PCU

PCET's
Pimpri
Chinchwad
University

Learn | Grow | Achieve

Pimpri Chinchwad Education Trust's

Pimpri Chinchwad University

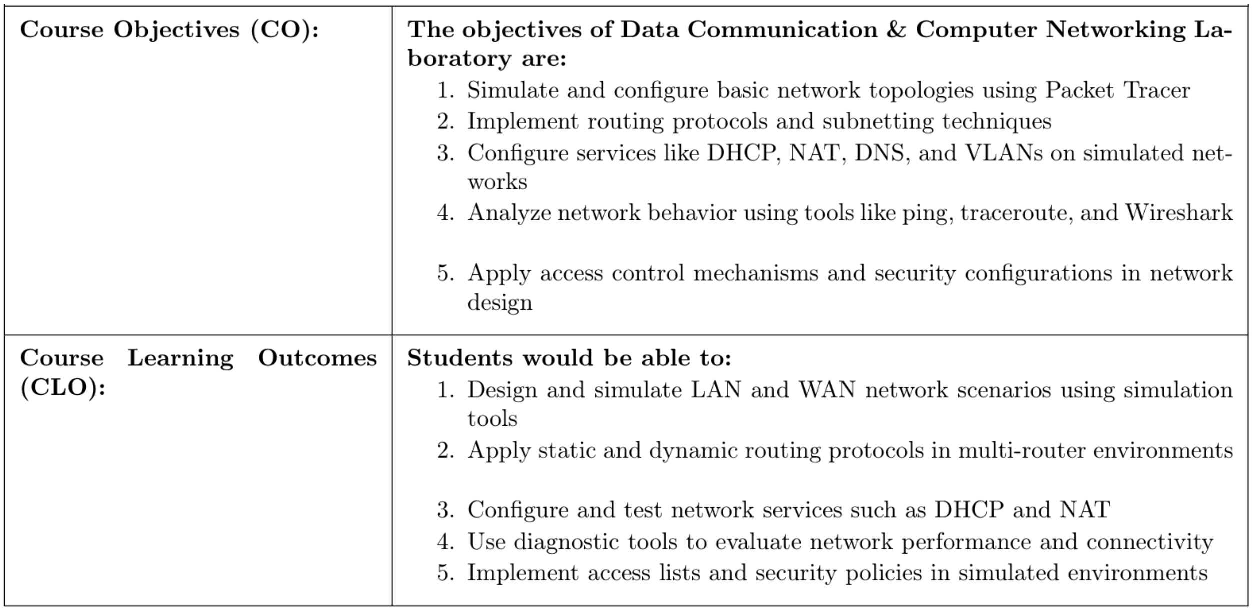
Sate Maval, Pune

Department of CSE-(AI&DS)

DCCN Lab Manual

Practical Number	Practical Title	Week Number	Details	CLO	Hours
1	Practical 1	1	Create a LAN with switches, routers, and PCs, Assign IP addresses and verify connectivity using ping	CLO1	2
2	Practical 2	2	Connect multiple routers and configure routing tables	CLO2	2
3	Practical 3	3	Configure RIP and OSPF; observe routing table changes	CLO2	2
4	Practical 4	4	Divide a class C network into multiple subnets, Implement subnet plan in a simulated network	CLO3	2
5	Practical 5	5	Use switches and routers to segment networks	CLO3	2
6	Practical 6	6,7	Set up a DHCP server to allocate dynamic IPs	CLO4	4
7	Practical 7	8,9	Implement Static and Dynamic NAT using a router	CLO4	4
8	Practical 8	10,11	Use Standard and Extended ACLs to permit/deny traffic	CLO5	4
9	Practical 9	12,13	Set up SSID, WPA2 security; simulate mobile client access	CLO5	4
10	Practical 10	14	Configure DNS mappings and simulate HTTP access	CLO5	2
11	Practical 11	15	Capstone Project (Smart Devices Case Study)	CLO5	2
Total Hours					**30**

