Course: SWE-Computer Network Practical			
Instructor	Dr. Asad Raza Malik	Practical/Lab No.	04
Date	21-08-2024	CLOs	03
Student's Roll no:		Point Scored:	
Date of Conduct:		Teacher's Signature:	

LAB PERFORMANCE INDICATOR	Subject Knowledge	Data Analysis and Interpretation	Ability to Conduct Experiment	Presentation	Calculation and Coding	Observation/ Result	Score

Topic	**To become familiar with the basic configuration of a switch using packet tracer software**
Objective	• The objective of this lab is to familiarize students with the basic configuration of a network switch using Cisco Packet Tracer software. Students will learn how to configure the switch's hostname, assign IP addresses, manage VLANs, and secure access to the switch.
Materials Required:	• Cisco Packet Tracer software installed on your computer • A Computer with a network interface card (NIC) • Ethernet cables (virtually connected within Packet Tracer). • A Cisco switch (emulated within Packet Tracer).

Lab Discussion: Theoretical concepts and Procedural steps

1. Introduction to Switches

Switches are networking devices that operate at the data link layer (Layer 2) of the OSI model. They are essential components in local area networks (LANs) and are responsible for connecting multiple devices, such as computers, printers, and servers, within a network. Switches use MAC addresses to forward data packets to the correct destination, ensuring efficient data transfer within the network.

Key Functions of a Network Switch:

1. **Data Forwarding:** Switches operate primarily at the Data Link Layer (Layer 2) of the OSI model, forwarding data frames between devices based on their MAC addresses.

2. **MAC Address Table:** Switches maintain a table of MAC addresses associated with each port, allowing them to forward data to the correct destination.

3. **Full-Duplex Communication:** Modern switches enable full-duplex communication, allowing devices to send and receive data simultaneously, doubling the effective bandwidth.

4. **Traffic Segmentation:** Switches can create VLANs (Virtual Local Area Networks), segmenting network traffic and enhancing security by isolating different groups of devices.

5. **Management and Security:** Managed switches offer features like port security, traffic monitoring, and remote configuration, providing greater control over the network.

Types of Switches:

- **Unmanaged Switches:** Basic, plug-and-play devices with no configuration options, suitable for small networks.
- **Managed Switches:** Provide advanced features like VLANs, QoS (Quality of Service), and SNMP (Simple Network Management Protocol) for monitoring and control, ideal for enterprise environments.
- **Layer 3 Switches:** Combine the functionality of both switches and routers, capable of routing data between different IP subnets.

Usage:

Switches are essential components in both small and large networks, ranging from home offices to data centers. They enable efficient data communication, reduce network congestion, and provide the foundation for more complex network architectures.

2. Importance of Switch Configuration

Proper switch configuration is crucial for a network's effective operation and security. Configuring a switch allows network administrators to control traffic, manage network devices, and secure the network from unauthorized access. Basic switch configuration includes setting up a hostname, assigning IP addresses for management purposes, configuring VLANs (Virtual Local Area Networks), and securing access to the switch using passwords and other security measures.

Key Configuration Concepts

1. Hostname Configuration:

- Assigning a hostname to a switch helps identify the device within the network. This is especially useful in environments with multiple switches, as it simplifies management and troubleshooting.

2. IP Address Configuration:

- Assigning an IP address to a switch allows network administrators to manage the device remotely. The IP address is usually assigned to a management interface, such as VLAN 1, and enables communication with the switch from other devices on the network.

3. VLAN Configuration:

- VLANs allow network segmentation, which improves network performance and security. By creating VLANs, network administrators can group devices based on function, department, or other criteria, reducing broadcast traffic and enhancing security by isolating certain devices from others.

4. Securing Access:

- Securing access to a switch is vital to prevent unauthorized users from changing the network configuration. This can be done by setting up passwords for console access, enabling secret passwords for privileged EXEC mode, and securing remote access via protocols like Telnet or SSH.

5. Saving the Configuration:

- Once a switch is configured, it is important to save the configuration to ensure the settings persist after rebooting. This is done using commands like `write memory` or `copy running-config startup-config`.

Lab Activities

Lab Objective

Learn how to set up and configure basic management access on Cisco switches and routers, including setting IP addresses, configuring basic security, and verifying connectivity.

Lab Equipment

- Cisco Routers (1 or more)
- Cisco Switches (1 or more)
- Console cables (for initial setup)
- Ethernet cables
- PC with terminal emulation software (e.g., PuTTY or Tera Term)
- Cisco Packet Tracer or GNS3 (optional for virtual labs)

Lab Tasks

1. Initial Setup

Step 1: Connect your PC to the console port of the switch or router using a console cable.

