EXPERIMENT 1

AIM: Introduction to cisco packet tracer and implementation of topology

Theory:

Cisco packet tracer is a network simulation tool that allows students and network professionals to design and simulate topologies without the need for physical hardware.
It provides an interactive learning environment to configure network devices as routers, switches & end devices.
Common tasks include assigning IP Addresses, configure routers & enabling basic services like DHCP.

Procedure:

1) **Initial Setup:**
Open Cisco Packet Tracer and sign in with your account (only required for the first-time setup).
2) **Star Topology:**
a. Place a 2960 switch on the workspace.
b. Add multiple PCs and connect them to the switch using copper straight-through cables.
c. Double-click each PC, go to Desktop → IP Configuration, and assign an IP address. Ensure all PCs are on the same network.
d. Rename each PC according to its IP address for clarity.
e. On any PC, open Command Prompt and use the ping command to check connectivity with other PCs.
3) **Mesh Topology:**
a. Place five PCs on the screen, each with a 2960 switch.
b. Connect each PC to its respective switch using copper straight-through cables.
c. Use copper crossover cables to interconnect the switches, forming a mesh topology.
d. Assign IP addresses to each PC and test the connection by pinging other devices.

EXPERIMENT 2

AIM: To implement DHCP in a network topology using Cisco Packet Tracer.

Theory;

Dynamic Host configuration Protocol (DHCP) is used to automatically assign IP Address to devices in a network, reducing the used for manual IP configuration.

Domain name system (DNS) translates Domain names into IP addresses, which allows users to access websites using easy to remember domain names rather than numerical IP Address.

DNS meanwhile acts as the phonebook of the internet. It allows user to use domain names instead of IP address. For instance, when a user types "www.example.com" DNS queries a DNS server to retrieve the corresponding IP Address, allowing the browser to connect to the correct server.

Procedure:

1) **Star Topology:**

a. Build a star topology (refer to Experiment 1 for steps).

b. Add a server and connect it to the switch using a copper straight-through cable.

c. Assign a static IP to the server.

d. Double-click the server, go to Services → DHCP, and enable the DHCP service. The starting IP address and subnet mask will auto-fill.

e. On each PC, change the IP configuration to DHCP. The server should now assign IPs automatically.

f. Test connectivity by pinging any PC on the network.

2) **Mesh Topology:**

a. Build a mesh topology (refer to Experiment 1 for steps).

b. Place a server and an additional switch, connecting the server to the switch using copper straight-through cables.

c. Use copper crossover cables to connect the new switch to the existing network switches.

d. Assign a static IP to the server.

e. Double-click the server, enable the DHCP service in the Services tab.

EXPERIMENT 3

AIM: To configure a single router in a network.

Theory:
Routers operate at Layer 3 of the OSI model the network layer, where they make forwarding decisions based on the destination IP address of a packet. In a network, routers facillitate communication between different sockets by routing paskets to the correct destination.

→ It can be configured manually in small networks by defining paths for packets. For example, the router is instructed that to reach a certain network, it should forward packets through a specific interface.

→ Connecting b/w different networks is tested using Ping, where devices on one network should be able to communicate with devices on another through the router.

Procedure:

1. Place a Router-PT on the workspace and connect it to a switch using a copper straight-through cable.
2. Connect multiple PCs to the switch using copper straight-through cables.
3. Double-click the router, go to Config → Interface → FastEthernet0/1 (or FastEthernet0/0):
   a. Enable the interface by checking "On".
   b. Assign an IP address and subnet mask.
4. Repeat the process for other interfaces if needed (e.g., FastEthernet0/2).
5. Assign static IPs to each PC by double-clicking them, going to Desktop → IP Configuration, and entering the IP and subnet mask.
6. Test connectivity by using the Command Prompt on a PC and pinging other PCs.

EXPERIMENT 4

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

Theory:

A wan enables communication b/w graphically distant exactions. The two routers must be configured with appropriate interfaces & WAN protocols to establish a reliable connection b/w the two networks.

→ Routers must be physically connected using ~~wan~~ WAN technologies, such as serial cables for leased lines.

→ Each router interface that connects to the WAN must have a public IP Addresses, which the internal LAN-facing interfaces will have private IP Addresses.

→ routers need to be configured with static or dynamic routes to forward packets from one LAN to the other over the WAN link.

→ After configuration, devices from one LAN should be able to communicate with devices in the other LAN, verifying the connecting through ping test.

