# INDEX

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Contents** | **Page Number** | **Remark** |
| 1. | Company Certificate of Internship | 3 |  |
| 2. | Overview of the organization | 5 |  |
| 2. | Chapter-1 Introduction To The Project | 6-9 |  |
| 3. | Chapter-2 System Requirement | 10-13 |  |
| 4. | Chapter-3 Understanding CPT and its working | 14-18 |  |
| 5. | Chapter-4 Understanding the Software & Technologies used | 19-33 |  |
| 6. | Chapter-5 Understanding the Various networking Concepts | 34-46 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 7. | Chapter-6 Networking commands | 47-72 |  |
| 8. | Chapter 7: Security Analysis | 73-75 |  |
| 9. | Chapter-8 Security Analysis | 76-77 |  |
| 10. | Chapter-9 Conclusion | 78-79 |  |
| 11. | Chapter-10 Bibliography | 80 |  |

**1. Overview of the organization**

**Tynor orthotics pvt. Ltd** firmly stand on the pillars of innovation and insights that enable us to deliver optimal care to individuals of all ages. As times have evolved, so have consumers' priorities regarding well-being. Gone are the days when people waited for injuries to happen before seeking a cure. Today, prevention takes center stage.

### About Tynor Orthotics pvt. Ltd.

Tynor Orthotics was founded in 1993, a time when orthopedic appliances were not only expensive but also challenging to obtain. Tynor was founded on the belief that healthcare should be proactive, not just curative. We began as a company focused on providing orthopedic solutions for various healthcare needs. We have now evolved as the leader in the Orthopedic industry, offering a wide range of comprehensive healthcare solutions.

Tynor has established itself as the premier manufacturer and exporter of best-in-class orthotic solutions at the forefront of this transformation.

# Chapter-1 Introduction To The Project

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | | Company Network | |
| **Release Date** | | AXXXX 0,2XXX | |
| **Software** | | Cisco Packet Tracer | |
| **Rated Difficulty** | | Rated difficulty for Chemistry  Moderate | |

|  |  |
| --- | --- |
| **Creator** | Mr. X |

This project involves the design and implementation of a secure, resilient network infrastructure for a newly expanded facility housing multiple departments, including Sales, Marketing, HR, IT, and more. The network is designed with a strong emphasis on performance, scalability, redundancy, and availability. Key components include the allocation of specific IP address ranges for management, WLAN, LAN, VoIP, and DMZ, as well as the integration of advanced technologies such as VLAN segmentation, EtherChannel, and OSPF routing.

To ensure seamless communication and robust security, the project implements a hierarchical network model with redundancy, spanning tree protocol enhancements, and wireless access points managed centrally through a Wireless LAN Controller (WLC). Additionally, the deployment of IP phones supports Voice over IP (VoIP) communication across departments. A Cisco ASA firewall secures the network with defined security zones, while Access Control Lists (ACLs) protect remote administrative access.

The network’s backbone is supported by high-availability protocols such as HSRP, enabling load balancing and failover capabilities. Static and dynamic IP addressing are used appropriately for different devices, while a centralized DHCP server dynamically assigns IPs across the network. The entire system is tested thoroughly to ensure reliable communication, secure data flow, and smooth operations within the infrastructure.

## What is the project about?

In today's interconnected world, a **secure and well-structured network** is crucial for multinational IT companies to ensure **efficient communication, data integrity, and protection against cyber threats**. This document outlines the **design and implementation** of a **robust, scalable, and secure network** tailored for a multinational IT enterprise.

## Goal of the Project

As businesses expand globally, **seamless connectivity and security** become essential for operational efficiency. The purpose of this network system is to:

* Provide **secure and reliable** communication across multiple international offices.
* Ensure **data confidentiality, integrity, and availability**.
* Implement **efficient access controls and network segmentation**.
* Support **scalability** to accommodate future growth and technological advancements.

## Target outcome

Ultimately, this Cisco Packet Tracer project aims to deliver a tangible and demonstrable model of a secure and scalable network solution that directly addresses the critical connectivity and security requirements of a multinational IT enterprise, providing a valuable learning experience in network design and implementation.

## Tools Used

Throughout the challenge, a variety of offensive security tools and utilities are used, including:

 Cisco Packet Tracer

 Cisco Routers (Simulated)

 Cisco Switches (Simulated)

 PCs (Simulated)

 Servers (Simulated)

 Firewalls (Simulated)

 VPN Concentrators/Endpoints (Simulated)

 RADIUS/TACACS+ Servers (Simulated - potentially)

 Network Monitoring Tools (within Packet Tracer)

 Cabling (Simulated)

 IP Addressing Schemes

 Subnetting Plans

 Network Protocols (TCP/IP, DNS, DHCP, HTTP/HTTPS)

 Security Protocols (IPsec, SSL/TLS)

## Difficulty Level

This CPT project is rated as intermediate, suitable for administrators who have a decent hands on practice on the packet tracer also on real components like switch, routers and firewalls.

## 1.6 Testes that needs to be done

Participants will develop and apply the following skills:

* Connectivity Verification (Ping tests)
* Access Control Testing (ACL validation)
* VLAN Functionality Testing (Traffic isolation)
* VPN Connection Testing (Secure tunnel establishment)
* DHCP Functionality Verification (IP address assignment)
* DNS Resolution Testing (Name to IP resolution)
* Basic Security Checks (Unauthorized access attempts - if applicable)
* Scalability Considerations (Conceptual validation)

# Chapter-2 System Requirements

This section outlines the hardware and software requirements needed to set up and run the CPT environment effectively. This ensures a smooth and reproducible experience for creator when they create design and while run it on simulation.

## Software requirements

Here are some likely system requirements for running a Cisco Packet Tracer project for a secure multinational IT network design:

* **Operating System:**
  + Windows 10 or 11 (64-bit recommended)
  + MacOS (latest supported versions)
  + Linux (various distributions supported, e.g., Ubuntu, Fedora)
* **Processor:**
  + Intel Pentium 4, Celeron (or equivalent AMD processor) or better
  + Multi-core processor recommended for larger simulations
* **RAM:**
  + 2 GB minimum
  + 4 GB or more recommended for larger and more complex network simulations
* **Hard Disk Space:**
  + 500 MB of free disk space for installation
  + Additional space required for saved project files
* **Display:**
  + Minimum resolution of 1024 x 768
  + Higher resolution recommended for better visualization
* **Graphics Card:**
  + No specific high-end graphics card required, but a basic card with sufficient memory is recommended for smooth operation.
* **Software:**
  + Cisco Packet Tracer (latest version recommended)
* **Internet Connection:**
  + Required for downloading the software and potentially for accessing online resources or tutorials.

**2.2 Network Requirements**

The company places a strong emphasis on achieving top tier performance, redundancy, scalability and availability within its network infrastructure. As such your task involves creating a comprehensive network design and executing implementation. To facilitate this endeavor, the Company has designed specific IP addresses ranges:

* **Management Network**: For the management, the IP address range of 192.168.10.24/24 has been allocated.
* **WLAN:** The WLAN network will operate within the IP address range of 10.20.0.0/16.
* **LAN:** For the local area network (LAN), the IP address ranges of 172.16.0.0/16.
* **VoIP:** For the local area network (LAN), the IP address ranges of 172.16.0.0/16.
* **DMZ:** The Demilitarized zone (DMZ) will be assigned IP address from the range 10.11.11.0/27, 197.200.100.0/30.
* **Public Address:** Public IP addresses from the range 105.100.50.0/30 from SEACOM and 197.200.100.0/30 from Safaricom.

**2.3 Technical requirements**

1. **Design Tool:** Utilize Cisco Packet Tracer for designing and implementing the network solution.
2. **Hierarchical Design:** Implement a hierarchical model that incorporates redundancy for enhanced network resilience.
3. **ISPs:** Establish connectivity to two ISPs within the network infrastructure.
4. **WLC:** Ensure that each department is equipped with a Wireless Access Point (WAP) to provide Wi-Fi access to employees, corporate users, external auditors, and guests, all centrally managed by the Wireless LAN Controllers (WLC).
5. **VLAN:** Maintain VLANs with the following IDs:

10 for Management, 20 for LAN, 50 for WLAN, 70 for VoIP, 190 for Black hole VLAN (to which all unused ports are assigned).

