Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 1
Introduction to Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco that allows users to create, configure, and simulate network designs and topologies. It is widely used in networking education to help students visualize and practice networking concepts without the need for physical hardware. This makes it an essential tool for both beginners and advanced students in networking courses, especially those preparing for Cisco certifications such as CCNA and CCNP.

Definition of Packet Tracer

Packet Tracer is a cross-platform network simulation program that enables users to design and simulate complex network infrastructures. It provides a virtual environment where students can create networking devices like routers, switches, firewalls, servers, and end-user devices such as computers and smartphones. The tool allows users to practice configuring these devices and testing network connectivity, making it easier to understand both the theoretical and practical aspects of networking.

Packet Tracer Interface Overview

The Packet Tracer interface is user-friendly, consisting of several key components that make network design and simulation intuitive:

1. Main Workspace:

This is the central area where the user can drag and drop devices to create network topologies. You can connect devices using various types of cables and see the real-time simulation of the network.

2. Device Selection Toolbar:

Located at the bottom of the interface, this toolbar contains categories such as network devices (routers, switches), end devices (PCs, laptops, phones), and connections (different types of network cables). Each category contains various models of devices that can be added to the workspace.

3. Connections and Cables:

Packet Tracer allows users to connect devices using a variety of cables such as straight-through, crossover, fiber optics, and more. It visually represents the physical layout of the network.

4. Network Device Configuration:

When a device is added to the workspace, you can double-click on it to open a configuration window. This allows you to configure device settings such as IP addresses, routing protocols, VLANs, and security settings.

5. Simulation Mode:

Packet Tracer offers both a real-time mode and a simulation mode. In real-time mode, the network functions as it would in a real-world environment. Simulation mode, however, allows users to step through the operations of the network packet by packet, making it ideal for understanding how data flows across the network and for troubleshooting.

6. Command Line Interface (CLI):

Many devices in Packet Tracer offer a CLI option that allows students to configure network devices using Cisco IOS commands. This feature helps students become familiar with real-world command-line network configurations.

Why Use Packet Tracer?

Packet Tracer offers several key benefits for students:

- Hands-On Practice Without Hardware: Students can design and troubleshoot networks without needing expensive equipment like routers, switches, or firewalls.

- Realistic Simulations: The tool closely mimics the behavior of actual Cisco devices, providing a nearly real-world experience for students.

- Multi-Platform Support: It works on various operating systems such as Windows, macOS, and Linux, making it accessible for many students.

- Free Educational Tool: Cisco provides Packet Tracer for free to students enrolled in its Networking Academy, helping them to continue their learning journey outside the classroom.

Conclusion

In summary, Cisco Packet Tracer is an invaluable tool for learning and practicing networking concepts. By familiarizing yourself with its interface and capabilities, you’ll be able to design, simulate, and troubleshoot complex networks with confidence. The hands-on experience you gain using Packet Tracer will reinforce your theoretical understanding and prepare you for real-world networking tasks as well as industry certifications.

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 2
Simple layer 2 Computer Network

Laboratory Experiment: Implementing a Layer 2 Network Using Packet Tracer

Objective: The objective of this experiment is to learn how to design and implement a simple Layer 2 network topology in Cisco Packet Tracer. By the end of the experiment, students will configure a network consisting of two switches and three PCs, ensuring that all terminals can successfully communicate with each other.

Materials Required:
1. Cisco Packet Tracer software installed on a computer.
2. A basic understanding of network switches, Ethernet cables, and the OSI model.

Network Topology Overview:

The network consists of:
- 3 PCs (PC0, PC1, PC2)
- 2 Switches (Switch0 and Switch1)
- Ethernet connections to interconnect devices.

Instructions:

Step 1: Setting Up the Network Topology
1. Open Cisco Packet Tracer.
2. Drag and drop the following devices onto the workspace: • 3 PCs (PC0, PC1, PC2) • 2 Switches (Switch0, Switch1)

3. Connect the devices using copper straight-through cables:

- Connect PC0 to Switch0.
- Connect PC1 to Switch0.
- Connect Switch0 to Switch1.
- Connect Switch1 to PC2.

