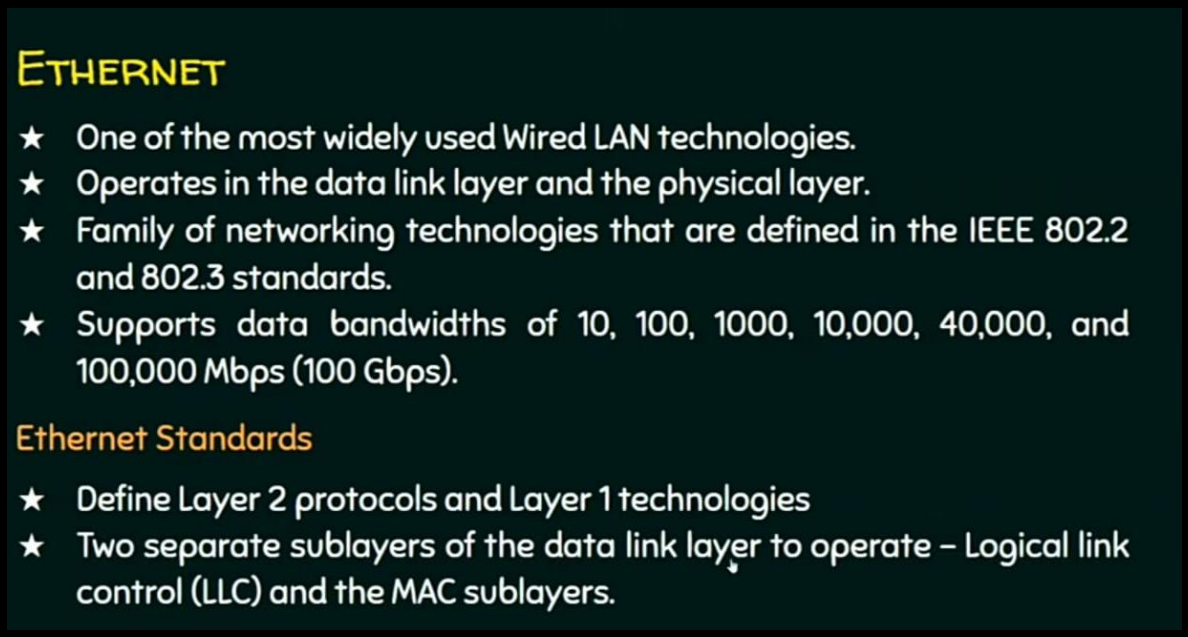
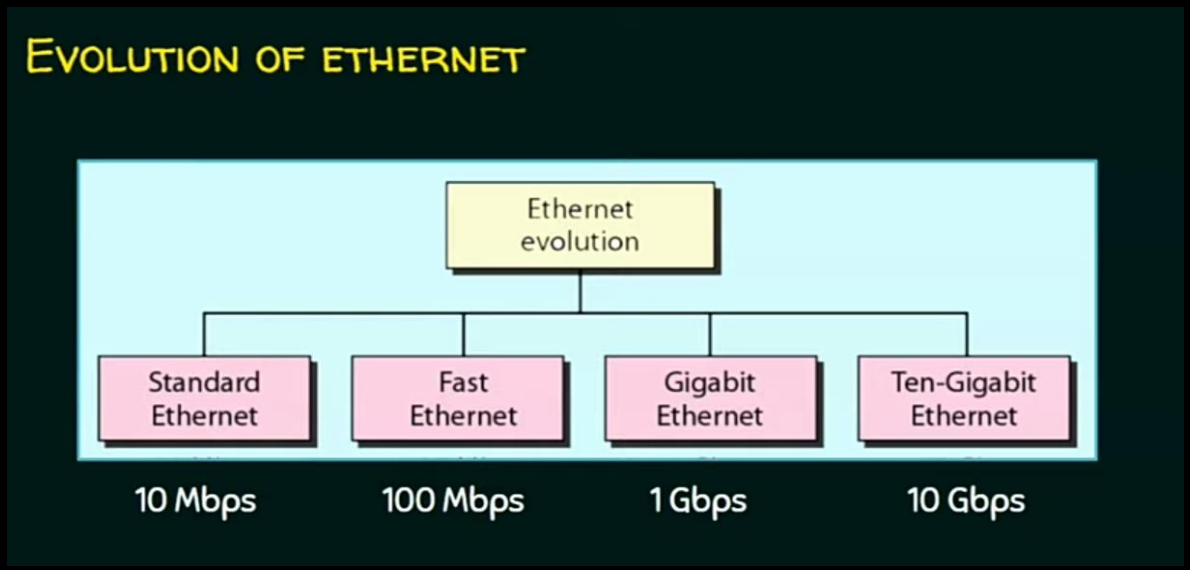
Fundamentals of Ethernet LANs & Cisco IOS

Ethernet LANs (Local Area Networks)

Ethernet is a traditional technology or standard communication protocol that is used to connect devices in a wired local area network (LAN) or a wide area network (WAN).

