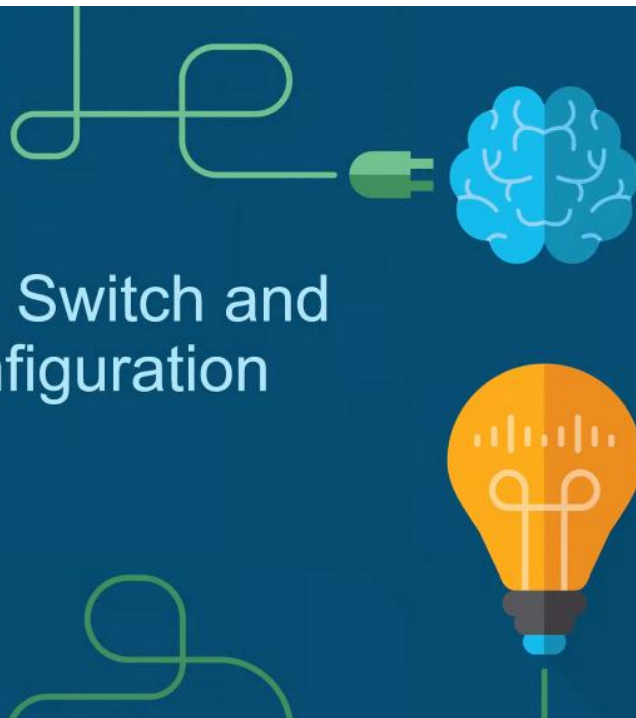




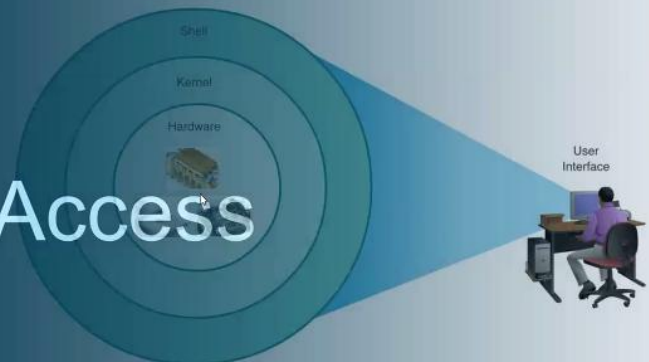
Module 2: Basic Switch and End Device Configuration

Instructor Materials

Introduction to Networks v7.0
(ITN)

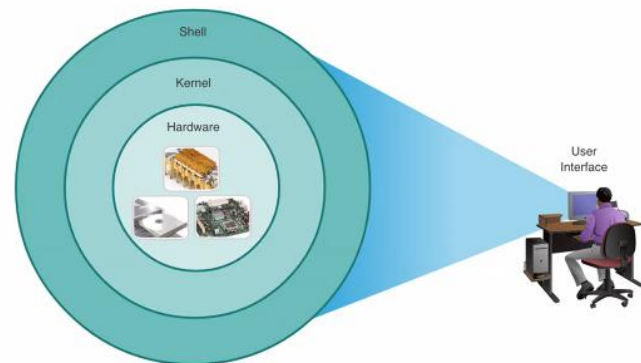


2.1 Cisco IOS Access



Operating Systems

- **Shell** - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
- **Kernel** - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- **Hardware** - The physical part of a computer including underlying electronics.



GUI

- A GUI allows the user to interact with the system using an environment of graphical icons, menus, and windows.
- A GUI is more user-friendly and requires less knowledge of the underlying command structure that controls the system.
- Examples of these are: Windows, macOS, Linux KDE, Apple iOS and Android.
- GUIs can fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI.



Purpose of an OS

PC operating system enables a user to do the following:

- Use a mouse to make selections and run programs
- Enter text and text-based commands



