WAMBUA SOLOMON MBITHI | P15/144649/2022

Mubarak Ahmed mohamud | P15/145186/2022

Mwangi Paul Kimaru | P15/139827/2020

Lab 1: Different types of Routers in computer networking

Discuss the different types of Routers in computer networking - their benefits, advantages and disadvantages. Give three examples (ref) of each type of router:

- Wired routers
- Wireless routers
- Core routers
- Edge routers
- VPN routers
- Virtual Routers

Research on Different Types of Routers

1. Wired Routers

- **Description**: Connect devices using Ethernet cables.
- **Advantages**:
  - Faster data transfer rates compared to wireless.
  - More secure as physical access is required to connect devices.
  - Less interference from other electronic devices.
- **Disadvantages**:
  - Limited mobility due to the need for physical connections.
  - Requires cabling which can be cumbersome and costly.
- **Examples**:
  - Linksys EA7500
  - TP-Link Archer A7
  - Netgear Nighthawk RAX40

2. Wireless Routers

- **Description**: Allow devices to connect wirelessly via Wi-Fi.
- **Advantages**:
  - Greater mobility and flexibility for users.
  - Easier to set up and expand a network.
  - Supports multiple devices without additional wiring.
- **Disadvantages**:
  - Potential security risks if not properly secured.
  - Signal interference can affect performance.
  - Generally slower than wired connections.
- **Examples**:
  - ASUS RT-AC66U

    - Google Nest WiFi
    - TP-Link Deco M5

3. Core Routers

- **Description**: Operate within the backbone or core of the network, directing data between different sub-networks.
- **Advantages**:
    - High-speed performance for large-scale networks.
    - Efficient handling of high traffic volumes.
    - Provide redundancy and reliability in data transfer.
- **Disadvantages**:
    - Typically expensive and require specialized knowledge to configure.
    - Can be complex and may need advanced maintenance.
- **Examples**:
    - Cisco ASR 9000 Series
    - Juniper MX Series
    - Arista 7280R Series

4. Edge Routers

- **Description**: Positioned at the edge of the network, connecting an enterprise network to the internet.
- **Advantages**:
    - Manage traffic between internal and external networks effectively.
    - Enhance security through various protocols and filters.
    - Optimize performance by routing traffic intelligently.
- **Disadvantages**:
    - Can become a bottleneck if not properly sized.
    - Often require higher maintenance and management overhead.
- **Examples**:
    - Cisco ISR Series
    - Mikrotik CCR Series
    - Fortinet FortiGate

5. VPN Routers

- **Description**: Enable secure connections to private networks over the internet using Virtual Private Network (VPN) technology.
- **Advantages**:
    - Provide enhanced security for remote users and offices.
    - Allow for secure access to sensitive information over public networks.
    - Can support multiple VPN connections.
- **Disadvantages**:
    - May introduce latency due to encryption/decryption processes.
    - Configuration can be complex, requiring technical expertise.

- **Examples**:
    - ASUS RT-AC5300
    - Netgear Nighthawk RAX80
    - TP-Link Archer C5400X

6. Virtual Routers

- **Description**: Software-based routers that can operate on virtualized hardware.
- **Advantages**:
    - Flexibility and scalability to adapt to changing network requirements.
    - Cost-effective as they eliminate the need for dedicated hardware.
    - Easy to manage and deploy in cloud environments.
- **Disadvantages**:
    - Dependent on the underlying hardware and can be limited by its performance.
    - May not handle high traffic volumes as efficiently as physical routers.
- **Examples**:
    - VyOS
    - pfSense
    - Cisco CSR1000V

Name three Router manufacturers/Vendors in the market?

Three Router Manufacturers/Vendors in Nairobi, Kenya

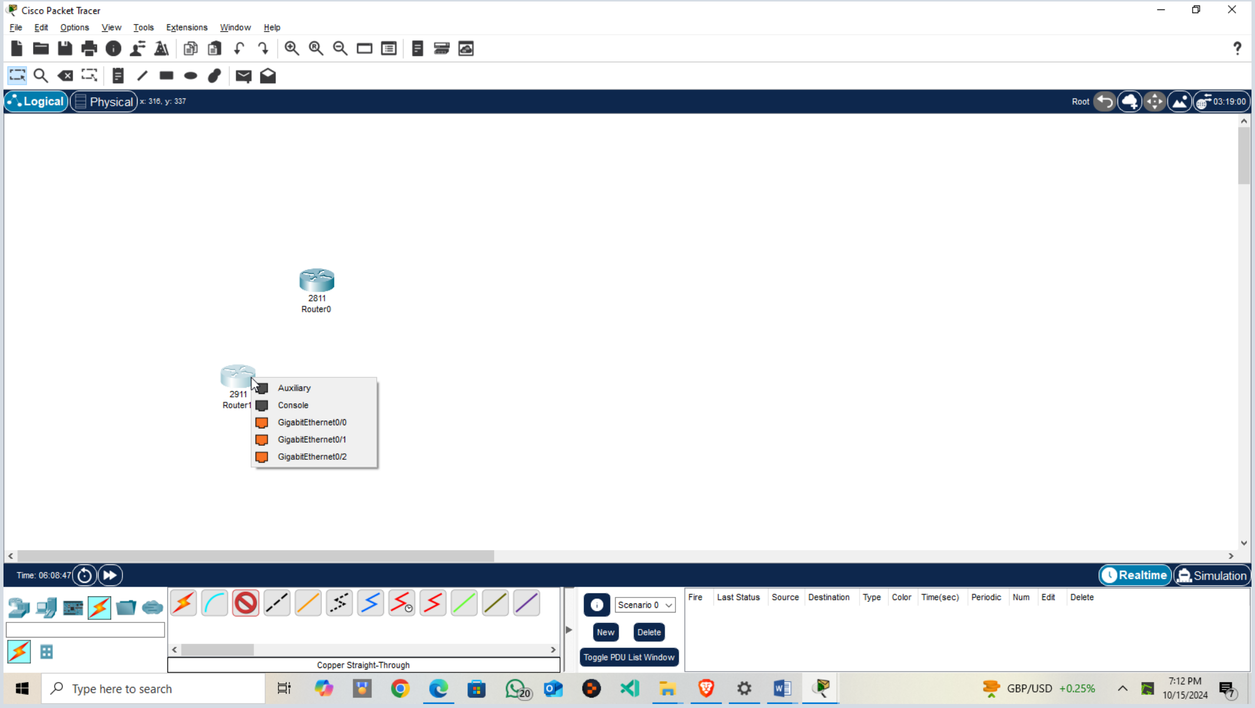
1. **Cisco Systems**
    - A leading manufacturer of networking hardware, including a wide range of routers for both enterprise and consumer use.
2. **TP-Link**
    - Known for producing affordable and reliable routers, TP-Link offers a variety of wired and wireless routers suitable for home and small business applications.
3. **D-Link**
    - A well-known vendor that provides a range of networking equipment, including routers designed for both home and commercial environments.

