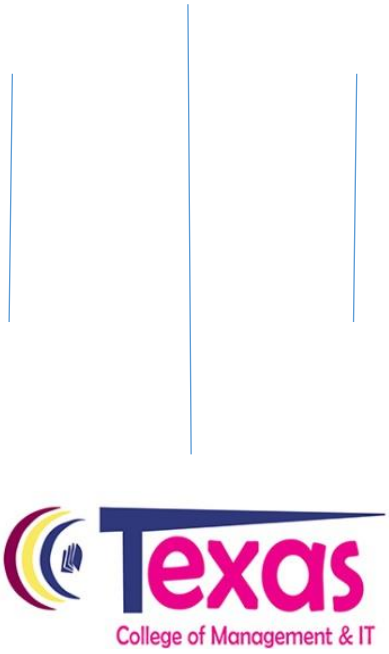
Enterprise Network Design and Implementation of Hierarchical Network to Ensure Scalability

ALINA SHRESTHA

TEXAS COLLEGE OF MANAGEMENT & IT



DEPARTMENT OF CYBER SECURITY AND NETWORK TECHNOLOGY

LINCOLN UNIVERSITY COLLEGE

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I express my heartfelt gratitude and regards to the respected person for the success of this project. This project had taught me a lot regarding my subject matter. The completion of this project required a lot of guidance and assistance from many individuals and I am extremely fortunate to have gotten this all along the completion of this project. I would like to extend my sincere thanks and gratitude to our respected Supervisor, Mr. Bigyan Mainali and Head of Department, Mr. Suman Thapaliya (Department of Computer Science) for his valuable suggestions, guidance, encouragement, and inspirations that assisted me in completing this work. His useful recommendations and co-operative behavior are acknowledged.

Finally, I would also like to express our sincere thanks to all our friends who helped us directly or indirectly during this project and especial thanks to supervisor and college for accepting my project.

ABSTRACT

As a business grows, so do its networking requirements. Enterprise networks are important, with size and complexity. Enterprise network infrastructure provides the communications path and services between users, processes, applications, services, and external networks. They are both local and wide area in scope.

Enterprise Network Design and Implementation of Hierarchical Network to Ensure Scalability is a research project that aims to show how it can handle key areas of enterprise network design mainly: virtual local area networks (VLAN), routing, switching and server network. The main goal of the project is to design a hierarchical enterprise network for businesses or organizations where principles such as modularity, resiliency and flexibility are applied. Real-time simulations and testing of the proposed network will be achieved through Cisco Packet Tracer.

As businesses grow and evolve, they hire more employees, open branch offices, and expand into global markets. These changes directly affect the requirements of a network which must be able to scale to meet the needs of business. These challenges have exposed the limitations of the existing ad hoc approach to network design and management. Hence, the design and implementation scheme has been proposed realizing the limitations of current enterprise infrastructure in context of Nepal.

Keywords: Enterprise network, hierarchical design, multi-layering, routing, switching,

VLAN, trunking

CHAPTER 1: INTRODUCTION

Computer networking is the most crucial part because this technology takes the most important responsibilities, rather than people doing the tasks as in previous decades. They connect people, support applications and services, and provide access to the resources that keep the businesses running.

An enterprise network is the backbone for facilitating an organization's communications and connecting computers and devices throughout departments. An enterprise network consists of a group of local area networks (LANs) interconnected using wide area networks (WANs). Typically, each constituent network is designed, provisioned, and optimized for its own purpose and business objectives. An enterprise network contains a number of internetworking devices (e.g., switches, routers, gateways, etc.) and is under the control of one big organization. It is an enterprise's relay backbone that helps connect computers and related devices across departments and workgroup networks, facilitating insight and data accessibility. An enterprise network reduces communication protocols, facilitating system and device interoperability, as well as improved internal and external enterprise data management. These networks are configured to connect a limited number of authorized systems, apps, and individuals which also helps to enable a secure and efficient communication channel to perform specific business operations.

Enterprise networks can have thousands of hosts and hundreds of networking devices which are interconnected by copper, fiber-optic, and wireless technologies. All Internet traffic flows through the enterprise edge, making security considerations necessary. Routers and switches provide connectivity, security, and redundancy while controlling broadcasts and failure domains. Network infrastructure diagrams, or topology diagrams, keep track of the location, function, and status of devices representing either the physical or logical network. A physical topology map uses icons to document the location of hosts, networking devices, and media. It is important to maintain and update physical topology maps to aid future installation and troubleshooting efforts. A logical topology map groups hosts by network usage, regardless of physical location. Host names, addresses, group information, and applications can be recorded on the logical topology map. Connection between multiple sites might be shown but do not represent actual physical locations.

Enterprise network construction necessitates the massive use of information and network technologies, computers, Internet, e-commence, and enterprise application management software in market for finished products. The aim of such construction is to raise operating efficiency of enterprises, enhance management, and lower capital expenditure as part of their drive to become modern and competitive. Thus, basic network infrastructure represents the first step towards the construction drive.

BACKGROUND

Networking is particularly important part in every sector of today's world. It provides a lot of benefit such as file or resource sharing, flexibility and boosting of storage capacity by connecting all computers. Network departments are connected, and vast amounts of data are transferred between them every day. Networks today are needed to deliver secure, measurable, and guaranteed services.

This project mainly focuses on Enterprise Network Design and Implementation of Hierarchical Network to Ensure Scalability. It describes how an advanced network can overcome the limitation of traditional network. The main purpose of an enterprise network is to reduce isolated users and workgroups. Hierarchical networks are among the easiest to design and implement as equipment and cables generally follow the logical structure of an organization. Hierarchical network topologies adapt well to business expansion, traffic shaping and network security models by segregating a LAN (Local Area Network) into logical parts that correspond to needs of the organization. All systems should be capable of communicate and supply desired information. Additionally, physical systems and devices should be able to keep and supply satisfactory performance, reliability, and security. Enterprise computing models are developed for this purpose, easing the exploration and improvement of established enterprise communication protocols and strategies. An enterprise network can integrate all systems, including Windows and Apple computers and operating systems (OS), Unix systems, mainframes and related devices like smartphones and tablets. A tightly integrated enterprise network effectively combines and uses different device and system communication protocols. Enterprise network hold number of sites and support thousands of users. A well-managed network allows users to work reliably. The enterprise network can have thousands of hosts and hundreds of networking devices which is often designed to provide dedicated interconnection with partners, home-based workers, and other support resources.

