



NETWORK PROTOCOLS AND SECURITY

23EC2210R 23EC2210A 23EC2210E

LAB MANUAL – 2024-25

STUDENT ID:
STUDENT NAME:

ACADEMIC YEAR: 2024-25

Table of Contents

Regular/ Advance/ ExP.:

- Session 1 Introduction to the laboratory and the tool used Cisco packet tracer
- Session 2 Execute the following networking commands like ipconfig, tracert, telnet, netsh, ping, nslookup and netstat in the command prompt with simple topology.
- Session 3 Configuration of basic switch setup using Huawei/Cisco network switch
- Session 4 Construction of Different VLANS and TRUNKING using cisco packet tracer
- Session 5 Configuration of Encapsulation dot 1Q using cisco packet tracer
- Session 6 Implementation of Smart home using Cisco packet tracer and verify the configuration
- Session 7 Configuration of ARP and Static Routing using Cisco network switch and verify the connectivity
- Session 8 Configuration of RIP and OSPF using Cisco network switch and verify the connectivity
- Session 9 Configuration of Network address translation in Cisco packet tracer and verify the configuration
- Session 10 Configure the Standard and Extended Access Control List using cisco packet tracer and verify the configuration
- Session 11 Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection
- Session 12 Write a python program for Transposition Technique using Rail fence Technique and columnar Technique.
- Session 13 Write a python program to implement of RSA Algorithm
- Session 14 Write a python program to implement of S-DES Algorithm
- Session 15 Write a python program for Substitution Technique using Caesar cipher and Mono Alphabetic cipher
- Session 16 Configuration of Basic wireless Settings SSID - LWR3000 Configure Wireless Linksys Routers sing Cisco Packet Tracer

A.Y. 2024-25 LAB CONTINUOUS EVALUATION SPLITUP

For Regular/ Advance/ ExP.:

| Sl. No. | Experiment Mark Division | Marks |
|----------------|---|--------------|
| 1. | Pre-Lab (10M) | 10 |
| 2. | In-Lab <ul style="list-style-type: none">• Program/ Procedure - 5 marks• Data and Results - 10 marks• Analysis & Inference - 10 marks | 25 |
| 3. | Post-Lab | 10 |
| 4. | Viva Voce | 05 |
| 5. | Total | 50 |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 1: Introduction to the laboratory and the tool used Cisco packet tracer

Learning outcome:

- Understand the purpose and importance of using a network simulation tool like Cisco Packet Tracer.
- Gain familiarity with the user interface and basic functionality of Cisco Packet Tracer.
- Learn how to navigate and explore the virtual network environment within Cisco Packet Tracer.
- Acquire knowledge of the various networking devices and components available in Cisco Packet Tracer and their respective functions.

Laboratory Overview

The laboratory setup focuses on network design, configuration, and troubleshooting using Cisco Packet Tracer. This versatile tool is essential for anyone looking to gain practical experience in networking concepts and Cisco technologies. The lab activities will cover a range of topics including basic networking, routing and switching, wireless networking, and network security.

Cisco Packet Tracer

What is Cisco Packet Tracer?

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco Systems. It allows users to create network topologies, configure devices, and simulate network traffic in a virtual environment. This tool is particularly useful for students and professionals who are preparing for Cisco certification exams such as CCNA (Cisco Certified Network Associate) and CCNP (Cisco Certified Network Professional).

Key Features

Network Simulation: Packet Tracer provides a virtual platform to design, configure, and troubleshoot networks without the need for physical hardware.

Device Configuration: Users can configure a wide range of Cisco devices including routers, switches, and wireless access points. This includes setting up IP addresses, configuring routing protocols, and implementing security measures.

Multi-User Functionality: Packet Tracer supports collaborative activities where multiple users can work on the same network topology simultaneously.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Real-time and Simulation Modes: Users can observe the behavior of the network in real-time or use the simulation mode to step through network events and protocols.

Learning and Assessment: The tool includes various built-in activities and tutorials that help users learn networking concepts and assess their understanding through practical application.

Using Cisco Packet Tracer in the Laboratory

Network Design: Users can drag and drop network devices to create complex network topologies. This visual representation helps in understanding the layout and connectivity of the network.

Configuration Tasks: Through the graphical user interface and command-line interface, users can perform a wide range of configuration tasks such as setting up VLANs, configuring OSPF routing, and enabling firewall rules.

Troubleshooting: The tool allows users to identify and resolve network issues by providing diagnostic tools such as ping, traceroute, and real-time error messages.

Simulation Exercises: The laboratory exercises will include various scenarios that mimic real-world networking problems. Users will be required to configure and troubleshoot the network to achieve the desired outcome.

Conclusion

Cisco Packet Tracer is an invaluable tool for anyone looking to gain hands-on experience in networking. Its robust feature set and user-friendly interface make it an ideal choice for educational purposes. Through the laboratory activities, users will develop a deeper understanding of networking concepts and become proficient in using Cisco technologies.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 2: Execute the following networking commands like ipconfig, tracert, telnet, netsh, ping, nslookup and netstat in the command prompt with simple topology.

Learning outcome:

- Understand the purpose of ipconfig and use ipconfig to display network configuration information for a Windows computer.
- Learn how to use ping to test network connectivity to a remote host.
- Learn how to use tracert and netstat to trace the route taken by network packets to a destination.
- Understand the purpose of nslookup (Name Server Lookup) and use nslookup to query DNS servers for information about domain names and IP addresses.

1. ipconfig

The ipconfig command is used to display the IP configuration of a computer.

>Ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : example.local

IPv4 Address. : 192.168.1.2

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

2. tracert

The tracert command traces the path that a packet takes to reach a destination.

>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]

over a maximum of 30 hops:

```
 1  1 ms  1 ms  1 ms 192.168.1.1
 2 10 ms 11 ms 12 ms 10.0.0.1
 3 20 ms 20 ms 21 ms 72.14.204.1
 4 30 ms 29 ms 30 ms 216.239.46.25
 5 40 ms 40 ms 40 ms 8.8.8.8
```

Trace complete.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

3. telnet

The telnet command is used to connect to remote devices or servers. Make sure Telnet is enabled on your computer.

telnet 192.168.1.1

Connecting To 192.168.1.1...

(Note: If Telnet is not installed, you can enable it from "Programs and Features" -> "Turn Windows features on or off" -> Check "Telnet Client")

4. netsh

The netsh command is used to configure network interfaces, IP addresses, and more.

netsh interface ip set address "Ethernet" static 192.168.1.10 255.255.255.0 192.168.1.1

Configuration of interface "Ethernet" is completed.

5. ping

The ping command tests connectivity between devices.

ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

| | | |
|-----------------------|---|-------------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

6. nslookup

The nslookup command queries DNS servers to obtain domain name or IP address mapping.

nslookup www.google.com

Server: mydnserver.local

Address: 192.168.1.1

Non-authoritative answer:

Name: www.google.com

Addresses: 142.250.184.68

142.250.184.100

142.250.184.139

142.250.184.101

142.250.184.102

142.250.184.113

7. netstat

The netstat command displays network connections, routing tables, and interface statistics.

netstat -an

Active Connections

| Proto | Local Address | Foreign Address | State |
|-------|-------------------|-------------------|-------------|
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING |
| TCP | 192.168.1.2:49152 | 172.217.3.110:443 | ESTABLISHED |
| UDP | 0.0.0.0:123 | *:* | |
| UDP | 192.168.1.2:137 | *:* | |
| UDP | 192.168.1.2:138 | *:* | |

Conclusion

These commands provide essential information and capabilities for network configuration and troubleshooting. By using Cisco Packet Tracer in combination with these commands, you can simulate and understand the real-world applications of networking principles in a controlled environment.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 3: Configuration of basic switch setup using Huawei/Cisco network switch.

Learning outcome:

- Identify and understand the physical components of a Huawei network switch, such as ports, LEDs, and console interfaces.
- Understand the concept of user authentication and password management.
- Develop the ability to navigate the switch's CLI, including using basic commands to view system information and switch status.
- Understand the essential settings, such as hostname, IP address, and gateway to make the switch accessible on the network
- Develop an understanding of best practices for switch configuration and management to ensure a stable and secure network.

Configuring a basic switch setup using a Cisco network switch

It involves several steps, including setting up the initial switch configuration, configuring VLANs, and setting up basic security. Here's a step-by-step guide to get you started:

Step 1: Access the Switch

1. **Connect to the Switch:** Use a console cable to connect your PC to the switch's console port. Open a terminal emulator program (e.g., PuTTY or Tera Term) and connect to the switch using the appropriate COM port settings (typically 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control).
2. **Enter Privileged EXEC Mode:**
Switch> enable
3. **Enter Global Configuration Mode:**
Switch# configure terminal

Step 2: Set Hostname and Passwords

1. **Set the Hostname:**
Switch(config)# hostname MySwitch
2. **Set Console Password:**
MySwitch(config)# line console 0
MySwitch(config-line)# password your_password
MySwitch(config-line)# login
MySwitch(config-line)# exit
3. **Set Enable Password:**
MySwitch(config)# enable secret your_enable_password

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Step 3: Configure VLANs

1. Create VLANs:

```
MySwitch(config)# vlan 10
```

```
MySwitch(config-vlan)# name Sales
```

```
MySwitch(config-vlan)# exit
```

```
MySwitch(config)# vlan 20
```

```
MySwitch(config-vlan)# name Engineering
```

```
MySwitch(config-vlan)# exit
```

2. Assign Ports to VLANs:

```
MySwitch(config)# interface range fastethernet 0/1 - 12
```

```
MySwitch(config-if-range)# switchport mode access
```

```
MySwitch(config-if-range)# switchport access vlan 10
```

```
MySwitch(config-if-range)# exit
```

```
MySwitch(config)# interface range fastethernet 0/13 - 24
```

```
MySwitch(config-if-range)# switchport mode access
```

```
MySwitch(config-if-range)# switchport access vlan 20
```

```
MySwitch(config-if-range)# exit
```

Step 4: Configure Basic Security

1. Disable Unused Ports:

```
MySwitch(config)# interface range fastethernet 0/25 - 48
```

```
MySwitch(config-if-range)# shutdown
```

```
MySwitch(config-if-range)# exit
```

2. Set Up Port Security:

```
MySwitch(config)# interface fastethernet 0/1
```

```
MySwitch(config-if)# switchport port-security
```

```
MySwitch(config-if)# switchport port-security maximum 2
```

```
MySwitch(config-if)# switchport port-security violation restrict
```

```
MySwitch(config-if)# switchport port-security mac-address sticky
```

```
MySwitch(config-if)# exit
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Step 5: Save Configuration

1. Save the Configuration:

MySwitch# copy running-config startup-config

Step 6: Verify Configuration

1. Check VLAN Configuration:

MySwitch# show vlan brief

2. Check Interface Status:

MySwitch# show interfaces status

3. Check Port Security:

MySwitch# show port-security interface fastethernet 0/1

To Do excise

Switch>en

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Switch-A

Switch-A(config)#line console 0

Switch-A(config-line)#password KLU123

Switch-A(config-line)#login

Switch-A(config-line)#exit

Switch-A(config)#line vty 0 15

Switch-A(config-line)#password KLU123

Switch-A(config-line)#login

Switch-A(config-line)#exit

Switch-A(config)#banner motd &Welcome to KL University&

Switch-A(config)#service password-encryption

Switch-A(config)#int vlan 1

Switch-A(config-if)#ip address 128.107.20.10 255.255.255.0

Switch-A(config-if)#no shut

To save the configuration

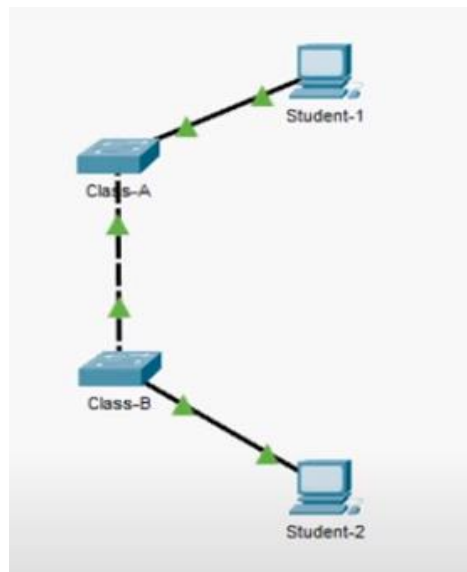
Switch-A#copy running-config startup-config

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Configuration of basic switch setup using Cisco network

| Device | Interface | IP Address | Subnet Mask |
|-----------|-----------|---------------|---------------|
| Class-A | VLAN 1 | 128.107.20.10 | 255.255.255.0 |
| Class-B | VLAN 1 | 128.107.20.15 | 255.255.255.0 |
| Student-1 | NIC | 128.107.20.25 | 255.255.255.0 |
| Student-2 | NIC | 128.107.20.30 | 255.255.255.0 |

switch

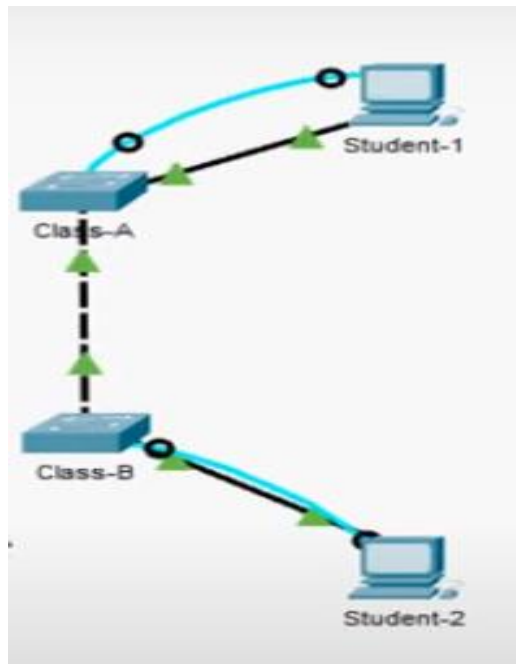


Requirements

- Use Console connection to access each switch
- Name Class-A and Class-B switches
- Use the KLU123 password for all lines
- Use the KLEF123 secret password
- Encrypt all clear text passwords
- Configure an appropriate message-of-the-day (MOTD) banner.
- Configure addressing for all devices according to the Addressing table
- Save your configuration
- Verify connectivity between all devices

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Configuration of Class-A and Class-B Switch using console port connection



| Class-A Switch | Class-B Switch |
|--|--|
| <pre> Switch>en Switch#config t Switch(config)#hostname Class-A Class-A(config)#line console 0 Class-A(config-line)#password KLU123 Class-A(config-line)#login Class-A(config-line)#exit Class-A(config)#line vty 0 15 Class-A(config-line)#password KLU123 Class-A(config-line)#login Class-A(config-line)#exit Class-A(config)#enable secret KLEF12 Class-A(config)#service password-encryption Class-A(config)#banner motd &Unauthorized access is strictly prohibited& Class-A(config)#interface vlan 1 Class-A(config-if)#ip address 128.107.20.10 255.255.255.0 Class-A(config-if)#no shutdown Class-A(config-if)#exit Class-A(config)#exit Class-A#copy running-config startup-config </pre> | <pre> Switch>en Switch#config t Switch(config)#hostname Class-B Class-B(config)#line console 0 Class-B(config-line)#password KLU123 Class-B(config-line)#login Class-B(config-line)#exit Class-B(config)#line vty 0 15 Class-B(config-line)#password KLU123 Class-B(config-line)#login Class-B(config-line)#exit Class-B(config)#enable secret KLEF12 Class-B(config)#service password-encryption Class-B(config)#banner motd &Unauthorized access is strictly prohibited& Class-B(config)#interface vlan 1 Class-B(config-if)#ip address 128.107.20.15 255.255.255.0 Class-B(config-if)#no shutdown Class-B(config-if)#exit Class-B(config)#exit Class-B#copy running-config startup-config </pre> |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

| Configuration of the PCs connected using console connection | |
|---|---|
| Student-1 | Student-2 |
| IP Address: 128.107.20.25 Subnet Mask: 255.255.255.0 | IP Address: 128.107.20.30 Subnet Mask: 255.255.255.0 |

Conclusion

This basic configuration ensures that your Cisco switch is properly set up with a hostname, passwords, VLANs, and basic security measures. By following these steps, you can create a manageable and secure network environment.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 4: Construction of different VLANS and TRUNKING using cisco packet tracer

Learning Outcome:

- Students should be able to explain what VLANs are and understand their purpose in network segmentation
- Understand how VLANs can improve network performance, security, and management.
- Configure VLANs on network switches, including creating, modifying, and deleting VLANs.
- Understand the concept of VLANs (Virtual Local Area Networks) and their significance in network segmentation and management.
- Understand and configure trunk ports on switches to allow the passage of VLAN traffic between switches.

Construction of different VLANS and TRUNKING using cisco packet tracer

Creating different VLANs (Virtual LANs) and configuring trunking between switches are common tasks in networking, and they can be effectively simulated using Cisco Packet Tracer. Here are the steps involved in constructing different VLANs and trunking using Cisco Packet Tracer:

Construction of Different VLANs:

1. Open Cisco Packet Tracer:

- Launch the Cisco Packet Tracer application on your computer.

2. Create the Network Topology:

- Add the required network devices to the workspace. For VLANs, you'll need multiple switches. Connect them using appropriate cables.

3. Access Switches:

- Double-click on each switch to access the device configuration.

4. Enter Global Configuration Mode:

- Enter global configuration mode using the following command:

Switch> enable Switch# configure terminal

5. Create VLANs:

- Use the following command to create VLANs. Replace <vlan_id> with the desired VLAN ID.

Switch(config)# vlan <vlan_id>

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

6. Assign VLAN Names:

- Optionally, assign names to the VLANs for better identification:

Switch(config-vlan)# name <vlan_name>

7. Assign VLANs to Switch Ports:

- Navigate to individual switch interfaces and assign them to specific VLANs:

Switch(config)# interface <interface_type> <interface_number>

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan <vlan_id>

- Repeat this process for each switch interface and VLAN.

8. Verify VLAN Configuration:

- Use the following commands to verify your VLAN configuration:

Switch# show vlan **Switch# show interfaces switchport**

Configuration of Trunking:

1. Connect Two Switches:

- Ensure that two switches are connected. Use a straight-through cable between their trunking interfaces.

2. Configure Trunking on the Interface:

- Access the configuration mode of the interface connected to the other switch and configure it as a trunk port:

Switch(config)# interface <interface_type> <interface_number>

Switch(config-if)# switchport mode trunk

3. Set Allowed VLANs:

- Optionally, restrict the allowed VLANs on the trunk to improve security:

Switch(config-if)# switchport trunk allowed vlan <vlan_list>

- Replace <vlan_list> with a comma-separated list of VLAN IDs.

4. Verify Trunk Configuration:

- Use the following command to verify the trunk configuration:

Switch# show interfaces trunk

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

5. Repeat for Additional Switches:

- If you have more switches, repeat the trunking configuration between them, connecting the trunking interfaces.

6. Test Connectivity:

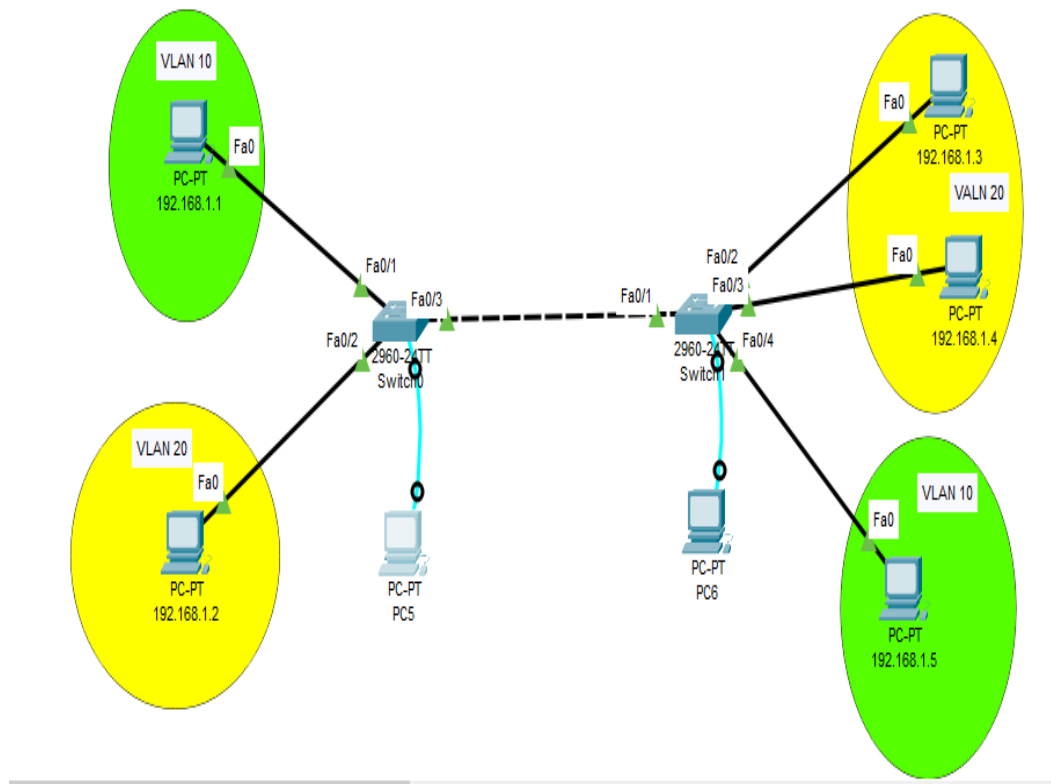
- Connect devices to the VLANs on different switches and verify that they can communicate across the network.

By following these steps, you can construct different VLANs and configure trunking between switches using Cisco Packet Tracer.

Construction of Different VLANs

Addressing Table

| Device | IP Address | Subnet Mask |
|--------|-------------|---------------|
| PC2 | 192.168.1.1 | 255.255.255.0 |
| PC3 | 192.168.1.2 | 255.255.255.0 |
| PC4 | 192.168.1.3 | 255.255.255.0 |
| PC5 | 192.168.1.4 | 255.255.255.0 |
| PC6 | 192.168.1.5 | 255.255.255.0 |



| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

| VLAN configuration in Switches | |
|--|---|
| Switch-A | Switch-B |
| <pre>Switch>en Switch#config t Switch(config)#vlan 10 Switch(config-vlan)#name green Switch(config-vlan)#exit Switch(config)#vlan 20 Switch(config-vlan)#name yellow Switch(config-vlan)#exit Switch(config)#exit Switch#show vlan brief Switch#config t Switch(config)#int fa0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit Switch(config)#int fa0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit Switch(config)#exit Switch#show vlan brief Switch#config t Switch(config)#int fa0/3 Switch(config-if)#switchport mode trunk Switch(config)#int fa0/1 Switch(config-if)#switchport mode trunk</pre> | <pre>Switch>en Switch#config t Switch(config)#vlan 20 Switch(config-vlan)#name yellow Switch(config-vlan)#exit Switch(config-vlan)#vlan 10 Switch(config-vlan)#name green Switch(config-vlan)#exit Switch(config)#exit Switch#show vlan brief Switch#config t Switch(config)#int range fa0/2-3 Switch(config-if-range)#switchport mode access Switch(config-if-range)#switchport access vlan 20 Switch(config-if-range)#exit Switch(config)#int fa0/4 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit Switch(config)#exit Switch#show vlan brief Switch#config t Switch(config)#int fa0/1 Switch(config-if)#switchport mode trunk Switch(config)#int fa0/3 Switch(config-if)#switchport mode trunk</pre> |

Configuration of PCs

PC2:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

PC3:

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

PC4:

IP Address: 192.168.1.3

Subnet Mask: 255.255.255.0

PC5:

IP Address: 192.168.1.4

Subnet Mask: 255.255.255.0

PC6:

IP Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Conclusion

By following the steps outlined, we successfully constructed different VLANs and configured trunking on Cisco switches using Cisco Packet Tracer. The process involved:

- Creating VLANs for logical network segmentation.
- Configuring trunk ports to carry VLAN traffic between switches.
- Assigning VLANs to access ports to group devices logically.

This configuration is crucial for network management and security, as it allows for better traffic control, reduced broadcast domains, and improved network performance. Properly implemented VLANs and trunking ensure that network resources are used efficiently and that communication between different segments is controlled and secure. This foundational skill in network management enables more complex and scalable network designs, catering to the diverse needs of modern network environments.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 5: Configuration of Encapsulation dot 1Q using cisco packet tracer

Learning outcome:

- Learners will learn how to configure the Encapsulation dot1Q protocol, which is used to tag VLAN information on Ethernet frames.
- Understand the importance of VLAN tagging and how it enables VLAN communication across different network devices..

Configuring encapsulation dot1Q (802.1Q) on a Cisco switch using Cisco Packet Tracer

It involves creating and assigning VLANs and then configuring trunk ports to carry multiple VLANs across a single physical link. Here's a step-by-step guide:

Step 1: Create VLANs

1. **Access the Switch:** Connect to your switch via the console port in Cisco Packet Tracer.
2. **Enter Privileged EXEC Mode:**
Switch> enable
3. **Enter Global Configuration Mode:**
Switch# configure terminal
4. **Create VLANs:**
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit

Step 2: Assign VLANs to Ports

1. **Assign Ports to VLAN 10:**
Switch(config)# interface range fastethernet 0/1 - 12
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

2. Assign Ports to VLAN 20:

