# University of Barishal

## Basic Computer Networking
## (2nd Batch)

**Submitted to**

**Md. Rashid Al Asif**

**Assistant Professor**

**Dept. of Computer Science & Engineering**

**University of Barishal**

**Submitted by**


**Name : Md Neyamat Ullah**

**St. ID : 02-002-05**

**Department : Economics**


**Submission date:15-11-2024**

# *"Configuring Basic Network Devices and IP Connectivity in Cisco Packet Tracer"*

**Abstract:** This project explores essential computer networking concepts, focusing on network design, routing, segmentation, traffic management, and security. The setup includes routers, switches, access points, and modems, implementing static routing, Routing Information Protocol (RIP), Virtual Local Area Networks (VLANs), and Quality of Service (QoS) with Differentiated Services Code Point (DSCP) marking to optimize performance and prioritize critical applications. The network design segments student, faculty, and office groups, with devices connected through a central switch and router, enabling communication both within and across segments. Results show successful communication, while discussions highlight opportunities to improve security with Access Control Lists (ACLs), use VLANs for segmentation, and implement separate subnets for better scalability. Future work will focus on enhancing segmentation, security, and network redundancy for larger environments.
This project demonstrates how foundational networking concepts are applied to create secure, scalable, and efficient network infrastructures.

## Introduction:

In a network, various devices play crucial roles in ensuring that data is transmitted and received efficiently. Routers are responsible for directing data traffic between different networks, such as connecting a local area network (LAN) to the internet. Switches, on the other hand, connect devices within a single network, such as computers, printers, and servers, allowing them to communicate with one another. Access points provide wireless connectivity, enabling devices like smartphones, laptops, and tablets to connect to a wired network without physical cables. Modems convert digital data from a network into a format suitable for transmission over telephone lines or cable systems, while also converting incoming data into a usable digital format for devices. Together, these devices create the infrastructure necessary for communication, ensuring that data can flow smoothly across the network.

In the field of computer networking, the ability to interconnect devices and ensure smooth, efficient communication has become fundamental to supporting modern digital infrastructure. Network components such as routing protocols, Virtual Local Area Networks (VLANs), and Quality of Service (QoS) are critical elements that enhance network efficiency, security, and traffic management. This project explores these concepts by implementing a series of foundational network configurations including the Routing Information Protocol (RIP), static routing, VLAN segmentation, and Differentiated Services Code Point (DSCP) marking for QoS. Each of these configurations is carefully designed to meet diverse organizational needs for performance, scalability, and security.

Routing is central to directing network traffic between devices and ensuring data reaches its destination accurately and efficiently. Both static routing and RIP are employed in this project to manage network pathways. Static routing, often used in smaller or fixed networks, provides explicit routes between segments, while RIP—an adaptive, distance-vector routing protocol—automatically exchanges route information with neighboring routers. This dynamic approach is beneficial in larger or changing network environments as it reduces the need for constant manual updates. According to Forouzan (2007), the combination of static and dynamic routing methods optimizes data flow, improves network reliability, and provides flexibility in configuring complex networks.

QoS is a further refinement to the network, specifically addressing the need for traffic prioritization as data demands grow. By using DSCP marking, the network distinguishes between different types of traffic, allowing latency-sensitive applications like VoIP (Voice over IP) and video streaming to take precedence over standard data. This prioritization ensures that time-sensitive data maintains high performance even during network congestion. As noted by Cisco (2019), DSCP-based QoS is instrumental in handling real-time applications, providing consistent and high-quality user experiences.