Step 2: Configuring the PCs

1. Assign IP addresses to each PC:

   • Open PC0, navigate to the Desktop tab, and select IP Configuration. Assign the following:

   • IP Address: 192.168.1.1 • Subnet Mask: 255.255.255.0

   • Repeat the process for PC1 and PC2, assigning: • PC1 IP Address: 192.168.1.2 • PC2 IP Address: 192.168.1.3

2. Ensure that all PCs have the same subnet mask (255.255.255.0).

Step 3: Testing Connectivity

1. Use the Command Prompt on each PC to test connectivity using the ping command:

   - From PC0, ping 192.168.1.2 (PC1) and 192.168.1.3 (PC2).
   - From PC1, ping 192.168.1.1 (PC0) and 192.168.1.3 (PC2).
   - From PC2, ping 192.168.1.1 (PC0) and 192.168.1.2 (PC1).

2. Verify that the packets are transmitted successfully, indicating connectivity between all devices.

Expected Outcome:

• All three PCs should be able to successfully send and receive data from one another using their IP addresses. • The switches will operate at Layer 2 of the OSI model, forwarding frames based on MAC addresses.

Discussion Questions:

1. What role do the switches play in this topology?
2. How does the subnet mask ensure communication between the devices?
3. What would happen if one of the PCs was assigned an IP address outside the 192.168.1.0/24 subnet?

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 3
Static Routing

Laboratory Experiment: Implementing Static Routing in a Simple Network Topology

Objective:

The objective of this experiment is to teach students the concept of static routing and how to configure it in Cisco Packet Tracer. By the end of this experiment, students will create a network topology consisting of two routers, two switches, and four PCs. Static routes will be configured to enable communication between all devices across the topology.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. A basic understanding of IP addressing, routing, and the OSI model.

Network Topology Overview:

The topology consists of:

- 2 Routers (Router0 and Router1) connected via a serial link.
- 2 Switches (Switch0 and Switch1), each connected to one router.
- 4 PCs (PC0, PC1, PC2, and PC3), with two PCs connected to each switch.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.

2. Drag and drop the following devices onto the workspace:
   - 2 Routers
   - 2 Switches
   - 4 PCs
3. Connect the devices:
   - Use a serial connection to connect Router0 to Router1.
   - Use copper straight-through cables to:
   - Connect Router0 to Switch0.
   - Connect Router1 to Switch1.
   - Connect PC0 and PC1 to Switch0.
   - Connect PC2 and PC3 to Switch1.

Step 2: Assigning IP Addresses

1. Define IP Addressing Scheme:
   - Subnet 1 (connected to Router0):
   - Router0 interface to Switch0: 192.168.1.1/24
   - PC0: 192.168.1.2/24
   - PC1: 192.168.1.3/24
   - Subnet 2 (connected to Router1):
   - Router1 interface to Switch1: 192.168.2.1/24
   - PC2: 192.168.2.2/24
   - PC3: 192.168.2.3/24
   - Serial link between Router0 and Router1:
   - Router0: 192.168.3.1/30
   - Router1: 192.168.3.2/30
2. Configure PCs:

- For each PC, open the Desktop tab > IP Configuration and assign the respective IP addresses and subnet masks.

3. Configure Routers:
   - Assign IP addresses to the router interfaces:
   - On Router0: Configure the interface connected to Switch0 and the serial interface.
   - On Router1: Configure the interface connected to Switch1 and the serial interface.

Step 3: Configuring Static Routes

1. On Router0:
   - Add a static route to reach Subnet 2 (192.168.2.0/24) via the serial interface:

```
ip route 192.168.2.0 255.255.255.0 192.168.3.2
```

2. On Router1:
   - Add a static route to reach Subnet 1 (192.168.1.0/24) via the serial interface:

```
ip route 192.168.1.0 255.255.255.0 192.168.3.1
```

Step 4: Testing Connectivity

1. Use the Command Prompt on each PC to test connectivity with all other PCs using the ping command:
   - From PC0, ping 192.168.1.3 (PC1), 192.168.2.2 (PC2), and 192.168.2.3 (PC3).
   - Repeat the process for PC1, PC2, and PC3.
2. Verify that the pings are successful for all devices.

Expected Outcome:

- All PCs should be able to communicate with each other across the topology.
- The routers will forward packets based on the static routes configured.

