

Cisco IOS Access

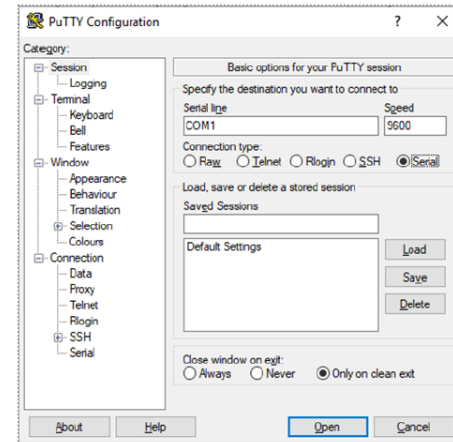
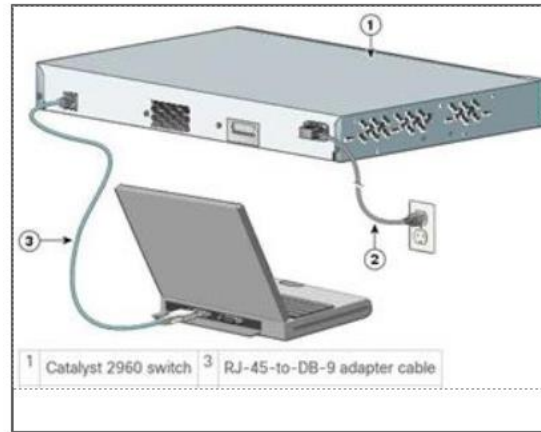
Operating system of the Cisco network devices

Cisco IOS Access

Access Methods

How to manage network device - how we can use operating system of the network device?

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- Console cable, computer and terminal emulation program needed



Cisco IOS Access

Access Methods

It is also possible to manage device using remote connections. There is two different methods to do that.

- **Secure Shell (SSH)** – Establishes a secure remote connection to a device, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

a network connection that is working properly is required

IOS Navigation

Primary Command Modes

User EXEC Mode:

- The mode where you first go when you connect to the device
- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>
```

```
Switch>
```

Privileged EXEC Mode:

- To this mode you can go using *enable* command
- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#
```

```
Switch#
```

Configuration Mode and Subconfiguration Modes

Global Configuration Mode:

- Used to access configuration options on the device
- To this mode you can go using *configure terminal* command in privileged mode

```
Switch(config) #
```

Line Configuration Mode:

- Used to configure console, SSH or Telnet access
- To enter these modes, use the different line commands in configure mode

```
Switch(config-line) #
```

Interface Configuration Mode:

- Used to configure a switch port or router interface
- To enter these modes, use the different interface commands in configure mode

```
Switch(config-if) #
```

Navigation Between IOS Modes

Privileged EXEC Mode:

- To move from user EXEC mode to privilege EXEC mode, use the **enable** command.

```
Switch> enable  
Switch#
```

Global Configuration Mode:

- To move in and out of global configuration mode, use the **configure terminal** command. To return to privilege mode, use the **exit** command.

```
Switch(config)#  
Switch(config)#exit  
Switch#
```

Line Configuration Mode:

- To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

```
Switch(config)#line console 0  
Switch(config-line)#exit  
Switch(config)#
```

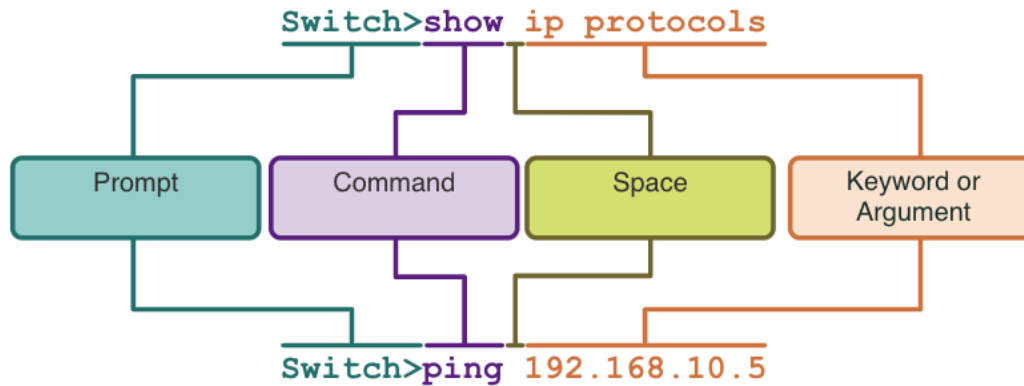
IOS Videos

There is a videos in Cisco Module 2 where you can learn more about

- *User EXEC mode*
- *Privilege EXEC mode*
- *Global Config mode*
- *Navigation Between IOS Modes*
 - enable
 - disable
 - configure terminal
 - exit
 - end
 - Control + Z on keyboard
 - Other commands to enter sub configuration modes

The Command Structure

Basic IOS Command Structure



- **Keyword** – This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
- **Argument** - This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5**).