PROBLEM STATEMENT

In today’s world computer has become an integral part of every sector for professional activities not only for professional activities but for personal activities also. As technologies have evolved

networking came into the picture and slowly from initial wired network technology, we moved to this wireless network technology. Starting from day to the end of the day everyone uses Internet for their work and this internet is nothing but vast network that connects computers all over the world. So, networking has become a key factor in every sector.

Back then, if people wanted to connect LANs that were not in the same location, they used point-to-point leased lines. These were typically DS0 (56 Kbps) connections, and then the more expensive T1/E1 or T3/E3 connections. The connections were first done using remote bridges at each end, and later with devices called routers, popularized by the company example Cisco.

At the beginning of the 1990s, Frame Relay service was introduced. Frame Relay service offered much lower monthly WAN (Wide Area Network) costs, far fewer physical connections to manage, allowed the expensive last-mile link bandwidth to be shared (and thus used more efficiently) across multiple remote connections, and required less expensive router hardware than the point-to-point alternative. Multiprotocol Label Switching (MPLS) is the successor to Frame Relay.

Then the Broadband Internet connections – ADSL and cable modem – came along beginning in the late 1990s to enable nearly universal high-speed Internet access, at much lower cost than T1-based access. As a result of the continuing increase in bandwidth available with these technologies, and more recently with 4G/LTE as well, most home users and many mobile users have higher-speed Internet access at their homes than the workers at smaller sites in most enterprises.

Managing a computer is not so difficult but managing an entire enterprise is a challenging task. System management includes a variety of functions for managing computers in a networked environment, including software distribution, version control, backup and recovery, printer spooling, job scheduling, virus protection and performance and capacity planning. Storage management is important as: firstly, there is an ever-increasing demand for storage due to the Internet, document management and data warehousing as well as increasing daily transaction volume in growing companies. Secondly, finding the time window in a 24/7 operation to copy huge databases for backup, archiving and disaster recovery has become more difficult. As all these managements need to be taken care of while building an enterprise network. Every node in a network needs to be looked after so that improper use of resources is forbidden and all computers get equal access in all areas and of course, adding ‘new’ sections of infrastructure need to meet the exact same specifications as the existing parts. That means the same bandwidth and reliability, latency and ease of use. Before the advancement in technology, Quality of Service (QoS) was not looked upon deeply but today QoS is one major factor in networking. QoS helps to meet the traffic requirements of sensitive applications, such as real-time voice and video, and to prevent the degradation of quality caused by packet loss, delay and jitter.

The major challenge today is to build an enterprise network so that the network is divided into hierarchical order of three layers: Core, Distribution and Access. Routing, switching, server network and security are other factors needed to build any network. The only way to face this

challenge is to build a proper enterprise network which includes of all necessary components used in networking and fulfilling all the criteria needed for the network.

Aim And Objectives

Today's world is about connecting people, systems and sharing data everywhere at any time. As organizations interconnected, these isolated LANs and their functions grew from file and print services to include critical applications; the critical nature and complexity of the networks also grew. It is aimed to propose an architecture for handling network requirements of an enterprise.

The primary focus is to design a computer network that can overcome geographical barriers through a robust WAN infrastructure. It also aims to design a network that can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users. That's network must be scalable. This can be instrumental for enterprises looking to connect wide number of their branches over many locations. This project aims to increase the use of systematic design for implementing a hierarchical and layered architecture. Well-organized design of a computer network will eventually lead to quicker implementation and fewer problems during network management. Utilizing concepts of hierarchical design will help towards scaling it use for the future. Network scalability will ensure that you can meet the increased demands.

To provide a framework for defining an enterprise network there are some project goals that need to be achieved. So, the major objectives of the project are as follows:

1. Design an enterprise level network architecture

2. Establish a streamlined network management methodology

3. Setup WAN architecture for bridging branches with geographical gap

4. Provide high bandwidth, congestion control and quality of service

5. Distribute network loads via redundancy and layers

6. Reliably deliver applications and provide reasonable response times from one

host to any host

7. Demonstrate scalability of the architecture for network growth and business

change

SCOPE

Every business wants to grow with time. If a business enterprise is to expand it must adopt a sustainable and a scalable network that allows its stakeholders a platform on which they can communicate. Thus, building a robust network for enterprise use is one of the best ways in which they can foster. Enterprise networks can manage to put down the barriers between information held on several systems of the network.

1. Eliminate isolated users and workgroups
2. Communicate and provide and retrieve information to all the computers in the network
3. Provide satisfactory performance, reliability and security
4. Facilitating the exploration and improvement of established enterprise communication protocols and strategies
5. Effectively combines and uses different device and system communication protocols
6. Allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources
7. Cost reduction by downsizing to microcomputer-based networks instead of using mainframes
8. Greater flexibility because of possibility to connect devices from various vendors

CHAPTER 2: LITERATURE REVIEW

INTRODUCTION

Routing And Switching in the Enterprise

A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router. It is a Layer 3 function that allows Internet Protocol (IP) packets to traverse multiple networks. Routers are used in homes and offices for setting up local network connections. More powerful routers operate all over the Internet, helping data packets reach their destinations.

Routing is essential to a network. When routing does not scale, there is a direct impact on the stability and performance of a network. Routers carry out two basic functions—they select a path between networks, and they securely transmit information packets across that path toward an intended destination. In so doing, they draw on routing protocols and algorithms. These algorithms are designed to plot routes using such criteria as throughput, delay, simplicity, low overhead, reliability/stability, and flexibility. When a packet is received at a router, the router opens it, looks at the network destination address, and then calculates the next hop in the best, or

lowest-cost, route to the destination. A hop is measured by the passage of a packet through a router. Routers play a critical role in networking by interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols.

In its objectives routers are classified the following way:

Core routers used by Internet Service Providers (ISPs) are the fastest and most powerful, sitting at the center of the internet and forwarding information along the main fiber optic backbone. Enterprise routers connect large organizations' networks to these core routers.

An edge router, also known as an access router, is a lower-capacity device that resides at the boundary of a LAN and connects it to the public internet or a private wide area network (WAN) and/or external local area network (LAN). Home and small office routers are considered subscriber edge routers.

Branch routers link an organization's remote office locations to its WAN, connecting to the primary campus network's edge routers. Branch routers often provide additional features, like time-division multiplexing, wireless LAN management capabilities and WAN application acceleration.

A logical router is a configured partition of a traditional network hardware, or physical, router. It replicates the hardware's functionality, creating multiple routing domains within a single router. Logical routers perform a subset of the tasks that can be handled by the physical router, and each can contain multiple routing instances and routing tables.

A wireless router works in the same way as the router in a hard-wired home or business local area network (LAN), but allows greater mobility for notebook or portable computers. Wireless routers use the 802.11g specification, a standard that offers transmission over short distances.