Discussion Questions:

1. What is the difference between static routing and dynamic routing?
2. What would happen if a static route was incorrectly configured on one of the routers?
3. How does the /30 subnet mask on the serial link between routers optimize IP address usage?

Extensions (Optional):

- Add an additional router and subnet to expand the topology, requiring more static routes.
- Experiment with removing a static route and observe the impact on network connectivity.

This lab provides hands-on experience with static routing and reinforces fundamental networking concepts.

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 4
Dynamic Routing

Laboratory Experiment: Implementing Dynamic Routing Using RIP in a Simple Network Topology

Objective:

The objective of this experiment is to introduce students to dynamic routing using the Routing Information Protocol (RIP). By the end of the experiment, students will configure a network topology with RIP, allowing all devices across the topology to communicate without manually configuring static routes.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Basic understanding of routing protocols and IP subnetting.

Network Topology Overview:

The topology consists of:

- 2 Routers (Router0 and Router1) connected via a serial link.
- 2 Switches (Switch0 and Switch1), each connected to one router.
- 4 PCs (PC0, PC1, PC2, and PC3), with two PCs connected to each switch.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.
2. Drag and drop the following devices onto the workspace:

- 2 Routers
- 2 Switches
- 4 PCs

3. Connect the devices:

- Use a serial connection to connect Router0 to Router1.
- Use copper straight-through cables to:
- Connect Router0 to Switch0.
- Connect Router1 to Switch1.
- Connect PC0 and PC1 to Switch0.
- Connect PC2 and PC3 to Switch1.

Step 2: Assigning IP Addresses

1. Define IP Addressing Scheme:

- Subnet 1 (connected to Router0):
- Router0 interface to Switch0: 192.168.1.1/24
- PC0: 192.168.1.2/24
- PC1: 192.168.1.3/24
- Subnet 2 (connected to Router1):
- Router1 interface to Switch1: 192.168.2.1/24
- PC2: 192.168.2.2/24
- PC3: 192.168.2.3/24
- Serial link between Router0 and Router1:
- Router0: 192.168.3.1/30
- Router1: 192.168.3.2/30

2. Configure PCs:

- For each PC, open the Desktop tab > IP Configuration and assign the respective IP addresses and subnet masks.

3. Configure Routers:

- Assign IP addresses to the router interfaces:
- On Router0:
- Configure the FastEthernet interface connected to Switch0.
- Configure the serial interface connected to Router1.
- On Router1:
- Configure the FastEthernet interface connected to Switch1.
- Configure the serial interface connected to Router0.

Step 3: Configuring RIP on Routers

1. Enable RIP on Router0:

- Access the router's CLI.
- Enter the following commands:

```
router rip
version 2
network 192.168.1.0
network 192.168.3.0
no auto-summary
```

2. Enable RIP on Router1:

- Access the router's CLI.
- Enter the following commands:

```
router rip
version 2
network 192.168.2.0
network 192.168.3.0
no auto-summary
```

Step 4: Testing Connectivity

1. Use the Command Prompt on each PC to test connectivity with all other PCs using the ping command:
   - From PC0, ping:
   - PC1: 192.168.1.3
   - PC2: 192.168.2.2
   - PC3: 192.168.2.3
   - Repeat the process for PC1, PC2, and PC3.
2. Verify that all pings are successful, indicating that RIP has dynamically shared routing information between the routers.

Expected Outcome:

- All PCs should successfully communicate with each other across the network.
- Routers will dynamically exchange routing information using RIP, eliminating the need for manual static route configuration.

Discussion Questions:

1. How does RIP differ from static routing in terms of configuration and scalability?

2. What is the purpose of using RIP version 2 instead of RIP version 1?
3. Why is the no auto-summary command necessary in this experiment?

Extensions (Optional):

- Increase the network complexity by adding a third router and observe how RIP propagates routes.
- Monitor RIP updates using the debug ip rip command on the routers.
- Experiment with disabling RIP on one router and observe its effect on network connectivity.

This lab experiment provides hands-on experience with configuring and verifying RIP, helping students understand the fundamentals of dynamic routing protocols.