Notice that all command can not give on all modes

The Command Structure

IOS Help Features

The IOS has two forms of help available: context-sensitive help and command syntax check.

- Context-sensitive help enables you to quickly find answers to these questions:
 - 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 verifies that a valid command was entered by the user.
 - If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Router#ping ?
WORD  Ping destination address or hostname
ip     IP echo
ipv6   IPv6 echo
```

```
Switch#interface fastEthernet 0/1
                        ^
% Invalid input detected at '^' marker.
```

Hot Keys and Shortcuts

- The IOS CLI provides hot keys and shortcuts that make configuring, monitoring, and troubleshooting easier.
- Commands and keywords can be shortened to the minimum number of characters that identify a unique selection. For example, the **configure** command can be shortened to **conf** because **configure** is the only command that begins with **conf**.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

The Command Structure

Hot Keys and Shortcuts (Cont.)

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Left Arrow	Moves the cursor one character to the left.
Right Arrow	Moves the cursor one character to the right.
Up Arrow or Ctrl+P	Recalls the commands in the history buffer, beginning with the most recent commands.

Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.

Videos – Context Sensitive, Command Syntax Checker, Hot Keys and Shortcuts

These videos will cover the following:

- Use the help command in user EXEC, privileged EXEC, and global config mode
- Finish commands and arguments with the help command
- Use the command syntax checker to fix syntax errors and incomplete commands
- Tab key (tab completion)
- Command shortening
- Up and down arrow key
- CTRL + C
- CTRL + Z
- CTRL + Shift + 6

Basic Device Configuration

Basic Device Configuration

Device Names

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."
- Guideline for naming devices:
 - Start with a letter
 - Contain no spaces
 - End with a letter or digit
 - Use only letters, digits, and dashes
 - Be less than 64 characters in length

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Note: To return the switch to the default prompt, use the **no hostname** global config command.

Configure Passwords

Multiple passwords must be set on a Cisco switch

Securing user EXEC mode access: (“console password”)

- First enter line console configuration mode using the **line console 0** command in global configuration mode.
- Next, specify the user EXEC mode password using the **password** *password* command.
- Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access: (“enable password”)

- First enter global configuration mode.
- Next, use the **enable secret** *password* command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Securing VTY line access: (“telnet password”)

- First enter line VTY configuration mode using the **line vty 0 15** command in global configuration mode.
- Next, specify the VTY password using the **password** *password* command.
- Finally, enable VTY access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Password Guidelines

- The use of weak or easily guessed passwords are a security concern.
- Password Guidelines:
 - Use passwords that are more than eight characters in length. The longer the better
 - Use a combination of upper and lowercase letters, numbers, special characters, and numeric sequences.
 - Avoid using the same password for all devices.
 - Do not use common words because they are easily guessed.



Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments.

Basic Device Configuration

Encrypt Passwords

- If you want passwords to be hidden in configuration files, use the command below
- To encrypt all plaintext passwords, use the **service password-encryption** global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Video – Secure Administrative Access to a Switch

This video will cover the following:

- Access the command line to secure the switch
- Secure access to the console port
- Secure virtual terminal access for remote access
- Encrypt passwords on the switch
- Configure the banner message
- Verify security changes

Configuring the switch IP address & Save Configurations

Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the SVI.

To configure an SVI on a switch:

- Enter the **interface vlan 1** command in global configuration mode.
- Next assign an IPv4 address using the **ip address** *ip-address subnet-mask command*.
- Finally, enable the virtual interface using the **no shutdown** command.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Save Configurations

Configuration Files

- There are two system files that store the device configuration:
 - **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the configurations that will be used by the device upon startup or reboot. Does not lose its contents when the device is powered off.
 - **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. It loses all of its content when the device is powered off or restarted.
 - To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