Switching is known as a process to forward packets coming in from one port to a port leading towards the destination. In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching had historically been a fairly simple process, which allowed bridges to outperform routers of the same era. After the MAC address table was built, a simple filtering and forwarding process was all that was needed.

Although all three layers of the hierarchical design model contain switches and routers, the access layer generally has more switches. The main function of switches is to connect hosts such as end-user workstations, servers, IP phones, web cameras, access points, and routers [20]. This means

that there are many more switches in an organization than routers. Switches come in many form factors:

1. Small standalone models sit on a desk or mount on a wall.
2. Integrated routers include a switch built into the chassis that is rack mounted.
3. High-end switches mount into a rack and are often a chassis-and-blade design to allow more blades to be added as the number of user's increases

High-end enterprise and service provider switches support ports of varying speeds, from 100 MB to 10 GB. An enterprise switch in an MDF connects other switches from IDFs using Gigabit fiber or copper cable. An IDF switch typically needs both RJ-45 Fast Ethernet ports for device connectivity and at least one Gigabit Ethernet port (copper or fiber) to uplink to the MDF switch. Some high-end switches have modular ports that can be changed if needed. For example, it might be necessary to switch from multimode fiber to single-mode fiber, which would require a different port. Port density on a switch is an important factor. In an enterprise environment where hundreds or thousands of users need switch connections, a switch with a 1RU height and 48 ports has a higher port density than a 1RU 24-port switch.

VLAN

VLAN is a custom network which is created from one or more local area networks. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN. VLANs can spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN. A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch.

Virtual Local Area Networks (VLANs) are extensively used in enterprise networks and are often used to ease management of hosts spread over physically disparate locations. Managing VLANs is one of the unique challenges facing network operators of today's enterprise networks. There exist industry standards like Cisco's VLAN Trunking Protocol to better manage VLANs, but are very limited in functionality. In this demonstration, we present the design of Virtual MAN, a VLAN visualization and management system for enterprise networks that can assist network operators in managing VLANs and in identifying misconfigurations. It can create more flexible network designs that group users by department instead of by physical location. The major benefits of using VLAN in enterprise networks include Flexible Network Partition and Configuration, Performance Improvement, Cost Savings.

Function of VLAN:

- Enhance LAN security. Layer 2 frames between VLANs are isolated. That is, users of a VLAN cannot communicate with users of a different VLAN. If users of different VLANs need to communicate with each other, Layer 3 devices, such as routers or Layer 3 switches, are required.
- VLANs reduce the incidence of collisions and decrease the number of network resources wasted by acting as LAN segments.
- VLAN offers flexible networking models, which groups different users based on their departments (i.e., their jobs and functions), rather than just physical locations of that network.

Techniques to Configure VLAN in Enterprise Network

1. Port Based VLAN

With port-based VLANs, the ports of a switch are simply assigned to VLANs, with no extra criteria. All devices connected to a given port automatically become members of the VLAN to which that port was assigned. In this case, the VLAN has a set of physical ports with one or more routers. Each router may have a VLAN, but a VLAN usually has several switches. Some port-based VLAN cannot include a physical segment.

2. MAC Based VLAN

The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. The MAC to VLAN configurations is shared across all ports of the device. The location of the VLAN stations can vary, because the MAC addresses are in the Network Interface Card (NIC).

3. Layer-3 Based VLAN

It is very important to emphasize that layer-3 based VLAN can use the switches to connect the users. The primary benefit of using a Layer 3-based VLAN is that users can physically move their workstations to any network jack without the workstation's network address being reconfigured.

4. Policy Based VLAN

Policy-based VLAN assignment allows plug-and-play of user terminals and provides secure data isolation for terminal users. The switch provides policy-based VLAN assignment based on just MAC and IP addresses or based on both MAC and IP addresses and interfaces. The switch that has policy-based VLAN assignment enabled processes only untagged frames, and treat tagged frames in the same manner as VLANs configured based on ports. When receiving an untagged frame, the switch determines the VLAN according to the policy matching both MAC and IP addresses of the frame, and transmits the frame in the VLAN.

PROTOCOLS

EIGRP (Enhanced Interior Gateway Routing Protocol):

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network. Uses of EIGRP protocol in Enterprise network helps in scalability of routing protocol that ensures when network grow larger.

BGP (Border Gateway Protocol):

The Border Gateway Protocol is the routing protocol for the Internet. The BGP protocol specifies a TCP-based communications method for establishing routed peering between Autonomous System (AS) border routers (ASBRs), that facilitate the exchange of information about routable IP prefixes. BGP peering exist between all active Internet Autonomous Systems.

BGP is a path vector protocol, and BGP-enabled ASBRs send path vector messages to each other with lists of Internet-routable IP prefixes along with an Autonomous System (AS) path—the list of ASNs that must be traversed to reach that prefix. When there are multiple paths to a destination, BGP has the ability to rank all the paths from most preferred to least preferred according to the information collected by an organization's routing policy, which is based on metrics like load, delay, reliability, cost, etc.

STP (Spanning Tree Protocol):

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches that provides path redundancy while preventing loops in the network. Spanning trees use an algorithm to search for the redundant links in the LAN and select the best paths. It is mainly used to put all links in either forwarding or blocking. After this process, all the links without a redundant link is likely to be in the forwarding state. The redundant links that were not as good as the selected links would be blocking. Spanning Tree never uses multiple links to the same destination. The reliability (fault tolerance) of the network is increase exponentially by the introduction of redundancy. The Spanning-Tree Protocol is used to create a loop-free logical topology from a physical topology that has loops.

VTP (VLAN Trunking Protocol):

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share

the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. The VLAN Trunking Protocol offers the benefit of maintaining configuration consistency throughout the whole network. VTP lowers the possible inconsistencies in configuration that normally come about once modifications are made in a network. Such inconsistencies may lead to security violations since VLANs have the capability of cross connecting when matching names are utilized.

Virtualization and Rise of Enterprise Networks

Enterprise network infrastructure has profoundly impacted information systems business world. Demands on enterprise networks continue to surge, a trend characterized by the increasing expectations of end users and the growth of devices and business applications. With network virtualization, IT organizations are acquiring the means to adapt to changing demands and align their networking capabilities with their virtualized storage and compute resources.