Lab 2: Inspecting Network devices

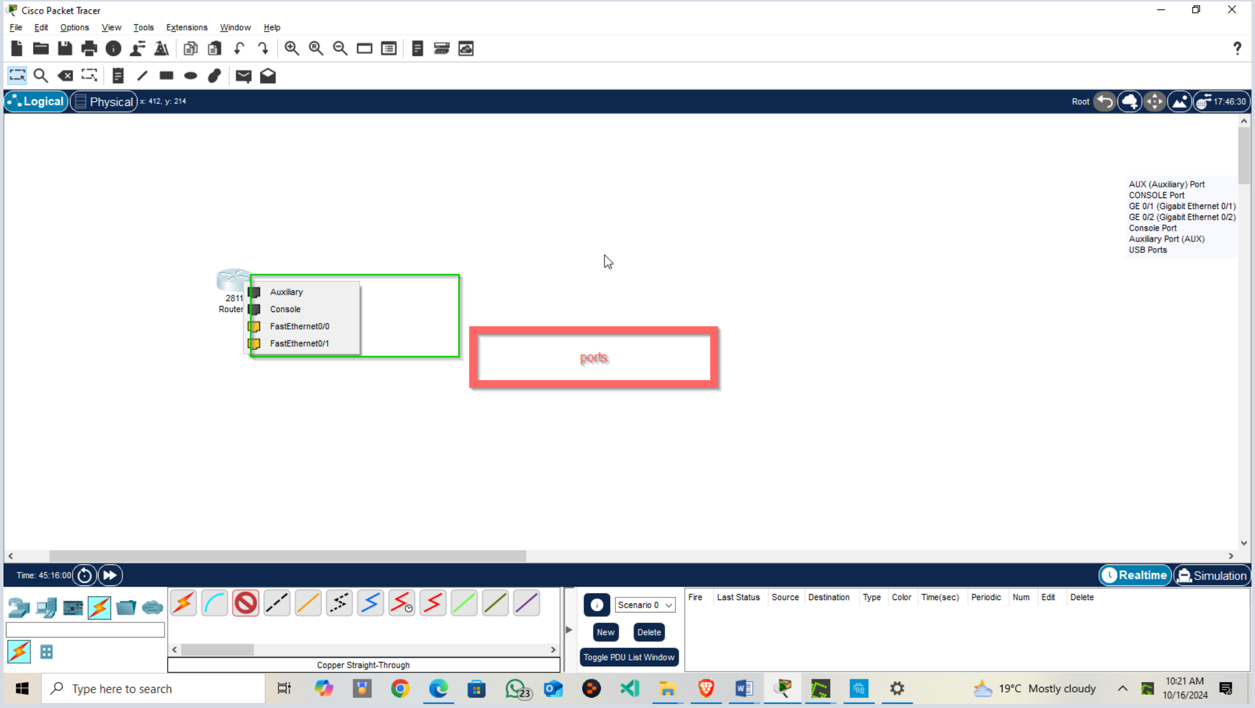
Inspect the following network devices (choose any two Cisco Routers in packet tracer) and Identify the following

● Number of ports the device has

Model 2911

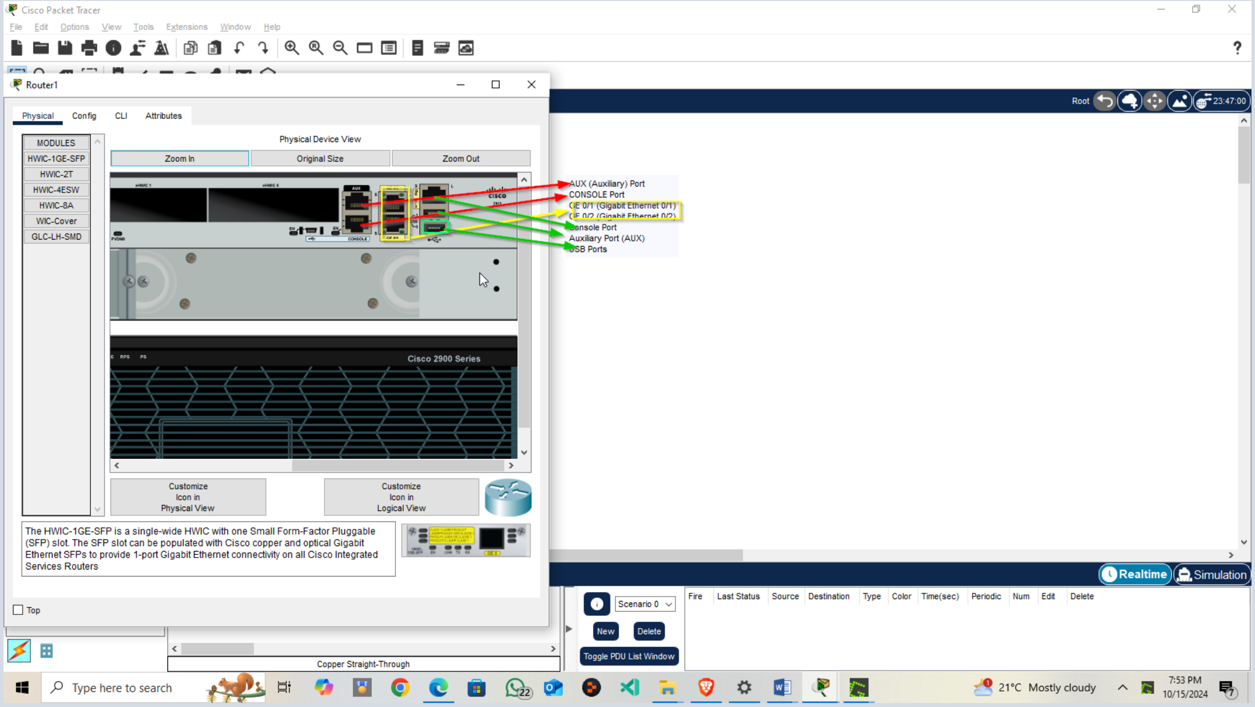


Model 2811



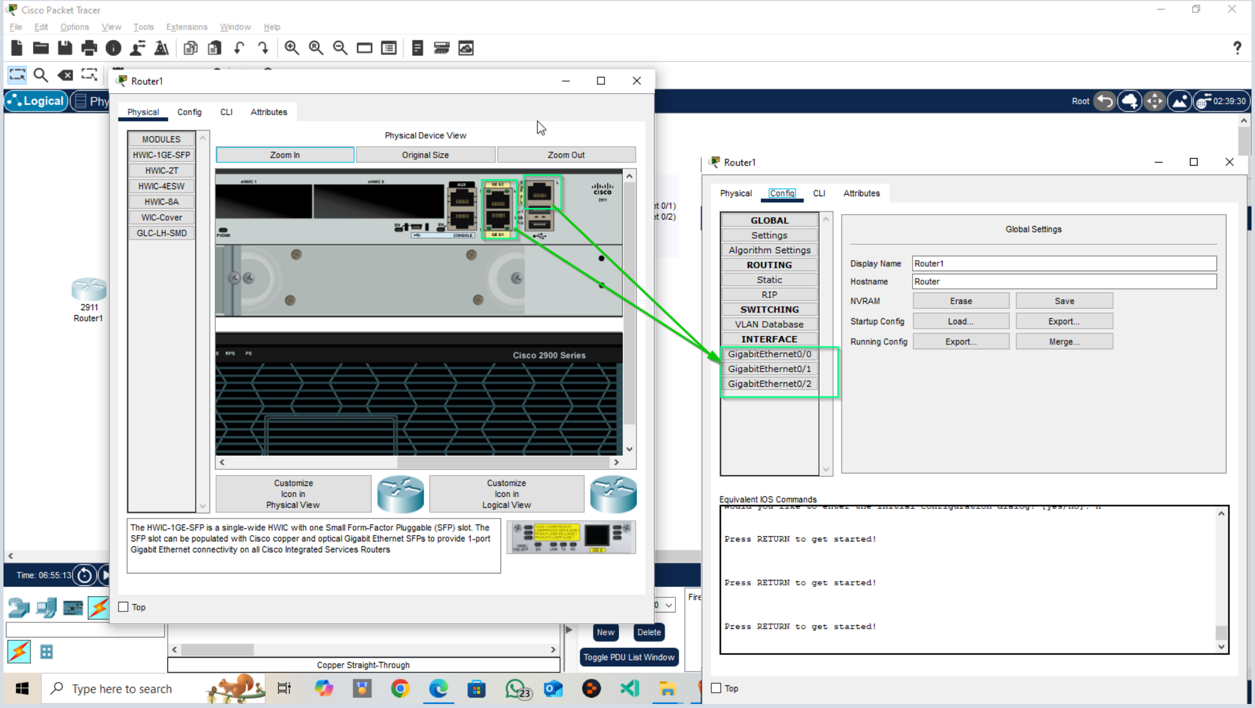
AUX (Auxiliary) Port
CONSOLE Port
GE 0/1 (Gigabit Ethernet 0/1)
GE 0/2 (Gigabit Ethernet 0/2)
Console Port
Auxiliary Port (AUX)
USB Ports