Ethernet's primary function is to transmit and receive data through cables, facilitating network communication between two or more cables. Transmission in a wired Ethernet network is attained through the use of fiber optic cable, whereas transmission in a wireless network is attained through the use of wireless technologies.





Ethernet Standards

The *Institute of Electrical and Electronics Engineers* (IEEE) develops global standards for networking and communication technologies. These standards define protocols, performance, and interoperability for devices and networks.

Ethernet has evolved over time with different standards, including.

Key IEEE Standards in Networking:

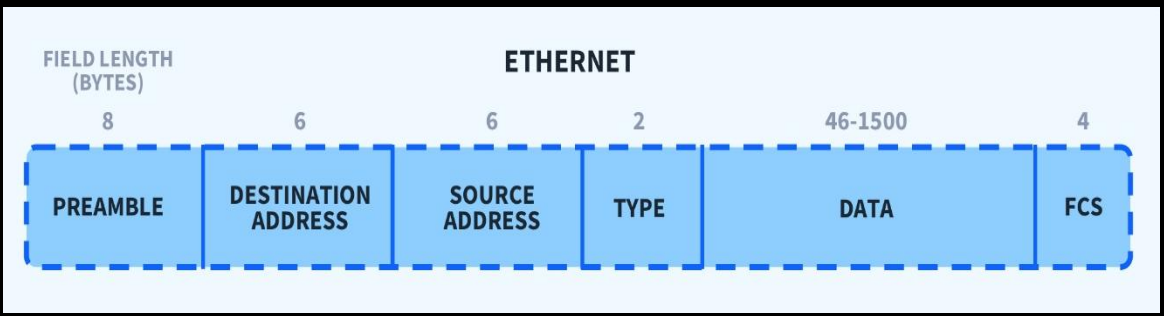
1. Ethernet (IEEE 802.3) - LAN Technology

- **10BASE-T** (10 Mbps, twisted pair)
- **100BASE-TX** (Fast Ethernet, 100 Mbps)
- **1000BASE-T** (Gigabit Ethernet, 1 Gbps)
- **10GBASE-T** (10 Gbps Fast Gigabit Ethernet)

2. Wireless Networks (IEEE 802.11) - Wi-Fi Standards

Ethernet Frames Format

Ethernet frames are used for communication between devices in a LAN. A typical Ethernet frame consists of:



- **Preamble** (7 bytes) – Synchronization
- **Start Frame Delimiter (SFD)** (1 byte) – Marks frame start
- **Destination MAC Address** (6 bytes)
- **Source MAC Address** (6 bytes)
- **EtherType/Length** (2 bytes) – Identifies the protocol

- **Payload** (46–1500 bytes) – Data being transmitted
- **Frame Check Sequence (FCS)** (4 bytes) – Error detection

➢ MAC Address and Addressing

Each device in an Ethernet LAN has a unique **MAC address** (Media Access Control), a 48-bit identifier. Devices communicate using MAC addresses within the LAN.