1. **Ether Channel:** Implement the Link Aggregation Control Protocol (LACP) for Ether Channel configuration, enhancing link aggregation efficiency.
2. **Telephony Service:** Configure VoIP on the voice gateway router and allocate dial numbers in a specific format (4..).
3. **STP Port Fast and BPDU Guard:** Configure Spanning Tree Protocol (STP) Port Fast and BPDU Guard to expedite port transitions from blocking to forwarding states.
4. **Subnetting:** Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group.
5. **Basic Settings:** Configure fundamental device settings, including, Hostnames, Console passwords, Enable passwords, Banner messages, Password encryption, Disabling IP domain lookup.
6. **Inter-VLAN Routing:** Enable devices in all departments to communicate by configuring the respective multilayer switch for inter-VLAN routing.
7. **Core Switch:** Assign IP addresses to the multilayer switch to enable routing and switching functionalities.
8. **DHCP Server:** Ensure that all devices in the network obtain IP addresses dynamically from the DHCP servers assigned to their respective VLANs.
9. **HSRP:** Implement Hot Standby Router Protocol (HSRP) to achieve redundancy, load balancing, and failover capabilities.
10. **Static Addressing:** Allocate static IP addresses to critical servers.
11. **Routing Protocol:** Utilize Open Shortest Path First (OSPF) routing protocol to advertise routes on the firewall, routers, and switches.
12. **Standard ACL for SSH:** Establish Access Control Lists (ACL) on the VTY line and configure Secure Shell (SSH) access for remote management using a Network Security Engineer PC.
13. **CISCO ASA firewall:** Configure default static routes, basic setting, security levels, zones and policies on the cisco ASA firewall to define access control and resource utilization within the network.

**2.4 Hardware requirements:**

* Hardware: Routers, switches, servers, end-user devices.
* Software: Network configuration tools, security firewalls, monitoring software.
* Protocols: TCP/IP, HTTP/HTTPS, DNS, DHCP, VPN for secure remote access.
* Human Resources: Network engineers, security experts, IT support staff.

## 

## Chapter-3 Understanding CPT & It’s Working

Cisco Packet Tracer provides a graphical user interface (GUI) where you can drag and drop virtual network devices like routers, switches, firewalls, PCs, and servers onto a canvas. These devices are not physical hardware but software emulations that mimic the behavior of real Cisco equipment. You can then connect these devices using virtual cables, choosing from various connection types like Ethernet, serial, and fiber.

The core functionality of CPT lies in its ability to simulate network protocols and operations. You can configure the virtual devices using command-line interfaces (CLIs) that are very similar to the IOS (Internetwork Operating System) found on real Cisco devices. This allows you to practice and learn networking concepts and commands without needing physical hardware. You can configure routing protocols (like RIP, OSPF, BGP), VLANs, access control lists (ACLs), VPNs, and various server roles (like DHCP, DNS, HTTP).

CPT also offers a simulation mode where you can observe data packets traversing the network in real-time. This visual representation helps in understanding how network protocols work, how data is encapsulated and decapsulated, and how traffic flows through different network segments. You can inspect packet headers and contents to diagnose connectivity issues and verify configurations.

## Network Layout

The secure multinational IT company network in Cisco Packet Tracer features a central, robust headquarters with core routers, VLAN-segmented switches, a high-availability firewall cluster, and a VPN hub connecting to the internet. Branch offices globally connect securely via VPN tunnels, each having local routers, VLAN-segmented switches, and firewalls. A DMZ at headquarters hosts public-facing servers like web and email, protected by an additional layer. Local networks within each office utilize switches for wired and wireless (WAPs) connectivity for employee PCs, all designed with security in mind through firewalls, VPNs, VLANs, and potentially ACL.

### Topology Overview

Here's a quick topology overview for your secure multinational IT company network in Cisco Packet Tracer:

It's a **hybrid topology**, primarily using a **hierarchical (or multi-tiered) model**.

* **Core Layer (HQ):** Acts as the central backbone with high-end routers and switches for fast, reliable inter-network communication. 1
* **Distribution Layer (HQ & Branches):** Provides connectivity and policy-based control between the core and access layers, often using Layer 3 switches for routing and VLAN management.
* **Access Layer (All Offices):** Where end-user devices (PCs, WAPs) connect to the network via switches.

### Connectivity

Both machines are connected via **cables like optic fiber, cat5, cat5e, and cat6**, ensuring full connectivity between them while connecting the remote PC sufficiently.

### Network Characteristics

 **Secure:** Implements firewalls, VPNs, VLANs, and potentially ACLs for robust protection.

 **Scalable:** Designed to accommodate future growth with modular design and hierarchical structure.

 **Reliable:** Features redundant core components (routers, firewalls) and stable inter-office VPN connections.

 **Segmented:** Utilizes VLANs to isolate traffic and enhance security within local networks.

 **Global:** Connects geographically dispersed offices securely via VPNs.

 **Hierarchical:** Organized in core, distribution, and access layers for efficient management and traffic flow.

**Security Considerations:**

 **Firewall Enforcement:** Strict traffic control at network perimeters and branch locations.

 **VPN Encryption:** Secure inter-office communication over public networks.

 **VLAN Segmentation:** Isolating sensitive data and limiting breach impact within LANs.

 **Access Control Lists (ACLs):** Granular control over network resource access.

 **DMZ Implementation:** Protected zone for public-facing servers.

 **Strong Authentication:** Secure access to network devices and resources (potentially RADIUS/TACACS+).

 **Regular Monitoring:** Ongoing surveillance for suspicious activity.

 **Security Awareness:** Importance of user education (though not directly in the CPT layout).

## Security and management control

**Security and management control** at the local network level. Here's the breakdown:

* **Prevent Unauthorized Access:** Passwords restrict physical and remote (e.g., Telnet, SSH) access to the switch's configuration interface. This prevents unauthorized individuals from making changes to the network settings, potentially disrupting operations or introducing security vulnerabilities.
* **Maintain Network Stability:** By controlling who can configure the switches, you reduce the risk of accidental misconfigurations that could lead to network outages or performance issues affecting local users.
* **Enhance Security Posture:** Securing each access layer switch is a fundamental security practice. If an attacker gains physical access to a building or manages to get onto the local network, passwords on the switches make it significantly harder for them to pivot further into the network or tamper with local network segments.
* **Facilitate Accountability:** Knowing who has access to configure network devices can aid in troubleshooting and identifying the source of any configuration errors or malicious activities. While individual logins are ideal, a strong password policy at least provides a basic level of accountability within the local team.
* **Enforce Security Policies:** Requiring passwords on all network devices aligns with standard security policies and best practices for protecting network infrastructure.

## Intent Behind Each step

Intent behind each step in building this secure multinational network in CPT:

* **Core Layer Setup (HQ):** Create a high-capacity, reliable backbone for all inter-office and internal communication.
* **Distribution Layer Setup (HQ & Branches):** Implement logical segmentation (VLANs) and routing policies to control traffic flow and enhance organization.
* **Access Layer Setup (All Offices):** Provide secure and managed network access for end-users and devices.
* **Firewall Implementation (All Offices):** Establish security perimeters to prevent unauthorized access and external threats.
* **VPN Configuration (HQ & Branches):** Create secure and encrypted tunnels for private communication over the public internet.
* **DMZ Creation (HQ):** Isolate public-facing servers to allow external access while protecting the internal network.
* **VLAN Design & Configuration (All Offices):** Segment network traffic based on department or function for security and efficiency.
* **IP Addressing & Subnetting:** Organize network devices logically for efficient routing and management.
* **Routing Protocol Configuration:** Enable communication between different network segments and offices.
* **Access Control List (ACL) Implementation:** Enforce granular security policies by controlling traffic based on specific criteria.
* **Testing & Verification:** Ensure all components are functioning as intended and security measures are effective.

# Chapter 4: Understanding the Components & Technologies Used

Cisco Packet Tracer (CPT) is a robust and versatile network simulation tool developed by Cisco Systems, primarily designed to aid students, instructors, and network professionals in learning and understanding networking concepts. It provides a realistic, albeit virtual, environment where users can create complex network topologies by dragging and dropping various network devices like routers, switches, firewalls, and end-user devices. These virtual devices behave much like their physical counterparts, running a simulated version of the Cisco IOS (Internetwork Operating System).

This allows for the configuration and experimentation with a wide range of networking protocols and technologies, including routing protocols (RIP, OSPF, BGP), VLANs, security features (ACLs, basic firewall configurations), and various server functionalities (DHCP, DNS, HTTP). The intuitive graphical interface, coupled with the command-line access to devices, makes CPT an invaluable tool for both beginners grasping fundamental concepts and experienced individuals prototyping network designs or troubleshooting scenarios without the need for expensive physical equipment.

The benefits of using Cisco Packet Tracer are numerous, especially in the realm of network education and preliminary design. It significantly reduces the cost associated with learning networking by eliminating the need for physical hardware. This accessibility allows a wider range of individuals to engage with network concepts and experiment freely without risk to live networks. CPT fosters a hands-on learning approach, enabling users to solidify their understanding through practical application.