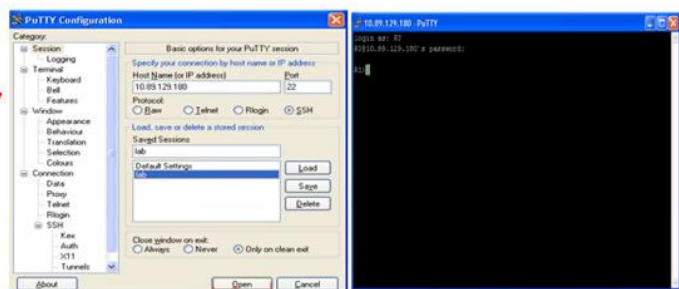
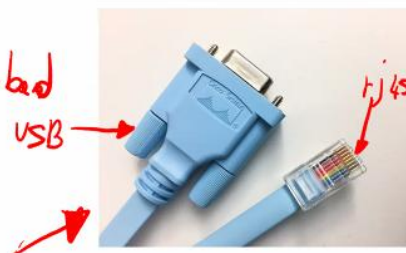
CLI-based network operating system enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs
- Use a keyboard to enter text and text-based commands
- View output on a monitor

```
analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive
[analyst@secOps ~]$
```

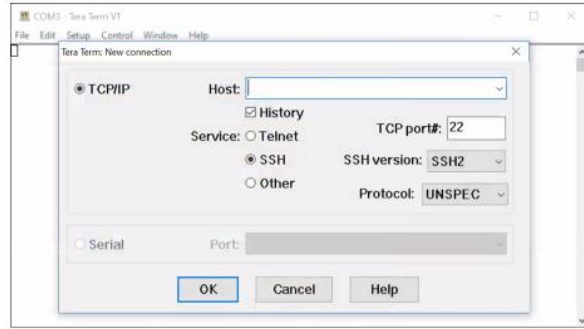
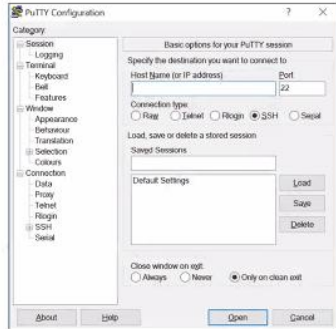
Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations. *-sick*
- **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.) *out-of-band*
- **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.) *tj4s*



Terminal Emulation Programs

- Terminal emulation programs are used to connect to a network device by either a console port or by an SSH/Telnet connection.
- There are several terminal emulation programs to choose from such as PuTTY, Tera Term and SecureCRT.



IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands *num limitato di comandi di stato del dispositivo*
- Identified by the CLI prompt that ends with the > symbol

```
Router>
Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features *posso dare tutti i comandi di monitoring (status)*
- Identified by the CLI prompt that ends with the # symbol

```
Router#
Switch#
```

interfaccia mode

Configuration Mode and Subconfiguration Modes

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

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

Interface Configuration Mode:

- Used to configure a switch port or router interface

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



Per interrompere un comando dentro alla CLI del router/switch: **ctrl+shift+6**

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 EXEC 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)#
```



Navigation Between IOS Modes (Cont.)

Subconfiguration Modes:

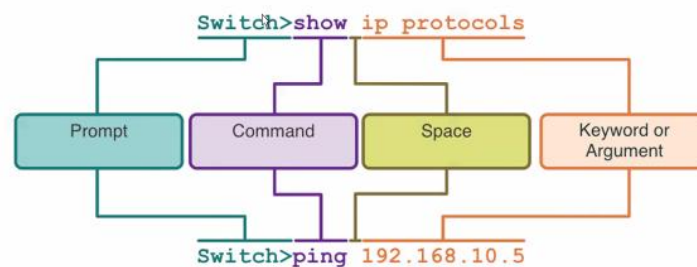
- To move out of any subconfiguration mode to get back to global configuration mode, use the **exit** command. To return to privilege EXEC mode, use the **end** command or key combination **Ctrl +Z**.
- To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from **(config-line)#** to **(config-if)#**.

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

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

2.3 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**).

Hot Keys and Shortcuts (Cont.)

- When a command output produces more text than can be displayed in a terminal window, the IOS will display a “**--More--**” prompt. The table below describes the keystrokes that can be used when this prompt is displayed.
- The table below lists commands that can be used to exit out of an operation.

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.

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.

Note: To see more hot keys and shortcuts refer to 2.3.5.

Basic Device Configuration

Configure Passwords

Securing user EXEC mode access:

- 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:

- 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#
```



Basic Device Configuration

Configure Passwords (Cont.)

Securing VTY line access:

- 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#
```

- 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.



Basic Device Configuration

Encrypt Passwords

- 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** command to verify that the passwords on the device are now encrypted.

