 Network Devices

A network device is any form of hardware or software that facilitates communication and connection among computers in a computer network.

I.4.1 Router

A router is a device that operates at the network layer of the ISO OSI Reference Model. What this means is that a router examines network addresses and makes decisions about whether or not data on a local area network should remain on the network or should be transmitted to a different network **[4]**

The actual network protocols used depends on the protocols that router is designed to work with **[5].**

I.4.2 Hub

A hub is a basic networking device that operates at the physical layer of the OSI model. A hub is simply a means of connecting Ethernet cables together so that their signals can be repeated to every other connected cable on the hub. Hubs may also be called repeaters for this reason, but it is important to understand that while a hub is a repeater, a repeater is not necessarily a hub **[6].**

However, because of their limited functionality and the presence of more advanced networking devices such as switches, hubs are less commonly used in modern network setups.

I.4.3 Switch

A switch is a networking device that operates at the Data Link layer (Layer 2) of the OSI model. It was intended to connect various devices within a local area network (LAN) and allow the seamless exchange of data between them.

Unlike hubs, switches have intelligence built into them to prevent devices from receiving all the data being sent on the network, even if it isn't destined for them **[7].**

I.4.4 Gateway

A gateway, also known as a protocol converter, is a networking device or software that serves as a passage to connect two networks operating on different networking models. It acts as a messenger agent, taking data from one system, interpreting it, and transferring it to another system.

I.5 OSI Model

The Open Systems Interconnection (OSI) Model was introduced in 1977 by the ISO, also known as the International Organization for Standardization. The OSI Model was an attempt at creating a standard networking model that is not part of any individual government. The OSI Model has since been used as a networking standard process.

The OSI Model constitutes of seven layers and this system is well known for these comprehensively divided sets of layers. In this model, session and presentation layers were added between the transport and application layers**. [8]**

The structure of the OSI model is represented in Figure I-6

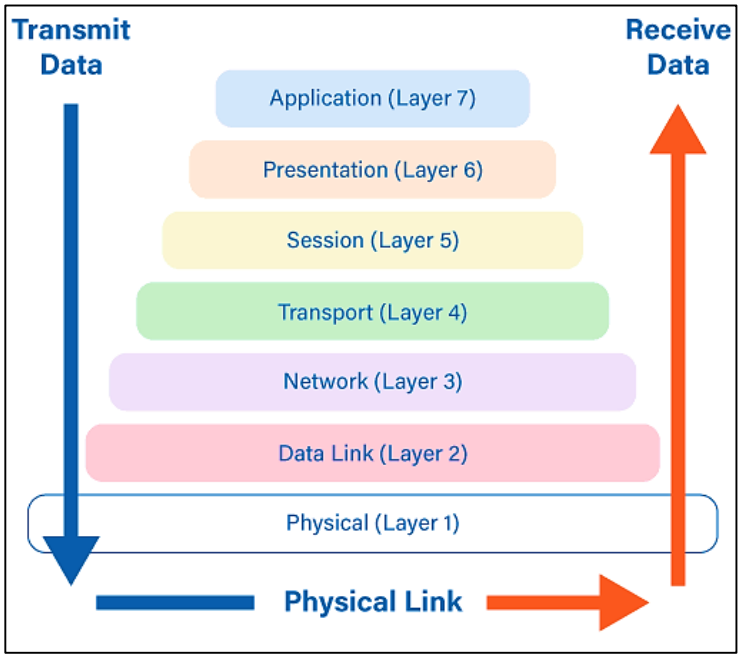

Figure I-6 OSI Model

I.5.1 OSI Model Layers

I.5.1.1 Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together**. [9]**

I.5.1.2 Data Link Layer

The data link layer is the second layer in the OSI model. It provides reliable and error-free transmission of data frames between adjacent nodes over a shared medium. It takes the raw bit stream from the physical layer and arranges it into frames. Additionally, it handles error detection and correction, flow control, and controls access to the shared medium through protocols such as Ethernet. The data link layer is commonly divided into two sub-layers: the Media Access Control (MAC) layer and the Logical Link Control (LLC)

MAC

This layer manages access to the physical network medium, assigns addresses (MAC addresses), and ensures that data packets are transmitted reliably to their destination.

LLC

Logical Link Control (LLC) is a sub layer that generally provides the logic for the data link as it controls the synchronization, multiplexing, flow control, and even error-checking functions of DLL (Data Link Layer**). [9]**

I.5.1.3 Network Layer

The network layer is responsible for transferring data between hosts on separate networks and determining the most efficient route for packet transmission. The sender's and receiver’s IP addresses are placed in the header by the network layer.

I.5.1.4 Transport Layer

The transport layer guarantees dependable and effective transmission of data from one host to another. It divides the received data from the upper layers into smaller segments,

incorporates essential sequencing and error-checking details, and then reconstructs them at the destination.

I.5.1.5 Session Layer

The Session Layer is the fifth layer in the OSI (Open Systems Interconnection) model, it is responsible for establishing, managing, and terminating connections between applications. It provides the mechanism for opening, closing, and managing a session between end-user application processes.

I.5.1.6 Presentation Layer

It is the sixth layer of the OSI model, responsible for representing and formatting data exchanged between networked systems. It ensures data is understood by the receiving system, regardless of format differences. The layer performs functions like data compression, encryption, and decryption for secure and efficient data transfer, it also handles data conversion, syntax, and semantics, ensuring data structure and meaning preservation.

I.5.1.7 Application Layer

The application layer, at the top of the OSI Reference Model stack, facilitates network services and interfaces for applications by implementing standardized protocols and services. Within this layer, data is packaged into messages or packets that are comprehensible to the specific application or service. It manages tasks like data formatting, session management, user authentication, and error handling, defining application-to-application communication frameworks.

I.6 TCP/IP Model

I.6.1 Definition

The TCP/IP model, which stands for Transmission Control Protocol/Internet Protocol model, is a comprehensive suite of communication protocols used to interconnect network devices on the internet and on most local networks. It serves as the foundational communication language of the internet. Developed in the 1970s by the Defense Advanced Research Projects Agency (DARPA), it has become the standard framework for digital network communications. The TCP/IP model consists of four layers. The following Figure I-7 presents how TCP/IP works:

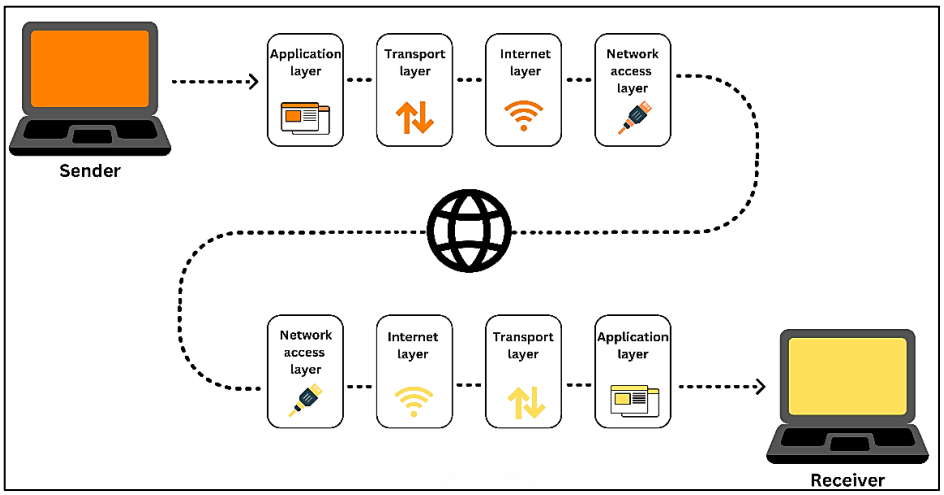

Figure I-7 TCP/IP Layers Model

I.6.2 TCP/IP Layers

I.6.2.1 Network Interface Layer

The Network Interface layer, also referred to as the Network Access layer, is responsible for placing TCP/IP packets onto the network medium and receiving TCP/IP packets from the network medium. TCP/IP was designed to be independent of the network access method, framing format, and medium.

I.6.2.2 Internet Layer

This layer is responsible for host-to-host communication and the routing of data across networks. It is positioned above the Link Layer (Network Interface Layer) and below the Transport Layer in the TCP/IP stack.

The Internet layer is in charge of addresses, directing capacities. The center conventions of the Internet Layer are IP, ARP, ICMP, OSPF, and IGMP**. [10]**

IP

The Internet Protocol is a routable convention in charge of IP addressing, routing, and the fragmentation and reassembly of packets.

ARP

The Address Resolution Protocol is in charge of the determination of the Internet layer location to the Network layer.

ICMP

The Internet Control Message Protocol is in charge of giving symptomatic capacities and reporting mistakes because of the unsuccessful conveyance of IP parcels.

OSPF

Open Shortest Path First is a key routing protocol in the TCP/IP model, operating at the network layer, similar to the Internet layer. It determines the best path for packets to reach their destination, specifically within autonomous systems.

IGMP

The Internet Group Management Protocol is in charge of the administration of IP multicast bunches.

I.6.2.3 Transport Layer

The Transport layer (otherwise the Host-to-Host Transport layer) is in charge of giving the Application layer session and datagram. The main protocols of this layer are TCP and UDP. **[10]**

TCP

Transmission Control Protocol, is one of the core protocols of the Internet Protocol Suite (TCP/IP). TCP is responsible for breaking data into packets, ensuring their reliable delivery, reassembling them at the destination.

UDP

User Datagram Protocol, is another core protocol of the Internet Protocol Suite (TCP/IP). It provides a one-to-one or one-to-many, connectionless, unreliable communications service.

I.6.2.4 Application Layer

The application layer is the scope within which applications create user data and communicate this data to other applications on another or the same host. The applications, or

processes, make use of the services provided by the underlying, lower layers, especially the transport layer, which provides reliable or unreliable pipes to other processes. This is the layer on which all higher-level protocols, such as SMTP, FTP, SSH, and HTTP, operate**. [11]**

SMTP

Is short form for Simple Mail Transfer Protocol, It is an internet protocol that is used to deliver emails from one mail server to another. SMTP helps establish communication between servers and enables email messages to be carried across networks, starting from the sender's email server to the recipient's mail server. It runs on the application layer of the TCP/IP suite of protocols.

FTP

File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions, have different ways to represent text and data, or have different directory structures. All these problems have been solved by FTP in a very simple way.

SSH

SSH, or Secure Shell, is a secure network protocol that facilitates encrypted communication and remote access between computers. Its primary purpose is to guarantee the confidentiality and integrity of data transmitted over untrusted networks.

HTTP

The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative hypermedia information systems. The development of HTTP was initiated by Tim Berners-Lee at CERN in 1989**. [12]**

HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example, by a mouse click or by tapping the screen in a web browser.

I.7 Comparison between OSI Model and TCP/IP Model

The OSI model and the TCP/IP model are two models with distinct conceptual frameworks that are used to understand and explain how network communication protocols work. They are similar in some ways, but they are also different in others, as shown in Table I-1:

OSI Model	TCP/IP Model
It was developed by the International Organization for Standardization (ISO)	Developed by the United States Department of Defense (DOD)
It has 7 layers	It has 4 layers
The OSI Model supports the Vertical approach	TCP/IP follows a horizontal approach
OSI is a theorical model	TCP/IP is a practical model
The transport layer, is only connection-oriented	The TCP/IP model is both connection-oriented and connectionless
OSI separate between the Session and Presentation layers	Session and Presentation layers are combined within the Application layer
Less reliable	More reliable

Table I-1 The Differences between OSI and TCP/IP Model

In the OSI model, data is encapsulated by adding a specific header at each layer as the data moves down from the application layer to the physical layer, creating a new protocol data unit. On the other hand, in the TCP/IP model, data is also encapsulated as it is moved down the layers. However, with different terminology, segments are formed at the transport layer, packets at the internet layer, and frames at the network interface layer.

Figure I-8 represents the structure of encapsulation and DE Capsulation of the OSI and TCP/IP models.

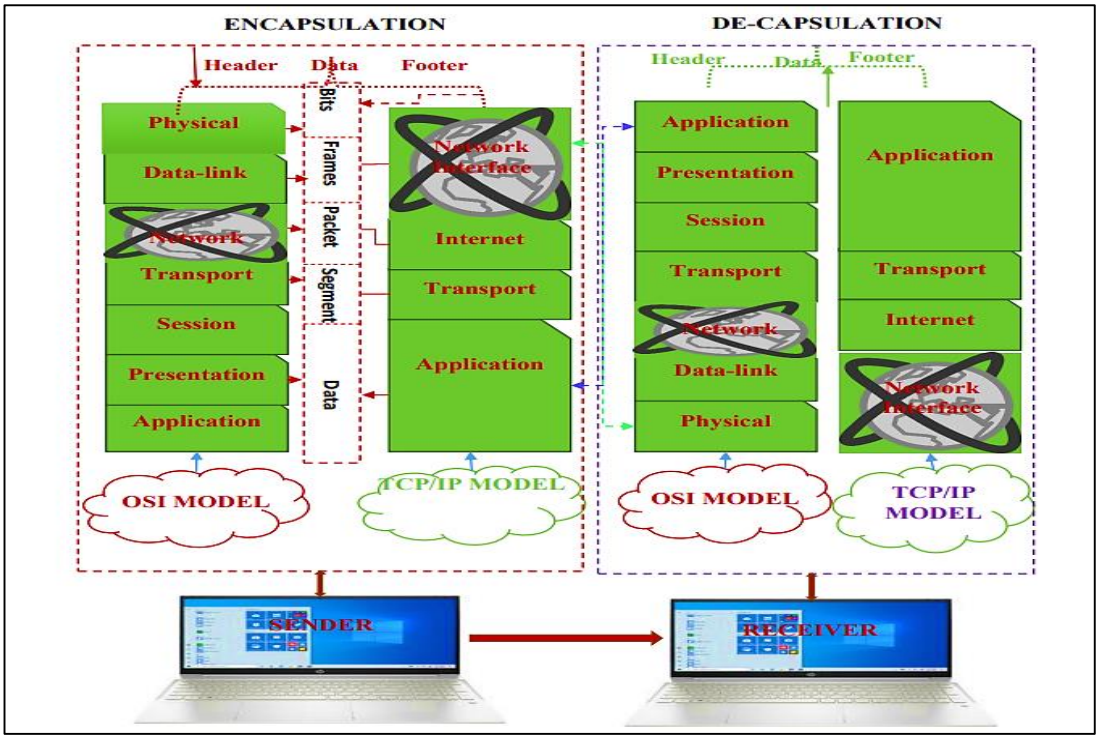

Figure I-8 Encapsulation and DE Capsulation of OSI and TCP/IP Model. **[13]**

Finally, we present the main points of similarities between the two OSI and TCP/IP models, summarized in Table I-2:

Similarities	**TCP/IP and OSI Model**
Structure	Both are arranged layered wise, which is also called an architectural model. These models have a stack of protocols it means the protocol is arranged in every layer
Networking	Both models are designed to facilitate networking by defining standardized protocols and communication methods
Communication	They describe the communication process in terms of data encapsulation and layer interactions
Components	Both models define components or layers that perform specific functions within the communication process

Table I-2 Similarities between OSI and TCP/IP Models

I.8 Conclusion

In this study that we've made of computer networks, we have been able to yield crucial insights into the basic elements and models that comprise modern communication systems. Our research focused on varying network structures, which we presented based on their distinctive properties and spatial applications. After this, we studied network topologies, looking into features like scalability, reliability, and maintenance. We have also presented network devices, which are significant for the easy flow of data and connectivity.

Overall, we were taught the basic concepts of the layered method of network communication, which includes the processes of encapsulation and DE capsulation based on the models OSI and TCP/IP. These models not only provide a structured framework for protocol development but also allow seamless and consistent data flow through different networks.

Chapter 2:

Understanding Routing: Key Protocols and Concepts

II. Introduction

Finding the best route for data to take in order to get to its destination is known as routing. In this chapter, we will discuss the importance of routing in network communication, its types, and the role of two main protocols: Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). We will also delve into the concept of a routing table, a crucial data structure used by routers to determine the best path for forwarding data, and the concept of convergence in routing. In this chapter, we will also focus on two prominent routing protocols: Distance Vector protocols, exemplified by RIP (Routing Information Protocol), and Link State protocols, exemplified by OSPF.

II.1 Introduction to Routing

II.1.1 Definition

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths. Routing is the process of selecting the best path using some predetermined rules. **[14]**

II.1.2 Importance of Routing

Routing is a fundamental concept in computer networks that involves selecting the most efficient paths for data packets to travel between devices and networks. It is essential for optimizing network performance, minimizing latency, and maximizing bandwidth usage. Routers use a routing table, which provides information about network topology, available routes, and metrics used to determine the best path for packet forwarding.

II.2 Routing Fundamentals

II.2.1 Types of Routing

Dynamic and static routing are types of routing that serve different purposes and are implemented in various network environments. The choice between them depends on factors such as network size, complexity, scalability requirements, and the level of administrative control desired.

The figure below summarizes the different types of routing:

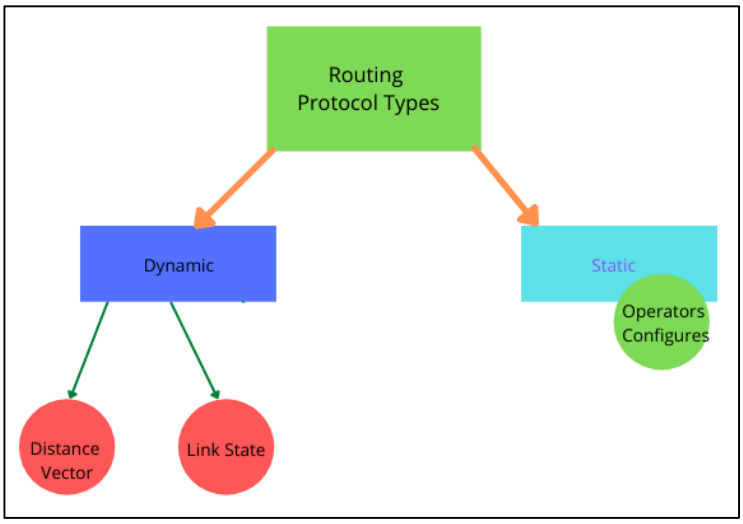

Figure II-1 Routing Types

II.2.1.1 Static Routing

Static routing is not a routing protocol; it is a method of configuring network routers where an individual has complete autonomy to define the paths that data packets should take to reach specific destinations **[15].** It involves defining next-hop addresses and particular routes in detail; these are fixed unless they are altered manually. Static routing requires explicit configuration by administrators and does not react automatically to changes in the network.

Static routing is frequently utilized in small networks, uncomplicated network configurations, or in particular situations where manual management of routing paths is desired. It is commonly used in instances where the network structure remains constant, changes are infrequent, and the network administrator seeks direct authority over routing choices.

II.2.1.1.1 Advantages of Static Routing

- Static routing is simple to implement and manage since it is easy to configure and comprehend.
- Static routes guarantee predictable routing behavior by giving data packets predefined pathways.

- Because static routing does not require maintenance of complex routing tables or ongoing routing updates, it uses less network resources than dynamic routing protocols.

- Route setting is entirely under the authority of network administrators, giving them exact control over routing paths.
- Because static routing lessens the likelihood of unauthorized route alterations and routing attacks, it can offer certain security benefits.

II.2.1.1.2 Disadvantages of Static Routing

- Static routes don't immediately adapt to network changes. Routes must be manually updated by network managers to keep up with network changes.
- In large and complicated networks, static routing becomes difficult to administer and maintain because each router needs to be manually configured.
- In dynamic network situations, static routing might not be suitable since routes must be regularly modified in response to shifting traffic patterns or network problems.
- Both automatic load balancing and traffic optimization over many paths are not supported by static routing.
- Static route configuration and maintenance can become challenging and prone to human error as networks get bigger.

II.2.1.2 Dynamic Routing

Dynamic routing protocols allow each router to automatically discover one or more paths to each destination in the network. When the network topology changes, such as when new paths are added or when paths go out of service, dynamic routing protocols automatically adjust the contents of the routing table to reflect the new network topology **[16].**

Different routing algorithms are used by dynamic routing protocols to identify the optimal path for packet forwarding. To choose the best path, these algorithms consider variables including available bandwidth, network congestion, and link reliability.

Dynamic routing protocols in computer networks include RIP, OSPF, and BGP, each with its own features and limitations, suited for smaller networks, service provider networks, and exterior gateways.

II.2.1.2.1 Advantages of Dynamic Routing

- Large networks can be easily managed and adapted to changes in network topology using dynamic routing protocols.
- Dynamic routing protocols have the ability to rapidly adapt to changes in the network, redirecting traffic and guaranteeing the efficient delivery of packets.
- By utilizing dynamic routing, network traffic can be efficiently distributed across multiple paths, resulting in improved network utilization through load balancing.
- Dynamic routing improves network reliability by offering redundancy and automatically rerouting in the event of failures.
- Dynamic routing helps minimize manual configuration, making network management easier.