```
Switch(config)# interface range fastethernet 0/13 - 24
```

```
Switch(config-if-range)# switchport mode access
```

```
Switch(config-if-range)# switchport access vlan 20
```

```
Switch(config-if-range)# exit
```

Step 3: Configure Trunk Ports

1. Configure Trunk Port on Switch 1:

```
Switch(config)# interface fastethernet 0/24
```

```
Switch(config-if)# switchport mode trunk
```

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

```
Switch(config-if)# exit
```

2. Configure Trunk Port on Switch 2 (if you have a second switch):

```
Switch2(config)# interface fastethernet 0/24
```

```
Switch2(config-if)# switchport mode trunk
```

```
Switch2(config-if)# switchport trunk encapsulation dot1q
```

```
Switch2(config-if)# exit
```

Step 4: Verify Configuration

1. Verify Trunk Configuration:

```
Switch# show interfaces trunk
```

2. Verify VLAN Configuration:

```
Switch# show vlan brief
```

Example Network Topology

- Connect two switches:** Use the crossover cable in Packet Tracer to connect FastEthernet 0/24 on Switch 1 to FastEthernet 0/24 on Switch 2.
- Connect PCs:** Connect PCs to the access ports on each switch. For example, connect a PC to FastEthernet 0/1 on Switch 1 and another PC to FastEthernet 0/13 on Switch 2.

Testing

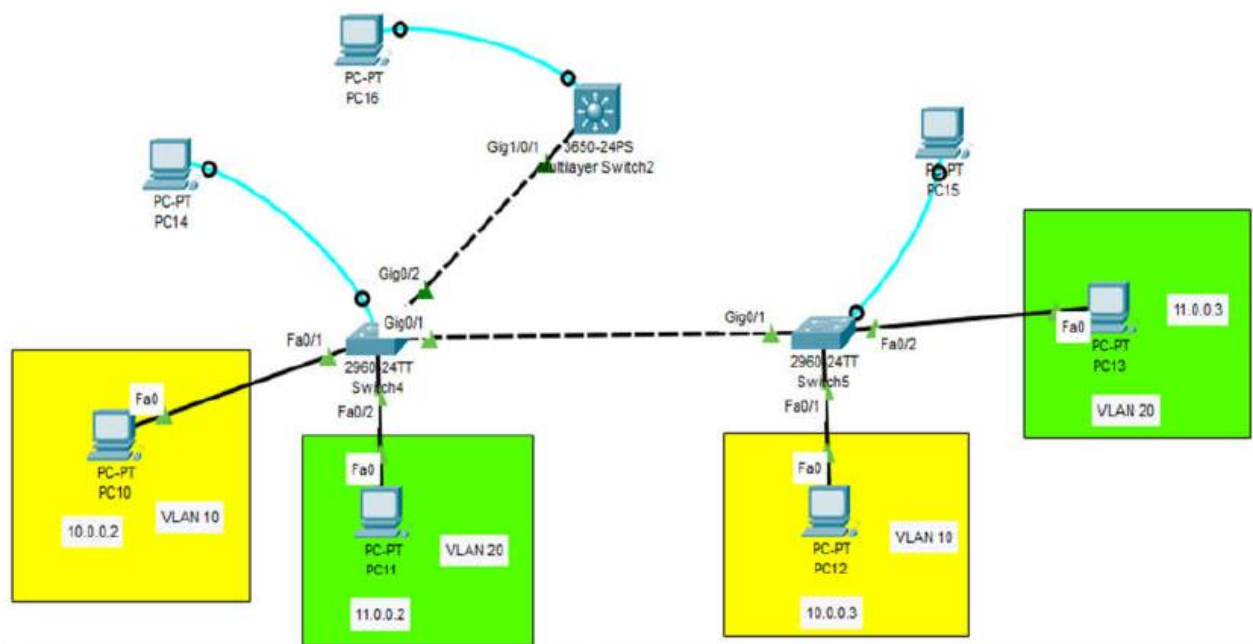
- Assign IP Addresses:** Make sure each PC in VLAN 10 and VLAN 20 has an IP address in the same subnet.
- Ping Test:** Verify connectivity by pinging from one PC to another in the same VLAN.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Configuration of Encapsulation dot 1Q using cisco packet tracer

Addressing Table

| | | | |
|-------------------------|----------|-----------|--------------|
| PC-10 | 10.0.0.2 | 255.0.0.0 | VLAN 10 |
| PC-11 | 11.0.0.2 | 255.0.0.0 | VLAN 20 |
| PC-12 | 10.0.0.3 | 255.0.0.0 | VLAN 10 |
| PC-13 | 11.0.0.3 | 255.0.0.0 | VLAN 20 |
| Multilayer Switch2(MLS) | 10.0.0.1 | 255.0.0.0 | VLAN 10 PORT |
| Multilayer Switch2(MLS) | 11.0.0.1 | 255.0.0.0 | VLAN 20 PORT |



NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

| Switch-4 | Switch-5 |
|---|---|
| Switch>en Switch#config t Switch(config)#vlan 10 Switch(config-vlan)#name Sales Switch(config-vlan)#vlan 20 Switch(config-vlan)#name Admin Switch(config-vlan)#exit Switch(config)#int f0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit Switch(config)#int f0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config)#int g0/1 Switch(config-if)#switchport mode trunk Switch(config)#int g0/2 Switch(config-if)#switchport mode trunk | Switch>en Switch#config t Switch(config)#vlan 10 Switch(config-vlan)#name Sales Switch(config-vlan)#vlan 20 Switch(config-vlan)#name Admin Switch(config-vlan)#exit Switch(config)#int f0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit Switch(config)#int f0/2 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20 Switch(config)#int g0/1 Switch(config-if)#switchport mode trunk |

| Configuration of Multilayer Switch |
|--|
| Switch>en Switch#config t Switch(config)#vlan 10 Switch(config-vlan)#name Sales Switch(config-vlan)#vlan 20 Switch(config-vlan)#name Admin Switch(config-vlan)#exit Switch(config)#int vlan 10 Switch(config-if)#ip address 10.0.0.1 255.0.0.0 Switch(config-if)#exit Switch(config)#int vlan 20 Switch(config-if)#ip address 11.0.0.1 255.0.0.0 Switch(config-if)#exit Switch(config)#int g1/0/1 Switch(config-if)#switchport mode trunk Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#exit Switch(config)#ip routing |
| Configuration of PCs |
| PC10: IP Address- 10.0.0.2 Subnet Mask- 255.0.0.0 Default Gateway- 10.0.0.1 PC11: IP Address- 11.0.0.2 Subnet Mask- 255.0.0.0 Default Gateway- 11.0.0.1 PC12: IP Address- 10.0.0.3 Subnet Mask- 255.0.0.0 Default Gateway- 10.0.0.1 PC13: IP Address- 11.0.0.3 Subnet Mask- 255.0.0.0 Default Gateway- 11.0.0.1 |

Conclusion

This configuration sets up 802.1Q encapsulation on trunk ports, allowing VLAN traffic to be carried across a single link between switches. By following these steps, you can manage multiple VLANs efficiently within your network using Cisco Packet Tracer.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 6: Implementation of Smart home using Cisco packet tracer and verify the configuration

Learning outcome:

- Understanding IoT Concepts and Gain a solid understanding of IoT and its applications in smart homes
- Configure Cisco routers and switches to create a functional network for the smart home.
- Learners will gain a comprehensive understanding of Smart Home technology and its applications.
- Learners will develop skills in designing network infrastructures that support Smart Home implementations

Home Automation Basics – Beginners Guide

Although not many people can see the need for having their smart fridge connected to the Internet, most people will find the ability to remotely control lights, security cameras and other home appliances very useful. If you are thinking about adding smart devices to your home then this guide to smart homes and home automation will give you a good basic understanding of how smart devices are connected and how they are controlled.

What is Home Automation?

Home automation or **domestics** is building automation for a home, called a **smart home** or **smart house**. It involves the control and automation of lighting. Home automation is one of several areas of the IOT (internet of things), and is often called **Home IOT**.

There are three distinct levels of home automation.

1. Monitoring
2. Control
3. Automation

Monitoring

The ability to view status of systems i.e

- What is the temperature?
- Is the door locked?
- Is The Light on or off

Control

The ability to change the state of a systems i.e

- Turn up the heating.
- Lock the Door
- Turning the light on or off

Automation

The ability to change the state of a system automatically in response to an event. i.e.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

- Turn on the heating if the outside temperature falls below a certain temperature.
- Turn the lights off when no one is a home.

Currently most smart home systems are at the **control level**.

Smart Home – Automation System Components

A home automation system will consist of

- End Devices like switches, sensors ,lights, locks etc
- Connection devices like hubs and Gateways.
- A Network or networks e.g. Wi-Fi, Zigbee etc
- Internet connection – maybe optional

Local Control and Cloud Control

All homes should be able to be controlled locally from within the home. This doesn't mean that they should have manual switches, but that they should be controllable across a local network. They should also **IMO** be controllable and **fully functional** without an Internet connection. In other words if you loose the Internet connection you should still be able to turn your lights on and off. Unfortunately not all systems will operate without an Internet connection. This article is worth reading.

As a General rule of thumb **Zwave** and **Zigbee** networks and devices will operate without an Internet connection. **Wi-Fi devices** will generally **require** an Internet connection. If the device is controllable directly using a smart phone then it requires an Internet connection. This reddit discussion is worth reading.

The Role of the Cloud In Smart Homes

Many Internet devices especially **Wi-Fi devices** are dependent on an Internet connection, and cloud services to function. Generally when you set up these devices you **register them** with the manufacturer on a cloud service. They can then be controlled via an App on a smart phone, Alexa etc but will require an Internet connection to function correctly. Although these devices are easy to setup and operate they are useless without an Internet connection. IMO the Internet should represent an alternative way of controlling devices, and not the only way.

Creating a smart home simulation using Cisco Packet Tracer involves integrating various IoT (Internet of Things) devices and configuring them to work together. Here's a step-by-step guide on how to set up a basic smart home environment in Cisco Packet Tracer:

Step 1: Set Up the Network Infrastructure

1. **Add a Home Gateway:**
 - Go to the "Network Devices" section and select a wireless router (e.g., Home Gateway).
 - Place it on the workspace.
2. **Add a Laptop:**
 - Go to the "End Devices" section and select a laptop.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

- Place it on the workspace.
- 3. **Connect the Laptop to the Home Gateway:**
 - Select the "Connections" tab and choose a straight-through cable.
 - Connect the laptop to one of the Ethernet ports on the Home Gateway.

Step 2: Add IoT Devices

1. **Add Smart Devices:**
 - Go to the "Home" section under "End Devices."
 - Add various smart devices like a smart light, smart thermostat, smart door lock, and smart TV to the workspace.
2. **Connect Smart Devices to the Home Gateway:**
 - Most smart devices connect wirelessly.
 - Click on each smart device and configure it to connect to the Home Gateway's wireless network.

Step 3: Configure the Home Gateway

1. **Configure Wireless Settings:**
 - Click on the Home Gateway.
 - Go to the "GUI" tab.
 - Set up the SSID (e.g., "SmartHomeNetwork") and configure security settings (e.g., WPA2-PSK).
2. **Configure the DHCP Server:**
 - Ensure the DHCP server is enabled to assign IP addresses to all devices in the network.

Step 4: Configure IoT Devices

1. **Configure the Smart Light:**
 - Click on the smart light.
 - Go to the "Config" tab.
 - Set the SSID to "SmartHomeNetwork".
 - Set up other settings as needed (e.g., default state, intensity).
2. **Configure the Smart Thermostat:**
 - Click on the smart thermostat.
 - Go to the "Config" tab.
 - Set the SSID to "SmartHomeNetwork".
 - Configure temperature settings and schedules.
3. **Configure the Smart Door Lock:**
 - Click on the smart door lock.
 - Go to the "Config" tab.
 - Set the SSID to "SmartHomeNetwork".
 - Set up access codes and lock/unlock schedules.
4. **Configure the Smart TV:**
 - Click on the smart TV.
 - Go to the "Config" tab.
 - Set the SSID to "SmartHomeNetwork".
 - Configure streaming services and other settings.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Step 5: Control IoT Devices

1. Use the Laptop to Control IoT Devices:

- Open the web browser on the laptop.
- Enter the IP address of the Home Gateway to access the control interface.
- Use the control interface to turn on/off devices, adjust settings, and monitor device statuses.

2. Use a Smartphone:

- Add a smartphone from the "End Devices" section.
- Connect it to the "SmartHomeNetwork".
- Use the built-in app or a web browser to control and monitor the smart devices.

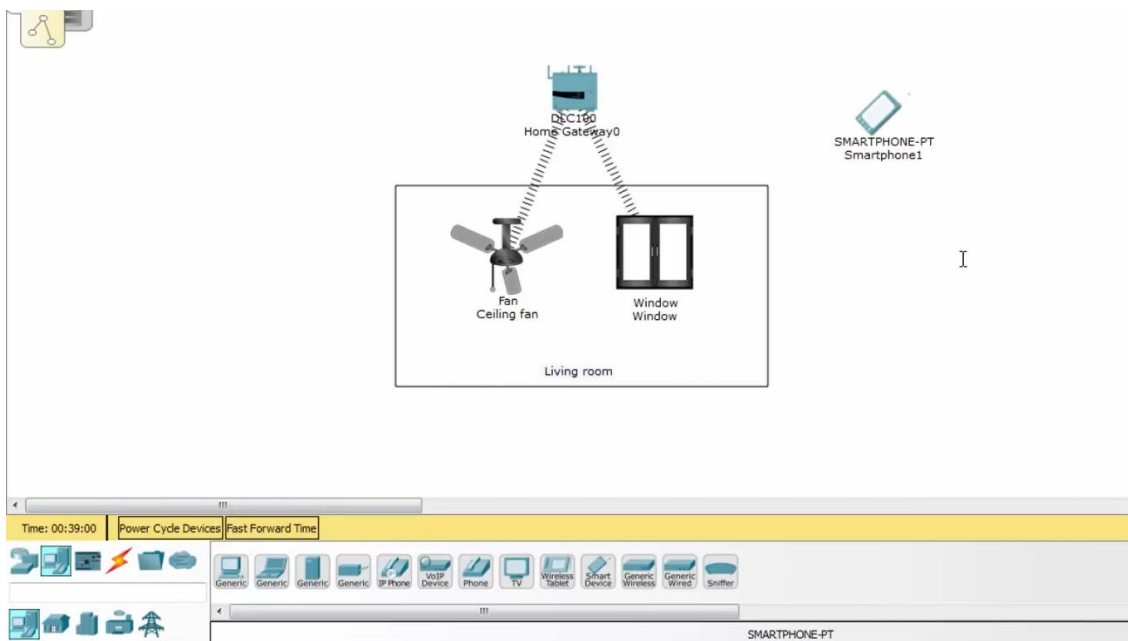
Step 6: Automation and Scripting

1. Create Automated Scripts:

- Some smart devices support scripts for automation.
- Create scripts to automate tasks, such as turning on the lights when it gets dark or adjusting the thermostat based on the time of day.

2. Test Automation:

- Ensure all automated tasks are working as expected by simulating different scenarios.



Conclusion

This setup allows you to simulate a smart home environment in Cisco Packet Tracer. By adding and configuring various IoT devices, you can create a realistic smart home network where devices are interconnected and controllable via a central hub. This simulation helps in understanding the integration and management of IoT devices in a home network.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 7: Configuration of ARP and Static Routing using Cisco network switch and verify the connectivity

Learning outcome:

- Understand the role of a router in a computer network and its importance in facilitating communication between different network segments.
- Gain familiarity with Huawei L3 network switches and their specific features and capabilities related to router functionality and static routing.

Configuring ARP (Address Resolution Protocol) and static routing on a Cisco network switch involves setting up the switch to handle ARP requests and responses, as well as defining static routes for network traffic. Below are the steps to configure ARP and static routing on a Cisco switch:

Step 1: Configure ARP on a Cisco Switch

ARP is generally automatically handled by Cisco switches and routers. However, you can configure static ARP entries if needed.

1. **Access the Switch:** Connect to your switch via the console port.
2. **Enter Privileged EXEC Mode:**
Switch> enable
3. **Enter Global Configuration Mode:**
Switch# configure terminal
4. **Add a Static ARP Entry:**
Switch(config)# arp 192.168.1.10 00a0.c91b.b2b8 ARPA

Step 2: Configure Static Routing on a Cisco Switch

To configure static routing, you need to ensure that the switch has Layer 3 capabilities (i.e., it is a Layer 3 switch).

1. **Enable IP Routing** (if necessary):
Switch(config)# ip routing
2. **Configure a Static Route:**
Switch(config)# ip route <destination-network> <subnet-mask> <next-hop-ip>
For example, to route traffic to the 192.168.2.0/24 network via the next-hop IP address 192.168.1.1:
Switch(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1

Step 3: Verify Configuration

1. **Verify ARP Table:**
Switch# show ip arp

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

2. Verify Static Routes:

```
Switch# show ip route
```

Example Topology and Configuration

Assume you have a simple network topology with two VLANs, two Layer 3 switches, and a router.

Switch 1 Configuration

1. Create VLANs and Assign IP Addresses:

```
Switch1(config)# vlan 10
```

```
Switch1(config-vlan)# name Sales
```

```
Switch1(config-vlan)# exit
```

```
Switch1(config)# vlan 20
```

```
Switch1(config-vlan)# name Engineering
```

```
Switch1(config-vlan)# exit
```

```
Switch1(config)# interface vlan 10
```

```
Switch1(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
Switch1(config-if)# no shutdown
```

```
Switch1(config)# interface vlan 20
```

```
Switch1(config-if)# ip address 192.168.20.1 255.255.255.0
```

```
Switch1(config-if)# no shutdown
```

2. Enable IP Routing:

```
Switch1(config)# ip routing
```

3. Configure Static Routes:

```
Switch1(config)# ip route 192.168.30.0 255.255.255.0 192.168.10.2
```

Switch 2 Configuration

1. Create VLANs and Assign IP Addresses:

```
Switch2(config)# vlan 30
```

```
Switch2(config-vlan)# name Management
```

```
Switch2(config-vlan)# exit
```

```
Switch2(config)# interface vlan 30
```

```
Switch2(config-if)# ip address 192.168.30.1 255.255.255.0
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Switch2(config-if)# no shutdown

2. Enable IP Routing:

Switch2(config)# ip routing

3. Configure Static Routes:

Switch2(config)# ip route 192.168.10.0 255.255.255.0 192.168.30.2

Switch2(config)# ip route 192.168.20.0 255.255.255.0 192.168.30.2

Router Configuration (if needed)

1. Assign IP Addresses to Interfaces:

Router(config)# interface gigabitEthernet 0/0

Router(config-if)# ip address 192.168.10.2 255.255.255.0

Router(config-if)# no shutdown

Router(config)# interface gigabitEthernet 0/1

Router(config-if)# ip address 192.168.30.2 255.255.255.0

Router(config-if)# no shutdown

2. Enable IP Routing (if not already enabled):

Router(config)# ip routing

Testing and Verification

1. Check ARP Entries:

Switch1# show ip arp

2. Check Static Routes:

Switch1# show ip route

3. Ping to Verify Connectivity:

Switch1# ping 192.168.30.1

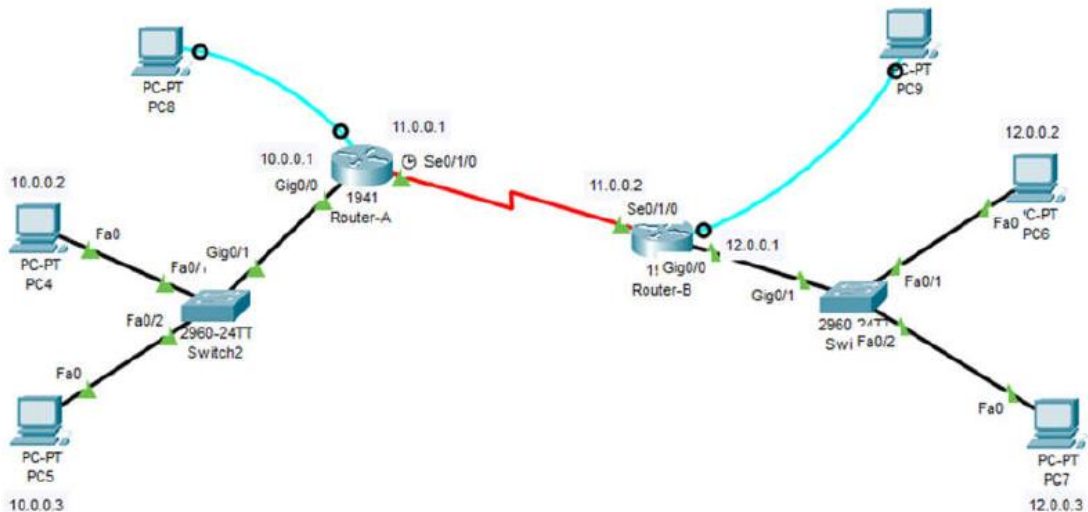
Configuration of Static Routing

Addressing Table

| Device | IP Address | Subnet Mask | Default Gateway |
|----------|-------------------|----------------------|------------------------|
| PC4 | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| PC5 | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 |
| PC6 | 12.0.0.2 | 255.0.0.0 | 12.0.0.1 |
| PC7 | 12.0.0.3 | 255.0.0.0 | 12.0.0.1 |
| Router-A | Interface: g0/0 | IP Address: 10.0.0.1 | Subnet Mask: 255.0.0.0 |
| | Interface: s0/1/0 | IP Address: 11.0.0.1 | Subnet Mask: 255.0.0.0 |
| Router-B | Interface: g0/0 | IP Address: 12.0.0.1 | Subnet Mask: 255.0.0.0 |
| | Interface: s0/1/0 | IP Address: 11.0.0.2 | Subnet Mask: 255.0.0.0 |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



Router Configuration

| Router-A | Router-B |
|---|---|
| Router>en Router#config t Router(config)#int g0/0 Router(config-if)#ip address 10.0.0.1 255.0.0.0 Router(config-if)#no shut Router(config-if)#exit Router(config)#int s0/1/0 Router(config-if)#clock rate 64000 Router(config-if)#ip address 11.0.0.1 255.0.0.0 Router(config-if)#no shut Router(config-if)#exit Router(config)#ip route 12.0.0.0 255.0.0.0 11.0.0.2 | Router>en Router#config t Router(config)#int g0/0 Router(config-if)#ip address 12.0.0.1 255.0.0.0 Router(config-if)#no shut Router(config-if)#exit Router(config)#int s0/1/0 Router(config-if)#ip address 11.0.0.2 255.0.0.0 Router(config-if)#no shut Router(config-if)#exit Router(config)#ip route 10.0.0.0 255.0.0.0 11.0.0.1 |

Conclusion

By following these steps, you can configure ARP and static routing on a Cisco switch, enabling communication between different VLANs and networks. This setup is essential for managing network traffic efficiently and ensuring proper connectivity in a multi-network environment.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 8: Configuration of RIP and OSPF using Cisco network switch and verify the connectivity

Learning outcome:

- Understanding OSPF Basics and its role in dynamic routing protocols.
- Demonstrate an understanding of basic Cisco switch configuration, including accessing the command-line interface (CLI) and configuring interfaces.
- Identify and specify the OSPF router ID and Choose the OSPF network type (point-to-point, broadcast, etc.) and configure it accordingly.
- Understand the concept of hierarchical OSPF and area design.

Configuring OSPF (Open Shortest Path First) on a Cisco network switch involves several steps. Here's a basic guide to help you configure OSPF and verify connectivity on a Cisco switch:

Note: OSPF is typically configured on routers rather than switches. If you are working with a Layer 3 switch, you can configure OSPF on the switch. If you are using a Layer 2 switch, you would configure OSPF on a connected router.

1. Access Switch CLI:

- Access the command-line interface (CLI) of your Cisco switch using a console cable, Telnet, or SSH.

2. Enter Global Configuration Mode:

- Enter global configuration mode by typing:
switch> enable switch# configure terminal

3. Configure OSPF:

- Enter OSPF configuration mode and specify an OSPF process ID (e.g., 1):
switch(config)# router ospf 1

4. Assign Router ID:

- Assign a router ID to the switch. This can be done manually or left to the system to choose. For manual assignment:
switch(config-router)# router-id <router_id>

5. Enable OSPF on Interfaces:

- Enable OSPF on the interfaces participating in OSPF. For each interface, use:

switch(config-router)# network <network_address> <wildcard_mask> area <area_id>

6. Verify OSPF Configuration:

- Verify OSPF configuration using the following commands:
switch# show ip ospf switch# show ip ospf interface

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

7. Exit Configuration Mode:

- Exit OSPF configuration mode and return to global configuration mode:
switch(config-router)# exit

8. Save Configuration:

- Save the configuration to ensure it persists after a reboot:
switch# write memory

9. Verify Connectivity:

- Verify OSPF connectivity by checking OSPF neighbor relationships and routing tables. Use commands such as:
switch# show ip ospf neighbor switch# show ip route

10. Test Connectivity:

- Test connectivity between devices in different OSPF areas to ensure that OSPF is routing traffic correctly.

11. Troubleshoot if Necessary:

- If there are issues with OSPF adjacency or routing, use troubleshooting commands like:
switch# show ip ospf interface switch# show ip ospf database

12. Monitor OSPF:

- Continuously monitor OSPF using commands such as:
switch# debug ip ospf events switch# debug ip ospf adj

13. Disable Debugging:

- Once troubleshooting is complete, disable debugging:
switch# undebug all

14. Save Final Configuration:

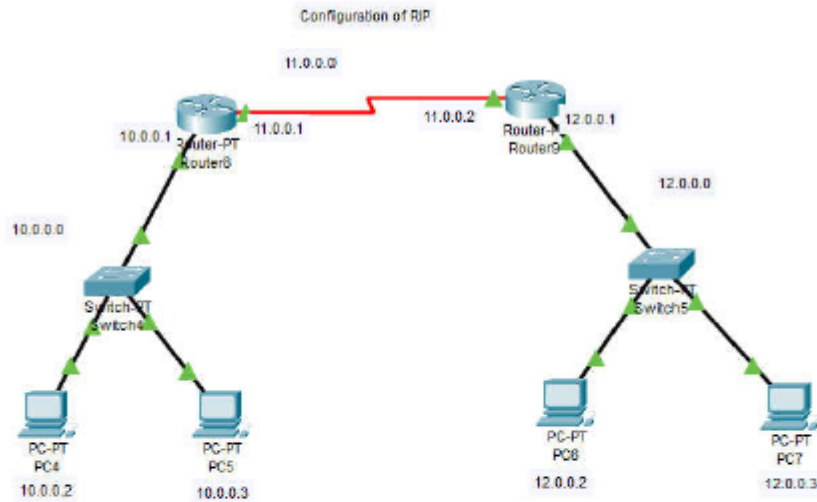
- Save the final configuration to ensure that it is persistent:
switch# write memory

By following these steps, you can configure OSPF on a Cisco switch, verify the OSPF configuration, and ensure proper connectivity.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Configuration of RIP (Routing Information Protocol)



Configuration for PCs

| | |
|---|---|
| PC4 IP Address: 10.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 | PC5 IP Address: 10.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 |
| PC6 IP Address: 12.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 | PC7 IP Address: 12.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 |

Configuration for Routers

| Fast Ethernet Port Configuration | |
|---|---|
| Router 8 Router>en Router#config t Router(config)# int f0/0 Router(config-if)# ip address 10.0.0.1 255.0.0.0 Router(config-if)# no shut | Router 9 Router>en Router#config t Router(config)# int f0/0 Router(config-if)# ip address 12.0.0.1 255.0.0.0 Router(config-if)# no shut |
| Serial Port Configuration | |
| Router 8 Router#config t Router(config)# int s2/0 Router(config-if)# ip address 11.0.0.1 255.0.0.0 Router(config-if)# no shut | Router 9 Router#config t Router(config)# int s2/0 Router(config-if)# ip address 11.0.0.2 255.0.0.0 Router(config-if)# no shut |
| RIP Configuration | |
| Router 8 Router#config t Router(config)# router rip Router(config-router)# network 10.0.0.0 Router(config-router)# network 11.0.0.0 | Router 9 Router#config t Router(config)# router rip Router(config-router)# network 11.0.0.0 Router(config-router)# network 12.0.0.0 |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Output

