Networking

A picture containing graphical user interface

Description automatically generated

Submitted By: Submitted To:

Student Name: **Amar Dagaura** Module Leader: **Mr. Manoj Tamang**

Coventry ID: **11780342** (Lecturer)

Module: ST5064CEM Networking

Contents

[Introduction 1](#_Toc124801042)

[Summary 1](#_Toc124801043)

[Objective 1](#_Toc124801044)

[Logical Design 2](#_Toc124801045)

[Physical Design 3](#_Toc124801046)

[Vlan Allocation in Network 4](#_Toc124801047)

[VLSM 4](#_Toc124801048)

[Subnetting https://www.fieldengineer.com/skills/subnetting 5](#_Toc124801049)

[Benefits of Subnetting https://www.fieldengineer.com/skills/subnetting 5](#_Toc124801050)

[Switch Virtual Interfaces (SVIs) 6](#_Toc124801051)

[Module Description 6](#_Toc124801052)

[Access Layer 6](#_Toc124801053)

[Distribution Layer 7](#_Toc124801054)

[Core Layer 7](#_Toc124801055)

[Edge Router 8](#_Toc124801056)

[Internet service provider 8](#_Toc124801057)

[Trucking 9](#_Toc124801058)

[Vlan 9](#_Toc124801059)

[Port Channel 10](#_Toc124801060)

[STP 11](#_Toc124801061)

[HSRP 12](#_Toc124801062)

[EIGRP Routing 12](#_Toc124801063)

[Default Static redistribute EIGRP 13](#_Toc124801064)

[OSPF Routing 14](#_Toc124801065)

[OSPF static Route 14](#_Toc124801066)

[BGP Routing 15](#_Toc124801067)

[NAT 15](#_Toc124801068)

[ACL 16](#_Toc124801069)

[VPN 16](#_Toc124801070)

[ICMP Ping with VPN (headquarter to branch pc) 18](#_Toc124801071)

[WLC (Wireless Access Point) 18](#_Toc124801072)

[DHCP SERVER 21](#_Toc124801073)

[Syslog Server 21](#_Toc124801074)

[AAA Server (Authorization, Authentication, Accounting) 22](#_Toc124801075)

[FTP server 24](#_Toc124801076)

[SMTP server 24](#_Toc124801077)

[SSH 25](#_Toc124801078)

[Telnet 26](#_Toc124801079)

[NTP server 26](#_Toc124801080)

[DHCP Snooping 27](#_Toc124801081)

[Port Security 28](#_Toc124801082)

[Port fast 28](#_Toc124801083)

[QOS 29](#_Toc124801084)

[User exec mode 29](#_Toc124801085)

[Risk Management 30](#_Toc124801086)

[Risk Management Structures 30](#_Toc124801087)

[**Response to Risks** 31](#_Toc124801088)

[**Importance of Risk Management** 31](#_Toc124801089)

[**Risk Analysis Process** 31](#_Toc124801090)

# Introduction

A Computers that are electronically linked together for the exchange of information are referred to as networks. Information that is frequently shared through networking includes resources like files, programs, and software. Given that it enables user collaboration across a large range, networking has several benefits that can be easily recognized in terms of security, efficacy, manageability, and cost effectiveness.

LAN networks are composed of a variety of computers connected to one another over a short distance, typically at homes, workplaces, or educational institutions. A network called a wide area network typically covers the entire world in addition to towns and countries.