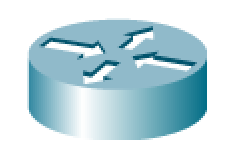
Beyond education, network professionals can leverage CPT to prototype small to medium-sized network designs, test configurations before deployment, and troubleshoot potential issues in a safe and controlled environment. While it's a simulation and doesn't perfectly replicate all nuances of real-world hardware, Cisco Packet Tracer provides a powerful and user-friendly platform for exploring the complexities of network infrastructure and security, making it an indispensable tool in the networking field.

## Routers

**Routers** are fundamental networking devices that operate at Layer 3 (Network Layer) of the OSI model. Their primary function is to forward data packets between different networks. Routers achieve this by examining the destination IP address of incoming packets and consulting their routing tables to determine the optimal path to the destination network.

They make intelligent forwarding decisions based on network topology, routing protocols (such as RIP, OSPF, and BGP), and configured policies. In a complex multinational network, routers are crucial for connecting geographically dispersed offices, facilitating communication over wide area networks (WANs), and providing connectivity to the internet.

They often implement security features like basic firewalls and access control lists to filter traffic and protect network segments. High-end routers in the core of a large network are designed for high throughput, redundancy, and the ability to handle complex routing algorithms for efficient and reliable data delivery across vast distances.

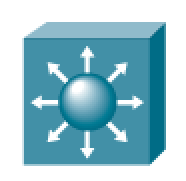


## Core or L3 Switch

**Core switches** reside at the heart of a network infrastructure, typically operating at Layer 2 (Data Link Layer) or Layer 3. Layer 3 core switches possess routing capabilities and are often used for high-speed inter-VLAN routing within a large local area network (LAN) or campus environment.

Their primary role is to provide a high-bandwidth, low-latency switching fabric for connecting distribution layer switches and other critical network components. Core switches are characterized by their high port density, fast backplane speeds, and robust architecture to handle massive amounts of traffic. Redundancy in power supplies and switching fabrics is a common feature to ensure network uptime.

Unlike access layer switches that connect directly to end-user devices, core switches primarily aggregate traffic from multiple distribution switches, forming the central nervous system of the LAN.



## L2 Switch

**Layer 2 (L2) switches** operate at the Data Link Layer and are responsible for forwarding traffic based on MAC addresses. They learn the MAC addresses of connected devices and build a MAC address table to efficiently switch frames within the same network segment or VLAN. L2 switches are commonly deployed at the access layer, connecting end-user devices like computers, laptops, and printers to the network.

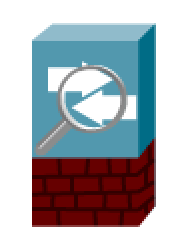
A key differentiation within L2 switches is the presence or absence of **Power over Ethernet (PoE)** capability. **PoE switches** can supply electrical power to connected devices, such as wireless access points, IP cameras, and VoIP phones, over the Ethernet cable, eliminating the need for separate power adapters.

**Non-PoE switches** only provide data connectivity. The choice between PoE and non-PoE switches depends on the types of devices being connected and the desired deployment flexibility..



## Firewall

**Firewalls** are critical security devices that act as a barrier between trusted internal networks and untrusted external networks (like the internet). They operate at various layers of the OSI model, inspecting incoming and outgoing network traffic based on a predefined set of rules. Firewalls control access by permitting or denying network traffic based on source and destination IP addresses, port numbers, and protocols. Modern firewalls often incorporate advanced features such as stateful packet inspection, intrusion prevention systems (IPS), content filtering, and VPN termination capabilities. In a multinational IT company, firewalls are deployed at the network perimeter, at branch offices, and potentially between internal network segments to enforce security policies, prevent unauthorized access, and protect sensitive data from cyber threats.

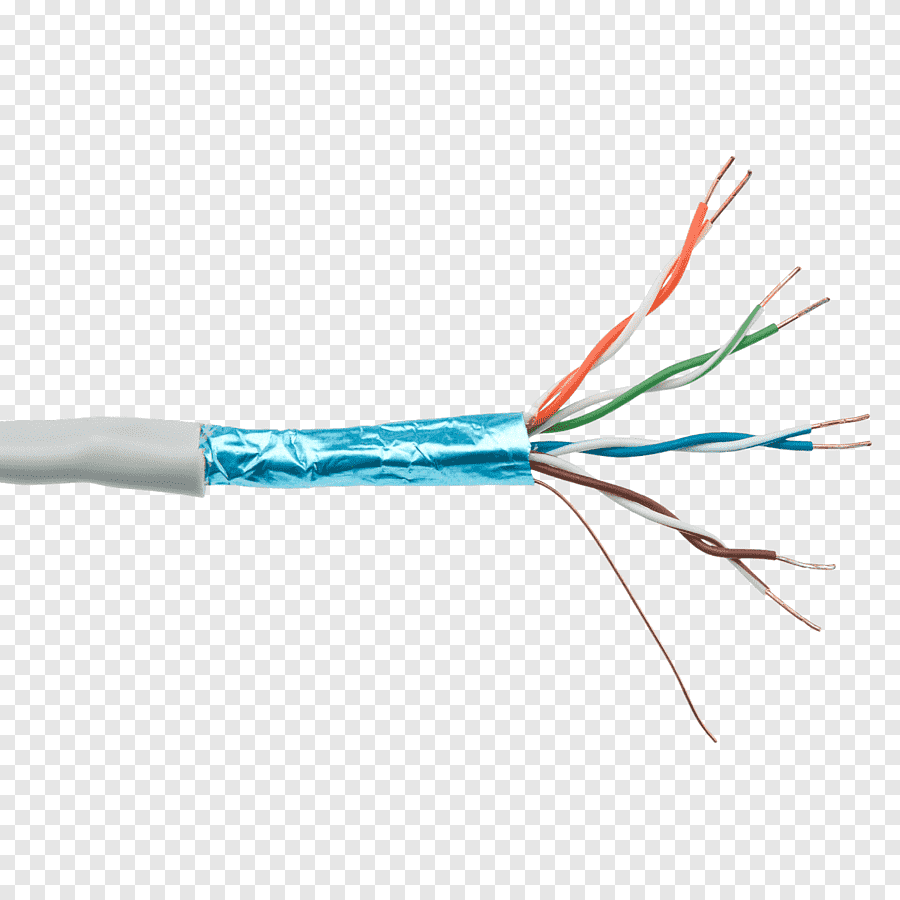


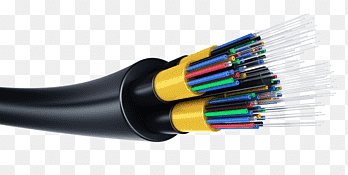
## 4.5 Cables

**Cables** are the physical media that transmit data signals across a wired network. The most common type of cable used in LANs is **Ethernet cable**, such as Cat5e, Cat6, and Cat6a, which consists of twisted pairs of copper wires. Different categories of Ethernet cables support varying data transfer speeds and are chosen based on the bandwidth requirements of the connected devices and the distance of the connection.

**Fiber optic cables** are used for high-speed, long-distance connections, often forming the backbone of large networks or connecting different buildings. Fiber cables transmit data as light pulses, offering higher bandwidth and immunity to electromagnetic interference compared to copper cables.

The proper selection and installation of cables are essential for ensuring reliable and high-performance network connectivity.





## 4.6 Access Points

## Access Points (APs) are networking devices that allow wireless devices, such as laptops, smartphones, and tablets, to connect to a wired network using Wi-Fi technology. APs act as a bridge between the wireless and wired networks, receiving data from wireless clients and forwarding it to the wired network, and vice versa.

## They operate at the Data Link Layer (Layer 2). Modern APs support various Wi-Fi standards (e.g., 802.11ac, 802.11ax) offering different data rates and features. Security is a critical consideration for wireless networks, and APs implement various security protocols like WPA2 and WPA3 to encrypt wireless communication and prevent unauthorized access.

## In a multinational company, strategically placed APs ensure comprehensive wireless coverage throughout office spaces, providing flexibility and mobility for employees.

## 

## 

**4.7 Cloud Cluster**

The **cloud** in the context of a network infrastructure typically refers to a collection of remote servers and data centers accessible over the internet. For a multinational IT company, cloud services can be utilized for various purposes, including data storage, application hosting, software as a service (SaaS), and infrastructure as a service (IaaS).

Connecting the internal network to the cloud is a crucial aspect of modern IT infrastructure. This connection often involves secure links, such as VPNs or dedicated leased lines, to ensure data privacy and security when communicating with cloud-based resources. Cloud services offer scalability, flexibility, and cost-effectiveness, allowing companies to offload certain IT functions and resources to external providers.

The network infrastructure must be designed to efficiently and securely connect to and utilize these cloud resources, ensuring seamless integration with on-premises systems.



**4.8 Computer**

A computer is an electronic device designed to process data according to a set of instructions, known as a program. It encompasses a central processing unit (CPU) that executes these instructions, memory (RAM) for temporary data storage, and storage devices (like hard drives or SSDs) for persistent data.

