INSTITUTE OF TECHNOLOGY & MANAGEMENT
www.itmgoi.in

श्रेष्ठ इंडस्ट्री इन्टरफेस के लिए
CMAI, AICTE & RGPV
द्वारा पुरस्कृत

INSTITUTE OF TECHNOLOGY
& MANAGEMENT
GWALIOR • MP • INDIA

Laboratory Manual

COMPUTER NETWORKS
(IT-502)

For

Third Year Student
Department: Information Technology

Department of Information Technology

Vision of IT Department

The Department of Information Technology envisions preparing technically competent problem solvers, researchers, innovators, entrepreneurs, and skilled IT professionals for the development of rural and backward areas of the country for the modern computing challenges.

Mission of the IT Department

- To offer valuable education through an effective pedagogical teaching-learning process.
- To shape technologically strong students for industry, research & higher studies.
- To stimulate the young brain entrenched with ethical values and professional behaviors for the progress of society.

Program Educational Objectives

Graduates will be able to

- Our graduates will show management skills and teamwork to attain employers' objectives in their careers.
- Our graduates will explore the opportunities to succeed in research and/or higher studies.
- Our graduates will apply technical knowledge of Information Technology for innovation and entrepreneurship.
- Our graduates will evolve ethical and professional practices for the betterment of society.

Program Outcomes (POs)

Engineering Graduates will be able to:

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering Fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data,and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilitiesand norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, andgive and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Course Outcomes

Computer Networks (IT 502)

CO1:	Have a good understanding of the OSI Reference Model and its Layers.
CO2:	Identify core networking and infrastructure components and the roles they serve; and given requirements and constraints, design an IT infrastructure including devices, topologies, protocols, systems software, management and security.
CO3:	Analyze the requirements for a given organizational structure and select the most appropriate networking architecture and technologies.
CO4:	Explain the transport layer and application layer operation. Evaluate and analysis of TCP, UDP and SCTP.
CO5:	Specify and identify deficiencies in existing protocols, and then go onto formulate new and better protocols.

Course	Course Outcomes	CO Attainment	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	Have a good understanding of the OSI Reference Model and its Layers.		2	1	0	1	1	0	0	0	1	1	0	0	0	0	0
CO2	Identify core networking and infrastructure components and the roles they serve; and given requirements and constraints, design an IT infrastructure including devices, topologies, protocols, systems software, management and security.		2	1	0	0	0	0	0	0	0	0	0	0	0	0	0
CO3	Analyze the requirements for a given organizational structure and select the most appropriate networking architecture and technologies.		2	1	1	1	0	0	0	0	0	0	0	0	0	0	0
CO4	Explain the transport layer and application layer operation. Evaluate and analysis of TCP, UDP and SCTP.		2	1	1	0	1	0	0	0	0	0	0	0	0	0	0
CO5	Specify and identify deficiencies in existing protocols, and then go onto formulate new and better protocols.		2	1	1	1	2	2	0	0	1	1	0	0	0	0	0

List of Programs

1. Study of Different Type of LAN& Network Equipment's

Local Area Networks (LANs) are networks that connect computers and devices within a limited geographical area, such as a home, office, or campus. Various network equipment plays crucial roles in the setup and operation of LANs. Here's an overview of different types of LANs and network equipment:

- **Ethernet Switches:**

  Function: Switches are used to connect multiple devices within a LAN. They operate at the data link layer (Layer 2) of the OSI model and use MAC addresses to forward data only to the intended recipient.

  Types: Managed switches allow for configuration and monitoring, while unmanaged switches operate with default settings.

- **Routers:**

  Function: Routers connect different networks and facilitate communication between them. In a home or small office setting, a router typically connects the local network to the Internet.

  Features: Routers often include firewall capabilities, Network Address Translation (NAT), and Dynamic Host Configuration Protocol (DHCP) for IP address assignment.

- **Access Points (APs):**

  Function: Access points enable wireless connectivity within a LAN. They allow Wi-Fi-enabled devices to connect to the network wirelessly.

  Types: Some access points are standalone devices, while others are integrated into routers or switches.

- **Network Interface Cards (NICs):**

  Function: NICs are hardware components that allow computers to connect to a network. They can be integrated into the motherboard or added as separate expansion cards.

  Types: Wired NICs for Ethernet connections and wireless NICs for Wi-Fi connectivity.