II.2.1.2.2 Disadvantages of Dynamic Routing

- Dynamic routing is more complex than static routing, necessitating knowledge of configuration and troubleshooting.
- Dynamic routing protocols utilize network resources and router capacity to exchange routing information.
- Dynamic routing protocols may be susceptible to security risks, necessitating the implementation of security measures like authentication and encryption.
- During a specific period of time, dynamic routing protocols experience a convergence time that can result in temporary disruptions to network stability.
- Dynamic routing provides less direct control over routing decisions compared to static routing.

II.3 Types of Routing Protocols

The optimal path for data packets to take when traveling between two devices or networks is determined by routing protocols. Routing protocols can be classified based on several criteria, some common ways to classify routing protocols based on the AS usage.

The figure below illustrates the popular routing protocols:

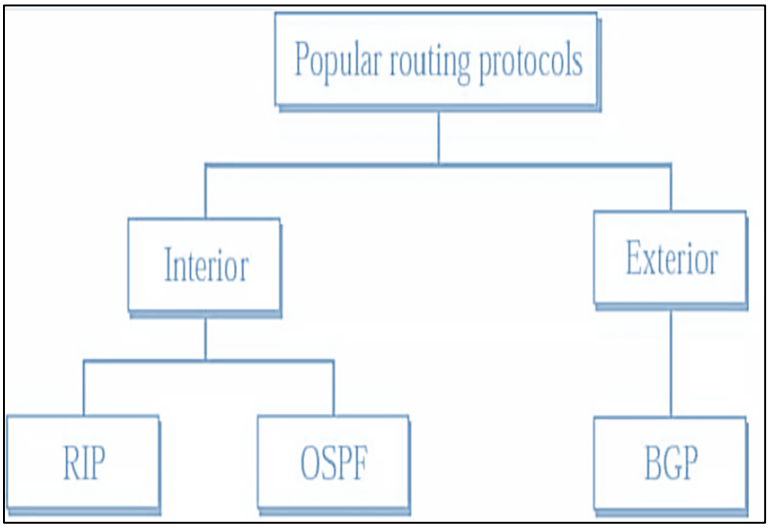

Figure II-2 Popular Routing Protocols

II.3.1 Autonomous System

An Autonomous System (AS) is an independently administered network, such as a network domain. **[17]** Choosing the type of routing protocol used depends on whether the routing is intra-autonomous system or inter-autonomous system.

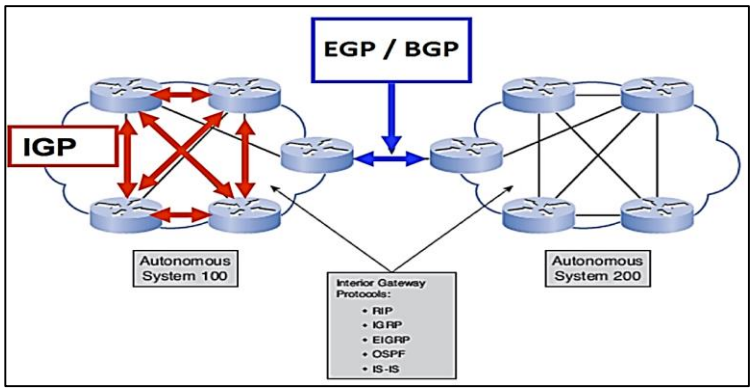

Figure II-3 Autonomous System

II.3.2 Interior Routing Protocols

Interior Routing Protocols, or Interior Gateway Protocols, are protocols that allow routers to communicate and exchange routing information within the internal network of an autonomous system or organization. They create and manage routing tables, which give routers

the information they need to choose the most efficient routes to various locations. In response to changes in the network topology, such as routing preferences or link outages, IRPs operate to guarantee effective packet forwarding.

Interior gateway protocols are used inside an organization's network and are limited to the border router**. [18]**

The most popular IGP has been the Routing Information Protocol. A newer IGP is the Open Shortest Path First protocol (OSPF). It is intended as a replacement for RIP. An older IGP that has fallen out of use is HELLO-the IGP used on the original NSFNET backbone in 1986**. [19]**

II.3.3 External Routing Protocols

The evolution of the ARPANET into the Internet required the numerous island networks to be interconnected using a more robust routing protocol. The Exterior Gateway Protocol (EGP) was selected for this purpose. EGP provided an efficient mechanism for routing among the various RIP domains**. [20]**

EGP stands for external gateway protocol, which is used to help routers in various autonomous systems inside a network, such as the Internet to communicate with one another and share information. By determining the most optimal path for data packet routing, enabling efficient traffic routing across interconnected networks.

Historically (and confusingly), the predominant EGP has been a protocol of the same name: EGP A newer EGP is the Border Gateway Protocol (BGP) that is currently used between the NSFNET backbone and some of the regional networks that attach to the backbone**. [19]**

II.4 Routing Table

A routing table is a data structure stored in a router or network device. It holds a list of specific routing destinations. When the router receives a packet of data, it consults the routing table to determine the appropriate destination for that data.

Every routing protocol has a unique information table. As an illustration, OSPF has the OSPF database. Which routes have been saved in each protocol's database is decided by the protocol itself. Aggregated routes, in which several smaller subnets are merged into a single,

bigger network address, can also be found in the routing table. By using this method, routing efficiency is increased and the size of the routing database is decreased.

The following Figure represents an example of routing table for three routers:

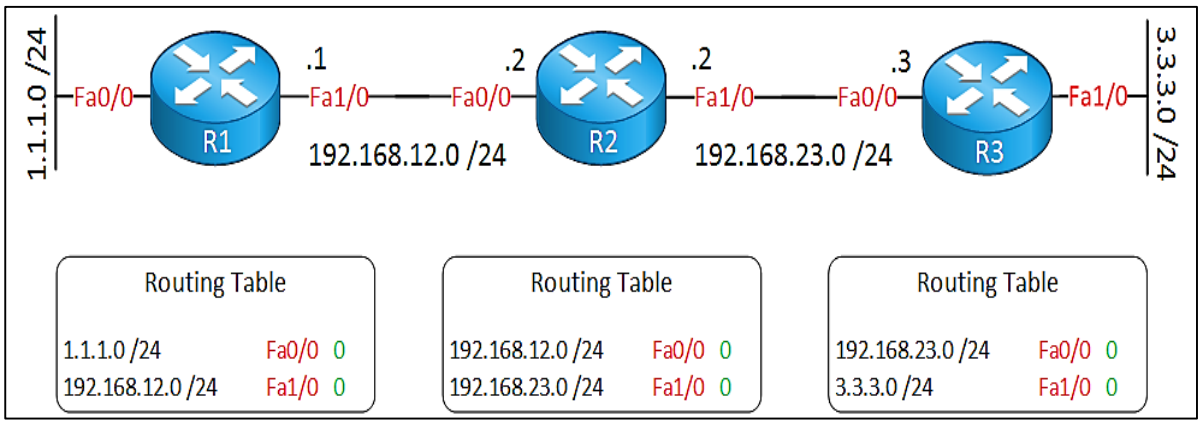

Figure II-4 Routing Table

The routing table contains the following components:

Network Destination

The column indicates the destination network or subnet, which is the range of IP addresses within a specific network.

Metric

The metric component assigns a value to a route, indicating its quality and preference, aiding routers in selecting the optimal path among multiple routes to the same destination. Lower metrics typically indicate a better path.

Outgoing Interface

In order for packets to reach the destination network, this component indicates which network interface they should be transmitted through.

Administrative Distance

Administrative distances are pre-assigned numerical values used by routers to determine the trustworthiness or reliability of routing information received from different routing protocols.

Next Hop

The IP address or interface of the next router or gateway, to which packets should be routed in order to reach the designated network destination, is indicated by the next hop component.

Routing Protocol

Identifies the routing protocol (such as RIP, OSPF, or BGP) that was used to identify the route.

II.5 Routing Metric

A routing metric is a number that a routing algorithm uses to determine whether to accept or reject a routing path for the transfer of data. Metrics can be calculated based on a single characteristic of a path. More complex metrics can be calculated by combining several path characteristics. **[21],** OSPF uses a metric called cost, which is based on the bandwidth of the link. The higher the bandwidth, the lower the cost, while RIP uses hop count as its metric.

The following are some of the characteristics that are used in determining a routing metric:

Hop Count

This measure shows how many routers, or hops, a packet needs to pass through in order to get to the intended network.

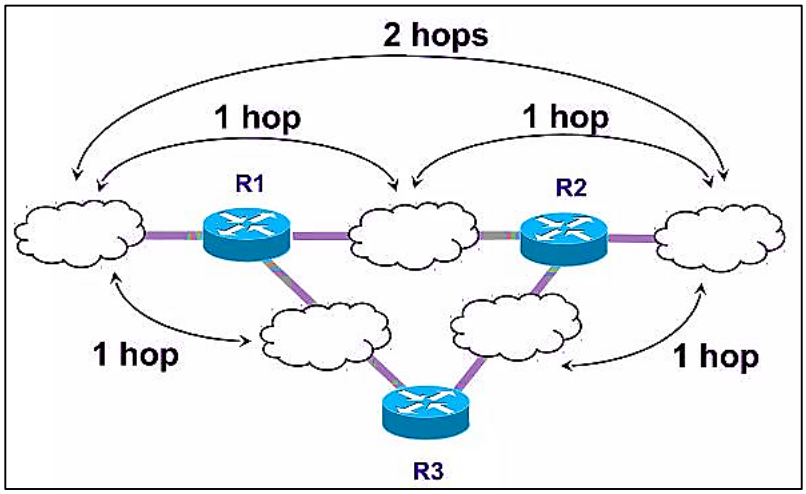

Figure II-5 Hop Count Structure

Bandwidth

Metrics based on bandwidth take into account a link's available bandwidth. Higher bandwidth paths are recommended since they can handle more traffic and perform better.

Delay

The length of time that is required to move a packet from source to destination **[21].**

Reliability

Reliability metrics measure the stability and reliability of a link. Paths with higher reliability, indicating fewer link failures or errors, are preferred.

Load

Load-based metrics consider the current traffic load or utilization on a link. Paths with lower load are favored to distribute traffic evenly across the network.

Cost

Cost-based metrics provide each path or link a numerical cost value. The cost can be based on a combination of factors such as bandwidth, delay, reliability, and administrative preferences. Lower-cost paths are typically preferred.

II.5.1 Hop Count and Bandwidth Metrics in Routing Protocols

The hop count is the total number of routers a packet needs to pass through to get to its final destination. Every router counts as one hop. Distance vector routing protocols like RIP prioritize the path with the fewest hops among multiple available paths.

On the other hand, bandwidth serves as a metric in various routing protocols, such as OSPF, which is a link state protocol. The route with the greatest bandwidth is considered the best choice in link state protocols.

II.6 Administrative Distance

Administrative Distance (AD) represents the level of trustworthiness of the routing information source. It is denoted by integers ranging from 0 to 255, where 0 signifies the highest trust and 255 indicates the lowest trust. AD is utilized to determine the preferred routing

source when multiple routes to the same destination are learned from different sources. Routers must decide which routes to include in the routing table before forwarding packets. When the router learns multiple routes for the same network from different routing protocols, the selection of the route for the routing table is based on the AD of the source routes.

The route with the lowest AD value takes precedence as the route source. The most preferred AD value is zero, which is typically assigned to directly connected routes and is generally not changed. Table II-1 represents a list of various routing protocols and their associated ADs:

Route Source	Administrative Distance
Connected	0
Static	1
External BGP	20
OSPF	**110**
IS-IS	115
RIP	120
Internal BGP	200
Unknown	255

Table II-1 Routing Protocols and Their Administrative Distances

II.7 Convergence

Convergence in routing is the process where all routers within a network come to a consensus on the topological details and make necessary updates to their routing tables. Whenever there is a change in the network's structure, like a link failure or addition, routers need to modify their routing tables to ensure the most efficient path calculations.

The purpose of convergence is to ensure that all routers possess synchronized routing information, which in turn facilitates smooth and reliable data transmission.

II.8 Routing Protocols

II.8.1 Distance Vector Routing Protocols

Distance vector protocols are sometimes referred to as Bellman-Ford protocols, named after the person who invented the algorithm used for calculating the shortest paths **[22].**In

distance vector routing, all nodes exchange information only with their neighboring nodes. Nodes participating in the same local network are considered neighboring nodes **[23],** allowing them to learn about the network topology and update their routing tables accordingly.

These protocols use the Bellman-Ford algorithm to select the optimal routes for data packet routing within a network. To do this, they calculate and keep up with routing tables that provide metrics and destination information. Routing Information Protocol (RIP) and Routing Information Protocol Version 2 (RIPv2) are examples of DV routing protocols.

II.8.1.1 Routing Information Protocol

RIP is a distance vector protocol. Distance vector protocols are usually described as implementing the Bellman-Ford algorithm to find the best pathways **[24].** One of the most old and basic dynamic routing protocols, it is frequently used in small- to medium-sized networks.

Routers regularly exchange updates with neighboring routers every 30 seconds, exchanging details about the networks they are aware of and the number of hops required to reach them. RIP has a maximum hop count of 15, so a destination of 16 would be considered inaccessible, and employs strategies such as split horizon, route poisoning, and hold-down timers to avoid routing loops.

There are two variations of RIP: RIPv1, which is classful and does not support subnetting, and RIPv2, which is classless and includes subnet information.

II.8.1.1.1 RIP V1

Routing Information Protocol version 1, or RIP v1, is an older distance-vector routing protocol used in computer networks. RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask **[25].** By exchanging entire routing tables on a regular basis via broadcast updates, RIP v1 routers are able to keep their network topology knowledge current.

II.8.1.1.2 Limitations of RIP V1

RIP v1 has limitations such as the following:

- RIP v1 experiences slow convergence times, causing routers to take longer to update their routing tables in response to network topology changes. This delay can lead to postponed routing updates and possible interruptions in network connectivity.

- It has a maximum hop count of 15, beyond which a route is considered unreachable. This constraint limits the scalability of networks that RIP v1 can efficiently handle.
- RIP v1 lacks support for variable-length subnet masks (VLSM), which reduces its capability to effectively allocate IP addresses and divide networks into subnets of varying sizes.
- RIP v1 lacks built-in authentication mechanisms, leaving it susceptible to different security risks like unauthorized route advertisements or spoofing attacks.
- During updates, RIP v1 exchanges complete routing tables, regardless of the number of changes. This results in larger routing tables being shared, which can cause higher network traffic and bandwidth consumption compared to protocols with incremental updates.

II.8.1.1.3 RIP v2

It is an upgraded version of RIP, which resolves certain issues found in RIP v1. Here are a few important enhancements and features of RIP v2:

- RIP v2 enables the use of VLSM, which permits better IP address allocation and the establishment of subnets with varying sizes in a network.
- It uses classless routing to advertise subnets with their subnet masks, providing more precise network information and improving routing decisions.
- RIP v2 includes authentication to ensure genuine and reliable routing updates, preventing unauthorized devices from injecting misleading information into the network.
- RIP v2 uses multicast updates instead of broadcasts, reducing network bandwidth usage and improving scalability.
- It maintains compatibility with RIP v1, allowing RIP v2 routers to receive routing updates from RIP v1 routers. On the other hand, RIP v1 routers are unable to comprehend the distinct features of RIP v2.

II.8.2 Link State Routing Protocols

Link-state protocols are a category of routing protocols that are used to create efficient routing tables and identify the optimal routes for data transmission. These protocols work by ensuring that routers exchange link-state advertisements (LSAs), which are informations that keeps the routers views of the network topology matched. Every router creates a link-state database (LSDB), which is an exhaustive representation of all the links in the network and their

attributes. Link-state protocols create an SPF tree, or shortest path tree, by utilizing tools such as Dijkstra's SPF (Shortest Path First) algorithm on the LSDB.

As a result, packet forwarding is effective, and network changes can be quickly adapted by routers using the most recent routing information. The first link-state routing protocol was developed for use in the ARPANET back in the 1980s, and this work was the springboard for a new generation of link-state routing protocols such as OSPF and IS-IS**. [26]**

Link-state routing protocols were designed to overcome the limitations of distance-vector routing protocols. Link-state routing protocols respond quickly to network changes, send triggered updates only when a network change has occurred, and send periodic updates (known as link-state refreshes) at long intervals, such as every 30 minutes. A hello mechanism determines the reachability of neighbors. **[21]**

II.8.2.1 Open Shortest Path First

OSPF is an IGP developed for use in IP-based networks. As an IGP, OSPF distributes routing information between routers belonging to a single autonomous system (AS) **[27].** OSPF uses the link-state routing algorithm to share network topology details, enabling routers to determine the shortest path and find the best routes for forwarding IP packets. It was created to accommodate hierarchical network structures, making it easier to scale and ensuring quick convergence.

OSPF is extensively utilized in large enterprise networks as it supports both IPv4 and IPv6 networks.

OSPF routers calculate the best path by summing the costs along the route. This metric calculation helps OSPF select the most efficient and reliable paths for routing traffic within the network. Additionally, OSPF allows administrators to customize the metric based on different factors, such as the type of service or network characteristics.

II.8.3 Difference between Distance Vector Routing and Link State Routing

Link state protocols and distance vector protocols are two different routing protocols used in computer networks, the key distinctions between them are as follows

	Distance Vector Protocols	Link State Protocols
Routing Algorithm	Based on the Bellman-Ford algorithm	Based on the shortest path first algorithm
Routing Information	Relies only on data from neighboring nodes	Uses information about all links in a network
Structure	Flat	Hierarchical
Routing Table Updates	Periodically send complete updates, regardless of any changes.	Send updates only when there are changes in the network topology
Convergence Time	Slower due to periodic updates and incremental changes	Faster due to efficient routing decisions and proactive updates
Scalability	Large networks can pose challenges due to frequent updates and slower convergence	Ideal for large and complex networks, providing quicker convergence and effective path selection

Table II-2 Difference between Distance Vector Routing and Link State Routing

II.8.4 Choosing between Routing Protocols

When deciding on an IGP for routing within a network, network administrators usually weigh the advantages of distance vector and link-state protocols. Distance vector protocols, like RIP, are simple to use and implement, but they may have slower convergence and limited scalability.

On the other side, link-state protocols like OSPF offer more advanced features, scalability, and efficient routing. OSPF's thorough understanding of the network's layout and hierarchical design make it a popular option for larger networks. In summary, while RIP is easy to understand, OSPF provides better scalability, reliability, and efficient routing.

II.9 Conclusion

In conclusion, the concept of routing is essential to how computer networks operate. Routing allows devices and networks to communicate effectively by moving data packets from source to a destination in an efficient manner

We have looked at a number of routing topics in this chapter, such as routing protocols, routing algorithms, and the variables that affect routing choices. As we have seen, routing protocols like RIP and OSPF that solve the limitations of RIP by offering improved efficiency, scalability, and security features. Those protocols give routers the foundation they need to communicate routing information and choose the most efficient routes to reach their destinations.

Another crucial component of routing is convergence, which makes sure that routers synchronize and update their routing data to take into account network changes.

Chapter 3:

OSPF: Fundamentals and Applications

III Introduction

OSPF is a crucial element in ensuring efficient network communication by determining the most optimal paths for data packets, especially in complex network infrastructures. Its scalability and reliability establish OSPF as an indispensable protocol for enhancing network performance.

In the upcoming chapter, we will delve into the intricate workings of OSPF, starting with its fundamental characteristics and then delving into critical aspects such as its metric system and zone segmentation to facilitate improved network administration. Additionally, we will explore how OSPF facilitates quick network convergence through the provision of real-time routing information and its security measures to strengthen defenses against unauthorized access and potential threats.

Lastly, we will evaluate the advantages and disadvantages of OSPF to aid in decision-making processes when incorporating this robust routing protocol into network configurations.

III.1 Introduction to OSPF

III.1.1 History and Version

The development of OSPF (Open Shortest Path First) was led by the OSPF working group of the Internet Engineering Task Force (IETF) in the late 1980s as a replacement for the Routing Information Protocol (RIP) due to its limitations in many terms. The work of the IETF OSPF working group, including contributions from Dr. John T. Moy and others, was important for the creation and standardization of OSPF, and as a result, they wrote the formal protocol specifications known as the OSPF RFCs (Request for Comments).

Below is a summary of the major enhancements and iterations that OSPF (Open Shortest Path First) has gone through since its founding:

OSPFv1

RFC 1131, which was released in October 1989, defined the first iteration of OSPF, or OSPFv1. It was the initial version of OSPF that was standardized and offered fundamental features for IP packet routing inside an independent system.