Input devices, such as keyboards and mice, allow users to interact with the computer, while output devices, like monitors, display the processed information. A computer can range from a stationary desktop unit with separate peripherals to integrated portable devices.

Its fundamental purpose is to perform calculations, manage information, run software applications, and facilitate various tasks from communication to complex simulations.



**4.9 Laptop**

A laptop, also known as a notebook, is a portable personal computer that integrates most of the components of a desktop computer into a single, battery-powered unit. It typically features a clamshell design with a screen on the inside of the upper lid and a keyboard and pointing device (touchpad or trackpad) on the inside of the lower lid.

Laptops are designed for mobility and convenience, allowing users to work or engage in computing tasks in various locations without needing to be tethered to a power outlet for extended periods (depending on the battery). While generally offering similar functionalities to desktop computers, laptops prioritize portability, often resulting in trade-offs in terms of processing power, graphics capabilities, and expandability compared to their desktop counterparts at a similar price point.



**4.10 Printer**

A printer is an output peripheral device that produces a tangible representation of digital information, usually on paper. It receives electronic data from a computer and transfers text or images onto the physical medium. Printers utilize various printing technologies, including inkjet (spraying liquid ink), laser (using toner and heat), and thermal (transferring wax-based ink or using heat-sensitive paper).

They are characterized by factors such as print speed (pages per minute), resolution (dots per inch for image quality), color capability (black and white or color), and connectivity options (USB, network). Printers serve the fundamental purpose of creating hard copies of documents, photographs, and other digital content, making information accessible in a physical format.



**4.11 Server**

A **server** is a powerful computer system or software application designed to provide specific services, resources, or data to other computers (known as clients) over a network. Unlike personal computers 1 primarily used for individual tasks, servers are built and optimized for continuous operation, high availability, and the ability to handle requests from multiple clients simultaneously. They form the backbone of modern IT infrastructure, enabling communication, resource sharing, and the delivery of applications and services across local networks and the internet.

A **server** is a powerful computer system or software application designed to provide specific services, resources, or data to other computers (known as clients) over a network. Unlike personal computers 1 primarily used for individual tasks, servers are built and optimized for continuous operation, high availability, and the ability to handle requests from multiple clients simultaneously. They form the backbone of modern IT infrastructure, enabling communication, resource sharing, and the delivery of applications and services across local networks and the internet.

The functionality of a server is largely defined by the software it runs. Different types of server software are designed for specific purposes. **Web servers**, such as Apache and Nginx, host websites and deliver web pages and related content to users' browsers. **File servers** act as centralized repositories for storing and managing files, allowing multiple users to access and share them. **Email servers**, like Microsoft Exchange Server and Postfix, handle the sending, receiving, and storage of electronic mail.

**Database servers**, such as MySQL, PostgreSQL, and Oracle, manage and provide access to structured data. **Application servers** host business applications and provide the underlying infrastructure for them to run and interact with clients. **DNS servers** translate domain names into IP addresses, enabling users to access websites using human-readable names. **DHCP servers** automatically assign IP addresses and network configuration parameters to client devices.

In the context of a multinational IT company, servers play a crucial role in supporting global operations. They host internal applications, manage user accounts and authentication, facilitate inter-office communication, store and share data across different locations, and provide access to cloud-based services. A well-designed and managed server infrastructure is essential for ensuring business continuity, operational efficiency, and the security of sensitive information in a globally distributed environment. The reliability, scalability, and security of these servers directly impact the productivity and 

**4.12 Routing Protocols**

**4.12.1 OSPF**

**OSPF (Open Shortest Path First)** is a link-state routing protocol operating within a single autonomous system (AS). Unlike distance-vector protocols, OSPF routers maintain a complete map of the network topology. They achieve this by exchanging link-state advertisements (LSAs) with their neighbors, detailing the state of their directly connected links.

Using the Shortest Path First (SPF) algorithm (Dijkstra's algorithm), each router independently calculates the shortest path to all destinations within the AS, resulting in a loop-free topology. OSPF is known for its fast convergence, efficient use of bandwidth (only sending updates when changes occur), and support for VLSM (Variable Length Subnet Masks).

It organizes networks into areas to improve scalability and manageability, with a backbone area (Area 0) serving as the central connecting point for all other areas. OSPF supports various authentication methods to secure routing updates and is well-suited for medium to large-sized enterprise networks requiring stability and efficient routing.

**4.12.2 EIGRP**

**EIGRP (Enhanced Interior Gateway Routing Protocol)** is an advanced distance-vector routing protocol, initially proprietary to Cisco but now an open standard. Often described as a hybrid protocol, EIGRP combines aspects of both distance-vector and link-state protocols. It uses the Diffusing Update Algorithm (DUAL) to ensure loop-free paths and achieve rapid convergence.

Unlike RIP, EIGRP only sends partial and bounded updates when network topology changes occur, minimizing bandwidth consumption. It supports VLSM and offers features like unequal-cost load balancing, allowing traffic to be distributed across multiple paths with different metrics.

EIGRP establishes neighbor relationships and exchanges routing information, maintaining a topology table of all known routes and their feasibility. It's well-suited for mid-sized to large enterprise networks, offering a balance of fast convergence, scalability, and ease of configuration compared to some link-state protocols.

**4.12.3 RIP**

**RIP (Routing Information Protocol)** is one of the oldest and simplest distance-vector routing protocols. It relies on hop count as its primary metric to determine the best path to a destination, with a maximum hop count of 15 (16 indicates infinity, or an unreachable network). RIP routers broadcast their entire routing tables to their directly connected neighbors every 30 seconds.

This periodic broadcasting of full routing tables makes it less efficient in terms of bandwidth usage and slower to converge compared to link-state or more advanced distance-vector protocols. RIPv1 is a classful routing protocol (doesn't support VLSM), while RIPv2 introduced support for classless routing, authentication, and multicast updates.

Due to its limitations in scalability and convergence speed, RIP is generally recommended for small networks or as a teaching tool to understand basic routing concepts.

**Chapter-5 Understanding the Various networking concepts**

Our exploration will delve into the fundamental building blocks of networks, starting with the basic hardware components like cables, switches, and routers, and extending to the logical frameworks that dictate how data is transmitted and organized. We will examine the layered models that provide a structured approach to understanding network communication, dissecting the roles and responsibilities of each layer. Furthermore, we will introduce key concepts such as IP addressing, subnetting, and routing, which are essential for identifying and directing traffic across networks, both small and large.

Understanding these networking concepts is not merely a technical exercise; it is crucial for anyone seeking to navigate, manage, or secure the increasingly interconnected world around us. Whether you are aspiring to a career in IT, a business professional relying on network infrastructure, or simply a curious individual seeking to understand the technology that powers our modern lives, this chapter will provide you with the essential knowledge to comprehend the language and logic of networking. By grasping these foundational principles, you will gain a deeper appreciation for the complexity and elegance of the systems that enable our digital interactions and lay the groundwork for exploring more advanced networking topics in the chapters to come.

**5.1 Access Control Lists (ACLs) - The Gatekeepers of Network Traffic**

Access Control Lists (ACLs) are the bedrock of network security, acting as the vigilant gatekeepers that determine which network traffic is permitted to pass through specific interfaces on routers and switches. Imagine a physical building with numerous doors and corridors. An ACL is like having security guards stationed at each entry and exit point, meticulously checking the credentials of every individual attempting to pass. These "credentials" in the network world are the attributes of network traffic: the source and destination IP addresses, the specific ports being used (like the door number), and the communication protocol (like the language being spoken).

The criteria for matching traffic can be highly specific. For instance, an ACE could be configured to deny all TCP traffic originating from a particular IP address destined for a specific port on a server, effectively blocking a specific type of unwanted connection. Conversely, another ACE could permit all HTTP traffic (port 80) from any source to a web server, allowing legitimate web browsing.

A crucial aspect of ACLs is the implicit deny statement. If a packet traverses an ACL and does not match any of the explicitly defined ACEs, a default, unspoken rule kicks in, which is to deny the traffic. This "deny all that is not explicitly permitted" philosophy is a cornerstone of secure network design, ensuring that only explicitly authorized traffic is allowed to flow.