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 5

Spanning Tree and Rapid Spanning Tree – part 1

Laboratory Experiment: Configuring and Analyzing RSTP Protocol in a Looped Network

Objective:

The objective of this experiment is to demonstrate the Rapid Spanning Tree Protocol (RSTP) in action using Cisco Packet Tracer. Students will learn how RSTP prevents network loops by blocking redundant ports, how to inspect spanning tree details, and how to manipulate the spanning tree topology by changing switch priorities to designate a new root bridge.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Basic knowledge of switches, the Spanning Tree Protocol (STP), and network loops.

Network Topology Overview:

The topology consists of:

- 4 Switches connected in a looped network.
- 4 PCs (PC0, PC1, PC2, PC3), each connected to a different switch.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.
2. Drag and drop the following devices onto the workspace:

- 4 Switches (Switch0, Switch1, Switch2, Switch3).
- 4 PCs (PC0, PC1, PC2, PC3).

3. Connect the devices:

- Use copper straight-through cables to:
- Connect Switch0 to Switch1.
- Connect Switch1 to Switch2.
- Connect Switch2 to Switch3.
- Connect Switch3 back to Switch0 (to create a loop).
- Connect each PC to one of the switches:
- PC0 to Switch0
- PC1 to Switch1
- PC2 to Switch2
- PC3 to Switch3.

Step 2: Configuring IP Addresses

1. Assign IP addresses to PCs:

- PC0: 192.168.1.2/24
- PC1: 192.168.1.3/24
- PC2: 192.168.1.4/24
- PC3: 192.168.1.5/24
- Set the default gateway to 192.168.1.1 (this is for testing, no gateway will be required for intra-network communication).

2. No IP configuration is required for the switches, as this is a Layer 2 experiment.

Step 3: Enabling and Verifying RSTP

1. Enable RSTP on the Switches (RSTP is the default spanning tree protocol on Cisco switches in Packet Tracer):
   - Access the CLI of each switch and verify the spanning tree mode:

```
Switch> enable
Switch# show spanning-tree
```

   - Ensure the protocol is listed as RSTP.

2. Verify Loop Prevention:
   - Run the show spanning-tree command on any switch to view the RSTP status and observe:
   - The root bridge (the switch with the lowest bridge ID).
   - Designated ports (forwarding traffic).
   - Blocked ports (preventing loops).

Step 4: Testing Network Connectivity

1. Use the Command Prompt on each PC to test connectivity by pinging all other PCs:
   - From PC0, ping PC1, PC2, and PC3.
   - Repeat this process for the other PCs.
2. Verify that all pings are successful, ensuring the network is functioning correctly despite the loop.

Step 5: Changing the Root Bridge

1. Check the Current Root Bridge:

- Use the show spanning-tree command on any switch to identify the root bridge (it will have all its ports as designated ports).