OSPFv2

RFC 2328 defines OSPFv2, which was released in April 1998. Compared to OSPFv1, this version added a number of features and improvements, such as support for variable-length subnet masking (VLSM), authentication methods, and improved scalability through the implementation of area hierarchy.

OSPFv3

RFC 5340 defines OSPFv3, which was released in July 2008. It is specifically designed for routing IPv6 traffic and replaces OSPFv2 in IPv6 networks. OSPFv3 brought in compatibility with IPv6 addresses, removed the necessity for address summarization, and implemented various improvements to meet the needs of IPv6 characteristics and demands.

Today, OSPF continues to be a widely embraced and essential routing protocol in enterprise and service provider networks. Its ability to achieve rapid convergence, support large networks, and provide adaptable routing policies has made it the preferred option for monitoring complex IP routing environments.

III.1.2 Characteristic

OSPF provides several features to facilitate efficient network routing. The following are some of the key features that are associated with OSPF:

- OSPF shares information about the condition of its links with adjacent routers, including details such as link cost, bandwidth, and interface status. By maintaining a complete network topology, OSPF can determine the shortest route to any destination.
- OSPF allows for load balancing through equal-cost multipath (ECMP), when multiple routes are available, traffic can be evenly distributed over the routes. More efficient network utilization results. **[28]**
- OSPF utilizes a hierarchical structure that includes areas. This division of an OSPF domain into multiple areas allows for scalability and efficient routing. Each area has its own set of routers and maintains localized routing information, which reduces the need for exchanging routing information across the entire network.

- OSPF prioritizes fast convergence by utilizing Hello packets, dead timers, and incremental SPF calculations. It can rapidly detect network changes, update routing tables, and reestablish connectivity to minimize downtime.
- The Designated Router (DR) is elected on multi-access networks like Ethernet. It creates the network LSA and synchronizes link state databases among routers. It facilitates efficient communication by exchanging LSAs with other routers during the flooding process.
- Virtual links. By allowing the configuration of virtual links, OSPF removes topological restrictions on area layout in an Autonomous System**.[29]**
- To safeguard the routing data exchanged between OSPF routers, OSPF offers mechanisms for authentication. It makes sure that only authorized routers are able to interact with the OSPF domain by utilizing authentication. This effectively guards against malicious routing updates and prevents unauthorized access.
- OSPF was designed to support networks of various sizes, with scalability being a key feature. By utilizing a hierarchical design with areas, OSPF effectively manages network expansion by limiting the amount of routing information and reducing overhead. This scalability is especially important for large enterprise networks.
- OSPF allows the use of variable-length subnet masks, which enable different-size subnets in the network to better meet the needs of the network and more efficiently use the network's limited IP address space**. [30]**
- OSPF is reliable and resilient, it includes mechanisms for identifying and resolving problems like link failures or congestion.
- OSPF uses the SPF algorithm, developed by Edger Dijkstra, to provide a loop-free topology**. [31]**

III.2 OSPF Router Types

III.2.1 Internal Router

An Internal Router (IR) works only within a single OSPF area. All its interfaces are connected to that area, and it does not have any connections to other areas. These routers handle traffic forwarding within their area and share routing information with other routers in the same area.

III.2.2 Area Border Router

An Area Border Router (ABR) is a router that connects different OSPF areas. It has interfaces in at least two areas and shares routing information between them. It maintains multiple Link State Databases (LSDBs), one for each connected area. The ABR summarizes routing details from non-backbone areas and inserts them into the backbone area.

III.2.3 Backbone Router

A Backbone Router is an OSPF router that is located in the backbone area (Area 0). It acts as a central router that establishes and manages the backbone infrastructure, connecting all other OSPF areas. The backbone router is crucial for exchanging routing information and maintaining connectivity across the entire OSPF network.

III.2.4 Autonomous System Border Router

This router exchanges routing information with routers outside the AS. It advertises AS external information throughout its system. AS boundary routers may be internal routers or ABRs**. [36]**

These classes are allowed to overlap. For example, all the border routers are automatically part of the backbone. In addition, a router that is in the backbone but not part of any other area is also an internal router**. [32].**

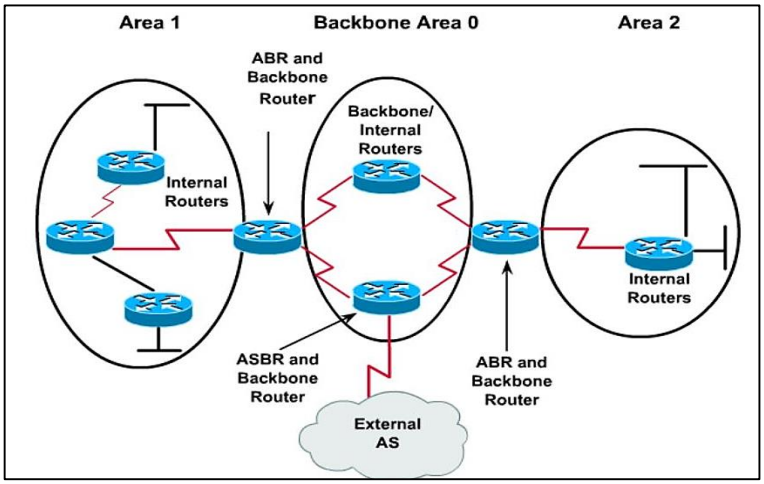

Figure III-1 OSPF Router Types

III.3 OSPF Link State Advertisements Types

In OSPF, routers share information about routes using LSAs. These LSAs give details about the network's status and help create a unified view of the network setup. OSPF has different types of LSAs, each with its own purpose.

The main table presents LSA's types :

Type	Name	Description
1	Router LSA	Every router running OSPF within an area generates this LSA, which provides details about the router's interfaces and the connected links. The LSA contains information about the router's ID, the networks directly connected to it, and the type of link.
2	Network LSA	This LSA is created by the designated router (DR) on a multi-access network. It provides information about the routers connected to the network and their relationship with the network. The Type 2 LSA is distributed within the same area to notify other routers about the presence of the network.
3	Summary LSA	Generated by ABRs, Type 3 LSAs carry summary route information between OSPF areas. Typically, this information is exchanged between a no backbone area and the backbone area, or vice versa. Type 3 LSAs are not refolded across area boundaries; instead, a receiving ABR generates its own Type 3 LSA summarizing its inter area routing information into any adjacent areas.**[35]**
4	ASBR Summary LSA	This LSA is created by an ABR to notify other areas about the presence of an Autonomous System Boundary Router (ASBR). It includes details about the ASBR's router ID and the metrics required to reach it. The Type 4 LSA assists in making routing decisions when connecting to external networks.

5	AS external LSA	This LSA is generated by an ASBR to advertise routes from external ASs into the OSPF domain. It carries information about the external networks, their metrics, and the ASBR's router ID. The Type 5 LSA allows OSPF routers to learn about and route to networks outside the OSPF domain.
7	NSSA external LSA	Type 7 LSAs are utilized in OSPF Not-So-Stubby Areas (NSSAs) to advertise routes from external autonomous systems. They contain details about external networks, metrics, and the router ID of the ASBR, similar to Type 5 LSAs. However, Type 7 LSAs are specific to NSSAs and are converted into Type 5 LSAs by the NSSA's Autonomous System Border Router (ASBR) before being flooded to other areas.

Table III-1 OSPF LSA'S Types with Description

III.4 OSPF Areas

In OSPF, a set of networks and routers that are linked together and share routing data is called an area. These areas help in dividing a large OSPF network into smaller, more manageable units, allowing for efficient routing, scalability, and control over the exchange of routing information. When dividing a network into areas in OSPF, there are some rules that should be taken into account. Such as:

- Each area is identified by a unique Area ID, which is a 32-bit number.
- Each OSPF network needs to have a backbone area (Area 0).
- Each non-backbone area must be connected to the backbone area through an ABR (Area Border Router). Areas can have a single Area Border Router or they can have multiple Area Border Routers**.[27]**
- Areas should have a contiguous set of network or subnet addresses. Without a contiguous address space, it is not possible to implement route summarization**. [27]**
- The boundary of an area is defined by the interfaces of routers that belong to that area.

The following figure illustrates an example of a network topology and layout of these OSPF areas:

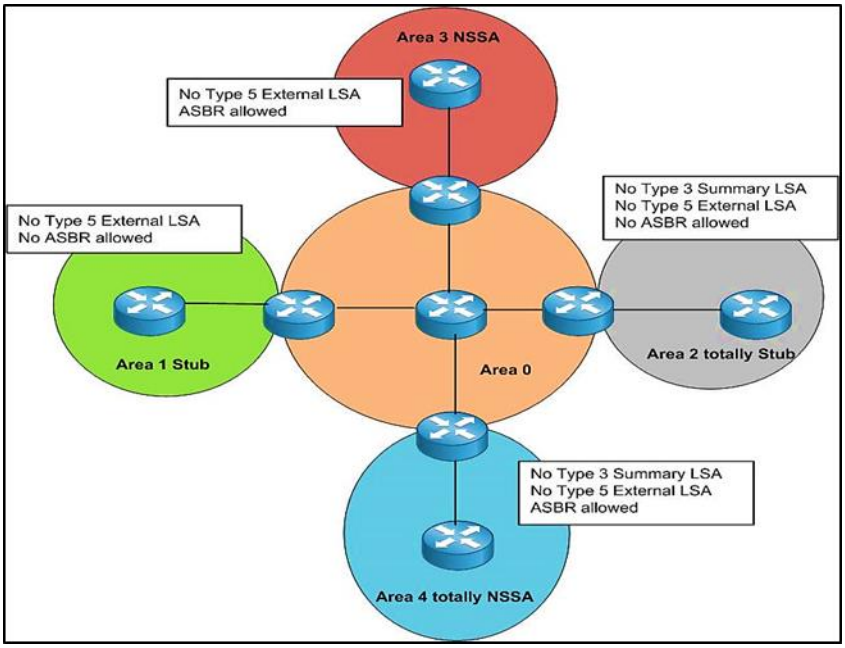

Figure III-2 OSPF Areas Types

OSPF supports different types of areas, providing flexibility and control in network design. Here are the OSPF area types that are commonly used:

III.4.1 Backbone Area

Every AS has a backbone area, called area 0. All areas are connected to the backbone, possibly by tunnels, so it is possible to go from any area in the AS to any other area in the AS via the backbone. **[32]**

The OSPF backbone area connects all network areas in OSPF. It facilitates the exchange of routing information between areas and enables route summarization to improve routing efficiency. It serves as the core of the hierarchical OSPF network structure, guaranteeing seamless connectivity and routing among different areas within the OSPF network.

III.4.2 Normal Area

A normal area, also known as a standard area, is an essential part of an OSPF network. It comprises a group of routers and their interconnected networks within the OSPF autonomous system (AS). A standard area is connected to the backbone area (Area 0) through one or more Area Border Routers (ABRs). Its primary function is to facilitate the exchange of routing information and enable the calculation of the shortest paths within the area**.**

Below are a few typical features of the normal Area:

- Routers in a normal area receive Type 3 LSAs from other areas through ABRs, containing summarized routing information for efficient routing and smaller routing tables.
- Autonomous System Boundary Routers inject External LSAs into normal areas, allowing the normal area to learn and route traffic to networks outside the OSPF domain.
- External default LSAs can be injected into normal areas, providing a default gateway for routing traffic to unknown destinations within the OSPF domain.

III.4.3 Stub Area

A stub area in OSPF is an area that restricts the flow of external route information and reduces the size of routing tables. It prevents the propagation of External LSAs (Type 5 LSAs) into the stub area. Instead, routers within the stub area receive summarized routing information about external routes through Type 3 Summary LSAs from the Area Border Router (ABR). This simplifies routing within the stub area and improves scalability.

Some Stub Area characteristics are shown below:

- The stub area provides access in and out of the region.
- The stub region prevents external LSAs from arriving.
- Within the stub region, the default path is specified.
- OSPF routes must be setup as stub routes inside the stub area.

III.4.4 Not-So-Stubby Area

An NSSA, or Not-So-Stubby Area, is an OSPF area that combines features from stub and standard areas. It overcomes the limitations of stub areas by allowing external routes within the area, while still maintaining route summarization and control over external route information.

Below are a few typical features of the Not-So-Stubby Area:

- NSSAs use Type 7 LSAs to transport external route within the area. These LSAs are created by an ASBR and distributed throughout the NSSA.

- The ABR converts Type 7 LSAs from the NSSA to Type 5 LSAs and distributes them to other OSPF areas.
- NSSAs can accept a default route from the ABR, similar to stub areas, which acts as a gateway for connecting to external networks. **[33]**

III.4.5 Totally Stubby Area

A Totally Stubby Area is an OSPF area configuration that severely limits the available routing information to routers within the area. Routers in a Totally Stubby Area only have a default route to reach destinations outside the area, which reduces the size of their routing tables and OSPF databases.

Here are some common characteristics of the Totally Stubby Area:

- The ABR injects a default route into the Totally Stubby Area, serving as the exit point for accessing external destinations.
- The ABR blocks Type 5 LSAs and Type 3 Summary LSAs in the Totally Stubby Area, reducing the routing table size.
- The ABR prevents Type 4 LSAs, which are ASBR summary routes, from entering the Totally Stubby Area. This ensures that information about the ASBRs in the OSPF network is not spread.

III.4.6 Totally Not So Stubby Area

The Totally NSSA, Totally or Not-So-Stubby Area, combines features of the Totally Stubby Area and the NSSA in OSPF. It allows for limited external routing connectivity while still managing and restricting routing information in the area. Here are some of its common characteristics:

- Similar to the Totally Stubby Area, the Totally NSSA blocks external and summary routes in the area, reducing the routing table and improving network efficiency.
- The Totally NSSA, like the Totally Stubby Area, receives a default route from Area 0 to route traffic beyond the OSPF domain
- The Totally NSSA allows limited external routing connectivity using Type 7 LSAs, with ASBR injecting external routes within the area.

- The ABR converts Type 7 LSAs from the Totally NSSA into Type 5 LSAs at the backbone border, distributing them throughout the OSPF domain to extend external routes.

III.4.7 Transit Area

This OSPF area is used to connect two or more border routers that are used to pass OSPF traffic from one area to another**. [34]**

III.5 OSPF Protocol Packets

III.5.1 OSPF Header

The OSPF header, as depicted in Figure III-3, is an important part of OSPF packets and functions as the header information within the data section of an IP packet. It includes important details about the OSPF packet itself. The following outlines the details of each field within the header:

Version Field

This contains the version of OSPF, the current version used is 2 (OSPFv2).

Type

This field indicates type of OSPF packet, such as Hello, Database Description (DBD), Link-State Request (LSR), Link-State Update (LSU), or Link-State Acknowledgment (LSAck).

Packet Length

This is the length of the entire OSPF packet, including the header. [**36]**

Router ID

This is the ID of the router that is originating the OSPF packet. [**36]**

Area ID

This field specifies the OSPF area to which the packet is associated.

Checksum

This allows the receiving router to determine whether the packet has been damaged in transit; if so, the packet is discarded**. [37]**

Authentication Type and Authentication

This indicates the type of authentication procedure in use. The authentication field for use is dependent upon the chosen authentication procedure**. [27]**

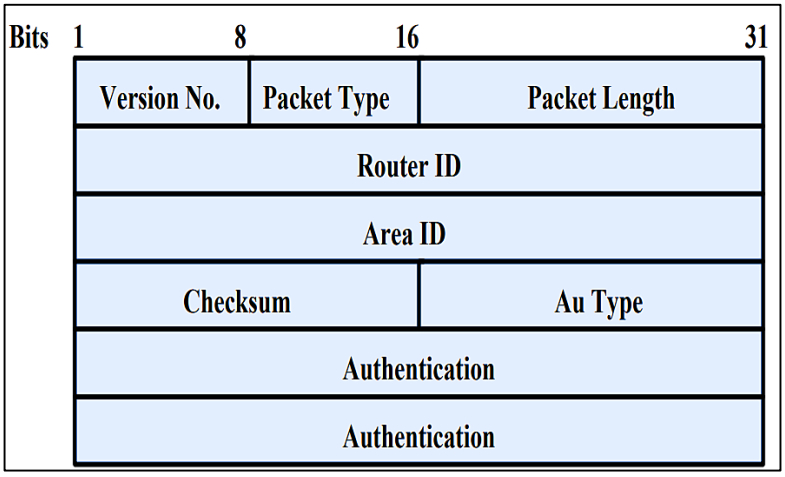

Figure III-3 OSPF Header

III.5.2 OSPF Packet Types

III.5.2.1 Hello Packets

OSPF Hello packets are responsible for discovering and maintaining neighbors. In most instances, the router sends Hello packets to the AIISPF Routers address (224.0.0.5) **[38].** Routers employ Hello packets to identify neighboring routers running OSPF on the same network segment and establish connections. Additionally, authentication mechanisms can be implemented to enhance security and protect the integrity of Hello packets.

The Hello interval parameter in OSPF controls the timing of Hello packet exchanges among routers, managing when routers send and receive Hello packets to facilitate communication (the hello interval of 10 seconds and the dead interval of 40 seconds). If a router does not receive this Hello packet within a certain time period (dead interval), it is termed

"dead," and all information transferred between routers is invalid. Hello packets are used to select designated (DR) and backup designated routers in broadcast or NBMA networks (BDR) **[33].** Here are the descriptions for each field of Hello packet:

Network Mask

This field shows the network mask associated with the interfaces of the sending router. It's determined by the IP Class Type (A, B, etc.).

The Hello Interval

It determines the duration in seconds between each transmission of Hello packets by the router.

Options

This section shows the OSPF capabilities and features that the sending router supports.

Router Priority

This field helps decide which routers become the designated router (DR) and backup designated router (BDR) on multi-access networks. The router with the highest priority becomes the DR, while the second highest becomes the BDR.

Dead Interval

It determines the duration in seconds after which a neighbor who is not responding is considered dead.

Designated Router

This field is used to indicate the router ID of the elected Designated Router. If there is no DR, this value is set to 0.0.0.0.

Backup Designated Router

This field is used to identify the BDR and lists the IP interface address of the BDR. If there is no BDR present, this field will be set to 0.0.0.0.

Neighbor

This field contains a list of OSPF router IDs of the neighboring routers.

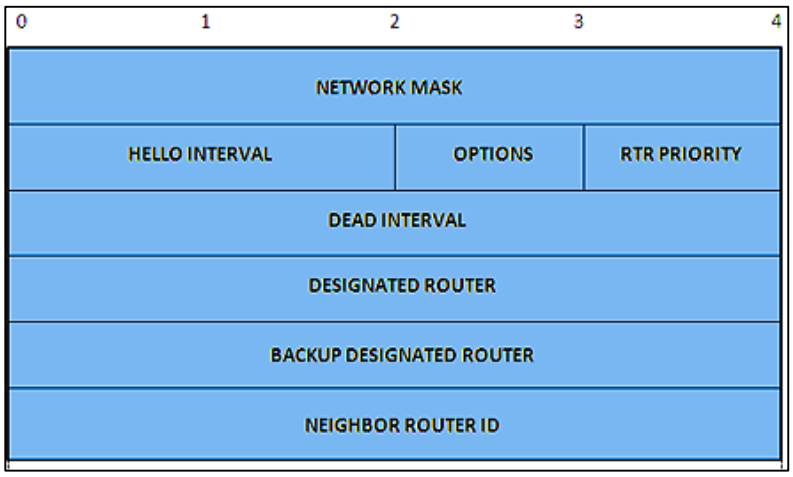

Figure III-4 Hello Packets Fields

III.5.2.2 Database Description Packets

Database Description (DBD) packets are essential in OSPF as they allow neighboring routers to exchange summarized information about their link-state databases (LSDB). These packets contain headers that provide details about LSAs in the LSDB, helping routers identify any missing or outdated LSAs. If any discrepancies are detected, routers can request the missing LSAs using Link-State Request (LSR) packets. By facilitating the DBD exchange process, the OSPF network ensures the accuracy and update of routing information.

Here are the specifics of every field in the DBD packets:

Interface MTU

Stands for "Maximum Transmission Unit" and it refers to the largest size of a data packet that can be transmitted over a specific network interface without fragmentation.

I

It a 1-bit flag, when this flag is set to one; it indicates that the DBD packet is serving as an initial message.

M

It is a 1-bit flag, when set to 1, it indicates that the DBD packet is an additional message.

MS

Is a 1-bit flag, when set to 0, it signifies that the router will act as a Slave, when set to 1, it means that the router will act as a Master.

DBD Sequence Number

Each DBD packet contains a sequence number that is used to sequence the exchange of DBD packets between routers. The sequence number is incremented for each new DBD packet sent.

The LSA Header

Contains information about the local router database.