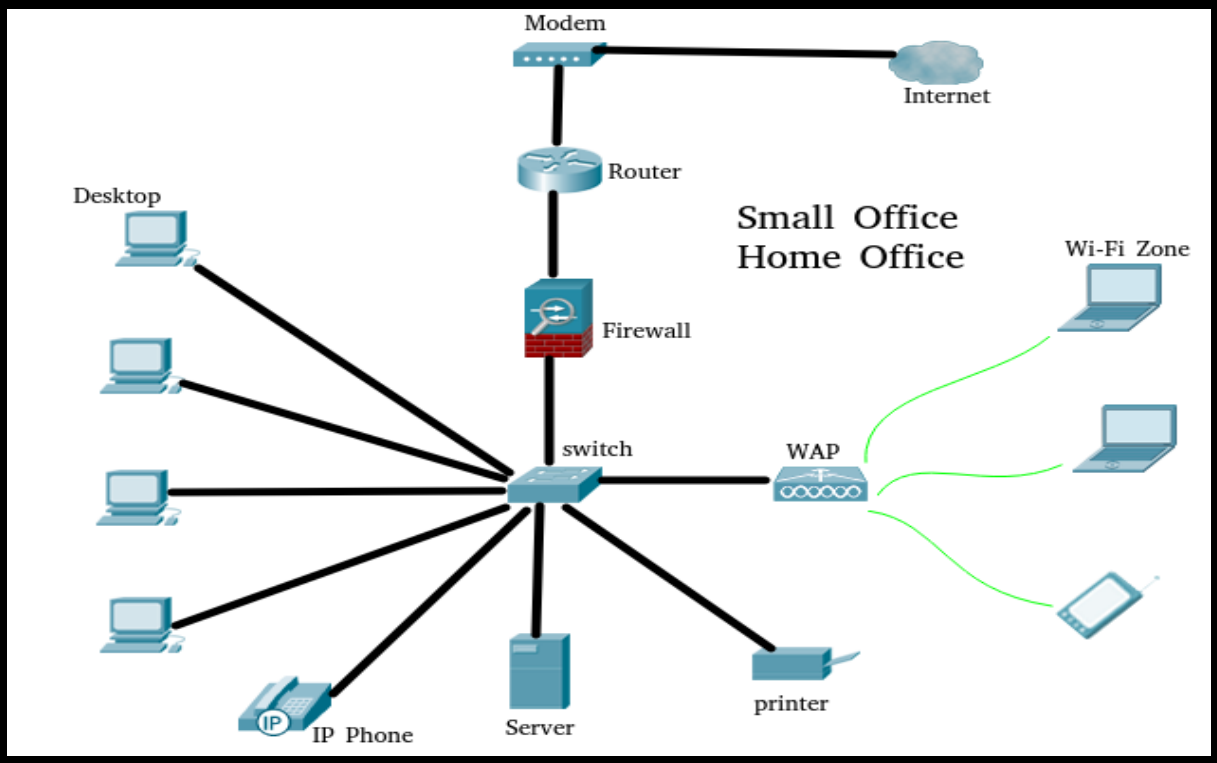
➢ CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Ethernet traditionally used CSMA/CD to avoid collisions. However, in full-duplex switched networks, collisions are eliminated.

➢ Cisco IOS (Internetwork Operating System)

Cisco devices use Cisco IOS, a proprietary operating system for routers and switches. It enables configuration, monitoring, and troubleshooting of network devices.

Small Office Home Office (SOHO)



- SOHO refers to a small-scale business setup operated from home or a small office.
- It is a type of Local Area Network connected to the internet via an ISP.

Components of SOHO Network

- **Router & Modem** – Connects the SOHO network to the internet.
- **Switch** – Allows multiple devices to communicate within the network.
- **Firewall** – Enhances network security.
- **Devices (Nodes)** – Computers, smartphones, printers, and IP phones.
- **Wireless Access Point (WAP)** – Provides Wi-Fi connectivity.

Types of SOHO Businesses:

- Online coaching, blogging, web development, software services, consulting, and remote support.

Benefits of SOHO

- **Cost-effective** – Reduces office space and infrastructure costs.
- **Flexible work hours** – Employees can work anytime.
- **Reduces travel time** – Saves fuel and minimizes pollution.
- **Increased productivity** – Less stress and more focus on work.

Data Flow in SOHO

- Information is transmitted as **data packets** over wired (Ethernet) or wireless (Wi-Fi) connections.
- The **router** manages network traffic using NAT/PAT.