Model 2911



AUX (Auxiliary) Port
CONSOLE Port
GE 0/1 (Gigabit Ethernet 0/1)
GE 0/2 (Gigabit Ethernet 0/2)
Console Port
Auxiliary Port (AUX)
USB Ports

The HWIC-1GE-SFP is a single-wide HWIC with one Small Form-Factor Pluggable (SFP) slot. The SFP slot can be populated with Cisco copper and optical Gigabit Ethernet SFPs to provide 1-port Gigabit Ethernet connectivity on all Cisco Integrated Services Routers



The HWIC-1GE-SFP is a single-wide HWIC with one Small Form-Factor Pluggable (SFP) slot. The SFP slot can be populated with Cisco copper and optical Gigabit Ethernet SFPs to provide 1-port Gigabit Ethernet connectivity on all Cisco Integrated Services Routers

Global Settings

Display Name: Router1

Hostname: Router

NVRAM

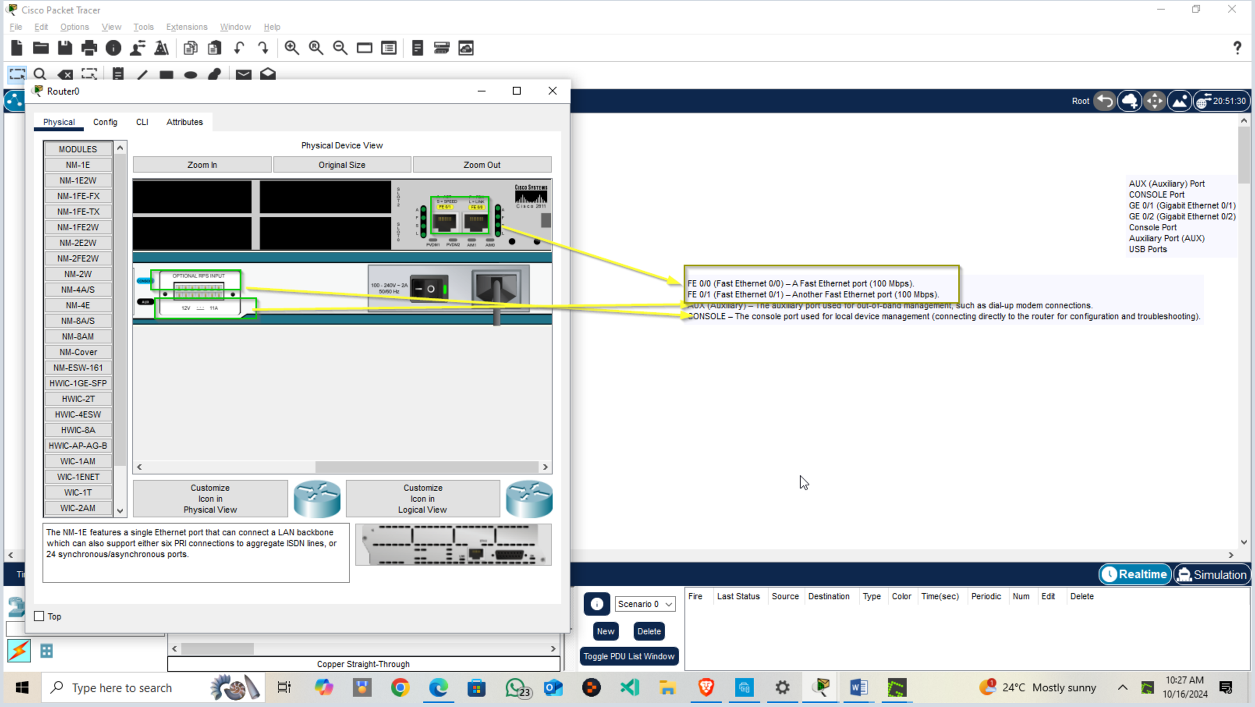
Startup Config

Running Config

Equivalent IOS Commands

```
Would you like to enter the initial configuration dialog? [yes/no]: n


Press RETURN to get started!



Press RETURN to get started!



Press RETURN to get started!
```

Model 2811

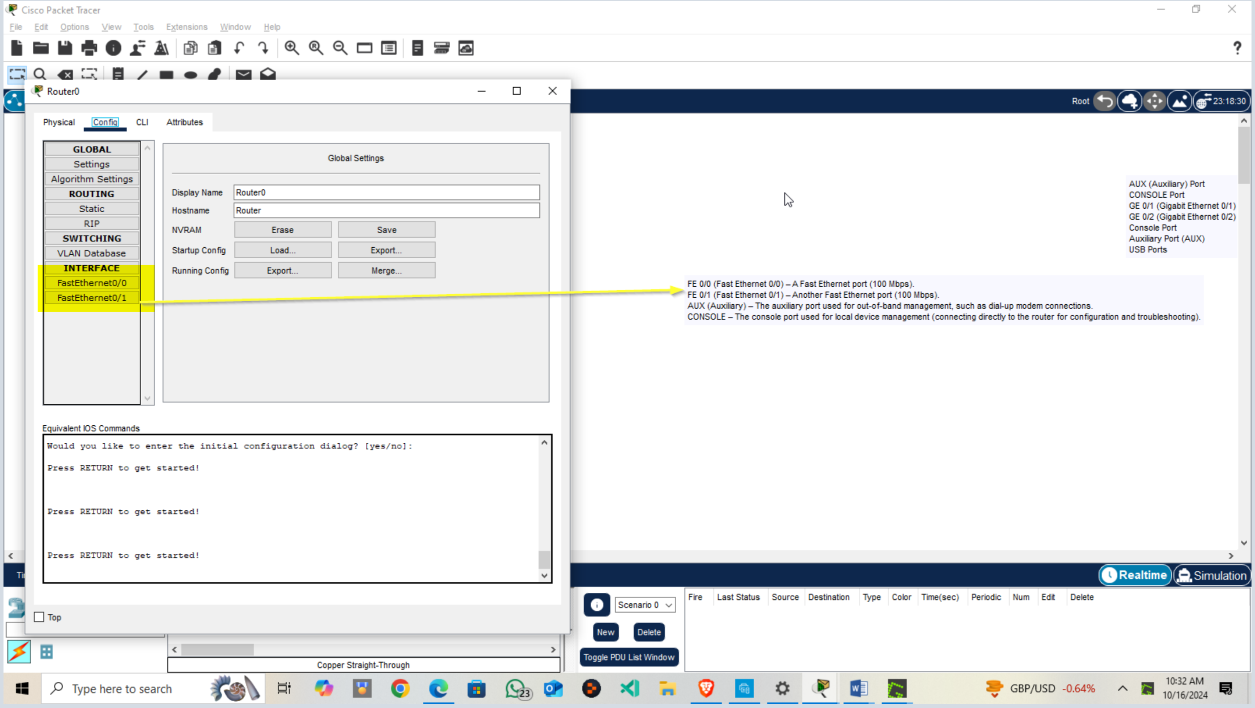


The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

☐ Top

AUX (Auxiliary) Port
CONSOLE Port
GE 0/1 (Gigabit Ethernet 0/1)
GE 0/2 (Gigabit Ethernet 0/2)
Console Port
Auxiliary Port (AUX)
USB Ports

FE 0/0 (Fast Ethernet 0/0) – A Fast Ethernet port (100 Mbps).
FE 0/1 (Fast Ethernet 0/1) – Another Fast Ethernet port (100 Mbps).
AUX (Auxiliary) – The auxiliary port used for out-of-band management, such as dial-up modem connections.
CONSOLE – The console port used for local device management (connecting directly to the router for configuration and troubleshooting).



