Roll No.: **Date:**

Exp. No.: 1

Title: Study of basic elements of Computer Networking with details of Networking Devices and troubleshooting commands.

Learning Outcomes

After completion of this experiment, students will be able to

1) Gain familiarity with essential network troubleshooting commands and their usage.
2) Develop the skills to diagnose and resolve common network connectivity issues using command-line tools.
3) Understand how to perform network connectivity tests and verify connectivity between devices using ping and traceroute.
4) Learn how to gather and interpret network configuration information using commands like ipconfig and ifconfig.
5) Acquire knowledge on performing DNS lookups and verifying DNS settings using nslookup or dig.
6) Gain insights into monitoring active network connections, ports, and services using the netstat command.

Aim

Study basic elements of computer networking and network troubleshooting commands for effective diagnosis and resolution of network issues.

Theory

Study minimum 5 networking components used in the computer networks and apply following trouble shooting commands:

1) Ping:
   - This command is used to test network connectivity and measure round-trip time (RTT) between devices. It helps verify if a device is reachable and assess network latency.
2) ipconfig:
   - Displays the IP configuration of network interfaces, including IP address, subnet mask, default gateway, and DNS servers. It is useful for diagnosing IP-related issues.
3) tracert:
   - Traces the route that packets take to reach a destination and provides information on network hops and latency at each hop. It helps identify network routing issues.
4) nslookup:
   - Performs DNS lookups to resolve domain names into IP addresses. It helps troubleshoot DNS-related issues and verify DNS configurations.
5) netstat:
   - Shows active network connections, listening ports, and network statistics. It can help identify open ports, established connections, and network services running on a system.
6) arp:

- Displays or modifies the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. It is useful for troubleshooting connectivity problems at the data-link layer.

7) route:
    - Views or modifies the local IP routing table. It is helpful for diagnosing and configuring routing issues in a network

Procedure

1. Open Command Prompt: Press the Windows key, type "Command Prompt," and select the app. Alternatively, press Windows key + R, type "cmd" in Run, and press Enter.
2. Identify the issue: Determine the specific problem, like connectivity, DNS, or a slow network.
3. Choose the relevant command: Select a command suited to the issue, e.g., "ping" for connectivity problems.
4. Enter the command: In the Command Prompt, type the command with parameters/options, like "ping <IP address>", and press Enter.
5. Review output: Check responses, errors, or relevant information displayed.
6. Interpret results: Analyze output to understand network connection status or error messages.
7. Perform additional commands: If needed, run more commands for further information or tests.
8. Take appropriate action: Based on the command results, resolve the network issue by adjusting settings, resetting devices, or seeking assistance.

Observation

Implement the network troubleshooting commands mentioned above and write down your observations.

Self-assessment

1. Discuss a scenario where a combination of network troubleshooting commands was necessary to resolve a complex network problem. Describe the problem and the commands used.
2. How do network troubleshooting commands contribute to your overall understanding of network diagnostics and problem-solving?
3. Can you think of any additional network troubleshooting commands or tools that complement the ones mentioned? Explain their relevance in troubleshooting network issues.

Concluding Remarks:

Roll No.: **Date:**

Exp. No.: 2

Title: **Study various types of network components.**
Introduction to the network simulator tool, Cisco packet tracer.

Learning Outcomes:

After completion of this experiment, students will be able to

1) have an understanding of networking components such as cables, connectors, hubs, switches, bridges, network interface cards (NIC), gates, and firewalls.
2) explain the function and installation of Packet Tracer.
3) create a simple simulated network using a packet tracker.

Aim

Study various types of network components. Introduction to the network simulator tool, Cisco packet tracer.

Theory

1) Fiber-optic cable

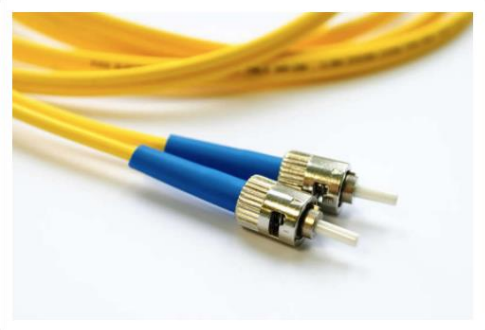


Figure 1: Fiber-optic cable

- These cables mostly consist of center glass and different layers of protective materials surrounding them. Fiber-Optic cabling transmits light in place of electronic signals, which removes the issue of electrical interference. This makes it an ideal selection for environments that contain a large amount of electrical interference.
- This type of network cable offers the ability to transmit signals over longer distances. It also provides the ability to carry information in a faster space.

Two types of fiber-optic cables are:

- Single-mode fiber (SMF)– This type of fiber optic cable uses only a single ray of light to carry data. Used for larger distance wiring.
- Multimode fiber (MMF)– This type of fiber-optic uses multiple rays of light to carry data. Less Expensive than SMF.

2) Coaxial cable

Figure 2: Coaxial cable

- Coaxial Cable is standard for 10 Mbps Ethernet cables. These types of cables consist of an inner copper wire cover with insulation and other shielding.
- It has a plastic layer that offers insulation between the braided metal shield and the center conductor. Coaxial cabling has a single copper conductor in its center.
- Types of coaxial cable are a) RG58 b) RG8 c) RG6, and d) RG59

3) Twisted-pair cable

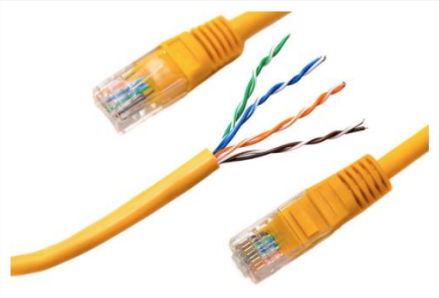


Figure 3: Twisted-pair cable

- Twisted-Pair Cabling is a type of cabling in which pairs of wires are twisted together to stop electromagnetic interference (EMI) from other wire pairs.
- Two types of twisted pair cables are a) Unshielded Twisted Pair b) Shielded Twisted pair

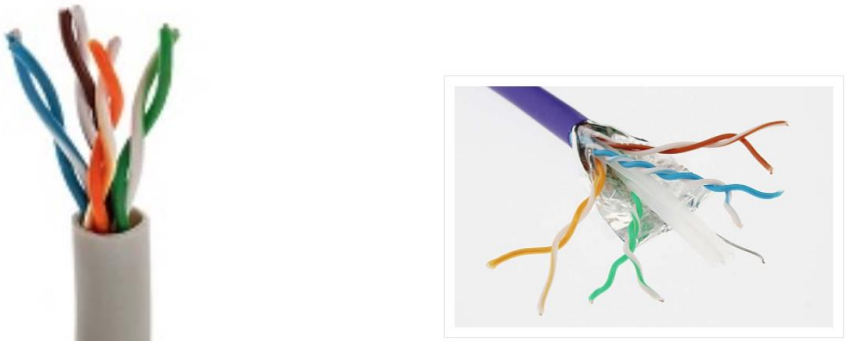


Figure 4a, 4b: Unshielded and Shielded Twisted-pair cables

4) Connectors
   - Connectors in networking are essential for establishing physical connections between devices.
   - Common connectors include RJ-45 for Ethernet, fiber optic connectors like SC and LC, BNC for video transmission, USB for peripheral devices, and HDMI for audio/video. Coaxial connectors are used in cable and satellite TV connections.
   - Choosing the right connector ensures reliable data transmission.

5) Hubs
   - A hub is a basic networking device that connects multiple Ethernet devices together.
   - It operates at the physical layer and broadcasts data to all connected devices. Hubs amplify and regenerate signals but create a single collision domain, leading to performance degradation.
   - They have limited bandwidth and have been largely replaced by switches in modern networks.

6) Switches
   - Switches are networking devices that connect multiple devices in a LAN and facilitate communication between them.
   - They operate at the data link layer and use packet switching to forward data based on MAC addresses.
   - Switches support unicast, broadcast, and multicast traffic and can also implement VLANs for network segmentation.
   - Switches provide better performance and management capabilities compared to hubs.

7) Bridges
   - Bridges are networking devices that connect LANs or network segments.
   - They operate at the data link layer and forward traffic based on MAC addresses.

- Bridges segment networks and improve performance by reducing congestion.
- While switches have largely replaced bridges, the term "bridge" is sometimes used interchangeably with switches.

8) Network Interface Card
   - A Network Interface Card (NIC), also known as a network adapter or network card, is a hardware component that allows a computer or other device to connect to a network.
   - It provides the physical interface between the device and the network medium, enabling communication with other devices on the network.

9) Gateway and Firewalls
   - Gateway, is a device or software component that serves as an entry or exit point for data traffic between different networks.
   - It acts as a bridge, facilitating communication and data transfer between networks that use different protocols, addressing schemes, or communication technologies.
   - Firewalls are network security devices or software that monitor and control incoming and outgoing network traffic based on predetermined security rules.
   - They act as a barrier between trusted internal networks and untrusted external networks, providing protection against unauthorized access, malicious activities, and potential threats.