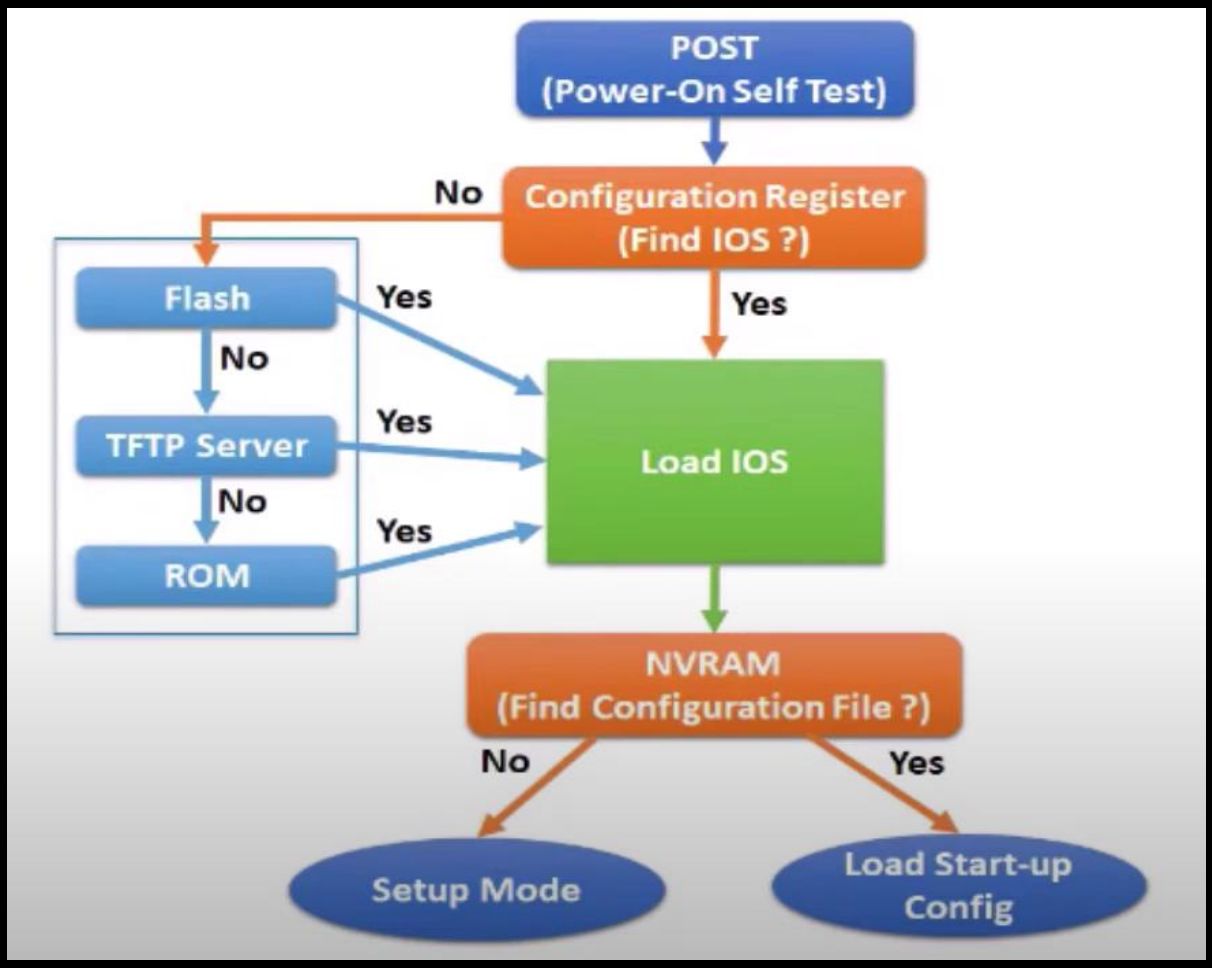
Basic SOHO Network Setup

- Network ID: 192.168.1.0/24 (Private IP addressing).
- Router to Firewall: 10.10.10.0/30
- Routing: Can use Static Routing or RIP (Routing Information Protocol).

Boot Process of Cisco IOS Router

Booting is the process of starting up a device (such as a router or switch) and loading its operating system (IOS in Cisco devices) into RAM so the device can function.

The Cisco router boot process consists of the following steps:



Step 1: Power-On Self-Test (POST)

- The router runs a hardware diagnostic test.
- It checks RAM, ROM, CPU, and interfaces.
- If POST is successful, the router proceeds to the next step.

Step 2: Load Bootstrap Program

- The router loads a small bootstrap program from ROM.
- The bootstrap is responsible for locating and loading the IOS.