Global Settings

Display Name: Router0
Hostname: Router
NVRAM: Erase | Save
Startup Config: Load... | Export...
Running Config: Export... | Merge...

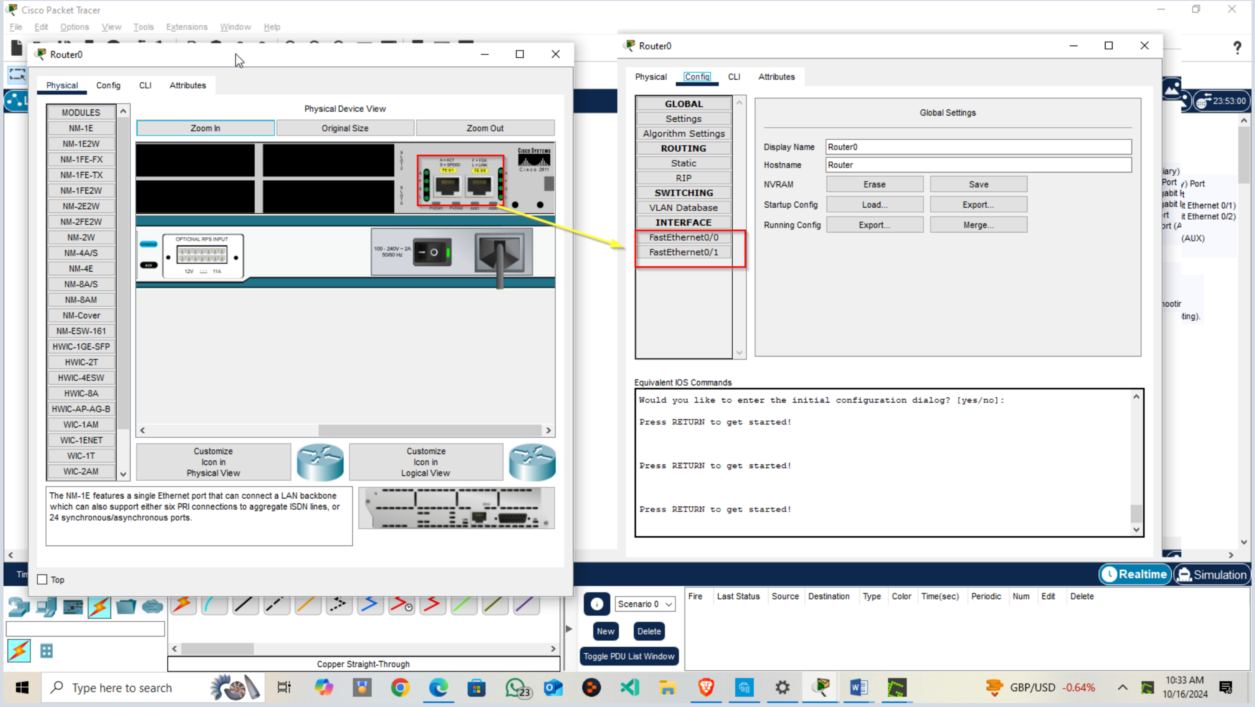
Equivalent IOS Commands

```
Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!



Press RETURN to get started!



Press RETURN to get started!
```

☐ Top

AUX (Auxiliary) Port
CONSOLE Port
GE 0/1 (Gigabit Ethernet 0/1)
GE 0/2 (Gigabit Ethernet 0/2)
Console Port
Auxiliary Port (AUX)
USB Ports

FE 0/0 (Fast Ethernet 0/0) – A Fast Ethernet port (100 Mbps).
FE 0/1 (Fast Ethernet 0/1) – Another Fast Ethernet port (100 Mbps).
AUX (Auxiliary) – The auxiliary port used for out-of-band management, such as dial-up modem connections.
CONSOLE – The console port used for local device management (connecting directly to the router for configuration and troubleshooting).



The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

Display Name: Router0

Hostname: Router

NVRAM: Erase / Save

Startup Config: Load... / Export...

Running Config: Export... / Merge...

```
Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!



Press RETURN to get started!



Press RETURN to get started!
```

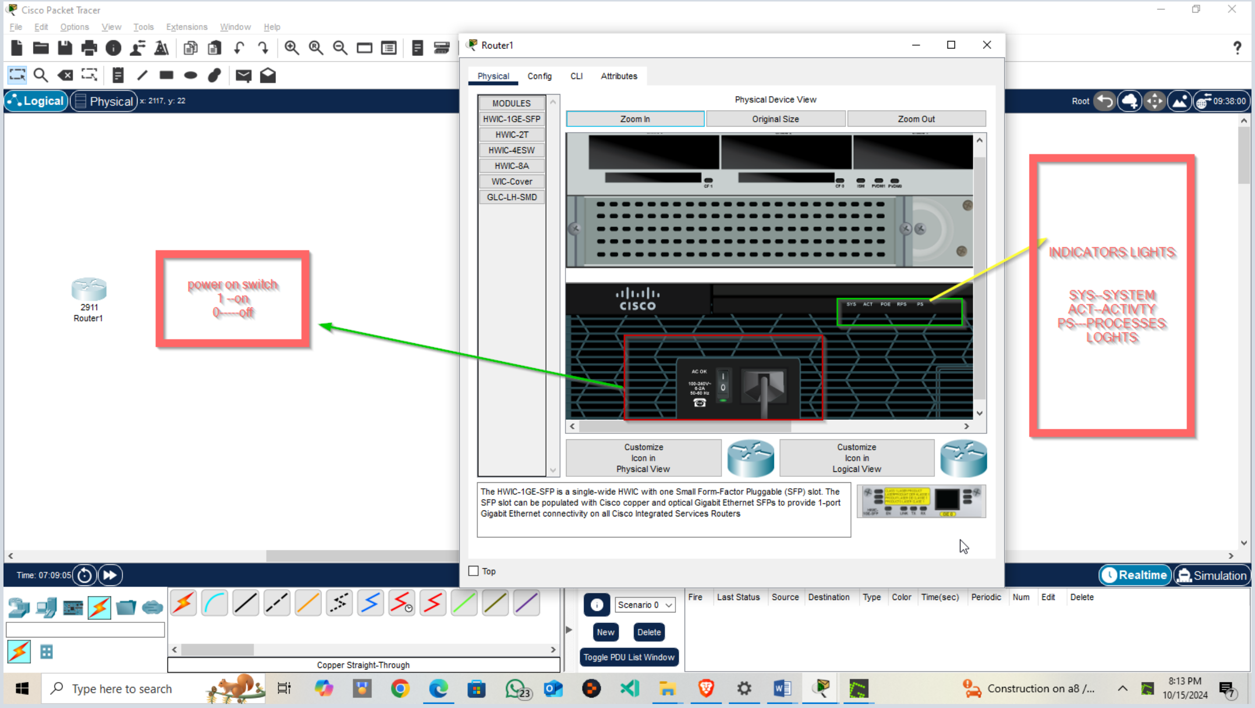
- The *Different type of ports* and what they are used for