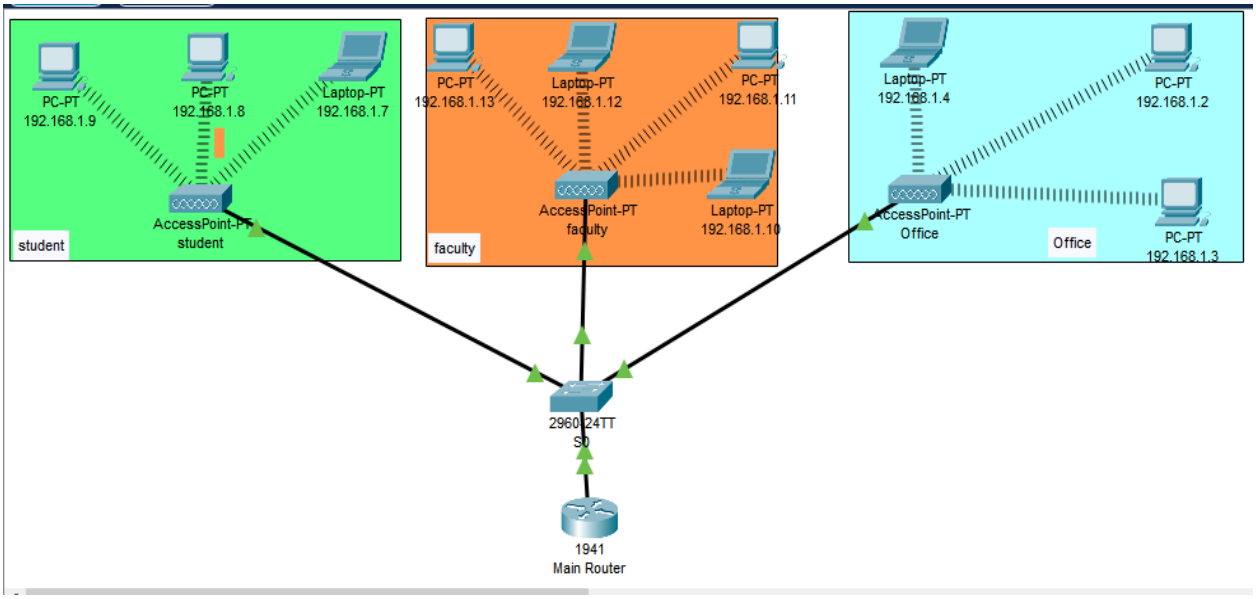
## Related Work:

Basic networking encompasses essential concepts that ensure efficient communication within a network, and includes areas like routing, traffic management, security, and network segmentation. Several studies and resources have contributed to shaping these concepts.

1. **Routing Protocols**: Static routing and dynamic routing protocols like RIP (Routing Information Protocol) are fundamental to understanding how networks make decisions about the best path for data. Static routing requires manual configuration, while dynamic protocols adjust automatically to changes. Protocols like RIP are foundational for simpler networks but have limitations in scalability and speed (Stevens, 2003; Kurose & Ross, 2017).
2. **Quality of Service (QoS)**: Managing network traffic is crucial for maintaining performance, especially with real-time applications. DSCP (Differentiated Services Code Point) is a QoS technique that helps prioritize traffic, ensuring that critical data like VoIP or video is transmitted with minimal delay. The role of QoS in optimizing network traffic is extensively documented in both academic studies and technical documentation (Stallings, 2013).
3. **VLANs and Network Segmentation**: Virtual LANs (VLANs) enable logical separation of network devices, improving security and traffic management. Research on VLANs focuses on how they reduce broadcast domains and enhance performance in enterprise networks. This concept is widely applied in practical network configurations and management guides (Meyers, 2012).
4. **Security Protocols**: Network security is a major focus, with protocols like **IPSec**, **SSL/TLS**, and **802.1X** providing critical measures for safeguarding data and controlling access. The integration of security in network configurations, including routing protocols and VLANs, is a key topic of current research, aiming to prevent unauthorized access and attacks (Zhao, 2016).

These foundational concepts in networking continue to evolve, particularly with emerging technologies like Software-Defined Networking (SDN), which offers dynamic control over traffic and network functions, reshaping network management practices (Fitzgerald, 2015).

## System Design:




This setup illustrates a basic, segmented network using wireless access points for each group (student, faculty, and office), which are all connected to a central switch and router for communication. Each segment has unique IP addresses within the same subnet (192.168.1.x), suggesting a flat network structure with no VLAN separation. This topology could be used for testing connectivity and basic inter-network routing configurations in Packet Tracer.