Step 3: Locate and Load Cisco IOS

- The bootstrap searches for Cisco IOS in the following order:

1. Flash memory (default location)
    - Flash memory is a type of computer storage that can retain data even when the power is off. It uses floating-gate transistors to trap electrons, which alters conductivity to represent data. It is not designed to be a long-term storage solution.
2. TFTP server (if configured)
    - A simulated Trivial File Transfer Protocol server that allows users to transfer files, like Cisco device configuration backups or IOS images, between a network device (like a router or switch) and the server.
3. ROM (Fallback IOS) – If no other IOS is found

Step 4: Load Startup Configuration (if available)

- The router searches NVRAM for the startup-config file.
- If found, it loads the configuration.
- If no configuration is found, the router enters Setup Mode.

Step 5: Router is Operational

- The router is now fully functional and ready for user input.

Managing Cisco IOS Files

What is Cisco IOS?

- Cisco **Internetwork Operating System (IOS)** is the software used in Cisco routers and switches.
- It provides **networking features** such as routing, switching, security, and administration.
- Stored in **flash memory** and loaded into **RAM** when the device starts.

Components of Cisco IOS Storage

1. **Flash Memory** – Stores the IOS image (persistent).
2. **RAM** – Stores the running configuration (temporary).
3. **NVRAM** – Stores the startup configuration (persistent).
4. **ROM** – Contains basic bootup firmware (ROMmon mode).

Checking and Verifying Cisco IOS Files

Checking the Current IOS Version

- To check the installed IOS version:
- show version
- Displays information such as **IOS version, uptime, memory, and interfaces**.

Checking Flash Memory Storage

- To list files stored in flash memory:
- show flash:
- Ensures sufficient space for upgrading or restoring IOS files.

Backing Up Cisco IOS Files

Why Backup is Important?

- Prevents data loss in case of **hardware failure or corruption**.
- Allows **quick recovery** after system crashes or upgrades.

Backing Up IOS to a TFTP Server

1. Ensure the router can reach the **TFTP server**:
2. ping <TFTP-server-IP>
3. Copy the IOS image to the TFTP server:
4. copy flash: tftp:
5. Enter the **TFTP server IP** and the **destination filename** when prompted.

Backing Up IOS to an FTP Server

1. Set FTP credentials:
2. ip ftp username <username>
3. ip ftp password <password>
4. Copy the IOS file to FTP:
5. copy flash: ftp:

Restoring Cisco IOS Files

Restoring from TFTP

1. Verify connection with the TFTP server:
2. ping <TFTP-server-IP>
3. Copy the IOS file back to flash memory:
4. copy tftp: flash:
5. Specify **server IP and filename**.

Restoring from FTP

1. Copy the IOS file from the FTP server:
2. copy ftp: flash:
3. Verify the copied file using:
4. show flash:

Upgrading Cisco IOS Files

Why Upgrade Cisco IOS?

- **Enhances security** by patching vulnerabilities.
- **Adds new features** and improves performance.
- **Fixes bugs** and optimizes device operations.

Steps to Upgrade Cisco IOS

1. Verify Available Storage

- Check flash memory before upgrading:
- show flash:

2. Delete the Old IOS (If Necessary)

- If storage is low, remove the old file:
- delete flash:<old_ios_filename>

3. Transfer the New IOS to the Device

- Using **TFTP**:
- copy tftp: flash:
- Using **FTP**:
- copy ftp: flash:

4. Configure the Router to Boot from the New IOS

configure terminal

boot system flash:<new_ios_filename>

exit

write memory

reload

Verify the New IOS Version

- After reboot, check the installed version:
- show version

Recovering from a Corrupt or Missing IOS (less important)

What Causes IOS Corruption?

- **Power failure** during an upgrade.
- **Incomplete file transfer** of IOS.
- **Flash memory corruption** due to hardware issues.

Steps to Recover Cisco IOS in ROMmon Mode

1. **Check if Flash Memory has an IOS Image**
2. dir flash:
3. **Use TFTP to Download a New IOS**
    - Set network parameters:
    - set IP_ADDRESS=<router-ip>
    - set NETMASK=<subnet-mask>
    - set DEFAULT_GATEWAY=<gateway-ip>
    - Transfer IOS via **TFTP**:
    - tftpdnld
4. **Manually Boot the New IOS**
5. boot flash:<ios_filename>
6. **Set Permanent Boot Configuration**
7. configure terminal
8. boot system flash:<ios_filename>
9. exit
10. write memory

Verifying and Managing IOS Files

Checking Boot Settings

- Verify the current boot sequence:
- show boot

Verifying File Integrity

- Use **checksum verification** to ensure the IOS file is not corrupt:
- verify flash:<ios_filename>