**Key Features:**

* **Precise Traffic Filtering:** Enables highly specific control over network traffic based on a wide range of packet attributes (source/destination IP, MAC addresses, protocols, ports, TCP flags, etc.).
* **Ordered Rule Processing (First-Match):** The sequential evaluation of Access Control Entries (ACEs) dictates that the first matching rule determines the action, emphasizing the importance of rule order.
* **Implicit Deny Mechanism:** Provides a fundamental security posture by blocking any traffic that does not explicitly match a permit rule, ensuring a "default-deny" approach.
* **Directional Application (Inbound/Outbound):** Offers flexibility in controlling traffic flow at network boundaries, allowing for tailored security policies at different points in the network.
* **Versatile Application Scope:** Can be implemented on router interfaces to control traffic between networks and on switch interfaces (VLAN interfaces or physical ports) to control traffic within a LAN.
* **Stateful vs. Stateless Capabilities (in some advanced ACL implementations):** While basic ACLs are stateless (evaluating each packet independently), some advanced implementations can track the state of connections, providing more context-aware filtering.
* **Time-Based ACLs (in some implementations):** Allow rules to be active only during specific timeframes, providing temporal control over network access.
* **Logging Capabilities:** Many network devices can log when traffic matches ACL rules, aiding in security monitoring and troubleshooting.

**5.2. SSH (Secure Shell) - The Secure Conduit for Remote Management**

Secure Shell (SSH) is not merely a protocol; it's a secure and indispensable tool for modern network administration and secure data transfer. In an era where network breaches and data interception are significant threats, SSH provides a robust, encrypted tunnel over inherently insecure networks like the internet. Imagine trying to have a private conversation in a crowded room. SSH creates a secure, soundproof booth where all communication between two parties is shielded from prying ears.

SSH operates at the application layer (Layer 7) of the OSI model, leveraging the reliability of the TCP protocol (typically on port 22). When an SSH client initiates a connection to an SSH server, a handshake process begins. During this handshake, the client and server negotiate a suite of cryptographic algorithms for encryption, authentication, and data integrity. Strong encryption algorithms, such as AES and ChaCha20, ensure that all data exchanged within the SSH session is scrambled and unintelligible to any unauthorized observers.

Authentication is a critical aspect of SSH. It verifies the identity of both the client and the server. The most common authentication methods are password-based authentication and public-key cryptography. Password-based authentication, while simpler to set up initially, involves transmitting the user's password over the encrypted SSH connection. While the connection itself is secure, relying solely on passwords can be vulnerable to brute-force attacks if weak passwords are used.

**Key Feature:**

* **End-to-End Encryption:** Employs strong cryptographic algorithms (e.g., AES, ChaCha20) to encrypt all data exchanged between the client and server, ensuring confidentiality.
* **Secure Authentication Mechanisms:** Supports both password-based authentication (encrypted during transit) and more robust public-key cryptography for enhanced security.
* **Integrity Protection:** Ensures that data transmitted over the SSH connection is not tampered with in transit, often using cryptographic hashing algorithms.
* **Secure Remote Command Execution:** Allows administrators to securely execute commands on remote servers and network devices, facilitating remote management and troubleshooting.
* **Secure File Transfer (SCP and SFTP):** Provides secure protocols for transferring files between systems, protecting data during transmission.
* **Port Forwarding (SSH Tunneling):** Enables the secure forwarding of other TCP ports over the SSH connection, allowing secure access to other services or bypassing firewall restrictions.
* **Widely Supported:** Implemented on virtually all modern operating systems and network devices, ensuring broad compatibility.

**5.3. TCL (Tool Command Language) - The Scripting Ally for Network Automation**

While not a networking protocol in the traditional sense, Tool Command Language (Tcl) is a powerful and versatile scripting language that has found significant utility in the realm of network automation and management. Think of Tcl as a skilled assistant who can understand and execute a series of instructions to automate repetitive and time-consuming network tasks. Its dynamic, interpreted nature allows for rapid development and execution of scripts, making it an agile tool for network engineers.

Many network devices, particularly those from Cisco and other vendors, provide Tcl interpreters embedded within their operating systems or offer APIs that can be accessed using Tcl. This allows network administrators to interact programmatically with the device's configuration and operational state. Instead of manually typing commands into a command-line interface (CLI), engineers can write Tcl scripts to perform tasks such as configuring multiple devices with consistent settings, collecting network statistics for monitoring and analysis, or automating basic troubleshooting steps.

Tcl's strength lies in its simplicity and extensibility. Its syntax is relatively easy to learn, making it accessible for network engineers who may not have extensive programming backgrounds. Furthermore, Tcl can be extended with custom modules and libraries to provide specific functionalities tailored to networking needs. For instance, there are Tcl libraries that facilitate interaction with SNMP (Simple Network Management Protocol) for device monitoring or with Telnet/SSH for interacting with device CLIs.

Consider a scenario where a network administrator needs to update the banner message on hundreds of network switches. Manually logging into each switch and typing the configuration commands would be incredibly time-consuming and prone to errors. A Tcl script could automate this entire process, securely connecting to each switch (perhaps via SSH), executing the necessary commands, and logging the outcome. Similarly, Tcl scripts can be used to automate the collection of interface statistics, check the status of routing protocols, or even perform basic compliance checks against a defined network configuration baseline.

**Key Features:**

* **Powerful Automation Capabilities:** Enables the creation of scripts to automate a wide range of network configuration, management, and monitoring tasks, saving time and reducing manual errors.
* **Embedded Interpreters on Network Devices:** Many network devices (especially Cisco) include built-in Tcl interpreters, allowing for direct scripting on the devices themselves.
* **API Interaction:** Provides a means to interact with network device APIs for programmatic configuration and data retrieval.
* **Extensive Libraries and Packages:** Offers various extensions and libraries that facilitate network-specific tasks, such as SNMP interaction, Telnet/SSH communication, and data parsing.
* **Rapid Development and Prototyping:** Its dynamic and interpreted nature allows for quick creation and testing of automation scripts.
* **Cross-Platform Compatibility:** Tcl interpreters are available for various operating systems, enhancing the portability of scripts.
* **Integration with Network Management Systems:** Often supported by network management platforms for custom automation workflows and integrations.

**5.4. DMZ (Demilitarized Zone) - The Fortified Buffer for Public Services**

The Demilitarized Zone (DMZ) is a crucial architectural element in network security, acting as a carefully controlled buffer subnetwork positioned between an organization's private internal network and the untrusted public internet. Its primary intent is to host outward-facing services – such as web servers, email servers, and DNS servers – in a segregated environment. This isolation prevents direct external access to the sensitive resources residing on the internal network. The DMZ serves as a sacrificial lamb in a security strategy; if a public-facing server is compromised, the attacker's access is limited to the DMZ, making it significantly harder to pivot into the more valuable internal network.

Traffic flow in and out of the DMZ is strictly governed by firewalls. An external firewall controls connections originating from the internet destined for the services within the DMZ, typically allowing only necessary ports and protocols (e.g., HTTP/HTTPS for web servers, SMTP/POP3/IMAP for email). An internal firewall then regulates traffic between the DMZ and the internal network, generally implementing a very restrictive policy that often denies all but explicitly permitted communication initiated from the internal network towards specific services in the DMZ. This dual-firewall approach creates a layered security posture, ensuring that even if the external defenses are breached, the internal network remains largely protected.

The implementation of a DMZ is a fundamental security best practice for any organization that offers services to the public. It provides a secure and manageable way to expose necessary services while minimizing the attack surface of the internal network. By carefully controlling the perimeter of the DMZ and the traffic flow across it, organizations can significantly reduce the risk of successful cyberattacks targeting their critical internal resources. The DMZ represents a strategic compromise between accessibility and security, allowing necessary external interaction without compromising the confidentiality and integrity of internal operations.

**Key Feature:**

The DMZ acts as a strategically placed, isolated subnetwork, forming a vital buffer zone between an organization's trusted internal network and the potentially hostile external internet. Its core function is to house public-facing services like web and email servers, ensuring their accessibility to external users while simultaneously shielding the more sensitive internal resources from direct exposure to cyber threats. This segregation is a cornerstone of defense-in-depth, limiting the potential damage in the event of a compromise of a public-facing server.

Traffic management within a DMZ relies heavily on a dual-firewall architecture. An external firewall meticulously controls inbound traffic from the internet to the DMZ, permitting only essential services on specific ports, effectively reducing the attack surface. Subsequently, an internal firewall governs the communication between the DMZ and the internal network, typically employing a stringent "deny-all" policy with explicitly defined exceptions for internal systems needing to access specific resources within the DMZ. This layered approach ensures that even if an attacker breaches the external defenses and gains access to the DMZ, further lateral movement into the internal network is significantly impeded.

By implementing a well-designed and managed DMZ, organizations achieve a critical balance between providing necessary external services and safeguarding their internal assets. This architectural pattern allows for controlled interaction with the outside world without directly exposing the core operational infrastructure to the inherent risks of the internet. The DMZ stands as a testament to proactive security planning, offering a secure and manageable environment for public-facing services while fortifying the internal network against potential intrusions originating from external sources.