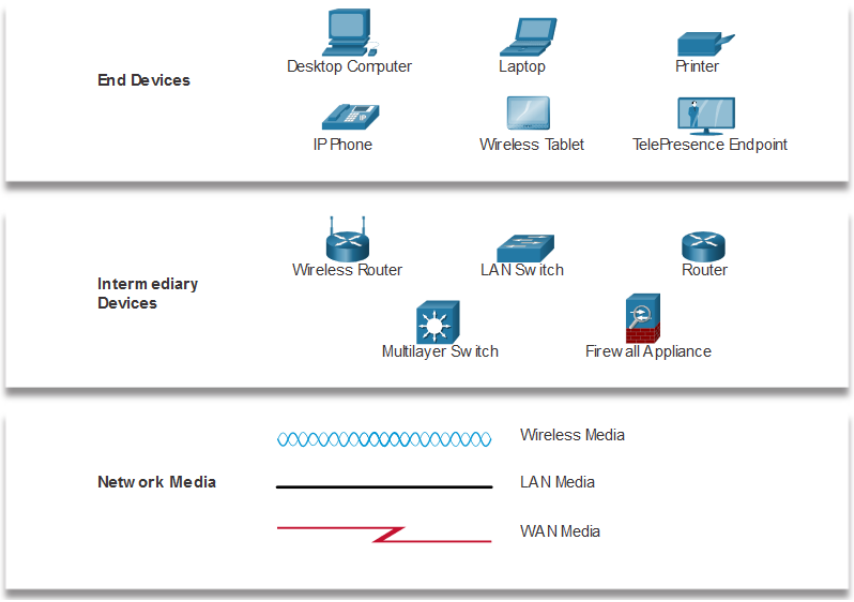


Figure 5: Network Devices and Media

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It provides a virtual environment where users can design, configure, and troubleshoot computer networks. Packet Tracer allows users to simulate network topologies, network devices, and network connections, enabling them to gain hands-on experience with networking concepts and technologies.

Procedure

Steps to help you get started with Packet Tracer:

1. Download and Install: Visit the Cisco Networking Academy website or another reliable source to download the latest version of the Cisco Packet Tracer. Install the software on your computer following the provided instructions.
2. Launch Packet Tracer: Open the Packet Tracer application once it is installed on your computer.
3. Create a New Project: In Packet Tracer, click on "File" in the top menu and select "New" to create a new project. Give the project a name and specify a location to save it.
4. Explore the Interface: Familiarize yourself with the Packet Tracer interface. You will see various panels and toolbars, including the device toolbar on the left, the workspace area in the middle, and options on the top menu. Take a moment to understand the purpose of each panel and toolbar.
5. Add Network Devices: Start building your network topology by adding devices from the device toolbar. Click on a device icon (e.g., router, switch, PC) and then click on the workspace area to place it. Repeat this step to add more devices as needed.
6. Connect Devices: Once you have placed devices on the workspace, use the appropriate cable type from the device toolbar to establish connections between devices. Click on a device's interface, then click on the corresponding interface of another device to create a connection.
7. Configure Devices: Double-click on a device to open its configuration window. Depending on the device type, you will see various settings and parameters that can be configured, such as IP addresses, routing protocols, VLANs, and more. Experiment with different configurations to learn how they impact network behavior.
8. Test and Troubleshoot: Once your network is configured, you can test its functionality. Send traffic between devices, ping IP addresses, or use applications to verify connectivity. If you encounter issues, troubleshoot the network by examining device configurations, connections, and network settings.
9. Explore Additional Features: Packet Tracer offers additional features such as simulation modes, traffic generators, and network analysis tools. Take some time to explore these features and understand how they can enhance your learning experience.

10. Save and Share: After completing your work, save the project by clicking on "File" and selecting "Save" or "Save As." You can also export the project for sharing with others.

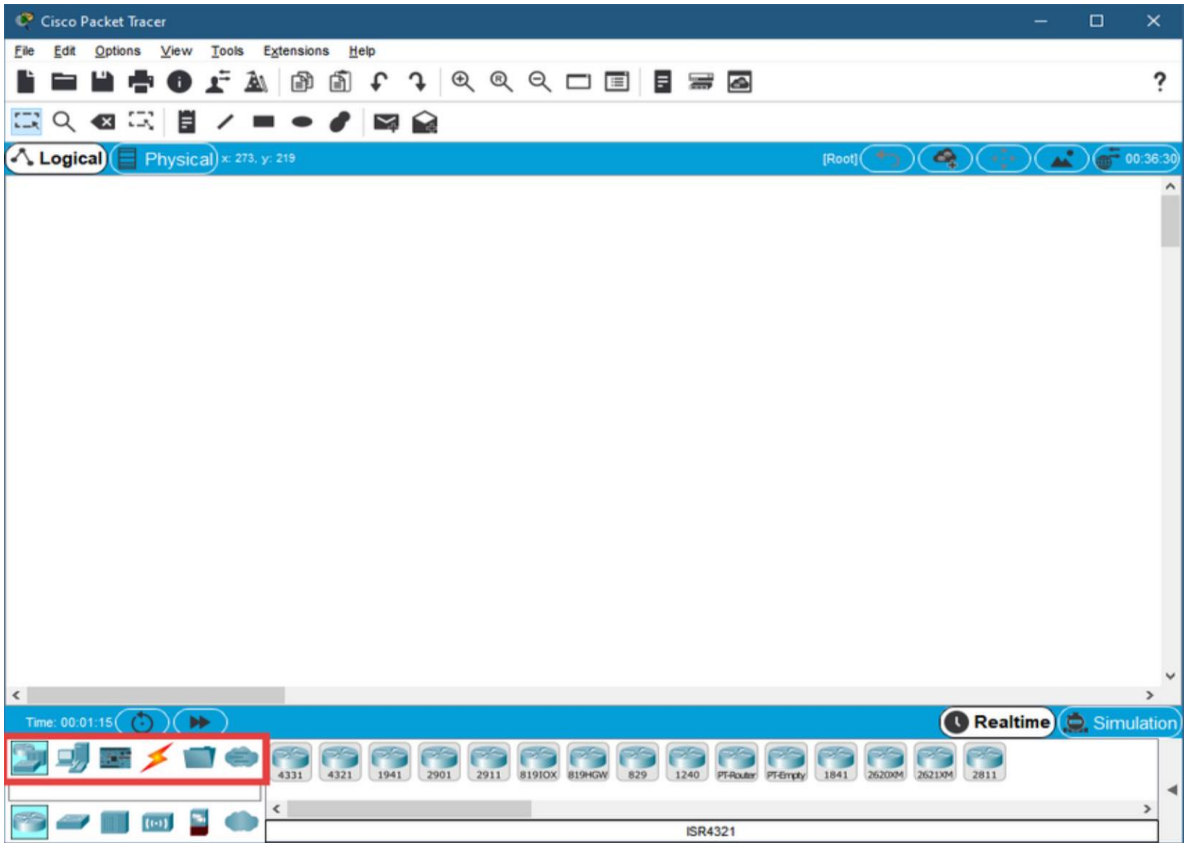


Figure 6: Cisco's Packet Tracer

- The top row of icons represents the category list consisting of: [Networking Devices], [End Devices], [Components], [Connections], [Miscellaneous], and [Multiuser].
- Each category contains at least one sub-category group.

GUI and CLI Configuration in Packet Tracer

The Physical tab provides an interface for interacting with the device including powering it on or off or installing different modules such as a wireless network interface card (NIC).