Managing Multiple IOS Images

- List available IOS files:
- dir flash:
- Set a **backup boot option**:
- boot system flash:<backup_ios_filename>

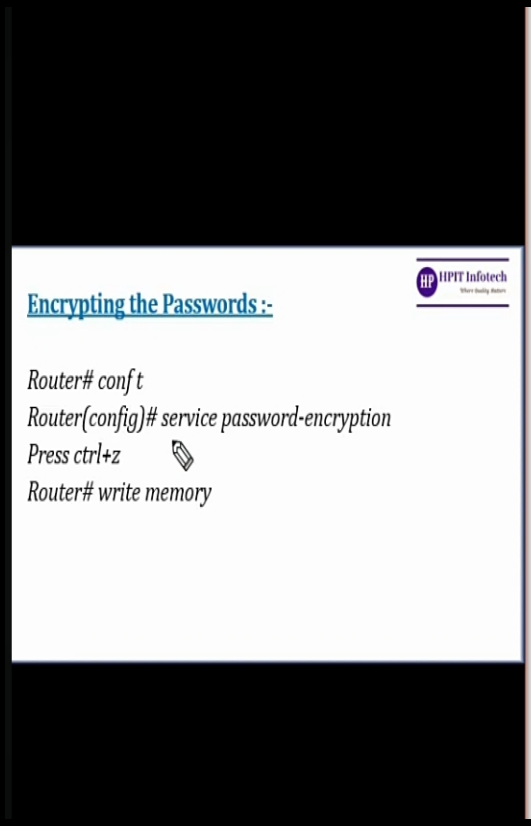
Summary of Cisco IOS File Management Commands

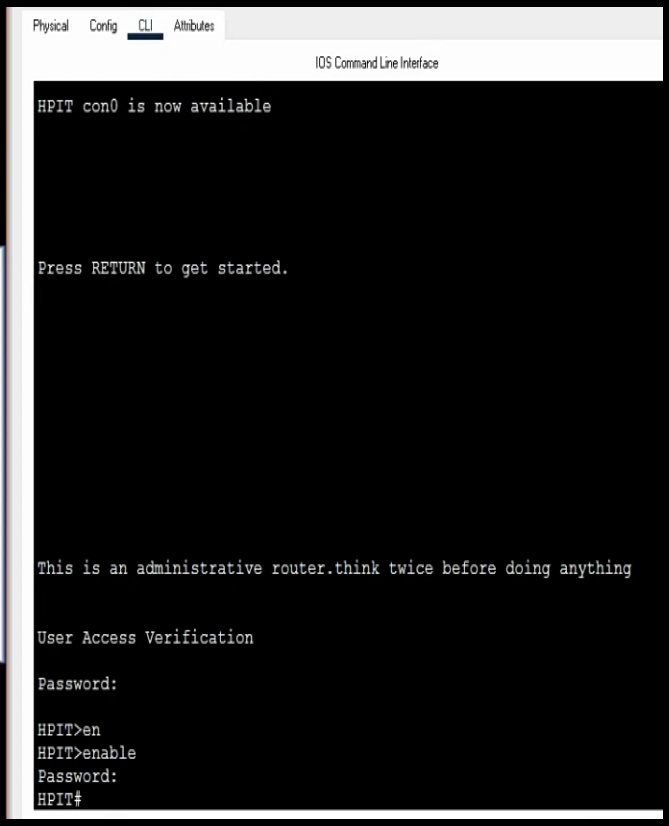
Task	Command
Check IOS version	show version
Check available flash storage	show flash:
Backup IOS to TFTP	copy flash: tftp:
Restore IOS from TFTP	copy tftp: flash:
Upgrade IOS using TFTP	copy tftp: flash:
Set IOS boot sequence	boot system flash:<ios_filename>

Task	Command
Delete an IOS file	delete flash:<ios_filename>
Recover IOS in ROMmon	tftpdnld
Verify IOS integrity	verify flash:<ios_filename>