As new technologies have evolved, enterprise systems have moved from initial proof-of-concept deployment to full-scale, global production deployment. Virtualization technology enables enterprise systems to improve server utilization. Virtualization makes provisioning network resources easier and more efficient. Networking software programs allow administrators to monitor the infrastructure, make changes to the network, provision resources, roll out updates to networking devices, and take action against detected security threats. The virtualized and software-based version of the network is an overlay on top of the physical network infrastructure. The physical network's devices like switches and routers still perform tasks like packet forwarding, while how to forward those packets is handled by the software running on the switches and routers.

Today every industry is being reshaped by technology. This digital transformation can lower IT costs and improve efficiency, visibility, and performance while driving business innovation. Major benefits of virtualization include the speed and ease of scaling network resources, updating policies, and centralized control. Another operational benefit is that a software-based network infrastructure makes scaling instances of VMs or containers easier and faster when resource demand increases. The network administrators also gain visibility, which improves an organization's network security posture because security software can see more of the network and report on vulnerabilities and security events. However, having more visibility means more information. Automated monitoring software is almost a necessity for network administrators to make sense of all that network data. Such software will condense the data and present it in a digestible way that's easier to manage. Major challenges of virtualization include potentially shifting cost to a managed service provider and the increased amount of network data.

CHAPTER 3: SYSTEM REQUIREMENT AND DEVELPOMENT

The minimum system requirements of the project are as follows:

Requirement Specification

Platform	Cisco Packet Tracer
Operating System	Windows 10
Processor	I3 or above
RAM	2GB or above
Disk space	2GB or above

TOOL REQUIRED:

Cisco Packet Tracer:

Cisco Packet Tracer is one of the most useful visual simulation programs for networking. This tool provides a network simulation to practice simple and complex networks. Cisco Packet Tracer has two workspaces—logical and physical. The logical workspace allows users to build logical network topologies by placing, connecting, and clustering virtual network devices. The physical workspace provides a graphical physical dimension of the logical network, giving a sense of scale and placement in how network devices such as routers, switches, and hosts would look in a real environment. The physical view also provides geographic representations of networks, including multiple cities, buildings, and wiring closets. It allows individuals to experiment with network behavior. It provides simulation, visualization, authoring, assessment and collaboration capabilities. The simulation-based environment helps users in decision making, creative and critical thinking. Key features of this tool are as follows:

1. Two workspaces: logical and physical
2. Two operating modes: real-time and simulation
3. Modular devices
4. Multiuser functionality
5. Help and support forums

System Analysis

System analysis is a detailed study of various operations performed by a design. It is a process of collecting and analyzing facts to find its aims and problem-solving technique that improves the system and ensures that all the components of the system work efficiently to carry out their purpose. That is a structural process related to four significant phases. They are study phase, design phase, development phase and implementation phase. A good analysis is essential for the development of a modern design.

There are various designs available for the enterprise network. The proposed design is intended to work across every enterprise with scalability, availability, rapid convergence and operational considerations. Design and development of networks that can be effectively used for wide range of applications are still challenging research problems because of the complexity involved. However, recent advances in network technologies have successfully addressed many of the complications hindering the wide deployment of hierarchical networks. So, designing and deploying such networks and effectively model them using simulation models is still an interesting topic in the area.

Network Design

Hierarchical Network Design

According to Lewis (2012), in order for the network to fully meet the needs of the enterprise, it needs to be designed in accordance with the three-level hierarchical model of network design. Such a network is easy to manage and can be scalable if necessary, and also provides the ability to quickly detect problems and problems.

Hierarchical Network Design model is the three-tier model. The design is divided into three layers i.e., Core Layer, Distribution Layer and Access Layer. Each layer has its own goals and functions. This assists in making the network scalable, stable, and deterministic.

The core layer is the backbone of the network. It interconnects all the distribution blocks. The core layer has a single purpose, and does not need many features. There are no security policies, no QoS, and no endpoints attached. The key design principles of the core layer are that it must be fast, it must be always available, and it must be reliable. It is critical that there is no single point of failure. If there is a failure, recovery must be as fast as possible.

The distribution layer is a multi-purpose layer. In particular, it needs to aggregate access layer traffic, and forward it to the rest of the network. There are likely many access layer switches in the network. Each of these switches has uplinks to the distribution layer switches. Many end devices across access layer switches are aggregated at the distribution layer. The distribution layer ensures about the packet that is properly routed towards the subnet and the VLANs in enterprise network. It provides intelligent routing, switching and network access policy function.

The access layer is the edge of the network where host devices connect. This includes workstations, and printers. Devices that extend the network, such as Phones, and Access Points, also attach here. The access layer ensures that packets are delivered to end user devices.