By Dr. Manisha V. Khadse



Course Objectives (CO):	**The objectives of Data Communication & Computer Networking Laboratory are:** 1. Simulate and configure basic network topologies using Packet Tracer 2. Implement routing protocols and subnetting techniques 3. Configure services like DHCP, NAT, DNS, and VLANs on simulated networks 4. Analyze network behavior using tools like ping, traceroute, and Wireshark 5. Apply access control mechanisms and security configurations in network design
Course Learning Outcomes (CLO):	**Students would be able to:** 1. Design and simulate LAN and WAN network scenarios using simulation tools 2. Apply static and dynamic routing protocols in multi-router environments 3. Configure and test network services such as DHCP and NAT 4. Use diagnostic tools to evaluate network performance and connectivity 5. Implement access lists and security policies in simulated environments

Guidelines for Laboratory /Term Work Assessment

Continuous assessment of laboratory work should be based on overall performance of Laboratory assignments by a student. Each Laboratory assignment assessment will assign credit/marks based on parameters, such as timely completion, performance, innovation, efficient codes, punctuality .

Operating System recommended: -64-bit Open-source Linux/Window or its derivative
Programming tools recommended: - Open-Source/C/C++/JAVA Programming tool like G++/GCC, Wireshark/Ethereal and Packet Tracer

Note: maintain Github account and Drive

Guidelines for Oral Examination Oral examination

Relevant questions may be asked at the time of evaluation to test the student's understanding of the fundamentals, effective and efficient implementations in term work. This will encourage, transparent evaluation and fair approach, and hence will not create any uncertainty or doubt in the minds of the students.

Practical 1: Basic LAN Configuration

Practical Title: Create a LAN with switches, routers, and PCs, Assign IP addresses and verify connectivity using ping

Aim: To design and configure a basic Local Area Network (LAN) using Cisco Packet Tracer and to verify network connectivity.

Objective:

- To understand the basic functions of switches and routers.
- To design a simple network topology using Cisco Packet Tracer.
- To manually assign IP addresses to PCs and router interfaces.
- To verify end-to-end connectivity using the `ping` command.

Theory: A **switch** is a networking device that connects multiple devices within a LAN. It operates at Layer 2 (Data Link Layer) of the OSI model and uses MAC addresses to forward data packets to the correct destination port. A **router** connects multiple networks and operates at Layer 3 (Network Layer). Its primary function is to determine the best path for data to travel between different networks. It also serves as a **default gateway**, allowing devices within a LAN to access external networks.

A **straight-through cable** is used to connect different devices (e.g., PC to Switch), while a **crossover cable** connects similar devices (e.g., Switch to Switch).

Steps:

1. **Create the Network Topology:**
    - Open Cisco Packet Tracer.
    - Drag and drop 2 PCs, 1 Switch (2960), and 1 Router (1841) from the device menu to the workspace.
    - Use the "Connections" tool (the lightning bolt icon) and select the copper straight-through cable.
    - Connect PC0 to the Switch, and PC1 to the Switch.
    - Connect the Switch to the Router. The topology should look like this:
2. **Assign IP Addresses:**
    - **PC0:**
        - Click on PC0 > **Desktop** > **IP Configuration**.
        - Enter **IP Address:** 192.168.1.2
        - Enter **Subnet Mask:** 255.255.255.0
        - Enter **Default Gateway:** 192.168.1.1
    - **PC1:**
        - Click on PC1 > **Desktop** > **IP Configuration**.
        - Enter **IP Address:** 192.168.1.3
        - Enter **Subnet Mask:** 255.255.255.0

        - Enter **Default Gateway:** 192.168.1.1
    - **Router:**
        - Click on the Router > **CLI** tab.

Enter the following commands:

```
Router>en
Router#conf t
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#show ip interface brief
```

3. **Verify Connectivity:**
    - Click on PC0 > **Desktop** > **Command Prompt**.
    - Type `ping 192.168.1.3` to check connectivity to PC1. A successful ping will show `Reply from 192.168.1.3`.
    - Type `ping 192.168.1.1` to check connectivity to the router. A successful ping will show `Reply from 192.168.1.1`.

Conclusion: In this practical, a basic LAN was successfully created using Cisco Packet Tracer. IP addresses were assigned to all devices, and connectivity was verified using the `ping` command, confirming that the network is functioning correctly.

Viva / Oral Questions:

1. What is the difference between a switch and a router?
2. What is the function of a default gateway? What happens if you don't assign one?
3. Explain the purpose of the `ping` command.
4. When do you use a straight-through cable versus a crossover cable?
5. What layer of the OSI model does a router operate on?

Practical 2: Router-to-Router Routing

Practical Title: Connect multiple routers and configure routing tables.