. Cisco 2911 Router

- **GigabitEthernet (G0/0, G0/1, etc.)**:
  - The Cisco 2911 has **2 GigabitEthernet ports** (G0/0, G0/1), which allow for higher-speed connections.
- **FastEthernet (F0/0, F0/1, etc.)**:
  - The Cisco 2911 usually does not include FastEthernet ports, but relies on GigabitEthernet ports.
- **Serial Ports (S0/0, S0/1)**:
  - This model can have **2 serial ports** (S0/0/0, S0/0/1), but you may need to install the appropriate serial modules in Packet Tracer.
- **Console Port**:
  - Like most Cisco routers, the **console port** is available for direct access.
- **Auxiliary (AUX) Port**:
  - This router also includes an **AUX port** for remote management via a modem.

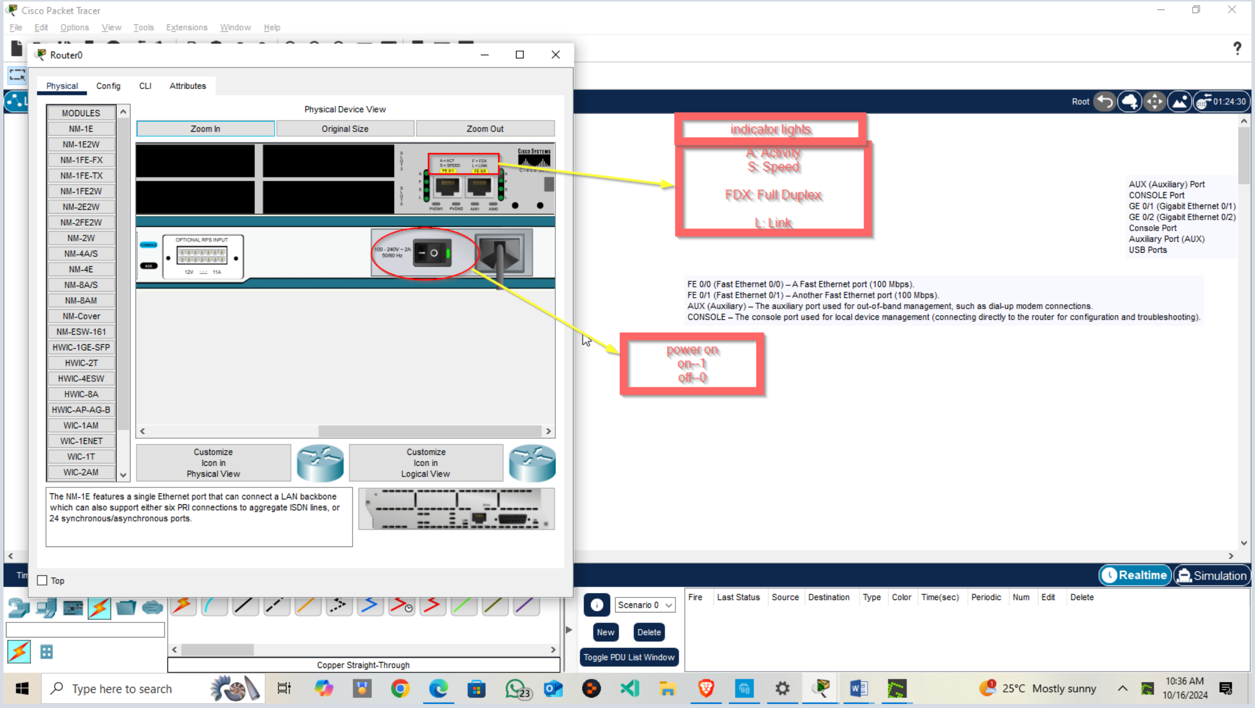
- Indicator lights
- Power on switch

Model 2911



The HWIC-1GE-SFP is a single-wide HWIC with one Small Form-Factor Pluggable (SFP) slot. The SFP slot can be populated with Cisco copper and optical Gigabit Ethernet SFPs to provide 1-port Gigabit Ethernet connectivity on all Cisco Integrated Services Routers

Model 2811



The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

indicator lights

A: Activity
S: Speed

FDX: Full Duplex

L: Link

power on
on--1
off--0

AUX (Auxiliary) Port
CONSOLE Port
GE 0/1 (Gigabit Ethernet 0/1)
GE 0/2 (Gigabit Ethernet 0/2)
Console Port
Auxiliary Port (AUX)
USB Ports

FE 0/0 (Fast Ethernet 0/0) – A Fast Ethernet port (100 Mbps).
FE 0/1 (Fast Ethernet 0/1) – Another Fast Ethernet port (100 Mbps).
AUX (Auxiliary) – The auxiliary port used for out-of-band management, such as dial-up modem connections.
CONSOLE – The console port used for local device management (connecting directly to the router for configuration and troubleshooting).

Lab 3: Connecting to a Router

● What are *three* different ways to connect to a cisco router? What are the different methods used for?

Ways to Connect:

These are the ***physical or network mechanisms*** *through which you establish a connection to the router:*

1. ***Console Port****: A physical connection using a console cable (RJ-45 to serial or USB).*
2. ***SSH or Telnet****: A remote network-based connection using IP (SSH over port 22, Telnet over port 23).*
3. ***Auxiliary (AUX) Port****: A physical connection using a modem or another serial connection.*

Methods Used:

These describe the ***communication protocol or approach*** *employed during the connection, focusing on how the data is transferred:*

1. ***Console Port****: Direct, local access to the router using a serial connection. It is used for initial configuration or when there is no network connectivity.*
2. ***SSH or Telnet****: Network-based remote access methods, where:*
   - ***SSH*** *is a secure, encrypted method.*
   - ***Telnet*** *is an unencrypted method, useful in trusted environments but considered insecure for remote connections.*
3. ***Auxiliary (AUX) Port****: Out-of-band management, typically used for remote access over a modem connection, allowing administrators to manage the router when network connectivity is unavailable.*

● What is an IOS? What is it used for?

IOS (Internetwork Operating System) *is the operating system that runs on most Cisco devices, including routers and switches. It provides the basic functionality for routing, switching, and other network management tasks. The IOS allows administrators to configure, manage, and troubleshoot the network hardware.*

● Briefly describe what happens when bringing up a router.