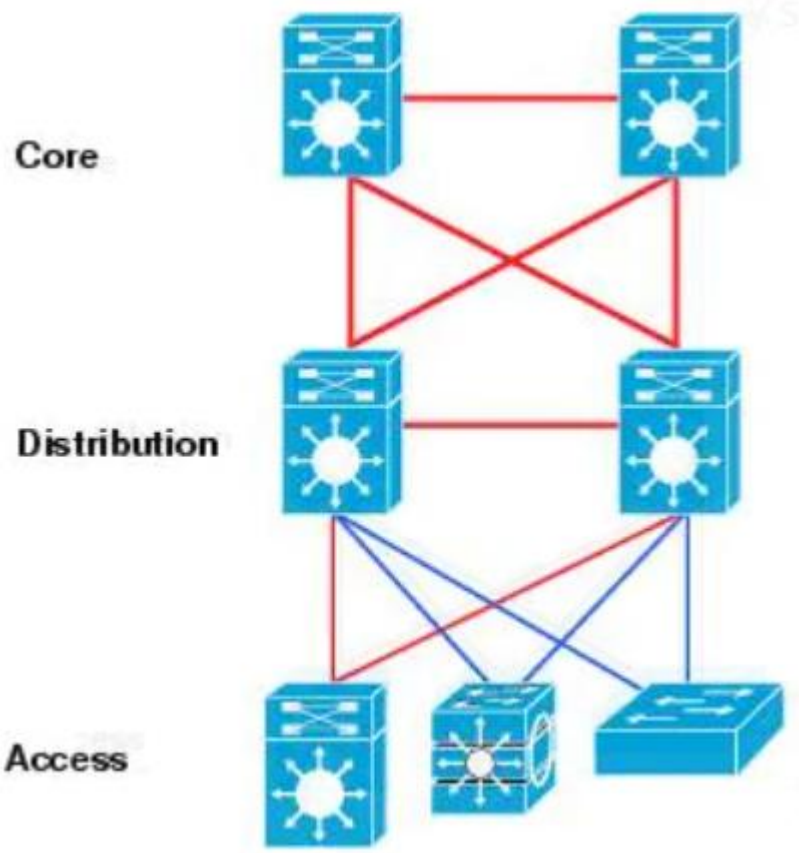


Figure 1: Hierarchical network design

Architecture for Multi-building and Collapsed Scenarios

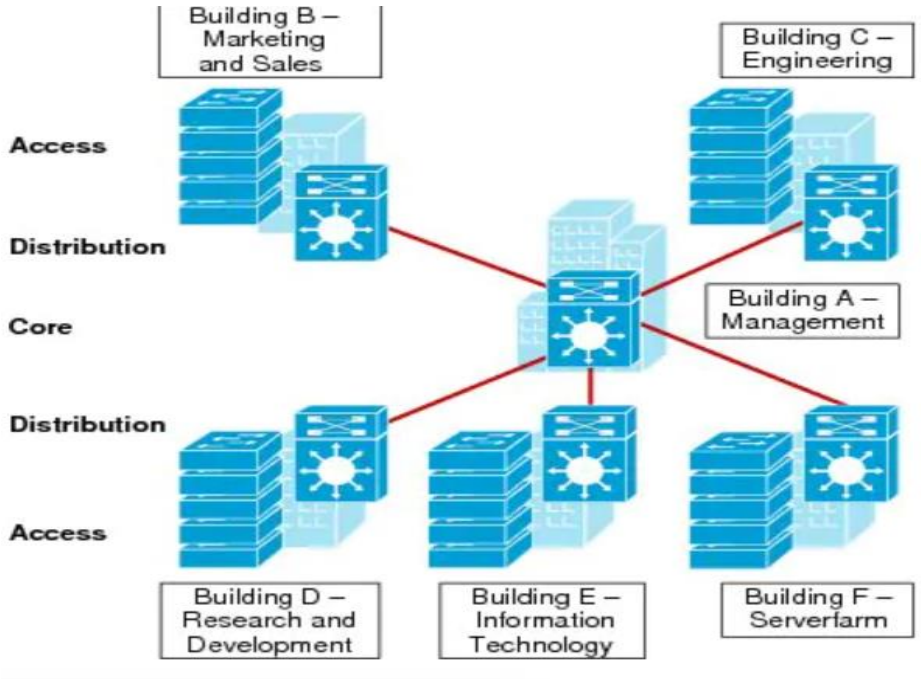


Figure 2: Multi-building enterprise network design

Figure 2 shows a three-tier enterprise network design for organizations where the access, distribution, and core are each separate layers. To build a simplified, scalable, cost-effective, and efficient physical cable layout design, it is recommended to build an extended-star physical network topology from a centralized building location to all other buildings on the same campus.

The figure above depicts an enterprise network that spans across multiple buildings. Having a dedicated core layer allows to accommodate growth without compromising the design of the distribution blocks, the data center, and the rest of the network. This is particularly important as the size of the campus grows either in number of distribution blocks, geographical area or complexity. Campus Networks and Wide Area Networks (WAN) are two types of networks, which allow sharing of networked resources between buildings or remote locations.

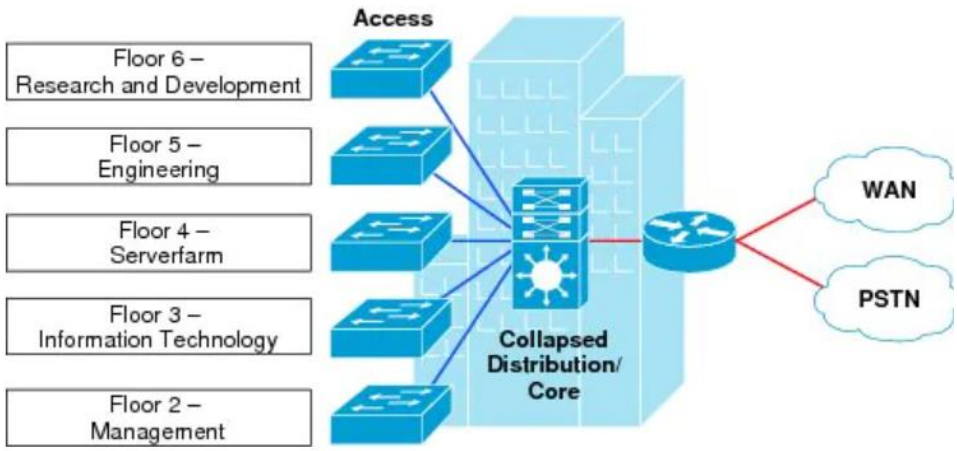


Figure 3: Collapsed core enterprise network design

In some cases, because of a lack of physical or network scalability restrictions, maintaining a separate distribution and core layer is not required. In smaller campus locations where there are fewer users accessing the network or in campus sites consisting of a single building, separate core and distribution layers may not be needed. This design model, illustrated in Figure 3, is more suitable for small to medium-size campus networks (ideally not more than three functional disruption blocks to be interconnected), where the core and distribution functions can be combined into one layer, also known as collapsed core-distribution architecture. The three-tier model is necessary for complex campuses that require access by multiple sites, devices and users. It results in a network that is scalable, cost-efficient and reliable for large enterprises. However, smaller campuses can reap similar benefits with a simpler model, scaled down to improve costs and oversight.