Procedure:

1. Place two Router-PT devices and connect them using a serial DCE cable.
2. Connect each router to its respective switch using a copper straight-through cable, and then connect PCs to the switches.
3. Double-click each router, go to Config → Interface → Serial0/0/0 (or Serial0/0/1): a. Enable the interface by checking "On".
   b. Assign an IP address and subnet mask. c. On one router, set the clock rate for the serial connection.
4. For LAN communication, configure the FastEthernet interfaces:
   a. Go to Config → Interface → FastEthernet0/1 and assign an IP address. b. Ensure the interface is enabled by checking "On".
5. On each router, go to Config → Routing and set static routes to allow communication between networks by entering the destination network, subnet mask, and next hop.
6. Test the WAN connection by pinging between PCs connected to different routers.

EXPERIMENT 5

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

Theory:

In static routing the network administrator manually adds routes to the router's routing table. For each destination network, a specific route is defined, & indicating the next hop that should be used to reach the destination.

→ Since the routes are manually defined, there is full control over how trafic is routed.

→ static routes doesn't require routers to exchange routing information, reducing bandwidth usage & processor load.

Procedure:

1. Place three Router-PT devices on the workspace and connect them using serial DCE cables.
2. Connect each router to its respective switch using copper straight-through cables, and connect PCs to each switch.
3. For each router, go to Config → Interface → Serial0/0/0 (or relevant interface) and assign IP addresses, subnet masks, and set the clock rate for one of the routers in each serial connection.
4. Configure the FastEthernet interfaces for LAN communication:
   a. Go to Config → Interface → FastEthernet0/1 on each router and assign an IP address.
   b. Ensure the interface is enabled by checking "On".
5. Configure static routes on each router by going to Config → Routing → Static and adding routes to other networks with the destination network, subnet mask, and next hop.
6. Assign static IPs to each PC and test the network by pinging across the devices connected to different routers.

EXPERIMENT 6

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

Theory:

Dynamic routing, protocols like RIP & IGRP, enable routers to automatically discover and maintain network changes ensuring efficient data transmission.

→ RIP is a distance-Vector Protocol that determines the best route based on heap count, with a maximum of 15 haps allowed. It regularly broadcast the routing table to neighbouring routers, simplifying setup that potentially causing delays in larger networks.

~~RIP vers~~

→ IGRP, a protocol developed by Cisco, uses a composite metric based on bandwidth, delay used & relaitibility to select optimal routes.

PROCEDURE-

For RIP Implementation:

1. Open Cisco Packet Tracer and create a network topology with multiple routers.
2. Connect routers using appropriate cables (e.g., serial or Ethernet).
3. Click on each router and enter the CLI (Command-Line Interface).
4. Enter global configuration mode: enable then configure terminal.
5. Enable RIP on each router: router rip.
6. Define the version of RIP: version 2 (if using RIP v2).
7. Configure network statements for connected networks: network [network address].
8. Exit RIP configuration: exit.
9. Verify RIP routing table: show ip route.
10. Test the RIP configuration by pinging from one router to another.

EXPERIMENT 7

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

Theory:

EIGRP is a dynamic routing protocol developed by Cisco that compiles the best features of distance-vector & Link state protocols, often termed as hybrid model. It uses composite metric based on bandwidth delay, loaded and reliability to determine optimal path for data transmission. EIGRP is more sufficient 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.

PROCEDURE-

1. Place multiple routers (e.g., Router-PT1, Router-PT2) and connect them using serial or Ethernet cables.
2. On each router, configure interfaces with IP addresses and subnet masks (e.g., Router-PT1: 192.168.1.1/24, Router-PT2: 192.168.2.1/24).
3. On each router, enter global config mode: `configure terminal`.
4. Enable EIGRP on each router with the command: `router eigrp <AS_number>`.
5. Define the networks to participate in EIGRP by using `network <network_address> <wildcard_mask>`.
6. On each router, verify EIGRP configuration with `show ip eigrp neighbours` and show ip route.
7. Test inter-router connectivity by pinging between devices on different networks.
8. Optionally, configure EIGRP settings like passive interfaces, delay, or bandwidth for optimisation.

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 Address 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, dynamic NAT, PAT which are used based on specific network needs.

PROCEDURE-

1. Place a router and switch, then connect PCs to the switch with copper straight-through cables.
2. On the router, configure **FastEthernet0/1** (inside) and **FastEthernet0/0** (outside) interfaces with IP addresses and subnet masks.
3. On the router CLI, enter global config mode: configure terminal and set interfaces with ip nat inside and ip nat outside.
4. Define a NAT pool with ip nat pool NAT_POOL 203.0.113.2 203.0.113.10 netmask 255.255.255.248.
5. Create an access list with access-list 1 permit 192.168.1.0 0.0.0.255 to match internal IPs.
6. Enable NAT with ip nat inside source list 1 pool NAT_POOL.
7. Assign static IPs to PCs (e.g., 192.168.1.x/255.255.255.0) and set the default gateway to 192.168.1.1.
8. Test connectivity by pinging between PCs and verify NAT with show ip nat translations on the router.