Aim: To connect two different networks using two routers and configure static routing to enable communication between devices on different networks.

Objective:

- To understand how to connect multiple routers in a network.
- To configure static routes on routers to enable inter-network communication.
- To verify connectivity between devices on different networks.

Theory: A **router** is a Layer 3 device that connects multiple networks. For a router to forward a packet to a different network, it must have a route to that network in its **routing table**. The routing table stores information about the paths to various destinations. In **static routing**, an administrator manually configures these routes.

Steps:

1. **Create the Network Topology:**
    - Open Cisco Packet Tracer.
    - Drag and drop two LANs from Practical 1, each with a PC, a switch, and a router.
    - Connect Router0 and Router1 using a serial cable. You will need to add a HWIC-2T module to each router. Turn off the router, drag the module, then turn it back on.
    - The topology should look like this:
2. **Assign IP Addresses:**
    - **LAN 1 (Network 192.168.1.0/24):**
        - PC0: 192.168.1.2, Subnet Mask 255.255.255.0, Default Gateway 192.168.1.1
        - Router0 (FastEthernet0/0): 192.168.1.1, Subnet Mask 255.255.255.0
    - **LAN 2 (Network 192.168.2.0/24):**
        - PC1: 192.168.2.2, Subnet Mask 255.255.255.0, Default Gateway 192.168.2.1
        - Router1 (FastEthernet0/0): 192.168.2.1, Subnet Mask 255.255.255.0
    - **Router-to-Router Link (Network 10.0.0.0/24):**
        - Router0 (Serial0/0/0): 10.0.0.1, Subnet Mask 255.255.255.0
        - Router1 (Serial0/0/0): 10.0.0.2, Subnet Mask 255.255.255.0
3. **Configure Static Routes:**
    - **On Router0 (to reach Network 192.168.2.0):**
        - Click on Router0 > **CLI** tab.
        - Enter the command: `Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2`
    - **On Router1 (to reach Network 192.168.1.0):**

        - Click on Router1 > **CLI** tab.
        - Enter the command: `Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1`

4. **Verify Connectivity:**
    - On PC0, open the **Command Prompt**.
    - Type `ping 192.168.2.2` to verify connectivity to PC1. The ping should be successful after the static routes are configured.

Conclusion: By manually configuring static routes on both routers, communication was established between two separate networks. This practical demonstrated how routing tables enable packets to be forwarded between different network segments.

Viva / Oral Questions:

1. What is the purpose of a routing table?
2. What is the difference between static and dynamic routing?
3. Why can't PC0 ping PC1 without the static route configuration?
4. What is the next-hop address in a static route?
5. How does a router determine the best path for a packet?

Practical 3: Dynamic Routing with RIP and OSPF

Practical Title: Configure RIP and OSPF; observe routing table changes.

Aim: To configure dynamic routing protocols like RIP and OSPF and observe how routers automatically exchange routing information.

Objective:

- To understand the concepts of RIP and OSPF.
- To configure RIP on a network topology.
- To configure OSPF on the same network topology.
- To observe how the routing table is updated automatically.

Theory: Dynamic routing protocols allow routers to automatically learn about network paths from other routers. This is more scalable than static routing. **RIP (Routing Information Protocol)** is a distance-vector protocol that uses hop count as its metric. **OSPF (Open Shortest Path First)** is a link-state protocol that uses a more sophisticated metric and is more scalable.

Steps:

1. **Create the Network Topology:**
    - Use the same two-router topology from Practical 2. Ensure all IP addresses are configured correctly on the interfaces.
2. **Configure RIP Routing:**
    - **On Router0:**
        - Click Router0 > **CLI** tab.

Enter the following commands:

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
```

- **On Router1:**
    - Click Router1 > **CLI** tab.

Enter the following commands:

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.2.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
```

3. **Verify RIP Configuration:**
   - On either router, use the command `show ip route` to view the routing table. You should see routes learned via RIP, indicated by an 'R'.
4. **Configure OSPF Routing (alternative configuration):**
   - **Remove RIP configuration first:**
     - On both routers, enter `no router rip`.
   - **On Router0:**

Enter the following commands:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
```

   - **On Router1:**

Enter the following commands:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
```

5. **Verify OSPF Configuration:**
   - On either router, use the command `show ip route` again. You should now see routes learned via OSPF, indicated by an 'O'.
   - Ping from PC0 to PC1 to confirm connectivity.