To check whether the OSPF configuration is running properly let's go to the command prompt of PC4 and give the following command as below

C:\>ping 12.0.0.2 (pinging PC6)

The output is as follows

```

Command Prompt

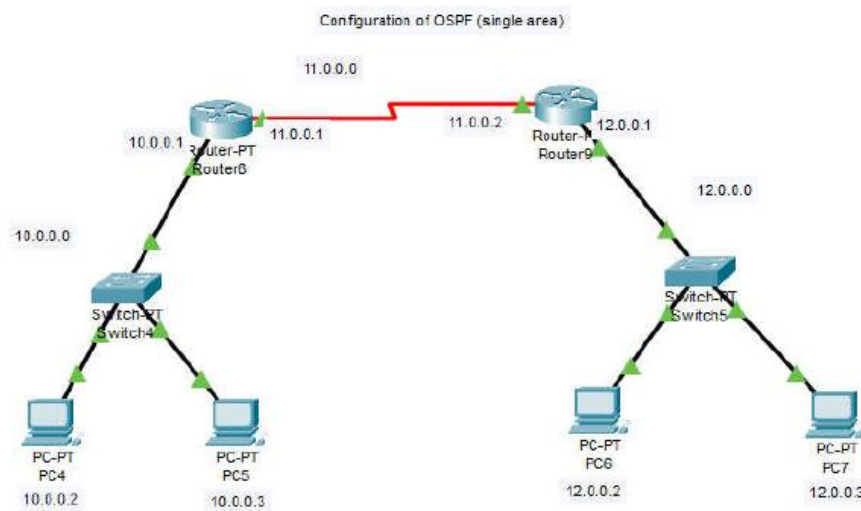
C:\>ping 12.0.0.2

Pinging 12.0.0.2 with 32 bytes of data:

Reply from 12.0.0.2: bytes=32 time=18ms TTL=126
Reply from 12.0.0.2: bytes=32 time=12ms TTL=126
Reply from 12.0.0.2: bytes=32 time=15ms TTL=126
Reply from 12.0.0.2: bytes=32 time=15ms TTL=126

Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 18ms, Average = 15ms
    
```

Configuration of OSPF (Open Shortest Path First Protocol)-Single Area



Configuration for PCs

| | |
|---|---|
| PC4 IP Address: 10.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 | PC5 IP Address: 10.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 |
| PC6 IP Address: 12.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 | PC7 IP Address: 12.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Configuration for Routers

| <u>Fast Ethernet Port Configuration</u> | |
|---|---|
| <u>Router 8</u> Router>en Router#config t Router(config)# int f0/0 Router(config-if)# ip address 10.0.0.1 255.0.0.0 Router(config-if)# no shut | <u>Router 9</u> Router>en Router#config t Router(config)# int f0/0 Router(config-if)# ip address 12.0.0.1 255.0.0.0 Router(config-if)# no shut |
| <u>Serial Port Configuration</u> | |
| <u>Router 8</u> Router#config t Router(config)# int s2/0 Router(config-if)# ip address 11.0.0.1 255.0.0.0 Router(config-if)# no shut | <u>Router 9</u> Router#config t Router(config)# int s2/0 Router(config-if)# ip address 11.0.0.2 255.0.0.0 Router(config-if)# no shut |
| <u>OSPF (Single Area) Configuration</u> | |
| <u>Router 8</u> Router#config t Router(config)# router ospf 1 Router(config-router)# network 10.0.0.0 0.255.255.255 area 0 Router(config-router)# network 11.0.0.0 0.255.255.255 area 0 | <u>Router 9</u> Router#config t Router(config)# router ospf 1 Router(config-router)# network 11.0.0.0 0.255.255.255 area 0 Router(config-router)# network 12.0.0.0 0.255.255.255 area 0 |

Output

To check whether the OSPF configuration is running properly lets go to the command prompt of PC4 and give the following command as below

C:\>ping 12.0.0.2 (pinging PC6)

The output is as follows

```
Command Prompt

C:\>ping 12.0.0.2

Pinging 12.0.0.2 with 32 bytes of data:

Reply from 12.0.0.2: bytes=32 time=18ms TTL=126
Reply from 12.0.0.2: bytes=32 time=12ms TTL=126
Reply from 12.0.0.2: bytes=32 time=15ms TTL=126
Reply from 12.0.0.2: bytes=32 time=15ms TTL=126

Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 18ms, Average = 16ms
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Conclusion

By following these steps, we successfully configured RIP and OSPF on Cisco network switches using Cisco Packet Tracer. The process involved:

- Enabling and configuring RIP for simple, distance-vector routing in smaller networks.
- Enabling and configuring OSPF for efficient, link-state routing in larger and more complex networks.
- Verifying routing tables and neighbor relationships to ensure proper route advertisement and learning.

Configuring both RIP and OSPF enhances the network's ability to dynamically learn and advertise routes, improving overall network efficiency and reliability. RIP is straightforward and easy to configure, making it suitable for smaller networks with limited complexity. OSPF, on the other hand, provides more advanced features and scalability, making it ideal for larger enterprise networks. Understanding and implementing these routing protocols is crucial for network administrators to ensure optimal routing performance and network connectivity in various environments.

| | | |
|-----------------------|---|-------------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 9: Configuration of Network address translation in Cisco packet tracer

Learning outcome:

- Learners will gain a solid understanding of Network Address Translation and its role in IP address translation between private and public networks.
- Learners will acquire hands-on experience in configuring different types of NAT in Cisco Packet Tracer.

Network Address Translation (NAT) is a technique used to translate private IP addresses to public IP addresses, allowing multiple devices on a local network to share a single public IP address for accessing the internet. Here's how to configure NAT on a Cisco router using Cisco Packet Tracer.

Step-by-Step Guide to Configuring NAT

Step 1: Set Up the Network Topology

1. **Add Devices:** Place a router, a switch, and multiple PCs in the workspace.
2. **Connect Devices:** Connect the PCs to the switch, and then connect the switch to the router's LAN interface. Connect the router's WAN interface to a simulated internet cloud or another router representing the ISP.

Step 2: Configure IP Addresses

1. **Assign IP Addresses to PCs:**
 - PC1: IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1
 - PC2: IP Address: 192.168.1.3, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1
2. **Configure the Router's LAN Interface:**
Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
3. **Configure the Router's WAN Interface:**
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip address 200.200.200.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Step 3: Configure the Default Route

Router(config)# ip route 0.0.0.0 0.0.0.0 200.200.200.2

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Step 4: Configure NAT

1. Define Inside and Outside Interfaces:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
```

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

2. Configure the Access Control List (ACL):

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

3. Configure NAT Overload (PAT):

```
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload
```

Step 5: Verify Configuration

1. Check NAT Translations:

```
Router# show ip nat translations
```

2. Check NAT Statistics:

```
Router# show ip nat statistics
```

Testing the Configuration

1. Ping an External IP Address from a PC:

- Open the command prompt on PC1.
- Execute the following command to ping an external IP address (e.g., 8.8.8.8):

```
ping 8.8.8.8
```

- If NAT is configured correctly, you should receive replies.

2. Check the NAT Translation Table on the Router:

```
Router# show ip nat translations
```

Example Configuration Summary

Here is a summarized version of the configurations:

Router Configuration:

enable

configure terminal

```
interface gigabitEthernet 0/0
```

```
ip address 192.168.1.1 255.255.255.0
```

```
ip nat inside
```

```
no shutdown
```

```
exit
```

```
interface gigabitEthernet 0/1
```

```
ip address 200.200.200.1 255.255.255.0
```

```
ip nat outside
```

```
no shutdown
```

```
exit
```

```
ip route 0.0.0.0 0.0.0.0 200.200.200.2
```

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

```
ip nat inside source list 1 interface gigabitEthernet 0/1 overload
```

```
end
```

```
write memory
```

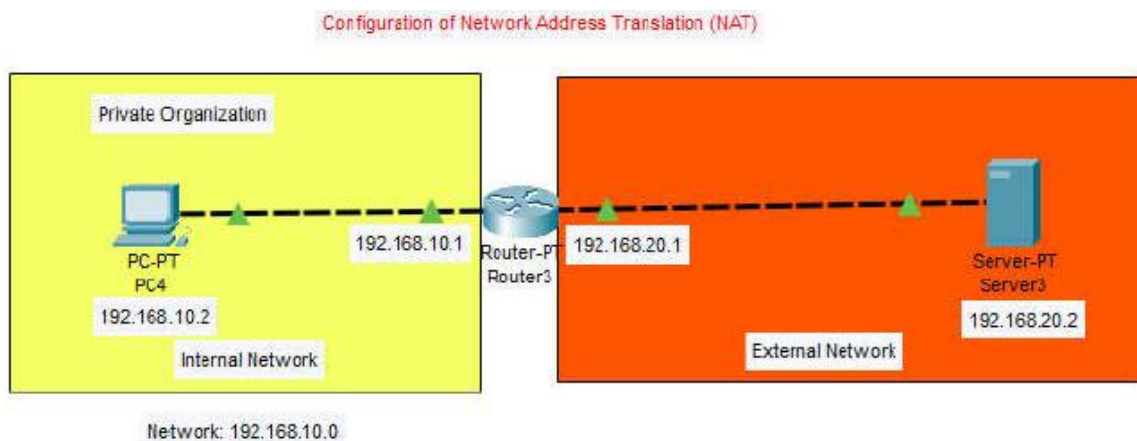
| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

PC Configuration:

- **PC1:**
 - IP Address: 192.168.1.2
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
- **PC2:**
 - IP Address: 192.168.1.3
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1

By following these steps, you will have successfully configured NAT on a Cisco router using Cisco Packet Tracer, allowing devices on the local network to share a single public IP address for internet access.

Configuration of Static Network Address Translation (NAT)



Static NAT Configuration

```
Router(config)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int f1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)# ip nat inside source static 192.168.10.2 100.100.100.100
Router(config)#exit
Router# debug ip nat
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Configuration for PCs

PC4

IP Address: 192.168.10.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.1

Server3

IP Address: 192.168.20.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.1

Configuration for Routers

Fast Ethernet Port Configuration

Router 2

```
Router>en
Router#config t
Router(config)# int f0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)#exit

Router(config)# int f1/0
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shut
```

RIP Configuration

Router 2

```
Router#config t
Router(config)# router rip
Router(config-router)# network 192.168.10.0
Router(config-router)# network 192.168.20.0
```

Output

To check whether the NAT configuration is running properly let's go to the Router and enable the NAT by giving the command “debug ip nat”

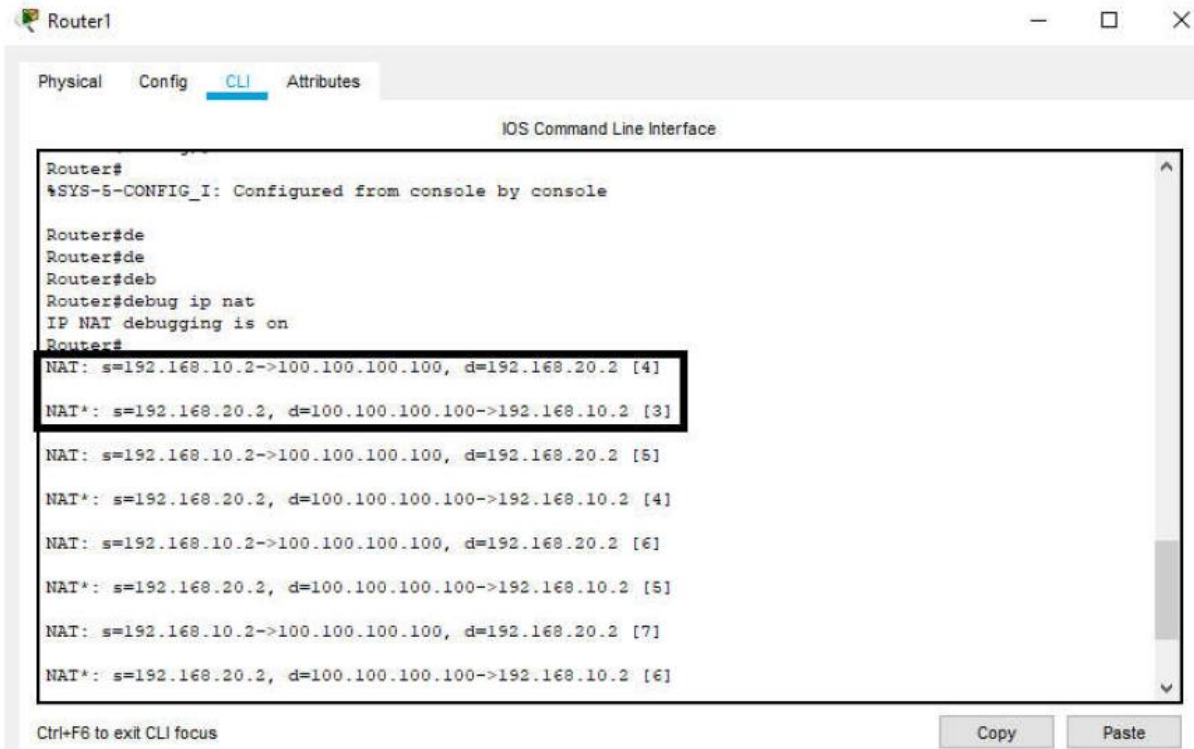
Then go to the command prompt of the PC4 and give the following command

C:\> ping 192.168.20.2

The output is as follows which means the conversion of private IP to public IP is successful.
The private IP -> 192.168.10.2 has been converted to the public IP -> 100.100.100.100

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



The screenshot shows the Cisco Packet Tracer interface for Router1. The 'CLI' tab is selected, displaying the IOS Command Line Interface. The configuration includes enabling NAT debugging and setting up static NAT mappings. The output shows successful configuration of two static NAT entries.

```
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router#de  
Router#de  
Router#deb  
Router#debug ip nat  
IP NAT debugging is on  
Router#  
NAT: s=192.168.10.2->100.100.100.100, d=192.168.20.2 [4]  
NAT*: s=192.168.20.2, d=100.100.100.100->192.168.10.2 [3]  
  
NAT: s=192.168.10.2->100.100.100.100, d=192.168.20.2 [5]  
NAT*: s=192.168.20.2, d=100.100.100.100->192.168.10.2 [4]  
  
NAT: s=192.168.10.2->100.100.100.100, d=192.168.20.2 [6]  
NAT*: s=192.168.20.2, d=100.100.100.100->192.168.10.2 [5]  
  
NAT: s=192.168.10.2->100.100.100.100, d=192.168.20.2 [7]  
NAT*: s=192.168.20.2, d=100.100.100.100->192.168.10.2 [6]
```

Conclusion

By following these steps, we successfully configured static NAT on a Cisco router using Cisco Packet Tracer. The process involved:

- Setting up the network topology with appropriate device connections.
- Assigning IP addresses to both LAN and WAN interfaces.
- Defining inside and outside NAT interfaces.
- Configuring static NAT to map a private internal IP to a specific public external IP.
- Verifying the configuration and testing connectivity to ensure proper operation.

Configuring static NAT is essential for scenarios where a device inside the private network needs to be accessible from the outside world using a fixed public IP address. This ensures that services such as web servers and other applications remain reachable and provide consistent service. Properly implemented static NAT enhances network functionality, enabling seamless communication between private internal networks and external public networks.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 10: Configure the Standard and Extended Access Control List using cisco packet tracer and verify the configuration

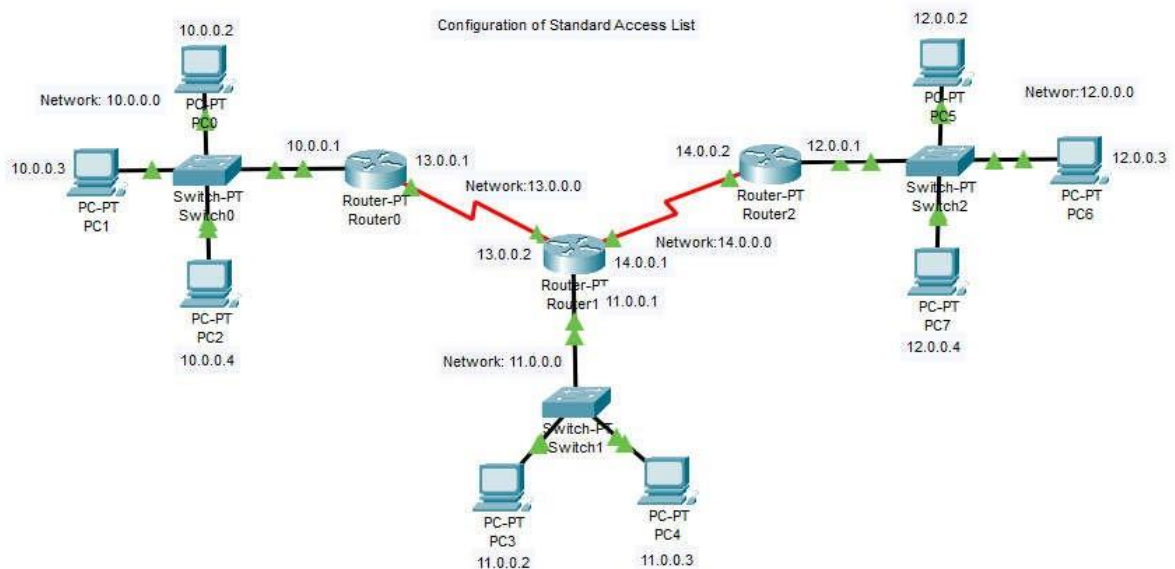
Learning outcome:

- Learn how to access and navigate Cisco Packet Tracer and Cisco IOS for configuration tasks.
- Gain hands-on experience in creating Standard ACLs using source IP addresses.
- Acquire skills in creating Extended ACLs with criteria including source and destination IP addresses, protocols, and port numbers.
- Apply Standard and Extended ACLs to network interfaces in both inbound and outbound directions.
- Understand the implications of applying ACLs in different directions on network traffic.

• Configuration of Standard Access List

- PC0(10.0.0.2),
- PC1(10.0.0.3) and
- the network (12.0.0.0) from accessing the network
- 11.0.0.0

Network Topology



- Configuration for PCs

PC0

IP Address: 10.0.0.2
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

PC1

IP Address: 10.0.0.3
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

PC2

IP Address: 10.0.0.4
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

| | | |
|--|--|--|
| <u>PC3</u> IP Address: 11.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 11.0.0.1 | <u>PC4</u> IP Address: 11.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 11.0.0.1 | |
| <u>PC5</u> IP Address: 12.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 | <u>PC6</u> IP Address: 12.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 | <u>PC7</u> IP Address: 12.0.0.4 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1 |

-
-
- **Configuration for Routers**

| <u>Fast Ethernet Port Configuration</u> | | |
|---|---|---|
| <u>Router0</u> Router>en Router#hostname R1 R1#config t R1(config)# int f0/0 R1(config-if)# ip address 10.0.0.1 255.0.0.0 R1(config-if)# no shut | <u>Router1</u> Router>en Router#hostname R2 R2#config t R2(config)# int f0/0 R2(config-if)# ip address 11.0.0.1 255.0.0.0 R2(config-if)# no shut | <u>Router2</u> Router>en Router#hostname R3 R2#config t R2(config)# int f0/0 R2(config-if)# ip address 12.0.0.1 255.0.0.0 R2(config-if)# no shut |
| <u>Serial Port Configuration</u> | | |
| <u>Router0</u> R1#config t R1(config)# int s2/0 R1(config-if)# ip address 13.0.0.1 255.0.0.0 R1(config-if)# no shut | <u>Router1</u> R2#config t R2(config)# int s2/0 R2(config-if)# ip address 13.0.0.2 255.0.0.0 R2(config-if)# no shut R2(config-if)# exit R2(config)# int s3/0 R2(config-if)# ip address 14.0.0.1 255.0.0.0 R2(config-if)# no shut | <u>Router2</u> R2#config t R2(config)# int s2/0 R2(config-if)# ip address 14.0.0.2 255.0.0.0 R2(config-if)# no shut |
| <u>Routing Protocol Configuration</u> | | |
| <u>Router0</u> R1#config t R1(config)# router rip R1(config-router)# network 10.0.0.0 R1(config-router)# network 13.0.0.0 | <u>Router1</u> R2#config t R2(config)# router rip R2(config-router)# network 11.0.0.0 R2(config-router)# network 13.0.0.0 R2(config-router)# network 14.0.0.0 | <u>Router2</u> R2#config t R2(config)# router rip R2(config-router)# network 12.0.0.0 R2(config-router)# network 14.0.0.0 |
| <u>Standard Access List Configuration</u> | | |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Router1