Network Control Services and Trust Boundary

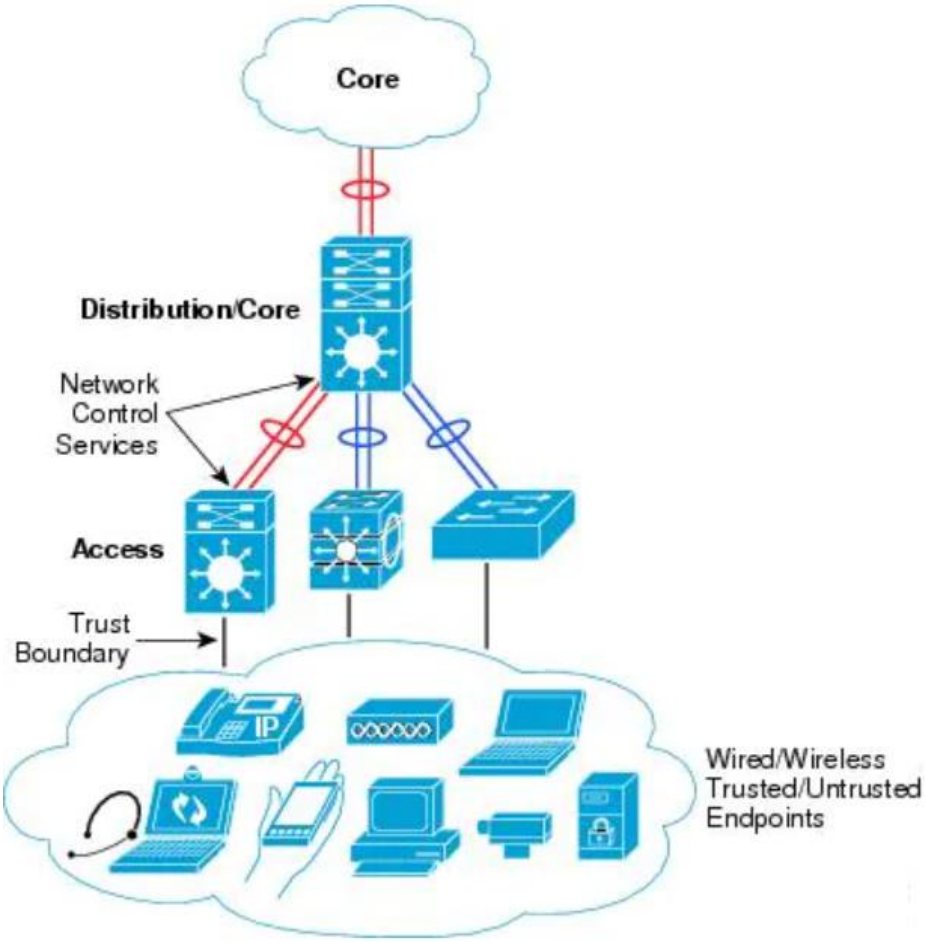


Figure 4: Access layer trust boundary and network control services

The access layer provides the intelligent demarcation between the network infrastructure and the computing devices that use the infrastructure. A flexible network design, and the demand for mobility are two requirements which drive the access layer design. A flexible network design allows any legitimate device to be connected anywhere in the network (e.g., IP Phone, printer, video surveillance camera, digital signage, etc.). Network users expect to be able to move around their devices (laptops, PDAs, printers, etc.) and gain network access wherever necessary. In order to allow devices to be moved within the network and ensure they associate with the correct network policies and services.

Access-layer Services and Capabilities

Service Requirements	Service Features
Discovery and Configuration Services	802.1AF, CDP, LLDP, LLDP-MED
Integrated Security Services	IBNS (802.1X), CISF - Port-Security, DHCP Snooping, DAI and IPSG
Network Identity and Access	802.1X, MAB, Web-Auth
Application Recognition Services	QoS marking, policing, queueing, deep packet inspection NBAR
Intelligent Network Control Services	PVST+, Rapid PVST+, EIGRP, OSPF, DTP, PAgP/LACP, UDLD, FlexLink, Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, Port Security, RootGuard
Energy Efficient Services	Power over Ethernet, EnergyWise, Energy efficient systems
Management Services	Auto-SmartPort Macro, Cisco Network Assistant

Multi-Layer and Routed-Access Network Design

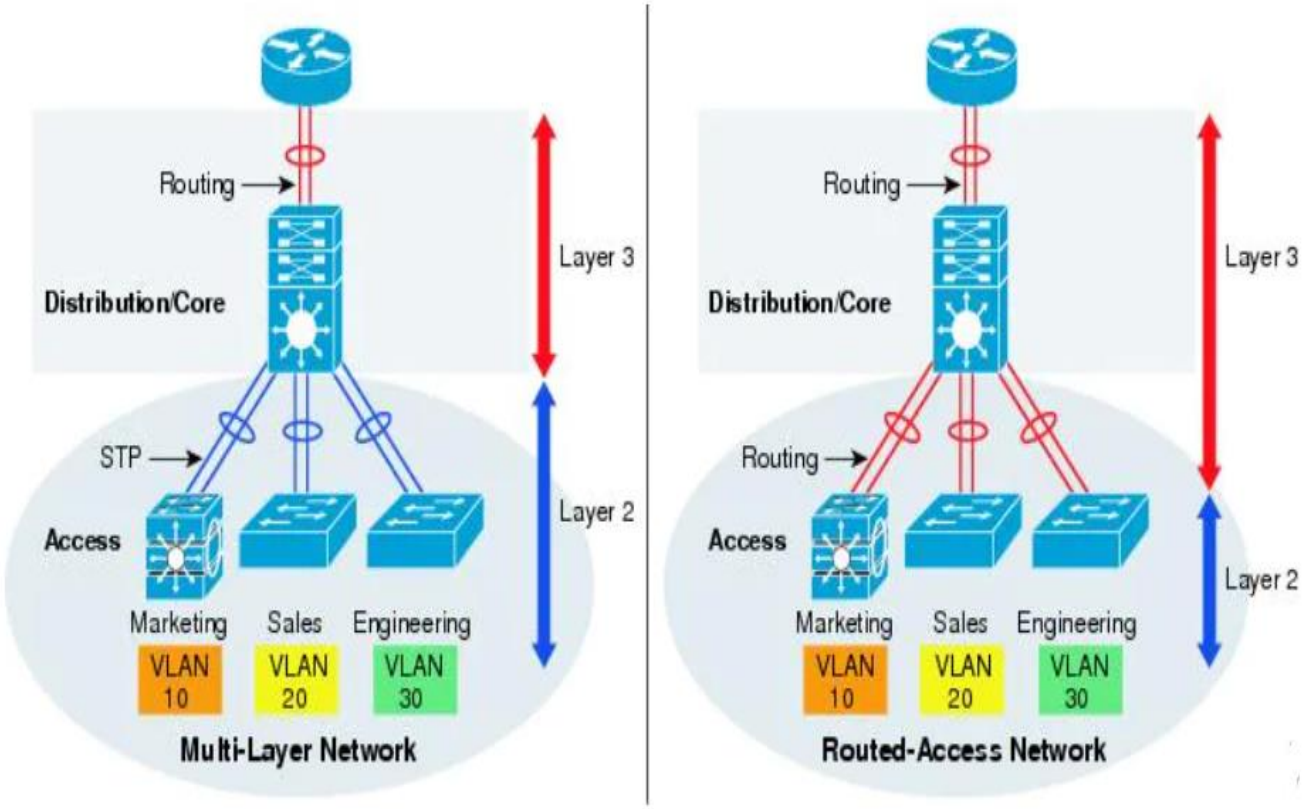


Figure 5: Control function in multi-layer and routed-access network design

Routing in the access-layer simplifies configuration, optimizes distribution performance, and improves end-to-end troubleshooting tools. Implementing routing in the access-layer replaces Layer-2 trunk configuration with single point-to-point Layer-3 interface in distribution layer. Placing Layer-3 function one tier down on access-switches, changes the multilayer network topology and forwarding path. Implementing Layer-3 function in the access-switch does not require a physical or logical link reconfiguration; the same EtherChannel in access-distribution block can be used. At the network edge, Layer-3 access-switches provides an IP gateway and become the Layer-2 demarcation point to locally connected endpoints that could be logically segmented into multiple VLANs.