Conclusion: This practical successfully demonstrated the configuration of two dynamic routing protocols, RIP and OSPF. By observing the routing tables, we saw how these protocols automatically discover and populate network paths, simplifying network management compared to static routing.

Viva / Oral Questions:

1. What is the main difference between RIP and OSPF?
2. What is a "hop count" in the context of RIP?
3. Why is OSPF considered more scalable than RIP?
4. What is the purpose of the "area" in OSPF configuration?
5. How do dynamic routing protocols handle network changes, such as a link going down?

Practical 4: Subnetting Implementation

Practical Title: Divide a class C network into multiple subnets, Implement subnet plan in a simulated network.

Aim: To divide a given Class C IP address space into multiple subnets and implement this subnet plan in a Cisco Packet Tracer simulation.

Objective:

- To understand the concept of subnetting.
- To create a subnetting plan for a Class C network.
- To configure devices with the appropriate IP addresses and subnet masks for each subnet.
- To verify communication within and between the created subnets.

Theory: Subnetting is the process of dividing a single large network into smaller, more manageable sub-networks. This improves network efficiency, security, and scalability. For a Class C network (e.g., `192.168.1.0/24`), we can borrow bits from the host portion of the IP address to create new subnets. The subnet mask determines how many bits are used for the network and how many for the host.

Steps:

1. **Subnetting Plan:**
   - Given the network `192.168.1.0/24`.
   - To create 4 subnets, we need to borrow 2 bits from the host portion (22=4 subnets).
   - The new subnet mask will be `255.255.255.192` (binary `11000000`).
   - The subnets will be:
     - Subnet 1: `192.168.1.0/26` (Network Address: `192.168.1.0`, Host Range: `192.168.1.1` to `192.168.1.62`, Broadcast: `192.168.1.63`)
     - Subnet 2: `192.168.1.64/26` (Network Address: `192.168.1.64`, Host Range: `192.168.1.65` to `192.168.1.126`, Broadcast: `192.168.1.127`)
     - Subnet 3: `192.168.1.128/26` (Network Address: `192.168.1.128`, Host Range: `192.168.1.129` to `192.168.1.190`, Broadcast: `192.168.1.191`)
     - Subnet 4: `192.168.1.192/26` (Network Address: `192.168.1.192`, Host Range: `192.168.1.193` to `192.168.1.254`, Broadcast: `192.168.1.255`)

2. **Create the Network Topology:**
    - Use Cisco Packet Tracer to create a topology with one router, and two switches, each with a few PCs connected to it. Connect the switches to different FastEthernet ports on the router.
3. **Assign IP Addresses and Subnet Masks:**
    - **Router:**
        - Configure `FastEthernet0/0` with an IP address from Subnet 1, e.g., `192.168.1.1` with subnet mask `255.255.255.192`.
        - Configure `FastEthernet0/1` with an IP address from Subnet 2, e.g., `192.168.1.65` with subnet mask `255.255.255.192`.
    - **PCs on Subnet 1:**
        - Assign IP addresses from `192.168.1.2` to `192.168.1.62` with subnet mask `255.255.255.192`. The default gateway for these PCs will be `192.168.1.1`.
    - **PCs on Subnet 2:**
        - Assign IP addresses from `192.168.1.66` to `192.168.1.126` with subnet mask `255.255.255.192`. The default gateway for these PCs will be `192.168.1.65`.
4. **Verify Connectivity:**
    - Ping from a PC in Subnet 1 to another PC in the same subnet (e.g., ping `192.168.1.3`).
    - Ping from a PC in Subnet 1 to its default gateway (e.g., ping `192.168.1.1`).
    - Ping from a PC in Subnet 1 to a PC in Subnet 2 (e.g., ping `192.168.1.67`). This verifies that the router is correctly routing between the subnets.

Conclusion: This practical successfully demonstrated the process of subnetting a Class C network. By dividing the network into smaller segments and configuring the router and hosts accordingly, we were able to establish and verify communication both within and between the newly created subnets.

Viva / Oral Questions:

1. What is the primary purpose of subnetting?
2. How do you calculate the number of subnets and hosts per subnet from a given subnet mask?
3. Explain how a router uses the subnet mask to determine which network a packet belongs to.
4. What is a broadcast address, and why is it important in subnetting?
5. What are the advantages of using subnetting in a large organization?