```
R1#config t
R1(config)# access-list 10 deny 10.0.0.2 0.0.0.0
R1(config)# access-list 10 deny host 10.0.0.3
R1(config)# access-list 10 deny 12.0.0.0 0.0.0.255
R1(config)# access-list 10 permit any
R1(config)# int f0/0
R1(config-if)# ip access-group 10 out
```

-
- **Output**
- To check whether the standard access list is working properly or not, we ping the PC3(11.0.0.2) from the PC0 (10.0.0.2) which had been blocked and we get the following result.

- **Pinging from 10.0.0.2(PC0)**

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

-
- **Pinging from 10.0.0.2(PC2)**
- Again we ping the PC3(11.0.0.2) from the PC2 (10.0.0.4) which had not been blocked and we get the following result.

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 11.0.0.2: bytes=32 time=1ms TTL=126
Reply from 11.0.0.2: bytes=32 time=12ms TTL=126
Reply from 11.0.0.2: bytes=32 time=4ms TTL=126
Reply from 11.0.0.2: bytes=32 time=13ms TTL=126

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 7ms
```

-
- **Pinging from 12.0.0.3(PC6)**
- Again we ping the PC3(11.0.0.2) from the PC5 (12.0.0.2) which had been blocked and we get the following result.

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.

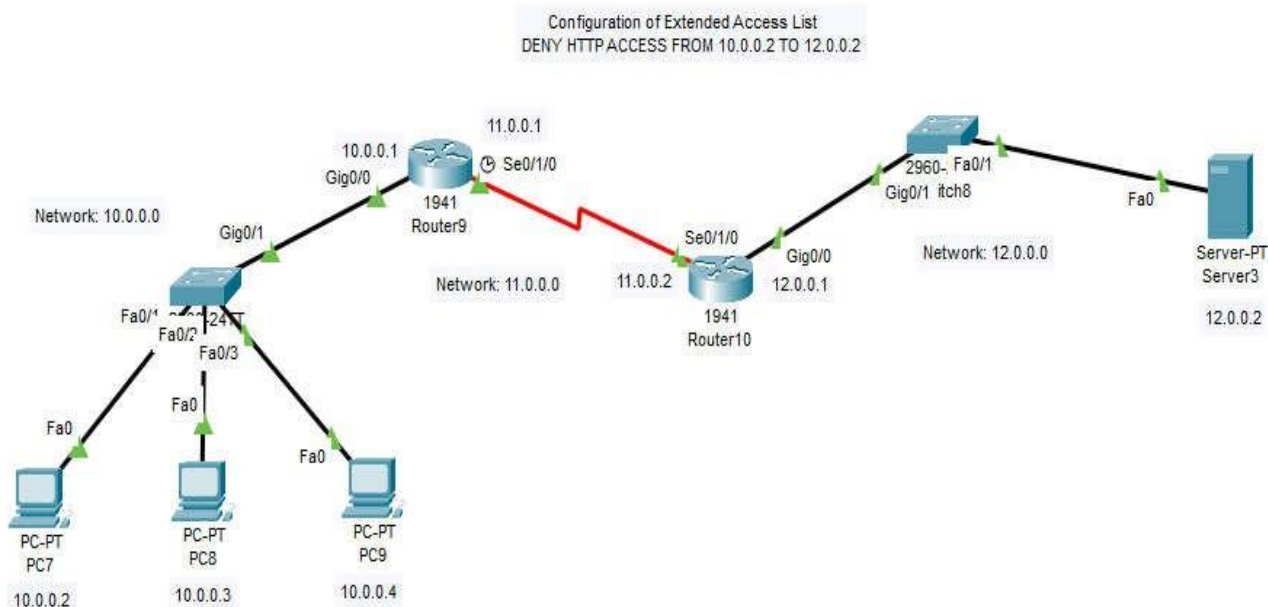
Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

CONFIGURATION OF EXTENDED ACCESS LIST

(Blocking host 10.0.0.2 to access web page running on Server 12.0.0.2)



Addressing Table

| Network Devices | Interface | IP Address | Default Mask | Gateway |
|-------------------|------------------------|------------|--------------|----------|
| PC-7 | Fast Ethernet (Fa0) | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| PC-8 | Fast Ethernet (Fa0) | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 |
| PC-9 | Fast Ethernet (Fa0) | 10.0.0.4 | 255.0.0.0 | 10.0.0.1 |
| Server-PT Server3 | Fast Ethernet (Fa0) | 12.0.0.2 | 255.0.0.0 | 12.0.0.1 |
| Router9 | Gigabit Ethernet(g0/0) | 10.0.0.1 | 255.0.0.0 | - |
| | Serial (s0/1/0) | 11.0.0.1 | 255.0.0.0 | - |
| Router10 | Gigabit Ethernet(g0/0) | 12.0.0.1 | 255.0.0.0 | - |
| | Serial (s0/1/0) | 11.0.0.2 | 255.0.0.0 | - |

Configuration for PCs

PC7

IP Address: 10.0.0.2
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

PC8

IP Address: 10.0.0.3
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

PC9

IP Address: 10.0.0.4
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1

Configuration for Server

Server-PT Server 3

IP Address: 12.0.0.2
Subnet Mask: 255.0.0.0
Default Gateway: 12.0.0.1

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Configuration for Routers

Fast Ethernet Port Configuration

Router 9

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
```

Router 10

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 12.0.0.1 255.0.0.0
Router(config-if)#no shutdown
```

Serial Port Configuration

Router 9

```
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
```

Router 10

```
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
```

Configuration of RIP

Router 9

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 11.0.0.0
```

Router 10

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)# network 11.0.0.0
Router(config-router)# network 12.0.0.0
```

Extended Access List Configuration

Router 9

```
Router(config)#ip access-list extended 120
Router(config-ext-nacl)#deny tcp host 10.0.0.2 host 12.0.0.2 eq 80
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#int g0/0
Router(config-if)#ip access-group 120 in
Router(config-if)#
```

OUTPUT

Before configuration of Extended Access List

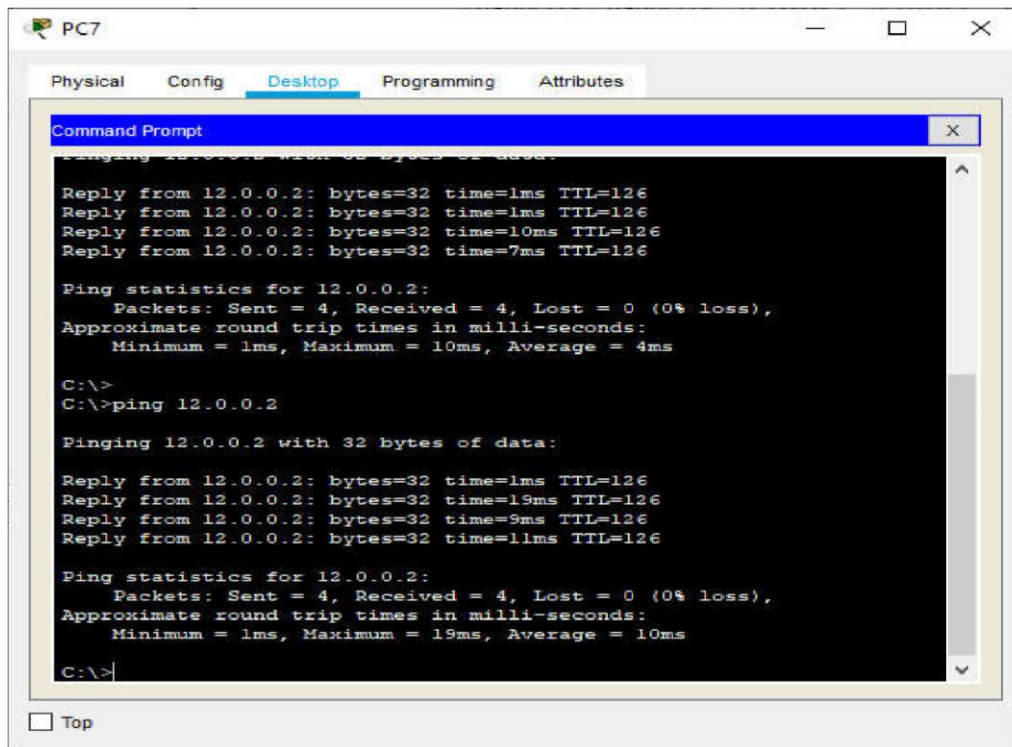
To check whether the Extended Access List configuration is running properly lets go to the command prompt of PC4 and give the following command as below

C:\>ping 12.0.0.2 (pinging Server-PT Server 3)

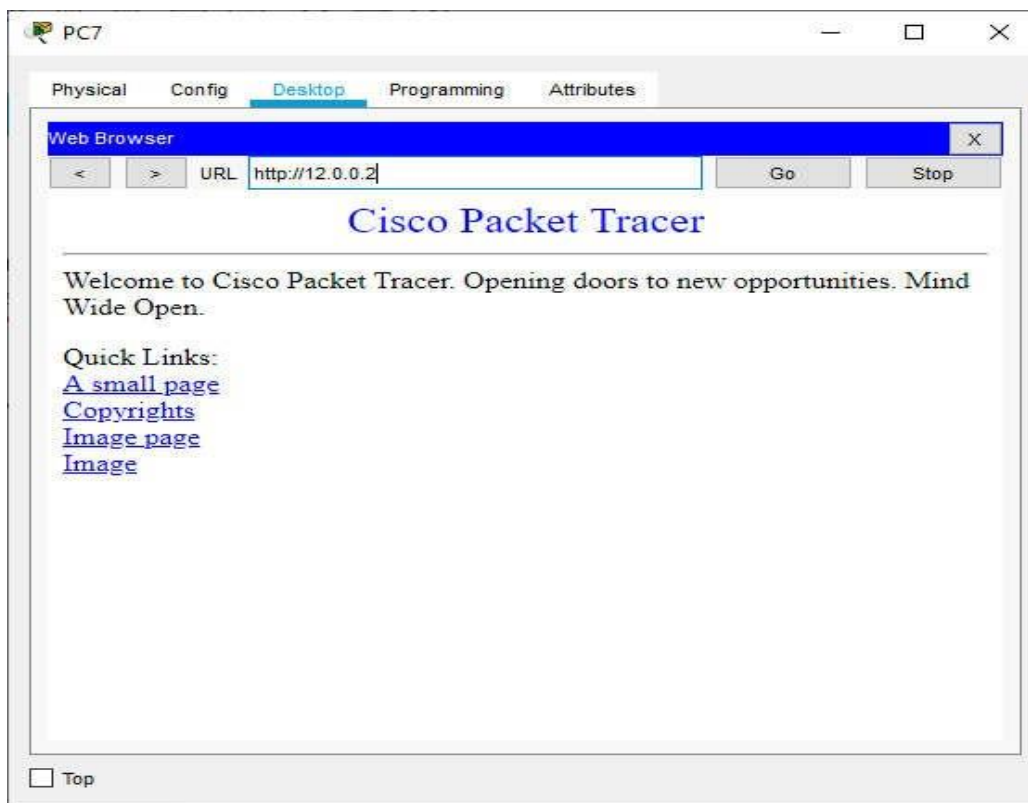
The output is as follows for service-1

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



For HTTP (WWW) Service

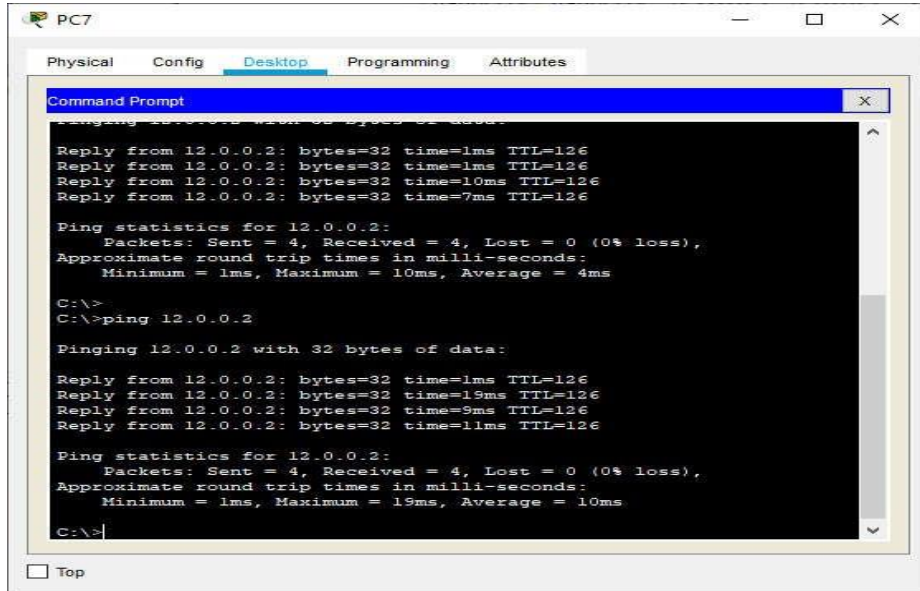


| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

After Configuration of Extended Access List

C:\>ping 12.0.0.2 (pinging Server-PT Server 3)

The output is as follows for service-1



```
PC7
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 12.0.0.2 with 32 bytes of data:
Reply from 12.0.0.2: bytes=32 time=1ms TTL=126
Reply from 12.0.0.2: bytes=32 time=1ms TTL=126
Reply from 12.0.0.2: bytes=32 time=10ms TTL=126
Reply from 12.0.0.2: bytes=32 time=7ms TTL=126

Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 4ms

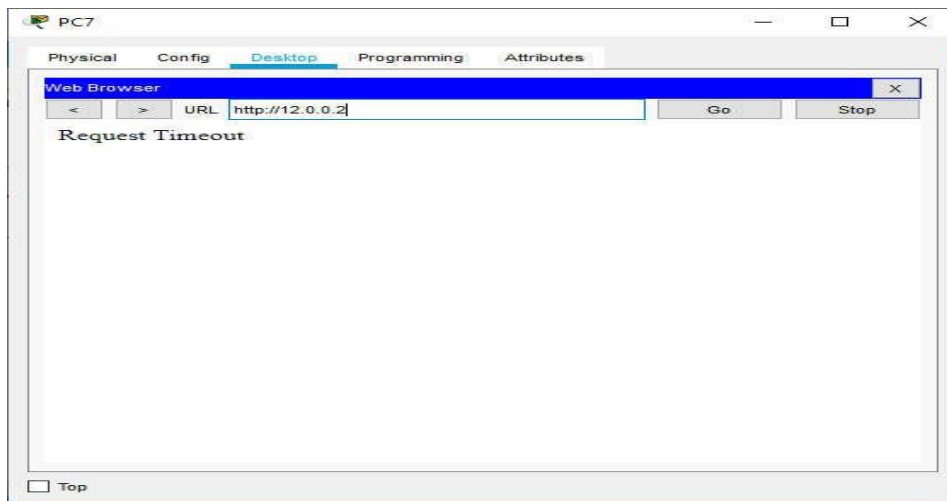
C:\>
C:\>ping 12.0.0.2

Pinging 12.0.0.2 with 32 bytes of data:
Reply from 12.0.0.2: bytes=32 time=1ms TTL=126
Reply from 12.0.0.2: bytes=32 time=19ms TTL=126
Reply from 12.0.0.2: bytes=32 time=9ms TTL=126
Reply from 12.0.0.2: bytes=32 time=11ms TTL=126

Ping statistics for 12.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 10ms

C:\>
```

For HTTP (WWW) Service



Conclusion

Standard ACLs are useful for simple filtering needs, while Extended ACLs provide more granular control over traffic, enhancing security and network management. Proper implementation of ACLs ensures that only authorized traffic is allowed, protecting network resources from unauthorized access and potential threats. By mastering the configuration of Standard and Extended ACLs, network administrators can effectively manage and secure their network environments.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 11: Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection

Learning outcome:

- Learners will gain a solid understanding of SMTP, FTP, DNS, and HTTP
- Learners will acquire hands-on experience in configuring SMTP, FTP, DNS, and HTTP services using Cisco Packet Tracer.
- Understand the basic concepts of DHCP, including IP address allocation, lease duration, and the role of DHCP servers

Implementation of SMTP, FTP, DNS and HTTP in Cisco packet tracer

In Cisco Packet Tracer, you can simulate the implementation of various network protocols such as SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), and HTTP (Hypertext Transfer Protocol) to understand how these protocols work in a network environment. Here are the general steps for implementing these protocols:

SMTP (Simple Mail Transfer Protocol):

1. Topology Setup:
 - Create a network topology in Cisco Packet Tracer with devices such as routers, switches, and PCs.
2. Device Configuration:
 - Configure an email client on a PC (e.g., Outlook) and an email server (e.g., Mail Server) on another PC.
3. SMTP Configuration:
 - On the email client, configure the SMTP settings to point to the IP address or domain name of the email server.
4. Email Testing:
 - Send test emails from the client to the server to simulate the SMTP communication.