Password Policies of Cisco Devices

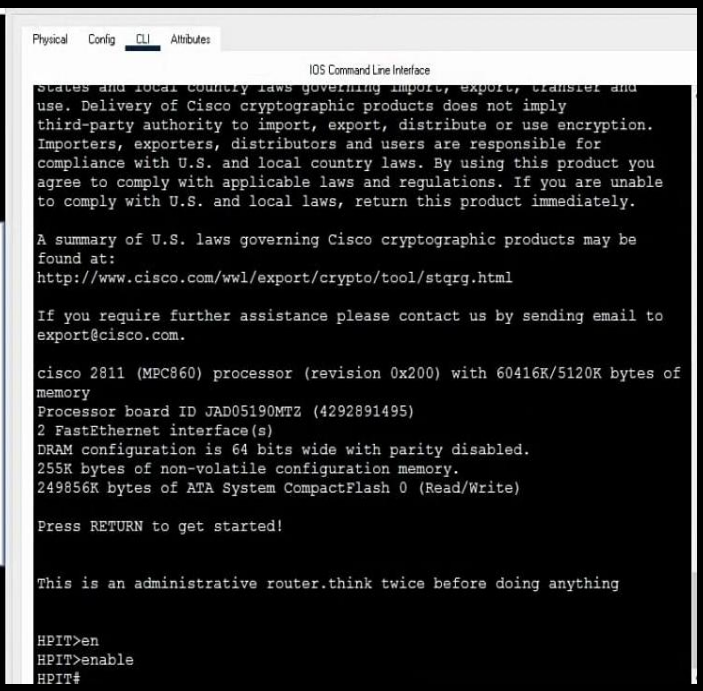
Security best practices recommend strong password policies for Cisco devices.





Setting a Line password
(user mode or login password):

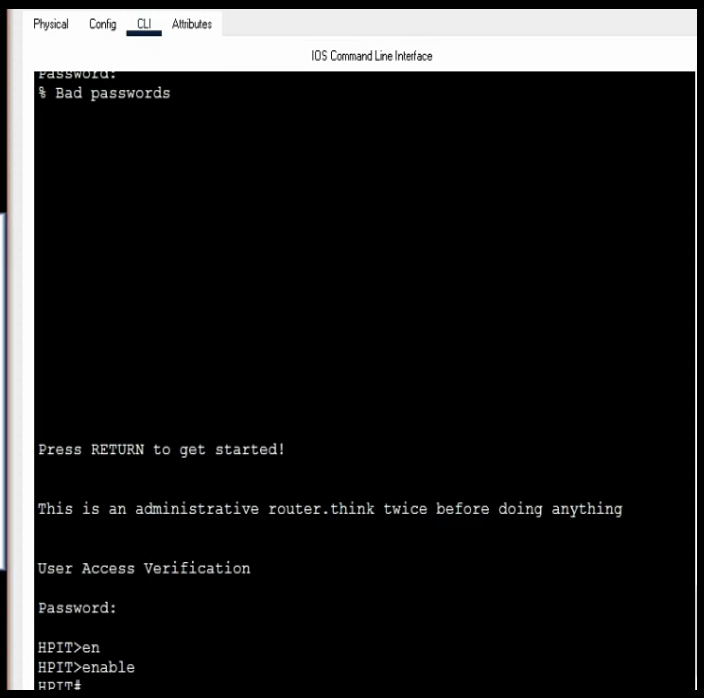
Router>enable
Router# conf t
Router(config)# line console 0
Router(config-line)#password hpit@123
Router(config-line)# login
Press ctrl+z
Router# write memory



Setting Privilege access password :

Router>enable
Router# conf t
Router(config)# enable password Cisco
OR
Router(config)# enable secret Cisco
Press ctrl+z
Router# write memory

Enable secret is secure because it shows password in encrypted form.



1. Setting a Password

Set passwords for different access levels:

Console Password

- Router(config)# line console 0
- Router(config-line)# password MySecret
- Router(config-line)# login

Enable Password

- Router(config)# enable password MySecret

Encrypted Enable Secret

- Router(config)# enable secret StrongSecret
- **Vty Password (for remote access)**
- Router(config)# line vty 0 4
- Router(config-line)# password RemoteSecret
- Router(config-line)# login

2. Encrypting Passwords

Prevent passwords from being displayed in clear text:

Router(config)# service password-encryption

Managing Administrative & Erasing Configuration: (less important)

Managing administrative tasks and erasing configurations are crucial for maintaining, troubleshooting, and securing network devices like routers and switches.