Practical 5: Network Segmentation with Switches and Routers

Practical Title: Use switches and routers to segment networks.

Aim: To understand and implement network segmentation using switches and routers to improve network performance and security.

Objective:

- To distinguish between collision and broadcast domains.
- To use a switch to create separate collision domains.
- To use a router to create separate broadcast domains.
- To understand the role of VLANs (Virtual LANs) in network segmentation.

Theory: Network segmentation is the process of dividing a computer network into smaller sub-networks. This reduces network traffic, improves security, and simplifies management. A **switch** segments a network into **collision domains**, meaning that devices connected to different switch ports do not compete for the same network medium, thereby reducing collisions. A **router** segments a network into **broadcast domains**, preventing broadcast traffic from one network from reaching another.

Steps:

1. **Create the Network Topology:**
   - Open Cisco Packet Tracer.
   - Create a simple topology with two PCs connected to a switch.
   - Add another switch and two more PCs, and connect this new switch to a different port on the first switch.
   - Add a router and connect the first switch to the router. The topology should demonstrate how switches and routers create different domains.
2. **Observe Collision and Broadcast Domains:**
   - On the initial topology (two PCs connected to a single switch), send a broadcast packet from one PC (using the "Add Simple PDU" tool). Observe that the broadcast packet is sent to all other devices connected to the same switch.
   - Now, connect the router to the switch. The router will prevent broadcast packets from passing through to other networks, showing that the router is the boundary of the broadcast domain.
   - Similarly, any data sent from one PC to another via the switch will be a unicast, not a collision, demonstrating how the switch has created separate collision domains for each connected device.
3. **Implement VLANs (Optional, but recommended):**
   - On the switch, go to the **CLI** tab and configure two VLANs, for example, VLAN 10 for "Sales" and VLAN 20 for "Marketing".
   - Assign specific switch ports to each VLAN.

    - Configure the router with a "router on a stick" setup to enable communication between the VLANs.

Conclusion: This practical demonstrated the fundamental principles of network segmentation. We observed how switches break up a network into multiple collision domains and how routers create separate broadcast domains. This knowledge is crucial for designing efficient and secure network architectures.

Viva / Oral Questions:

1. What is a collision domain, and how does a switch help reduce collisions?
2. What is a broadcast domain, and how does a router affect it?
3. How do VLANs provide an additional layer of network segmentation?
4. What is the "router on a stick" configuration, and why is it used?
5. Why is network segmentation important for security?

Practical no -6: Setup a DHCP Server to Allocate Dynamic IPs (Cisco Packet Tracer)

Aim:

To configure a Cisco Router as a DHCP server so that it dynamically allocates IP addresses to client PCs in a network using Cisco Packet Tracer.

Requirements:

1. Cisco Packet Tracer software.
2. One router, one switch, and multiple PCs.
3. Proper cabling between devices.

Procedure:

Step 1: Network Topology

- Drag and drop:
  - 1 Router (e.g., 2911)
  - 1 Switch
  - 2–3 PCs
- Connect:
  - Router ↔ Switch (straight cable)
  - PCs ↔ Switch (straight cables)

Step 2: Assign IP on Router Interface

Click on Router → CLI tab, then enter:

```
Router> enable
Router# configure terminal
Router(config)# interface gig0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 3: Configure DHCP on Router

```
Router(config)# ip dhcp pool LAB-NET
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
```

Step 4: Exclude IP Addresses

Exclude addresses you don’t want to assign dynamically (e.g., router’s IP):

```
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Step 5: Configure PCs

On each PC:

- Open Desktop tab → IP Configuration.
- Select DHCP instead of Static.

Step 6: Verify DHCP Allocation

On PC → Command Prompt → type:

```
ipconfig
```

Each PC should get a unique IP from the router in range 192.168.1.11 – 192.168.1.254.

Output:

PCs successfully receive dynamic IP addresses from the DHCP-enabled router.

Result/Conclusion:

Thus, a Cisco Router was configured as a DHCP Server in Packet Tracer, and PCs were automatically assigned IP addresses.

