Ishaan Jain 06117702722 CSE-B

Experiment 1

AIM: Introduction to Networking Simulation Tools – Cisco Packet Tracer

Theory:

Introduction to Network Simulation Tools- Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco systems. It allows users to visualize and simulate complex networking environments, making it essential tool for students, network administrations and proffesionals studying for Cisco certification such as CCNA. It provides a virtual environment for creating, configuring and troubleshooting network topologies without the need for physical hardware.

Features of Cisco Packet Tracer:

- Device Simulation: Allows the creation of network topologies using virtual routers, switches, PC's, other networking devices.
- Networking Protocols: Supports a wide range of protocols including TCP/IP, DHCP, DNS, OSPF and more, enabling users to simulate real world networking scenarios.
- Interactive Learning: The tool provides a hand-on experience for learners, allowing them to configure devices and troubleshoot issues as if they were working with real equipment.
- Multi-user Mode: User can collaborate and simulate networks in real time with others over the internet.

Applications:

Learning and Practice: It is widely used for educational purpose > helping students gain practical networking skills.

2. Design of Network: Packet Tracer is ideal for planning and testing network designs before deploying them in real environment.

3. Troubleshooting: It can be used to troubleshoot network problems and test solutions in a risk free - virtual environment.

Ishaan Jain 06117702722 CSE-B

Experiment 2

AIM: To implement the DHCP onto the Network Topology using Cisco Packet Tracer.

Theory:

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that automatically assigns IP address and other network configuration parameters to devices on a network, allowing them to communicate efficiently. DHCP reduces the need for manual configuration, simplifying the management of large networks.

In a typical network, every device needs a unique IP address to communicate. DHCP automates the process by assigning IP address dynamically from a defined range or pool. This ensures that device can join the network without requiring manual IP configuration.

DHCP Operations:

DHCP works through a four-step process:

1. DHCP Discover: The client broadcast a request to find a DHCP server
2. DHCP offer: The DHCP server responds with an available IP address and network details.
3. DHCP request: The client request to lease the offered IP address
4. DHCP acknowledgement: The server confirms the lease and assigns the IP address.

Benefits of DHCP :

- Automatic IP address Assignment : DHCP simplifies the process of IP address automatically.
- Efficient use of IP addresses : It ensures efficient allocation of available IP address within a network.
- Centralized Network Management : DHCP allows administrators to manage IP settings from a centralized location, reducing configuration errors.

Experiment 3

AIM: To configure a single router in a network.

Theory:

A router is a networking device that forwards data packets between computer networks. Routers direct traffic on the internet by determining the best path for data to travel from the source to the determination. Configuring a router is essential for ensuring smooth communication across different network segments.

In this experiment, a single router will be configured to enable communication between multiple devices on the same or different networks. Routers use IP addresses to make forwarding decisions, routing packets to their intended decisions.

Basic Router Configuration Steps:

- Accessing the router: Connect to the router via a console cable or Telnet/SSH for remote access. Once connected, enter priveleged EXEC mode to begin configuration.
- Configuring Interfaces: Routers have multiple interfaces. Each interface must be assigned an IP address to allow data transmission. This includes enabling the interface after assigning IP.
- Setting Up Routing: Static or dynamic routing protocols can be used for communication between different network segments. Static routes are manually configured, while dynamic routes are automatic.
- Assigning Hostname and Password: To secure the router, administrations assign a hostname and password for accessing different modes.
- Saving Configuration: Once the router is configured, the changes should be saved to persist after a reboot.

Ishaan Jain 06117702722 CSE-B

Experiment 4

AIM: To configure WAN between two routers using Router-PT.

Theory:

A Wide Area Network (WAN) is a telecommunications network that extends over a large geographic area, connecting multiple local area networks (LAN). WAN's enable communication between devices across long distances, such as between different cities or even countries. Router play a crucial role in establishing WAN connections by forwarding data packets between networks.

Router-PT, a simulation tool in Cisco Packet Tracer, will be used to configure a WAN between two routers. The routers will be configured to exchange data across a simulated WAN link, enabling communication between two seperate networks.