- ***POST (Power-On Self Test)****: The router performs a self-test to ensure that all hardware components are functioning correctly.*
- ***Loading the Bootstrap****: After POST, the router loads the bootstrap program from ROM to initialize the hardware and locate the IOS.*
- ***Loading the IOS****: The IOS is loaded from flash memory or another storage location.*
- ***Locating and Loading the Configuration File****: The router looks for the startup configuration file in NVRAM. If it finds one, it loads and applies the configuration; if not, the router enters setup mode, prompting the user to configure the router.*

- ***Running Configuration****: Once the configuration file is loaded, the router starts its services and applies the network configurations.*

Lab 4: Router’s Command Line Interface

1. How do you access the Router’s command Line Interface?
   Using terminal emulation software such as PuTTY or Tera Term, you can connect to the router via console, SSH, or Telnet to access its command line interface (CLI).
2. Distinguish between the different configuration modes that you can be in when configuring a router.
   - User EXEC Mode: Basic mode with limited commands, indicated by Router>.
   - Privileged EXEC Mode: Provides access to all commands, including configuration commands, indicated by Router#.
   - Global Configuration Mode: Used to make system-wide changes, accessed through the configure terminal command, indicated by Router(config)#. Can configure interfaces here.
   - Interface Configuration Mode: Specific to configuring interfaces, entered by selecting an interface from global config, indicated by Router(config-if)#.
3. What aspects of the router can you configure in each mode?
   - User Exec Mode: check router info and perform basic testing commands such as pinging other hosts.
   - Privileged EXEC Mode: check configurations, find errors, and make system-wide configuration changes.
   - Global Configuration Mode: Configuration of hostnames, routing protocols and passwords.
   - Interface Configuration Mode: Configuration of IP addresses and routing protocols.
4. How do you enter and exit each mode? What kind of CLI prompt do you get when configuring a router in each mode?
   - From user Exec to Privileged EXEC: Use enable command.
   - From Privileged EXEC to Global Configuration: Use configure terminal.
   - From Global Configuration to Interface Configuration: Use interface [type] [number] (e.g., interface gig0/1).
   - To Exit: Use exit to go back one level, and disable to exit Privileged EXEC Mode back to User EXEC Mode.
5. Briefly describe the basic editing and help features of a router.
   - Features for editing: Tab for automatic command completion, Ctrl+A to navigate to the beginning of a command line, Ctrl+E to travel to the end, and Ctrl+C to cancel a command.
   - Help Features : You can use? to get help on possible commands at any time, or you can partially type a command and then? to get a list of possibilities.

Lab 5: Router Configuration (Administrative) through CLI

Explain the reasons why each of these configurations is important. Highlight the commands used for accomplishing the required configuration in each case.

Setting router passwords (enable, auxiliary, console, telnet, enable secret (password Encryption))

Securing router access avoids unauthorised alterations and guarantees that only trustworthy users can configure the equipment.

a. Enable Password: Prevents unauthorised access to the priviledged EXEC mode.

```
Router(config)# enable password <password>
```

b. Enable Secret: An encrypted, more secure form of the enable password.

```
Router(config)# enable secret <password>
```

c. Auxiliary password :Secures access via auxiliary ports

```
Router(config)# line aux 0
Router(config-line)# password <password>
Router(config-line)# login
```

d. Console Password: Secures access via the console port.

```
Router(config)# line console 0
Router(config-line)# password <password>
Router(config-line)# login
```

e. Telnet/VTY Password: Secures remote access via Telnet.

```
Router(config)# line vty 0 4
Router(config-line)# password <password>
Router(config-line)# login
```

f. Password Encryption: Secures all plaintext passwords within the configuration.

```
Router(config)# service password-encryption
```

Setting router banners

Router banners provide critical information or legal disclaimers when users connect to the router.

```
Router(config)# banner motd #Authorized Access Only#
```

Performing Interface Configurations (Bringing up a router interface, Configuring IP address, Serial interfaces)

Configuring router interfaces is required for network connectivity. Proper interface configuration allows the router to communicate with other devices in the network.

a. Bringing up a router interface :

```
Router(config)# interface <interface_name>
Router(config-if)# no shutdown
```

b. Configuring IP address :

```
Router(config-if)# ip address <ip_address> <subnet_mask>
```

c. Serial interfaces (used for WAN connections) :

```
Router(config)# interface serial 0/0
Router(config-if)# ip address <ip_address> <subnet_mask>
Router(config-if)# no shutdown
```

Setting router Hostname

The hostname is used to identify the router in the network. Setting a unique hostname allows network administrators to readily identify the router, particularly in big networks.

- ➢ Router(config)# hostname <new_hostname>

Setting Interface descriptions

Interface descriptions provide context for what each interface connects to. Descriptions facilitate network management by providing human-readable information about interface roles or connected devices.

- ➢ Router(config-if)# description <description_text>

Viewing, saving and erasing router configurations

Managing router configurations is key to maintaining network stability. Saving configurations guarantees that changes are kept even after a reboot. Erasing a configuration restores the router to its factory defaults, which can be handy for reconfiguring or troubleshooting.

- ➢ Router# show running-config
- ➢ Router# copy running-config startup-config
- ➢ Router# erase startup-config

Routing Protocol Configuration

Routing protocols are essential for dynamic routing in a network. Routing protocols such as RIP, OSPF, and EIGRP enable routers to dynamically communicate information and find the optimum paths for sending traffic. Routing protocols such as RIP, OSPF, and EIGRP enable routers to dynamically communicate information and find the optimum paths for sending traffic.

- ➢ Router(config)# router rip
- ➢ Router(config-router)# network <network_address>

What is a running configuration in routers? Why is it important to save running configurations?

The running configuration comprises the router's current and active settings. It lives in the router's RAM and is volatile (meaning it is lost if the router is turned off or restarted).

The importance of saving running configurations:

Saving the running configuration ensures that any modifications made to the router's settings are retained in non-volatile memory (NVRAM). This allows the router to restore the saved configuration when it reboots, providing network continuity.

Lab 6: Testing and Verifying Router Configuration

Explain what you can test/verify with each of these commands. What is the resultant output?

Show interface

This command provides extensive information about each router interface, such as physical and logical status, traffic statistics, and problems. You can inspect whether the interface is up or down, check IP addressing, monitor bandwidth utilisation, and detect issues such as collisions or dropouts.

- Router# show interface

Resultant Output:

The output displays the interface's operational state (up or down), the associated IP address, bandwidth, duplex mode, packet counts (input/output), and error counts (for example, collisions and CRC errors).

Show IP interface

This command displays extra information about the IP configuration on router interfaces, such as IP addresses, ACLs (Access Control Lists), and IP-related parameters.You can check an interface's IP address, ICMP redirection status, and security features such as ACLs.

- Router# show ip interface

Resultant Output:

It displays whether the interface is operational, whether it has been issued an IP address, whether any access control lists are in use, and other IP-specific information (for example, NAT active or disabled).

Show IP brief

This command displays a short summary of all interfaces, including their IP address and status (up or down). This command is useful for quickly determining the IP address and status of all interfaces. You can determine whether an interface is "administratively down" or working.

- Router# show ip interface brief

Resultant Output:

It provides a quick, tabular overview of the interfaces, including the IP address given to each interface and whether they are operational (up or down).

Show protocols

This command displays the status of the routing protocols as well as the IP configuration for each interface. You can check whether IP routing is enabled and the status of certain protocols on interfaces. It also shows you the IP address associated to each interface.

- Router# show protocols

Resultant Output:

The output contains both the global routing protocol configuration and the status of each protocol on specified interfaces. It also shows the IP addresses assigned to the interfaces.

Show controllers

This command displays extensive information on the hardware controllers for certain interfaces, such as serial or physical layer devices. You can check whether the serial interface is using a DCE or DTE cable and the clock rate settings, which are required for WAN connections.

- Router# show controllers serial 0/0

Resultant Output:

The output includes information about the hardware (such as clock rates, DTE/DCE status, and cabling details) and interface controllers.

Lab 7: IP Routing

Configure and Verify IP routing:

Static routing

Static routing requires manually setting a path for packets to take from one network to another. This is beneficial in small, stable networks or when you require exact control over the routing path.

Configuration:

To set up a static route, use the ip route command. You define the target network, subnet mask, and next-hop IP address or exit interface.