FTP (File Transfer Protocol):

1. Topology Setup:
 - Create a network topology with devices that support FTP, such as PCs or servers.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

2. Device Configuration:

- Set up an FTP server on one PC and configure an FTP client on another.

3. FTP Configuration:

- Configure the FTP client with the server's IP address or domain.

4. File Transfer:

- Initiate file transfers from the client to the server or vice versa to simulate FTP communication.

DNS (Domain Name System):

1. Topology Setup:

- Create a network topology with DNS servers, client devices, and routers.

2. Device Configuration:

- Set up a DNS server on a PC or a dedicated DNS server device. Configure client devices to use the DNS server.

3. DNS Configuration:

- Populate the DNS server with domain names and corresponding IP addresses.

4. Name Resolution:

- Test DNS name resolution by attempting to access websites using domain names from client devices.

HTTP (Hypertext Transfer Protocol):

1. Topology Setup:

- Set up a network topology with web servers, client devices, and routers.

2. Device Configuration:

- Configure a web server on a PC or a dedicated web server device. Set up web clients on other devices.

3. HTTP Configuration:

- Populate the web server with web pages or applications.

4. Web Browsing:

- Access web pages hosted on the server from client devices to simulate HTTP communication.

General Tips:

• Router Configuration:

- Ensure that routers are properly configured to route traffic between devices.

• Addressing:

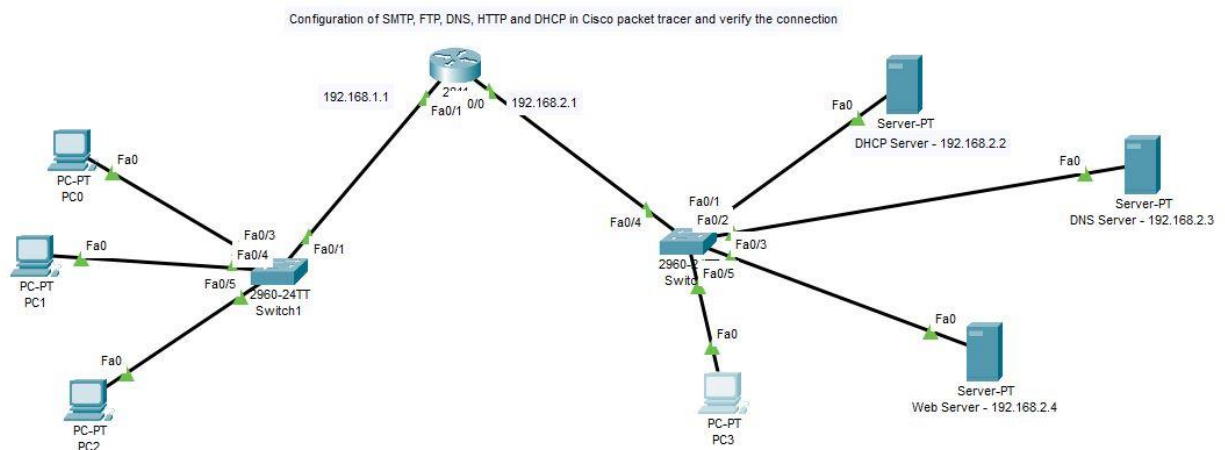
| | | |
|-----------------------|---|-------------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

- Use proper IP addressing and subnetting to ensure devices can communicate within the network.
- Firewall Settings:
 - Adjust firewall settings on devices if necessary to allow traffic for the respective protocols.
- Packet Tracer Simulation:
 - Utilize Packet Tracer's simulation mode to observe the flow of packets and troubleshoot any issues.

By following these steps, you can simulate the implementation of SMTP, FTP, DNS, and HTTP in Cisco Packet Tracer, allowing you to understand how these protocols operate in a network environment.

Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection



ADDRESSING TABLE

| Device Name | Device Configuration Name | IP Address |
|-------------|---------------------------|--|
| PC0 | Client PC | DHCP |
| PC1 | Client PC | DHCP |
| PC2 | Client PC | DHCP |
| PC3 | Client PC | DHCP |
| Switch-1 | Switch 2960 | - |
| Switch-2 | Switch 2960 | - |
| Router0 | 2811 | Fa0/1 - 192.168.1.1 Fa0/0 – 192.168.2.1 |
| Server PT | Web Server | 192.168.2.4 |
| Server PT | DNS Server | 192.168.2.3 |
| Server PT | DHCP | 192.168.2.2 |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

CONFIGURATION

| | |
|--|--|
| Server PT (Web Server) IP Address- 192.168.2.4 Subnet Mask-255.255.255.0 Default Gateway: 192.168.1.1 DNS Server- 192.168.2.3 | Server PT (DHCP Server) IP Address- 192.168.2.2 Subnet Mask-255.255.255.0 Default Gateway: 192.168.1.1 DNS Server- 192.168.2.3 |
| Server PT(DNS Server) IP Address- 192.168.2.3 Subnet Mask-255.255.255.0 Default Gateway: 192.168.1.1 DNS Server- 192.168.2.3 | |

Router CONFIGURATION – CLI commands

| | |
|--|--|
| <u>DHCP configuration</u> Router> Router>en Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#int fa0/1 Router(config-if)#ip address 192.168.1.1 255.255.255.0 Router(config-if)#int fa0/0 Router(config-if)#ip address 192.168.2.1 255.255.255.0 Router(config-if)#exit | Router(config)#int fa0/1 Router(config-if)#ip helper-address 192.168.2.2 Router(config-if)# |
|--|--|

| | | |
|-----------------------|---|-------------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

DHCP configuration

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.2.1

DNS Server: 192.168.2.3

Start IP Address: 192 168 2 10

Subnet Mask: 255 255 255 0

Maximum Number of Users: 50

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|-------------|-----------------|-------------|------------------|---------------|----------|-------------|-------------|
| serverPool1 | 192.168.1.1 | 192.168.2.3 | 192.168.1.10 | 255.255.255.0 | 50 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 192.168.2.1 | 192.168.2.3 | 192.168.2.10 | 255.255.255.0 | 50 | 0.0.0.0 | 0.0.0.0 |

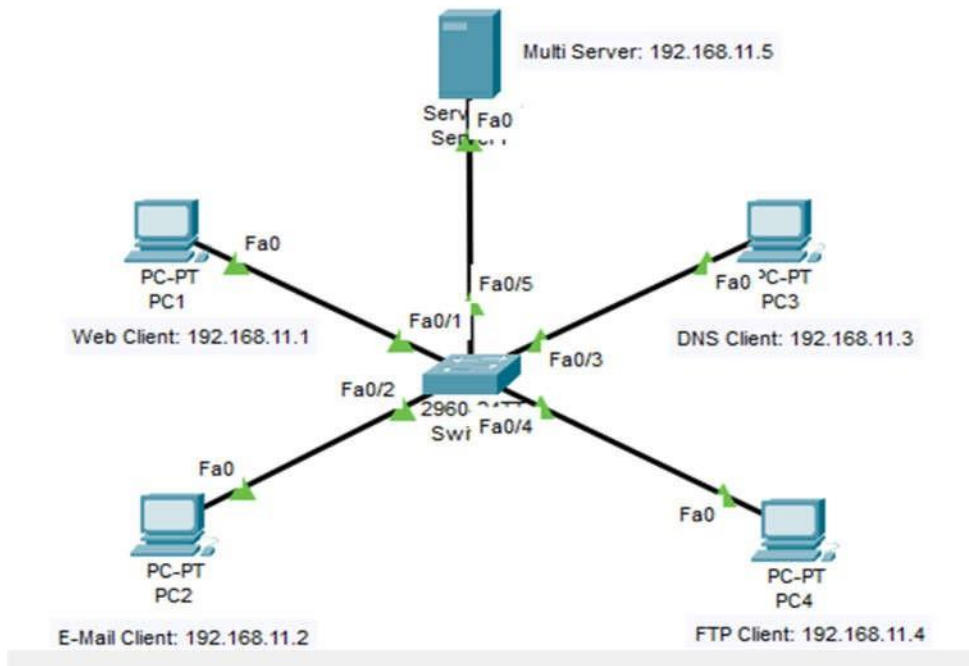
☐ Top

Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Analyze the PDU's for TCP and UDP communications using cisco packet tracer



ADDRESSING TABLE

| Device Name | Device Configuration Name | IP Address |
|-------------|---------------------------|--------------|
| PC1 | Web Client | 192.168.11.1 |
| PC2 | E-Mail Client | 192.168.11.2 |
| PC3 | DNS Client | 192.168.11.3 |
| PC4 | FTP Client | 192.168.11.4 |
| Server | Multi Server | 192.168.11.5 |

CONFIGURATION

| | | |
|---|--|---|
| PC1(Web Client) IP Address- 192.168.11.1 Subnet Mask-255.255.255.0 DNS Server- 192.168.11.5 | PC2(E-Mail Client) IP Address- 192.168.11.2 Subnet Mask-255.255.255.0 DNS Server- 192.168.11.5 | Server(Multi Server) IP Address- 192.168.11.5 Subnet Mask-255.255.255.0 DNS Server- 192.168.11.5 |
| PC3(DNS Client) IP Address- 192.168.11.3 Subnet Mask-255.255.255.0 DNS Server- 192.168.11.5 | PC4(FTP Client) IP Address- 192.168.11.4 Subnet Mask-255.255.255.0 DNS Server- 192.168.11.5 | |

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Service Configuration in Server

1. DNS service configuration

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record** ▼

Address

Add **Save** **Remove**

| No. | Name | Type | Detail |
|-----|------|------|--------|
|-----|------|------|--------|

DNS Cache

☐ Top

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record** ▼

Address

Add **Save** **Remove**

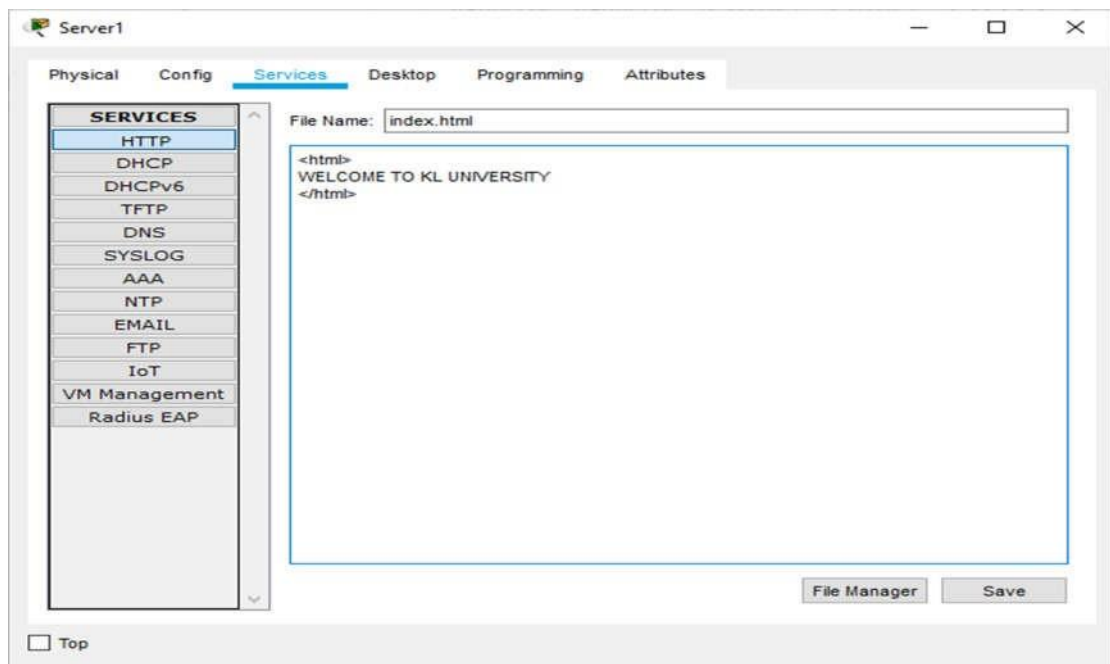
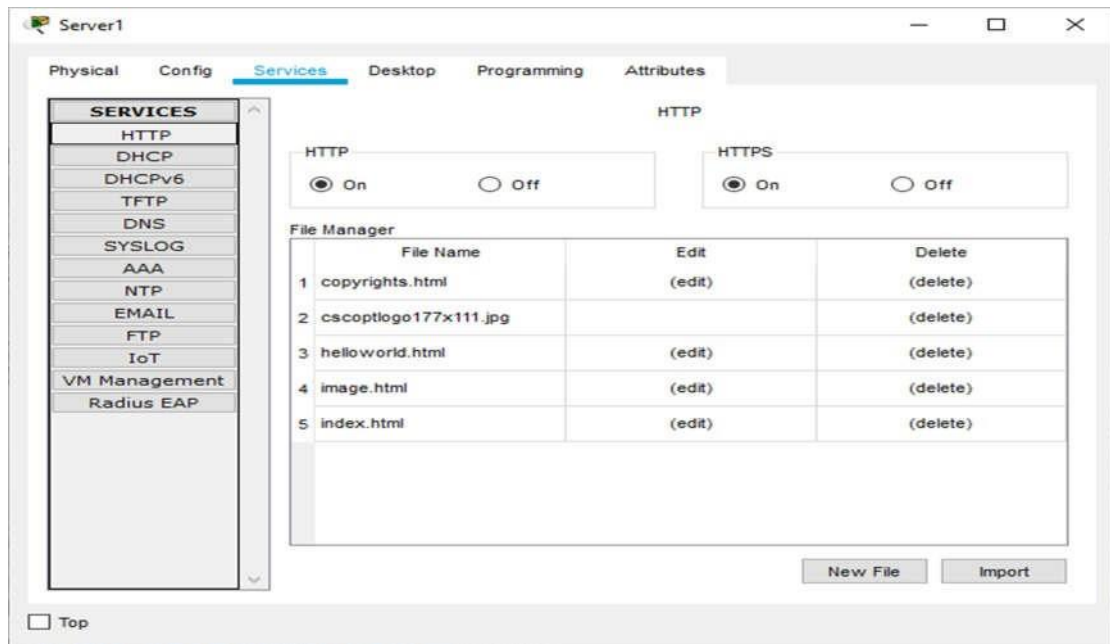
| No. | Name | Type | Detail |
|-----|----------------|----------|--------------|
| 0 | www.google.com | A Record | 192.168.11.5 |

DNS Cache

☐ Top

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

HTTP Service Configuration



To check the DNS resolution working properly, in the command prompt of **DNS Client** give the command in the command prompt `C:\>nslookup www.google.com`

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



```
Command Prompt

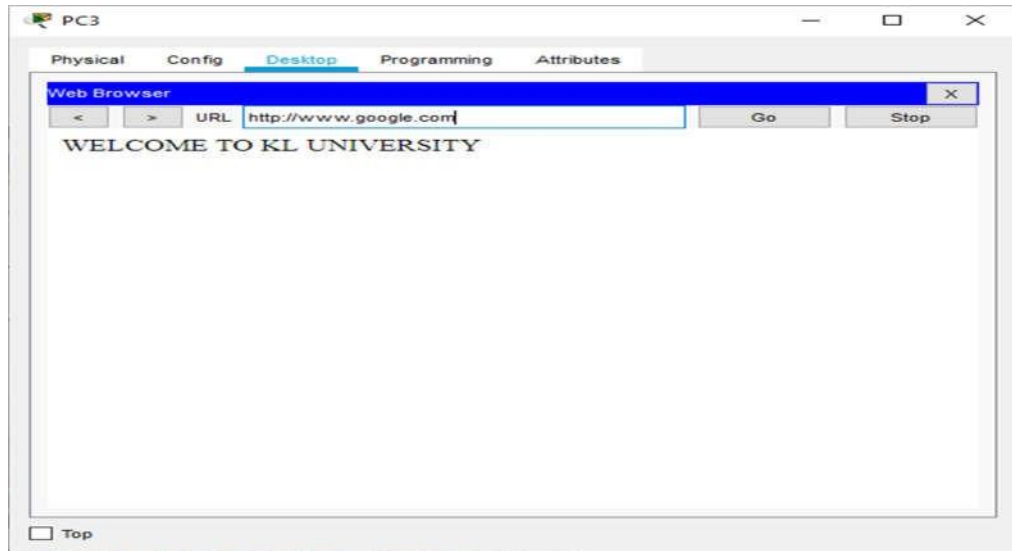
Packet Tracer PC Command Line 1.0
C:\>nslookup www.google.com

Server: [192.168.11.5]
Address: 192.168.11.5

Non-authoritative answer:
Name: www.google.com
Address: 192.168.11.5

C:\>|
```

Open the browser and give in the URL “www.google.com”



E-Mail configuration in PC1 (Web Client) and PC2 (E-Mail Client)

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

The screenshot shows a configuration window for PC1 with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Configure Mail' dialog is open, displaying the following fields:

- User Information:**
 - Your Name: Tushar
 - Email Address: tushar@gmail.com
- Server Information:**
 - Incoming Mail Server: 192.168.11.5
 - Outgoing Mail Server: 192.168.11.5
- Logon Information:**
 - User Name: tushar
 - Password: [masked]

Buttons at the bottom include Save, Clear, and Reset. A 'Top' link is at the bottom left.