# Summary

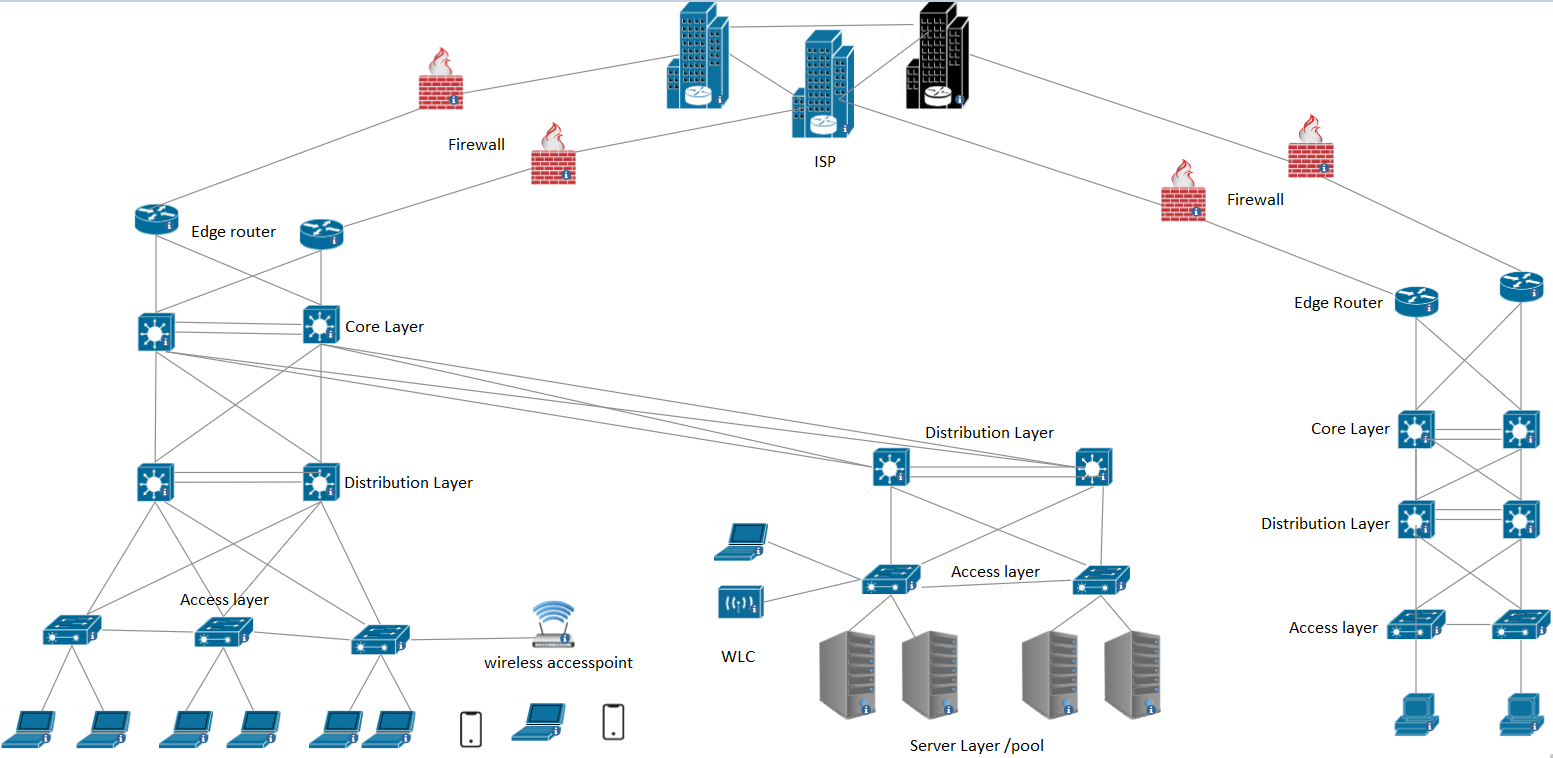
As a Layer 2 Network system admin used to design a complete managed network for Headquarter (KATHMANDU) and Branch (DHANGADHI)of “**Hats Private Limited.” Company.** An efficient network architecture is determined by a variety of elements. “The primary one is the needs of the client, which are surrounded by numerous technical and business objectives like scalability, security, management, availability, and cost. A service level or network performance requirement is another thing that many clients want to set. Given all the requirements and technical goals of Network Hats Private Limited, located at (Headquarter) and (Branch).”

# Objective

The main objective of this project is to create, set up, maintain, and enhance the Network Hats network.

* expanded network capability.
* little latency for users.
* a network infrastructure with a high throughput and redundancy.
* Determine the main weak points in the current network and offer solutions to fix them.
* Connection to the Internet and off-site branch that is secure and dependable.
* Through a centralized location, establish control over the network.
* users' ease of access.
* improved use of the network's resources.
* Evaluate the current network to find key sites of failure and make recommendations for how to fix the problem.
* Ensure a secure link to the Internet and distant branches.
* Implement a centralized strategy to consolidate network administration.

# Logical Design

The diagram below shows how the logical topology has been divided into different possible structures. Such as ISP, Edge layer, Core layer, distribution layer and Access layer. Also have included different devices like PCs, servers, wireless access point and wireless controller (WLC).