2. Change the Root Bridge:

- Select a new switch to become the root bridge (e.g., Switch2).
- On Switch2, lower its priority value to make it the root bridge:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 priority 4096
```

- The switch with the lowest priority becomes the root bridge. The default priority is 32768, so setting a lower value (e.g., 4096) will override it.

3. Verify the New Root Bridge:

- Use the show spanning-tree command on all switches to confirm the new root bridge and observe the changes in the port roles (e.g., root ports and designated ports).

Expected Outcomes:

1. Port Blocking: RSTP blocks redundant ports to prevent loops, which can be observed using the show spanning-tree command.
2. Root Bridge Election: The switch with the lowest bridge ID (priority + MAC address) becomes the root bridge. Changing the priority forces a new root bridge election.
3. Connectivity: Despite the looped topology, all PCs should successfully communicate due to RSTP's loop prevention mechanisms.

Discussion Questions:

1. What is the role of RSTP in preventing loops in this topology?
2. How does changing the switch priority affect the spanning tree topology?
3. What happens to the network if all switches have the same default priority?

Extensions (Optional):

1. Add more switches and loops to observe how RSTP scales.
2. Use the debug spanning-tree command on the CLI to monitor RSTP activity in real time.

This lab helps students understand the operation of RSTP in looped topologies and provides hands-on experience with spanning tree configuration and analysis.

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 6

Spanning Tree and Rapid Spanning Tree – part 2

Extended Laboratory Experiment: Integrating a Router into an RSTP-Enabled Network

Objective:

This extended experiment builds on the previous RSTP laboratory. In addition to learning how RSTP prevents loops in a network, students will configure and integrate a router into the topology. The router will act as the default gateway for all PCs, enabling inter-subnet communication.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Basic knowledge of IP routing, subnetting, and the RSTP protocol.

Extended Network Topology Overview:

- 4 Switches connected in a looped topology using RSTP.
- 4 PCs connected to the switches (one PC per switch).
- 1 Router connected to one of the switches (e.g., Switch0).
- The router will provide a default gateway for all PCs.

Steps:

Step 1: Adding the Router

1. Extend the existing topology by adding a Router (Router0) to the workspace in Cisco Packet Tracer.
2. Connect Router0 to Switch0 using a copper straight-through cable.

Step 2: Configuring the IP Address Scheme

1. Assign Subnets for Each Switch:

Each switch represents a different subnet:

- Subnet 1 (Switch0 and PC0): 192.168.1.0/24
- Router0 (connected to Switch0): 192.168.1.1
- PC0: 192.168.1.2
- Subnet 2 (Switch1 and PC1): 192.168.2.0/24
- PC1: 192.168.2.2
- Subnet 3 (Switch2 and PC2): 192.168.3.0/24
- PC2: 192.168.3.2
- Subnet 4 (Switch3 and PC3): 192.168.4.0/24
- PC3: 192.168.4.2

2. Configure PCs:

- For each PC, assign the respective IP address and subnet mask using the Desktop tab > IP Configuration.
- Set the default gateway on each PC to the IP address of Router0 for its subnet (e.g., 192.168.x.1).

3. Configure Router Interfaces:

- Access Router0’s CLI and assign IP addresses to its interfaces:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface gigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

- Repeat the process for additional interfaces to define subinterfaces for other subnets using Router-on-a-Stick configuration if needed.

Step 3: Configuring RSTP on Switches

1. Ensure RSTP is enabled on all switches:
   - Use the show spanning-tree command to verify RSTP is active.
2. Observe blocked and forwarding ports:
   - Verify that redundant links are blocked to prevent loops.

Step 4: Testing Connectivity

1. Use the Command Prompt on each PC to test connectivity by pinging:
   - The router interface in its subnet (e.g., 192.168.x.1).
   - PCs in other subnets (e.g., PC0 to PC2).
   - The pings should succeed, demonstrating that the router is forwarding traffic between subnets.
2. Verify RSTP Functionality:
   - Run the show spanning-tree command on the switches to confirm the roles of ports (root, designated, or blocked).

Step 5: Changing the Root Bridge

1. Change the root bridge as described in the original experiment by altering switch priorities.
2. Verify the effect on the spanning tree topology using the show spanning-tree command.

Expected Outcomes:

1. RSTP Loop Prevention: RSTP blocks redundant links to prevent loops.
2. Inter-Subnet Routing: The router enables communication between PCs in different subnets.
3. Dynamic Spanning Tree Topology: Changing switch priorities alters the root bridge and adjusts port roles dynamically.

Discussion Questions:

1. How does the addition of a router change the network's behavior compared to the RSTP-only topology?
2. What is the impact of modifying the root bridge on the overall traffic flow?
3. How does RSTP ensure efficient path selection even when loops exist?

Extensions (Optional):

1. Monitor and debug RSTP activity using debug spanning-tree on the switches.
2. Expand the topology to include a second router connected to one of the other switches, demonstrating multi-router interconnectivity.

This extended experiment combines Layer 2 loop prevention with Layer 3 routing, giving students a comprehensive understanding of network functionality.

Module: Switching And Routing I

Class: Third

Instructure: Prof. Dr. Rana Fareed Ghani

Lecture 7

Multiple VLans on a single switch

Laboratory Experiment: Configuring VLANs in a Simple Network Topology Using Cisco Packet Tracer

Objective:

The objective of this experiment is to introduce students to Virtual Local Area Networks (VLANs). By the end of the experiment, students will be able to:

1. Create VLANs on a switch.
2. Assign interfaces to VLANs.
3. Test connectivity within VLANs and observe communication restrictions across different VLANs.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Basic understanding of Layer 2 switching and Ethernet communication.

Network Topology Overview:

- 1 Switch (Switch0).
- 4 PCs (PC0, PC1, PC2, PC3):
- PC0 and PC1 belong to VLAN 10.
- PC2 and PC3 belong to VLAN 20.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.
2. Drag and drop the following devices onto the workspace:
- 1 Switch (Switch0).
- 4 PCs (PC0, PC1, PC2, PC3).
3. Use copper straight-through cables to connect each PC to the switch:
- PC0 to Switch0 (Port FastEthernet 0/1).
- PC1 to Switch0 (Port FastEthernet 0/2).
- PC2 to Switch0 (Port FastEthernet 0/3).
- PC3 to Switch0 (Port FastEthernet 0/4).

Step 2: Assigning IP Addresses

1. Configure IP addresses for the PCs using the Desktop tab > IP Configuration:
- PC0: 192.168.10.2/24
- PC1: 192.168.10.3/24
- PC2: 192.168.20.2/24
- PC3: 192.168.20.3/24
2. Ensure each PC is configured with the correct subnet mask (255.255.255.0). No default gateway is required as this is an intra-switch experiment.

Step 3: Configuring VLANs on the Switch

1. Access the Switch CLI:
- Click on the switch and select the CLI tab.

2. Create VLANs:

- Enter configuration mode:

```
Switch> enable
Switch# configure terminal
```

- Create VLAN 10 and VLAN 20, and assign names to them:

```
Switch(config)# vlan 10
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
```

3. Verify VLAN Creation:

- Use the following command to display the existing VLANs:

```
Switch# show vlan brief
```

- You should see VLAN 10 (Engineering) and VLAN 20 (Sales) listed.

4. Assign Interfaces to VLANs:

- Assign FastEthernet 0/1 and 0/2 to VLAN 10:

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

- Assign FastEthernet 0/3 and 0/4 to VLAN 20:

```
Switch(config)# interface fastEthernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

Step 4: Testing Connectivity

1. Test communication within each VLAN:

- Open the Command Prompt on PC0 and ping PC1 (192.168.10.3). The ping should succeed.

- Open the Command Prompt on PC2 and ping PC3 (192.168.20.3). The ping should succeed.

2. Test communication across VLANs:

- From PC0, attempt to ping PC2 or PC3. The ping should fail because VLANs isolate traffic at Layer 2.

Expected Outcomes:

1. Intra-VLAN Communication: PCs within the same VLAN can communicate successfully.
2. Inter-VLAN Isolation: PCs in different VLANs cannot communicate directly.
3. VLAN Details: The show vlan brief command displays VLAN configurations and port assignments.

Discussion Questions:

1. What is the purpose of VLANs in a network?
2. How does VLAN isolation improve network performance and security?
3. What would be required to enable communication between VLANs?

Extensions (Optional):

1. Add a router or configure a Layer 3 switch to enable inter-VLAN routing and test inter-VLAN communication.
2. Experiment with different VLAN names and IP address ranges.
3. Use the show running-config command to examine the configuration file and verify VLAN settings.

This lab experiment provides a foundation for understanding VLANs, their configuration, and their role in segmenting a network for improved traffic management and security.**Lecture 8**

Lecture 8
Multiple VLANs on Multiple switches

Laboratory Experiment: Configuring Inter-VLAN Routing with Two Switches and a Router Using Cisco Packet Tracer

Objective:

The objective of this extended experiment is to demonstrate how to configure Inter-VLAN Routing in a topology consisting of two switches and one router. By the end of the experiment, students will understand how to:

1. Configure VLANs across multiple switches.
2. Use a router to enable communication between VLANs.
3. Test inter-VLAN connectivity successfully.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Knowledge of VLAN basics, IP subnetting, and static routing.

Extended Network Topology Overview:

- 2 Switches (Switch0 and Switch1).
- 1 Router (Router0).
- 4 PCs:
- PC0 and PC1 belong to VLAN 10 (Engineering).
- PC2 and PC3 belong to VLAN 20 (Sales).