WAN Configuration Overview:

1. Connecting the Routers: To create a WAN connection, both routers are physically or virtually connected via their serial interfaces. In simulation tools like Packet Tracer, this connection can be made using a serial cable between the serial ports of the two routers.
2. Configuring IP Address: Each router's serial interface must be assigned an IP Address from the same subnet to ensure proper communication over the WAN link
3. Enabling Interfaces: The serial interfaces of both routers must be enabled using the no shutdown command. By default, interfaces are in a "shutdown" state.

4. Setting Up Routing: Static or dynamic protocols are configured to enable data packet forwarding across the WAN. Static routing requires manually configuring routes on both routers, while dynamic routing automates the process

5. Testing Connectivity: After configuring WAN connection, ping tests are used to verify connectivity between the networks connected to each other.

Benefits of WAN configuration:

- Interconnectivity Across locations: WAN allows organizations or users to connect LAN's located far apart, enabling resources sharing and communication across distances.
- Centralized Management: WAN's facilitate centralized management and network administration for geographically distributed offices.
- Scalability: WAN configuration can easily be scaled to include more routers and networks.

Experiment 5

AIM: To configure static routing between three routers using Router-PT.

Theory:

Static Routing is a routing technique where routes are manually configured by the network administrator. Unlike dynamic routing, which automatically adjust to changes in the network, static routing requires the administrator to define specific routes for data packets to follow. This method is useful in small network or stable environments where the topology does not change frequently.

Key Concepts:

1. Router Configuration: Each router will have its interfaces assigned with unique IP address. Proper IP addressing is crucial for enabling communication between routers.
2. Static Routing Configuration: Configuration on each static routes hop IP addresses or the exit interfaces that leads to destination network.
3. Routing Table: Each router's routing table will be updated to reflect the new routes. This table helps the router determine the best path to forward packets to their destinations.
4. Testing Connectivity: After configuring static routes, ping tests will be conducted between devices connected to different routes to verify successful communications across the network.

Benefits of Static Routing:

- Predictable Routing Behaviour provides consistent and predictable packet forwarding.
- Low Overhead: Since there is no need for routing update, static routing consumes fewer network resources compared to dynamic routing protocols.
- Simplicity: It is a straightforward to setup, making it ideal for small networks.

EXPERIMENT 6

AIM: To implement the Dynamic Routing Protocols: RIP, IGRP using Cisco Packet Tracker.

Theory: Dynamic Routing Protocols like RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol), enable routers to automatically discover and maintain network paths. They help adjust routes in response to network changes ensuring efficient data transmission.

* RIP is a distance-vector protocol that determines the best route based on hop count, with a maximum of 15 hops allowed. It regularly broadcast the routing table to neighbouring routers, simplifying setup but potentially causing delays in larger networks. RIP version 2 adds support for subnet masks and multicasting, making it more effective for modern networks.

IGRP, a protocol developed by Cisco, uses a composite metric based on bandwidth, delay, load and reliability to select optimal routes. By combining these factors, IGRP offers better adaptability in networks with varying link speeds. However, IGRP is proprietary to Cisco devices, limiting its application in multi-vendor networks.

EXPERIMENT 7

AIM: To construct multiple router networks and implement the EIGRP Protocol.

Theory:

EIGRP (Enhanced Interior Gateway Routing Protocol) is a dynamic routing protocol developed by CISCO that combines the best features of distance-vector and link-state protocols, often termed as "hybrid" model. It uses a composite metric based on bandwidth, delay, load and reliability to determine optimal path for data transmission. EIGRP is more efficient than RIP as it supports faster convergence and has the ability to detect routing changes quickly. This protocol uses Autonomous Systems to group routers and uses the Diffusing update Algorithm (DUAL) for loop-free routing updates. EIGRP supports subnet masks and offers flexible network scalability, making it suitable for large, complex networks.

Ishaan Jain
06117702722
CSE-B

EXPERIMENT 8

AIM: To implement the Network Address Resolution (NAT) using Cisco Packet Tracker.

Theory: Network Address Translation is a process used to map private IP addresses to a public IP address or range of addresses, allowing devices on a local network to access external networks through a single IP. NAT is essential in conserving public IP addresses and providing security by hiding internal IP addresses from external networks. There are several types of NAT, including static NAT, dynamic NAT, PAT which are used based on specific network needs. In this experiment, we implement dynamic NAT, where a pool of public IP's is created and internal IP's are mapped to the available addresses in the pool.