Step 2: Open terminal emulation software and connect to the device using the following settings:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Step 3: Power on the switch or router and wait for the command line interface (CLI) to be available.

2. Basic Configuration on Router

Step 1: Enter privileged EXEC mode:

```
    Router> enable
```

Step 2: Enter global configuration mode:

```
Router# configure terminal
```

Step 3: Set a hostname:

```
Router(config)# hostname Router1
```

Step 4: Configure the router's management interface (e.g., GigabitEthernet0/0):

```
Router1(config)# interface GigabitEthernet0/0

Router1(config-if)#     ip     address     192.168.1.1
255.255.255.0

Router1(config-if)# no shutdown

Router1(config-if)# exit
```

3. Basic Configuration on Switch

Step 1: Enter privileged EXEC mode:

```
Switch> enable
```

Step 2: Enter global configuration mode:

```
Switch# configure terminal
```

Step 3: Set a hostname:

```
Switch(config)# hostname Switch1
```

Step 4: Configure the management VLAN interface (typically VLAN 1):

```
Switch1(config)# interface vlan 1

Switch1(config-if)#     ip     address     192.168.1.2
255.255.255.0

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

Switch1(config-if)# exit

4. Secure Management Access

Step 1: Set console and VTY passwords:

```
Router1(config)# line console 0
Router1(config-line)# password cisco
Router1(config-line)# login
Router1(config-line)# exit

Router1(config)# line vty 0 4
Router1(config-line)# password cisco
Router1(config-line)# login
Router1(config-line)# exit
```

Step 2: Enable SSH on the router for secure remote management:

```
Router1(config)# ip domain-name yourdomain.com
Router1(config)# crypto key generate rsa
Router1(config)# line vty 0 4
Router1(config-line)# transport input ssh
Router1(config-line)# exit
```

5. Verify Connectivity

Step 1: Verify IP connectivity by pinging between devices:

```
Router1# ping 192.168.1.2
```

Step 2: Check the configuration by running the following commands:

For router:

```
Router1# show running-config
```

For switch:

Switch1# show running-config

6. Save Configuration

Step 1: Save the configuration on both the router and switch:

```
Router1# write memory
Switch1# write memory
```

End of Lab

You have successfully configured basic management access on a Cisco router and switch. This includes setting up IP addresses, configuring console and VTY access, and verifying connectivity.

Student Worksheet:

Independent Task: Implementing VLANs and Port Security on a Cisco Switch

Task Overview

Students will independently configure VLANs, assign VLANs to switch ports, and implement port security on a Cisco switch. This task is designed to test their understanding of VLAN segmentation and network security.

Task Details

Scenario: Tech Solutions Ltd. has expanded and added a new department called Finance. The company requires the following configuration on their existing network switch:

- Create a new VLAN for the Finance department.
- Assign specific ports to this new VLAN.
- Implement port security on these ports to restrict unauthorized devices.
- Verify the configuration and test for any security breaches.

Requirements:

1. **Create and Name a New VLAN:**
   - Create VLAN 40 for the Finance department.
   - Name the VLAN Finance.
2. **Assign Ports to VLAN 40:**
   - Assign ports Fa0/15 to Fa0/20 to VLAN 40.
3. **Implement Port Security:**
   - Enable port security on ports Fa0/15 to Fa0/20.
   - Allow a maximum of 2 MAC addresses per port.

    - Configure the ports to restrict unauthorized devices.

4. **Verify the Configuration:**
    - Use appropriate commands to verify that the VLAN is created and ports are assigned correctly.
    - Check that port security is enabled and functioning as expected.
5. **Testing:**
    - Connect a device to one of the secured ports and confirm it is allowed to communicate within VLAN 40.
    - Attempt to connect an unauthorized device to see if it is restricted.
6. **Documentation:**
    - Document each step of your configuration process.
    - Provide screenshots of command outputs that verify your configuration.
    - Write a brief summary of the steps you took and any challenges faced during the task.

Submission:

- Submit the running configuration of the switch using the show running-config command.
- Include your documentation and screenshots as part of your submission.

Assessment Criteria:

- Correct creation and naming of the new VLAN.
- Accurate assignment of ports to VLAN 40.
- Proper implementation and verification of port security.
- Clear and concise documentation with evidence of configuration.

This task challenges students to apply their knowledge independently, reinforcing their understanding of VLANs and port security while providing a practical scenario that mimics real-world network administration.

---End---