The screenshot shows a configuration window for PC2 with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Configure Mail' dialog is open, displaying the following fields:

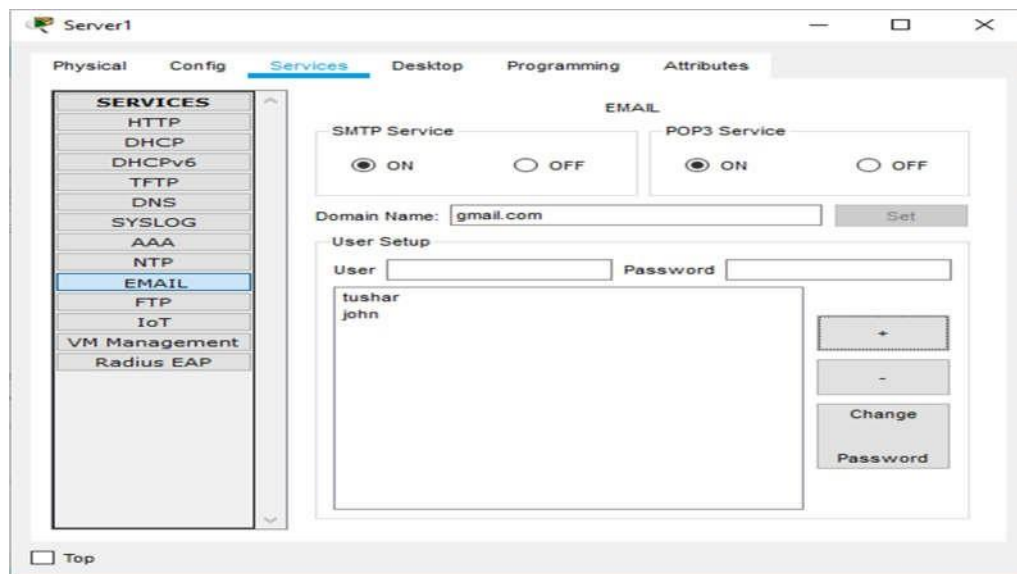
- User Information:**
 - Your Name: John
 - Email Address: john@gmail.com
- Server Information:**
 - Incoming Mail Server: 192.168.11.5
 - Outgoing Mail Server: 192.168.11.5
- Logon Information:**
 - User Name: john
 - Password: [masked]

Buttons at the bottom include Save, Clear, and Reset. A 'Top' link is at the bottom left.

E-Mail service configuration in server (Multi Server)

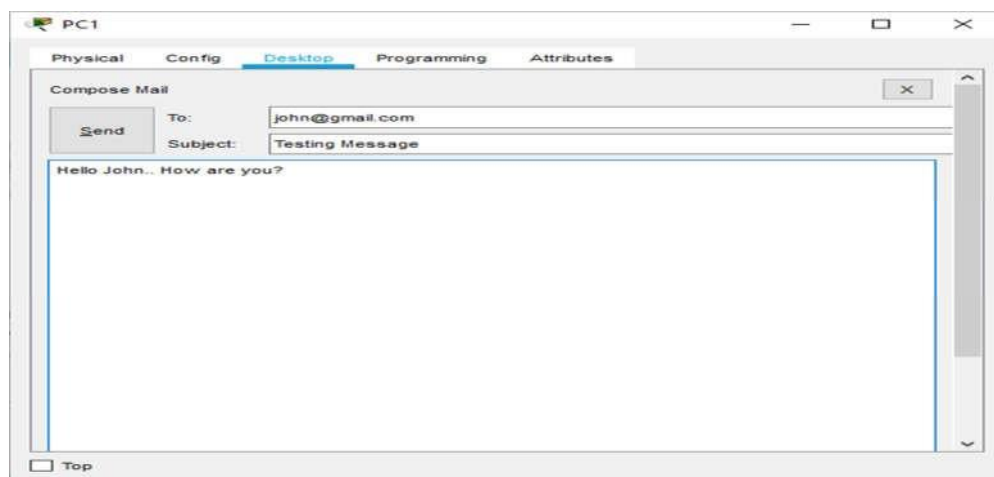
| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



Verification of the E-Mail configuration

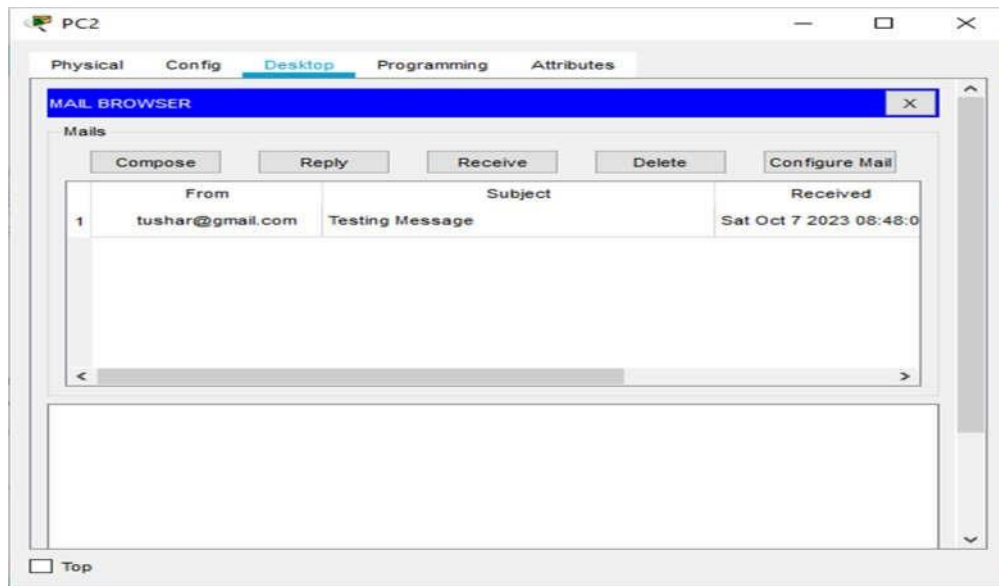
In PC1 (Web Client)



Go to Email of **PC2(E-Mail Client)** you will find the following message send from PC1(Web Client)

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

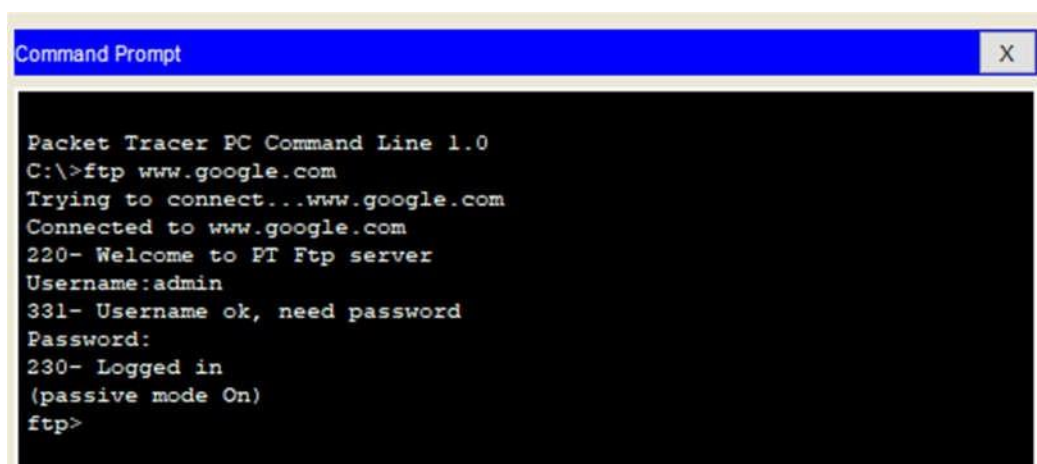
NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



FTP Configuration in Server



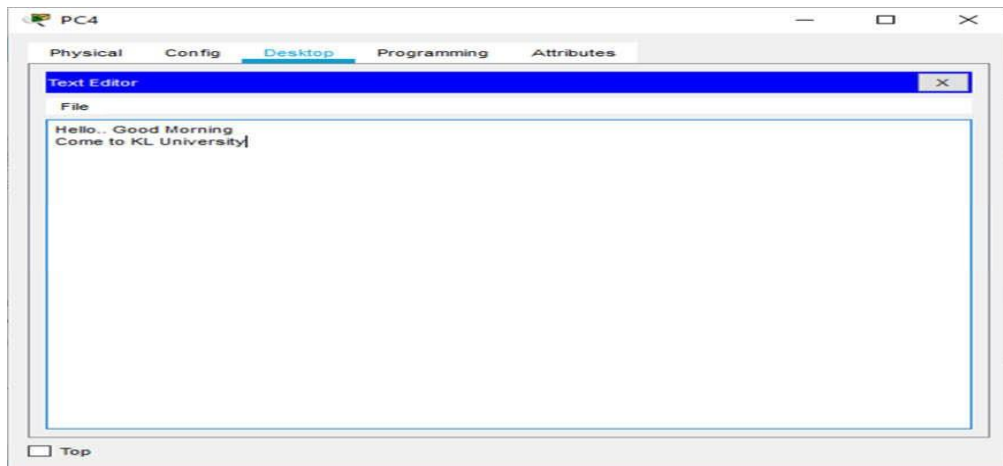
For checking FTP configuration in the command prompt of PC4 (FTP Client) give the command “ftp www.google.com”, you will get the following output



Now open the text editor of PC4 (FTP Client) and write some text and save as text.txt

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



From command prompt of PC4 (FTP Client) transfer the file to the server. For that first run the ftp service by giving command “c:\>ftp www.google.com”. Then provide the user ID and password. Then give the command “ftp>put text.txt” to upload the file in the server.

```
C:\>ftp www.google.com
Trying to connect...www.google.com
Connected to www.google.com
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put text.txt

Writing file text.txt to www.google.com:
File transfer in progress...

[Transfer complete - 42 bytes]

42 bytes copied in 0.051 secs (823 bytes/sec)
ftp>
```

From command prompt of PC3 (DNS Client) download the file from the server. For that first run the ftp service by giving command “c:\>ftp www.google.com”. Then provide the user ID and password. Then give the command “ftp>get text.txt” to download the file from the server.

```
Command Prompt
C:\>nslookup www.google.com

Server: [192.168.11.5]
Address: 192.168.11.5

Non-authoritative answer:
Name: www.google.com
Address: 192.168.11.5

C:\>ftp www.google.com
Trying to connect...www.google.com
Connected to www.google.com
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get text.txt

Reading file text.txt from www.google.com:
File transfer in progress...
```

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Implementation of DHCP in Cisco packet tracer

Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and other network configuration information to devices on a network.

Here are the steps involved in the implementation of DHCP in Cisco Packet Tracer:

1. Build the Network Topology:

- Launch Cisco Packet Tracer and create a network topology by adding devices such as routers, switches, and PCs to the workspace.
-

2. Configure Router Interfaces:

- Access the command-line interface (CLI) of the router where you want to configure DHCP.
- Enter global configuration mode using the enable command and then configure terminal.
- Navigate to the interface configuration mode (e.g., interface FastEthernet0/0) for the interface connected to the local network.
- Use the ip address command to assign an IP address and subnet mask to the interface.

3. Enable DHCP on the Router:

- Enter the DHCP configuration mode by using the ip dhcp pool command, followed by a pool name.
- Define the network address and subnet mask for the DHCP pool.
- Specify the range of IP addresses to be dynamically assigned to devices in the network using the network and default-router commands.

Example:

Router(config)# ip dhcp pool MY_POOL

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

Router(dhcp-config)# exit

4. Configure DNS Servers (Optional):

- Optionally, configure DNS servers to be assigned to DHCP clients using the dns-server command in DHCP pool configuration mode.

Example:

Router(dhcp-config)# dns-server 8.8.8.8

5. Enable DHCP on the Router Interface:

- Enter the interface configuration mode for the interface connected to the local network.
- Use the ip dhcp server command to enable DHCP on the interface.

Example:

Router(config)# interface FastEthernet0/0

Router(config-if)# ip dhcp server MY_POOL

Router(config-if)# exit

6. Verify DHCP Configuration:

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

- Use the show ip dhcp binding command on the router to view a list of devices that have obtained IP addresses from the DHCP server.

Example:

Router# show ip dhcp binding

7. Test DHCP Configuration:

- Power on the client devices (PCs) in the network and set their network interfaces to obtain IP addresses automatically (DHCP).

8. Observe DHCP Requests and Responses:

- Use Packet Tracer's simulation mode to observe DHCP request and response messages between clients and the DHCP server.

9. Document Your Configuration:

- Create documentation that includes the DHCP configuration settings, such as the pool name, network address, subnet mask, default gateway, and DNS server information.

10. Save Configuration: - Save your router's configuration to ensure that your DHCP settings are preserved even after a reboot. Use the write memory or copy running-config startup-config command.

By following these steps, you can successfully implement DHCP in Cisco Packet Tracer, providing dynamic IP address assignments to devices in your simulated network.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 12: Write a python program for Transposition Technique using Rail fence Technique and columnar Technique.

Learning outcome:

- Understand the principles and operations of both the Rail Fence and Columnar ciphers. Be familiar with their historical context and modern applications.
- Learn how to encrypt and decrypt messages using both the Rail Fence and Columnar ciphers. Understand the algorithms and processes involved
- Understand how the Rail Fence cipher works, where letters are written diagonally in a "zigzag" pattern..
- Understand where they are suitable and how they've been historically employed.

Rail fence Technique

Implementing the Rail Fence transposition technique is relatively straightforward. It involves arranging the characters of a plaintext message in a zigzag pattern along a set number of "rails" or rows, then reading the characters in a specific order to create the ciphertext.

Here are the steps for implementing the Rail Fence technique:

Step 1: Choose the Number of Rails (Rows)

- Decide on the number of rails or rows you want to use for the Rail Fence. This determines the depth of the zigzag pattern.

Step 2: Prepare the Plaintext

- Take your plaintext message, remove spaces, and special characters if necessary, and ensure it is in a suitable format.

Step 3: Create the Zigzag Pattern

- Start at the top-left corner of your rail (row 1).
- Write the first character of your plaintext in this position.
- Continue writing characters diagonally, moving down one rail after each character, until you reach the bottom rail.
- When you reach the bottom rail, start moving diagonally up toward the top rail, following the zigzag pattern. Repeat this process until you've used all characters from your plaintext.

Step 4: Reading the Ciphertext

- Read the characters along each rail from left to right, starting with the top rail and moving downward.
- Concatenate the characters from each rail to form the ciphertext.

Step 5: Encryption Example

- Let's say you have a plaintext message: "HELLO WORLD" and you want to use 3 rails.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Create the zigzag pattern as follows:

H.....O.....L
E.....L.....W.....R.....D
L.....O

Read the characters from left to right along each rail: "HORDELLWOL."

The ciphertext is "HORDELLWOL."

Step 6: Decryption (Optional)

- To decrypt a Rail Fence-encrypted message, you need to know the number of rails used.
- Create an empty zigzag pattern with the same number of rails.
- Fill in the ciphertext characters in the pattern following the same zigzag pattern.
- Read the characters in the pattern from left to right to reveal the original plaintext.

Step 7: Key Management

- For decryption, it's crucial to know the number of rails used. This information serves as the decryption key.

By following these steps, you can successfully implement the Rail Fence transposition technique to encrypt and decrypt messages. Keep in mind that the security of the Rail Fence cipher is relatively low, and it is primarily used for educational or illustrative purposes.

Columnar Transposition Technique

Implementing the Columnar Transposition Technique involves a series of steps to encrypt and decrypt messages. Below are the steps to implement the Columnar Transposition Technique:

Encryption using Columnar Transposition:

1. **Select a Keyword:** Choose a keyword or key phrase that will determine the order of columns for transposition. For example, let's use the keyword "CRYPTO" for this demonstration.
2. **Write the Message:** Write down your plaintext message in rows beneath the keyword, starting from left to right. The keyword dictates the order of the columns.

Example:

Keyword: CRYPTO

Plaintext: THIS IS A SECRET MESSAGE

Arranged in columns:

CRYPTO

THISIS

ASECRET

MESSAGE

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

3. **Order the Columns:** Rearrange the columns alphabetically based on the letters in your keyword. In this case, the keyword "CRYPTO" would be ordered as "COPRTY."

Example:

CRYPTO
THISIS
ASECRET
MESSAGE

Rearranged:

COPRTY
TSIHIS
AETSREC
GMEASSE

4. **Read the Ciphertext:** Read the message row by row, from left to right. This is your ciphertext.

