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.:

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** • **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**

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.

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.

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

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

6. nslookup

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

nslookup www.google.com

Server: mydnsserver.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.

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

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

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

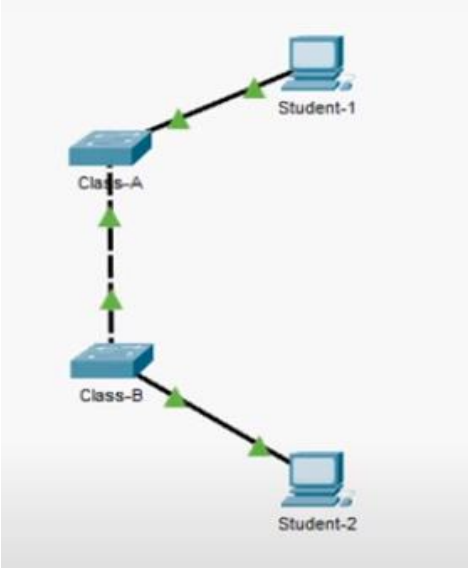
To save the configuration

Switch-A#copy running-config startup-config

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

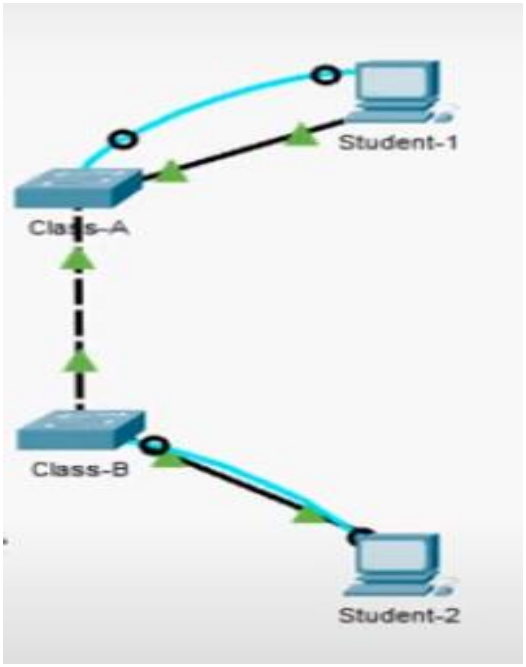
switch



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

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



Class-A Switch	Class-B Switch
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**	**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**

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.

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>

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

5. Repeat for Additional Switches:

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

6. Test Connectivity:

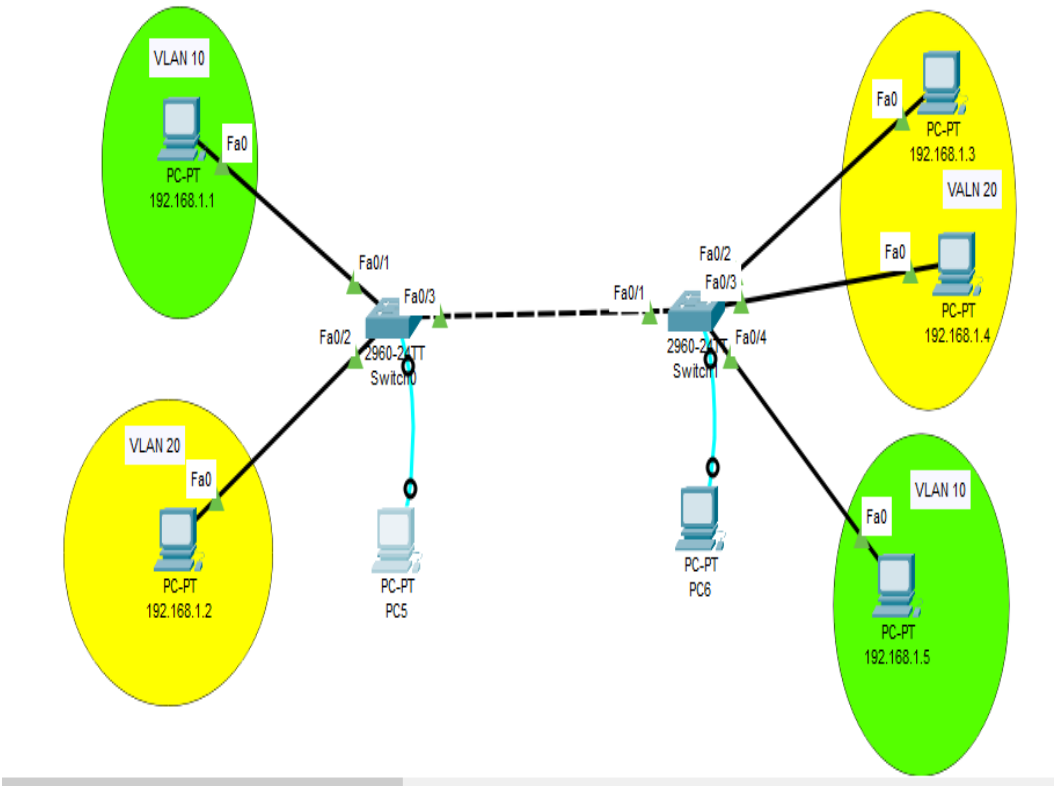
- Connect devices to the VLANs on different switches and verify that they can communicate across the network.

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



VLAN configuration in Switches

Switch-A	Switch-B
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	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

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.

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

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

1. **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.
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.

