Jodhpur Institute of Engineering & Technology
Scheme and Syllabus
Branch: CSE (AI and ML)

Syllabus - V Semester
5AIML4-23: Computer Networks Lab

Credits: 1.5 **Max. Marks: 75(IA:45, ETE: 30)**
0L+0T+3P **End Term Exam: 3 Hours**

.

Unit	Objectives
1	Simulation of different type of LAN using NS2 simulator.
2	Simulation and Implementation of Network topologies i.e. Star, Bus, Ring etc. using NS2 simulator.
3	Implement various types of error correcting techniques. (Such as CRC-12, CRC-16 and CRC CCIP)
4	Implement the data link layer framing methods. (Such as character count, character-stuffing and bit stuffing)
5	Implement various sorting technique used in buffers.
6	Implement a simple data link layer that performs the flow control using the sliding window protocol, and loss recovery using the Go-Back-N mechanism
7	Implement leaky bucket algorithm.
8	Implement distance vector routing algorithm for obtaining routing tables at each node.
9	Implement Dijsktra's algorithm to compute the shortest path through a network.
10	Implement the concept of data encryption and data decryption.

Suggested References/Books:
1. Computer Networks -- Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education/PHI
2. Computer Networking: A Top-Down Approach - James Kurose , 7th Edition. Pearson
Education/PHI
3. An Engineering Approach to Computer Networks-S. Keshav, 2 nd Edition, Pearson Education
4. Data Communications and Networking – Behrouz A. Forouzan. Third Edition TMH.
5. Computer Networking: A Top-Down Approach - James Kurose - 7th edition. Pearson

EXPERIMENT 1

Overview of the Cisco Packet Tracer user interface:

Main Window
The main window of Cisco Packet Tracer is divided into several sections:

1. **Menu Bar**: Located at the top of the window, the menu bar provides access to various menus, such as File, Edit, View, and Help.

2. **Toolbar**: Below the menu bar, the toolbar provides quick access to frequently used tools and features, such as New, Open, Save, and Undo.

3. **Workspace**: The workspace is the main area where you design and build your network topology. You can drag and drop devices, connect them with cables, and configure their properties.

4. **Device Panel**: Located on the left side of the workspace, the device panel displays a list of available devices, such as routers, switches, PCs, and servers. You can drag and drop devices from this panel into the workspace.

5. **Physical View**: Located at the bottom of the workspace, the physical view displays a graphical representation of your network topology, including devices and cables.

6. **Logical View**: Located at the bottom of the workspace, the logical view displays a hierarchical representation of your network topology, including devices, protocols, and connections.

Device Properties

When you select a device in the workspace, its properties are displayed in the **Device Properties** panel, located on the right side of the window. The device properties panel allows you to configure various settings, such as:

Device Settings: Configure device-specific settings, such as IP addresses, subnet masks, and default gateways.

Interfaces: Configure interface settings, such as IP addresses, duplex modes, and speeds.

Protocols: Configure protocol settings, such as OSPF, EIGRP, and RIP.

Security: Configure security settings, such as access control lists (ACLs) and firewall rules.

Simulation
The **Simulation** tab, located at the top of the window, allows you to simulate network traffic and analyze network behavior. You can:
Start Simulation: Start the simulation and observe network traffic and behavior.
Stop Simulation: Stop the simulation and analyze the results.
Step Simulation: Step through the simulation one packet at a time.
Packet Capture: Capture and analyze packets as they traverse the network.

Tools
The **Tools** menu, located at the top of the window, provides access to various tools and features, such as:
Packet Debugger: Debug packets as they traverse the network.
Network Analyzer: Analyze network traffic and behavior.
Topology Summary: View a summary of your network topology.

Device Report: Generate a report on device configurations and settings.
https://skillsforall.com/course/getting-started-cisco-packet-tracer?courseLang=en-US#

Internet Control Message Protocol (ICMP)

Overview

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices, such as routers, to send error messages and operational information. It is integral to the Internet Protocol Suite and plays a crucial role in diagnostics and network management.