- **Hubs:**

  Function: Hubs are basic networking devices that connect multiple devices in a LAN. Unlike switches, hubs broadcast data to all connected devices.

  Note: Hubs are less commonly used today, as switches provide more efficient data transmission.

- **Modems:**

  Function: Modems (Modulator-Demodulator) convert digital signals from computers into analog signals for transmission over telephone lines or cable systems and vice versa.

Types: DSL modems, cable modems, and fiber-optic modems are examples.

- **Firewalls:**
  Function: Firewalls protect a network by monitoring and controlling incoming and outgoing network traffic. They can be implemented in both hardware and software forms.
  Types: Stateful inspection firewalls, proxy firewalls, and application-layer firewalls.

- **Network Cables:**
  Types: Ethernet cables (e.g., Cat5e, Cat6), fiber optic cables, and coaxial cables are used to connect devices within a LAN.

- **Power over Ethernet (PoE) Devices:**
  Function: PoE devices, such as PoE switches and injectors, provide power to devices like IP cameras, VoIP phones, and wireless access points over the same Ethernet cable used for data transmission.

- **Network Analyzers:**
  Function: Tools used for monitoring and analyzing network traffic, identifying performance issues, and troubleshooting.

- **VPN (Virtual Private Network) Appliances:**
  Function: VPN appliances establish secure connections over the Internet, allowing remote users to access the LAN securely.

2. Study of standard Network topologies i.e. Star, Bus, Ring etc

Network topology refers to the physical or logical layout of a computer network. Different network topologies have distinct structures and impact how data is transmitted between devices. Here's an overview of some standard network topologies:

- **Star Topology:**

Description: In a star topology, all devices are connected to a central hub or switch. The hub or switch serves as a central point for data transmission.

Advantages:
- Easy to install and manage.
- Fault isolation - an issue with one device does not affect others.
- Scalability - easy to add or remove devices.

Disadvantages:
Dependence on the central hub - if it fails, the entire network may be affected.
Costlier to implement compared to some other topologies.

Use Cases: Common in home networks and small to medium-sized business networks.

- **Bus Topology:**

Description: In a bus topology, all devices share a common communication line, known as the bus. Data is transmitted along the bus, and each device reads the data. Devices not intended to receive the data ignore it.

Advantages:
- Simple and inexpensive to implement.
- Well-suited for small networks with limited devices.

Disadvantages:
Limited scalability - adding more devices can lead to increased collisions.
If the main bus fails, the entire network is affected.

Use Cases: Less common in modern networks but may be found in small setups.

- **Ring Topology:**

Description: In a ring topology, each device is connected to exactly two other devices, forming a closed loop or ring. Data travels in one direction through the ring.

Advantages:
- Simple and easy to install.
- Equal access to the network for all devices.

Disadvantages:
A failure in one device or connection can disrupt the entire network.
Adding or removing devices can be complex.

Use Cases: Uncommon in wired LANs but used in some token ring networks.

- **Mesh Topology:**
Description: In a mesh topology, every device is connected to every other device in the network. It provides multiple paths for data transmission, enhancing reliability.

Advantages:
- High redundancy and fault tolerance.
- Data can take multiple routes, reducing the risk of network congestion.

Disadvantages:
Expensive to implement due to the large number of connections.
Complex to manage and configure.

Use Cases: Common in critical infrastructure and large-scale enterprise networks.

- **Hybrid Topology:**
Description: Hybrid topologies combine two or more different types of topologies. For example, a network might have a star-bus or a star-ring configuration.

Advantages:
- Offers flexibility and can be tailored to specific organizational needs.
- Provides a balance between different topologies.

Disadvantages:
Complexity increases with the combination of different topologies.
Requires careful planning to avoid issues.

Use Cases: Common in large and diverse networks to address specific requirements.

3. Study of Tool Command Language (TCL)

Tool Command Language (Tcl) is a scripting language designed for ease of embedding into other applications and for providing a flexible, high-level interface. It's widely used in various fields, particularly in the realm of software development, where it serves as a scripting language for different applications. Here's a brief study of Tcl:

Introduction:
Purpose: Tcl was created with the goal of providing a simple, extensible scripting language for applications.
Embeddability: Tcl is known for its ease of embedding into other applications. It can serve as an extension language for applications written in languages like C, C++, and Java.