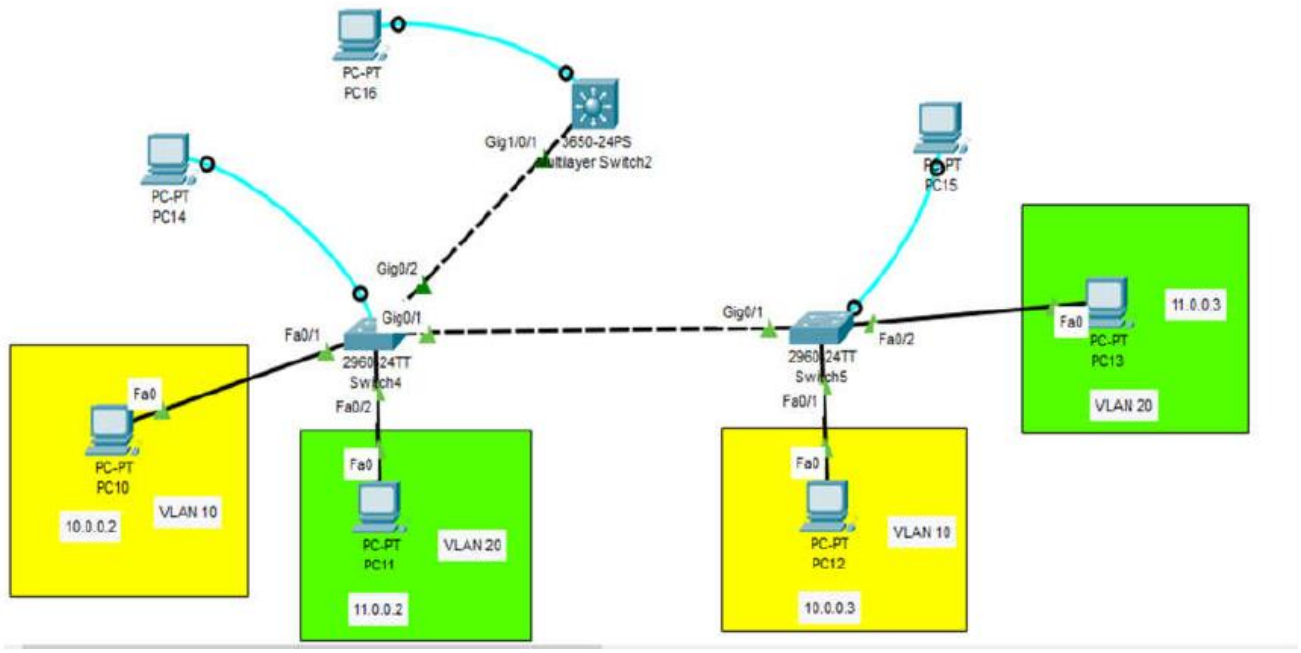
Testing

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

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



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)#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.

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.

- 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.

- 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

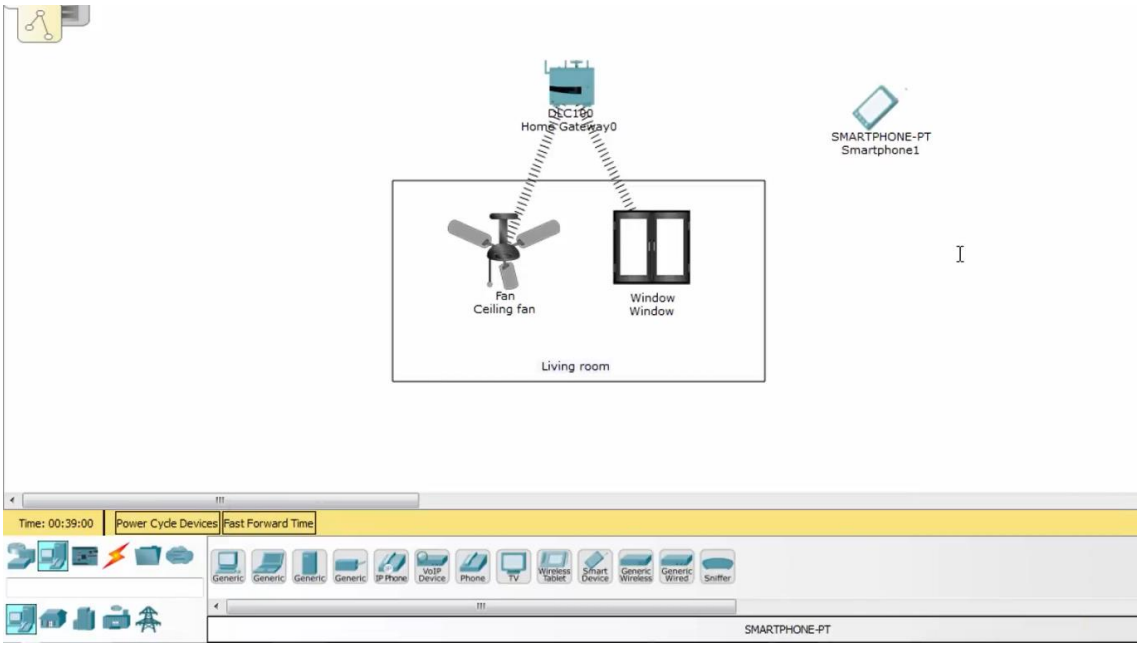
1. **Configure the Smart Light**:
   - Click on the smart light.
   - Go to the "Config" tab.
   - Set the SSID to "SmartHomeNetwork".
   - Set up other settings as needed (e.g., default state, intensity).
2. **Configure the Smart Thermostat**:
   - Click on the smart thermostat.
   - Go to the "Config" 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.

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.