<table>
<tr><th colspan="6">OSPF Header with Type =2</th></tr>
<tr><td>Interface MTU</td><td>options</td><td>l</td><td>M</td><td>MS</td><td>0</td></tr>
<tr><td colspan="6">Database Description Sequence Number</td></tr>
<tr><td colspan="6">Link State Advertisement (LSA) Header</td></tr>
</table>

Figure III-5 LSA Header Contents

III.5.2.3 Link State Request Packets

A Link-State Request (LSR), which is an OSPF Packet Type 3, is used to request missing or outdated LSAs from neighboring routers during the synchronization of the LSDB. After exchanging Database Description (DBD) packets, each router compares the LSA Headers with its own database. If a router finds that it does not have the latest information for any LSA, it generates LSR packets and sends them to its neighbors, asking for the updated LSAs.

These are the details for each field found in the LSR packets:

LS Type

This field indicates the type of LSA requested, specifying the specific type of LSA needed by the router from its neighbors to update or complete its OSPF database.

The Link State ID

This field serves as an identifier used in LSAs to uniquely distinguish LSAs within an OSPF domain, it differs based on the type of LSA.

Advertising Router

This field carries the OSPF RID of the router that originated the LSA. It identifies the source of the information contained in the LSA.

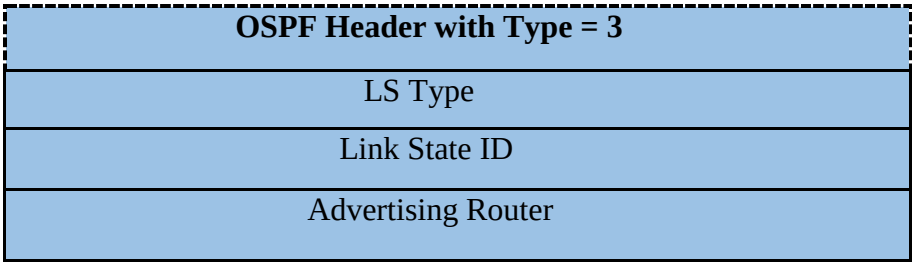

Figure III-6 Link State Request Packets

III.5.2.4 Link State Update Packets

LSU packets in OSPF are used to distribute LSAs to nearby routers in the OSPF network. These packets contain the actual LSAs that a router is sharing. When a router has new or updated LSAs to share, it puts them into LSU packets and sends them out. These packets are sent in response to Link-State Request packets or as part of the regular OSPF flooding process to ensure that the LSDB is synchronized across the network. When neighboring routers receive LSU packets, they update their own LSDBs with the LSAs, allowing them to have the most up-to-date routing information.

The details for each field in the LSU packets are as follows:

Number of Advertisements

Refers to the quantity of Link State Advertisements (LSAs) included within a single transmission, depending on the network's topology and the updates being propagated.

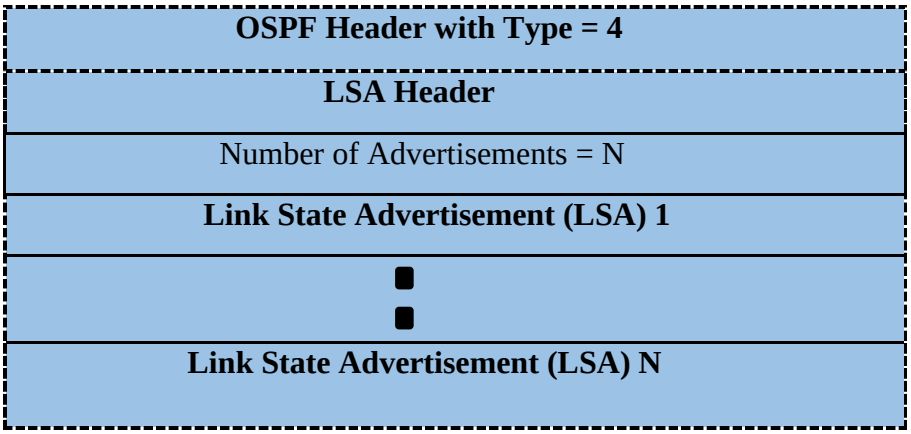

Figure III-7 Link State Update Packets

III.5.2.5 Link State Acknowledgement Packets

The Link-State Acknowledgement (LSAck) packet is used in OSPF to confirm the receipt of Link-State Update packets that contain updated Link-State Advertisements.

When a router receives an LSU packet from a neighboring router, it sends an LSAck packet to acknowledge the successful receipt and processing of the LSAs. While the LSAck packet does not contain any new LSAs, it is essential for maintaining reliable communication and synchronization within the OSPF network.

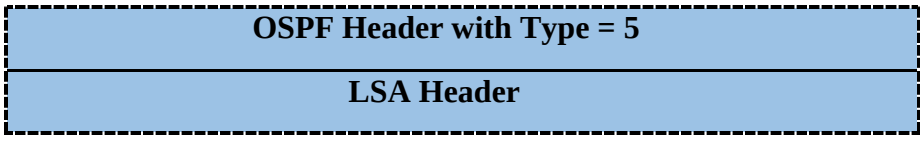

Figure III-8 Link-State Acknowledgement Packets

III.7 OSPF Network Types

III.7.1 Point to Point Network

A Point-to-Point (P2P) network is a network type that establishes a direct connection between two nodes or devices, as shown in Figure III-9. Within this network, communication takes place directly between the two endpoints without the involvement of any intermediary network devices. This setup ensures a dedicated and exclusive link between the two points, enabling efficient and secure communication. P2P networks are frequently used for point-to-point communication over serial connections or dedicated leased lines.

Figure III-9 OSPF Point to Point Network

III.7.2 Broadcast Multi Access Networks

A Broadcast Multi-Access (BMA) network is a type of network that connects multiple devices to a shared medium. Communication in a BMA network happens through broadcast messages that are transmitted to all devices on the network. These networks are commonly used in Ethernet LANs to facilitate effective communication among multiple devices without the need for individual point-to-point connections. To improve network efficiency, a designated router (DR) can manage the broadcasting process. BMA networks are advantageous when multiple devices need simultaneous access to the same information, such as broadcasting updates or announcements.

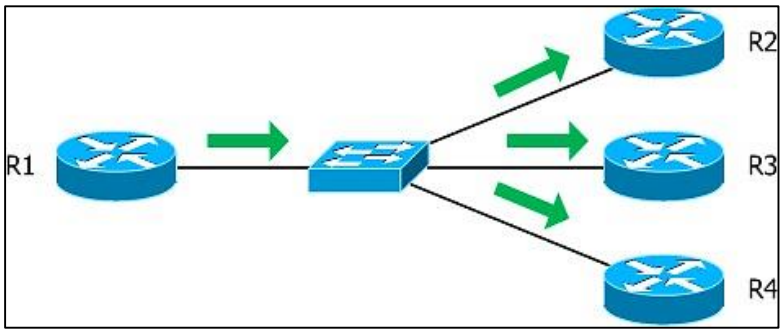

Figure III-10 OSPF Broadcast Multi Access Networks

III.7.3 Non Broadcast Multi Access Networks

Non-Broadcast Multi-Access (NBMA) networks do not support broadcasting messages to all devices at once. Instead, they use unicast communication, where messages are sent directly to the recipient. Each device needs to be manually configured to ensure messages reach the right recipient. To work around IP address restrictions, NBMA networks might use Network Address Translation (NAT) to allow multiple devices to share a single public IP address when communicating outside the network.

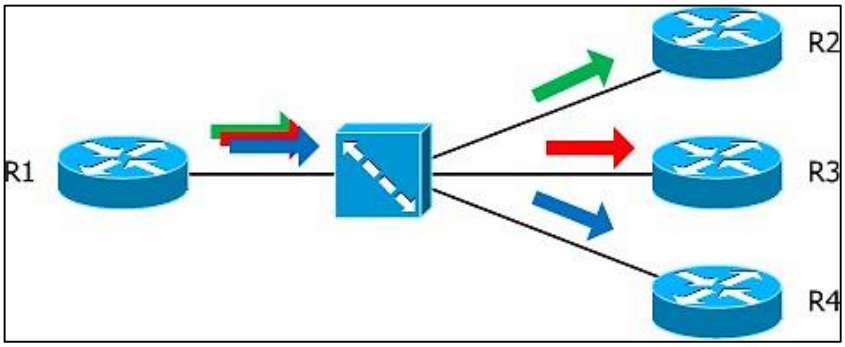

Figure III-11 OSPF A Non Broadcast Multi Access Networks

III.7.4 Point to Multipoint Network

Point-to-Multipoint is a communication setup in which a single sender device sends data to multiple receiver devices at the same time. It can utilize broadcast or multicast techniques and is beneficial for tasks such as video conferencing and multimedia streaming. P2MP networks provide scalability and minimize bandwidth usage by sending data only once to reach numerous recipients. These networks can be structured in hub-and-spoke or mesh configurations, with addressing being a key factor.

P2MP networks are useful for situations that require one-to-many or one-to-group communication, optimizing network resources while facilitating efficient data transmission to multiple devices.

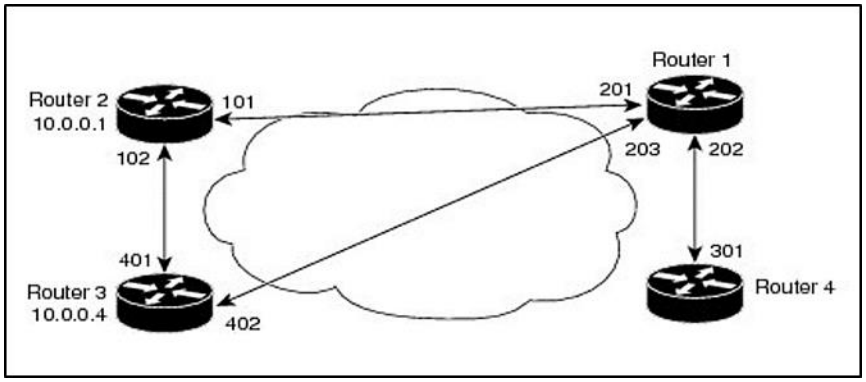

Figure III-12 OSPF Point to Multipoint Network

III.8 OSPF Neighbor Relationship

An OSPF neighbor refers to the connection or relationship between two OSPF routers, where they exchange routing information, synchronize databases, and communicate to maintain an accurate network topology view. In the OSPF protocol, the neighboring routers go through multiple states as they establish and maintain the adjacency relationship. These states signify the different stages involved in forming a strong connection between OSPF routers.

III.8.1 Neighbor State

The OSPF neighbor states indicate the progress and status of the neighbor relationship. The following table describes those states:

State	Description
Down	At this initial point, the communication has not been established for routers. No Hello packet has been received by the router.
Attempt	This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval**.[39]**
Init	One router in this state has received a Hello packet from a neighboring router, indicating the possibility of establishing a neighbor relationship. However, bidirectional communication has not yet been verified.

Two-Way	After establishing bidirectional communication, routers move to the Two-Way state by exchanging Hello packets and confirming that traffic can be sent and received on the OSPF interface. In multi-access networks, DR and BDR can be elected if they were needed.
Exstart	Indicates that the routers are preparing to share link state information. Master/slave relationships are formed between routers to determine who will begin the exchange**.[40]**
Exchange	During this phase, the routers share Database Description (DBD) packets in order to compare the information in their Link State Databases (LSDBs) and detect any missing or outdated Link State Advertisements (LSAs) that require updating or exchanging.
Loading	During the Loading phase, OSPF routers exchange Link State Request (LSR) and Link State Update (LSU) packets to request and receive any missing or outdated link-state information.
Full	This state indicates that routers have successfully synchronized their link-state databases, fully understand the network's topology, and are ready to make routing decisions and forward traffic.

Table III-2 Description of OSPF Neighbor States

III.8.2 Establishing OSPF Neighbor Relationships

OSPF adjacency is the process of establishing a connection between OSPF routers to exchange routing information. This allows routers to share updates and keep an accurate network topology view.

OSPF adjacency involves a series of steps, including the following:

Step 1: Hello Packet Exchange

During the Hello Packet Exchange phase, a router transmits Hello packets on its interfaces, which are then received and processed by neighboring routers. Afterwards, the neighboring routers examine the information contained in the Hello packets.

Step 2: Parameter Matching

Routers compare the parameters within the Hello packets to determine compatibility and form an adjacency.

OSPF routers will only become neighbors if the following parameters within Hello packet are identical on each router **[40]:**

• Area ID

• Area Type (stub, NSSA, etc.)

• Prefix

• Subnet Mask

• Hello Interval

• Dead Interval

• Network Type (broadcast, point-to-point, etc.)

• Authentication

If the parameters in the Hello packets exchanged during the OSPF adjacency formation do not match between routers, they will be unable to establish an adjacency.

Step 3: Master/Slave Relation

OSPF neighbor adjacency uses the Master/Slave determination to establish communication between routers based on priority. The router with a higher RID is the master, initiating the exchange process; while the router with a lower RID is the slave. The master sends a summary packet of the Link State Database, followed by the slave router sending its DBD packet.

Step 4: Database Synchronization

Routers exchange Database Description Packets during OSPF adjacency formation to synchronize their link-state databases. In case of any differences between the databases, routers

exchange LSR and LSU packets. This entire process guarantees that the link-state information across the OSPF network remains consistent and up-to-date.

Step 5: Full Neighbor State

In the Full state, routers have synchronized link-state databases and a comprehensive understanding of the network's topology. By sharing routing updates through LSU packets, they establish a fully functional OSPF adjacency. This enables them to make informed routing decisions using up-to-date network data.

Figure III-13 summarizes the process for forming OSPF neighbor adjacencies between two routers.

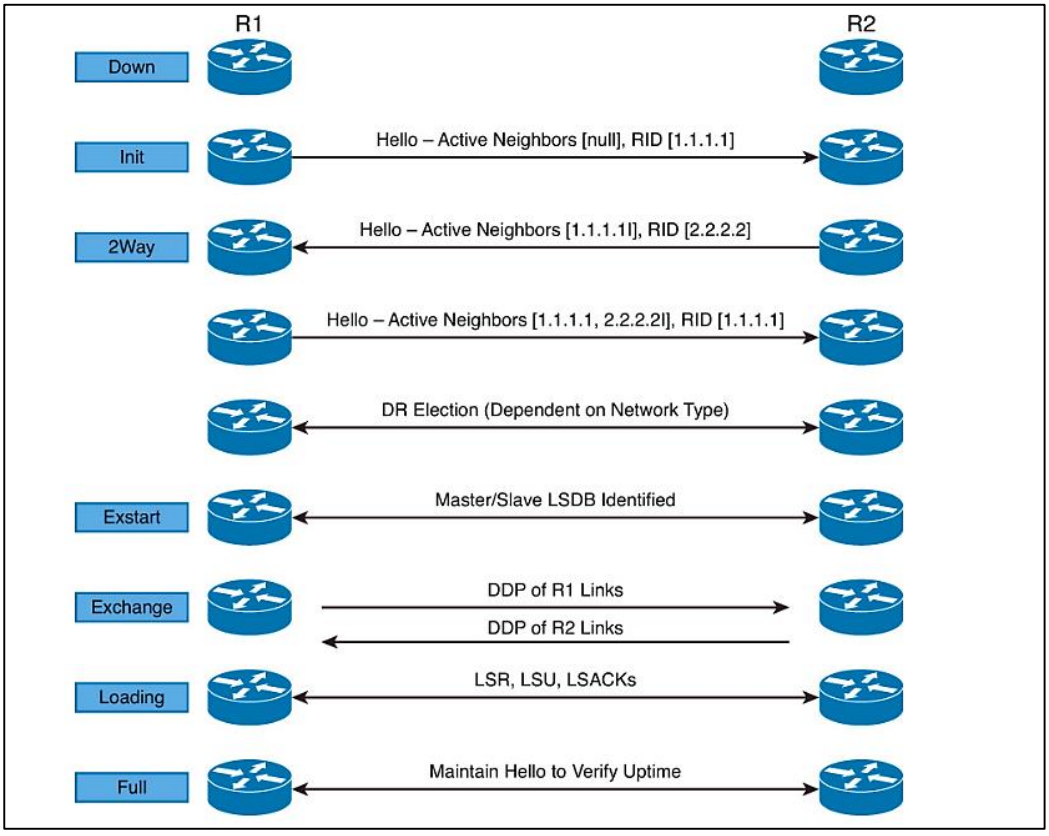

Figure III-13 Process for Forming OSPF Neighbor Adjacencies. [**38]**

III.9 OSPF Tables

The OSPF tables work together to share routing information, calculate the most efficient path, and identify the best routes within the OSPF domain. Each table has a specific

purpose and provides important details for OSPF routers to make informed routing decisions and transmit packets efficiently. The OSPF tables are as follows:

III.9.1 Neighbor Table

Neighbor table to keep a list of routers that form a relationship, and status of the designated router/backup designated router, and the status of the link, hello, and dead time interval **[41].** The OSPF neighbor table facilitates the establishment and maintenance of OSPF adjacencies between routers, as well as monitoring the status and characteristics of these adjacencies.

III.9.2 Topology Table

The OSPF Topology Table, also known as the SPF Tree or Shortest Path Tree, is a table utilized in the OSPF SPF algorithm to represent the network topology as a tree with the router as the root. This table is generated by examining the LSDB and calculating the shortest path to each network prefix based on OSPF cost metrics. It serves as the basis for building the OSPF routing table.

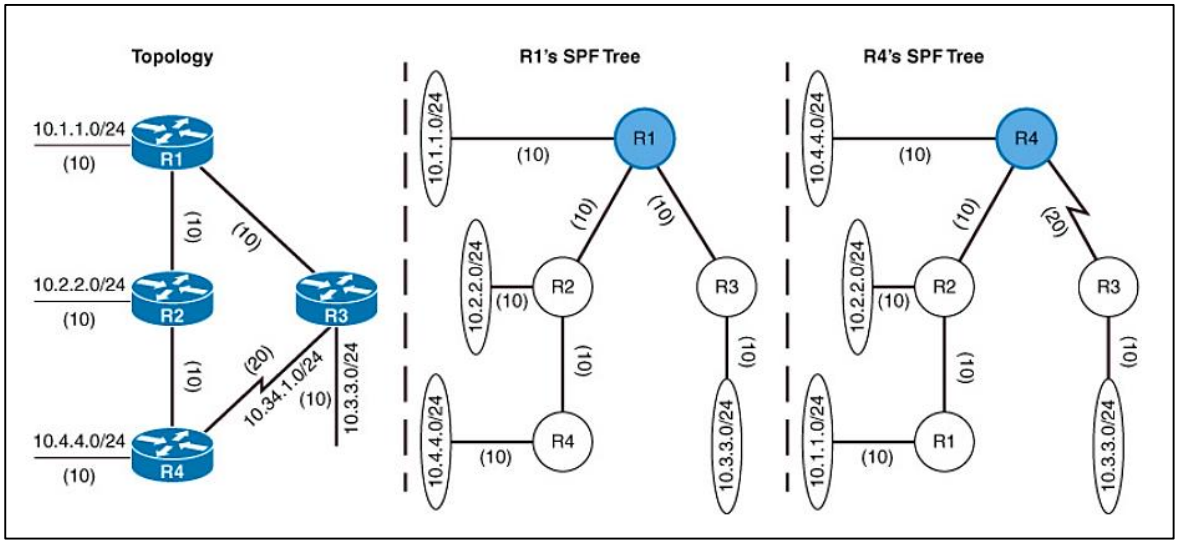

Figure III-14 Representation of OSPF Topology Table**. [38]**

III.9.3 Routing Table

The main table utilized for determining forwarding paths is the OSPF Routing Table. It stores the shortest path routes to various destination networks within the OSPF domain, along

with details like network prefixes, next-hop routers, outgoing interfaces, and OSPF cost metrics. This table is constructed using data from the LSDB and the OSPF SPF algorithm.

III.10 OSPF Metric

The OSPF metric is a numerical value that represents the cost or preference of a specific route or path. It is calculated based on the configured bandwidth of the links. By default, OSPF uses the inverse of the link bandwidth as the metric, meaning that links with higher bandwidths have lower metric values. As a result, these links are considered more favorable and are more likely to be selected as the preferred path.

The formula used to calculate the metric of one interface is **[42]:**

$$metric = \frac{reference\ bandwidh}{bandwidth}$$

By default, the reference bandwidth in OSPF is set to 100 Mbps. It is possible to alter or adapt it to a varying value depending on the specific needs of the network.

III.11 OSPF Convergence

The OSPF convergence process entails OSPF routers swiftly adapting to network topology changes. This process involves identifying topology changes, such as link failures, and recalculating routes. With OSPF's rapid convergence, routers can promptly adjust, guaranteeing efficient and dependable routing.

Routing convergence consists of two components:

III.11.1 Detection of Topology Changes

OSPF routers utilize various techniques, such as hello packets and keep lives, to effectively monitor the status of neighboring routers and promptly detect any modifications in the network's structure, such as link failures or new connections.