Syntax:
Simplicity: Tcl has a minimalistic and straightforward syntax, making it easy to learn and use.
Command-Based: Programs in Tcl are composed of commands, and each command typically consists of a command name followed by arguments.

Variables:
Dynamic Typing: Tcl uses dynamic typing, meaning variables can hold values of any type.
Variable Names: Variable names start with a letter and can include letters, digits, and underscores.

Control Flow:
Conditional Statements: Tcl supports standard conditional statements like if, elseif, and else.
Loops: The language includes loops such as while and for loops.

Procedures:
Definition: Tcl allows the creation of procedures using the proc command.
Parameter Passing: Parameters are passed by value, and the number of parameters is not fixed.

Scripting in Tcl:
Interactive Mode: Tcl can be used interactively in a shell-like environment.
Script Files: Scripts are typically stored in files with a .tcl extension.

Built-in Commands:
Extensive Library: Tcl has a rich set of built-in commands for various tasks, including string manipulation, file I/O, and mathematical operations.
Package System: The package system allows for modularization and organization of code.

Tk Toolkit:
Graphical User Interface (GUI): Tcl is often used in conjunction with the Tk toolkit to

create graphical user interfaces.
Widgets: Tk provides a set of widgets (buttons, labels, etc.) that can be used to build GUI applications.

- **Error Handling:**
  Exception Handling: Tcl uses a mechanism known as "return codes" for error handling.
  Try-catch: The try and catch commands provide a basic exception handling mechanism.

- **Platform Independence:**
  Cross-Platform Support: Tcl scripts are generally platform-independent, allowing scripts to run on different operating systems without modification.

- **Community and Extensions:**
  Active Community: Tcl has an active community of developers and users.
  Extensions: Various extensions and packages are available, expanding Tcl's capabilities.

- **Use Cases:**
  Scripting Language: Tcl is widely used as a scripting language for automation and rapid application development.
  Embedded Systems: Its embeddability makes it suitable for use in embedded systems.
  GUI Development: Tcl, along with Tk, is commonly used for developing GUI applications.

Tcl's simplicity, embeddability, and extensibility make it a versatile scripting language, particularly in scenarios where ease of integration and quick development are crucial. While it may not be as prevalent as some other scripting languages, Tcl continues to have a niche and loyal user base in various domains.

4. Study of Application layer protocols-DNS, HTTP, HTTPS, FTP and TelNet

- **Domain Name System (DNS):**

  Purpose: DNS is used to translate human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.

  Operation: It operates over both TCP and UDP, with UDP being more common for standard queries.

  Port: Typically uses port 53.

- **Hypertext Transfer Protocol (HTTP):**

  Purpose: HTTP is the foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted between web browsers and web servers.

  Operation: It operates over TCP and is a stateless protocol, meaning each request from a client is independent of previous requests.

  Port: Typically uses port 80.

- **Hypertext Transfer Protocol Secure (HTTPS):**

  Purpose: HTTPS is the secure version of HTTP. It adds a layer of security by using encryption, usually provided by TLS or SSL protocols.

  Operation: Like HTTP, it operates over TCP, but the communication is encrypted for enhanced security.

  Port: Typically uses port 443.

- **File Transfer Protocol (FTP):**

  Purpose: FTP is used for the transfer of files between a client and a server on a computer network.

  Operation: It can operate in both active and passive modes, and it uses two separate channels for **communication:** the command channel (control) and the data channel.

  Ports: Uses port 21 for command and control, and additional ports for data transfer.

- **Telnet:**

  Purpose: Telnet is a network protocol that provides a command-line interface to communicate with a device on a network.

  Operation: It operates over TCP and allows a user to access a remote device or server as if they had a direct connection.

  Security Concerns: Telnet is considered insecure because the communication, including passwords, is transmitted in plain text.

Port: Typically uses port 23.

These application layer protocols play crucial roles in enabling communication and data exchange between different devices on a network. Understanding their functionalities, security implications, and typical usage scenarios is essential for network administrators and developers working with networked applications. Additionally, the shift towards using secure versions, such as HTTPS instead of HTTP and the deprecation of less secure protocols, is an ongoing trend to enhance the security of internet communication.

5. Performing an Initial Switch Configuration

Cisco Packet Tracer is a simulation tool that allows users to create a network topology and configure devices like routers and switches. Here's a step-by-step guide on performing an initial switch configuration using Cisco Packet Tracer:

Assumptions:

- Cisco Packet Tracer is installed on your computer.
- You have a basic understanding of Cisco IOS commands.