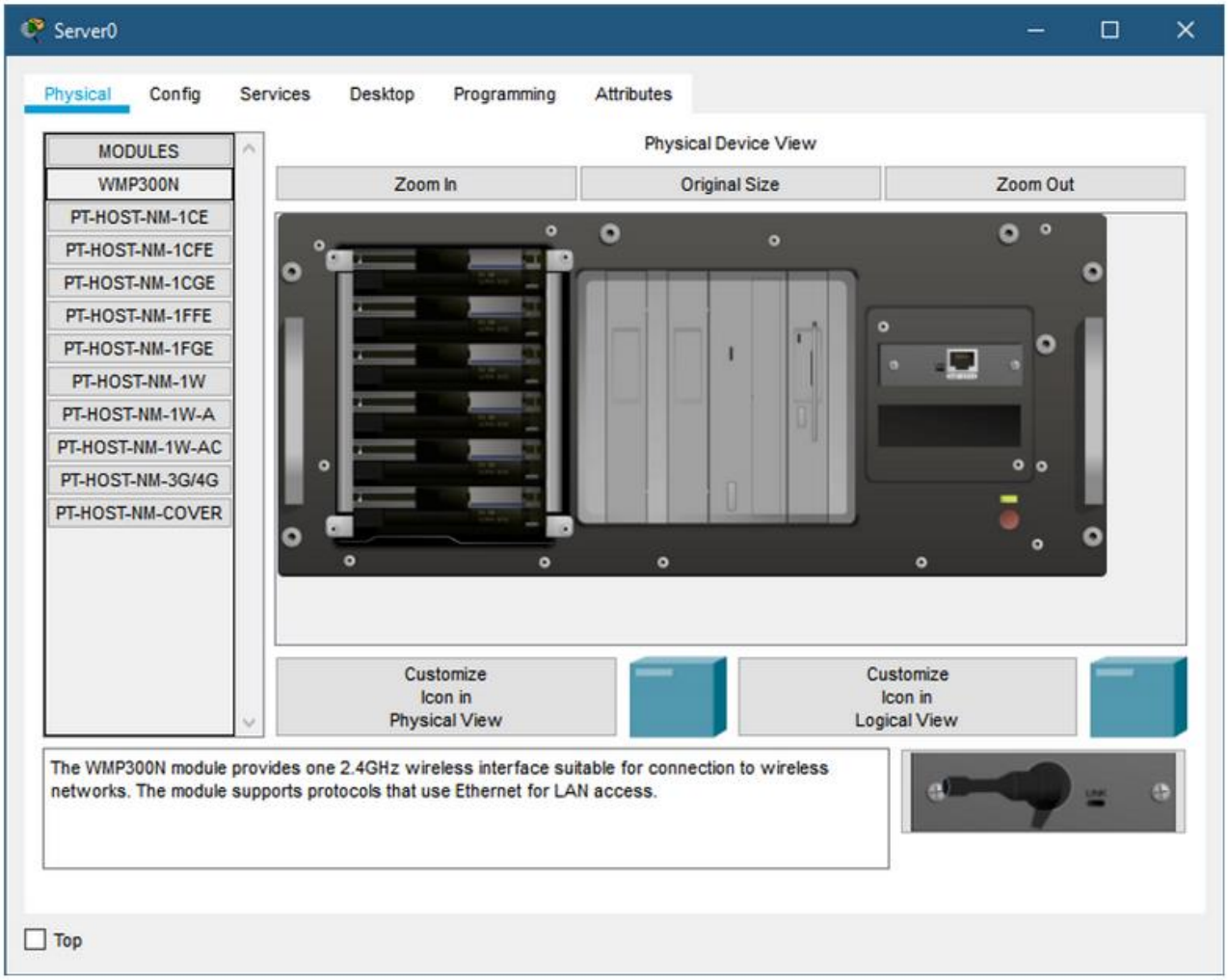


Figure 7: Physical tab in Cisco's Packet Tracer

The Config tab is a learning tab in Packet Tracer. This tab provides a way to do basic configurations. It will show the equivalent CLI commands that perform the same action if someone was configuring using the CLI tab.

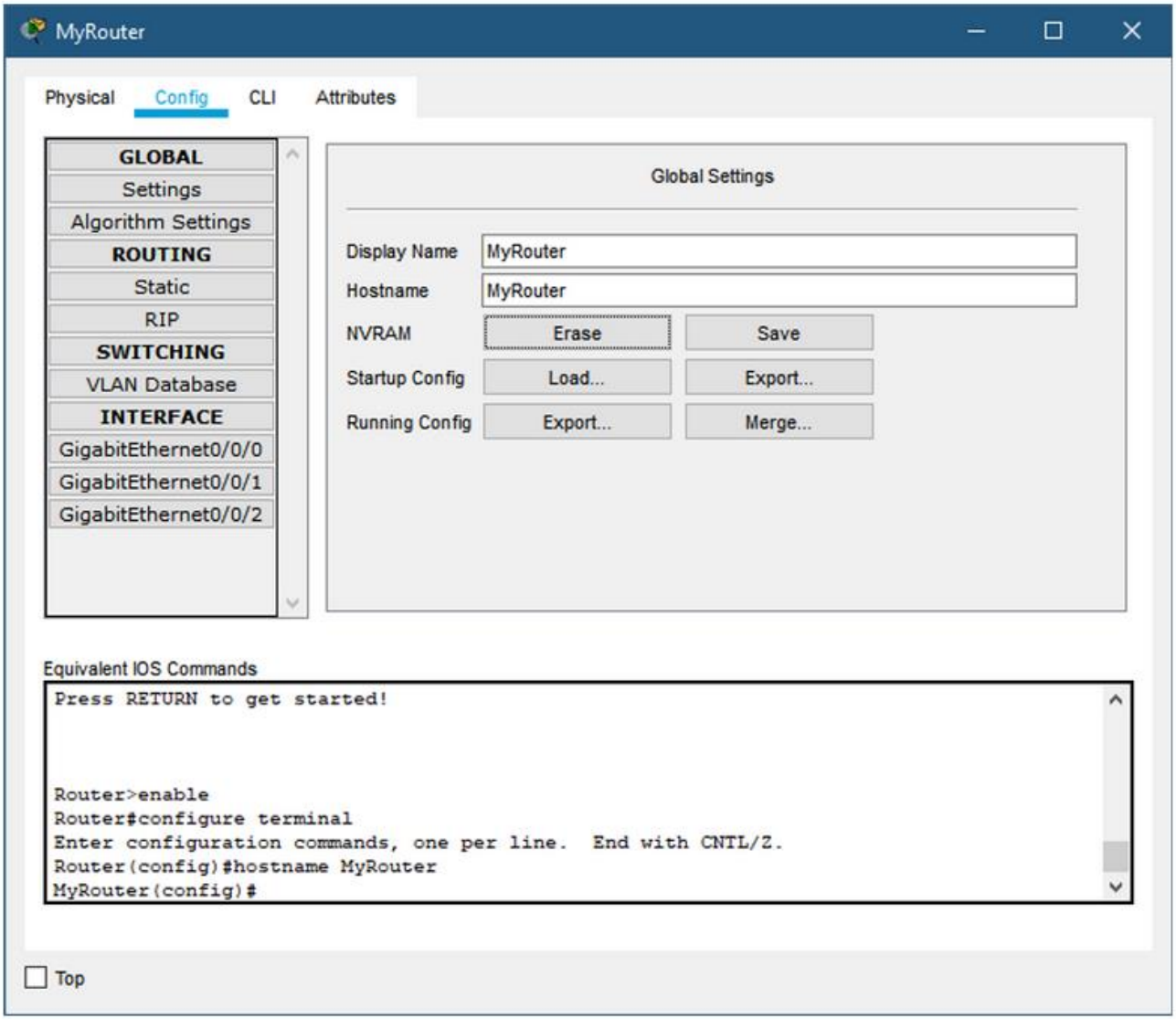


Figure 8: Config tab in Cisco's Packet Tracer

The CLI tab provides access to the CLI interface. Here, you can practice configuring the device at the command line.