# Physical Design

**Map

Description automatically generated with low confidenceDiagram

Description automatically generated**The Cisco Packet Tracer is useful for these kinds of tasks. This program allows users to test out potential network setups in a simulated environment before committing to them in a more realistic one. (Cisco Packet Tracer version 8.2.2)

# Vlan Allocation in Network

Table

Description automatically generatedA Company network has a sizable broadcast domain. Switches flood the network with broadcast traffic, even inside distinct IP Subnets, which compromises security and performance. VLAN is employed in this project to divide several LAN-based networks.

The 802.1Q VLAN tagging standard is applied in this network. The native VLAN 80 will be applied to packets without any VLAN tags which is also called Native Vlan.

# VLSM

Table

Description automatically generated“VLSM standing for Variable Length Subnet Mask, occurs when subnet design uses multiple masks in the same network. It means that more than one mask is used for various subnets of a network. VLSM is equivalent to subnetting subnets, which means that VLSM enables network engineers to divide the IP address space into subnet hierarchies of different sizes.” So VLSM allows network engineers to create subnets with varying host counts with only small numbers of addresses being wasted.

It is also defined as a subnetting process for a subnet. Because subnets might vary in size, VLSM is employed to enhance their availability. It may also be described as a procedure for subnetting a subnet.

# Subnetting

The purpose of subnetting is to build a computer network that is quick, effective, and dependable. More effective pathways are required to carry the traffic across networks as they get bigger and more complicated. All network traffic would experience bottlenecks and congestion if it all took the same path at the same time, leading to slow and ineffective backlogs. It reduces the number of routers that network traffic must transit through by setting up a subnet.

Table

Description automatically generatedParent Network of Headquarter: 192.168.1.0/24 child network had taken from parent network for the HQ. Branch network had taken from parent network of 192.168.2.0/25 for creating a child network for branch.

# Benefits of Subnetting

* Subnetting splits broadcast domains to facilitate effective traffic routing, enhancing network efficiency and speed.
* Traffic is kept inside the specified network thanks to a subnet mask. As a result, there is less severe congestion, and the network is not put under as much stress. Data packets need to travel less distance when using sub-networks, which improves network speed.
* In large enterprises, effective organization is essential. Businesses can fully control their traffic, packet forwarding, network, and routers thanks to subnetting.

# Switch Virtual Interfaces (SVIs)

The parent network of headquarter is **192.168.1.0/24** and Branch Parent Network is **192.168.2.0/128.** I took all child network from parent networkwith the help of subnetting.

Table

Description automatically generated

# Module Description

Cisco Packet Tracer is used to design physical diagram. Packet tracer helps to configure well managed network diagram with implementing, simulating the network using the cisco packet tracer network simulation tool. The network basically based on 3-layer, Core layer, Distribution layer and Access layer.

# Access Layer

Packets are supplied to end user devices through the access layer, Due to its emphasis on tying client nodes to the network, this layer is also referred to as the desktop layer. The Data Link and Access layer of the reference model for OSI are equivalent to the Access Network layer of the TCP/IP paradigm. It specifies the hardware and protocols needed to link a host to a network. connection and transfer data across it. For delivery within the physical network, packets from the Internet layer are passed down to the Network Access layer. The networking edge, where information enters or departs the campus network, is represented by the access layer. An access layer switch's main duty has historically been to give users network access. Switches in the distribution layer, which handle routing, reliability of service, and security protocols, are connected to switches at the access layer.

Diagram

Description automatically generated

# 

# Distribution Layer

Diagram

Description automatically generatedMany crucial services are provided by the distribution layer, which serves as an interface between the access layer and the core layer. A link between the various access sites and the core layer as well as a dividing line between the access and core layers are represented by the distribution layer. Distribution layer connection is based on policy, and it controls department or workgroup access. For access devices, this layer offers redundant connections. Additionally, redundant connections provide you the chance to load-balance different devices. To enhance the performance of the routing protocol, the distribution layer might summarize routes from the access layer. In certain networks, the distribution layer only employs dynamic routing protocols while speaking with core routers and provides a default route to access-layer routers.

# Core Layer

The backbone of the network is the core layer. It links several network levels on campus. The core layer connects the campus to the rest of the network by acting as an aggregate for all other campus blocks. The core layer's main functions are to offer fault isolation and fast backbone connectivity. In the core layer EIGRP routing protocol is used for routing. all network layers relate to core layer.

##### Diagram Description automatically generated

# Edge Router

Diagram

Description automatically generatedThis router makes certain that its network's network is connected to other networks, a wide area network, or the Internet.