Quality of Service

Quality of service (QoS) is the use of mechanisms or technologies to control traffic and ensure the performance of critical applications. It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications. QoS is typically applied to networks that carry traffic for resource-intensive systems.

Using QoS in networking, organizations have the ability to optimize the performance of multiple applications on their network and gain visibility into the bit rate, delay, jitter, and packet rate of their network. This ensures they can engineer the traffic on their network and change the way that packets are routed to the internet or other networks to avoid transmission delay. This also ensures that the organization achieves the expected service quality for applications and delivers expected user experiences.

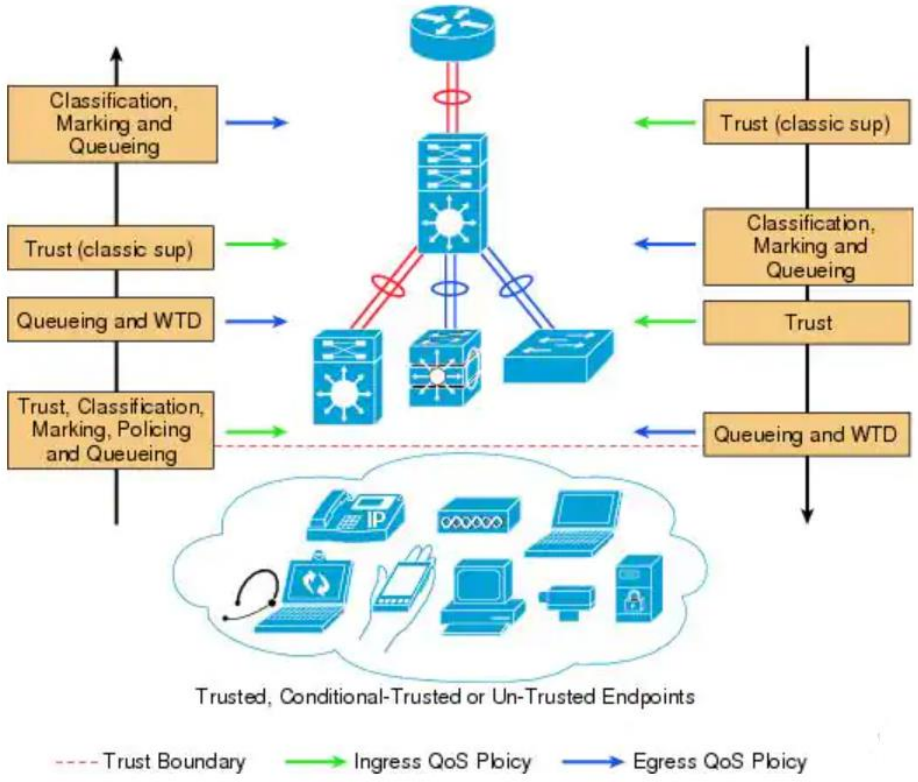


Figure 6: Enterprise network QoS framework

QoS needs to be designed and implemented considering the entire network. This includes defining trust points, and determining which policies to enforce at each device within the network. Figure 6 depicts QoS trust model that guides QoS policy implementation in the main and remote site networks. The devices (routers, switches) within the internal network are managed by the system administrator, and hence are classified as trusted devices.

Access-layer switches communicate with devices that are beyond the network boundary and within the internal network domain. QoS trust boundary at the access-layer communicates with various devices that could be deployed in different trust models (Trusted, Conditional-Trusted, or Un-Trusted). The QoS function is unidirectional. It provides flexibility to set different QoS polices for traffic entering the network versus traffic that is exiting the network. The access-switch provides the entry point to the network for end devices. The access- switch must decide whether to accept the QoS markings from each endpoint, or whether to change them. This is determined by the QoS policies, and the trust model with which the endpoint is deployed. End devices are classified into one of three different trust models, each with its own unique security and QoS policies to access the network:

- Untrusted—An unmanaged device that does not pass through the network security policies. For example, employee-owned PC or network printer. Packets with 802.1p or DSCP marking set by untrusted endpoints are reset to default by the access-layer switch at the edge. Otherwise, it is possible for an unsecured user to take away network bandwidth that may impact network availability and security for other users.

- Trusted—Devices that passes through network access security policies and are managed by network administrator. For example, secure PC or IP endpoints (i.e., servers, cameras, DMP, wireless access points, VoIP/video conferencing gateways, etc.). Even when these devices are network administrator maintained and secured, QoS policies must still be enforced to classify traffic and assign it to the appropriate queue to provide bandwidth assurance and proper treatment during network congestion.

- Conditionally-Trusted—A single physical connection with one trusted endpoint and an indirect untrusted endpoint must be deployed as conditionally-trusted model. The trusted endpoints are still managed by the network administrator, but it is possible that the untrusted user behind the endpoint may or may not be secure.

