Project report on

"Basic Network Design and Simulation Using Cisco Packet Tracer"

Basic Computer Networking

(2nd Batch)

Submitted to

Md. Rashid Al Asif

Assistant Professor

Dept. of Computer Science & Engineering

University of Barishal

Submitted by

Name : Sayma Jahan

St. ID : 02-002-23

Department : Economics

"Basic Network Design and Simulation Using Cisco Packet Tracer"

Abstract: The network framework presented in this paper is intended to provide effective communication, security, and scalability in a small to medium-sized office setting. The network is comprised of a 2960-24TT switch to distribute traffic to individual access points across departments and a central Main Router (1941 Router) for external access and inter-departmental routing. In the 192.168.1.0/24 network, each department (Office, Library, Accounts, Finance) is given a unique range of IP addresses, offering logical segmentation for better security and traffic control. Access Control Lists (ACLs) on the router and WPA2/WPA3 encryption on access points are examples of security techniques that limit access between departments. With plans to develop the network as the company does, the design guarantees scalability and flexibility for future expansion. This method provides a strong, trustworthy network foundation while balancing simplicity and security.

Introduction: Networking is the practice of connecting computers and other devices to share data, resources, and services. At its core, networking involves the transfer of information between devices over a variety of mediums, including cables, wireless connections, and the internet. At the heart of networking, devices such as computers, routers, switches, and access points communicate by following protocols like TCP/IP and HTTP. Every device on a network has a unique IP address, allowing it to be identified and located. Networks can vary in size, from small local area networks (LANs) within a home or office to wide area networks (WANs) that span larger distances, like the internet. The structure of a network is known as its topology, which could be something like a star or bus layout. Security is also a key part of networking, with tools like firewalls, encryption, and VPNs used to protect data and ensure safe communication. In essence, networking allows devices to work together, communicate, and share resources efficiently. Understanding the basics of networking is essential for anyone working with technology, as it forms the backbone of communication in today's digital world.

The foundation of contemporary communication systems is networking, which permits data transfer between devices via local, regional, and international networks. Network design, management, and troubleshooting all require a basic understanding of networking fundamentals. Virtual Local Area Networks (VLANs), Quality of Service (QoS) methods like DSCP, dynamic routing protocols like RIP, and static routing are some of the fundamental networking components.

Static routing is a straightforward routing technique in which a router's routes are manually specified. Static routing is better suited for smaller or simpler networks since it gives greater control over routing choices than dynamic routing, which automatically adjusts to changes in the network structure.

One of the earliest dynamic routing systems for figuring out the optimal path for data packets is the Routing Information Protocol (RIP). Hop count is the statistic employed by RIP, which is still utilized for teaching purposes and in smaller or more straightforward networks despite being less effective in bigger networks.

A marking system called Differentiated Services Code Point (DSCP) is used to categorize and control network traffic. In order to prioritize more important data (like speech or video) over less urgent traffic (like email or file downloads), network devices can use it to determine the kind of traffic and apply policies for priority handling. Consistent network performance is maintained by this QoS method.
A physical network can be conceptually divided into several separate networks using virtual local area networks, or VLANs. Grouping devices according to their function, even if they are not physically situated together, improves security, optimizes network traffic, and makes management easier.
These elements work together to assist network managers in maintaining strong network performance, optimizing network efficiency, and effectively managing traffic, all of which contribute to seamless communication across different systems and applications.

Related Work: The area of basic networking encompasses a wide range of ideas, tools, and procedures that are necessary for computer network construction, administration, and troubleshooting. Research papers, industry standards, and textbooks have all extensively addressed the study and use of networking principles. Network segmentation, routing mechanisms, basic networking models, and performance optimization strategies are all covered in the relevant work in this field. Here, we give a summary of the relevant research in each of these fields.

1. **Models and Protocols for Networking**
   Two essential frameworks for comprehending the interactions between networking protocols are the TCP/IP Model and the OSI Model (Open Systems Interconnection). Network operations (including physical transmission, routing, and application data exchange) are logically organized through the division of the network communication process into seven layers by the OSI model. Internet communication protocols are based on the TCP/IP architecture, which simplifies these tasks into four levels. Both models are essential to scholarly discourse and serve as the basis for networking certifications like CompTIA Network.

