**Lab**

**Configuring a Network Operating System.**

1. **Access method**

* **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
* **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
* **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

Can be accessed through **Terminal Emulation Program** such as PuTTY, Tera Term and SecureCRT.

****

****

1. **IOS Navigation**
2. Primary command mode

* User EXEC mode

Allow access to only limited number of basic monitoring commands.

Identified by > symbol.

* Privileged EXEC mode

Allows access to all commands and features

Identified by # symbol.

**Command: enable**

1. Configuration and sub-configuration modes

* Global configuration mode

Used to access configuration options on the device

**Command: configure terminal**

* Line configuration mode

Used to configure console, SSH and Telnet access.

**Command: line *console 0***

*Line (followed by the management line type)*

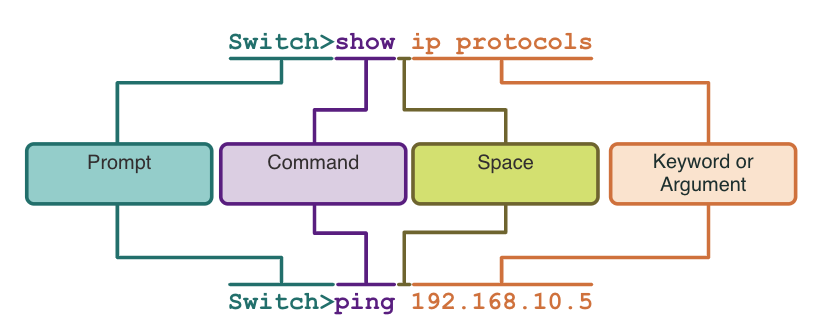
* Interface configuration mode

Used to configure a switch port or router interface

**Command: Interface *fa0/1***

*Interface (followed by the interface or port type)*

1. Basic 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). e.g. show history, show interfaces

1. **IOS help features**

* **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?

**Example command: ping ?**

* **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.

1. **Hotkeys & 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**.
* Some of the hotkeys:

|  |  |
| --- | --- |
| **Keystroke** | **Description** |
| **Tab** | Completes a partial command name entry. |
| **Backspace** | Erases the character to the left of the cursor. |
| **Left Arrow** or**Ctrl+B** | Moves the cursor one character to the left. |
| **Right Arrow** or**Ctrl+F** | 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. |

1. **Basic Device Configuration**
2. Set unique hostname

Guidelines

* 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

*(in global configuration mode)*

**Command: hostname Sw-Level-3**

1. Set password

To secure **user EXEC mode**.

*(in line console configuration mode)*

**Command:**

**line console 0**

**password cisco**

**login**

**end**

To secure **privileged EXEC mode**.

*(in global configuration mode)*

**Command:**

**enable secret class**

**exit**

To secure VTY line access.

Note: VTY lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

*(in global configuration mode)*

**Command:**

**line vty 0 15**

**password cisco**

**login**

**end**

1. Encrypt password

* The startup-config and running-config files display most passwords in plaintext.
* To encrypt all plaintext passwords, use the **service password-encryption** global config command.
* Use the **show running-config** privileged EXEC modecommand to verify that the passwords on the device are now encrypted.

*(in global configuration mode)*

**Command:**

**service password-encryption**

**exit**

1. Set banner messages

* A banner message is important to warn unauthorized personnel from attempting to access the device.
* To create a banner message of the day on a network device, use the banner **motd # the message of the day #** global config command.

*(in global configuration mode)*

**Command:**

**banner motd #Authorized Access Only!#**

1. **Save configuration**

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 commands that will be used by the device upon startup or reboot. Flash 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. RAM is volatile memory. 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.

*(in privileged EXEC mode)*

**Command:**

**copy running-config startup-config**

1. **Ports & Addresses – (facts)**

* The use of IP addresses is **the primary means of enabling 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**.
* An **IPv4 subnet mask is a 32-bit value** that **differentiates the network portion** of the address from the **host portion**. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.
* The **default gateway address** is the **IP address of the router** that the host will use to **access remote networks**, including **the internet**.
* Interfaces & Ports - Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.



1. **Configure IP addressing**

Can be configure **manually or automatically (DHCP)**

\*\* 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.