NAT, VPN, ACLs are applied in the edge router to make connection between branch and headquarter. Edger router works like a gateway for outbound and inbound. With the help of edger router connect branch with this headquarter. An edge router may offer connectivity with other networks and autonomous systems in place of offering connection with the internal network, which the core router already controls. The router applies labels to outgoing data by utilizing the data's metadata to decide which label should be applied.

# Internet service provider

Diagram

Description automatically generatedThere are different types of ISPs provide internet. Many companies are connected to the ISP for getting a public routing for communication, file sharing, data transferring.

# Trucking

A picture containing text

Description automatically generatedGraphical user interface, text, table

Description automatically generatedTrunk used to share Vlan information and Vlan. To transfer VLAN traffic from one switch to another, trunks are necessary. Switches communicate with one another about VLAN settings via the VLAN trucking protocol. The trucking link between the two switches utilizing the router allows the VLANs to interact with one another. The function of tunneling must be activated on both ends of a connection. For instance, if two switches are linked together, both switch ports must be set up for trucking and must use the same tagging scheme (ISL or 802.1Q).

# Vlan

Graphical user interface, table

Description automatically generatedA VLAN is a private network made up of many local area networks. Devices can be joined to form a single logical network if they are enabled on various networks. This combination produces a Virtual LAN that is managed similarly to a physical LAN as the result. Security risk reduction: When it comes to security risk reduction, VLAN does this by limiting the

number of hosts that can collect copies of frames that the switch can flood. Enhance security: You can maintain hosts that contain sensitive data on a different VLAN to enhance security. Change the network: You may easily change the network by setting a port into the appropriate VLAN.

# Port Channel

Text

Description automatically generated with medium confidenceA port channel is a logical interface that is created by combining many physical ports. For enhanced capacity and redundancy, a port channel can combine up to eight different active lines. Additionally, traffic across all these physical interfaces is load balanced via port channeling. As prolonged as at least one physical interface inside the port channel is active, the port channel remains in operation.

Text

Description automatically generated with low confidence

**VTP**

A picture containing table

Description automatically generatedBy default, every catalyst switch acts as a server. To spread VLAN information throughout a network or domain, a server is necessary. Any update that must be made throughout the domain is controlled by the VTP server. The whole VTP domain will be informed when a change is performed on the server. The NVRAM stores the settings for the VTP server. Although VTP client switches can transmit and receive updates like servers can, they are limited in their ability to establish, modify, and remove VLANs. To put it another way, none of the ports on the client switch may be added to a new VLAN without the server switch's consent or notice.

# 

# STP

Table

Description automatically generatedText

Description automatically generatedIn the case of an active link breakdown, the Spanning Tree Protocol enables network designers to preserve automated path redundancy while simultaneously avoiding bridge loops. When several computers in a network attempt to reply to a signal, bridge loops develop, which can overwhelm the network. Each incoming signal is routed to the machine that should receive it and act accordingly using STP. Rapid- pvst is faster than pvst mode.

# HSRP

Text

Description automatically generatedThe FHRP family of protocols includes the Hot Standby Router Protocol. It is a protocol that Cisco only uses. Only Cisco routers may use it. It enables one router to take over automatically if another fails. To put it another way, it offers a gateway router redundancy by immediately switching out a malfunctioning gateway router with one that is operational.

# 

# EIGRP Routing

Table

Description automatically generated with medium confidenceThis protocol is a development of the older IGRP Cisco protocol, which is now disregarded. Classless routing, VLSM, route summarization, incremental updates, load balancing, and many more practical characteristics are supported by EIGRP. Since EIGRP is a proprietary Cisco protocol, every router in a network running it must be a Cisco router.

Text

Description automatically generated

## Default Static redistribute EIGRP.

Text, letter

Description automatically generated

# OSPF Routing

Graphical user interface, text, table

Description automatically generatedText

Description automatically generatedA routing protocol that may be utilized for huge corporate networks is OSPF Open Shortest Path First. In internal networks of businesses, it is the routing protocol that is most frequently utilized. However, for effective routing in a big network, just employing OSPF is not enough. To design OSPF effectively, one must have a thorough understanding of how it operates.