Viva Questions with Answers

1. Q: What is DHCP?
   A: DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network configurations (like gateway, DNS) to client devices.
2. Q: Why do we use DHCP instead of manual IP assignment?
   A: DHCP reduces manual work, prevents IP conflicts, ensures centralized management, and makes it easy to scale large networks.
3. Q: What is the default port number used by DHCP?
   A: DHCP uses UDP port 67 (server) and UDP port 68 (client).
4. Q: What are the different types of IP allocation in DHCP?
   A:
   - Dynamic Allocation: IP is leased temporarily and can change.
   - Automatic Allocation: Permanent assignment from a range.
   - Manual Allocation (Static Binding): Specific IP assigned to a specific device (based on MAC address).
5. Q: Explain the DHCP working process.

Practical 7: Static and Dynamic NAT

Practical Title: Implement Static and Dynamic NAT using a router.

Aim: To configure and verify both Static and Dynamic NAT (Network Address Translation) on a Cisco router to allow devices on a private network to access the internet.

Objective:

- To understand the purpose of NAT.
- To configure Static NAT to map a private IP to a public IP.
- To configure Dynamic NAT to allow multiple private IPs to share a pool of public IPs.
- To verify the NAT translation using the `show` command.

Theory: Network Address Translation (NAT) is a process that translates private IP addresses into public IP addresses. This is essential for conserving public IP addresses and for security. **Static NAT** creates a one-to-one mapping between a private IP and a public IP, which is useful for servers. **Dynamic NAT** translates multiple private IP addresses to a pool of public IP addresses, allowing multiple devices to share a smaller number of public IPs.

Steps:

1. **Create the Network Topology:**
   - Open Cisco Packet Tracer.
   - Create a topology with a private LAN (PC, Switch, Router) and connect the router to a "Cloud" (representing the internet) and then to a web server.
   - The router will act as the NAT device.
2. **Assign IP Addresses:**
   - **Private LAN:**
     - PC: `192.168.1.10`, Subnet Mask `255.255.255.0`, Default Gateway `192.168.1.1`
     - Router (FastEthernet0/0): `192.168.1.1`, Subnet Mask `255.255.255.0`
   - **Public Network (Cloud to Server):**
     - Router (FastEthernet0/1): `209.165.200.225`, Subnet Mask `255.255.255.224`
     - Server: `209.165.200.226`, Subnet Mask `255.255.255.224`
3. **Configure Static NAT:**
   - **On the Router:**
     - Set the inside and outside interfaces: `interface fastethernet 0/0` > `ip nat inside`, `interface fastethernet 0/1` > `ip nat outside`.
     - Create the static mapping: `ip nat inside source static 192.168.1.10 209.165.200.227`

4. **Configure Dynamic NAT (alternative to Static NAT):**
    - **On the Router:**
        - Define the private IP address range: `access-list 1 permit 192.168.1.0 0.0.0.255`
        - Define the public IP address pool: `ip nat pool public-ips 209.165.200.228 209.165.200.229 netmask 255.255.255.224`
        - Create the dynamic mapping: `ip nat inside source list 1 pool public-ips overload`
5. **Verify NAT:**
    - From the PC, ping the public server (`ping 209.165.200.226`).
    - On the router, use the command `show ip nat translations` to view the active NAT mappings.

Conclusion: This practical successfully demonstrated the implementation of both Static and Dynamic NAT. We were able to translate private IP addresses into public ones, allowing a device on a private network to communicate with a public server, showcasing the essential role of NAT in modern networks.

Viva / Oral Questions:

1. What is the primary function of NAT?
2. What is the difference between Static NAT and Dynamic NAT?
3. What is NAT Overload (PAT), and why is it important?
4. How does NAT help to conserve public IP addresses?
5. What are the inside and outside interfaces in NAT configuration?

Practical 8: Access Control Lists (ACLs)

Practical Title: Use Standard and Extended ACLs to permit/deny traffic.

Aim: To configure and implement both Standard and Extended Access Control Lists (ACLs) to control network traffic on a Cisco router.

Objective:

- To understand the purpose of ACLs in network security.
- To configure a Standard ACL to filter traffic based on source IP address.
- To configure an Extended ACL to filter traffic based on source/destination IP, protocol, and port number.
- To apply ACLs to router interfaces and test their functionality.

Theory: An **Access Control List (ACL)** is a numbered or named list of rules that a router uses to control which packets can pass through its interfaces. **Standard ACLs** filter traffic based only on the source IP address. They are generally placed close to the destination. **Extended ACLs** provide more granular control, allowing filtering based on source/destination IP, protocol (e.g., TCP, UDP), and port number. They should be placed as close to the source as possible.