2. **Protocols and Routing Mechanisms**
   A crucial component of networking is routing, which is the process of choosing routes for data transfer between networks. Usually utilized in smaller or more regulated contexts, static routing entails manually configuring routing tables. By exchanging routing information, dynamic routing protocols like EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), and RIP (Routing Information Protocol) dynamically adapt to changes in the network. In particular, RIP employs hop count as its statistic and is frequently covered in beginning networking courses. Research articles that examine subjects like routing optimization and the adaptation of routing protocols to large-scale networks go into great detail into the development of these protocols.

3. Quality of Service (QoS) and Traffic Management

Managing network traffic effectively is vital for ensuring performance, particularly in networks handling voice, video, and other time-sensitive applications. Differentiated Services Code Point **(**DSCP**)** is a widely used QoS mechanism that marks packets to indicate their level of service priority. Researchers and industry leaders, including those from Cisco, have provided a deep analysis of traffic management strategies, QoS policies, and DSCP's role in managing network congestion and optimizing real-time traffic. These concepts are particularly emphasized in large-scale networks to ensure minimal packet loss and delay.

4. Network Segmentation and VLANs

Virtual Local Area Networks (VLANs) are essential for network segmentation, enabling the creation of logically separated networks within a physical network infrastructure. VLANs improve security, optimize traffic flow, and reduce broadcast domains. This concept is central to network design and has been widely discussed in academic literature, particularly in the context of enterprise networks. Furthermore, the configuration and management of VLANs have been explored in various Cisco white papers and online courses, which delve into the practical aspects of VLAN implementation in both small and large networks.

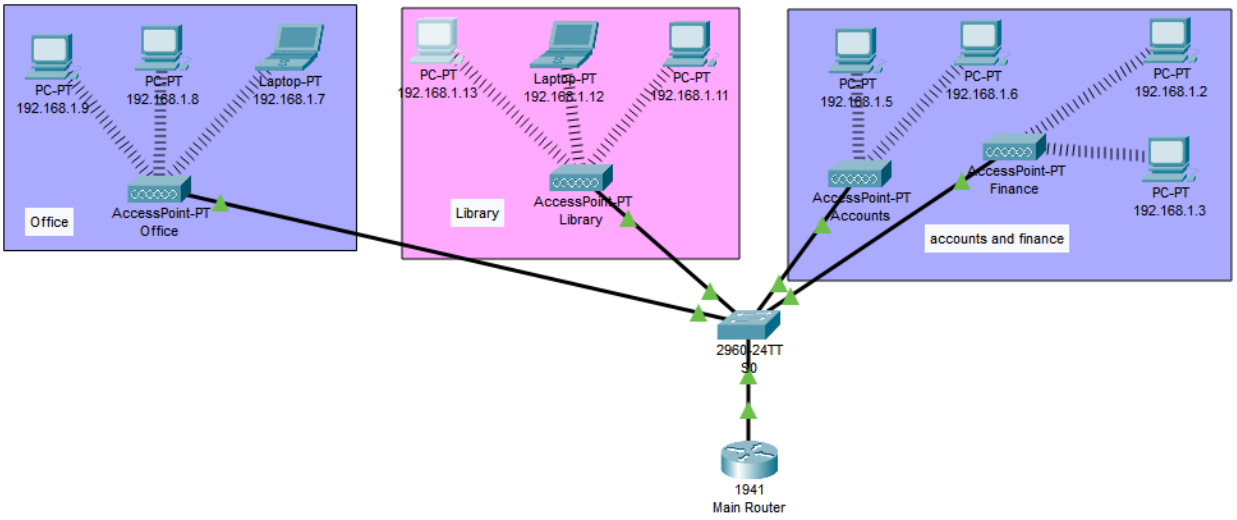
5. Security of Networks

In networking, security refers to making sure that resources and data are shielded against assaults and unwanted access. Research articles and textbooks usually discuss common security protocols like IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), and 802.1X for network access control. To safeguard network infrastructure, a large body of research focuses on securing routing protocols, controlling VLAN access, and putting strong authentication procedures in place.