## OSPF static Route

Graphical user interface, text

Description automatically generated

# BGP Routing

Text

Description automatically generatedThe Border Gateway Protocol (BGP) is essentially the Internet's global navigation system. It is a type of digital postal service that gives public Internet networks and autonomous systems (AS) the routing data they need to direct traffic to one another. The major issue is that although the Internet seems to be a single network and operates as such, it is made up of several administrative domains that coexist peacefully. The Internet wouldn't function without BGP. The global Internet routing table, or phone book for the Internet, is created and maintained using BGP. This basically functions as a route matrix that instructs edge routers in a particular AS how to transmit traffic to an IP address outside the home network. From here, the ideal path for traffic may be determined.

# NAT

The capacity to convert a private Internet Protocol (IP) address or a collection of IP addresses into a single, public IP address is known as network address translation (NAT). You may use this to conceal private Internet Protocol (IP) addresses, shielding them from IP scans, which are frequently conducted before assaults.

Text

Description automatically generated

Text

Description automatically generated

# ACL

Table, calendar

Description automatically generated with medium confidence At the router's interface, ACLs operate according to a set of rules that specify how to forward or block a packet. ACLs limit, block, or permit just the packets that are going from source to destination, acting as a stateless firewall. Using an ACL is primarily intended to secure your network. In the absence of it, any traffic is either let to enter or depart, leaving it more open to unwelcome and hazardous traffic. With an ACL, you may, for instance, give traffic flow control or disallow routing modifications to increase security.

# VPN

Your internet protocol (IP) address is hidden by a VPN, making it nearly impossible to track your online activities. Your internet behavior, including the links you click and the files you download, is concealed by a VPN so that cybercriminals, organizations, governmental bodies, or other snoops cannot see it.

Text

Description automatically generated

Text

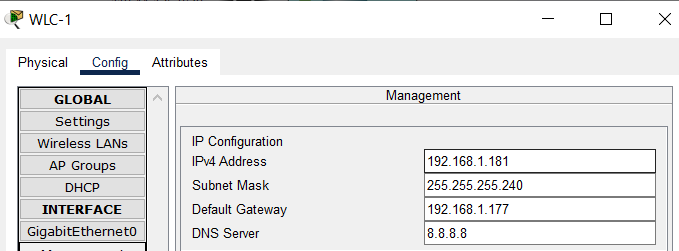
Description automatically generated with low confidence

# Graphical user interface Description automatically generatedICMP Ping with VPN (headquarter to branch pc)

# WLC (Wireless Access Point)

Due to the Internet's widespread use of wireless devices, most individuals now almost take wireless connection for granted everywhere. No matter the size or location of corporate wireless networks, the Cisco Wireless Controller (WLC) range of devices offers a unified approach to their configuration, management, and support. The last ten years have seen a huge increase in the use of Cisco WLCs as businesses switch from isolated Access Point (AP) deployment designs to a centralized controller-based design to take advantage of the increased capability and redundancy that come with controller-based designs.

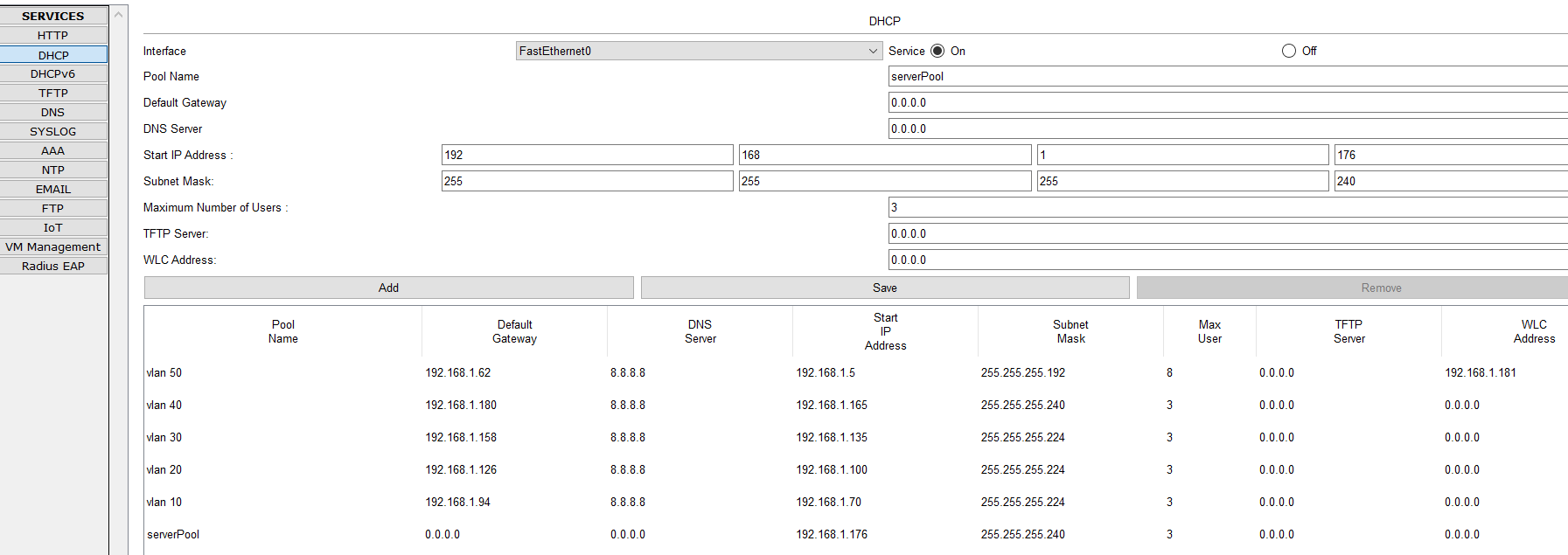
Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