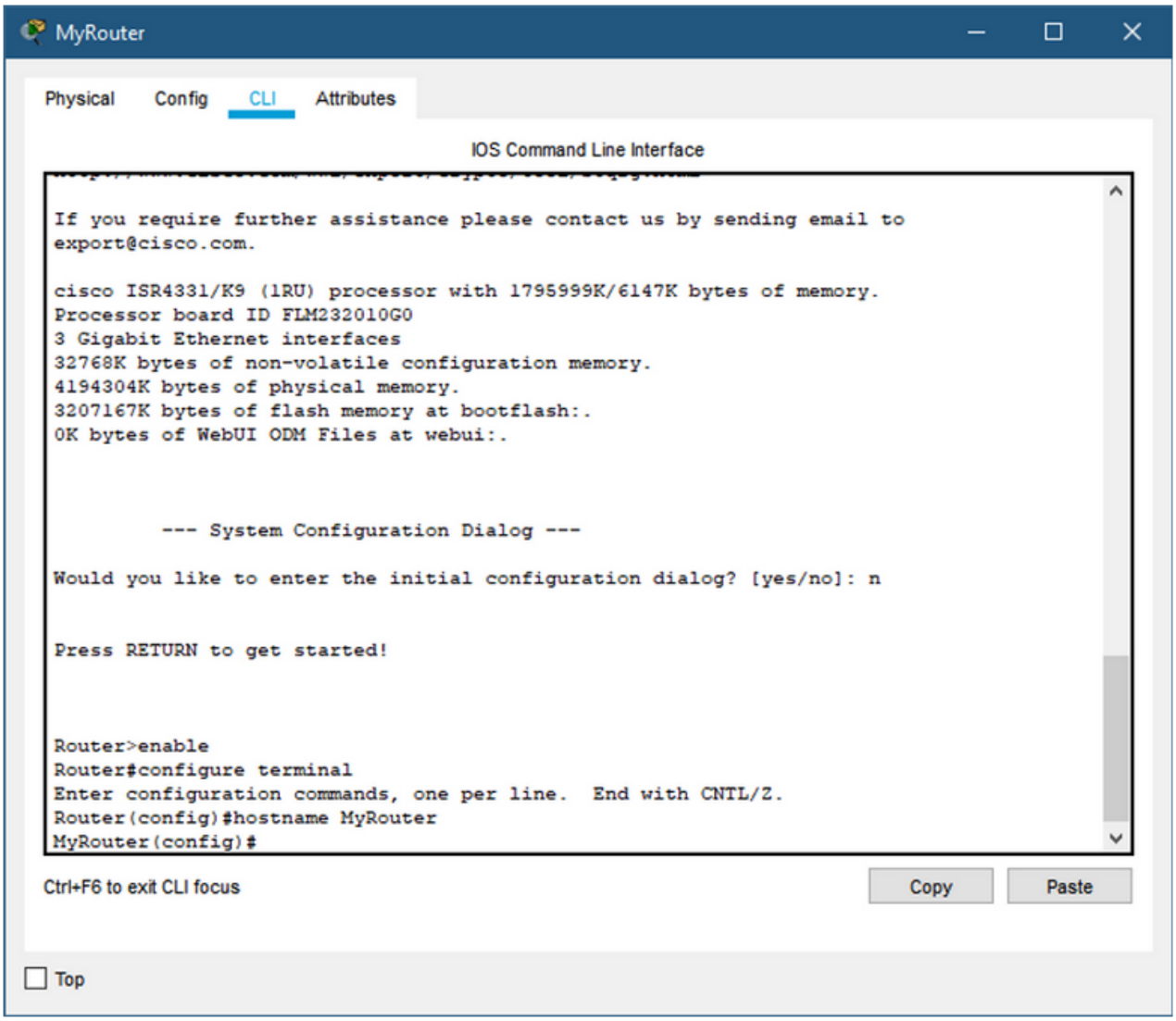


Figure 9: CLI tab in Cisco's Packet Tracer

For some of the end devices Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a web browser, and much more.

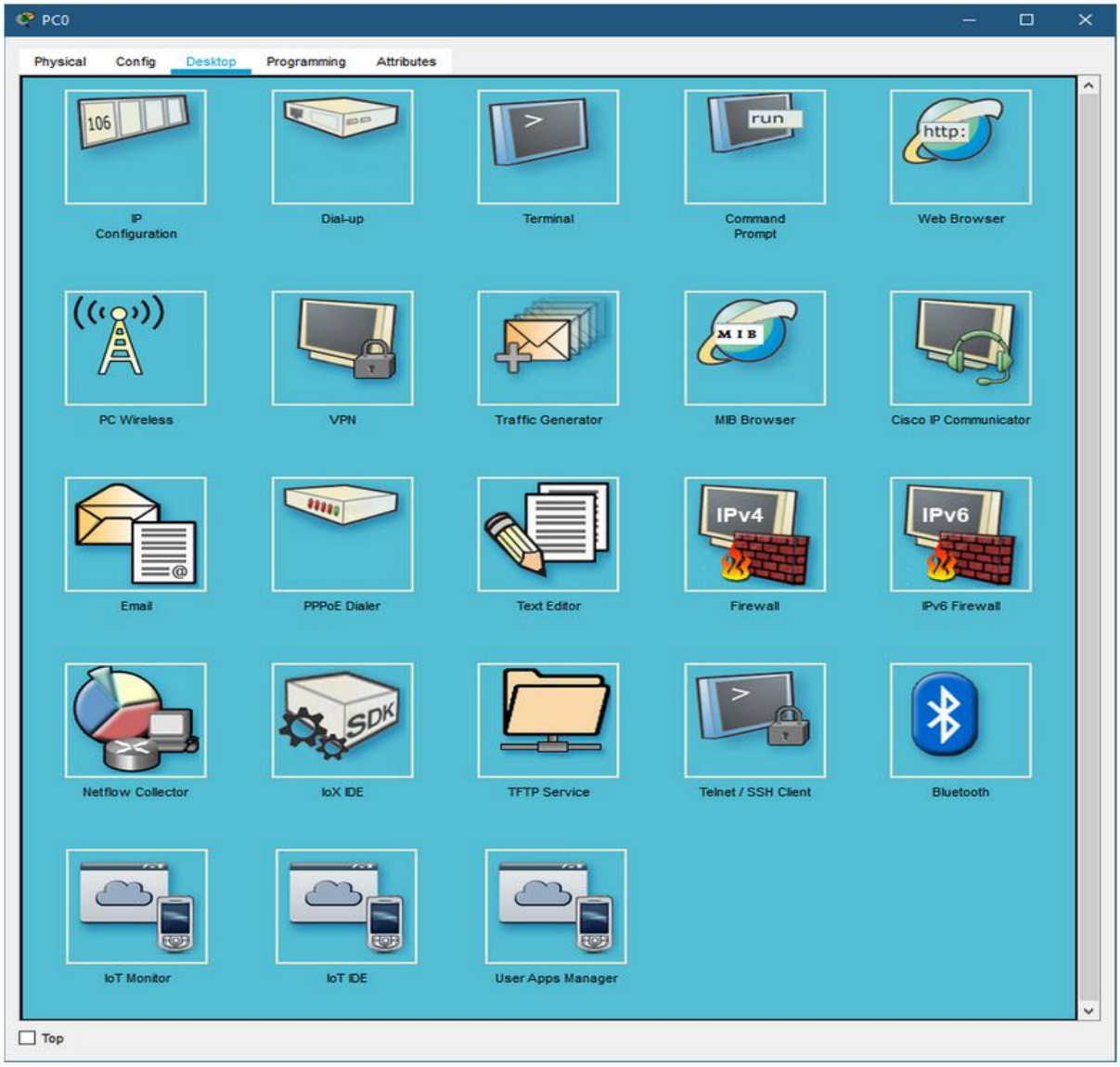


Figure 10: Desktop interface in Cisco's Packet Tracer

If you are configuring a server, the server has all of the functions of a host with the addition of one more tab, the Services tab. This tab allows a server to be configured as a web server, a DHCP server, a DNS server, or various other servers visible in the graphic.

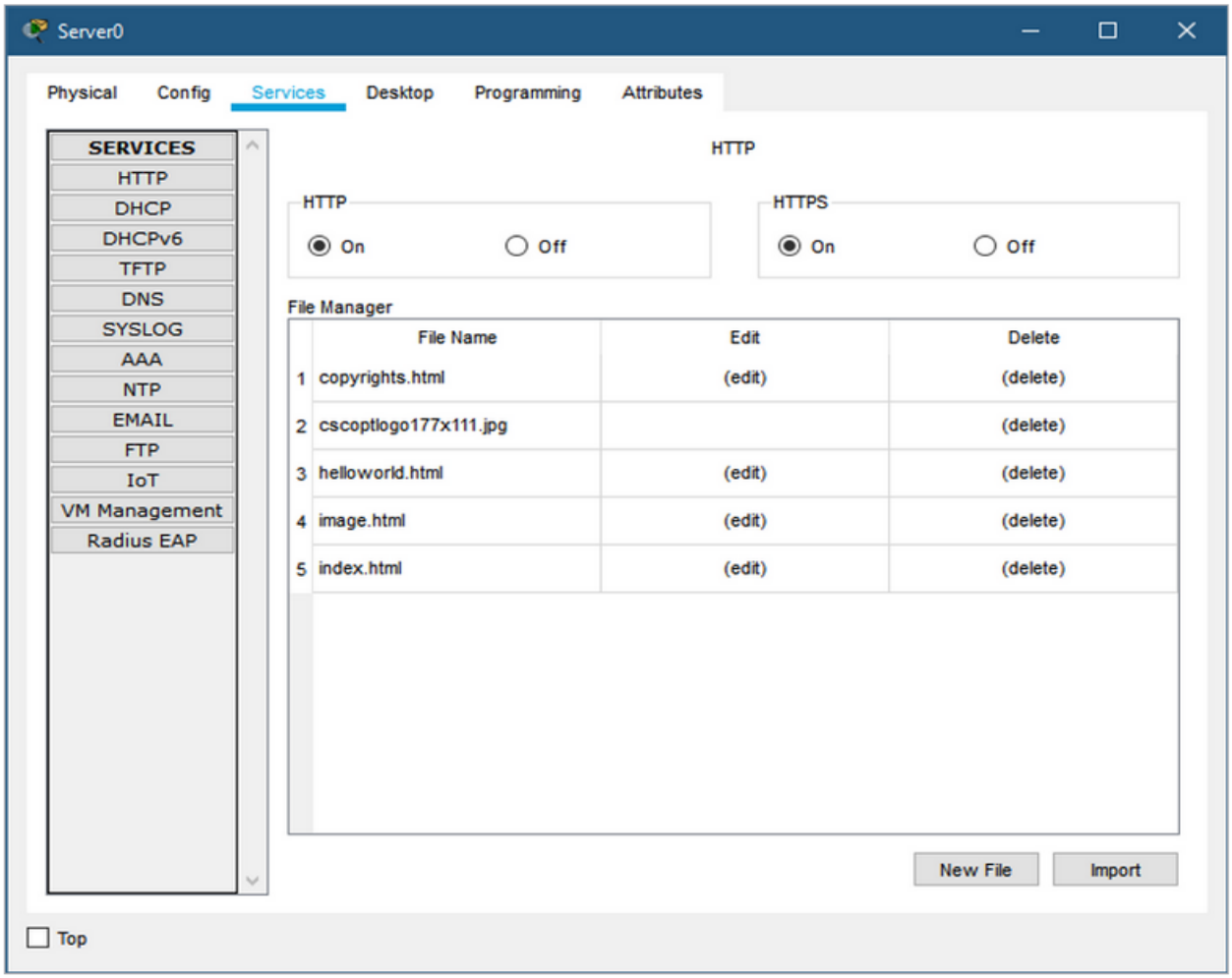


Figure 11: Services tab in Cisco's Packet Tracer

Observation

Implement a design for a small network to include two switches and two PCs as shown below. Write down your observations on how a packet is transferred.