1. Manage Administrative Configurations

This refers to configuring, securing, and managing **Cisco network devices** to ensure proper operation and security. Some key aspects include:

a) Assigning Administrative Access

- Configuring **user privilege levels** (privilege exec level <level> <command>).
- Setting up **passwords for access control** (console, VTY, and enable passwords).
- Implementing **role-based access control (RBAC)** for security.
- Using **AAA (Authentication, Authorization, and Accounting)** for centralized login management.

b) Configuring Remote Access

- Enabling **SSH** (ip domain-name, crypto key generate rsa, transport input ssh).
- Configuring **Telnet (less secure)** for remote administration.

c) Saving and Backing Up Configurations

- **Saving configurations** to NVRAM:
- copy running-config startup-config
- **Backing up configurations** to an external server (TFTP/FTP):
- copy running-config tftp:
- **Restoring configurations** from backup:
- copy tftp: running-config

d) Managing Logs and System Monitoring

- **Viewing logs** (show logging).
- **Configuring syslog servers** for centralized logging (logging host <IP>).
- Setting **clock & NTP (Network Time Protocol)** for accurate timestamps (ntp server <IP>).

2. Erasing Configurations in Cisco Devices

This involves **removing existing configurations** from a Cisco router or switch when resetting the device, troubleshooting, or decommissioning it.

a) Erasing the Startup Configuration (Factory Reset)

This removes all saved configurations and reboots the device to its **default factory settings**:

erase startup-config

reload

b) Erasing the Running Configuration (Temporary Reset)

- Running configuration is stored in **RAM**, meaning changes are **not saved permanently**.
- To reset without rebooting:
- configure terminal
- default interface <interface-name>
- exit
- To reset the entire running configuration without rebooting:
- write erase
- reload

c) Clearing Specific Configurations

- **Clearing VLAN Database (on switches)**:
- delete flash:vlan.dat
- reload
- **Resetting a specific interface** to default settings:
- default interface GigabitEthernet0/1
- **Clearing routing configurations**:
- no ip route <destination> <subnet> <next-hop>

What is an IOS Image in Cisco Devices?

A **Cisco IOS (Internetwork Operating System) image** is the firmware or software that runs on Cisco networking devices such as routers, switches, and firewalls. It provides the operating system functionalities, including:

- **Routing & Switching** operations
- **Network Security** features
- **Device Management**
- **Advanced Networking Protocols**

Key Features of an IOS Image

1. **File Format:**
    - Typically, the image file has a **.bin** extension (binary format).
    - Example: c1900-universalk9-mz.SPA.157-3.M3.bin
2. **Storage Location:**
    - Stored in **Flash Memory** (flash: or bootflash:).
    - Can also be stored on a **TFTP Server** for upgrades.
3. **Execution:**
    - Loaded into **RAM** when the device boots up.
    - **Bootstrap program** (stored in ROM) finds and loads the IOS image.

Types of Cisco IOS Images

Cisco provides different types of IOS images depending on features and device models:

IOS Image Type	Description
universalk9	Supports all advanced features (Security, Routing, Switching). Requires a license.

IOS Image Type	Description
universalk9_npe	No Payload Encryption version (does not include cryptographic features like VPNs).
ipbase	Basic IP routing and switching features.
advancedipservices	Enhanced IP services, including MPLS and VPN support.
lanbase	For Layer 2 switching only (used in switches).
enterprise	Full-featured enterprise version with extensive routing and security.

Checking the Current IOS Image

To check which IOS image is running on a Cisco device, use:

show version

Example Output:

Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.4, RELEASE SOFTWARE (fc3)

System image file is "bootflash:isr4300-universalk9.16.06.04.SPA.bin"

- **IOS Version:** 16.6.4
- **Image Type:** universalk9
- **Location:** bootflash:

Where is the IOS Image Stored?

The IOS image is typically stored in **Flash Memory**. You can view available images with:

show flash:

or

dir flash:

Example output:

Directory of flash:/

1 -rw- 550114467 isr4300-universalk9.16.06.04.SPA.bin

This means the IOS image is present in the flash memory.

Upgrading or Replacing an IOS Image

If you need to **upgrade** or **replace** an IOS image, you can do it using:

- **TFTP Server**
- **USB Drive**
- **SCP/FTP Transfer**

Example command to copy an IOS image from a TFTP server:

copy tftp://192.168.1.100/isr4300-universalk9.16.06.04.SPA.bin flash:

To set the new image as the boot file:

conf t

boot system flash:isr4300-universalk9.16.06.04.SPA.bin

exit

write memory

reload