- Router(config)# ip route <destination_network> <subnet_mask> <next_hop_address>

Example :

- Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.2

Verification:

To verify the static route configuration, use the show ip route command, which displays the routing table.

- Router# show ip route

The "S" in the routing table indicates that this is a static route.

Default Routing

Default routing is used when a router does not have a specified route to a destination network and must redirect packets to a default route.

Configuration:

To configure the default route, enter 0.0.0.0/0 and it will match any destination.

- Router(config)# ip route 0.0.0.0 0.0.0.0 <next_hop_address>

Example:

- Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

Verification:

Use show ip route to confirm that the default route is present.

- Router# show ip route

The "*" indicates a default route.

Dynamic routing: RIP

Dynamic routing systems, such as RIP, automatically learn and broadcast routes within a network, eliminating the need for manual changes in changing settings.

Configuration:

RIP is a distance-vector routing protocol that distributes routes across neighbouring routers. To configure RIP, you must specify which networks should participate in RIP routing.

```
Router(config)# router rip
Router(config-router)# version 2  # To enable RIP version 2
Router(config-router)# network <network_address>
```

Example:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
```

Verification:

Use show ip protocols to verify that RIP is running and see which networks are being advertised.

```
Router# show ip protocols
```

Switches

SWITCH L2 LAB

1. **Unmanaged Switches:** These provide connectivity without the needing the user to configure. Example: NETGEAR GS308

Advantages:

- They are inexpensive
- They are to use
- The have a plug and play functionality

Disadvantages:

- Not good for security.
- Features such as Quality of Service are not there.
- Does not feature monitoring capabilities.

2. **Managed Switches:** allow the configuration of a network as well as monitoring through the use of tools such as VLANs and SNMP. Example: Cisco Catalyst 2960

   Advantages:

   - Enhanced security
   - Capable of monitoring
   - Advanced features such as VLANs are available

   Disadvantages:

   - Are complex to configure
   - Are expensive

3. **Cut-through Switch:** a technique that allows for forwarding of a frame as soon as the destination MAC has been determined.

   Advantages:

   - It has low latency

   Disadvantages:

   - Error checking is not done hence forwarding of corrupted frames is possible

4. **Store and forward switch:** A technique whereby a switch will store an entire frame before it forwards it. Therefore, enabling error checking. Example: Cisco Catalyst Switches

   Advantages:

   - Very reliable
   - Contains an error checking mechanism

   Disadvantages:

   - Has high latency

5. **Stackable vs non-stackable switches:**

a. **Stackable switch:** It can be connected to create one logical switch; therefore, making network management easy. Example: Cisco Catalyst 9300

b. **Non-stackable switch:** Are managed individually and they operate independently e.g. NETGEAR GS105

6. **Chassis Switch:** It is a large modular switch employed in enterprise networks. You can remove or add line cards. E.g. Cisco catalyst 6500

Advantages:

- Has high port density
- It is highly scalable

Disadvantage:

It is expensive

LAB 2: INSPECTING NETWORK DEVICE

Switch:

Has 24 fast ethernet ports and 2 gigabit ethernet ports.

Fast Ethernet ports: you can use them to connect end devices such as other switches and PCs

Gigabit Ethernet Ports: connect to backbone connection or to faster devices.

Indicator Lights:

- **System light:** shows if switch is on
- **Port status:** shows amber if there are problems and green if active.

Hub:

Has 6 ethernet ports for normal data transfer. All devices connected to a hub will receive the same signal.

Indicator light: A hub has activity lights that show the port is being used for data transmission.

LAB3: DIFFERENT TYPES OF NETWORK CABLES AND CONNECTORS

Connecting Unlike Devices:

You can use a straight-through cable (Ethernet). Connector: RJ 45

Connecting like devices: PC-PC, ROUTER-ROUTER, SWITCH-SWITCH, HUB-HUB, ROUTER-PC

To connect like devices in the above examples, use a cross-over cable. Connector RJ 45

For router to router, you can also use a serial cable and a DB60 connector

Console into the Switch from your Computer:

You can use the rollover cable (console cable)

The connector will be an RJ 45 at the switch and a serial DB9 at the PC

Software: To connect, you will need a software such as Tera Term or PuTTY, which will enable communication with the switch.

Cable Type: RJ45-to-DB9 (or USB-to-RJ45, if using an adapter)

Pin Configuration: Rollover cables have a specific pinout where each pin on one end connects to the corresponding opposite pin on the other end (1 to 8, 2 to 7, and so on).

- **RJ45 Connector Pinout (on the Switch side)**:
  1. Pin 1 → Connects to Pin 8
  2. Pin 2 → Connects to Pin 7
  3. Pin 3 → Connects to Pin 6
  4. Pin 4 → Connects to Pin 5
  5. Pin 5 → Connects to Pin 4
  6. Pin 6 → Connects to Pin 3
  7. Pin 7 → Connects to Pin 2
  8. Pin 8 → Connects to Pin 1
- **DB9 Connector Pinout (on the PC side)**:
  - Pin 1: **Carrier Detect** (CD) — Not typically used in console connections.
  - Pin 2: **Receive Data** (RXD) — Receives data from the switch.
  - Pin 3: **Transmit Data** (TXD) — Sends data to the switch.
  - Pin 4: **Data Terminal Ready** (DTR) — Used for flow control.
  - Pin 5: **Signal Ground** (GND) — Common ground between devices.
  - Pin 6: **Data Set Ready** (DSR) — Used for flow control.
  - Pin 7: **Request to Send** (RTS) — Used for flow control.
  - Pin 8: **Clear to Send** (CTS) — Used for flow control.
  - Pin 9: **Ring Indicator** (RI) — Not typically used.

Wire Color (RJ45 side):

The wire colors can vary depending on the manufacturer, but a typical color scheme for the **RJ45-to-DB9 console cable** might be:

1. Pin 1 (Blue)
2. Pin 2 (Orange)
3. Pin 3 (Black)
4. Pin 4 (Red)
5. Pin 5 (Green)
6. Pin 6 (Yellow)
7. Pin 7 (Brown)
8. Pin 8 (White)

Since this is a rollover cable, the pins on one side are reversed on the other end of the cable.

Connector Names:

- **RJ45** (Switch Side): Used to connect to the console port of the switch or router.
- **DB9 Serial** (PC Side): Older PCs may have a serial port for direct connection.
    - Alternatively, modern PCs use a **USB-to-Serial Adapter**, where the USB connects to your PC and the RJ45 connects to the switch.

What Each Pin Does:

- **Pin 1**: Carrier Detect (not used in console setup).
- **Pin 2**: Receives data from the switch (RXD).
- **Pin 3**: Sends data to the switch (TXD).
- **Pin 4**: Flow control (DTR, optional).
- **Pin 5**: Ground (GND).
- **Pin 6**: Flow control (DSR, optional).
- **Pin 7**: Flow control (RTS, optional).
- **Pin 8**: Flow control (CTS, optional).

LAB 4

The reason why each of these configurations are important with their commands

1. Setting passwords (User Mode, Privileged Mode, Telnet and Console Access passwords)

Importance of setting passwords are essential for securing the network and preventing unauthorized access to the router or switch.

User Mode passwords are beneficial in protecting the basic access to the devices only allowing authorized personnel to view device settings.

Privileged Mode passwords provide a second layer of security by securing the device's configuration parameters, which are more sensitive and important to network operation.

Console and Telnet access passwords secure both local console and distant Telnet access points, allowing only trusted users to manage the device.

Some of the commands to execute are:

a. User Mode Password