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

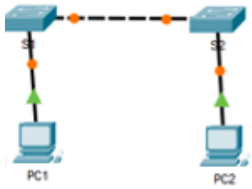


Figure 12: Network in Cisco's Packet Tracer

Self-Assessment:

1. How do you add a PC to the workspace in Cisco Packet Tracer, and what configurations can you make to the PC?
2. How do you configure a default gateway on a PC in Cisco Packet Tracer, and why is it necessary for devices to communicate with devices on different networks?
3. How do you use the "CLI" (Command Line Interface) to configure devices in Cisco Packet Tracer, and what are some basic commands you can use?

Conclusion

Roll No.: **Date:**

Exp. No.: 3

Title: Study and Configure Bus, and Mesh Network Topologies in Cisco Packet Tracer.

Learning Outcomes

After Completion of this experiment, students will be able to

1) have an understanding of bus and mesh network topologies.
2) create a network with bus and mesh topologies in Packet Tracer.

Aim

Study types of bus and mesh network topologies. Configure a network using Bus and Mesh topology in packet tracer.

Theory

1) Bus Topology

- In this topology, all devices are connected to a single communication line, often called a "bus."
- Each device shares the same communication medium and can transmit and receive data.
- However, the entire network can be affected if there is a break or failure in the main communication line.

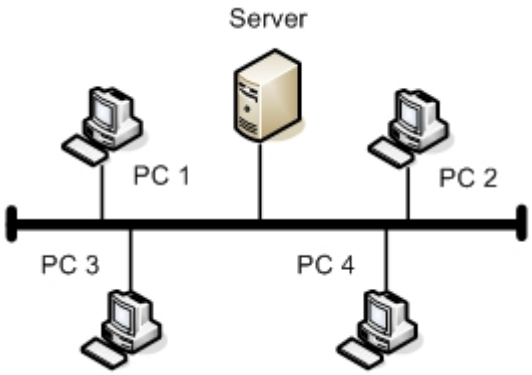


Figure 1: Bus Network Topology

2) Mesh Topology:

- A mesh topology provides a direct point-to-point connection between every device in the network.
- Each device has a dedicated connection to every other device, resulting in redundant paths.
- This redundancy enhances fault tolerance and ensures that if one path fails, data can still be transmitted through alternative routes.
- Mesh topologies can be fully connected (every device connected to every other device) or partially connected (selected devices have direct connections).

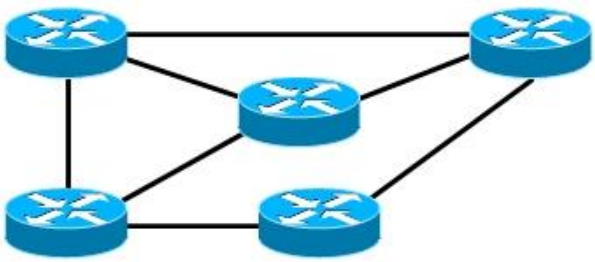


Figure 2: Mesh Network Topology

Bus topology

Procedure to implement Bus topology in Packet Tracer

a. Open Packet Tracer and create a new project.
b. Drag and drop (n) switch icons onto the workspace to represent the switches.
c. Drag and drop (n) computer icons onto the workspace to represent the PCs.
d. Connect a PC to a switch (1 PC to 1 Switch) using copper straight-through cables. Each PC should have its own dedicated copper straight-through cable connecting it to the switch.
e. Repeat step 4 for all other (n) PCs.
f. Next, connect the switches together in a linear chain using copper crossover cables. Connect the first switch to the second switch using a crossover cable, the second switch to the third switch using another crossover cable, and so on.
g. Verify that all (n) PCs are connected to their switch, and the switches are connected in a linear chain using crossover cables, forming a bus topology.
h. Configure IP addresses for the devices. Right-click on each device and select "Configure" or "Desktop" to access the device's configuration options. Assign unique IP addresses to each PC on the network. Make sure that the subnet masks are the same for all devices.
i. You have now created a bus topology using (n) switches and (n) PCs in Packet Tracer.
j. Observe how a packet is transferred from the source to the destination PCs in a bus topology in Packet Tracer.

Verification

1) Ping test. Select the "Desktop" view for one of the devices (e.g., a computer) by right-clicking on it and selecting "Desktop." Open a command prompt or terminal window on the device.
2) Use the ping command to test connectivity between devices. ping one computer from the other by using its IP address. Type the following command in the command prompt or terminal window as shown in Figure.
3) If the ping is successful, you should see replies indicating that the packets were sent and received. This confirms that the bus topology is functioning properly.
4) Repeat the ping test for all devices connected to the bus to ensure connectivity between them.

OR

5) Select a source device (e.g., PC 1) from which you want to send the packet. Select a destination device (e.g., PC 2) from which you want to send the packet.
6) Click and hold the PDU icon in the toolbar, then drag it from the toolbar to the source PC.
7) Release the mouse button to drop the PDU onto the source PC.
8) Click and drag the PDU from the source PC to the destination PC on the bus topology.
9) Release the mouse button to drop the PDU onto the destination PC.
10) Observe the behavior of the bus topology.

Mesh Topology

Procedure to implement Mesh topology in Packet Tracer

1) Open Packet Tracer and create a new blank project.
2) Drag and drop four PCs from the "End Devices" section onto the workspace.
3) Drag and drop four switches from the "Switches and Hubs" section onto the workspace.
4) Connect each PC to all four switches using Ethernet cables. To do this, follow these steps for each PC: a. Click on a PC to select it. b. Click on an available Ethernet port (represented by a small square) on the PC. c. Drag the cable to one of the switches and release it on an available port. d. Repeat this process to connect the PC to all four switches.
5) Now, you need to connect the switches to each other to create the mesh topology. Follow these steps for each switch: a. Click on a switch to select it. b. Click on an available Ethernet port to select it. c. Drag the cable to another switch and release it on an available port. d. Repeat this process for all switches, connecting each switch to the other three switches.
6) Once all the connections are made, you should have a mesh topology with four PCs and four switches, and each PC connected to all four switches.
7) Save your project.
8) Now you can start configuring IP addresses on the PCs and test communication between them. To configure IP addresses: a. Click on a PC to select it. b. Click on the "Config" tab in the right-hand panel. c. Enter the IP address, subnet mask, and default gateway for each PC. Make sure that each PC has a unique IP address within the same subnet.
9) After configuring the IP addresses, you can use the "Command Prompt" utility on each PC to ping other PCs and test the connectivity in the mesh topology.
10) Configure IP addresses for each PC. Double-Click on a PC to open the configuration window. Set an appropriate IP address for each PC. Ensure that the IP addresses are within the same subnet. You can use IP addresses like 192.168.0.1, 192.168.0.2, 192.168.0.3, and 192.168.0.4 with a subnet mask of 255.255.255.0.

Verification

1) Test the connectivity between the PCs by opening the "Command Prompt" or "Terminal" on each PC and pinging the IP addresses of the other PCs. For example, from PC1, you can ping PC2 using the command "ping 192.168.0.2".
2) Verify that all the PCs are able to communicate with each other successfully.

OR

3) Select a source device (e.g., PC 1) from which you want to send the packet. Select a destination device (e.g., PC 2) from which you want to send the packet.
4) Click and hold the PDU icon in the toolbar, then drag it from the toolbar to the source PC.
5) Release the mouse button to drop the PDU onto the source PC.
6) Click and drag the PDU from the source PC to the destination PC on the bus topology.
7) Release the mouse button to drop the PDU onto the destination PC.
8) Observe the behavior of the Mesh topology.

Observation

Implement the above topologies and write your observations briefly.