* 1. **LASP (Link Aggregation Control Protocol) - The Bandwidth Booster and Resilience Builder**

Link Aggregation Control Protocol (LACP), standardized under IEEE 802.3ad, is a dynamic protocol that empowers network devices to automatically negotiate and manage the bundling of multiple physical Ethernet links into a single, high-bandwidth logical link. Imagine individual water pipes combining into a larger conduit; LACP achieves a similar effect for network data. This aggregation not only dramatically increases the available bandwidth between connected devices, such as switches and servers, but also introduces a significant layer of link redundancy.

The process begins with devices configured for link aggregation communicating with each other using LACP packets. These packets advertise their capabilities and willingness to participate in an aggregation group. Based on configuration consistency (e.g., speed, duplex settings) and administrative policies, the protocol determines which physical links can be combined into the logical bundle, often referred to as a LAG (Link Aggregation Group) or port channel. Once the LAG is established, traffic is intelligently distributed across the active member links using various load-balancing algorithms. This ensures optimal utilization of the aggregated bandwidth.

The resilience aspect of LACP is equally crucial. If one or more of the physical links within the LAG experience a failure, the protocol automatically detects the loss and redistributes the traffic across the remaining active links. This failover mechanism is typically seamless and transparent to end-users and applications, ensuring continuous network connectivity and preventing service disruptions. LACP can operate in active mode, where a device actively initiates the negotiation to form a LAG, or in passive mode, where a device only participates in a LAG if the other end initiates the process. This standards-based protocol ensures interoperability between equipment from different vendors, making it a widely adopted technology for enhancing both the capacity and reliability of critical network connections.

**Key features:**

Link Aggregation Control Protocol (LACP) serves as a dynamic mechanism for combining multiple physical Ethernet links into a single logical channel, effectively multiplying the available bandwidth between interconnected network devices. This aggregation not only provides a significant boost in data throughput, allowing for faster and more efficient communication, but also introduces a vital element of link-level redundancy, enhancing the overall resilience of the network infrastructure. By treating multiple physical connections as one logical pathway, LACP optimizes data transmission and provides a safeguard against individual link failures.

The operation of LACP involves an automated negotiation process between participating network devices. Through the exchange of LACP control packets, devices advertise their capabilities and configurations, allowing them to dynamically identify compatible links that can be bundled together into a Link Aggregation Group (LAG). Once formed, the LAG intelligently distributes network traffic across its member links based on configured load-balancing algorithms, ensuring efficient utilization of the aggregated bandwidth. This dynamic management simplifies configuration and ensures that the link aggregation adapts to changes in the physical link status.

Beyond its bandwidth-enhancing capabilities, LACP provides crucial link redundancy. Should any of the physical links within a LAG fail, the protocol swiftly detects the disruption and automatically redistributes traffic across the remaining operational links. This seamless failover mechanism ensures continuous connectivity and minimizes the impact of hardware failures on network services. As a standardized protocol (IEEE 802.3ad), LACP promotes interoperability across different vendors' equipment, making it a universally applicable solution for building high-capacity and highly available network connections in diverse networking environments.

**5.6. HSRP (Hot Standby Router Protocol) - The Guardian of the Default Gateway**

Hot Standby Router Protocol (HSRP) is a Cisco-developed first-hop redundancy protocol (FHRP) designed to provide a highly available default gateway for hosts on a local area network (LAN). In essence, HSRP allows a group of routers to collaborate, presenting a single, virtual IP address and MAC address as the default gateway to the connected devices. This creates the illusion of a single, resilient router, ensuring that even if the physical router currently acting as the gateway fails, another router in the group can seamlessly take over, maintaining uninterrupted network connectivity for the end-users.

Within an HSRP group, one router assumes the role of the active router, responsible for forwarding traffic destined for the virtual IP address. One or more other routers in the group function as standby routers, constantly monitoring the health and status of the active router. These standby routers exchange periodic multicast hello messages with the active router to confirm its operational status. If the active router fails to send these hello messages within a configurable timeframe, a standby router with the next highest priority automatically assumes the active role, a process known as failover.

The transition during a failover is designed to be transparent to the end-user devices. Because the hosts are configured with the virtual IP address and MAC address as their default gateway, they continue to send traffic to the same logical address, regardless of which physical router is currently active. This seamless failover ensures that network connectivity is maintained without requiring any manual reconfiguration on the client devices. HSRP offers preemption, a feature that allows a higher-priority standby router to reclaim the active role once it recovers from a failure. This protocol is a cornerstone of high-availability network design, ensuring that the loss of a single router does not disrupt network access for LAN clients.

**Key Features:**

Hot Standby Router Protocol (HSRP) is a Cisco-engineered first-hop redundancy protocol that orchestrates a group of routers to act as a unified, highly available default gateway for devices within a local area network (LAN). By presenting a single virtual IP address and MAC address, HSRP shields end-users from the complexities of underlying router failures, ensuring continuous network access. This collaborative approach among routers creates a resilient first point of contact for all outgoing traffic from the LAN, preventing single points of failure from disrupting network connectivity.

In an HSRP configuration, one router is designated as the active router, bearing the responsibility of forwarding all traffic directed towards the virtual IP address. Simultaneously, one or more standby routers diligently monitor the active router's health through periodic exchange of multicast "hello" messages. Should the active router falter and cease sending these heartbeat signals, a standby router, prioritized based on its configured value, swiftly assumes the active role. This automatic failover mechanism ensures a rapid transition of gateway responsibilities, minimizing any potential downtime experienced by connected devices.

The beauty of HSRP lies in its transparency to the end-users. Because client devices are configured to use the consistent virtual IP and MAC address as their default gateway, the underlying switch in active routers remains seamless. Whether the original active router or a standby has taken over, the destination for outgoing traffic remains the same, requiring no manual intervention or reconfiguration on the client side. Optional preemption allows a higher-priority router to reclaim the active role upon recovery, ensuring that the most capable device serves as the primary gateway. HSRP is a vital component in building robust and fault-tolerant LAN infrastructures.

**5.7. Inside Servers**

* Located within the organization's protected internal network.
* Host critical internal applications, databases, and file shares.
* Access restricted to authorized internal users and devices.
* Subject to stringent security measures (authentication, patching, backups).
* Essential for core business operations and data management.
* Protected by firewalls and internal security policies.

**5.8. DHCP (Dynamic Host Configuration Protocol)**

* Automated assignment of IP addresses and network configuration.
* Centralized management of IP address allocation.
* Prevents IP address conflicts.
* Reduces manual configuration overhead.
* Provides essential network parameters (subnet mask, gateway, DNS).
* Lease-based IP address assignment.

**5.9. DNS (Domain Name System)**

* Translates human-readable domain names to IP addresses.
* Hierarchical and distributed naming system.
* Essential for internet and network resource access.
* Relies on a global network of DNS servers.
* Caches resolved IP addresses for faster lookups.
* Supports various record types (A, MX, CNAME, etc.).

**5.10. NAS (Network Attached Storage)**

* Centralized file-level storage accessible over the network.
* Provides data access to multiple clients.
* Often features RAID for redundancy and performance.
* Utilizes file-sharing protocols (NFS, SMB/CIFS).
* Offers user authentication and access control mechanisms.
* Simplifies data sharing and backup within a network.

**Chapter-6 Network Commands**

**6.1 Basic Commands**

en

conf t

hostname HOSTNAME

line console 0

password cisco

login

logging synchronous

exec-timeout 3 0

exit

enable password cisco

banner motd #NO ILLEGAL ACTIVITY MUST BE DONE!!!#

no ip domain-lookup

service password-encryption

username cisco password cisco

ip domain-name adityajoshi.com

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

login local

transport input ssh

exit

access-list 1 permit 192.168.10.0 0.0.0.255

access-list 1 deny any

line vty 0 15

access-class 1 in

exit

dowrite

**6.2 VLAN assignment plus all access and trunk ports on l2 and l3 switches**

############################ MK-SW, HR-SW, FINANCE-SW, ADMIN-SW, ICT-SW########################################

int range fa0/1-2

switchport mode trunk

exit

vlan 10

name MGT

VLAN 20

NAME LAN

VLAN 50

NAME WLAN

VLAN 70

NAME VoIP

VLAN 199

NAME Blachole

exit

int range fa0/3-4

switchport mode access

switchport access vlan 20

exit

int range fa0/5-6

switchport mode access

switchport access vlan 70

exit

int range fa0/7

switchport mode access

switchport access vlan 50

exit

do wr

############################ SERVER-SW ########################################

int range fa0/1-2, fa0/7

switchport mode trunk

exit

vlan 10

name MGT

VLAN 20

NAME LAN

VLAN 50

NAME WLAN

VLAN 70

NAME VoIP

VLAN 90

NAME INSIDE-SERVERS

exit

int range fa0/3-5

switchport mode access

switchport access vlan 90

exit

int fa0/6

switchport mode access

switchport access vlan 50

exit

do wr

############################ MLT1 & MLT2 ########################################

int range gig1/0/3-8

switchport mode trunk

exit

vlan 10

name MGT

VLAN 20

NAME LAN

VLAN 50

NAME WLAN

VLAN 70

NAME VoIP

VLAN 90

NAME INSIDE-SERVERS

exit

do wr

################################# modification ########################################