Purpose and Functions

1. **Error Reporting:**
    - **Destination Unreachable:** Informs the sender that the destination is unreachable.
    - **Time Exceeded:** Indicates that the Time to Live (TTL) of a packet has expired.
    - **Redirect:** Advises the sender to use a different route.
2. **Diagnostics:**
    - **Echo Request/Reply (Ping):** Used to test the reachability of a host and measure round-trip time.
    - **Timestamp Request/Reply:** Used to synchronize clocks between hosts.

ICMP Message Structure

ICMP messages are encapsulated within IP packets and consist of several fields:

- **Type:** Identifies the type of ICMP message.
- **Code:** Provides additional context for the message type.
- **Checksum:** Used for error-checking the ICMP header and data.
- **Rest of Header:** Contains type-specific information.
- **Data:** Contains the original IP header and the first 8 bytes of the original payload (used for error reporting).

Common ICMP Types and Codes

- **Type 0:** Echo Reply
- **Type 3:** Destination Unreachable
  - **Code 0:** Network Unreachable
  - **Code 1:** Host Unreachable
  - **Code 2:** Protocol Unreachable
- **Type 5:** Redirect
  - **Code 0:** Redirect Datagram for the Network
- **Type 8:** Echo Request
- **Type 11:** Time Exceeded
  - **Code 0:** TTL Exceeded in Transit

Usage and Applications

- **Ping Utility:** Uses ICMP Echo Request and Echo Reply messages to test network connectivity.
- **Traceroute Utility:** Utilizes ICMP Time Exceeded messages to trace the path packets take to a destination.
- **Network Troubleshooting:** ICMP messages help diagnose network problems by providing feedback on network issues.

Dynamic Host Configuration Protocol (DHCP)

Overview

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks. DHCP allows devices to obtain IP addresses and other configuration parameters dynamically.

Purpose and Functions

1. **IP Address Allocation:**
   - **Automatic Allocation:** DHCP server assigns a permanent IP address to a client.
   - **Dynamic Allocation:** DHCP server assigns an IP address to a client for a limited period (lease).
   - **Manual Allocation:** IP address is manually assigned by the network administrator, and the DHCP server only conveys it.
2. **Configuration Parameters Distribution:**
   - **Subnet Mask:** Defines the network and host portions of an IP address.
   - **Default Gateway:** Specifies the router IP address for outbound traffic.
   - **DNS Servers:** Provides IP addresses of DNS servers for hostname resolution.
   - **Other Parameters:** Includes domain name, lease duration, and other options.

DHCP Operation

DHCP operates based on a client-server model and follows a four-step process known as DORA:

1. **Discovery:**

    - The client broadcasts a DHCPDISCOVER message to locate DHCP servers.
2. **Offer:**
    - DHCP servers respond with a DHCPOFFER message, offering an IP address and configuration parameters.
3. **Request:**
    - The client replies with a DHCPREQUEST message, indicating acceptance of the offer.
4. **Acknowledgment:**
    - The DHCP server sends a DHCPACK message, finalizing the lease and configuration.

DHCP Message Structure

DHCP messages are encapsulated within UDP packets and include several fields:

- **Operation (op):** Indicates message type (e.g., request or reply).
- **Hardware Type (htype):** Specifies network interface type.
- **Hardware Address Length (hlen):** Length of the hardware address.
- **Transaction ID (xid):** Identifies the DHCP transaction.
- **Client IP Address (ciaddr):** Client's current IP address.
- **Your IP Address (yiaddr):** IP address assigned to the client.
- **Server IP Address (siaddr):** IP address of the DHCP server.
- **Gateway IP Address (giaddr):** IP address of the relay agent.
- **Client Hardware Address (chaddr):** Client's hardware address.
- **Options:** Various configuration options, including lease time and DHCP messages.

Usage and Applications

- **Network Initialization:** Automates the assignment of IP addresses and configuration settings to devices joining a network.
- **Network Management:** Simplifies the administration of IP address management and reduces configuration errors.
- **Roaming and Mobility:** Facilitates the dynamic reconfiguration of mobile devices as they move between networks.

Both ICMP and DHCP are essential protocols in the operation and management of IP networks, providing crucial services for error reporting, diagnostics, and automatic configuration. Understanding these protocols is vital for network engineers to design and maintain efficient and reliable networks