Self-Assessment:

1. In a bus topology with five computers, one of the computers is not able to communicate with the others. Troubleshoot the issue using Packet Tracer and identify the possible reasons for the problem.
2. Compare the fault tolerance capabilities of bus and mesh topologies in Packet Tracer. Discuss which topology is more resilient to failures and explain the reasons behind it.
3. Discuss the scalability of bus and mesh topologies. How do these topologies handle an increasing number of devices? Explain the factors that may limit the scalability of each topology.

Conclusion

Roll No.: **Date:**

Exp. No.: 4

Title: Study different types of networks and build LAN, WAN, and MAN using a Cisco packet tracer.

Learning Outcomes:

After Completion of this experiment, students will be able to

1) have an understanding of various types of networks.
2) identify different types of networks.
3) build LAN, WAN, and MAN using Cisco Packet Tracer.

Aim

To develop a comprehensive understanding of various network types, enable identification of different networks, and practice building LAN, WAN, and MAN using Cisco Packet Tracer.

Theory

Networks play a vital role in modern networking by enabling communication and resource sharing among devices. Various types of networks serve different purposes to meet the diverse needs of users and organizations. The most prominent types of networks include Local Area Networks (LANs), Wide Area Networks (WANs), Metropolitan Area Networks (MANs), Storage Area Networks (SANs), Virtual Private Network (VPN), Wireless Network, and Cloud Network.

Three most common types of networks:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

LANs, WANs, and MANs

Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

LANs

- A LAN is a network infrastructure that spans a small geographical area.
- Interconnect end devices in a limited area.
- Administered by a single organization or individual.
- Provide high-speed bandwidth to internal devices.

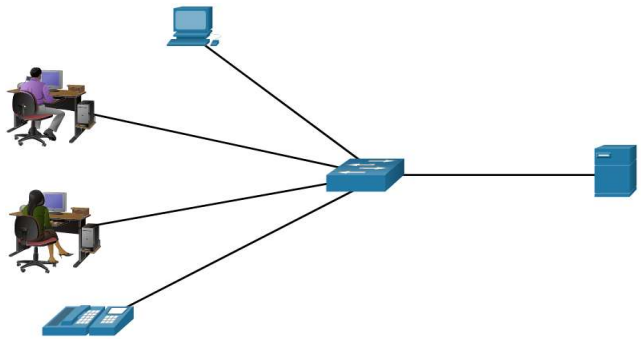


Figure 1: LAN Network Infrastructure

Procedure to implement LAN in Packet Tracer

1) Launch Cisco Packet Tracer and create a new network project.
2) From the "End Devices" section in the Packet Tracer palette, drag and drop (n) PCs/laptops onto the workspace. **Example, 2PC's and 2 Laptops:**
3) Similarly, drag and drop a switch onto the workspace.
4) Connect one end of an Ethernet cable to the Fast Ethernet (FE) port of PC1 and connect the other end to one of the switch ports.
5) Connect one end of another Ethernet cable to the FE port of PC2 and connect the other end to a different switch port.
6) Connect one end of a third Ethernet cable to the FE port of laptop1 and connect the other end to another switch port.
7) Connect one end of a fourth Ethernet cable to the FE port of laptop2 and connect the other end to another switch port.
8) Ensure all the connections are properly made and the devices are powered on.
9) Now, you have successfully implemented a LAN using two PCs, two laptops, and a switch in Cisco Packet Tracer.

Verification

- You can test the connectivity by assigning IP addresses to the devices within the same subnet.
- Right-click on each device, select "Configure," and set the IP address, subnet mask, and default gateway accordingly.
- You can then ping or perform other network tests between the devices to verify the connectivity within the LAN

WANs

- A WAN is a network infrastructure that spans a wide geographical area.
- Interconnect LANs over wide geographical areas.
- Typically administered by one or more service providers.
- Typically provide slower speed links between LANs.
-

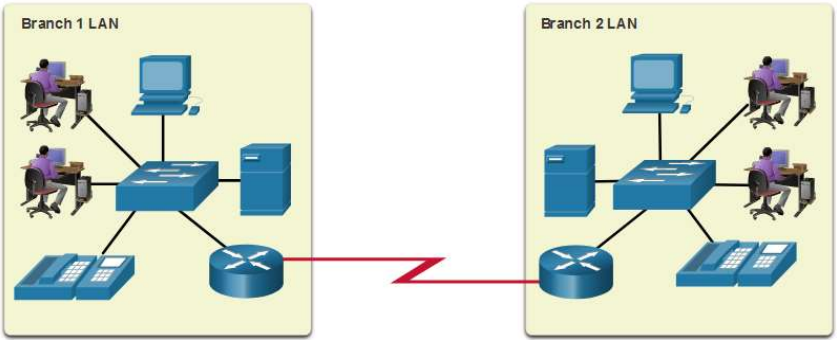


Figure 2: WAN Network Infrastructure

Procedure to implement WAN in Packet Tracer

- Introduce router into the LAN network to establish the WAN connectivity.
- Connect the LAN switches to the router using serial interfaces.
- Configure the router interfaces with appropriate IP addresses (Default gateways of your PC's/Laptops).

Verification

- Test the connectivity between LANs by pinging devices across different LANs.

MANs

- A MAN is a network that spans a larger geographical area than a LAN.
- It connects multiple Local Area Networks over high speed links such as fiber optic cables.
- A MAN can be built by a single organization to connect multiple offices spanning a few building that are not very far from each other or it might be operated as public utility.

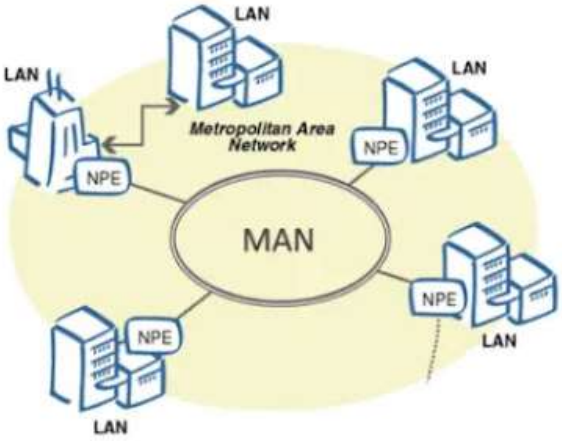


Figure 3: MAN Network Infrastructure

Observation

- In terms of LAN, a WAN and MAN acts as an extension or interconnection of multiple LANs.
- Implement a simple WAN network, and MAN network.

Self-Assessment:

1. What are some challenges associated with managing and securing a WAN compared to a LAN?
2. List the limitations or constraints that you faced of simulating WAN networks in Packet Tracer?

Conclusion

Roll No.: **Date:**

Exp. No.: 5

Title: Create a Simple Network Using Packet Tracer. (Intranet, Internet, and Laptop/PC/Mobile devices)

Learning Outcomes:

After Completion of this experiment, students will be able to

1. Understand and explain the common types of network-internet, intranet, and extranet.
2. Simulate the network using the internet, intranet, and extranet in packet tracer.

Aim

To help understand different network types (internet, intranet, and extranet) and practice simulating them using Packet Tracer.

Theory

The Internet

- The internet is a worldwide collection of interconnected LANs and WANs.
- LANs are connected to each other using WANs.
- WANs may use copper wires, fiber optic cables, and wireless transmissions.
- The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:
  IETF
  ICANN
  IAB

Intranets and Extranets

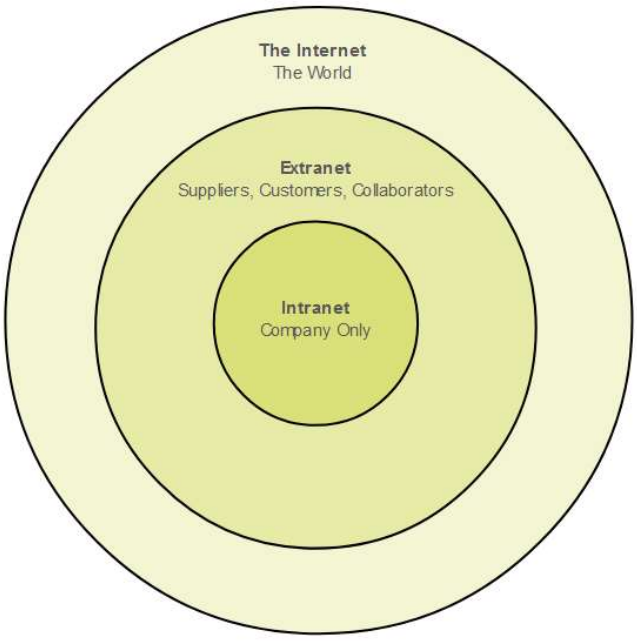


Figure 1: The internet and Intranet

- An intranet is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.
- An organization might use an extranet to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.