III.11.2 Recalculation of Routes

After a failure has been detected, the router that detected the failure sends a link-state packet with the change information to all routers in the area. All the routers recalculate all their routes by using the Dijkstra (or SPF) algorithm **[27].**

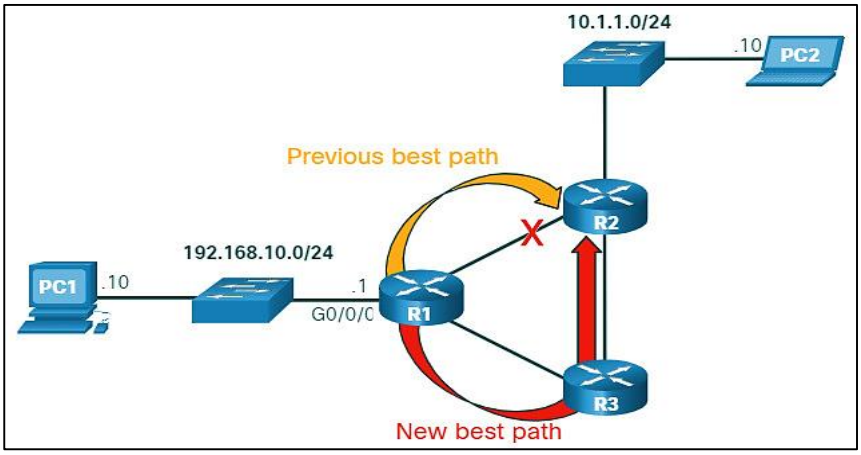

Figure III-15 Recalculation of Routes

Figure III-15 illustrate the operation of Recalculation of routes**.**

III.12 OSPF Operation

The main operation of the OSPF protocol occurs in the following consecutive stages and leads to the convergence of the internetwork **[43]:**

1. Compiling the LSDB.
2. Calculating the Shortest Path First (SPF) Tree.
3. Creating the routing table entries.

III.12.1 Compiling the LSDB

During this phase, OSPF routers exchange LSAs to create the LSDB and gather information about the network's topology. Each router sends out its own LSA containing its configuration. When a router receives LSAs from other routers, it passes them on to its neighboring routers. This process allows routers to build a complete picture of the network's topology in the LSDB.

III.12.2 Calculating the Shortest Path First Tree

After gathering information from the LSDB, OSPF routers run the SPF algorithm to determine the best route to each network in the network topology. Using Dijkstra's algorithm and the LSDB, the SPF algorithm calculates the most efficient path by considering the overall metrics. This results in the creation of the SPF Tree.

III.12.3 Creating the Routing Table Entries

Routing table entries are established using the SPF Tree. These entries include details regarding destination networks, next-hop routers, outgoing interfaces, and metrics. Routers utilize these entries to optimize packet-forwarding choices. The routing table entries are regularly updated to adapt to changes in the network's topology.

III.13 OSPF Authentication

OSPF authentication is used to confirm the authenticity of OSPF routing updates shared among routers, ensuring that only trusted routers are involved in the OSPF routing process and preventing unauthorized or malicious routers from introducing incorrect routing information into the network.

The OSPF authentication type and authentication data are carried in the header of every OSPF message. The Au Type field indicates the type of authentication used **[44]:**

Au Type = 0 — Null (no authentication) authentication

Au Type = 1— Simple password authentication

Au Type = 2— MD5 cryptographic authentication

III.13.1 Null Authentication

This authentication type does not utilize any authentication mechanisms. It means that OSPF packets are not verified, and routers accept all OSPF updates from neighboring routers without any authentication. Null authentication is the default configuration in OSPF.

III.13.2 Simple Password Authentication

Also known as Plain Text Authentication, this technique involves using a common password or key that is set up on OSPF interfaces. Routers exchange OSPF packets that include the password in clear text. Upon receiving an OSPF packet, a router verifies the received password against the locally configured password. If they are identical, the packet is considered authentic.

III.13.3 MD5 Cryptographic Authentication

In OSPF, MD5 authentication requires a shared secret key on all routers. A message digest is created using the MD5 algorithm during packet exchange, combining packet fields and the shared key. The receiving router independently calculates the digest and compares it with the received digest. If they match, the packet is considered authentic, and the router trusts the source. If they do not match, the packet is unauthenticated.

III.14 OSPF in Modern Network Infrastructures

III.14.1 Enterprise Networks

OSPF is commonly utilized in enterprise networks, including those present in sizable corporations, government entities, or educational establishments. It facilitates effective routing within the internal network structure of the organization, fostering smooth connectivity among different departments, offices, and data centers.

The following figure represents an example of a conceptual model of an enterprise network system based on OSPF:

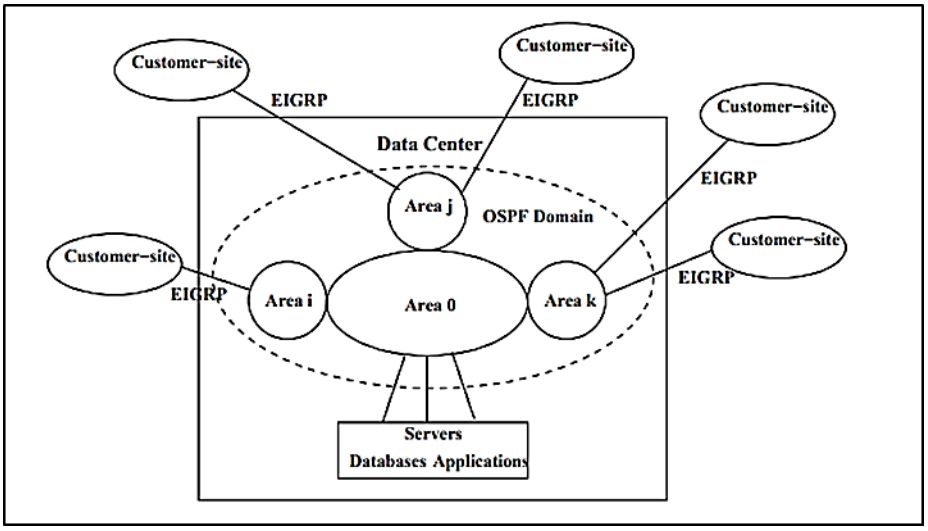

Figure III-16 Enterprise Network Topology Based on OSPF **[45].**

III.14.2 Internet Service Provider Networks

ISPs commonly use OSPF to direct traffic in their backbone networks and regional networks. OSPF provides ISPs with the capability to improve routing, regulate traffic flow, and ensure consistent connectivity for their customers. The scalability and resilience of this protocol make it a suitable choice for the intricate and extensive networks operated by modern ISPs.

III.14.3 Internet Exchange Point Networks

IXPs are vital hubs where ISPs and network providers connect their networks. OSPF implementation at these points effectively manages routing between networks, enabling smooth traffic exchange and efficient peering. OSPF at IXPs ensures uninterrupted connectivity and optimal routing for diverse network infrastructures.

III.15 Advantages and Disadvantages of OSPF

III.15.1 Advantages

- Runs on most routers, ensuring smooth communication between devices.
- Utilizes the SPF algorithm to provide a loop-free topology.

- Fast convergence in dynamic network environments.
- Supports ECMP routing for load balancing.
- Hierarchical design with routing areas for increased efficiency.
- Scalable and capable of handling large networks.

III.15.2 Disadvantages

- Managing and configuring networks is challenging, especially in large networks.
- Requires significant network resources (memory, CPU, bandwidth).
- The SFP algorithm requires high CPU usage **[46].**
- More memory is needed to maintain neighborhood tables, routing and topology **[46].**

III.16 Conclusion

This chapter has provided a comprehensive examination of OSPF, a highly effective link-state routing protocol. Our exploration has revealed that OSPF offers scalability, resilience, and efficient routing in extensive and intricate network environments. The use of metrics allows OSPF routers to make optimal decisions regarding path selection, while zone segmentation enhances scalability and reduces routing burdens.

Network convergence ensures consistent and up-to-date routing information, and OSPF authentication provides protection against unauthorized access. Additionally, we have discussed the benefits of OSPF, including its support for large networks, rapid convergence, and inherent load balancing capabilities.

However, we have also acknowledged the potential challenges associated with OSPF, such as complex configuration requirements and increased resource demands.

Chapter IV:

OSPF Optimization: Strategies for Improved Network Routing

IV. Introduction

In the final chapter, we will explore the revamp of a current network structure with the goal of enhancing the functionality of the OSPF protocol. The initial structure, as detailed in the mentioned article **[47],** encountered various challenges that had a negative impact on the effectiveness of OSPF and the overall network operation. To tackle these challenges, we have taken on the task of rethinking the structure, with a particular emphasis on decreasing latency, streamlining routing, and reducing the OSPF cost. Through a comprehensive evaluation of the current structure and considering the specific needs of the network, we have devised a new layout that aims to resolve the previously identified issues, enhance OSPF efficiency, and demonstrate how the new layout aligns with OSPF best practices.

IV.1 Cisco Packet Tracer in Network Simulation

Cisco Packet Tracer is a versatile network simulation tool developed by Cisco Systems. It provides a platform for designing, configuring, and troubleshooting computer networks in a virtual environment. Originally designed for educational purposes, Packet Tracer has become widely utilized by networking professionals, students, and instructors worldwide.

This software offers a user-friendly graphical interface that allows users to simulate networks by connecting various virtual network devices, such as routers, switches, PCs, servers, and more. Through it, users can create complex network topologies, implement different networking protocols, and test configurations without the need for physical hardware.

Figure IV.1 below shows a general overview of Packet Tracer

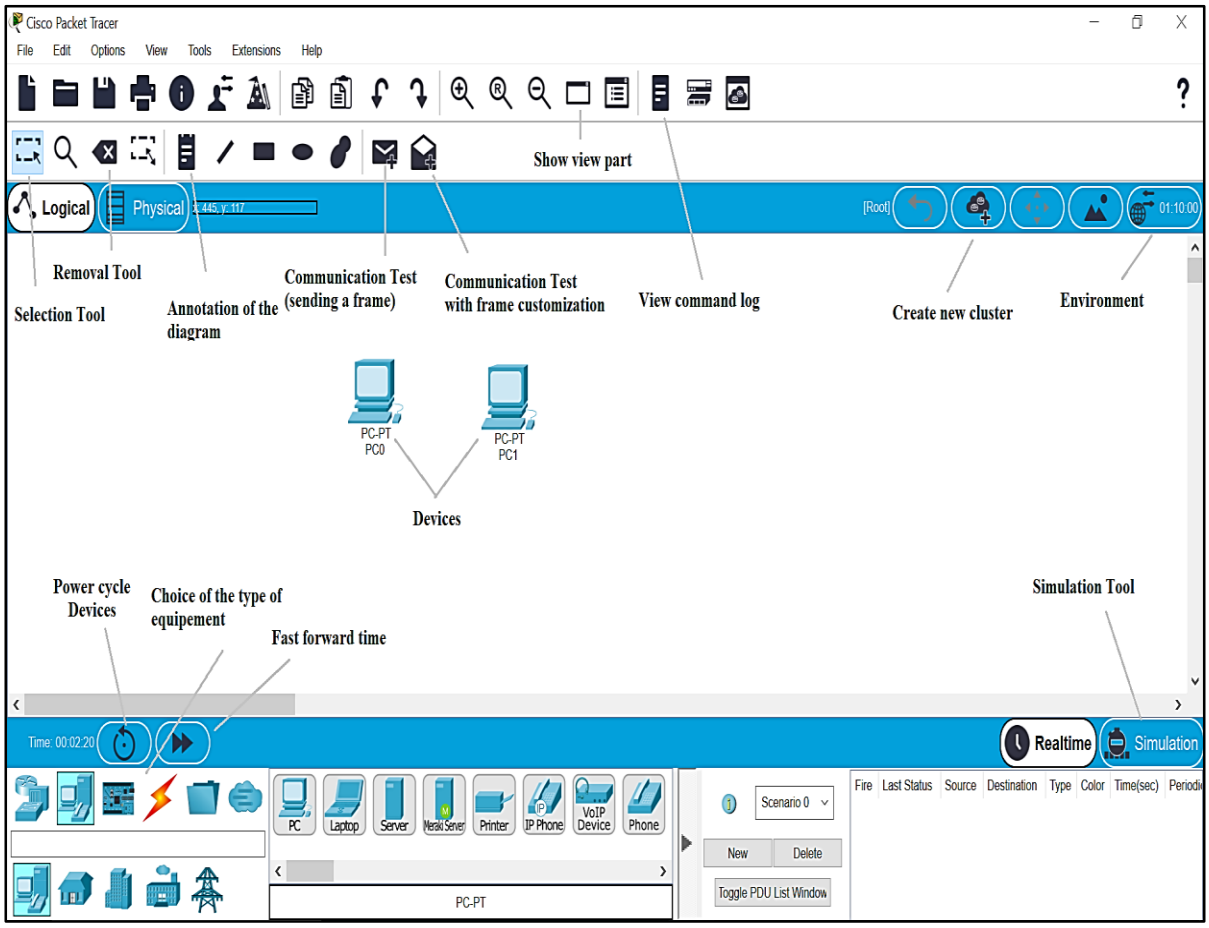

Figure IV.1 Packet Tracer Simulator Tasks

The user builds his network in the work area according to his topology, the equipment is grouped into categories (router, switch or PC).When a category is selected, the user can choose between several different devices:

- **Routers:** router 1941, router 1841, router 2911, PT-Router, PT-Empty...
- **Switches :** PT Switch, 2960 …
- **End Devices :** PCs , Laptop , server …
- **Connection :** we have cables like (Copper straight , Serial DTE …)

We will utilize a combination of interface types as we design our topology, incorporating the modules shown in the Figure IV.2

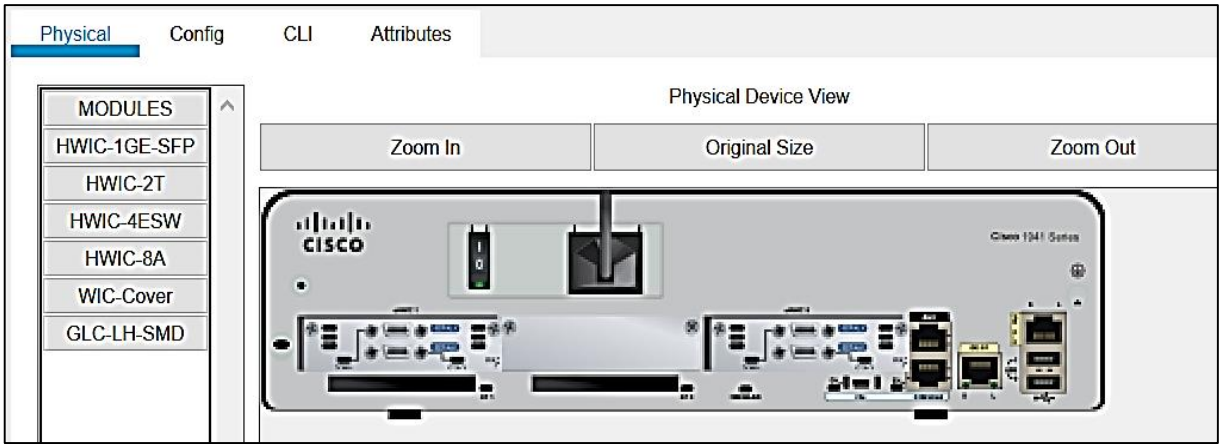

Figure IV.2 The Modules of Router 1941

We've activated Serial interfaces by following those steps:

- **Step 1 :** Device must be turned off
- **Step 2 :** Adding HWIC-2T Module to device
- **Step 3 :** Device must be Powered ON to finish the process

We chose Copper Straight-Through cables, to connect the GigaEthernet interfaces in order to interconnect the main routers with the PCs. To interconnect the routers with different IP addresses, we chose serial links.

IV.2 Methodology for Network Upgrade and Performance Evaluation

To ensure a comprehensive and systematic approach to revamping the network, we followed a detailed methodology that involved multiple iterative phases. This process aimed to identify and rectify existing issues, compare performance metrics, and implement enhancements in a step-by-step manner.

The following activity diagram illustrates the key phases of our methodology:

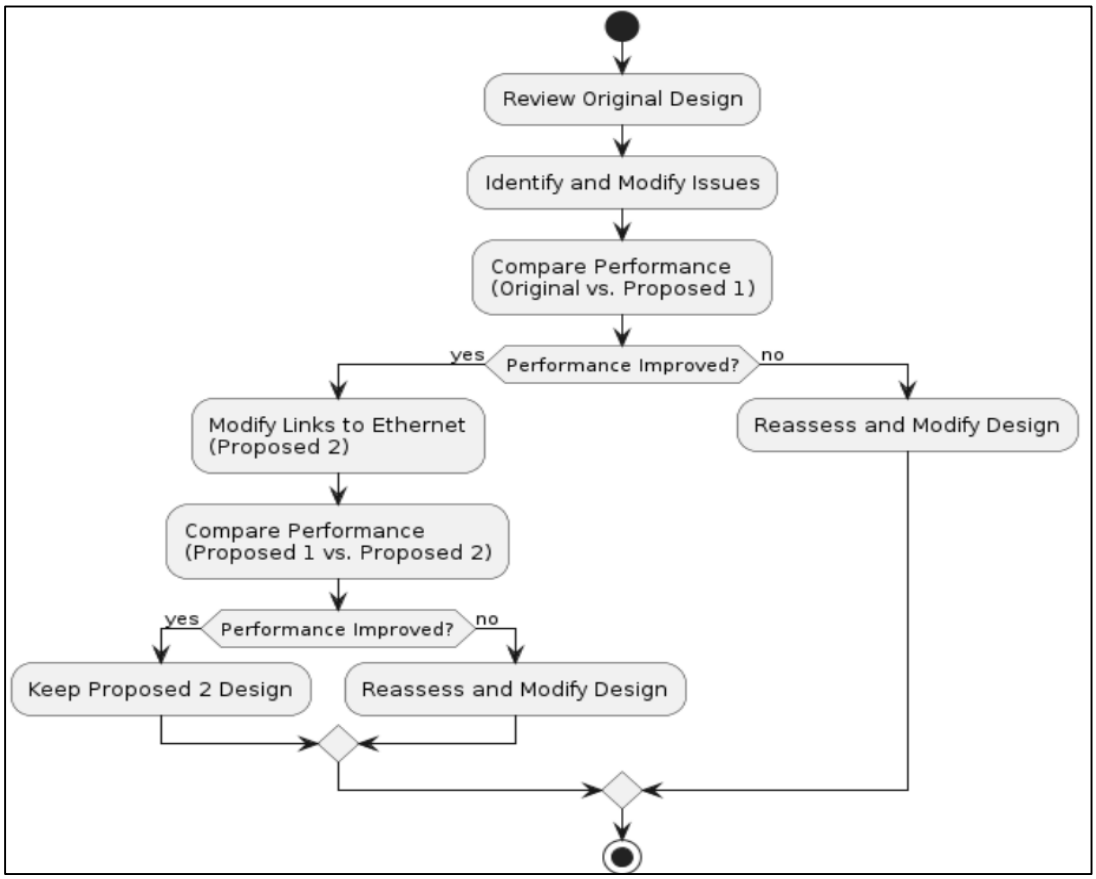

Figure IV.3 Systematic Network Design Improvement Methodology

IV.3 Analysis of Current Network Design

The original topology outlined in the article **[47]** was designed to address the challenges associated with peering connections across multiple regions, autonomous systems (ASes), and stub networks by utilizing the OSPF protocol. OSPF played a crucial role within the internal gateway protocol (IGP) of the ISP/IXP network. The network configuration featured a variety of OSPF areas, including the Backbone Area, Standard Area, Stub Area, NSSA, and discontinuous area. In addition to OSPF, the authors incorporated other protocols, such as EIGRP and RIP. The network design comprised different types of OSPF routers, such as the Backbone Area Router (BR), Internal Router (IR), Area Border Router (ABR), and AS Border Router (ASBR), as shown in the following figure.