- Switch0 and Switch1 are connected, and the router is connected to Switch0 for Inter-VLAN Routing.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.
2. Drag and drop the following devices onto the workspace:
- 2 Switches (Switch0 and Switch1).
- 1 Router (Router0).
- 4 PCs (PC0, PC1, PC2, PC3).
3. Use copper straight-through cables to connect the devices:
- PC0 to Switch0 (Port FastEthernet 0/1).
- PC1 to Switch0 (Port FastEthernet 0/2).
- PC2 to Switch1 (Port FastEthernet 0/1).
- PC3 to Switch1 (Port FastEthernet 0/2).
- Connect Switch0 to Switch1 (Port FastEthernet 0/24 on both switches).
- Connect Router0 to Switch0 (Port FastEthernet 0/0).

Step 2: Assigning IP Addresses

1. Assign the following IP Addresses to the PCs:
- PC0: 192.168.10.2/24 (Default Gateway: 192.168.10.1).
- PC1: 192.168.10.3/24 (Default Gateway: 192.168.10.1).
- PC2: 192.168.20.2/24 (Default Gateway: 192.168.20.1).
- PC3: 192.168.20.3/24 (Default Gateway: 192.168.20.1).
2. Configure the Router0 interface for Inter-VLAN Routing.

Step 3: Configuring VLANs on the Switches

1. Access Switch0 CLI and create VLANs:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
```

2. Assign Interfaces to VLANs on Switch0:

- Assign FastEthernet 0/1 and 0/2 to VLAN 10:

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

- Assign FastEthernet 0/24 to trunk mode to communicate with Switch1:

```
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

3. Access Switch1 CLI and repeat the VLAN configuration steps for VLAN 10 and VLAN 20.
4. Assign Interfaces to VLANs on Switch1:

- Assign FastEthernet 0/1 and 0/2 to VLAN 20:

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

- Assign FastEthernet 0/24 to trunk mode to communicate with Switch0:

```
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

Step 4: Configuring the Router

1. Enable Router-on-a-Stick:

- Access the Router CLI.
- Configure subinterfaces for VLANs on the router interface connected to Switch0 (FastEthernet 0/0):

```
Router> enable
Router# configure terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# no shutdown

Router(config)# interface fastEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

Router(config)# interface fastEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

2. Verify Subinterface Configuration:

- Use the command show ip interface brief to ensure the subinterfaces are up and running.

Step 5: Testing Connectivity

1. Test Intra-VLAN Communication:
- From PC0, ping PC1 (192.168.10.3)—the ping should succeed.
- From PC2, ping PC3 (192.168.20.3)—the ping should succeed.
2. Test Inter-VLAN Communication:
- From PC0, ping PC2 (192.168.20.2)—the ping should succeed.
- From PC3, ping PC1 (192.168.10.3)—the ping should succeed.

Expected Outcomes:

1. Intra-VLAN Communication: PCs within the same VLAN communicate successfully.
2. Inter-VLAN Communication: PCs in different VLANs communicate through the router.
3. Trunk Ports: Switch0 and Switch1 use trunk ports to carry VLAN traffic between them.

Discussion Questions:

1. What is the role of the router in this topology?
2. Why is a trunk port required between switches?
3. How does the router differentiate between VLAN traffic on the same physical interface?

Extensions (Optional):

1. Add a second router to create a more complex inter-VLAN routing scenario.
2. Introduce a third VLAN to demonstrate scalability.
3. Configure and test additional trunk links between switches for redundancy.

This experiment provides practical knowledge of VLAN segmentation, trunking, and inter-VLAN routing in a network.

Lecture 9

VLANs and RSTP

Laboratory Experiment: Integrating VLANs and RSTP in a Looped Switch Topology

Objective:

This experiment aims to demonstrate the integration of VLANs and Rapid Spanning Tree Protocol (RSTP) in a network. Students will:

1. Configure VLANs across multiple switches.
2. Observe RSTP blocking ports to eliminate loops in the network.
3. Ensure connectivity within VLANs while isolating traffic between different VLANs.

Materials Required:

1. Cisco Packet Tracer software installed on a computer.
2. Basic knowledge of VLANs, RSTP, and Layer 2 switching.

Network Topology Overview:

- 3 Switches (Switch0, Switch1, Switch2) interconnected to form a loop.
- 6 PCs distributed across 3 VLANs:
- VLAN 10 (Engineering): PC0 and PC1 connected to Switch0.
- VLAN 20 (Sales): PC2 and PC3 connected to Switch1.
- VLAN 30 (HR): PC4 and PC5 connected to Switch2.
- RSTP is configured to prevent loops by blocking one of the ports.
- PCs in the same VLAN can communicate, while traffic is isolated between different VLANs.