Steps:

- Open Cisco Packet Tracer:
  Launch Cisco Packet Tracer on your computer.

- Create a Network Topology:
  Drag and drop the necessary components from the device list to the workspace. For this example, add a switch to the workspace.

- Connect Devices:
  Use the copper straight-through cables to connect devices. Connect the switch to a computer or another switch.

- Power on the Devices:
  Click on each device and use the "Physical" tab to power on the devices.

- Access the Switch CLI:
  Click on the switch to select it, then click on the "CLI" (Command Line Interface) tab.

Enter Privileged EXEC Mode:

bash Copy code

```bash
Switch> enable
Switch#
```

Enter privileged EXEC mode by typing enable and press Enter.

Enter Global Configuration Mode:

```bash
Switch# configure terminal
Switch(config)#
```

Enter global configuration mode using the configure terminal command.

Set Hostname:

```bash
Switch(config)# hostname [your-switch-name]
```

Replace [your-switch-name] with the desired hostname for the switch.

Configure Management Interface (if applicable):

If your switch has a management interface (e.g., VLAN 1), configure it with an IP address:

```bash
Switch(config)# interface vlan 1
Switch(config-if)# ip address [ip-address] [subnet-mask]
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Set Console Password:

```bash
Switch(config)# line console 0
Switch(config-line)# password [your-console-password]
Switch(config-line)# login
```

Set Telnet/SSH Password (if applicable):
If you plan to use Telnet or SSH for remote management, configure the password:

```bash
Switch(config)# line vty 0 15
Switch(config-line)# password [your-telnet-ssh-password]
Switch(config-line)# login
```

Encrypt Passwords (Optional):
For security, it's recommended to encrypt passwords:

```bash
Switch(config)# service password-encryption
```

Save Configuration:

```bash
Switch(config)# end
Switch# write memory
```

Verify Configuration:
Check the configuration settings:

```bash
Switch# show running-config
```

Exit and Reboot (if necessary):
Exit configuration mode and reboot if required:

```bash
Switch# exit
Switch> reload
```

6. Performing an Initial Router Configuration

Cisco Packet Tracer is a simulation tool that allows users to create a network topology and configure devices like routers. Here's a step-by-step guide on performing an initial router configuration using Cisco Packet Tracer:

Assumptions:

- Cisco Packet Tracer is installed on your computer.
- You have a basic understanding of Cisco IOS commands.

Steps:

- **Open Cisco Packet Tracer:**
  Launch Cisco Packet Tracer on your computer.

- **Create a Network Topology:**
  Drag and drop the necessary components from the device list to the workspace. For this example, add a router to the workspace.

- **Connect Devices:**
  Use the copper straight-through cables to connect devices. Connect the router to a switch or another router.

- **Power On the Devices:**
  Click on each device and use the "Physical" tab to power on the devices.

- **Access the Router CLI:**
  Click on the router to select it, then click on the "CLI" (Command Line Interface) tab.

Enter Privileged EXEC Mode:

```bash
Router> enable
Router#
```

Enter privileged EXEC mode by typing enable and press Enter.

Enter Global Configuration Mode:

```bash
Router# configure terminal
Router(config)#
```

Enter global configuration mode using the configure terminal command.

Set Hostname:

```bash
Router(config)# hostname [your-router-name]
```

Replace [your-router-name] with the desired hostname for the router.

Configure Interfaces:

Configure interfaces with IP addresses. For example, for the first Ethernet interface:

```bash
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address [ip-address] [subnet-mask]
Router(config-if)# no shutdown
Router(config-if)# exit
```

Set Console Password:

```bash
Router(config)# line console 0
Router(config-line)# password [your-console-password]
Router(config-line)# login
```

Set Telnet/SSH Password (if applicable):

If you plan to use Telnet or SSH for remote management, configure the password:

```bash
Router(config)# line vty 0 15
Router(config-line)# password [your-telnet-ssh-password]
Router(config-line)# login
```

Encrypt Passwords (Optional):

For security, it's recommended to encrypt passwords:

```bash
Router(config)# service password-encryption
```

Set IP Routing (if applicable):

Enable IP routing if the router needs to forward packets between different networks:

```bash
Router(config)# ip routing
```

Save Configuration:

```bash
Router(config)# end
Router# write memory
```

Verify Configuration:

Check the configuration settings:

```bash
Router# show running-config
```

Exit and Reboot (if necessary):

Exit configuration mode and reboot if required:

```bash
Router# exit
Router> reload
```

This basic configuration should provide a foundation for the router to function on the simulated network. In a real-world scenario, additional settings such as routing protocols, access control lists (ACLs), and security features may be necessary.

7. Configure the DHCP server using Cisco packet Tracer

Configuring a DHCP (Dynamic Host Configuration Protocol) server on a router using Cisco Packet Tracer involves several steps. DHCP allows devices on a network to automatically obtain IP addresses and other network configuration information. Below are the steps to configure a DHCP server on a Cisco router using Packet Tracer:

Assumptions:

- You have a Cisco router in your Packet Tracer topology.
- The router has at least one available interface (e.g., GigabitEthernet0/0) to connect to the DHCP clients.
- You are familiar with basic Cisco IOS commands.

Steps:

- **Access the Router CLI:**
  Click on the router to select it, then click on the "CLI" (Command Line Interface) tab.

Enter Global Configuration Mode:

```bash
Router> enable
Router# configure terminal
Router(config)#
```

Enter global configuration mode using the configure terminal command.

Navigate to the Interface Configurations:

```bash
Router(config)# interface [interface-type] [interface-number]
```

Replace [interface-type] and [interface-number] with the appropriate values. For example:

```bash
Router(config)# interface GigabitEthernet0/0
Router(config-if)#
```

Configure IP Address for the DHCP Pool:

```bash
Router(config-if)# ip address [ip-address] [subnet-mask]
Router(config-if)# no shutdown
Router(config-if)# exit
```

Replace [ip-address] and [subnet-mask] with the desired IP address and subnet mask.

Configure DHCP Pool:

```bash
Router(config)# ip dhcp pool [pool-name]
Router(dhcp-config)# network [network-address] [subnet-mask]
Router(dhcp-config)# default-router [default-gateway]
Router(dhcp-config)# dns-server [dns-server-address]
Router(dhcp-config)# exit
```

Replace [pool-name], [network-address], [subnet-mask], [default-gateway], and [dns-server-address] with your specific values.

Verify DHCP Pool Configuration:

```bash
Router# show ip dhcp pool
```

Save Configuration:

bash Copy code

```
Router# write memory
```

Now, the router is configured as a DHCP server. Devices connected to the specified interface will be assigned IP addresses automatically.

Example Configuration:

bash Copy code

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# ip dhcp pool mypool
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit

Router# show ip dhcp pool
```

This example assumes that the router interface is connected to devices that need DHCP-assigned addresses on the 192.168.1.0/24 network. Adjust the configuration parameters according to your network requirements.

8. Configure the DNS server using Cisco packet Tracer

In Cisco Packet Tracer, configuring a DNS (Domain Name System) server is not directly supported since Packet Tracer primarily focuses on simulating networking devices such as routers and switches. However, you can simulate the functions of a DNS server using a router or a server device.

Here's a general guideline on how you can simulate a basic DNS service on a router in Packet Tracer:

Assumptions:

- You have a Cisco router in your Packet Tracer topology.
- The router has at least one available interface (e.g., GigabitEthernet0/0).
- You are familiar with basic Cisco IOS commands.

Steps:

Access the Router CLI:

Click on the router to select it, then click on the "CLI" (Command Line Interface) tab.

Enter Global Configuration Mode:

bash Copy code

```bash
Router> enable
Router# configure terminal
Router(config)#
```

Enter global configuration mode using the configure terminal command.

Configure IP Address for the Interface:

bash Copy code

```bash
Router(config)# interface [interface-type] [interface-number]
Router(config-if)# ip address [ip-address] [subnet-mask]
Router(config-if)# no shutdown
Router(config-if)# exit
```

Replace [interface-type], [interface-number], [ip-address], and [subnet-mask] with the appropriate values.

Configure DNS Server (Simulated):

```bash
Router(config)# ip name-server [dns-server-address]
```

Replace [dns-server-address] with the IP address of a simulated DNS server. In a real-world scenario, this would be the actual IP address of a DNS server.

Save Configuration:

```bash
Router# write memory
```

Now, the router is configured to act as a DNS server (simulated). Devices connected to the specified interface can use this router as their DNS server.