```
Switch(config)# line console 0
Switch(config-line)# password [password]
Switch(config-line)# loginSetting Hostname
```

b. Privileged Mode Password

```
Switch(config)# enable secret [password]
```

c. Telnet Access Password

```
Switch(config)# line vty 0 4
Switch(config-line)# password [password]
Switch(config-line)# login
```

2. Setting Hostname

Setting Hostname is important in that hostnames distinguish network devices by assigning them distinct identifiers. This is especially important in larger networks with many interconnected devices. A concise and descriptive hostname makes device identification easier while monitoring and troubleshooting. It also simplifies the management of configuration files, logs, and warnings when devices are named based on their job or location in the network.

Command to execute is:

```
Switch(config)# hostname [hostname]
```

3. Setting Message of the Day

When a user uses the device, the MOTD is often used to show essential legal notices or network-related warning messages. This helps to reinforce security regulations and informs users about their responsibilities and constraints when using the system. It can also show maintenance windows or contact information for network administrators in case of an issue. Although not a security measure in and of itself, it functions as a deterrent and compliance mechanism.

Command to execute is:

```
Switch(config)# banner motd #[message]#
```

4. Setting Management ip address and mask

The management IP address is necessary for remote administration. Administrators can administer the switch or router remotely using protocols such as Telnet, SSH, or HTTP/HTTPS after assigning it an IP address. This is particularly valuable in large, scattered networks. The subnet mask controls the extent of the network with which the device can directly communicate, ensuring effective routing of data.

Command to execute is:

```
Switch(config)# interface vlan 1

Switch(config-if)# ip address [ip address] [subnet mask]

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

5. Setting Interface descriptions

Interface descriptions help to show the purpose of each port such as which device is connected to it or what function the port performs such as uplink to another switch or connection to a certain server. This is extremely useful for troubleshooting and doing network audits. Clear interface descriptions minimize errors during configuration updates and improve network administration.

Command to execute is:

```
Switch(config)# interface [interface id]
Switch(config-if)# description [description]
```

6. Save System Configurations

Saving the operating configuration to the startup configuration ensures that any modifications made to the device's settings are kept following reboot. If the device is not stored, it will revert to its old settings when restarted, potentially causing network difficulties or downtime.

Command to save system configuration is:

```
Switch# copy running-config startup-config
```

7. Erase Switch Configuration

When decommissioning a device and repurposing it for a different network, you must first erase its configuration. This restores the device to its factory defaults, removing any custom settings that may conflict with the new environment or security regulations. This provides a clean slate for reconfiguration, preventing the persistence of existing configurations that could cause problems.

Command to erase switch configuration is:

```
Switch# erase startup-config
Switch# reload
```

8. Setting the IP Default Gateway

For the switch or device to communicate with devices on various subnets or outside of its local network, the default gateway is necessary. Traffic meant for external networks would be lost in the absence of a default gateway, reducing the device's communication range. Complete network operation is ensured by properly configuring this, especially for switches that require remote management or communication with other network levels.

Command to set up the IP Default Gateway is:

```
Switch(config)# ip default-gateway [ip address]
```

9. Setting Port Security

Port security improves security by limiting how many devices can connect to a switch port. It prohibits unauthorized devices from connecting to the network by specifying which MAC addresses are permitted on a port. This is especially critical in contexts with minimal physical security such as open office spaces or public places since it protects against potential network breaches.

Command for setting port security is:

```
Switch(config)# interface [interface id]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum [number]
Switch(config-if)# switchport port-security violation [shutdown/protect/restrict]
```

10. Set Speed and Duplex Mode

Network performance problems like collisions and errors can be caused by difference in the speed and duplex settings between devices. Network administrators can minimize problems such as packet loss and boost overall network performance by manually adjusting these settings to ensure constant and optimum communication between devices.

Command for set speed and duplex mode is:

```
Switch(config)# interface [interface id]
Switch(config-if)# speed [10/100/1000]
Switch(config-if)# duplex [half/full]
```

11. Disable Unused Ports

Turning off unneeded switch ports is a simple yet effective security technique. It prevents unauthorized devices from connecting to the network and narrows the attack surface for prospective breaches. In addition to improving security, it conserves network resources by reducing wasteful traffic from idle ports.

Command for disabling ports is:

```
Switch(config)# interface [interface id]
Switch(config-if)# shutdown
```

12. Configuring VLANs

VLANs are used to separate network traffic, resulting in smaller broadcast domains while boosting security and performance. Its separate network traffic, lowering congestion and minimizing the spread of broadcast storms. It also improves security by separating sensitive data and preventing it from traversing the whole network.

Command for configuring VLANs is:

a. Create VLAN:

```
Switch(config)# vlan [vlan number]
Switch(config-vlan)# name [vlan name]
```

b. Assigning VLAN to port

```
Switch(config)# interface [interface id]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan [vlan number]
```

13. Configure Access and Trunk Ports

Access ports connect end devices, such as PCs and printers, to a specific VLAN, ensuring that each device communicates only within its designated VLAN. Trunk ports can carry several VLANs between switches, allowing them to be extended over different network segments. Trunk ports that are properly configured allow tagged VLAN traffic to pass between switches while maintaining VLAN segmentation across the network.

Command for configuring access and trunk ports are:

a. Access port

```
Switch(config)# interface [interface id]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan [vlan number]
```

b. Trunk port

```
Switch(config)# interface [interface id]
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan [vlan numbers]
```

LAB 5

Testing and verifying switch configuration

1. Show version

This command provides detailed information on the router or switch, including the IOS version, system uptime, hardware specifications, and license information. What was verified are:

a. IOS version currently running on the device
b. System uptime.
c. Configuration register value.
d. Device model and serial number.
e. Amount of memory in the device

The resultant output is:

```
Cisco IOS Software, C3560 Software (C3560-IPSERVICESK9-M), Version 12.2(55)SE3,
RELEASE SOFTWARE (fc1)
System image file is "flash:c3560-ipservicesk9-mz.122-55.SE3.bin"
```

```
cisco WS-C3560-24PS (PowerPC405) processor (revision K0) with 131072K/8192K bytes of memory.
```

2. Show running-config

This command displays the currently active configuration in the device’s RAM. What was verified are:

a. Current interface settings such as the IP addresses
b. Security settings that consist of password configurations
c. Routing protocols and their settings
d. VLAN configurations, NAT settings and access control lists.

The resultant output is:

```
interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
line vty 0 4
 password cisco
 login
```

3. Show ip interface brief

The command provides a brief overview of the IP addresses assigned to interfaces and their operational status. What was verified is:

a. IP addresses assigned to each interface
b. The up/down status and up/down protocol status of each interface
c. Shows interface that are operational, administratively down or have no IP assigned.

The resultant output is:

```
Interface            IP-Address      OK? Method Status                Protocol
GigabitEthernet0/1   192.168.1.1     YES manual up                    up
Vlan1                unassigned      YES unset  administratively down down
```

4. Show mac address-table/clear mac address-table

For **show mac address-table,** it shows the mac address table which consist the mac addresses learned by the switch and the associated interfaces.

For **clear mac address-table,** it clears the dynamic mac address entries in the table.

What was verified is:

a. Mac address currently associated with each switch port.
b. Which ports are forwarding traffic for specific devices based on their mac addresses.
c. Aids troubleshoot issues related to traffic forwarding or network loops.

The resultant output is:

```
VLAN    MAC Address       Type       Ports

----    -----------      --------    -----      -----------

10     0050.56be.efaf    DYNAMIC     Gi0/1

20     00e0.b059.cddd    DYNAMIC     Gi0/2
```