*(in global configuration mode)*

**Command:**

**interface vlan 1**

**ip address 192.168.1.10 255.255.255.0**

**no shutdown**

**\*\* To verify your connectivity: PING - PDU**

**Lab:**

**2.3.7 - Packet Tracer - Navigating the IOS (PKA files)**

**2.5.5 - Packet Tracer - Configuring Initial Switch Settings (PKA files)**

**2.7.6 - Packet Tracer - Implementing Basic Connectivity (PKA files)**

**Instruction**

1. **Download the three PKA files from teams -> Lab Materials – Lab 2 folder**
2. **Complete user profile (figure 1)**

\*\* Additional info: your tp number



Figure 1

After that click **ok**. You will be prompted with text box – change the user info & reset the activity – click **yes**

1. **Run the tutorial by following instruction in PT Activity window.**
2. **Check Result**

Once you finished will the tutorial on PT Activity window click **“Check Result”** (figure 2) and then save and submit it.

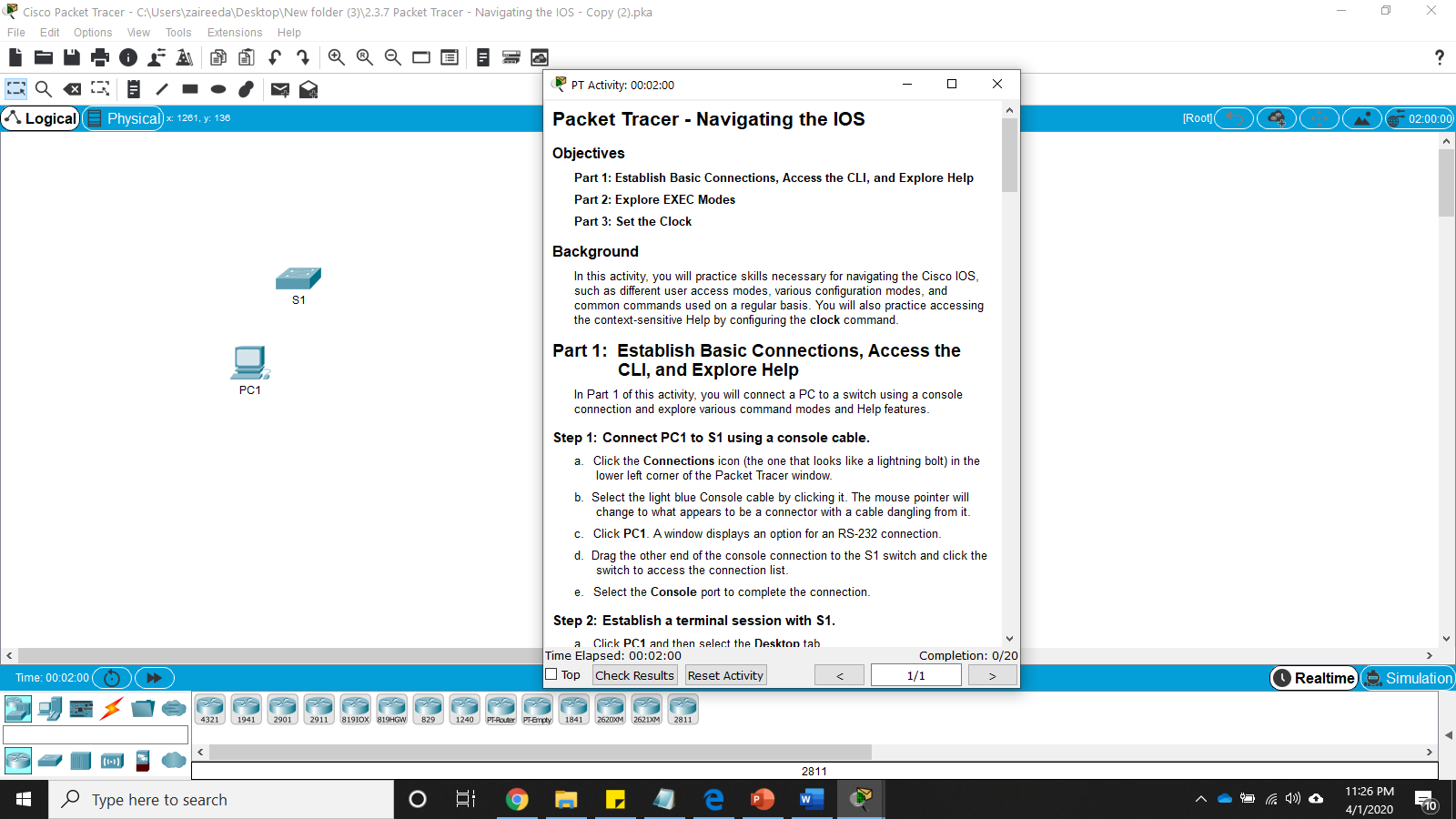


Figure 2

1. **Prove of lab work:**

Submit your lab works through teams -> **Lab 2 submission** folder