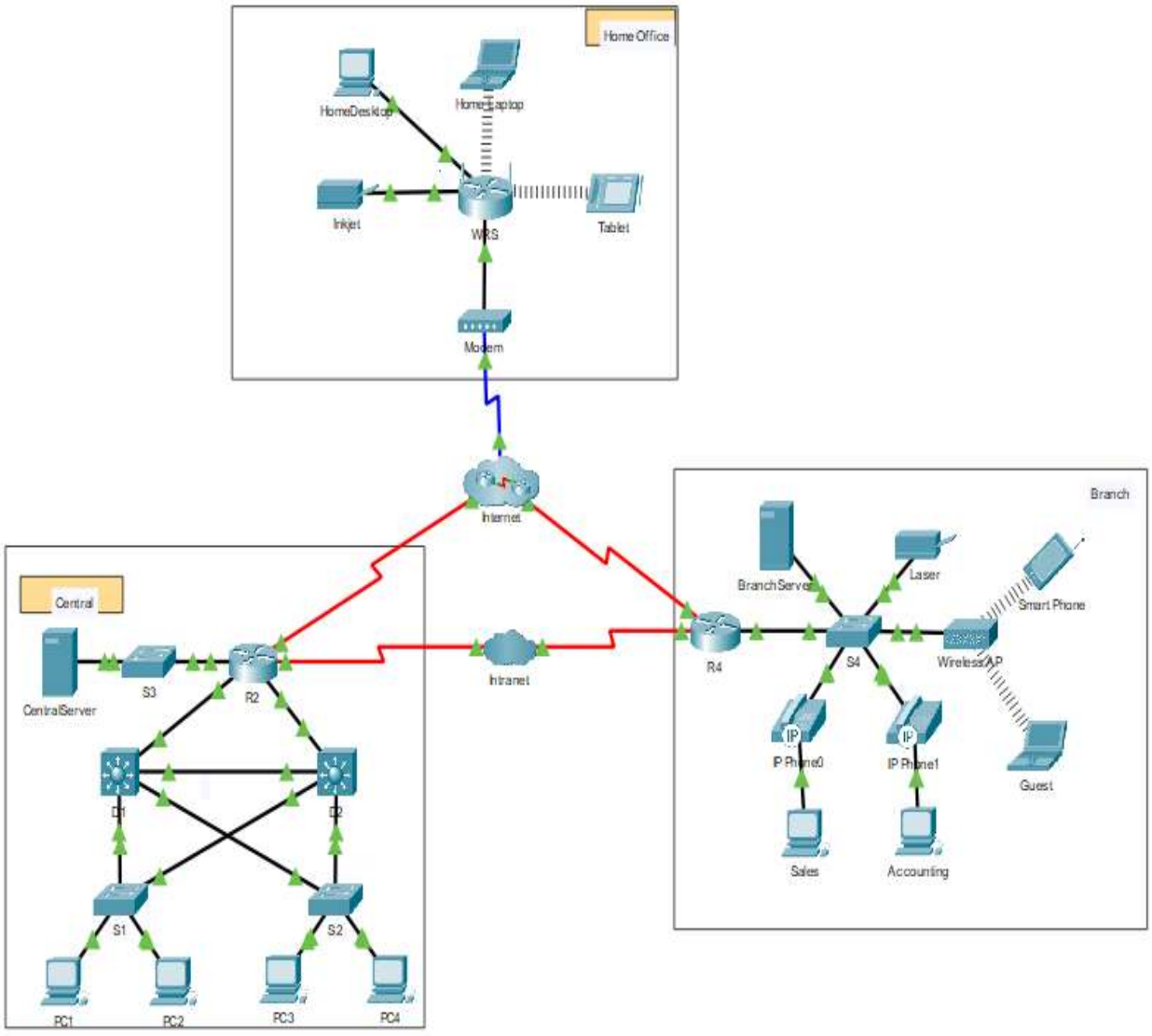


Figure 2: Internet, Intranet, and Extranet network in Packet Tracer

Observation

Configure the network as shown in Figure 20 using packet tracer.

Self-Assessment:

1. What are some challenges associated with managing and securing a WAN compared to a LAN?

2. List the limitations or constraints that you faced of simulating WAN networks in Packet Tracer?

Conclusion

Roll No.: **Date:**

Exp. No.: 6

Title: Implementation and Study of Sliding Window Protocols (Go-Back-N and Selective Repeat)

Learning Outcomes:

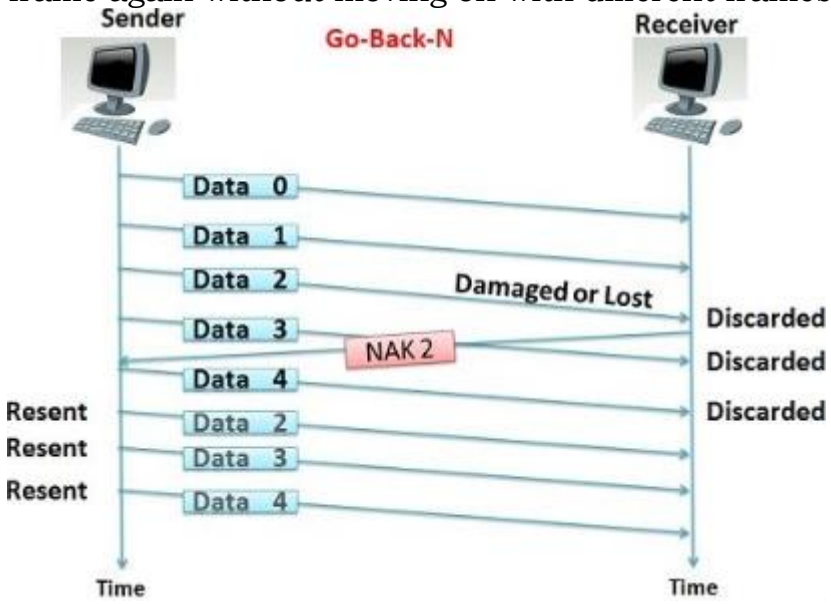
After Completion of this experiment, students will be able to

1) Students will be able to understand and simulate Go-Back-N and Selective Repeat protocols.

Theory:

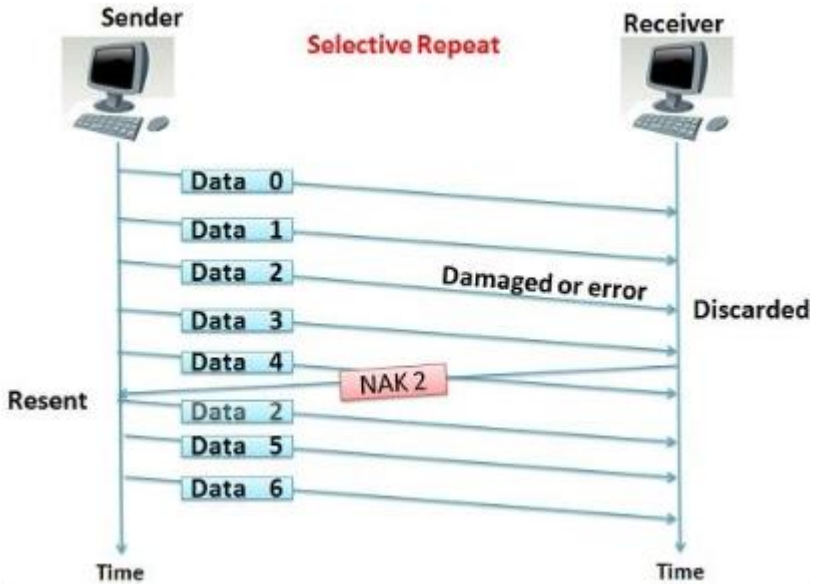
Go-Back-N Protocol

- In this protocol, the frames are sent again if they are lost while being transmitted.
- The size of the receiver buffer will be one, while the size of the sender buffer is predefined.
- The receiver cancels the frame if it gets corrupted; when the sender's timer for an acknowledgment to be received expires, the sender sends the same frame again without moving on with different frames.



Selective Repeat Protocol

- Selective repeat automatic repeat request works with the data link layer and uses the sliding window method to send frames.
- Only the corrupted frame during transmission is sent again in its execution, while the further requests get acknowledged.
- The window size in both the sender and receiver is the same.
- This protocol helps in saving on bandwidth as compared to **Go Back-N ARQ**, which processed the whole frames again without selectively choosing to send the faulty frames.



Procedure:

Implement Go-Back-N and Selective Repeat protocols using a programming language of your choice.

