Chapter 2 Configure a Network Operating System

Jose Noe Vazquez Gutierrez

1. Network Operating System

The OS on home routers is usually called **firmware**. The most common method for configuring a home router is by using a web browser-based GUI

The Cisco Internetwork Operating System (**Cisco IOS**) is a generic term for the collection of network operating systems used by Cisco networking devices.

It enables device hardware to function and provides an interface for users to interact

Computer-based network devices use an operating system called a *network operating system.*

2. Operating Systems

Kernel: The portion of the OS that communicates between HW and SW of a computer and manages how resources are used to meet SW requirements

Hardware: The physical part of a computer including underlying electronics

Shell: The user interface that allows users to request specific task, **CLI** (command line interface) or **GUI** (graphical user interface)

3. Access Methods

There are several ways to access the CLI environment and configure the device.

Telnet: Used for remote management without a securely encrypted connection, data is sent in plaintext

SSH: Used for remote management, this method provides password encrypted authentication and transport of session data, this keeps the user ID, pass, and details of the management session private

Console: Used for an initial configuration and maintenance purposes only (out-of-band access), by connecting a special cable (rollover or console cable) to the console port

AUX port: a legacy auxiliary port that was used to establish a CLI session remotely using a modem (out-of-band).

4. Terminal Emulation Programs

Putty, Tera Term, SecureCRT, OS X Terminal

These programs allow you to enhance your productivity by adjusting window sizes, changing font sizes, and changing color schemes.

5. Cisco IOS Command Modes of Operation

As a security feature, the Cisco IOS software separates **management access**

Privileged Exec Mode: Allows access to all the commands and features. To access this mode you need to type the *enable* command in the User exec Mode. prompt: hostName#

User Exec Mode: Allows access to only a limited number of basic monitoring commands, it is a view-only mode. prompt: hostName>

6. Configuration Command Modes

To configure the device, the user must enter Global Configuration Mode (**Global Config Mode**). To access this mode you need to type the *configure terminal* command in the Privileged exec Mode. prompt: hostName**(config)#**

From this mode you can enter to different sub-configuration modes.

Interface Configuration Mode - Used to configure a switch port or router network interface. default prompt: hostName(config-if)#.

Line Configuration Mode - Used to configure console, SSH, Telnet, or AUX access. default prompt: hostName(config-line)#

7. Navigate Between IOS Modes

Press **exit** to return to the previous command mode.
end or **ctrl+z** to return to the privileged exec mode from any other mode.
enable from the user exec mode to enter to the privileged exec mode.
disable from the privileged exec mode to return to the user exec mode.

8. IOS command structure

Keyword: a specific parameter defined in the operating system
Argument: not predefined; a value or variable defined by the user

prompt **--command--keyword/argument**
Switch>show ip protocols
Switch>ping 192.168.10.5

9. IOS command Syntax

Boldface: Commands and keywords
Italics: arguments
[an optional element**]**
{a required element**}**
[x {y | z}] a required choice within an optional element

10. IOS help features

Context-Sensitive Help

To access context-sensitive help, simply enter a question mark, **?**, at the CLI.

- Enables you to quickly find which commands are available in each command mode
- Which commands start with specific characters or group of characters
- Which arguments and keywords are available to particular commands

Command Syntax Check

It verifies that a valid command was entered by the user, and it will provide feedback describing what is wrong with the command.

11. Hotkeys

CLI Line Editing

tab: completes a partial command entry
backspace: erases the character to the left of the cursor
Ctrl+D: erases the character right to the cursor
Ctr+E: Moves the cursor to the end of the command line
Ctr+A: Moves the cursor to the beginning of line

At the "----More----" prompt

Enter key: Display the next line
Space bar: Display the next screen
Any key: Ends the display string, returning to privileged exec

Break keys

Ctrl+C: Ends the configuration mode and returns to the privileged exec mode. When in setup mode, aborts back to the command prompt
Ctrl+Shift+6: All-purpose break sequence. use to abort DNS lookups, traceroutes, pings, etc.
Ctrl+Z=end

12. Basic device configuration

Address Schemes

IP Addresses

Use the **S1(config)#no ip domain-lookup** command to prevent unwanted DNS lookup on a switch

The **ping** command can be used to test connectivity to another device on the network or a website on the Internet. C:\ping x.x.x.x

They enable devices to locate one another and establish end-to-end communication on the Internet.

The structure of an IPv4 address is called **dotted decimal notation** and is represented by four decimal numbers between 0 and 255.