6. New Technologies in Networking

New ideas like Software-Defined Networking (SDN) and Network Function Virtualization (NFV) have been brought about by the quick development of networking technology. Network administrators may now dynamically regulate network behavior thanks to these technologies, which also make network administration more flexible and scalable. Research in this field looks at how these developments can be combined with conventional network configurations (such VLANs and QoS settings) to increase network flexibility and efficiency in cloud-based settings.

System Design: The network design for a small to medium-sized office is depicted in the diagram below, with a central main router and a 2960-24TT switch connecting several departments. Using a uniform 192.168.1.0/24 addressing scheme, each department (Office, Library, Accounts, and Finance) has its own access point that grants department devices network access.



This image depicts a network system design with different departments connected through a central router and access points. Here's a detailed system design based on the diagram

Network Architecture:

Main Router**:**
Network Address: 192.168.1.0

Gigabit Ethernet 0/0:

IP Address: 192.168.1.0

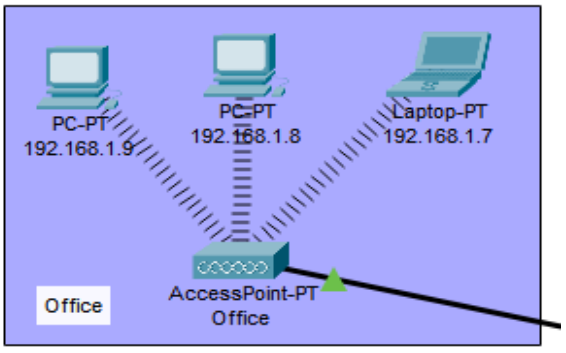
Subnet Mask: 255.255.255.0

Serial 0/1/0:

IP Address: 11.0.0.2

Subnet Mask: 255.255.255.0

Office:



IP Addresses:

Laptop- 192.168.1.7

PC- 192.168.1.8

PC- 192.168.1.9

Subnet Mask- 255.255.255.0

Library:

IP Addresses:

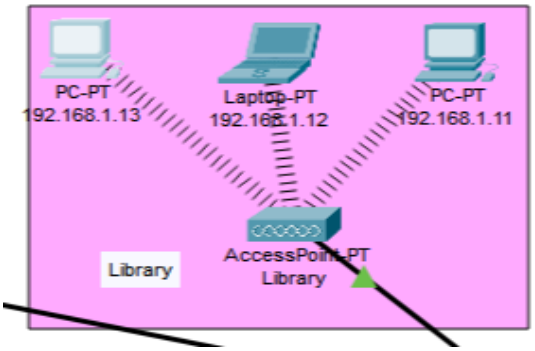
Laptop- 192.168.1.10

Laptop- 192.168.1.12

PC- 192.168.1.11

PC- 192.168.1.13

Subnet Mask- 255.255.255.0



Accounts:

IP Addresses:

PC- 192.168.1.5

PC- 192.168.1.6

Subnet Mask- 255.255.255.0

Finance:

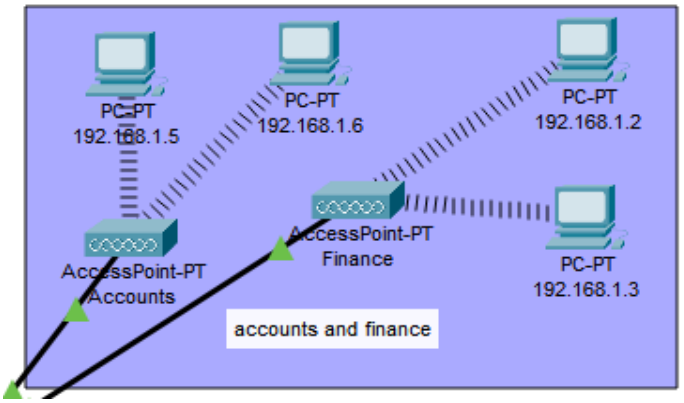
IP Addresses:

PC- 192.168.1.2

PC- 192.168.1.3

Laptop- 192.168.1.4

Subnet Mask- 255.255.255.0



Wireless Access Points:

SSID	**Password**
1) Office	1234567890
2) Library	1234567890
3) Accounts	1234567890
4) Finance	1234567890

This design ensures efficient communication, security, and control within a small to medium-sized network.

Result and Discussion:

Routing Analysis:

- Analyze the advantages and disadvantages of using static routing.