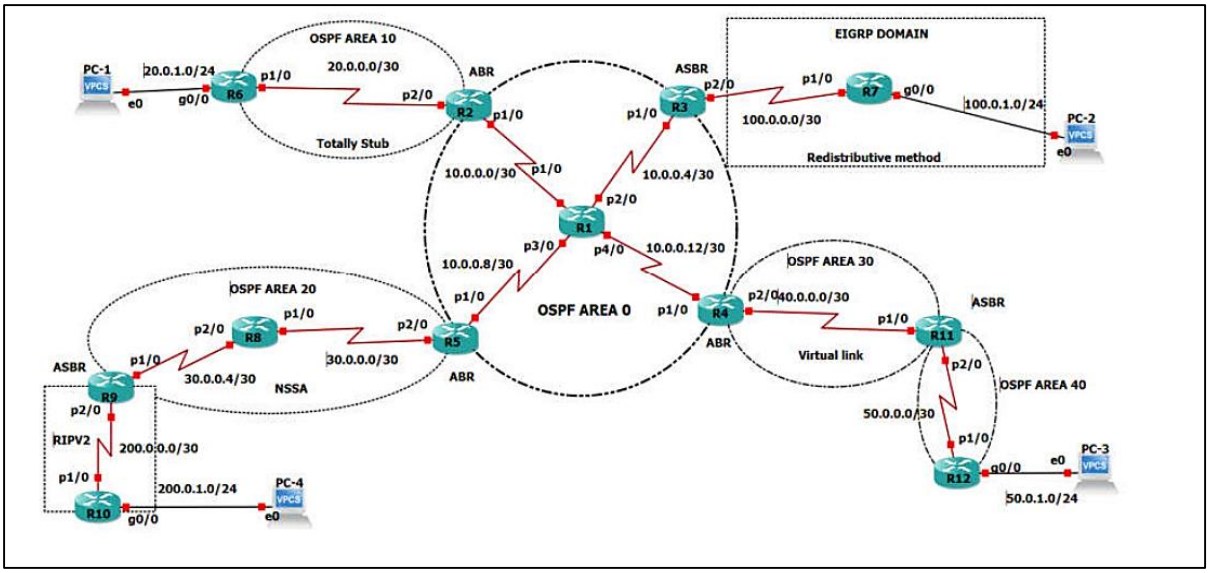

Figure IV.4 Implementation Design Structure of Multiple Areas, Stubs and Protocols **[47]**

The hub-and-spoke topology used in the OSPF backbone area presents several disadvantages. This topology inherently has a single point of failure at the central router, which can disrupt communication across the network if the router fails. Scalability is another issue, as the central router must handle increasing traffic from all connected spokes, potentially leading to performance bottlenecks. Additionally, routing inefficiencies arise because all inter-spoke traffic must traverse the central router, causing higher latency and bandwidth constraints. Moreover, using RIP version 2 (RIPv2) exacerbates these issues with its limited 15-hop count, slow convergence, high bandwidth usage, lack of advanced features, and weak security.

IV.4 Upgrading the Original Network Design

To address the issues of the original design, we plan to upgrade the backbone area's topology from a hub-and-spoke configuration to a full mesh topology. This transformation aims to enhance network resilience, improve redundancy, and provide multiple paths for traffic flow, thereby increasing overall network efficiency. Additionally, we intend to replace the RIPv2 routing protocol with a Not-So-Stubby Area (NSSA) configuration using OSPF. This change will overcome the limitations of RIPv2, offering a more robust and flexible routing solution.

Figure IV.5 illustrates our proposed design structure.

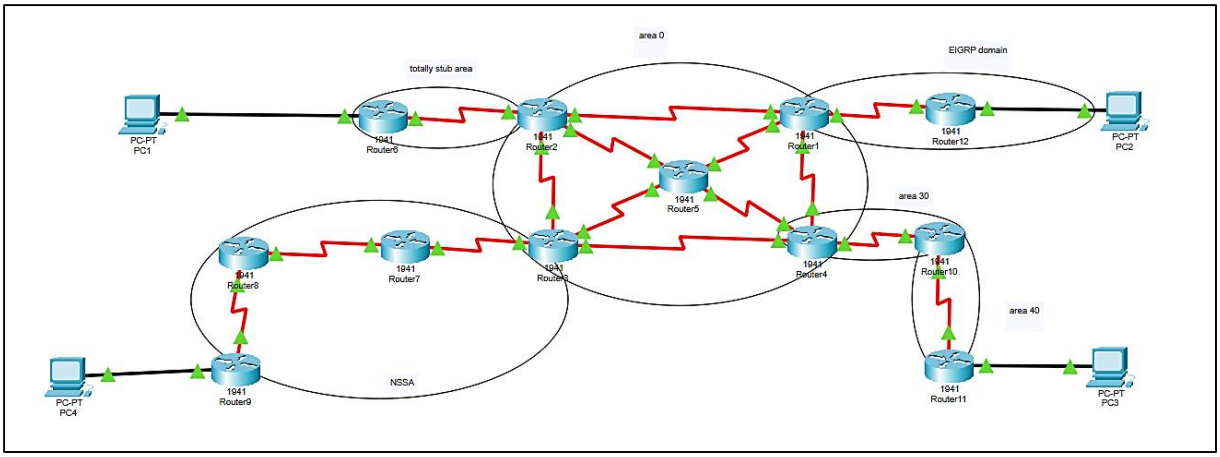

Figure IV.5 Structure of Proposed Design

IV.5 Addressing Plan

The table below summarizes the static assignment of IP/mask addresses to router interfaces with their appropriate zone.

Pereferic	Interface	IP Address	Mask	Zone
Router 1	S 0/0/0	10.0.0.1	255.0.0.0	Area 0
	S 0/0/1	12.0.0.1	255.0.0.0	Area 0
	S 0/1/0	11.0.0.1	255.0.0.0	Area 0
	S 0/1/1	80.0.0.1	255.0.0.0	EIGRP
Router 2	S 0/0/0	10.0.0.2	255.0.0.0	Area 0
	S 0/0/1	13.0.0.1	255.0.0.0	Area 0
	S 0/1/0	14.0.0.2	255.0.0.0	Area 0
	S 0/1/1	20.0.0.2	255.0.0.0	Area 10
Router 3	S 0/0/0	13.0.0.2	255.0.0.0	Area 0
	S 0/0/1	15.0.0.1	255.0.0.0	Area 0
	S 0/1/0	17.0.0.2	255.0.0.0	Area 0
	S 0/1/1	40.0.0.2	255.0.0.0	Area 20

Router 4	S 0/0/0	12.0.0.2	255.0.0.0	Area 0
	S 0/0/1	15.0.0.2	255.0.0.0	Area 0
	S 0/1/0	16.0.0.1	255.0.0.0	Area 0
	S 0/1/1	60.0.0.1	255.0.0.0	Area 30
Router 5	S 0/0/0	11.0.0.2	255.0.0.0	Area 0
	S 0/0/1	14.0.0.1	255.0.0.0	Area 0
	S 0/1/0	17.0.0.1	255.0.0.0	Area 0
	S 0/1/1	16.0.0.2	255.0.0.0	Area 0
Router 6	S 0/0/0	20.0.0.1	255.0.0.0	Area 10
	GE 0	9.0.0.1	255.0.0.0	Area 10
Router 7	S 0/0/0	40.0.0.1	255.0.0.0	Area 20
	S 0/0/1	50.0.0.1	255.0.0.0	Area 20
Router 8	S 0/0/0	50.0.0.2	255.0.0.0	Area 20
	S 0/0/1	90.0.0.1	255.0.0.0	Area 20
Router 9	GE 0	19.0.0.1	255.0.0.0	Area 20
	S 0/0/0	90.0.0.2	255.0.0.0	Area 20
Router 10	S 0/0/0	60.0.0.2	255.0.0.0	Area 30
	S 0/0/1	70.0.0.1	255.0.0.0	Area 40
Router 11	S 0/0/0	70.0.0.2	255.0.0.0	Area 40
	GE 0	18.0.0.2	255.0.0.0	Area 40
Router 12	GE 0	8.0.0.2	255.0.0.0	EIGRP

	S 0/0/0	**80.0.0.2**	**255.0.0.0**	**EIGRP**
PC1	**Net Card**	**9.0.0.2**	**255.0.0.0**	**Area 10**
PC2	**Net Card**	**19.0.0.2**	**255.0.0.0**	**EIGRP**
PC3	**Net Card**	**18.0.0.1**	**255.0.0.0**	**Area 40**
PC4	**Net Card**	**8.0.0.1**	**255.0.0.0**	**Area 20**

Table IV.1 Addressing Table

IV.6 Topology Configuration

IV.6.1 Configuring Interfaces and Router Names

The following Exec modes provide different levels of access and control over the router's configuration and operation:

User EXEC Mode

This mode is automatically initiated as the default mode. This mode offers restricted access to fundamental monitoring and troubleshooting commands, with the prompt concluding with a ">" symbol.

The Privileged EXEC Mode

Also referred to as Enable Mode or Privileged Mode, grants users complete access to the router's configuration and allows the execution of privileged commands. Access to this mode is gained by issuing the **"enable"** command from the User EXEC mode and providing the privileged password if one has been set. The prompt for this mode usually concludes with a "#" symbol.

Global Configuration Mode

This mode allows users to modify router settings that affect the entire system. To enter this mode, users must type **"configure terminal"** from privileged EXEC mode. In Global Configuration Mode, users can configure interfaces, routing protocols, security features, and more. The prompt typically shows the router's hostname followed by **"(config) #".**

Interface Configuration Mode

This mode allows users to configure individual router interfaces. To access this mode, use the command **"interface [interface-name]"** in global configuration mode. Here, users can configure settings such as IP addresses, encapsulation, and bandwidth. The prompt in this mode typically shows the router's hostname followed by **"(config-if) #".**

The following figure illustrates the configuration of Router1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#
Router1(config)#interface Serial0/0/0
Router1(config-if)#ip address 10.0.0.1 255.0.0.0
Router1(config-if)#ip address 10.0.0.1 255.0.0.0
Router1(config-if)#no shutdown
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/0/1
Router1(config-if)#ip address 11.0.0.1 255.0.0.0
Router1(config-if)#ip address 11.0.0.1 255.0.0.0
Router1(config-if)#no shutdown
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/1/0
Router1(config-if)#ip address 12.0.0.1 255.0.0.0
Router1(config-if)#ip address 12.0.0.1 255.0.0.0
Router1(config-if)#no shutdown
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/1/1
Router1(config-if)#ip address 80.0.0.1 255.0.0.0
Router1(config-if)#ip address 80.0.0.1 255.0.0.0
Router1(config-if)#no shutdown
Router1(config-if)#do wr
Building configuration...
[OK]
```

Figure IV.6 Router 1 Configuration

IV.6.2 Configuring the OSPF Protocol on Routers

OSPF is configured by employing the **"router ospf process-id"** command in the global configuration. To differentiate routers within its topology, OSPF utilizes IP addresses to create identifiers. However, IOS allows for the direct assignment of a router's RID using the **"router-id"** command. This specific command was chosen to set the identifier of each router. Additionally, OSPF network configuration involves specifying the networks to participate in OSPF routing using the **"network"** command, followed by the network address and wildcard mask.

```
Router1(config)#router ospf 1
Router1(config-router)#router-id 0.0.0.1
Router1(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router1(config-router)#network 11.0.0.0 0.0.0.255 area 0
Router1(config-router)#network 12.0.0.0 0.0.0.255 area 0
Router1(config-router)#do wr
Building configuration...
[OK]
```

Figure IV.7 Router 1 OSPF Configuration

IV.6.3 Configuration of OSPF Areas

IV.6.3.1 Totally Stubby Area

To define an area as a totally stub area, we will use the "**area-id stub no-summary"** command in router configuration mode.

```
Router6(config)#router ospf 1
Router6(config-router)#router-id 0.0.0.6
Router6(config-router)#network 20.0.0.0 0.0.0.255 area 10
Router6(config-router)#network 9.0.0.0 0.0.0.255 area 10
Router6(config-router)#area 10 stub no-summary
Router6(config-router)#do wr
Building configuration...
[OK]
```

Figure IV.8 Router 6 OSPF Configuration Totally Stub Area

IV.6.3.2 Not-So-Stubby Area

To configure an OSPF area as a Not-So-Stubby Area (NSSA), we will use the following command: "**area-id nssa.** "We will also configure the "**default-information originate"** command on the ABR connecting the NSSA area to the OSPF backbone, which generates a type-7 NSSA external default route. This default route will be later distributed throughout the NSSA area, allowing routers in the NSSA area to reach destinations in the EIGRP domain through the OSPF backbone.

By combining these commands, we can control the flow of external routing information and provide a clear default path for external traffic.

```
Router7(config)#router ospf 1
Router7(config-router)#router-id 0.0.0.7
Router7(config-router)#network 40.0.0.0 0.0.0.255 area 20
Router7(config-router)#network 50.0.0.0 0.0.0.255 area 20
Router7(config-router)#area 20 nssa
Router7(config-router)#default-information originate
Router7(config-router)#do wr
Building configuration...
[OK]
```

Figure IV.9 Router 7 OSPF Configuration (NSSA)

IV.6.4 Configuring the OSPF authentication

In this configuration, we are setting up MD5 cryptographic authentication for OSPF on Router1.

First, we will configure the OSPF MD5 authentication on each interface of Router1 using the"**ip ospf message-digest-key [key ID] md5 [password]"** command as illustrated in Figure IV.10. This applies the MD5 authentication to each specific interface.

Next, we will enable message-digest (MD5) authentication on the same interface using the"**ip ospf authentication message-digest"** command.

```
Router1(config)#
Router1(config)#interface Serial0/0/0
Router1(config-if)#ip ospf message-digest-key 1 md5 OSPFpassw0rd
Router1(config-if)#ip ospf authentication message-digest
Router1(config-if)#interface Serial0/0/1
Router1(config-if)#ip ospf message-digest-key 1 md5 OSPFpassw0rd
Router1(config-if)#ip ospf authentication message-digest
Router1(config-if)#interface Serial0/1/0
Router1(config-if)#ip ospf message-digest-key 1 md5 OSPFpassw0rd
Router1(config-if)#ip ospf authentication message-digest
Router1(config-if)#interface Serial0/1/1
Router1(config-if)#ip ospf message-digest-key 1 md5 OSPFpassw0rd
Router1(config-if)#ip ospf authentication message-digest
Router1(config-if)#do wr
Building configuration...
[OK]
```

Figure IV.10 Router 1 OSPF Authentication Configuration

In the router OSPF configuration section, we will enable message-digest authentication for the entire OSPF area 0 using the "**area ID authentication message-digest**" command as shown in Figure IV.11.

```
Router1(config)#router ospf 1
Router1(config-router)#area 0 authentication message-digest
Router1(config-router)#do wr
Building configuration...
[OK]
```

Figure IV.11 Router OSPF Area 0 Configuration

IV.6.5 Redistribution Method

To configure redistribution between OSPF and EIGRP, we will utilize the following commands at the border router:

For redistributing OSPF into EIGRP, we will employ **"router eigrp <eigrp process-id>"** followed by **"redistribute ospf <ospf process-id> metric <metric-values>."**

For redistribute EIGRP into OSPF, initiate **"router ospf <ospf process-id>"** and then **"redistribute eigrp <eigrp process-id> subnets.**

```
Router1(config)#router ospf 1
Router1(config-router)#redistribute eigrp 1 subnets
Router1(config-router)#exit
Router1(config)#router eigrp 1
Router1(config-router)#redistribute ospf 1 metric 1544 20000 255 1 1500
Router1(config-router)#do wr
Building configuration...
[OK]
```

Figure IV.12 Configuration of Redistribution Method

IV.6.6 Computers Configuration

In the Packet Tracer simulator, we have the ability to assign IP addresses to computers within the **"Desktop"** tab. By accessing the **"IP Configuration"** window, we are able to configure the network parameters for the computers (PC1 to PC4), including the IP address, subnet mask, and gateway.

IV.7 Verification and Interpretation of the Implementation

IV.7.1 Verification of IP Addressing and Interfaces

Verifying IP addressing and interfaces on a Cisco device is crucial for precise network configuration, resolving connectivity issues, and ensuring network reliability.

It helps detect misconfigurations or conflicts that hinder connectivity and confirms physical and logical connections for effective troubleshooting. To see the IP addresses configured on the interfaces of Router1, we will use the command **"sh ip interface brief ".**

```
Router1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.0.0.1        YES manual up                    up
Serial0/0/1            12.0.0.1        YES manual up                    up
Serial0/1/0            11.0.0.1        YES manual up                    up
Serial0/1/1            80.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Figure IV.13 Verification of IP Addresses and Interfaces on Router 1

IV.7.2 Verification of the Routing Protocols Functionality

To ensure the proper functioning of a routing protocol, it is essential to verify that it operates accurately and efficiently within a network environment. In order to accomplish this, we will employ the subsequent command **" show ip protocol "**for Router1.

The figure below represents the operation of the "**show ip protocol**" command.

```
Router1#sh ip protocol

Routing Protocol is "eigrp  1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 1, ospf 1
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.0.0.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: enabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     80.0.0.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
    80.0.0.2        90            5911988
  Distance: internal 90 external 170



Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.0.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
    eigrp 1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.0.0.255 area 0
    11.0.0.0 0.0.0.255 area 0
    12.0.0.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    0.0.0.1              110      00:02:32
    0.0.0.2              110      00:02:02
    0.0.0.3              110      00:01:43
    0.0.0.4              110      00:01:13
    0.0.0.5              110      00:01:13
    0.0.0.10             110      00:22:12
  Distance: (default is 110)
```

Figure IV.14 Routing Protocols Verification on Router 1

IV.7.3 OSPF Interfaces Verification

Adding an interface to the OSPF process is synonymous with establishing a link. OSPF relies on interfaces to identify neighboring devices, exchange routing data, and construct its

routing table. Each OSPF-enabled interface possesses its unique set of parameters and assumes the duty of disseminating network topology information to its OSPF neighbors.

The **"show ip ospf interface"** command provides a comprehensive overview of the configuration shown in Figure IV.15 and the status of OSPF-enabled interfaces. Executing this command reveals that MD5 authentication is enabled on the interface, with the authentication key identified by the key ID 1.

```
Router1#sh ip ospf interface

Serial0/0/0 is up, line protocol is up
  Internet address is 10.0.0.1/8, Area 0
  Process ID 1, Router ID 0.0.0.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 0.0.0.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Serial0/1/0 is up, line protocol is up
  Internet address is 11.0.0.1/8, Area 0
  Process ID 1, Router ID 0.0.0.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 0.0.0.5
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

```
Serial0/0/1 is up, line protocol is up
  Internet address is 12.0.0.1/8, Area 0
  Process ID 1, Router ID 0.0.0.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 0.0.0.4
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Figure IV.15 Router 1 OSPF Interfaces Verification

IV.7.4 Neighboring Routers Verification

Verifying the connectivity of neighboring routers is essential to ensure that OSPF adjacencies are established and maintained, allowing for the smooth exchange of routing information. To achieve this, the following command can be used: **"sh ip ospf neighbor".**

```
Router1#
Router1#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.5           0   FULL/  -        00:00:39    11.0.0.2        Serial0/1/0
0.0.0.4           0   FULL/  -        00:00:38    12.0.0.2        Serial0/0/1
0.0.0.2           0   FULL/  -        00:00:31    10.0.0.2        Serial0/0/0
```

Figure IV.16 Router 1 Verification of Neighbor Routers

The **"State"** column shows **"FULL"** for all OSPF neighbors, indicating that the authentication is successful.

IV.7.5 Verification of the Link State Database

The LSDB contains the various types of LSAs packets generated or collected by a router based on the areas it belongs to. The reliability of LSAs propagation across a zone depends on the reliability of the links between routers.

By using the command **"show ip ospf database",** it is possible to observe the content of the database, as represented in Figure IV.17:

```
Router1#sh ip ospf database
            OSPF Router with ID (0.0.0.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
0.0.0.1         0.0.0.1         473         0x80000007 0x0059d5 6
0.0.0.5         0.0.0.5         473         0x80000009 0x005004 8
0.0.0.4         0.0.0.4         464         0x80000008 0x00c8b3 7
0.0.0.2         0.0.0.2         464         0x80000007 0x004ed7 6
0.0.0.10        0.0.0.10        463         0x80000002 0x00b704 1
0.0.0.3         0.0.0.3         310         0x80000008 0x0029e5 6

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
40.0.0.0        0.0.0.3         464         0x80000001 0x00f003
20.0.0.0        0.0.0.2         464         0x80000001 0x00fa0e
9.0.0.0         0.0.0.2         464         0x80000002 0x00927f
60.0.0.0        0.0.0.4         463         0x80000001 0x00e4f9
60.0.0.0        0.0.0.10        463         0x80000001 0x00c018
70.0.0.0        0.0.0.10        463         0x80000002 0x003c91
18.0.0.0        0.0.0.10        463         0x80000003 0x00eb14
50.0.0.0        0.0.0.3         289         0x8000000a 0x00ddc2
90.0.0.0        0.0.0.3         271         0x8000000c 0x0052e3
19.0.0.0        0.0.0.3         256         0x80000012 0x00ee87

                Summary ASB Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.1         0.0.0.4         444         0x80000002 0x005c7b
0.0.0.1         0.0.0.3         294         0x80000008 0x00567c
0.0.0.1         0.0.0.10        291         0x80000007 0x00ab61
0.0.0.3         0.0.0.3         7           0x8000005a 0x00201e
0.0.0.3         0.0.0.10        7           0x8000002d 0x005014
0.0.0.3         0.0.0.4         2           0x80000035 0x00e1c0
```

```
                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
80.0.0.0        0.0.0.1         475         0x80000001 0x00afbf 0
8.0.0.0         0.0.0.1         475         0x80000001 0x005b5c 0
0.0.0.0         0.0.0.7         297         0x80000001 0x00f2d8 1
```

Figure IV.17 Router 1 Verification of LSDB

IV.7.6 Routing Table Verification

The "**show ip route**" command in OSPF is utilized to exhibit the routing table, encompassing all routes acquired by the router via OSPF, other routing protocols, or manually configured.