Example:

Ciphertext: "CTT AIG EME HSAS RST SEO S"

Decryption using Columnar Transposition:

1. **Select a Keyword:** Choose the same keyword used for encryption, in this case, "CRYPTO."
2. **Determine the Number of Columns:** Count the number of columns, which is equal to the length of your keyword.
3. **Calculate the Number of Rows:** To find the number of rows, divide the length of the ciphertext by the number of columns. If there's a remainder, add one row.

Example:

- Ciphertext length: 23
- Number of columns: 6 (based on the keyword)
- Rows = $23 / 6 = 3$ rows with a remainder of 5, so we add one more row for a total of 4 rows.

4. **Recreate the Grid:** Create a grid with the same number of columns as the keyword and the calculated number of rows. Fill in the grid with the ciphertext in a row-by-row manner, left to right.

Example:

Keyword: CRYPTO
Ciphertext: CTT AIG EME HSAS RST SEO S
Reconstructed grid:
CTTAIG
EMEHSA
SRSTSE
OS

5. **Sort the Columns:** Sort the columns based on the keyword (in alphabetical order). In this case, it would be sorted as "COPRTY."

Example:

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Sorted grid:

COPRTY

TSIHIS

AETSREC

GMEASSE

6. Read the Plaintext: Read the message row by row, from left to right. This is your plaintext.

Example:

Plaintext: "THIS IS A SECRET MESSAGE"

By following these steps, you can encrypt and decrypt messages using the Columnar Transposition Technique.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 13: Write a python program to implement of RSA Algorithm

Learning outcome:

- Learners will gain a comprehensive understanding of public key cryptography and the principles behind it.
- To understand and implement the concept of RSA Algorithm.

Implementing the RSA (Rivest-Shamir-Adleman) algorithm involves several steps for generating keys and performing encryption and decryption.

Here are the steps for implementing the RSA algorithm:

Key Generation:

Step 1: Select Two Large Prime Numbers (p and q):

Choose two distinct prime numbers, p and q. These should be large enough to provide security. The security of RSA relies on the difficulty of factoring the product of these two prime numbers ($n = p * q$).

Step 2: Calculate n and $\phi(n)$:

Calculate $n = p * q$, the modulus used for both the public and private keys.

Calculate $\phi(n)$ (Euler's totient function), which is the number of positive integers less than n that are coprime to n. $\phi(n) = (p - 1) * (q - 1)$.

Step 3: Select an Encryption Key (e):

Choose an encryption key (e) such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$. Common choices include small prime numbers like 3 or 65537 ($2^{16} + 1$). The value of e becomes part of the public key.

Step 4: Calculate the Decryption Key (d):

Calculate the modular multiplicative inverse of e modulo $\phi(n)$. In other words, find d such that $(d * e) \% \phi(n) = 1$. The value of d becomes part of the private key.

Encryption:

Step 5: Message Encoding:

Convert the plaintext message into an integer M. This can be done using various encoding schemes (e.g., ASCII, Unicode).

Step 6: Encryption:

Compute the ciphertext C by raising M to the power of e modulo n: $C = (M^e) \% n$.

Decryption:

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Step 7: Decryption:

Compute the plaintext message M by raising C to the power of d modulo n : $M = (C^d) \% n$.

Step 8: Message Decoding:

Convert the integer M back to the original plaintext message using the same encoding scheme used for encryption.

Key Management:

Step 9: Key Storage and Protection:

Safeguard the private key, as it should be kept secret. The public key can be openly shared.

Cryptographic Strength and Security Considerations:

Step 10: Key Length Selection:

The security of RSA depends on the key length. Ensure that you use sufficiently long keys to resist attacks. For modern applications, key lengths of 2048 bits or higher are recommended.

Step 11: Periodic Key Renewal:

Consider periodically generating new key pairs and transitioning to them to enhance security.

Step 12: Protect Against Attacks:

Be aware of potential attacks on RSA, such as factoring attacks and timing attacks. Implement countermeasures and best practices to protect against these threats.

Step 13: Test and Validate:

Test the RSA implementation thoroughly to ensure that it functions correctly and securely.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 14: Write a python program to Implement S-DES algorithm

Learning outcome:

- Understand the fundamental concepts of encryption, including plaintext, cipher text, keys, and the goals of encryption (confidentiality and security).
- Learn the principles of block ciphers, where data is encrypted in fixed-size blocks.
- Gain a comprehensive understanding of the S-DES algorithm, including its structure, rounds, and key generation process.
- Understand the security strengths and weaknesses of the S-DES algorithm. Explore potential vulnerabilities and attacks.

The Simplified Data Encryption Standard (S-DES) algorithm is a simplified version of the Data Encryption Standard (DES) and is used for educational purposes. It provides a great way to understand the fundamentals of encryption.

Below are the steps to implement the S-DES algorithm:

Key Generation:

Initial Key (10 bits): Start with a 10-bit binary key (e.g., 1010000010). This key will be used to generate two 8-bit subkeys, K1 and K2.

Permutation 10 (P10): Perform an initial permutation of the key using the P10 permutation table. This shuffles the bits of the key.

Split into Two 5-bit Halves: Split the 10-bit result into two 5-bit halves.

Circular Left Shifts: Perform a circular left shift (LS-1) on both 5-bit halves. This means that the leftmost bit is moved to the rightmost position.

Permutation 8 (P8): Combine the two 5-bit halves and perform a permutation using the P8 table to generate the first subkey, K1.

Apply Another Circular Left Shift: Perform another circular left shift (LS-2) on the original two 5-bit halves.

Permutation 8 (P8): Combine the two 5-bit halves and perform a permutation using the P8 table again to generate the second subkey, K2.

Data Encryption:

Initial Permutation (IP): Perform the initial permutation (IP) on the 8-bit plaintext to rearrange its bits.

Split into Two 4-bit Halves: Split the 8-bit result into two 4-bit halves, referred to as L0 and R0.

Round 1 (Feistel Network):

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Expansion (E/P): Expand the R0 half to 8 bits using the E/P table.

XOR with K1: XOR the result with the first subkey, K1.

Substitution Boxes (S-Boxes): Split the 8 bits into two 4-bit halves. Each 4-bit half goes through a specific S-box substitution.

Permutation 4 (P4): Combine the outputs of the S-boxes and permute the bits using the P4 table.

XOR with L0: XOR the result with the original L0 half.

Swap Halves: Swap the two halves, so L1 becomes R0, and R1 becomes L0.

Round 2 (Feistel Network):

Repeat the steps of Round 1, but use the second subkey, K2.

Inverse Initial Permutation (IP⁻¹): Perform the inverse of the initial permutation on the combined result of L2 and R2.

Data Decryption:

The decryption process follows the same steps as encryption, but the subkeys are used in reverse order (K2 is used first, then K1).

The final output is the original plaintext.

These steps outline the basic implementation of the S-DES algorithm for encrypting and decrypting data. It's a simplified version of the DES algorithm, offering insight into the principles of Feistel networks, permutations, and S-box substitutions..

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

Lab 15: Write a python program for Substitution Technique using Caesar cipher and Mono Alphabetic cipher

Learning outcome:

- Understanding of Caesar Cipher and its historical significance
- Understand the limitations of Caesar cipher in terms of security and vulnerability to brute-force attacks
- Understand the Vigenère cipher as an extension of the Caesar cipher and learn how to use it for more complex encryption.
- Understanding of Mono-alphabetic Cipher and its role in encryption
- Analyze Mono-alphabetic cipher-encrypted text and use frequency analysis and other methods to break the encryption.

Implementing the Substitution Technique using the Caesar cipher

Implementing the Substitution Technique using the Caesar cipher is a straightforward process. Here are the steps to encrypt and decrypt messages using the Caesar cipher:

Encryption using Caesar Cipher:

Select a Shift Value: Choose a shift value, often denoted as "k," which determines how many positions each letter in the plaintext should be shifted in the alphabet. The shift value can be any integer between 1 and 25.

Write the Message: Write down your plaintext message that you want to encrypt. For this example, let's use the message "HELLO" with a shift value of 3.

Shift Letters: Apply the shift value to each letter in the plaintext message. Move each letter in the alphabet forward by the specified number of positions.

Example:

Plaintext: HELLO

Shift value: 3

Encrypted message: KHOOR

Ciphertext: The encrypted message "KHOOR" is your ciphertext.

Decryption using Caesar Cipher:

Know the Shift Value: To decrypt a Caesar cipher, you need to know the same shift value used for encryption. In this case, it's 3.

Write the Ciphertext: Write down the ciphertext you want to decrypt. For our example, it's "KHOOR."

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Reverse the Shift: Apply the reverse shift value to each letter in the ciphertext. Move each letter backward in the alphabet by the specified number of positions.

Example:

Ciphertext: KHOOR

Shift value: 3 (in reverse)

Decrypted message: HELLO

Plaintext: The decrypted message "HELLO" is your plaintext.

By following these steps, you can encrypt and decrypt messages using the Caesar cipher. The security of the encryption depends on the choice of the shift value, and it's a relatively simple substitution technique. Note that the Caesar cipher is a type of symmetric key cipher, so the same key (shift value) is used for both encryption and decryption.

Implementing the Substitution Technique using the Mono-Alphabetic cipher

Implementing the Substitution Technique using the Mono-alphabetic cipher involves substituting each letter of the plaintext with a corresponding letter or symbol in the cipher text. Here are the steps to encrypt and decrypt messages using the Mono-alphabetic cipher:

Encryption using Mono-alphabetic Cipher:

Generate a Mono-alphabetic Key: Create a one-to-one mapping of each letter in the alphabet to another letter or symbol. This key will be used for both encryption and decryption. The key can be randomly generated or based on a specific pattern.

Example Mono-alphabetic Key:

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text: K T P F M S W J U D Y G V H L Z C N B R Q X O A E I

Write the Message: Write down the plaintext message you want to encrypt. For this example, let's use the message "HELLO."

Substitute Letters: Replace each letter in the plaintext message with its corresponding letter or symbol from the Mono-alphabetic key.

Example:

Plaintext: HELLO

Encrypted message: MTPPA

Cipher text: The encrypted message "MTPPA" is your cipher text.

Decryption using Mono-alphabetic Cipher:

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Use the Same Mono-alphabetic Key: To decrypt a message encrypted with the Mono-alphabetic cipher, you need to use the same Mono-alphabetic key that was used for encryption.

Example Mono-alphabetic Key:

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text: K T P F M S W J U D Y G V H L Z C N B R Q X O A E I

Write the Cipher text: Write down the cipher text you want to decrypt. For our example, it's "MTPPA."

Reverse Substitution: For each letter in the cipher text, find the corresponding letter in the Mono-alphabetic key and replace it with the original letter from the alphabet.

Example:

Cipher text: MTPPA

Decrypted message: HELLO

Plaintext: The decrypted message "HELLO" is your plaintext.

By following these steps, you can encrypt and decrypt messages using the Mono-alphabetic cipher. The security of this encryption depends on the security of the Mono-alphabetic key.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

Lab 16: Configuration of Basic wireless Settings SSID - LWR3000 Configure Wireless Linksys Routers using Cisco Packet Tracer

Learning outcome:

- Understanding Wireless Networking Fundamentals
- Gain a solid grasp of wireless networking concepts, including the operation of SSID, wireless encryption, and wireless access points.
- Learn how to configure the SSID on a Linksys router, including naming the wireless network, and understand the role of the SSID in wireless communication
- Understand the importance of securing wireless networks and learn how to set up basic security measures such as WPA2 (Wi-Fi Protected Access 2) encryption.

Configuration of Basic wireless Settings SSID - LWR3000 Configure Wireless Linksys Routers using Cisco Packet Tracer

Configuring basic wireless settings for an SSID (Service Set Identifier) on a Linksys router using Cisco Packet Tracer involves setting up the wireless network name, security settings, and other parameters. Here are the steps to configure basic wireless settings:

Materials and Tools:

- A computer with Cisco Packet Tracer installed
- A compatible Linksys router model in Packet Tracer
- Access to the Packet Tracer software

Steps:

1. Start Cisco Packet Tracer:

- Launch the Cisco Packet Tracer application on your computer.

2. Create a Network Topology:

- Create a network topology in Packet Tracer by adding devices to the workspace. Ensure you have a Linksys router in the topology.

3. Power On the Router:

- Power on the Linksys router by clicking on the router's icon and selecting "Power."

4. Access the Router's Web Interface:

- Access the router's web-based management interface. In Packet Tracer, you can do this by clicking on the router, selecting "Desktop," and then choosing "Command Line Interface." In the command line interface, you can use the

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

enable command and enter the router's configuration mode by typing **configure terminal**.

5. Configure the SSID:

- In the router's configuration mode, configure the SSID (Wireless Network Name) for your wireless network. Use the following command:

Router(config)# ssid <SSID_name>

6. Enable the Wireless Interface:

- Make sure the wireless interface is enabled on the router. You can use the following commands:

Router(config)# interface wlan0 Router(config-if)# no shutdown

7. Set the Security Mode:

- Choose the security mode for your wireless network. Common options include WPA2 (recommended for security) and WEP (less secure). Use the following commands to set the security mode and passphrase (replace **<password>** with your desired passphrase):

Router(config-if)# encryption mode ciphers aes-ccm

Router(config-if)# encryption vlan 1 mode ciphers aes-ccm

Router(config-if)# authentication open

Router(config-if)# authentication key-management wpa version 2

Router(config-if)# wpa-psk ascii <password>

8. Configure Additional Wireless Settings:

- Depending on your network requirements, you may need to configure additional settings such as the channel, transmit power, or wireless mode (e.g., 802.11n or 802.11ac).

9. Save the Configuration:

- Save your configuration to ensure that your settings are preserved. Use the following command:

Router(config-if)# end Router# write memory

10. Test Your Wireless Network:

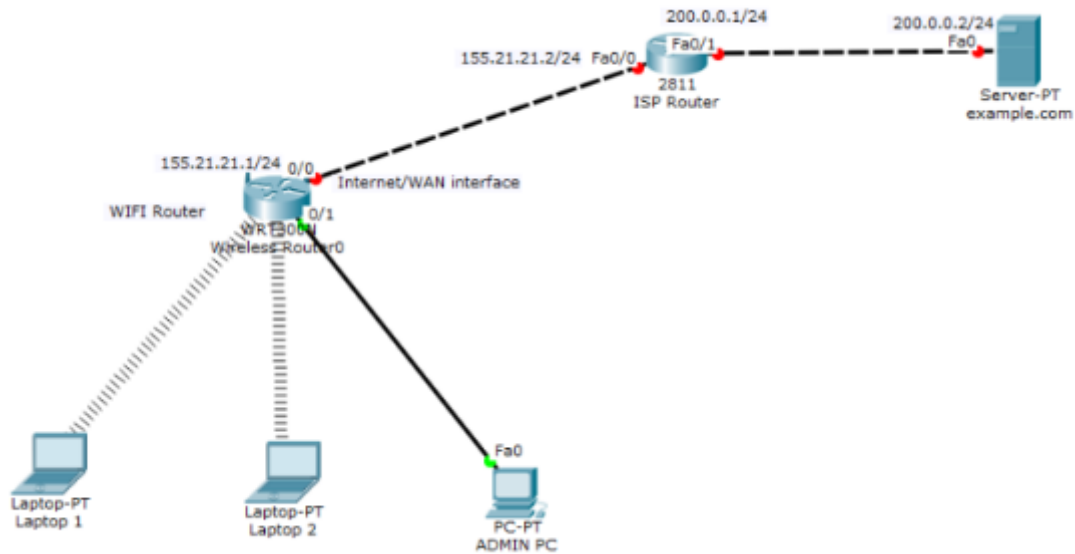
- Connect a wireless device to the newly configured SSID using the provided passphrase. Verify that the device can access the network.

11. Document Your Configuration:

- It's essential to document your configuration for future reference. Record the SSID, security settings, and any other relevant details.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024



Configuring basic wireless settings on Linksys routers, such as the SSID, is essential for creating a functional and secure wireless network. This process involves setting up the Service Set Identifier (SSID), configuring security settings, and ensuring proper connectivity for all devices on the network. Here's a recap and conclusion of the steps taken to achieve this configuration:

1. Setting Up the SSID:

- Access the Linksys router's configuration interface through a web browser.
- Navigate to the wireless settings section and configure the SSID to a desired name, such as "LWR3000".
- Ensure the SSID is broadcasted to allow devices to discover and connect to the network easily.
-

2. Configuring Wireless Security:

- Enable WPA2-PSK encryption to secure the wireless network.
- Set a strong password to protect the network from unauthorized access.
- Apply the security settings to safeguard the data transmitted over the wireless network.
-

3. Configuring the DHCP Server:

- Ensure the DHCP server is enabled on the router to automatically assign IP addresses to connected devices.
- Configure the DHCP range to manage the pool of IP addresses efficiently.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |

NETWORK PROTOCOLS AND SECURITY – LAB MANUAL – 2024

4. Connecting Devices:

- Connect various devices such as laptops, smartphones, and IoT devices to the newly configured wireless network.
- Verify connectivity by checking IP address assignment and internet access.

5. Testing and Verification:

- Perform a series of tests to confirm that the wireless network is functioning correctly.
- Check the connection status of devices, ensure they can access the internet, and verify that they are connected to the correct SSID.

Conclusion

By following the steps outlined, we successfully configured a basic wireless network on a Linksys router using Cisco Packet Tracer. This included setting up the SSID "LWR3000", securing the network with WPA2-PSK encryption, and ensuring proper IP address assignment through DHCP. The configuration process is straightforward and crucial for establishing a reliable and secure wireless environment. Ensuring that wireless settings are correctly configured enhances network performance, security, and user satisfaction. This configuration provides a solid foundation for further network expansion and management, enabling seamless connectivity for all wireless devices within the network.

| | | |
|----------------|---------------------------------|------------------------|
| Course Title | NETWORK PROTOCOLS & SECURITY | ACADEMIC YEAR: 2023-24 |
| Course Code(s) | 23EC2210R, 23EC2210A, 23EC2210E | |