Advantages of Static Routing:

1) **Simplicity:**

Static routing is straightforward and easy to configure. It's a simple and direct way to specify how traffic should flow.

2) **Predictability:**

Since routes are manually configured, network administrators have full control and predictability over the routing table. This can simplify troubleshooting.

3) **Resource Efficiency:**

Static routes use fewer network resources compared to dynamic routing protocols as they don't involve continuous communication or exchange of routing information.

4) **Security:**

Static routes can enhance security by reducing the attack surface. There is no risk of malicious routing information being injected into the network.

Disadvantages of Static Routing:

1) **Scalability:**

Static routing becomes cumbersome in large networks, as each route must be configured manually. It's not practical for environments that frequently change.

2) **Maintenance Overhead:**

Ongoing maintenance becomes challenging, especially in dynamic environments where network changes are frequent. Any modification requires manual updates to the routing table.

3) **Lack of Adaptability:**

Static routes do not adapt to changes in the network. If a link or router fails, manual intervention is needed to update route

Static Routing vs. Dynamic Routing Protocols:

- Compare and contrast static routing with dynamic routing protocols.

Static Routing Protocols:

- **Configuration:** Routes are manually configured by the network administrator.
- **Scalability:** Less scalable in large and dynamic networks.
- **Adaptability:** Lacks adaptability to network changes.
- **Overhead:** Lower overhead as it doesn't involve continuous updates.

Dynamic Routing Protocols:

- **Configuration:** Routes are dynamically learned and updated by routers using routing protocols.
- **Scalability**: More scalable, suitable for larger and dynamic networks.
- **Adaptability**: Adapts to network changes automatically.
- **Overhead**: Higher overhead due to continuous exchange of routing information.

- Explain the concept and use of a default route. Include an example scenario.

Concept and Use of Default Route:

A default route, often represented as 0.0.0.0/0, is a route that matches all packets and is used when there is no specific match in the routing table. It acts as a catch-all for traffic that doesn't match any other route.

Example Scenario:

Imagine a network with multiple internal subnets and a single connection to the internet. Instead of manually specifying a route for every possible destination on the internet, a default route can be used.

ip route 0.0.0.0 0.0.0.0 <next-hop or exit interface>

In this example, all traffic not matching a specific internal route will follow the default route, directing it to the next-hop or exit interface that leads to the internet. This simplifies the routing table and is especially useful in scenarios where a concise route is sufficient for outbound traffic.

Conclusion and Future work: The network architecture offer a strong and safe framework that supports the organization's expansion while satisfying its present demands. Dependable departmental communication is ensured by the design's centralization of routing through the Main Router and effective interdepartmental traffic management. In addition to providing the flexibility to scale as new departments or devices are added, the 2960-24TT Switch also helps preserve network structure and security by using different IP address ranges for each department. Network security and efficiency are enhanced by security features like WPA2/WPA3 encryption and Access Control Lists (ACLs), which help safeguard sensitive resources and limit access where needed.

Looking ahead, there are opportunities to further enhance the network's performance and security. As the organization expands, implementing **VLANs** could provide stronger isolation between departments, improving both security and network efficiency. Additionally, introducing **Quality of Service (QoS)** could optimize bandwidth for critical applications, such as VoIP or video conferencing, ensuring they receive higher priority during periods of heavy traffic. To further improve network reliability, adding redundancy measures like backup routers or UPS systems would enhance fault tolerance. Finally, exploring **cloud integration** could provide scalable storage and applications, supporting the organization's growth while reducing dependency on on-premises infrastructure.

Reference:

1. Meyers, M. (2012). *CompTIA Network+ Guide to Managing and Troubleshooting Networks* (3rd ed.). McGraw-Hill Education. https://www.mheducation.com
2. Meyers, M. (2020). *CompTIA Network+ Guide to Managing and Troubleshooting Networks* (6th ed.). McGraw-Hill Education. https://www.mheducation.com
3. Stevens, W. R. (2003). *TCP/IP Illustrated, Volume 1: The Protocols* (2nd ed.). Addison-Wesley.
4. Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.
5. Tanenbaum, A. S., & Wetherall, D. (2011). *Computer networks* (5th ed.). Prentice Hall.
6. Forouzan, B. A. (2013). *Data communications and networking* (5th ed.). McGraw-Hill.