With the IPv4 address, a **subnet mask** is also necessary. An IPv4 subnet mask is a 32-bit value that separates the network portion of the address from the host portion.

The **default gateway** address is the IP address of the router that the host will use to access remote networks, including the Internet.

Interfaces and ports

Cisco IOS Layer 2 switches have physical ports for devices to connect.

These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (**SVIs**).

These are virtual interfaces because there is no physical hardware on the device associated with it. An SVI is created in software.

An SVI provides a means to **remotely manage a switch** over a network using IPv4.

The **default** SVI is interface **VLAN1**.

SVI Configuration:
• Switch(config)#**interface vlan 1**
• Switch(config-if)# **ip address** *x.x.x.x z.z.z.z* //ip and mask
• Switch(config-if)# **no shutdow** //this's 'cause the vlan1 is not activated by default

⚠ With this configuration, any device **CONNECTED** to a port on the switch will have **connection** (ping) with this Switch.

To have **access** to the switch CLI, we need configure a line VTY to allow Telnet acces, and set the privileged exec password, after doing this we can use:

C:\telnet ip_address_of_the_SVI
on the CMD of a windows PC

If we want to **access to the switch from another network** we need to add a default gateway:
Switch(config)#ip default-gateway x.x.x.x

Use **show running-config** to see how the configuration has been added.
And **show ip interface brief** to see the condition of the switch interfaces.

When configuring a vlan different from the number 1, use:
Switch(config)#*vlan number_of_the_vlan*
With this, we add the vlan to the vlan data base

then, use:
Switch(config)#interface vlan *number_of_the_vlan*
to configure it

use Switch#**show vlan brief** to see the vlan database

Dynamic Host Configuration Protocol (DHCP)

The **DNS** server addresses are the IPv4 addresses of the Domain Name System (DNS) servers, which are used to translate IP addresses to domain names

IP address information can be entered into end devices *manually*, or using a protocol to do this (DHCP)

It is possible to display the IP configuration settings on a Windows PC by using the **ipconfig**

To manually configure an IPv4 address on a Windows host:
• Open the Control Panel >
• Network and Internet > Network Sharing Center >
• Change adapter settings and choose the adapter
• Right-click and select Properties
• Highlight Internet Protocol Version 4 (TCP/IPv4) and click Properties

Save the Running Configuration File

Use the **reload** command in the privileged EXEC mode to restore the startup-config.

Use the **erase startup-config** command to erase the startup configuration file, and **reload** the device

Switch# **copy running-config startup-config**
or: Switch#write

startup-config - The file stored in Non-volatile Random Access Memory (**NVRAM**) that contains all of the commands that will be used by the device upon startup or reboot.

running-config - The file stored in Random Access Memory (**RAM**) that reflects the current configuration.

View the running configuration file.
Switch#**show running-config**

View the startup configuration file.
Switch#**show startup -config**

Device name (hostname)

It is useful to identify a device (e.g. for a remote session)

Hostname should:
• Start with a letter
• Contain NO spaces
• End with a letter or a digit
• Uses only letter, digits and dashes
• Be less than 64 characters length

Switch>enable
Switch#configure terminal
Switch(config)#**hostname** Sw-Floor-1
Sw-Floor-1(config)#

Use **no hostname** at global configuration mode to remove the configured hostname and return the switch to the default prompt,

Banner Messages

It is a method for declaring that only authorized personnel should attempt to gain entry into the device.

Banner Message Of The Day (MOTD):
Switch(config)# **banner motd** #*my message*#

This message will be displayed on all subsequent attempts to access the device until the banner is removed.

Secure Device Access

Virtual terminal (**VTY**) lines enable remote access to the device.

• **privileged EXEC**: Switch(config)# enable secret *yourpassword*

When choosing a password:
• Use more that 8 characters
• Use a combination of upper and lowercase letters, numbers, special characters, and/or numbers
• Avoid using the same password for all devices
• Don't use common words

• **user EXEC**:
-----Switch(config)#line console 0
-----Switch(config-line)#password *yourpassword*
-----Switch(config-line)#login

• **remote access**:
-----Switch(config)#line vty 0 15
-----Switch(config-line)#password *yourpassword*
-----Switch(config-line)#login

Encrypt Passwords

Thi command applies weak encryption to all unencrypted passwords:
Switch(config)#**service password-encryption**
This encryption applies only to passwords in the configuration file.

Use the **show running-config** command within the user exec, to verify that passwords are now encrypted.