# DHCP SERVER

A computer that assigns IP addresses to networked devices is known as a DHCP server. Devices that join to the network are given IP addresses automatically using this method. Typically, a range of IP addresses that are usable on the network are distributed by the DHCP server.

**Graphical user interface, text, application, email

Description automatically generated**

# Syslog Server

The Syslog protocol has been in use for many years and is used to send event messages between information systems and software programs. Due to the layered architecture of the Syslog protocol, any combination of transport protocols may be used to send Syslog messages. Additionally, it offers a message style that makes it possible to give vendor-specific extensions in an organized manner. The storage of log messages on a centralized server, which can offer a linked view of all the log data produced by various system components, is frequently encouraged by syslog best practices. Otherwise, manually connecting each related log message and examining each log file separately would take a very long time.

**A picture containing background pattern

Description automatically generated**

Graphical user interface, application

Description automatically generated

# AAA Server

An architecture that authenticates users, provides them permission, and keeps track of their activities is defined as AAA. Without AAA, the network design is "open," allowing anybody to access it and do anything they want without being tracked. Small firms frequently employ open network design, which allows for physical access management to offices. ISPs, whose access must be tightly managed and accounted for, are ill-suited to open network design.

**Text

Description automatically generated**A screenshot of a computer

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

# FTP server

Graphical user interface, text, application

Description automatically generatedFile Transfer Protocol is referred to as FTP. This is a network/communication protocol used on a TCP/IP" Transmission Control Protocol/Internet Protocol" network to transmit files between computers. You might need to enter a username and a password to access the server's files, depending on the sort of server you're using. Anonymous FTP refers to server connections that don't demand any type of authentication before granting access to the files.

Text

Description automatically generated

# SMTP server

Large-scale email transmission and reception are the sole functions of an SMTP server. SMTP servers can help in this situation You are unable to send emails to recipients if there is no SMTP server. The server also checks to see if the outgoing message is coming from an active email account. SMTP protocols make guarantee that the message is returned to the sender if the email cannot be delivered.

Graphical user interface, application

Description automatically generated

# 

# SSH

A network security protocol called Safe Shell (SSH) uses encryption and authentication techniques to achieve features like secure access and file transfer. Telnet and FTP are examples of traditional remote login or file transfer protocols that communicate data in cleartext, which has several security problems. These techniques are progressively losing favor as cyber security becomes more crucial.

In an unsecure network environment, SSH encrypts and authenticates network data to offer a secure login and other secure network services. The SSH protocol is supported by most devices and has become a popular alternative to Telnet and other insecure remote shell protocols.