Steps:

1. **Create the Network Topology:**
   - Use a topology with two routers connecting two separate LANs (similar to Practical 2). A third PC can be added to the second LAN to demonstrate the ACL filtering.
2. **Configure a Standard ACL:**
   - **Aim:** Block PC0 (`192.168.1.10`) from reaching the server on the other network.
   - **On Router1 (the router connected to the destination):**
     - Enter the command: `access-list 1 deny 192.168.1.10 0.0.0.0`
     - Enter the command: `access-list 1 permit any`
     - Apply the ACL to the interface: `interface fastethernet 0/0` > `ip access-group 1 in`
3. **Verify the Standard ACL:**
   - Ping the server from PC0 (it should fail).
   - Ping the server from PC1 (it should succeed). This demonstrates that the ACL is working correctly.
4. **Configure an Extended ACL (alternative to Standard ACL):**
   - **Aim:** Block Telnet traffic (TCP port 23) from PC0 to the server.
   - **On Router0 (the router closest to the source):**
     - Enter the command: `access-list 101 deny tcp 192.168.1.10 0.0.0.0 192.168.2.10 0.0.0.0 eq 23`

        - Enter the command: `access-list 101 permit ip any any`
        - Apply the ACL to the interface: `interface fastethernet 0/0` > `ip access-group 101 out`

5. **Verify the Extended ACL:**
    - From PC0, try to Telnet to the server's IP address (it should fail).
    - From PC1, try to Telnet to the server's IP address (it should succeed).

Conclusion: This practical successfully demonstrated the use of both Standard and Extended ACLs. We configured ACLs to filter traffic based on source IP, protocol, and port number, showing how ACLs are a powerful tool for controlling network access and enhancing security.

Viva / Oral Questions:

1. What is the difference between a Standard and an Extended ACL?
2. Where should a Standard ACL be placed, and where should an Extended ACL be placed? Why?
3. What is the "implicit deny" rule in ACLs?
4. How do you apply an ACL to a router interface?
5. Why are ACLs considered a fundamental component of network security?

Practical 9: Wireless Network Configuration

Practical Title: Setup SSID, WPA2 security; simulate mobile client access.

Aim: To configure a basic wireless network with an SSID and WPA2 security and to connect a wireless device to it using Cisco Packet Tracer.

Objective:

- To understand the components of a wireless network.
- To configure a wireless router with a Service Set Identifier (SSID).
- To enable WPA2 security on the wireless network.
- To connect a mobile device or a laptop with a wireless adapter to the network.

Theory: A wireless network uses radio waves to connect devices. The **SSID (Service Set Identifier)** is the name of the wireless network that is broadcast to identify it. **WPA2 (Wi-Fi Protected Access 2)** is a security protocol that encrypts wireless traffic to prevent unauthorized access. Using WPA2 with a strong password is a best practice for wireless network security.

Steps:

1. **Create the Network Topology:**
   - Open Cisco Packet Tracer.
   - Drag and drop a Wireless Router (e.g., WRT300N) from the device menu.
   - Add a Laptop (or a smartphone). For the Laptop, you will need to replace its wired adapter with a wireless one (turn off the device, remove the old adapter, drag in the wireless one, and turn the device back on).
   - Connect the Laptop to the Wireless Router.
2. **Configure the Wireless Router:**
   - Click on the Wireless Router.
   - Go to the **GUI** tab.
   - Under the **Setup** tab, ensure the IP address is configured (e.g., `192.168.0.1`).
   - Go to the **Wireless** tab.
   - Change the **SSID** to a desired name, for example, `MySecureWiFi`.
   - Under **Wireless Security**, select **WPA2 Personal**.
   - Set a strong **passphrase**, for example, `CiscoPacketTracer`.
3. **Connect the Wireless Client:**
   - Click on the Laptop.
   - Go to the **Desktop** tab, then click **PC Wireless**.
   - Click the **Connect** tab.
   - The SSID `MySecureWiFi` should appear in the list. Select it and click **Connect**.
   - Enter the WPA2 passphrase you configured earlier.
   - The device should now be connected and receive an IP address from the router's DHCP server.
4. **Verify Connectivity:**

    - From the Laptop's **Command Prompt**, use the command `ipconfig` to view the assigned IP address.
    - Use the `ping` command to test connectivity to the router's IP address (e.g., `ping 192.168.0.1`).