The following figure illustrates the routing table for Router1:

```
Router1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    8.0.0.0/8 [90/2172416] via 80.0.0.2, 00:06:15, Serial0/1/1
O IA 9.0.0.0/8 [110/129] via 10.0.0.2, 00:05:53, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/8 is directly connected, Serial0/0/0
L       10.0.0.1/32 is directly connected, Serial0/0/0
     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.0.0.0/8 is directly connected, Serial0/1/0
L       11.0.0.1/32 is directly connected, Serial0/1/0
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.0.0.0/8 is directly connected, Serial0/0/1
L       12.0.0.1/32 is directly connected, Serial0/0/1
O    13.0.0.0/8 [110/128] via 10.0.0.2, 00:05:53, Serial0/0/0
O    14.0.0.0/8 [110/128] via 10.0.0.2, 00:05:53, Serial0/0/0
                [110/128] via 11.0.0.2, 00:05:53, Serial0/1/0
O    15.0.0.0/8 [110/128] via 12.0.0.2, 00:05:53, Serial0/0/1
O    16.0.0.0/8 [110/128] via 11.0.0.2, 00:05:53, Serial0/1/0
                [110/128] via 12.0.0.2, 00:05:53, Serial0/0/1
O    17.0.0.0/8 [110/128] via 11.0.0.2, 00:05:53, Serial0/1/0
O IA 18.0.0.0/8 [110/193] via 12.0.0.2, 00:05:43, Serial0/0/1
O IA 19.0.0.0/8 [110/321] via 10.0.0.2, 00:02:24, Serial0/0/0
                [110/321] via 11.0.0.2, 00:02:24, Serial0/1/0
                [110/321] via 12.0.0.2, 00:02:24, Serial0/0/1
```

```
O IA 20.0.0.0/8 [110/128] via 10.0.0.2, 00:05:53, Serial0/0/0
O IA 40.0.0.0/8 [110/192] via 10.0.0.2, 00:05:53, Serial0/0/0
                [110/192] via 11.0.0.2, 00:05:53, Serial0/1/0
                [110/192] via 12.0.0.2, 00:05:53, Serial0/0/1
O IA 50.0.0.0/8 [110/256] via 10.0.0.2, 00:02:59, Serial0/0/0
                [110/256] via 11.0.0.2, 00:02:59, Serial0/1/0
                [110/256] via 12.0.0.2, 00:02:59, Serial0/0/1
O IA 60.0.0.0/8 [110/128] via 12.0.0.2, 00:05:53, Serial0/0/1
O IA 70.0.0.0/8 [110/192] via 12.0.0.2, 00:05:43, Serial0/0/1
     80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       80.0.0.0/8 is directly connected, Serial0/1/1
L       80.0.0.1/32 is directly connected, Serial0/1/1
O IA 90.0.0.0/8 [110/320] via 10.0.0.2, 00:02:44, Serial0/0/0
                [110/320] via 11.0.0.2, 00:02:44, Serial0/1/0
                [110/320] via 12.0.0.2, 00:02:44, Serial0/0/1
```

Figure IV.18 Routing Table Verification of Router 1

IV.7.7 OSPF Virtual Link Verification

To establish connectivity between Router1 and the backbone area, we had to configure a virtual link between Router 4 and Router 10. After configuring the virtual link, verify the OSPF configuration on both routers using commands like "**show ip ospf virtual-link**" to ensure that the virtual link has been established successfully.

```
Router10#sh ip ospf virtual-link
Virtual Link OSPF_VL0 to router 0.0.0.4 is up
  Run as demand circuit
  Transit area 30, via interface Serial0/0/0, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency State FULL
    Index 1/2, retransmission queue length 0, number of retransmission 0
        First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
        Last retransmission scan length is 0, maximum is 0
        Last retransmission scan time is 0 msec, maximum is 0 msec
```

Figure IV.19 Router 10 OSPF Virtual Link Verification

```
Router#sh ip ospf virtual-link
Virtual Link OSPF_VL0 to router 0.0.0.10 is up
  Run as demand circuit
  Transit area 30, via interface Serial0/1/1, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency State DOWN
    Index 1/2, retransmission queue length 0, number of retransmission 0
        First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
        Last retransmission scan length is 0, maximum is 0
        Last retransmission scan time is 0 msec, maximum is 0 msec
```

Figure IV.20 Router 4 OSPF Virtual Link Verification

IV.7.8 Computers Connectivity Verification

The ping command sends response requests to a destination address using the ICMP protocol. It sends ICMP Echo Request packets, which help determine if the recipient is reachable or not. If the recipient receives the packets, it responds by sending ICMP Echo Reply packets. This test is commonly used to verify connectivity between devices.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC1	PC3	ICMP		0.012	N	1	(edit)	
	Successful	PC1	PC4	ICMP		0.026	N	2	(edit)	
	Successful	PC2	PC3	ICMP		0.042	N	3	(edit)	
	Successful	PC2	PC4	ICMP		0.055	N	4	(edit)	
	Successful	PC3	PC4	ICMP		0.071	N	5	(edit)	

Figure IV.21 Testing Computers Connectivity

The figure above illustrates the proper functioning of the tests between the four computers.

IV.8 Comparative Analysis between the Implementation Designs

The purpose of conducting a comparative analysis of the implementation designs is to evaluate and assess various approaches to network design in relation to latency, cost, and failure. This analysis entails comparing the original design with the recommended design. Through an examination of these crucial factors, valuable insights can be obtained regarding the performance and dependability of each design.

IV.8.1 OSPF Cost

In the implemented solution, the OSPF cost for particular destinations has decreased due to the presence of multiple direct paths leading to those destinations. This allows OSPF to choose the most efficient and cost-effective path, leading to decreased latency and enhanced network performance.

```
Gateway of last resort is not set

D     8.0.0.0/8 [90/2172416] via 80.0.0.2, 00:10:20, Serial0/1/1
O IA  9.0.0.0/8 [110/193] via 11.0.0.2, 00:00:30, Serial0/1/0
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.0.0.0/8 is directly connected, Serial0/1/0
L        11.0.0.1/32 is directly connected, Serial0/1/0
O     12.0.0.0/8 [110/64] via 12.0.0.0, 00:10:20, Serial0/0/1
O     13.0.0.0/8 [110/192] via 11.0.0.2, 00:00:30, Serial0/1/0
O     14.0.0.0/8 [110/128] via 11.0.0.2, 00:00:30, Serial0/1/0
O     15.0.0.0/8 [110/128] via 12.0.0.2, 00:09:36, Serial0/0/1
O     16.0.0.0/8 [110/128] via 11.0.0.2, 00:09:36, Serial0/1/0
O     17.0.0.0/8 [110/128] via 11.0.0.2, 00:09:36, Serial0/1/0
O IA  18.0.0.0/8 [110/193] via 12.0.0.2, 00:09:36, Serial0/0/1
O IA  19.0.0.0/8 [110/321] via 11.0.0.2, 00:00:30, Serial0/1/0
O IA  20.0.0.0/8 [110/192] via 11.0.0.2, 00:00:30, Serial0/1/0
O IA  40.0.0.0/8 [110/192] via 11.0.0.2, 00:00:30, Serial0/1/0
O IA  50.0.0.0/8 [110/256] via 11.0.0.2, 00:00:30, Serial0/1/0
O IA  60.0.0.0/8 [110/128] via 12.0.0.2, 00:09:36, Serial0/0/1
O IA  70.0.0.0/8 [110/192] via 12.0.0.2, 00:09:36, Serial0/0/1
      80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        80.0.0.0/8 is directly connected, Serial0/1/1
L        80.0.0.1/32 is directly connected, Serial0/1/1
O IA  90.0.0.0/8 [110/320] via 11.0.0.2, 00:00:30, Serial0/1/0
```

Figure IV.22 OSPF Cost Results of Original Design

The figure below represents the results of OSPF cost related to the article topology.

```
Gateway of last resort is not set

D    8.0.0.0/8 [90/2172416] via 80.0.0.2, 00:02:37, Serial0/1/1
O IA 9.0.0.0/8 [110/129] via 10.0.0.2, 00:02:10, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/8 is directly connected, Serial0/0/0
L       10.0.0.1/32 is directly connected, Serial0/0/0
     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.0.0.0/8 is directly connected, Serial0/1/0
L       11.0.0.1/32 is directly connected, Serial0/1/0
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.0.0.0/8 is directly connected, Serial0/0/1
L       12.0.0.1/32 is directly connected, Serial0/0/1
O    13.0.0.0/8 [110/128] via 10.0.0.2, 00:02:10, Serial0/0/0
O    14.0.0.0/8 [110/128] via 11.0.0.2, 00:02:10, Serial0/1/0
                [110/128] via 10.0.0.2, 00:02:10, Serial0/0/0
O    15.0.0.0/8 [110/128] via 12.0.0.2, 00:02:20, Serial0/0/1
O    16.0.0.0/8 [110/128] via 11.0.0.2, 00:02:20, Serial0/1/0
                [110/128] via 12.0.0.2, 00:02:20, Serial0/0/1
O    17.0.0.0/8 [110/128] via 11.0.0.2, 00:02:20, Serial0/1/0
O IA 18.0.0.0/8 [110/193] via 12.0.0.2, 00:02:10, Serial0/0/1
```

```
O IA 19.0.0.0/8 [110/321] via 11.0.0.2, 00:02:10, Serial0/1/0
                [110/321] via 12.0.0.2, 00:02:10, Serial0/0/1
                [110/321] via 10.0.0.2, 00:02:10, Serial0/0/0
O IA 20.0.0.0/8 [110/128] via 10.0.0.2, 00:02:10, Serial0/0/0
O IA 40.0.0.0/8 [110/192] via 11.0.0.2, 00:02:10, Serial0/1/0
                [110/192] via 12.0.0.2, 00:02:10, Serial0/0/1
                [110/192] via 10.0.0.2, 00:02:10, Serial0/0/0
O IA 50.0.0.0/8 [110/256] via 11.0.0.2, 00:02:10, Serial0/1/0
                [110/256] via 12.0.0.2, 00:02:10, Serial0/0/1
                [110/256] via 10.0.0.2, 00:02:10, Serial0/0/0
O IA 60.0.0.0/8 [110/128] via 12.0.0.2, 00:02:20, Serial0/0/1
O IA 70.0.0.0/8 [110/192] via 12.0.0.2, 00:02:10, Serial0/0/1
     80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       80.0.0.0/8 is directly connected, Serial0/1/1
L       80.0.0.1/32 is directly connected, Serial0/1/1
O IA 90.0.0.0/8 [110/320] via 11.0.0.2, 00:02:10, Serial0/1/0
                [110/320] via 12.0.0.2, 00:02:10, Serial0/0/1
                [110/320] via 10.0.0.2, 00:02:10, Serial0/0/0
```

Figure IV.23 OSPF Cost Results of Proposed Design

The decrease in OSPF cost signifies that our proposed topology offers improved connectivity and more efficient routing options. It allows for better load distribution across the network and minimizes the dependency on a central router. These benefits contribute to enhanced network performance and lower latency for the affected destinations.

IV.8.2 Latency

Network latency, which refers to the delay experienced during data transmission across a network, is a crucial factor in network planning. Lower latency is preferred as it ensures swifter communication and responsiveness.

To test the connectivity and compare the latency of the designs, we will use the **ping** command from PC1 to PC4. This command allows us to check the reachability of the destination host (PC4) from the source (PC1), measure the round-trip time for packets sent, and identify any packet loss along the way.

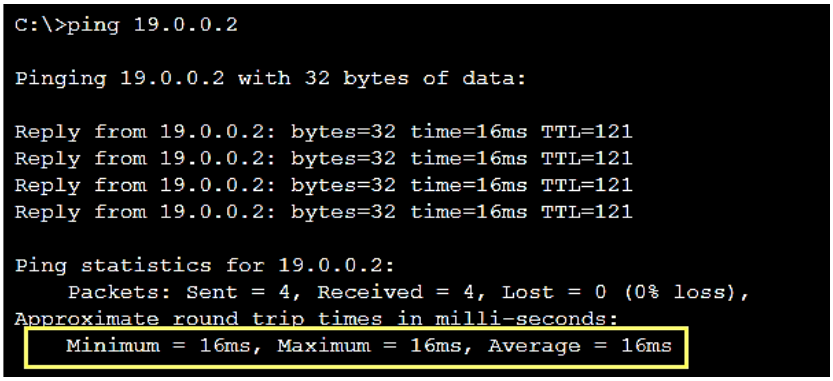

Figure IV.24 Latency Results of Original Design

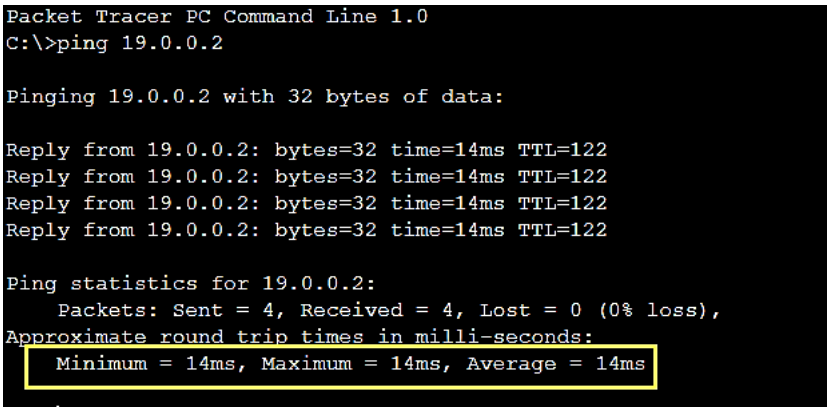

Figure IV.25 Latency Results of Proposed Design

The **ping** results reveal that our design exhibits lower latency values compared to the network setup described in the article. Specifically, our proposed design showcases latencies of 14ms, 14ms, and 14ms, while the article's configuration demonstrates latencies of 16ms, 16ms, and 16ms. These results confirm that the changes made in the redesign have effectively enhanced the overall network performance and responsiveness by reducing the number of hops and optimizing the routing path.

The Time-To-Live (TTL) value in the **ping** command indicates the maximum number of routers that a packet can traverse before being discarded. When comparing the TTL values between the proposed design (TTL=122) and the original design (TTL=121)

We can say that the higher TTL value observed in the proposed design strongly suggests a more direct and optimized routing path.

IV.8.3 In Case of Failure

There are several reasons for network disruptions, which can range from hardware problems to configuration errors. One frequent cause of network breakdowns is link failure. This can be caused by factors such as cable deterioration, connector malfunctions, interface breakdowns, or equipment failures.

As part of the testing process, we will simulate network changes in both the original and proposed designs by removing specific links. For the original design, we will remove the link between Router2 and Router5, while for the proposed design, we will remove the link between Router2 and Router1. Following these modifications, we will utilize the **traceroute** command from PC1 to PC2 to trace the path taken by packets within each network configuration. This will allow us to compare the routing behavior of the two implementations.

```
C:\>tracert 8.0.0.1

Tracing route to 8.0.0.1 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       9.0.0.1
  2    1 ms       1 ms       0 ms       20.0.0.2
  3    1 ms       *          1 ms       20.0.0.2
  4    *          4 ms       *          Request timed out.
  5    1 ms       *          1 ms       20.0.0.2
  6    *          1 ms       *          Request timed out.
  7    1 ms       *          1 ms       20.0.0.2
  8    *          1 ms       *          Request timed out.
  9    1 ms       *          0 ms       20.0.0.2
  10    *          4 ms       *          Request timed out.
  11    0 ms       *          1 ms       20.0.0.2
  12    *          2 ms       *          Request timed out.
  13    0 ms       *          0 ms       20.0.0.2
  14    *          0 ms       *          Request timed out.
  15    3 ms       *          0 ms       20.0.0.2
  16    *          0 ms       *          Request timed out.
  17    0 ms       *          2 ms       20.0.0.2
  18    *          1 ms       *          Request timed out.
  19    4 ms       *          1 ms       20.0.0.2
  20    *          1 ms       *          Request timed out.
  21    0 ms       *          0 ms       20.0.0.2
  22    *          4 ms       *          Request timed out.
  23    0 ms       *          1 ms       20.0.0.2
  24    *          1 ms       *          Request timed out.
  25    1 ms       *          1 ms       20.0.0.2
  26    *          1 ms       *          Request timed out.
  27    3 ms       *          1 ms       20.0.0.2
  28    *          3 ms       *          Request timed out.
  29    0 ms       *          1 ms       20.0.0.2
  30    *          0 ms       *          Request timed out.

Trace complete.
```

Figure IV.26 Original Design Result in Case of Failure

```
C:\>tracert 8.0.0.1

Tracing route to 8.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      9.0.0.1
  2    0 ms      1 ms      0 ms      20.0.0.2
  3    1 ms      5 ms      2 ms      14.0.0.1
  4    11 ms     10 ms     4 ms      11.0.0.1
  5    11 ms     2 ms      11 ms     80.0.0.2
  6    11 ms     15 ms     12 ms     8.0.0.1

Trace complete.
```

Figure IV.27 Proposed Design Result in Case of Failure

Based on the results of deleting one link and observing the packet forwarding behavior in our design and the article's design, we can make the following observations:

Our proposed design demonstrates superior redundancy and path diversity compared to the design presented in the article. In the event that one link is removed, our network can identify an alternate route for packet forwarding. This emphasizes the existence of multiple paths connecting the source and destination, thereby increasing fault tolerance and resilience in scenarios involving link failures.

On the other hand, the original design appears to have a single point of failure. When the link is removed, it could disrupt connectivity or prevent the packet from finding an alternative route. This is because the network traffic depends heavily on the central hub router, and removing the link connecting the hub to another router could leave no other pathway available.

IV.8.4 Summary of Improvements

The updated design showcases significant improvements in routing efficiency, network performance, and redundancy. With lower OSPF costs and multiple available paths to various destinations, it demonstrates a highly resilient and optimized network configuration. Notably, the reduced round trip time emphasizes a tangible improvement in the network's operational efficiency and speed.

Additionally, the implementation of OSPF authentication using MD5 provides robust security measures by ensuring the integrity and authenticity of OSPF routing updates. This added layer of security safeguards against unauthorized access and data manipulation.

IV.9 Performance Enhancement Experiment

In the final phase of our OSPF implementation, we are proposing a crucial upgrade to enhance network performance by replacing current serial connections with high-capacity Ethernet cables. This change is expected to significantly improve network efficiency by supporting higher data throughput without significant delays, thereby streamlining load distribution and potentially decreasing the OSPF cost. Ethernet cables are particularly well suited for this upgrade due to their common usage and short distance connections for data centers, which matches with the standard needs of Internet Exchange Points (IXPs), where devices are usually collocated in the same facility or building.

The next section will compare the performance of the two designs, emphasizing the benefits of integrating Ethernet as the primary technology for OSPF.

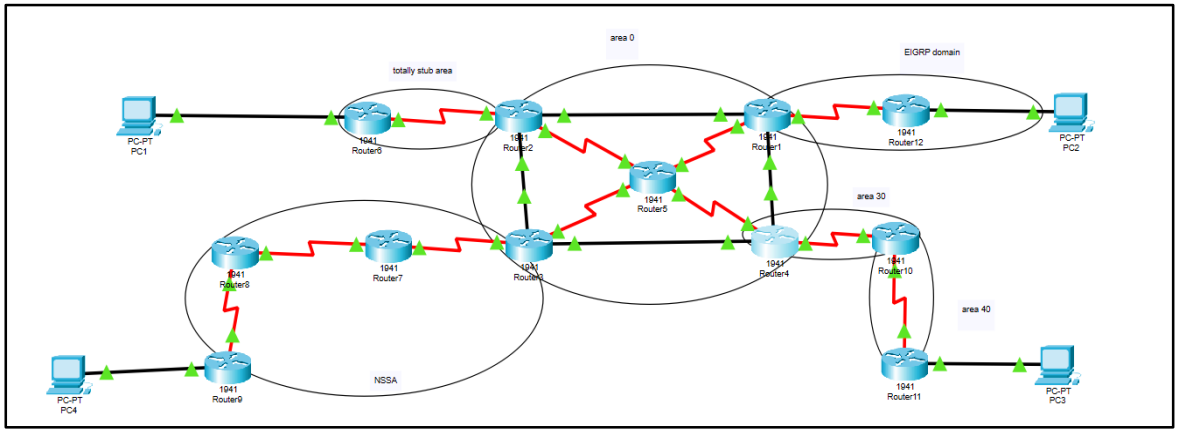

Figure IV.28 Proposed Design with Ethernet Connectivity

IV.10 Comparing OSPF Implementations: Serial Links VS Ethernet Cables

In this comparative analysis, we will analyze the effects of cable selection on network performance. Specifically, we will focus on the utilization of serial and Ethernet cables within the OSPF framework. Our assessment will include critical performance metrics such as bandwidth, latency, and OSPF cost. The goal of this study is to highlight the nuanced differences between these two cable types and their impact on network optimization.