A picture containing graphical user interface

Description automatically generated

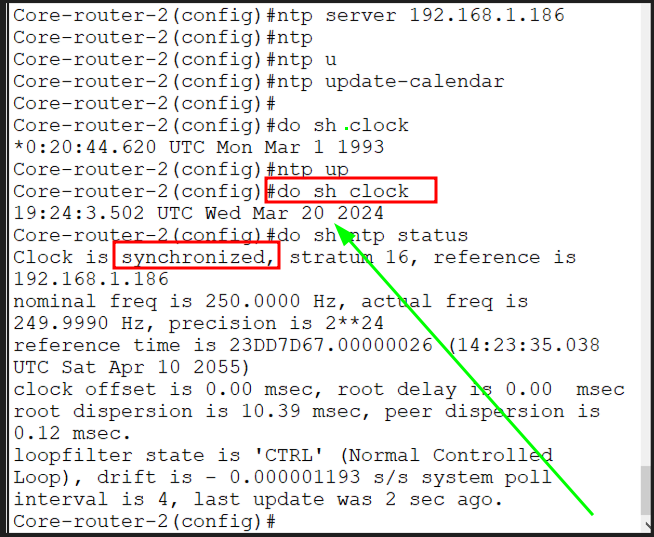
# Telnet

Text

Description automatically generatedA user can communicate with a distant device using the application protocol telnet. A user on a client computer can connect to the command-line interface of a distant system that is running a Telnet server program using a program known as a Telnet client. Network administrators frequently use Telnet to connect to and control distant devices. By telnetting to a distant device's IP address or hostname, a network administrator can connect to the device. After that, a virtual terminal that can communicate with the distant host will be shown to the network administrator.

# NTP server

NTP is a standard Internet protocol that was created by University of Delaware professor David L. Mills. The application on the NTP- Current Network Protocol server, which is running on any server or computer platform, is referred to as a "network time server" in general. This rule applies to network appliances (tray mount, rack, etc.), which obtain and use time from an outside source to keep time in sync with their internal clocks before supplying time to their associated networks. Utilizing NTP, or Network Time Protocol, is how this is accomplished.



# DHCP Snooping

Application

Description automatically generatedTo automatically configure IP addresses on networking devices, network administrators utilize DHCP. One of the most often used networking protocols is DHCP. DHCP is used by almost all current networks. It also experiences the most attacks from attackers because of its popularity. only available on switches, DHCP Snooping. This shows that DHCP snooping is only possible on switches. With other gear, such as servers and routers, it is incompatible. All switches, whether multilayer switches or layer 2 switches, normally allow DHCP snooping.

# Port Security

Text, table

Description automatically generatedAnother significant resource that may be utilized to compromise security is a port. Physical ports (physical docking places where users may attach additional devices to their computers) and logical ports are the two categories into which ports are divided (well-programmed docking points through which data flows over the internet). The secret to security and its effects is a logical port.

# Port fast

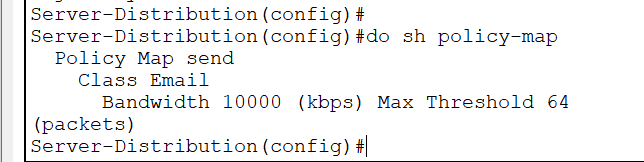
When an end user PC is plugged into an access port of a switch, it takes around 52 seconds (in the normal setup) for the port to become operational while the port switches between STP port states (from blocking to forwarding). The switch port is completely unavailable for data forwarding at this period. Cisco developed a method to skip the port's listening and learning phases and put it immediately in the forwarding state. Topology Change Notification (TCN) BPDU is never transmitted for port up/down events, which is another feature of Port Fast. When several end-user workstations are starting up or shutting down simultaneously in a big network, the benefit is a streamlined TCN transfer.

Text

Description automatically generated

# QOS

Regardless of network capacity, telecom operators may guarantee networks, apps, and services are highly performant thanks to the tools and technology known as quality of service (QoS). QoS solutions make ensuring that high-priority networks and services function as intended and transmission stays rapid by providing network administrators with visibility into crucial indicators and enabling them to distribute bandwidth to mission-critical applications as traffic ebbs and flows.



# 

# User exec mode

Graphical user interface, text, email

Description automatically generatedGraphical user interface, text, application

Description automatically generatedThe first mode a user can access after login into the router is User Mode. The prompt that appears after the router's name indicates that it is in user mode. In this mode, the user is only able to issue the most fundamental instructions, such those that display the system's status. From this state, the router cannot be configured or restarted.

# Risk Management

The detection, analysis, and reaction to risk elements that are inherent in a business's operations are all included in risk management. Effective risk management is acting proactively rather than reactively to influence future events as much as feasible. As a result, good risk management can lessen both the likelihood of a risk happening and its possible consequences.

# Risk ManagementRisk Management Structures

Structures for risk management are intended to do more than merely identify current hazards. The uncertainties should be calculated and their impact on a firm should be predicted via a sound risk management framework. The outcome is a decision between taking risks or rejecting them. The risk tolerance thresholds that a firm has already established for itself determine whether risks are accepted or rejected.