Algorithm:

Algorithm 1: Go-Back-N Sender

```
Function Sender is
    send_base ← 0;
    nextseqnum ← 0;
    while True do
        if nextseqnum < send_base + N then
            send packet nextseqnum;
            nextseqnum ← nextseqnum + 1;
        end
        if receive ACK n then
            send_base ← n + 1;
            if send_base == nextseqnum then
                stop timer;
            else
                start timer;
            end
        end
        if timeout then
            start timer;
            send packet send_base;
            send packet send_base + 1;
            ...
            send packet nextseqnum − 1;
        end
    end
end
```

Algorithm 2: Go-Back-N Receiver

```
function Receiver is
    nextseqnum ← 0;
    while True do
        if A packet is received then
            if The received packet is not corrupted and
             sequence_number == nextseqnum then
                deliver the data to the upper layer;
                send ACK nextseqnum;
                nextseqnum ← nextseqnum + 1;
            else
                /* If the packet is corrupted or out of
                   order, simply drop it                  */
                send ACK nextseqnum − 1;
            end
        else
    end
end
```

Self-Assessment:

- Frame an algorithm for the Selective Repeat protocol as done in the above-mentioned manner for the Go-Back-N protocol.
- Imagine a scenario where a Go-Back-N sender with a window size of 3 is communicating with a Selective Repeat receiver with a window size of 4. If the sender has sent frames 1 to 6, and the receiver has acknowledged frames 1 to 3, what actions will both the sender and receiver take?

Conclusion

Experiment 7: Packet Capturing and Analysis with Wireshark

Objective: Objective of this lab is to get familiar with the packet sniffer tool "Wireshark" and conduct the packet capturing and packet analysis for various tasks related to HTTP protocol.

Brief theory on Wireshark and HTTP protocol:

Refer the Documents given.

Tasks:

(I)Getting basic information on HTTP protocol:

Procedure:

1. Please check Wireshark icon on your PC (or check it through "Start" in Windows) and open the Wireshark.
2. Please get familiar with the Wireshark (if you haven't studied before) and look for the packet filter window on the top left corner in Wireshark and enter 'http' in the filter window. Please don't start the packet capture yet. Give some time (a minute or so)
3. Go through capture option and check the interface. You should have the LAN interface selected for packet capture.
4. Click on the start button and begin packet capturing.
5. In a separate window open a web browser and type the following: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html.
6. Stop the packet capture.

   From the packet listing window look at the HTTP GET/ response message and investigate the details by answering to the following questions:

   Q.1 Please note down the IP address of your machine and the destination machine (gaia.cs.umass).

   Q.2 What do you observe in the HTTP request message.

   Q.3 Write down the details of the HTTP response message such as status code, content length and file modified last time.

   To perform the following task, ensure that the browser cache is cleared. Go to Tools>options>clear history to clear the cache.

   (II) GET request/response interaction:

   Procedure: As performed earlier in the first task,

- ***Packet sniffing*:** start the Wireshark and enter the following link and run it on your browser**:**

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html.

- ***Stop packet capture*** and use 'http' as a filter to see only HTTP related packets and answer the following question.

Q.4 Write down your interesting observations for the GET request and response messages.

(III) **Getting long document from server:**

Procedure: To perform this task, ensure that cache is cleared. Check again your web browser history and clear it. (Follow the instruction advised in the previous task to clear the cache).

- Start Wireshark and enter the following link to retrieve a long file from UMass server:
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html.

- Stop the packet capture and filter the packets by entering 'http' in the packet filter window. Based on the above activity, answer the following questions:

Q.5 As you are retrieving long document, how many request packets are sent from the client to the server.

Q.6 Write down your understanding on how the HTTP long file is supported by underlying TCP.

Q.7 Inspect the packet which contains the status code and phrase of the response message.

(IV) Getting a password protected document from the server:

Procedure: In this task, you are trying to access a secured file stored on UMass server. Username is: *wireshark-students* and password is: network.

Start the packet capture and enter the following URL on the browser running on your machine:

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html.

Q.8 Write down your interesting observations for the request and response messages while performing this task.

Reference:

1. http://www.wireshark.org.
2. HTTP 1.1, Website: http://www.ietf.org/rfc/rfc2616.txt.
3. **J. F. Kurose and K.W. Ross, "Computer Networking: A Top-Down Approach featuring the Internet".**

Please note : To support your answers for the above mentioned questions, take snap shots of the observations. Attach the prints in your file with the above writeup.

Roll No.: **Date:**

Exp. No.: 8

Title: Implementation of Shortest Path Algorithm (Dijkstra's Algorithm)

Learning Outcomes:

After Completion of this experiment, students will be able to understand and implement Shortest Path Algorithm (Dijkstra's Algorithm)

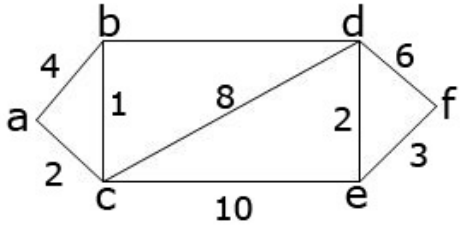
Theory:

Dijkstra's Shortest Path Algorithm is a popular algorithm for finding the shortest path between different nodes in a graph. Dijkstra's algorithm finds the solution for the single-source shortest path problems only when all the edge weights are non-negative on a weighted, directed graph.

Procedure:

Fix a node as the *initial node*; let the *distance of node "Y"* be the distance from the *initial node* to "Y". In Dijkstra's algorithm, some initial distance values are assigned, and these values are improved step by step. The algorithm procedure is given below:

1. A tentative distance value is assigned to every node; this value is set to zero for the initial node, and to infinity for all other nodes.
2. All nodes unvisited are marked, and the initial node is set as current. An *unvisited set* (a set of all the unvisited nodes) consisting of all the nodes is created.
3. For the current/initial node, take into account all the unvisited nearby nodes, and calculate their tentative distances. Make a comparison of the current assigned value and the newly calculated tentative distance; assign the smaller value.
4. A visited node is never to be checked again. So, after finishing above steps with all the neighbors of the current node, make that node as visited and remove is from the unvisited set.
5. Stop the algorithm if, when planning a route between two specific nodes, the destination node has been marked visited.
6. Also, stop the algorithm if, when planning a complete traversal, the smallest tentative distance among the nodes in the unvisited set is infinity. This case is a result of no connection between the initial node and the remaining unvisited nodes.
7. Find the unvisited node assigned with the smallest tentative distance value, and this will be the new "current mode". Go back to step 3, and continue.



Here, *a*, *b*, *c*, *d*, *e* and *f* are nodes of the graph, and the number between them are the distances of the graph. Now, using Dijkstra's algorithm we can find the shortest path between initial node *a* and the remaining vertices. For this, the adjacency matrix of the graph above is:

w(u,v)	a	b	c	d	d	f
a	0	4	2	INF	INF	INF
b	4	0	1	5	INF	INF
c	2	1	0	8	10	INF
d	INF	5	8	0	2	6
e	INF	INF	10	2	0	3
f	INF	INF	INF	6	3	0

Source Code in C:

```
#include<stdio.h>
#include<conio.h>
#include<process.h>
#include<string.h>
#include<math.h>
#define IN 99
#define N 6
int dijkstra(int cost[][N], int source, int target);
int main()
{
   int cost[N][N],i,j,w,ch,co;
   int source, target,x,y;
   printf("\t The Shortest Path Algorithm ( DIJKSTRA'S ALGORITHM in C \n\n");
   for(i=1;i< N;i++)
   for(j=1;j< N;j++)
   cost[i][j] = IN;
   for(x=1;x< N;x++)
   {
      for(y=x+1;y< N;y++)
      {
         printf("Enter the weight of the path between nodes %d and %d: ",x,y);
         scanf("%d",&w);
         cost [x][y] = cost[y][x] = w;
      }
      printf("\n");
   }
   printf("\nEnter the source:");
   scanf("%d", &source);
   printf("\nEnter the target");
```

```
    scanf("%d", &target);
    co = dijsktra(cost,source,target);
    printf("\nThe Shortest Path: %d",co);
}
int dijsktra(int cost[][N],int source,int target)
{
    int dist[N],prev[N],selected[N]={0},i,m,min,start,d,j;
    char path[N];
    for(i=1;i< N;i++)
    {
        dist[i] = IN;
        prev[i] = -1;
    }
    start = source;
    selected[start]=1;
    dist[start] = 0;
    while(selected[target] ==0)
    {
        min = IN;
        m = 0;
        for(i=1;i< N;i++)
        {
            d = dist[start] +cost[start][i];
            if(d< dist[i]&&selected[i]==0)
            {
                dist[i] = d;
                prev[i] = start;
            }
            if(min>dist[i] && selected[i]==0)
            {
                min = dist[i];
                m = i;
            }
        }
        start = m;
        selected[start] = 1;
    }
    start = target;
    j = 0;
    while(start != -1)
    {
        path[j++] = start+65;
        start = prev[start];
    }
    path[j]='\0';
```

```
    strrev(path);
    printf("%s", path);
    return dist[target];
}
```

Self-Assessment:

1. Enlist types of routing algorithms in Computer network?
2. Explain shortest path routing in Computer network?
3. What is static routing and dynamic routing?
4. What is spanning tree algorithm?
5. What is need of different routing algorithms in Computer network?

Conclusion