Enterprise Network Design

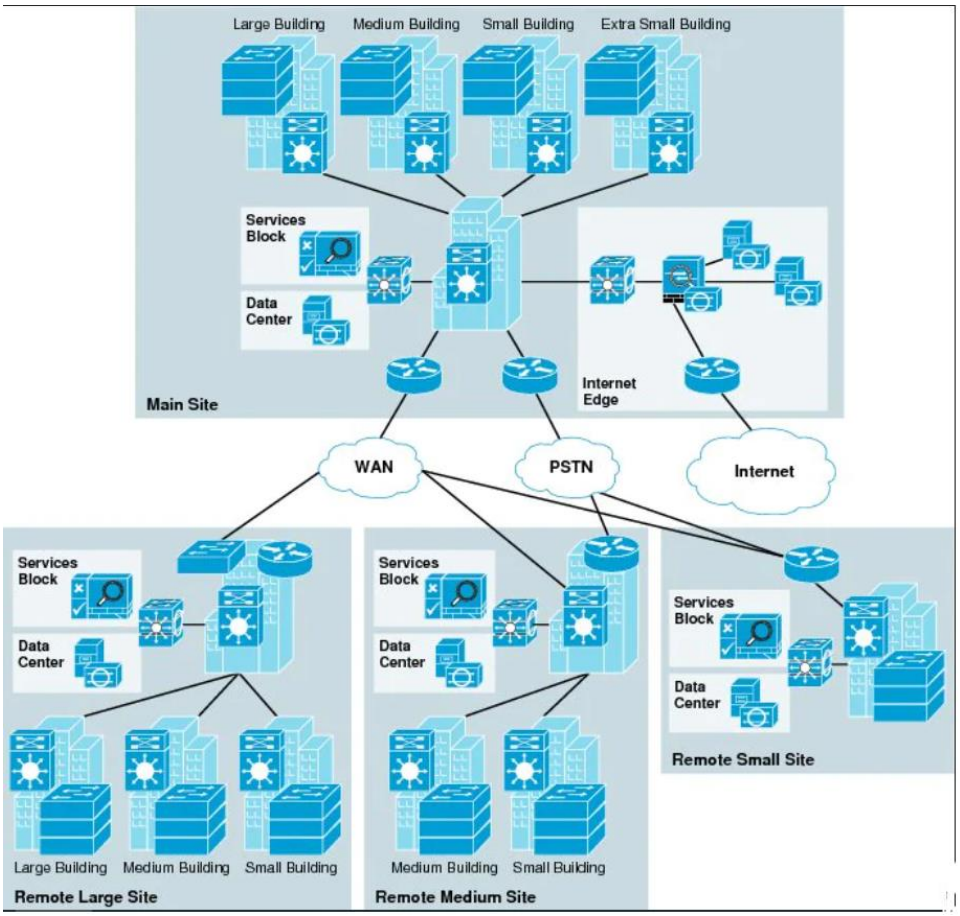


Figure 7: Enterprise network design profile

Figure 7 denotes design used for an enterprise network. It is intended to represent as many enterprise network environments as possible. To accomplish this, a modular design is used representing sites of varying sizes. The profile is built upon a network foundation consisting of a

main site, where the majority of the critical applications reside. Connected through a Metro Ethernet WAN are remote sites of varying sizes. Each site can coexist in a small enterprise network or can be treated as separate modules. The design for remote sites of varying sizes provides flexibility, modularity, and scalability as the enterprise grows.

Suggested Network Design

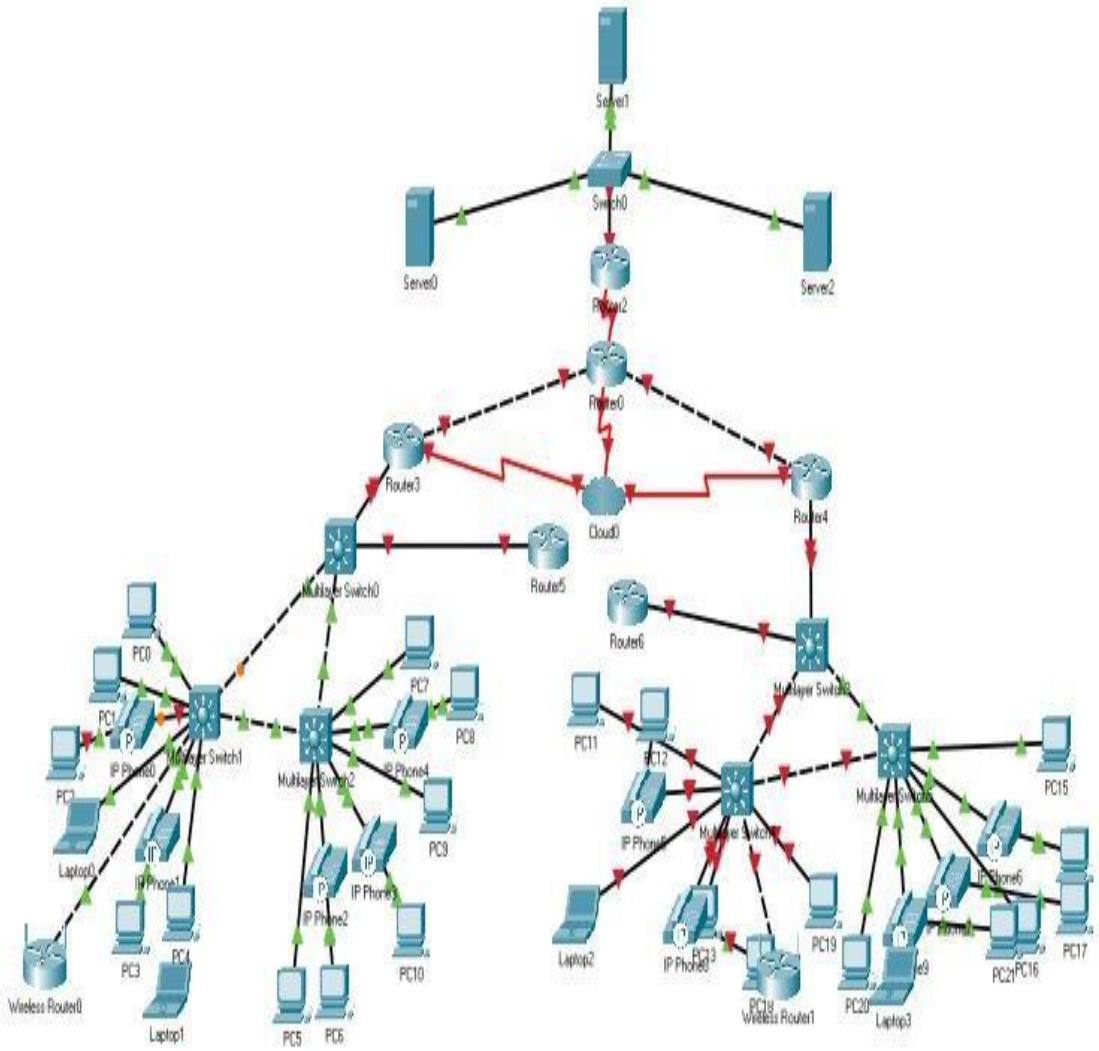


Figure 8: The proposed network design topology.

The network design goal in this phase is to develop a systematic approach that takes into consideration the needs, goals, policies, and procedures; the technical

goals and constraints; and the existing and future network infrastructure. This includes physical models, logical models, and functional models.

CHAPTER 4: Testing

Testing is an important part of network design and deployment. It is carried to explore the network functionality or to identify problems. It is usually performed before deployment so as to minimize the risks of real-world errors and problems. This ensures implementation of the network to be smooth. Network testing in Packet Tracer is achieved through ping, access of services like web or email, end-to-end connection through IP telephones and simulation through simple or complex PDU.

Test Cases

CHAPTER 5: RESULT ANALYSIS

CHAPTER 6: CONCLUSION, LIMITATION AND FUTURE ENHANCEMENT