INT range fa0/5-6

no switchport access vlan 70

switchport voice vlan 70

exit

do wr

**6.2.1 VLAN assignment plus all access and trunk ports on l2 and l3 switches**

FOR SERVERROOM SWITCH

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

INT range FA0/3-6, FA0/8-24

spanning-tree portfast

spanning-tree bpduguard enable

ex

do wr

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

for all switches

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

INT range FA0/3-24

spanning-tree portfast

spanning-tree bpduguard enable

ex

do wr

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

DMZ

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

INT range FA0/1-24

spanning-tree portfast

spanning-tree bpduguard enable

ex

do wr

**6.3 Etherchannel**

MLT1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

interface range gig1/0/9-11

channel-group 1 mode active

ex

interface port-channel 1

switchport mode trunk

ex

do wr

MLT2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

interface range gig1/0/9-11

channel-group 1 mode passive

ex

interface port-channel 1

switchport mode trunk

ex

do wr

**6.4 Subnetting and IP addressing**

MLT1

IP Routing

int gig1/0/1

no switchport

no shut

ip address 10.2.2.1 255.255.255.252

int gig1/0/2

no switchport

no shut

ip address 10.2.2.5 255.255.255.252

ex

do wr

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

MLT2

IP Routing

int gig1/0/1

no switchport

no shut

ip address 10.2.2.9 255.255.255.252

int gig1/0/2

no switchport

no shut

ip address 10.2.2.13 255.255.255.252

ex

do wr

**6.5 HSRP and Inter-VLAN routing on the L3 switches plus ip dhcp helper addresses**

CORE-SW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

interface Vlan10

ip address 192.168.10.3 255.255.255.0

ip helper-address 10.11.11.38

standby 10 ip 192.168.10.1

!

interface Vlan20

ip address 172.16.0.3 255.255.0.0

ip helper-address 10.11.11.38

standby 20 ip 172.16.0.1

!

interface Vlan50

ip address 10.20.0.2 255.255.0.0

ip helper-address 10.11.11.38

standby 50 ip 10.20.0.1

!

interface Vlan90

ip address 10.11.11.34 255.255.255.224

standby 90 ip 10.11.11.33

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CORE-SW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

interface Vlan10

ip address 192.168.10.2 255.255.255.0

ip helper-address 10.11.11.38

standby 10 ip 192.168.10.1

!

interface Vlan20

ip address 172.16.0.2 255.255.0.0

ip helper-address 10.11.11.38

standby 20 ip 172.16.0.1

!

interface Vlan50

ip address 10.20.0.3 255.255.0.0

ip helper-address 10.11.11.38

standby 50 ip 10.20.0.1

!

interface Vlan90

ip address 10.11.11.35 255.255.255.224

standby 90 ip 10.11.11.33

**6.6 OSPF in the firewall, routers, switches**

Core-SW1

!

router ospf 35

router-id 1.1.1.1

network 10.2.2.0 0.0.0.3 area 0

network 10.2.2.4 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0

network 172.16.0.0 0.0.255.255 area 0

network 10.20.0.0 0.0.255.255 area 0

network 10.11.11.0 0.0.0.31 area 0

exit

do wr

!

Core-SW2

!

router ospf 35

router-id 1.1.2.2

network 10.2.2.8 0.0.0.3 area 0

network 10.2.2.12 0.0.0.3 area 0

network 192.168.10.0 0.0.0.255 area 0

network 172.16.0.0 0.0.255.255 area 0

network 10.20.0.0 0.0.255.255 area 0

network 10.11.11.0 0.0.0.31 area 0

exit

do wr

!

SEACOM-ISP

!

router ospf 35

router-id 1.1.3.3

network 105.100.50.0 0.0.0.3 area 0

network 105.100.50.4 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

do wr

!

SAFARICOM-ISP

!

router ospf 35

router-id 1.1.4.4

network 197.200.100.0 0.0.0.3 area 0

network 197.200.100.4 0.0.0.3 area 0

network 30.30.30.0 0.0.0.3 area 0

do wr

!

Router3

!

router ospf 35

router-id 1.1.5.5

network 8.0.0.0 0.255.255.255 area 0

network 20.20.20.0 0.0.0.3 area 0

network 20.20.30.0 0.0.0.3 area 0

do wr

!

**6.7 Firewall interface security zones and levels**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ena

config t

hostname FWL1

int gig1/3

no shut

ip address 10.2.2.2 255.255.255.252

nameif INSIDE1

SECURITY-LEVEL 100

EX

int gig1/4

no shut

ip address 10.2.2.10 255.255.255.252

nameif INSIDE2

SECURITY-LEVEL 100

EX

int gig1/5

no shut

ip address 10.11.11.7 255.255.255.224

nameif DMZ

SECURITY-LEVEL 70

EX

int gig1/1

no shut

ip address 105.100.50.2 255.255.255.224

nameif OUTSIDE1

SECURITY-LEVEL 0

EX

int gig1/2

no shut

ip address 197.200.100.2 255.255.255.252

nameif OUTSIDE2

SECURITY-LEVEL 0

EX

DO WR

WR MEM

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ena

config t

hostname FWL2

int gig1/3

no shut

ip address 10.2.2.6 255.255.255.252

nameif INSIDE1

SECURITY-LEVEL 100

EX

int gig1/4

no shut

ip address 10.2.2.14 255.255.255.252

nameif INSIDE2

SECURITY-LEVEL 100

EX

int gig1/1

no shut

ip address 105.100.50.6 255.255.255.224

nameif OUTSIDE1

SECURITY-LEVEL 0

EX

int gig1/2

no shut

ip address 197.200.100.6 255.255.255.252

nameif OUTSIDE2

SECURITY-LEVEL 0

EX

WR MEM

**6.7.1 Firewall routing- OSPF + static Routes**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.1

route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.1 70

router OSPF 35

router-id 1.1.8.8

network 105.100.50.0 255.255.255.252 area 0

network 197.200.100.0 255.255.255.252 area 0

network 10.11.11.0 255.255.255.224 area 0

network 10.2.2.0 255.255.255.252 area 0

network 10.2.2.8 255.255.255.252 area 0

ex

wr mem

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.5

route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.5

router OSPF 35

router-id 1.1.9.9

network 105.100.50.4 255.255.255.252 area 0

network 197.200.100.4 255.255.255.252 area 0

network 10.2.2.4 255.255.255.252 area 0

network 10.2.2.12 255.255.255.252 area 0

ex

wr mem

**6.8 Firewall inspection policy configuration**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

object network INSIDE1-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1, OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDE1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2, OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2, OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1, OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2, OUTSIDE2) dynamic interface

object network DMZ-OUTSIDE1

subnet 10.11.11.0 255.255.255.224

nat (DMZ, OUTSIDE1) dynamic interface

object network DMZ-OUTSIDE2

subnet 10.11.11.0 255.255.255.224

nat (DMZ, OUTSIDE2) dynamic interface

WR MEM

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

FW2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

!

object network INSIDE1-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDE1-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDE2-OUTSIDE1

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDE2-OUTSIDE2

subnet 172.16.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

object network INSIDEw1-OUTSIDEw1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE1) dynamic interface

object network INSIDEw1-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE1,OUTSIDE2) dynamic interface

object network INSIDEw2-OUTSIDE1

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE1) dynamic interface

object network INSIDEw2-OUTSIDEw2

subnet 10.20.0.0 255.255.0.0

nat (INSIDE2,OUTSIDE2) dynamic interface

!

**6.9 Inspection policies**

10-INSPECTION POLICIES

FW1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

access-list RES extended permit icmp any any

access-list RES extended permit tcp any any eq 80

access-list RES extended permit tcp any any eq 53

access-list RES extended permit udp any any eq 53

access-group RES in interface DMZ

access-group RES in interface OUTSIDE1

access-group RES in interface OUTSIDE2

do wr

FW2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

!

access-list RES extended permit icmp any any

access-list RES extended permit tcp any any eq 80

access-list RES extended permit tcp any any eq 53

access-list RES extended permit udp any any eq 53

!