Steps:

Step 1: Setting Up the Topology

1. Open Cisco Packet Tracer.

2. Drag and drop the following devices onto the workspace:
- 3 Switches (Switch0, Switch1, Switch2).
- 6 PCs (PC0–PC5).
3. Connect the devices as follows:
- PC0 to Switch0 (FastEthernet 0/1).
- PC1 to Switch0 (FastEthernet 0/2).
- PC2 to Switch1 (FastEthernet 0/1).
- PC3 to Switch1 (FastEthernet 0/2).
- PC4 to Switch2 (FastEthernet 0/1).
- PC5 to Switch2 (FastEthernet 0/2).
- Switch0 to Switch1 (FastEthernet 0/24 on both).
- Switch1 to Switch2 (FastEthernet 0/23 on both).
- Switch2 to Switch0 (FastEthernet 0/24 on both).

Step 2: Configuring VLANs on Each Switch

1. Access the CLI of Switch0:
- Create VLANs and name them:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
Switch(config)# vlan 30
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
```

- Assign interfaces to VLAN 10 for PC0 and PC1:

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

- Set the inter-switch connection (FastEthernet 0/24) to trunk mode:

```
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

2. Repeat VLAN Configuration for Switch1 and Switch2:

- For Switch1, assign FastEthernet 0/1 and 0/2 to VLAN 20, and set trunk mode for FastEthernet 0/23 and 0/24.

- For Switch2, assign FastEthernet 0/1 and 0/2 to VLAN 30, and set trunk mode for FastEthernet 0/24 and 0/23.

Step 3: Configuring RSTP on All Switches

1. Enable RSTP globally on all switches:

```
Switch> enable
Switch# configure terminal
Switch(config)# spanning-tree mode rapid-pvst
```

2. Verify that RSTP is running:

```
Switch# show spanning-tree
```

- Observe which ports are forwarding and which are blocked. One port should be blocked to prevent the loop.

Step 4: Assigning IP Addresses

1. Configure IP addresses for the PCs based on their VLANs:

- PC0 and PC1 (VLAN 10):
- PC0: 192.168.10.2/24
- PC1: 192.168.10.3/24
- PC2 and PC3 (VLAN 20):
- PC2: 192.168.20.2/24
- PC3: 192.168.20.3/24

- PC4 and PC5 (VLAN 30):
- PC4: 192.168.30.2/24
- PC5: 192.168.30.3/24

2. No default gateway is needed, as this is an intra-switch communication experiment.

Step 5: Testing Connectivity

1. Test communication within each VLAN:

- From PC0, ping PC1 (192.168.10.3)—the ping should succeed.
- From PC2, ping PC3 (192.168.20.3)—the ping should succeed.
- From PC4, ping PC5 (192.168.30.3)—the ping should succeed.

2. Test communication across VLANs:

- From PC0, attempt to ping PC2 or **PC4`. The ping should fail because VLANs isolate traffic at Layer 2.

3. Check RSTP behavior:

- Use the command show spanning-tree on any switch to verify which port is blocked by RSTP.

Expected Outcomes:

1. RSTP Functionality: One of the inter-switch ports is blocked to prevent loops, as shown in the show spanning-tree output.
2. Intra-VLAN Communication: PCs within the same VLAN communicate successfully.
3. Inter-VLAN Isolation: Traffic is isolated between VLANs, ensuring network segmentation.

Discussion Questions:

1. Why is RSTP necessary in a network with a looped topology?
2. How do VLANs enhance network segmentation and security?
3. What happens if RSTP is disabled in this setup?

Extensions (Optional):

1. Configure a router-on-a-stick to enable inter-VLAN routing and test communication between VLANs.
2. Increase the number of switches or VLANs to demonstrate scalability.
3. Experiment with changing the RSTP root bridge priority to observe its effect on the blocked ports.

This experiment demonstrates the interplay between VLANs and RSTP, emphasizing how these technologies improve network performance, reliability, and segmentation.