Example Configuration:

```bash
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# ip name-server 8.8.8.8
```

This example assumes that the router interface is connected to devices that need DNS resolution. Adjust the configuration parameters according to your network requirements.

9. Simulate the connection of switch

To simulate the connection of a switch using Cisco Packet Tracer, you can follow these steps. We'll simulate a basic network topology with a switch, a router, and two PCs.

Assumptions:

- Cisco Packet Tracer is installed on your computer.
- You are familiar with basic Cisco Packet Tracer operations.

Steps:

- **Open Cisco Packet Tracer:**
  Launch Cisco Packet Tracer on your computer.

- **Create a New Blank Workspace:**
  Click on "File" and select "New Blank Workspace."

- **Add Devices:**
  Drag and drop the following devices from the device list to the workspace:
  Two PCs
  One Switch (e.g., Cisco 2960)
  One Router (e.g., Cisco 2911)

- **Connect Devices:**
  Use the appropriate cables to connect the devices. Connect PCs to the switch, the switch to the router, and the router back to the switch (for a simple network loop).

- **Configure Devices:**
  Click on each device and configure basic settings such as IP addresses on the PCs and router interfaces. For example:
  Configure PC1 with IP address 192.168.1.2/24 and default gateway 192.168.1.1.
  Configure PC2 with IP address 192.168.2.2/24 and default gateway 192.168.2.1.
  Configure the router interfaces and set IP addresses (e.g., GigabitEthernet0/0 with 192.168.1.1/24 and GigabitEthernet0/1 with 192.168.2.1/24).
  Configure the switch with a hostname.

- **Power On Devices:**
  Click on each device and use the "Physical" tab to power on the devices.

- **Simulate the Network:**
  Click on "Simulation" mode at the bottom of the screen.
  Use the "Capture/Forward" button to simulate time passing and network activity.

- **View Connectivity:**

Click on "Desktop" on each PC, open a command prompt, and use commands like ping to test connectivity between PCs and the router.

- **Review Switch Configuration:**
  If you want to review the switch configuration, click on the switch, then click on the "CLI" tab to enter the Command Line Interface.

- **Save Your Packet Tracer Project:**
  Click on "File" and select "Save" to save your Packet Tracer project.

This basic simulation allows you to observe how devices are connected and communicate in a network. You can further explore features like VLANs, trunking, and more advanced configurations as you become more familiar with Packet Tracer.

10. Study IP Addressing Scheme. An organization having IP Address 205.10.5.0, needs 12 subnets, design the sub netting

To design a subnetting scheme for an organization with the given IP address 205.10.5.0 and the requirement for 12 subnets, you need to determine the appropriate subnet mask and subnet ranges. Here's a step-by-step guide:

Given Information:
IP Address: 205.10.5.0
Required Subnets: 12

Steps for Subnetting:

- **Determine the Number of Bits for Subnetting:**
  Identify the number of bits needed to represent the required number of subnets. In this case, you need at least 4 bits (2^4 = 16, which is more than 12).

- **Determine the Subnet Mask:**
  For 4 bits of subnetting, the subnet mask will be 255.255.255.240 in decimal or /28 in CIDR notation.

- **Calculate the Number of Hosts per Subnet:**
  Determine the number of usable hosts per subnet. With a /28 subnet mask, there are 2^(32-28) - 2 = 14 usable addresses per subnet.

- **Identify Subnet Ranges:**
  Determine the subnet ranges based on the number of subnets and the subnet mask. Increment the network address by the subnet size to get the range for each subnet.

- **Allocate Subnets:**
  Allocate the identified subnets to different departments, branches, or purposes within the organization.

- **Subnetting Calculation:**
  IP Address: 205.10.5.0
  Subnet Mask: 255.255.255.240 (or /28 in CIDR notation)
  Usable Hosts per Subnet: 14

- **Subnet Ranges:**
  Subnet 1: 205.10.5.0 - 205.10.5.15
  Subnet 2: 205.10.5.16 - 205.10.5.31

Subnet 3: 205.10.5.32 - 205.10.5.47
...
Subnet 12: 205.10.5.176 - 205.10.5.191

Notes:

The subnet ranges are calculated by incrementing the host portion of the IP address by the subnet size (16 in this case).

Ensure that the number of subnets and usable hosts per subnet meet the organization's requirements.

This subnetting scheme allows the organization to have 12 subnets with 14 usable hosts each. Adjustments can be made based on the specific needs and growth expectations of the organization.