They consist of budgeting, cost management, planning, and organizing. Because the emphasis is on proactive risk management in such a scenario, the company often does not encounter many shocks.

**Response to Risks**

One of the following is typically used as a response to risks:

• **Avoidance:** A company tries to remove a specific risk by eliminating its root cause.

• **Acceptance:** A company could have to take a risk in some circumstances. If a company entity creates contingencies to lessen the impact of the risk, should it materialize, then this alternative is viable.

A company must adopt a problem-solving strategy while developing contingencies. The result is a thorough strategy that may be carried out as soon as the situation calls for it. Because it can manage risks as they materialize, such a strategy will help a corporate organization to tackle obstacles or blockages to its success.

**Importance of Risk Management**

Because it equips a company with the tools it needs to effectively identify and manage possible hazards, risk management is a crucial activity. When a danger is recognized, it is simple to minimize it. Additionally, risk management gives a corporation a foundation on which to make wise decisions.

The greatest method for a firm to be ready for events that can impede progress and growth is to identify and manage risks. A company's chances of success increase when it assesses its strategy for dealing with possible challenges and then creates structures to meet them.

Progressive risk management also makes ensuring that issues with a high priority are handled as aggressively as feasible. Additionally, the management will be armed with the data they need to decide wisely and maintain the company's profitability.

**Risk Analysis Process**

To identify and rank risks for the goal of analyzing and addressing them, risk analysis is a qualitative method to problem-solving. The risk analysis procedure is as follows:

**1. Identify existing risks**

Brainstorming is the primary method for identifying risks. To assess all the many risk sources, a company gathers its staff in one place. The following step is to rank all of the detected hazards according to importance. Prioritization makes sure that the risks that can have a substantial impact on a business are dealt with more immediately because it is impossible to reduce all current hazards.

**2. Assess the risks**

Finding an acceptable remedy comes first, followed by recognizing the issue in many situations. Prior to determining the best way to manage risks, a company should identify their root causes by asking, "What generated such a risk and how may it effect the business?"

**3. Develop an appropriate response**

When a corporate entity decides to evaluate potential solutions to reduce recognized risks and avoid their recurrence, it must consider the following: What steps can be made to stop the danger that has been identified from happening again? What should you do in addition if it does happen again?

**4. Develop preventive mechanisms for identified risks**. The strategies can be implemented if hazards arise.

**Conclusion**

Now that we've covered some of the most important TCP/IP and network building blocks, you have the foundational knowledge needed to look at the more pressing security concerns in a converged context. Understanding the construction of networks helps you identify the physical or logical vulnerabilities that are exposed when one network design is chosen over another. Understanding the formation of packets will help you to better grasp how they may be built or altered to serve a particular function. You can better predict what could happen to packets as they go from source to destination if you understand how packets are transported and delivered. To recognize, comprehend, and address vulnerabilities in a converged network, it's essential to have a solid understanding of networking fundamentals and TCP/IP**.**

**Reference**

Cisco Wireless. (n.d.). Retrieved January 16, 2023, from <https://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/>

Cisco Wireless. (n.d.). Retrieved January 16, 2023, from <https://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/>

*Network Address Translation (NAT)*. GeeksforGeeks. (2021, December 13). Retrieved January 16, 2023, from <https://www.geeksforgeeks.org/network-address-translation-nat/>

Cisco Wireless. (n.d.). Retrieved January 16, 2023, from <https://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/>

Written by Steve Symanovich for NortonLifeLock. (n.d.). *What is a VPN?* Norton. Retrieved January 16, 2023, from [https://us.norton.com/blog/privacy/what-is-a-vpn#](https://us.norton.com/blog/privacy/what-is-a-vpn)

*CISCO CCNA - Port Fast & Bpdu Guard*. CertificationKits.com. (n.d.). Retrieved January 16, 2023, from <https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-switching/cisco-ccna-port-fast-a-bpdu-guard/>

Cisco Wireless. (n.d.). Retrieved January 16, 2023, from <https://www.firewall.cx/cisco-technical-knowledgebase/cisco-wireless/>

<https://www.quora.com/What-is-core-layer-network-technologies>

<https://www.easytechjunkie.com/what-is-an-edge-router.htm>

<https://www.thewindowsclub.com/what-is-vlan-why-do-we-use-vlans>

<https://www.orbit-computer-solutions.com/vtp-modes-of-operation/>