!

access-group RES in interface OUTSIDE1

access-group RES in interface OUTSIDE2

**6.10 VoIP Configuration**

voip configuration

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Router>ena

Router#config t

Router(config)#int f0/0

Router(config-if)#no shut

Router(config)#int f0/0.70

Router(config-subif)#ip address 172.30.0.1

Router(config-subif)#ip address 172.30.0.1 255.255.0.0

Router(config-subif)#encapsulation dot1q 70

Router(config-subif)#ip address 172.30.0.1 255.255.0.0

Router(config-subif)#ex

Router(config)#service dhcp

Router(config)#ip dhcp pool VOIP.POOL

Router(dhcp-config)#network 172.30.0.0 255.255.0.0

Router(dhcp-config)#default-router 172.30.0.1

Router(dhcp-config)#option 150 ip 172.30.0.1

Router(dhcp-config)#ex

Router(config)#telephony-service

Router(config-telephony)#max-ephones 30

Router(config-telephony)#max-dn 30

Router(config-telephony)#ip source-address 172.30.0.1 port 2000

Router(config-telephony)#auto assign 1 to 30

Router(config-telephony)#ex

Router(config)#ephone-dn 1

Router(config-ephone-dn)#number 401

Router(config-ephone-dn)#ephone-dn 2

Router(config-ephone-dn)#number 402

Router(config-ephone-dn)#ephone-dn 3

Router(config-ephone-dn)#ephone-dn 3

Router(config-ephone-dn)#number 403

Router(config-ephone-dn)#ephone-dn 4

Router(config-ephone-dn)#number 404

Router(config-ephone-dn)#ephone-dn 5

Router(config-ephone-dn)#number 405

Router(config-ephone-dn)#ephone-dn 6

Router(config-ephone-dn)#number 406

Router(config-ephone-dn)#ephone-dn 7

Router(config-ephone-dn)#number 407

Router(config-ephone-dn)#ephone-dn 8

Router(config-ephone-dn)#number 408

Router(config-ephone-dn)#ephone-dn 9

Router(config-ephone-dn)#number 409

Router(config-ephone-dn)#ephone-dn 10

# Chapter 7: Security Analysis

A thorough **security analysis** of the described multinational IT company network design would involve a systematic evaluation of the implemented security controls and the overall network architecture to identify potential vulnerabilities and assess the effectiveness of the security posture. This analysis would examine each component and its configuration in relation to established security best practices and potential threat vectors.

The analysis would start with the perimeter security, focusing on the **firewalls** at the headquarters and branch offices. It would assess the rule sets configured on these firewalls to ensure they are restrictive, following the principle of least privilege, and effectively control traffic flow between the internal network, the DMZ, and the internet.

The configuration of stateful inspection, intrusion prevention systems (IPS) if implemented, and logging mechanisms would also be scrutinized. The **DMZ** itself would be a focal point, ensuring that only necessary services are exposed and that strict traffic controls are in place between the DMZ and both the internal and external networks.

Internal security measures would also be heavily analyzed. The implementation of **VLAN segmentation** and the effectiveness of **Access Control Lists (ACLs)** on routers and switches in controlling traffic flow between different internal segments would be evaluated. The security of the **inside servers**, including operating system hardening, patch management, access controls, and data encryption, would be assessed.

The use of **SSH** for secure remote management of network devices and servers would be examined, focusing on the strength of encryption algorithms and authentication methods (e.g., the use of strong passwords or public-key authentication). The configuration of network services like **DHCP** and **DNS** would also be reviewed for potential security weaknesses, such as rogue DHCP servers or DNS spoofing vulnerabilities.

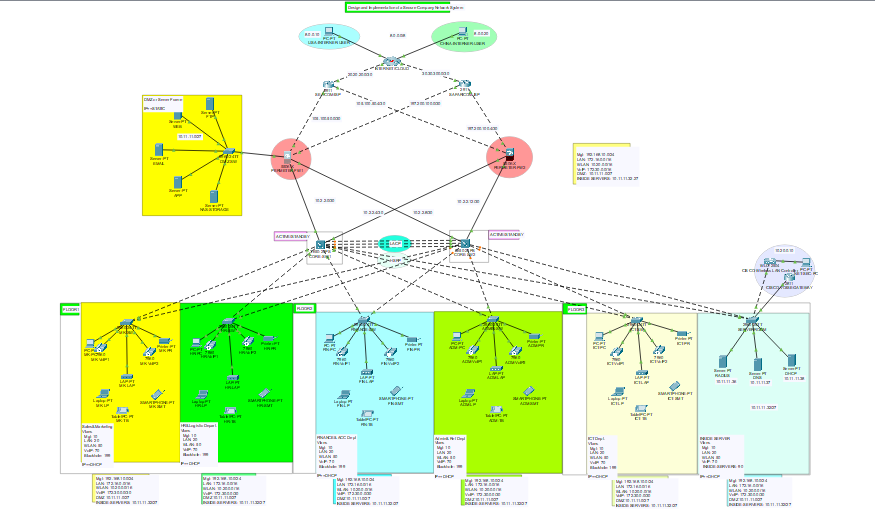
The analysis would also consider the availability and redundancy aspects. The implementation of **HSRP** for default gateway redundancy would be evaluated for its effectiveness in ensuring network uptime in case of router failures. The use of **LASP** for link aggregation would be examined for both its bandwidth enhancement and link redundancy capabilities. Finally, the security of the **NAS** device, if implemented, would be analyzed, including access controls, data encryption, and backup strategies.

The overall goal of the security analysis is to provide a comprehensive understanding of the network's security posture, identify areas for improvement, and ensure the confidentiality, integrity, and availability of the organization's IT assets.

**Chapter 8: Topology Diagrams**

This chapter outlines diagrams for better understanding.

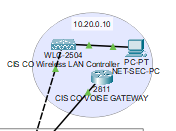
**Full Diagram**



**Lowest topology Diagram**

# 

**VoIP Diagram**



**Firewall Diagram**

# 

**Server Farm Diagram**

# 

**Core Switch Diagram**

# 

**Cloud cluster with remote system**

# 

# Chapter 9: Conclusion

# In conclusion, the described secure multinational IT company network design, leveraging technologies like firewalls, VPNs, VLANs, ACLs, SSH, HSRP, and LASP, aims to establish a robust and resilient infrastructure capable of supporting global operations while prioritizing security. The hierarchical topology, with a well-defined core, distribution, and access layers, provides scalability and manageability. The strategic implementation of a DMZ ensures secure exposure of public-facing services, while the segmentation achieved through VLANs and ACLs limits the potential impact of security breaches within the internal network.

# Secure remote management via SSH, coupled with redundant network paths provided by HSRP and aggregated links via LASP, enhances operational efficiency and network availability. The inclusion of inside servers for critical data and applications, along with essential services like DHCP and DNS, forms the backbone of internal operations.

# While the design incorporates numerous security considerations, ongoing vigilance, regular security audits, and adherence to best practices are crucial to maintaining a strong security posture and adapting to the evolving threat landscape in a globally interconnected world. The effectiveness of this design in a real-world scenario would depend on meticulous configuration, rigorous testing, and continuous monitoring.

# Ultimately, the architecture outlined represents a thoughtful approach to constructing a secure and scalable network foundation for a multinational IT enterprise. By strategically layering security controls at various levels – from perimeter firewalls and secure inter-office VPNs to internal VLAN segmentation and granular access controls – the design aims to minimize vulnerabilities and protect critical assets.

# The emphasis on redundancy and high availability through technologies like HSRP and LASP further underscores the commitment to ensuring business continuity across geographically diverse locations. While the logical design provides a strong framework, the true efficacy of this network hinges on diligent implementation, consistent enforcement of security policies, and proactive adaptation to emerging threats. Continuous monitoring, regular security assessments, and user education will be paramount in maintaining the integrity and resilience of this global network in the face of an ever-evolving cybersecurity landscape.

# Chapter 10: Bibliography

### Youtube

* + Cisco Packet Tracer Tutorials - Numerous creators on YouTube provided invaluable visual demonstrations and step-by-step guides for understanding and implementing various networking concepts and designs within the Cisco Packet Tracer environment..

### Stack overflow

* + [*https://stackoverflow.com/questions*](https://stackoverflow.com/questions)

The collaborative question-and-answer website served as a valuable resource for understanding specific networking concepts, troubleshooting potential configuration issues within Cisco Packet Tracer, and exploring diverse perspectives on network design and implementation through community-driven discussions and solutions.GTFOBins

### Deepak Sood

* + [www.youtube.com/@TECHGURUDEEPAKSOOD](http://www.youtube.com/@TECHGURUDEEPAKSOOD)

Their comprehensive explanations and tutorials on advanced networking topics, security principles, and practical applications significantly contributed to a deeper understanding of the underlying technologies and best practices incorporated in this network design..

### OpenAI

*https://www.openai.com*

OpenAI's large language model provided valuable assistance in generating detailed explanations of complex networking concepts, structuring the overall document, and refining the language for clarity and comprehensiveness.

### Mentors and family

### The expert guidance and insightful feedback from mentors, combined with the unwavering encouragement, understanding, and patience of family, were instrumental in the successful development and completion of this project.