Conclusion: This practical successfully demonstrated the setup of a basic wireless network with a custom SSID and WPA2 security. We were able to simulate a wireless client connecting to the network, confirming that the security and connectivity settings were configured correctly.

Viva / Oral Questions:

1. What is an SSID, and what is its purpose?
2. What is the difference between WPA and WPA2 security?
3. Why is it important to secure a wireless network?
4. What is a MAC address filter, and how can it be used for security?
5. How does a wireless router typically assign IP addresses to clients?

Practical 10: DNS and HTTP Configuration

Practical Title: Configure DNS mappings and simulate HTTP access.

Aim: To configure a DNS server to map a domain name to an IP address and to simulate web (HTTP) access from a client using Cisco Packet Tracer.

Objective:

- To understand the purpose of DNS.
- To configure a DNS server with an A record.
- To configure a web server with an HTML page.
- To verify HTTP access from a client using the domain name.

Theory: DNS (Domain Name System) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates domain names (e.g., `www.example.com`) into IP addresses (e.g., `192.168.1.100`), which computers use to locate each other. **HTTP (Hypertext Transfer Protocol)** is the protocol used to transfer data over the web.

Steps:

1. **Create the Network Topology:**
   - Open Cisco Packet Tracer.
   - Create a simple topology with a PC, a switch, and a server. The server will act as both the DNS server and the web server.
2. **Assign IP Addresses:**
   - **PC:** `192.168.1.10`, Subnet Mask `255.255.255.0`, Default Gateway `192.168.1.1`, **DNS Server:** `192.168.1.20`
   - **Server:** `192.168.1.20`, Subnet Mask `255.255.255.0`
   - You will need a router to act as the default gateway in a more complex setup, but for this simple practical, a switch connecting the PC and server is sufficient if they are in the same subnet.
3. **Configure the Web Server (HTTP Service):**
   - Click on the Server > **Services** tab > **HTTP**.
   - Make sure the HTTP service is **On**. You can edit the `index.html` file to add a simple message, like "Welcome to the web server!".
4. **Configure the DNS Server (DNS Service):**
   - Click on the Server > **Services** tab > **DNS**.
   - Make sure the DNS service is **On**.
   - Create a new **A Record**:
     - **Name:** `www.example.com`
     - **Address:** `192.168.1.20`
   - Click **Add**.

5. **Simulate HTTP Access:**
    - On the PC, go to **Desktop** > **Web Browser**.
    - In the URL bar, type `www.example.com` and press **Go**.
    - The web page you created on the server should load. This demonstrates that the DNS server correctly translated the domain name to the IP address, allowing the HTTP request to succeed.

Conclusion: This practical successfully demonstrated the fundamental roles of DNS and HTTP. We configured a DNS server to map a human-readable domain name to an IP address and then used a web browser to access a web server using that domain name, showcasing the seamless interaction between these two essential protocols.

Viva / Oral Questions:

1. What is the primary function of a DNS server?
2. What is an A record in DNS?
3. What is HTTP, and what is it used for?
4. How does a web browser find a website's IP address when you type a URL?
5. Why is a DNS server essential for the internet to work as we know it?

Mini project Guidelines:

Mini Projects/ Case Study –Cisco packet Tracer /IOT etc

Group: Each group 4 to 5 students.

Mini Project Domain: IOT/Cloud
Simulation: Cisco Packet Tracer

Objective

- To provide hands-on experience in computer networking concepts.
- To simulate, configure, and troubleshoot networks using Cisco Packet Tracer.
- To bridge theoretical knowledge with practical applications.

Deliverables

- **Packet Tracer File (.pkt)** – Working simulation.
- **Project Report** (Word/PDF) containing:
  - Title, objectives, and scope.
  - Design & topology diagram.
  - Configuration details.
  - Results and screenshots.
  - References.

By Dr. Manisha V. Khadse

- ## Evaluation Criteria

Parameter	Marks Distribution
Problem Definition & Relevance	10
Network Design & Addressing	20
Configuration & Implementation	25
Testing & Troubleshooting	15
Documentation & Report	20
Presentation & Viva	10
Total	**100**

By Dr. Manisha V. Khadse