IV.10.1 Bandwidth

The bandwidth of the Ethernet connection (1000 mbps) shown in Figure IV.29 is considerably greater when compared to that of the serial cable (1,544 mbps) represented in Figure IV.30. More precisely, the Ethernet connection boasts a bandwidth that is approximately 647 times larger than that of the serial cable.

```
Router#sh interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0001.42e2.2d01 (bia 0001.42e2.2d01)
  Internet address is 10.0.0.1/8
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
```

Figure IV.29 Bandwidth Result with Ethernet Connectivity

```
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.0.0.1/8
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
```

Figure IV.30 Bandwidth Result of Serial Links

With the higher bandwidth offered by Ethernet cables, the network can accommodate larger volumes of data traffic without experiencing congestion or slowdowns. This results in smoother and more efficient data transmission.

IV.10.2 OSPF Cost

When we replace the serial links with Ethernet cables, the OSPF cost will typically decrease due to the higher bandwidth provided by the Ethernet cable, for example:

- **9.0.0.0/8** has a cost of 66 over Ethernet compared to 129 over serial.
- **13.0.0.0/8** has a cost of 2 over Ethernet compared to 128 over serial.
- **40.0.0.0/8** has a cost of 66 over Ethernet compared to 192 over serial.
- **90.0.0.0/8** has a cost of 194 over Ethernet compared to 320 over serial.

As a result, routers within the network will be more likely to choose the Ethernet links as the optimal routes due to their lower OSPF cost, which can lead to improved network performance.

```
Router1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    8.0.0.0/8 [90/2172416] via 80.0.0.2, 00:08:54, Serial0/0/1
O IA 9.0.0.0/8 [110/66] via 10.0.0.2, 00:09:12, GigabitEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/8 is directly connected, GigabitEthernet0/0
L       10.0.0.1/32 is directly connected, GigabitEthernet0/0
     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.0.0.0/8 is directly connected, Serial0/0/0
L       11.0.0.1/32 is directly connected, Serial0/0/0
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.0.0.0/8 is directly connected, GigabitEthernet0/1
L       12.0.0.1/32 is directly connected, GigabitEthernet0/1
O    13.0.0.0/8 [110/2] via 10.0.0.2, 00:11:03, GigabitEthernet0/0
O    14.0.0.0/8 [110/65] via 10.0.0.2, 00:10:27, GigabitEthernet0/0
O    15.0.0.0/8 [110/2] via 12.0.0.2, 00:11:03, GigabitEthernet0/1
O    16.0.0.0/8 [110/65] via 12.0.0.2, 00:09:34, GigabitEthernet0/1
O    17.0.0.0/8 [110/66] via 10.0.0.2, 00:10:17, GigabitEthernet0/0
                [110/66] via 12.0.0.2, 00:10:17, GigabitEthernet0/1
O IA 18.0.0.0/8 [110/130] via 12.0.0.2, 00:08:23, GigabitEthernet0/1
O IA 19.0.0.0/8 [110/195] via 10.0.0.2, 00:01:00, GigabitEthernet0/0
                [110/195] via 12.0.0.2, 00:01:00, GigabitEthernet0/1
O IA 20.0.0.0/8 [110/65] via 10.0.0.2, 00:09:12, GigabitEthernet0/0
O IA 40.0.0.0/8 [110/66] via 10.0.0.2, 00:09:12, GigabitEthernet0/0
                [110/66] via 12.0.0.2, 00:09:12, GigabitEthernet0/1
```

```
O IA 20.0.0.0/8 [110/65] via 10.0.0.2, 00:09:12, GigabitEthernet0/0
O IA 40.0.0.0/8 [110/66] via 10.0.0.2, 00:09:12, GigabitEthernet0/0
                [110/66] via 12.0.0.2, 00:09:12, GigabitEthernet0/1
O IA 50.0.0.0/8 [110/130] via 10.0.0.2, 00:01:00, GigabitEthernet0/0
                [110/130] via 12.0.0.2, 00:01:00, GigabitEthernet0/1
O IA 60.0.0.0/8 [110/65] via 12.0.0.2, 00:08:46, GigabitEthernet0/1
O IA 70.0.0.0/8 [110/129] via 12.0.0.2, 00:08:23, GigabitEthernet0/1
     80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       80.0.0.0/8 is directly connected, Serial0/0/1
L       80.0.0.1/32 is directly connected, Serial0/0/1
O IA 90.0.0.0/8 [110/194] via 10.0.0.2, 00:01:00, GigabitEthernet0/0
                [110/194] via 12.0.0.2, 00:01:00, GigabitEthernet0/1
```

Figure IV.31 OSPF Cost Results with Ethernet Connectivity

IV.10.3 Latency

Transitioning the backbone area links from serial to Ethernet stabilized the latency at 14ms. This stability in latency reflects consistent performance in data transmission times across the network. The maintenance of latency at 14ms shows that the network is operating reliably and consistently, ensuring predictable application performance. Overall, this latency stability demonstrates the effectiveness of the backbone link transition from serial to Ethernet maintaining the network's performance standards.

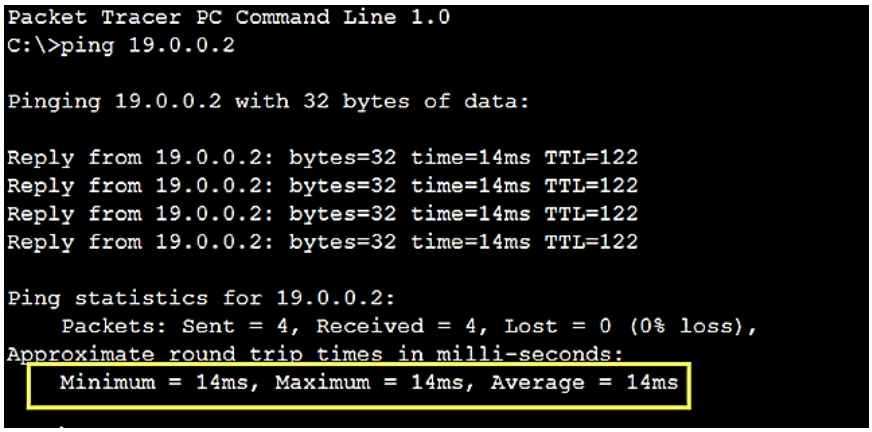

Figure IV.32 Latency Results with Ethernet Connectivity

IV.10.4 Summary of Improvements

Transitioning from serial cables to Ethernet cables led to a 647-fold increase in bandwidth, significantly enhancing data transfer rates. OSPF costs were reduced, optimizing routing paths and improving network efficiency. Additionally, latency stabilized at 14ms, ensuring consistent and reliable performance. Overall, these changes resulted in a more efficient, reliable, and high-performing network.

IV.11 Overall Network Performance Improvements

The enhanced network design demonstrates significant improvements in various areas, such as routing efficiency, network performance, and redundancy. By reducing OSPF costs and offering multiple available paths, the routing process is optimized, ensuring efficient transmission of data across the network. Furthermore, the utilization of Ethernet cables at the Internet Exchange Point (IXP) provides additional benefits. These cables have higher bandwidth capabilities, allowing the network to handle larger volumes of traffic effortlessly. Consequently, congestion is minimized, resulting in smoother data flow and enhanced overall network performance.

Additionally, the stable latency achieved through Ethernet connections guarantees consistent and predictable transfer times for data, thereby enhancing user experience and application performance. Moreover, the integration of OSPF authentication with MD5 encryption adds an extra layer of security to the network. This security measure protects against unauthorized access and data manipulation by ensuring the integrity and authenticity of routing

updates. In combination, these improvements result in a highly resilient, optimized, and secure network configuration that can effectively address the challenges of modern networking requirements.

IV.12 Conclusion

In this chapter, we have detailed our objectives and the successful execution of an updated network structure aimed at improving the OSPF protocol's performance. Our main goals included reducing latency, simplifying routing, minimizing OSPF costs, and ensuring network security. By carefully assessing the network's needs, we have met these objectives by introducing a new design that enhances OSPF efficiency and follows industry standards. Moreover, we have integrated OSPF authentication to enhance network security.

The result is a highly efficient and secure network system that fulfills our goals, offering better latency, improved routing, cost-effectiveness, and increased security measures.

This comprehensive thesis has provided a thorough understanding of network fundamentals, routing mechanisms, and the intricacies of the OSPF protocol, highlighting their critical roles in efficient data communication. By examining various network topologies, devices, and layered architectures, we have established a solid foundation for appreciating how networks operate. A detailed exploration of routing, including the importance of routing protocols and the functions of routing tables, has shed light on the processes that ensure data reaches its intended destination efficiently.

A deep dive into OSPF has revealed its scalability, reliability, and security features, which are essential for modern network infrastructures.

Finally, the practical application of revamping a network structure to enhance OSPF performance underscores the importance of continuous network optimization.

Configuration

"enable ": Allows access to privileged execution mode
"configure terminal "Allows switching to global configuration mode
"hostname": Allows to specify a router name
"ip address subnet mask": Allows specifying the IP address of the interface in interface configuration mode with a 32-bit mask to match the entire interface address
"network address wildcard mask area-id": Allows announcing IP networks
"interface [interface-name]": Command used to access and configure settings for a specific interface on a networking device
"no shutdown": To activate the interfaces
"do wr ": It's used to save the running configuration of a device to its startup configuration، effectively saving any changes made during the current session
"router ospf process-id": Enables OSPF routing with the specified process number
"router-id": it used to manually set the unique identifier for an OSPF router
"area-id stub no-summary": it used in OSPF to configure an area as a stub area and prevent it from receiving summary LSAs from other areas
"area-id nssa": is a command used in OSPF to configure an area as a Not-So-Stubby Area (NSSA)، allowing limited external route advertisements
"default information originate": Ensures that all routers in the OSPF area have a default route to reach destinations outside the OSPF autonomous system, typically for internet access or other external networks.
"ip ospf message-digest-key [key ID] md5 [password]": it is used to configure MD5 authentication for OSPF on an interface، specifying a key ID and password for the authentication
"ip ospf authentication message-digest": is a command used to enable MD5 authentication for OSPF on an interface
"area ID authentication message-digest": to enable MD5 authentication for all OSPF interfaces within a specified area
"router eigrp <eigrp process-id>": to enter the EIGRP routing protocol configuration mode for a specified process ID
"redistribute ospf <ospf process-id> metric <metric-values>": redistribute OSPF routes into another routing protocol , setting the specified metric values for the redistributed routes
"router ospf <ospf process-id> ": enter OSPF router configuration mode for a specified OSPF process ID
"redistribute eigrp <eigrp process-id> subnets": it is used to redistribute EIGRP routes into OSPF within OSPF router configuration mode, and it includes the subnets of the EIGRP routes.
"ping": to test connectivity between devices by sending ICMP echo request packets and measuring the response time
"bandwidth value": The Cisco IOS automatically determines a cost based on the interface bandwidth. For OSPF to function properly, it is essential to set the correct interface bandwidth.
" ip ospf cost [1-65535]": Allows explicitly defining the cost of the link

Verification

"show ip interface brief": Checks the configured IP addresses and the status of each interface

"show interfaces": Displays information related to all the interfaces on the router

"show ip protocol": Displays OSPF configuration information

"show ip ospf interface": Displays detailed information about OSPF interfaces

"show ip ospf interface type number": Displays timer intervals and adjacencies; determines if OSPF is enabled on the interface , checks if interfaces between routers are in the same OSPF area. Displays the interface priority value and other information such as network type, RID, and cost

"show ip ospf neighbor detail": Verifies that OSPF routing has formed adjacencies in detail. Observes the OSPF neighbor tables. Displays OSPF neighbor information for each interface

"show ip ospf": Indicates the number of times the Shortest Path First (SPF) algorithm has been executed. Also indicates the link-state update intervals

"show ip ospf database": Displays the contents of the topological database. This command also indicates the router ID, OSPF process ID, and several types of database entries (LSAs)

"show ip route": Displays the routing table

"show ip ospf virtual-link": OSPF virtual links are used to connect OSPF areas that are not physically contiguous to Area 0 , also known as the backbone area. This command is useful for verifying the status and configuration of this virtual link.

A. BILBIOGRQPHI

[1]. **Forouzan, Behrouz A.** "Data Communication and Networking. Data Communication and Networking fourth edition". New York: McGraw-Hill, 2007.

ISBN 978-0-07-296775-3 - ISBN 0-07-296775-7

[2]. Andrew S. Tanenbaum, David J. Wetherill. "Computer Networks". Computer Networks Fifth Edition". United States of America: Pearson Education, 2011.

ISBN-13: 978-0-13-212695-3 / ISBN- 10: 0-13-212695-8 (alk. paper).

[4]. Held, Gilbert. "Data Communications Networking Devices: Operation, Utilization and Lan and Wan Internetworking, 4th Edition ". s.l.: Wiley, 2001.

ISBN: 978-0-470-84182-2

[5]. Titz, Edward. "Cisco Networking All-in-One for Dummies 1st Edition". September 20, 2011. ISBN-10: 9780470945582 / ISBN-13: 978-0470945582

[6]. Donahue, Gary. "Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam 2nd Edition" . United States: O'Reilly Media, 2011.

ISBN-10 : 1449387861 / ISBN-13 : 978-1449387860.

[7]. Davies, Gordon. "Networking Fundamentals ". UK: Packt, 2019.

ISBN: 9781838643508.

[15]. Academy, Cisco Networking. "Routing Protocols Companion Guide ". United States of America: Cisco Systems, 2014.

ISBN-10: 1-58713-323-7 ISBN-13: 978-1-58713-323-7.

[16]. Malbotra, Ravi. "IP Routing ". s.l.: O'Reilly Media, Inc, 2002. ISBN: 9780596002756.

[17]. Chwan-Hwa (John) Wu, J. David Irwin "Introduction to Computer Networks and Cybersecurity". Boca Raton, Florida: CRC Press, 2013.

ISBN: 9780429101311.

[19]. **Stevens, W. Richard.**" Tcp/ip illustrated volume 1 ". United States of America : Corporate, 2011. ISBN-13: 978-0-321-33631-6.

[20]. **Zaheer Aziz, Johnson Liu, Abe Martey , Faraz Shamim.** "Troubleshooting IP Routing Protocols". États-Unis Cisco Press, 2002.

ISBN-13: 978-1587143724.

[21]. **McQuerry, Steve.** "Interconnecting Cisco Network Devices ", Part 2 (ICND2). s.l. : Cisco Press, 2008. ISBN: 9781587055676.

[22]. **Sam Halabi, Danny McPherson.**" Internet Routing Architectures, Second Edition". s.l. : Cisco Press, 2000.

ISBN: 157870233X.

[23]. **Mir, Nader F.** "Computer and Communication Networks" . s.l. : Pearson, 2006

ISBN : 0131747991.

[24]. **Hartpence, Bruce.**" Packet Guide to Routing and Switching". s.l. : O'Reilly Media, Inc, 2011.

ISBN: 9781449306557.

[25]. **Lammle, Todd.**"CCNA Routing and Switching Complete Study Guide, 2nd Edition ". s.l. : Sybex, 2016.

ISBN: 9781119288282.

[26]. **Kenyon, Tony.**" Data Networks: Routing, Security, and Performance Optimization ". s.l. : Elsevie, 2002.

ISBN: 0080503667, 9780080503660.

[27]. **Thomas M. Thomas, Atif Kahn.** "Network Design and Case Studies (CCIE Fundamentals), 2nd Edition". s.l. : Cisco Systems, Inc, 1999.

ISBN-10: 1-57870-167-8 / ISBN-13: 978-1-57870-167-4.

[30]. **Jeffrey S. Beasley, Piyasat Nilkaew.** 'Networking Essentials, 6th edition " . s.l. : Pearson IT Certification, 2021.

ISBN-13: 9780137455799.

[31]. Glen E. Clarke, Richard Deal. "CCT/CCNA Routing and Switching All-in-One Exam Guide"

s.l. : McGraw Hill, 2021.

ISBN :1260469786, 9781260469783.

[32]. Tanenbaum, Andrew S. "Computer Networks, Fourth Edition". s.l. : Pearson, 2002.

ISBN: 9780130661029.

[34]. Chris Carthern, William Wilson, Noel Rivera. "Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA 2nd Edition " . s.l. : Kindle Edition Apress, 2021

ISBN-13 : 978-1484266717.

[35]. Doug Marschke, Harry Reynolds. " Junos enterprise routing " . s.l. : O' Reilly, 2008.

ISBN: 978-0-596-51442-6.

[36]. Tadimety, Phani Raj." OSPF: A Network Routing Protocol" . s.l. : Apress Berkeley, CA, 2015. p. 144.

ISBN: 978-1-4842-1411-4.

[37]. Moy, John T. " OSPF: anatomy of an Internet routing protocol ". s.l. : Reading, Mass.: Addison-Wesley , 1998.

ISBN: 0201634724.

[38]. Brad Edgeworth, Aaron Foss, Ramiro Garza Rios. " IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols ". s.l. : Cisco Press, 2014.

ISBN : 0133846768 , 9780133846768.

[44]. Doyle, Jeff. "OSPF and IS-IS: Choosing an IGP for Large-Scale Networks ". s.l. : Addison-Wesley Professional, 2005.

ISBN: 0321168798.

B. WEBIOGRQPHI

[3]. **Bus Topology .** Computer Hope. [En ligne] 12 october 2023. [Citation : 6 February 2024.] https://www.computerhope.com/jargon/b/bustopol.htm

[9]. **geeksforgeeks.** [En ligne] [Citation : 08 02 2024.] https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/.

[14]. **What is Routing.** amazon . [En ligne] [Citation : 18 02 2024.]

https://aws.amazon.com/what-is/routing/.

[18]. **Interior Gateway Protocol.** "sciencedirect". [Enligne] [Citation: 18/02/2024] https://www.sciencedirect.com/topics/computer-science/interior-gateway-protocol.

C. JOURNAL ARTICLE

[8]. **Fraihat, Ahmad.** "Computer Networking Layers Based on the OSI Model ". Test Engineering and Management. July - August 2020, Vol. 83.

[10]. **TCP/IP PROTOCOL LAYERING.** "International Journal of Computer Science and Information Technology Research ", January - March 2015, Vol. 3, pp. (415-417).

[11]. **Uddin2, Pranab Bandhu Nath1 Mofiz.** "TCP-IP Model in Data Communication and Networking " American Journal of Engineering Research (AJER) . 18 novemeber 2015, Vol.

[13]. **Nnamani, Kelvin .Ndubuisi.**" Comparative Analysis of OSI and TCP/IP Models in Network Communication ". Quest Journals, 2021, Journal of Software Engineering and Simulation

[33]. **A Comparative Analysis of OSPF and EIGRP Routing.** 2, s.l.: Journal of Transactions in Systems Engineering, 2023, Vol. I.

ISSN: 2806-2973.

[41]. **Link Recovery Comparison between OSPF & EIGRP.** [En ligne] IACSIT Press, 2012. [Citation : 29 03 2024.]

https://studylib.net/doc/8273142/link-recovery-comparison-between-ospf-and-eigrp.

[42]. **Tomas Macha, Radko Krkos , Vit Novotny.** "PROPOSAL OF LOAD AWARE ROUTING FOR OSPF ROUTING ". 2013, Vol. 20, 3.

[45]. **A Case Study of OSPF Behavior in a Large Enterprise Network. "**Amen Sheikh,

DOI: 10.1145/637201.637236

[46]. **G. TSOCHEV, K. POPOVA, I. STANKOV.** "DIGITAL INFORMATION TELECOMMUNICATION TECHNOLOGIES ". A Comparative Study by Simulation of OSPF and EIGRP Routing Protocols. Informatics and Automation, 2022, Vol. 21

[47]. **Dancing with Multiple Stub, Discontinuous Areas, and routing protocols of OSPF in IXP.** s.l.: Journal of Physics: Conference Series, 2021.

D. REPORT

[12]. **Fielding, R.; Nottingham, M.; Reschke, J**. (June 2022). HTTP Semantics. IETF. Doi: 10.17487/RFC9110. RFC 9110

Vol. 7. I ISSN: (Online):2321-3795 / ISSN: (Print):2321-3809

[29]. **Moy, John.** "OSPF protocol analysis ". Westborough, United States: s.n., 1991.