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

```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```



COMANDI UTILI:

- PASSWORD line console -> se ci colleghiamo con cavo
- PASSWORD enable secret -> per accedere ai privilegi del device
- PASSWORD vty -> password per accedere con SSH o Telnet (vty)
- USER
 - Enable
- PRIVILEGE
 - running-config
- GLOBAL
 - line console 0
 - line vty 0 15
 - interface f0/1

 - hostname S1
 - service password-encryption
- LINE
 - Password
 - Login
- INTERFACE

Basic Device Configuration

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.

Note: The “#” in the command syntax is called the delimiting character. It is entered before and after the message.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

The banner will be displayed on attempts to access the device.

Press RETURN to get started.

Authorized Access Only!

User Access Verification

Password:

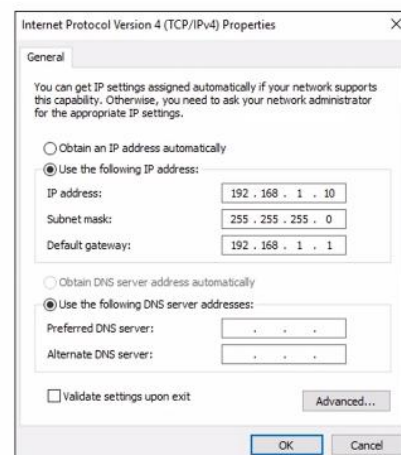


© 2019, 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 47

Ports and Addresses

IP Addresses

- 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.



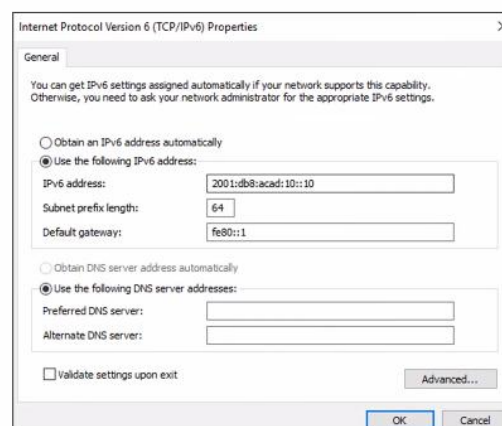
© 2019, 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 48

Ports and Addresses

IP Addresses (Cont.)

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon ":".
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

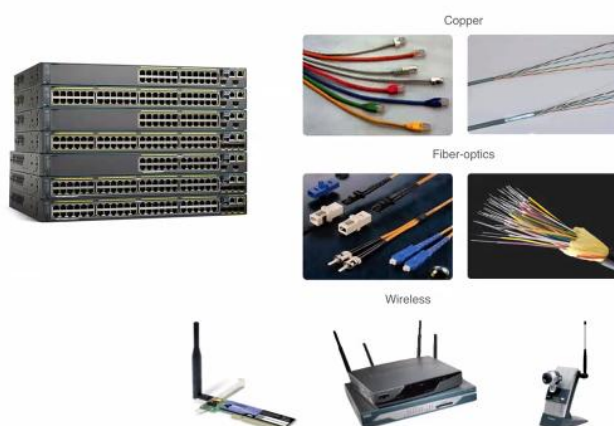
Note: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.



Ports and Addresses

Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits. Some of the differences between various types of media include:
 - Distance the media can successfully carry a signal
 - Environment in which the media is to be installed
 - Amount of data and the speed at which it must be transmitted
 - Cost of the media and installation



2.7 Configure IP Addressing



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 60

Configure IP Addressing

Manual IP Address Configuration for End Devices

- End devices on the network need an IP address in order to communicate with other devices on the network.
- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).
- To manually configure an IPv4 address on a Windows PC, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the **Local Area Connection Properties**.
- Next, click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window. Then configure the IPv4 address and subnet mask information, and default gateway.



Note: IPv6 addressing and configuration options are similar to IPv4.



© 2019, 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 61

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
```



Per salvare la configurazione del dispositivo:

- enable -> password -> configure terminal
- **copy running-config startup-config** (salva la configurazione attuale nella configurazione di avvio, così al riavvio riparte con la configurazione aggiornata)

Per mostrare lo stato del dispositivo:

- **show running-config** (mostra configurazione attuale, modificata in live)
- **show startup-config** (mostra configurazione salvata in memoria, può differire dalla running-config)