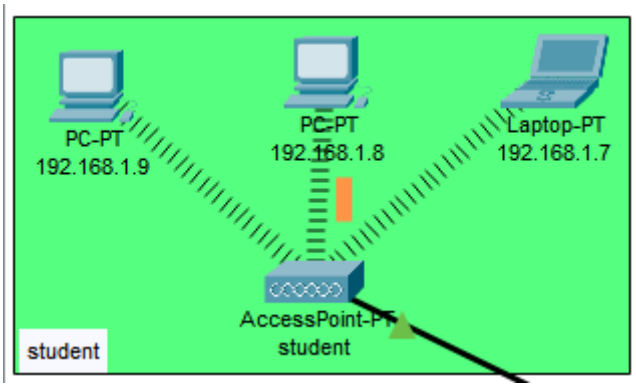
## Network Architecture:

Main Router:
Network Address: 192.168.1.0

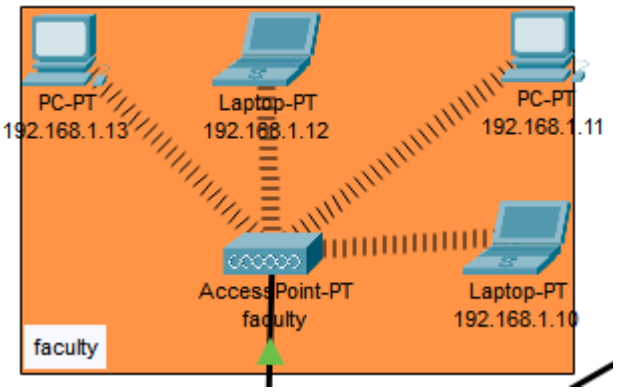
Gigabit Ethernet 0/0:
IP Address: 192.168.1.0
Subnet Mask: 255.255.255.0

Serial 0/1/0:
IP Address: 11.0.0.2
Subnet Mask: 255.255.255.0

**Student:**
**IP Addresses:**
**Laptop-** 192.168.1.7
**PC-** 192.168.1.8
**PC-** 192.168.1.9
**Subnet Mask-** 255.255.255.0



**Faculty:**
**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




**Office:**
**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) Students | 1234567890 |
| 2) Faculty | 1234567890 |
| 4) Office | 1234567890 |

## 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 routes.

**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:

This project demonstrates a basic network design with segmented access for student, faculty, and office groups, connected via a central router and switch. The setup successfully allows intra-segment and inter-segment communication, providing a foundation for understanding network topology, wireless access points, and routing basics. However, due to the single-subnet configuration, there is a lack of logical isolation between segments, which could pose security and management challenges in a real-world scenario. Implementing additional security and segmentation measures, would enhance network control, scalability, and security.

Future improvements could focus on implementing VLANs for logical isolation between segments and adding Access Control Lists **(**ACLs**)** to restrict unnecessary traffic. Additionally, using separate subnets for each group would make the network more efficient and easier to manage. These changes would enhance security and make the network more suitable for larger environments.

## Reference:


- Forouzan, B. A. (2007). *Data Communications and Networking*. McGraw-Hill Education.
- Gallo, J. (2018). *Networking Basics: The Complete Guide to Routing, Switching, VLANs, and Security*. Tech Republic.
- Cisco Systems, Inc. (2019). *Quality of Service Networking*. Retrieved from Cisco.com
- Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (7th ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Prentice Hall.
- Cisco Systems. (2023). *Introduction to networking*. Cisco Press.
- Open Networking Foundation. (2021). *Software-defined networking (SDN)*. https://www.opennetworking.org/what-is-sdn/
- Zhang, Y., & Xu, Z. (2023). *Edge computing in 5G networks*. Springer.
- Tanenbaum, A. S., & Wetherall, D. (2011). *Computer networks* (5th ed.). Prentice Hall.
- Forouzan, B. A. (2013). *Data communications and networking* (5th ed.). McGraw-Hill.