Lab-1

Operating System

OS Shell

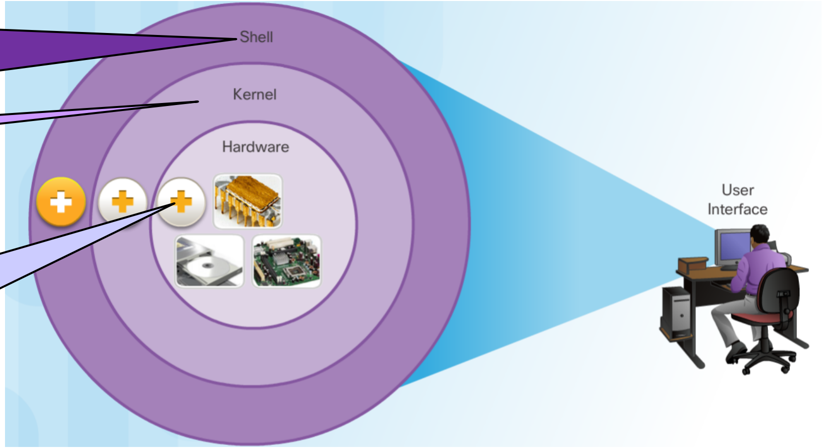
- The OS shell is either a command-line interface (CLI) or a graphical user interface (GUI) and enables a user to interface with applications.

OS Kernel

- The OS kernel communicates directly with the hardware and manages how hardware resources are used to meet software requirements.

Hardware

- The physical part of a computer including underlying electronics.



Purpose of OS

- **Using a GUI enables a user to:**
  - Use a mouse to make selections and run programs
  - Enter text and text-based commands

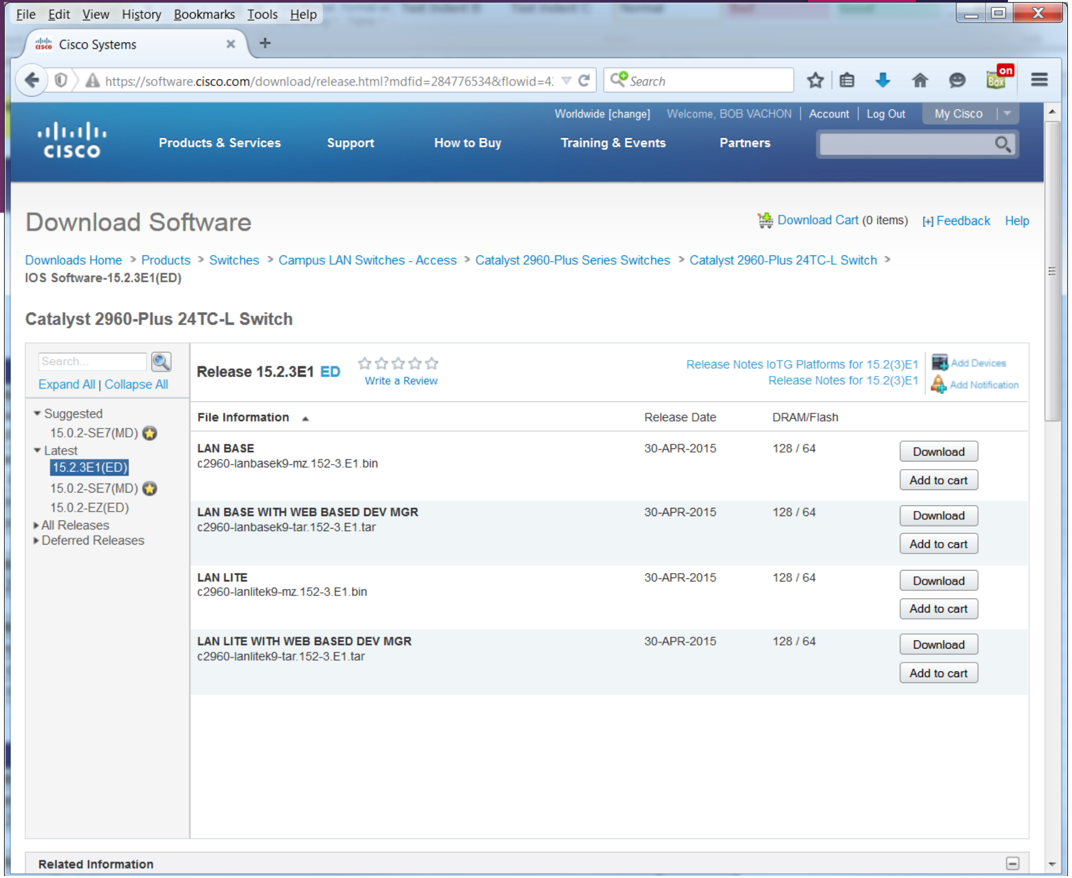
- **Using a CLI on a Cisco IOS switch or router enables a network technician to:**
  - Use a keyboard to run CLI-based network programs
  - Use a keyboard to enter text and text-based commands

- **There are many distinct variations of Cisco IOS:**
  - IOS for switches, routers, and other Cisco networking devices
  - IOS numbered versions for a given Cisco networking devices

Purpose of OS (Cont.)

- All devices come with a default IOS and feature set. It is possible to upgrade the IOS version or feature set.
- An IOS can be downloaded from cisco.com. However, a Cisco Connection Online (CCO) account is required.

Note: The focus of this course will be on Cisco IOS Release 15.x.



Download Software

Download Cart (0 items) [+] Feedback Help

Downloads Home > Products > Switches > Campus LAN Switches - Access > Catalyst 2960-Plus Series Switches > Catalyst 2960-Plus 24TC-L Switch >
IOS Software-15.2.3E1(ED)

Catalyst 2960-Plus 24TC-L Switch

Release 15.2.3E1 ED

Release Notes IoTG Platforms for 15.2(3)E1
Release Notes for 15.2(3)E1

File Information	Release Date	DRAM/Flash	
LAN BASE c2960-lanbasek9-mz.152-3.E1.bin	30-APR-2015	128 / 64	Download Add to cart
LAN BASE WITH WEB BASED DEV MGR c2960-lanbasek9-tar.152-3.E1.tar	30-APR-2015	128 / 64	Download Add to cart
LAN LITE c2960-lanlitek9-mz.152-3.E1.bin	30-APR-2015	128 / 64	Download Add to cart
LAN LITE WITH WEB BASED DEV MGR c2960-lanlitek9-tar.152-3.E1.tar	30-APR-2015	128 / 64	Download Add to cart

Related Information

Access Methods

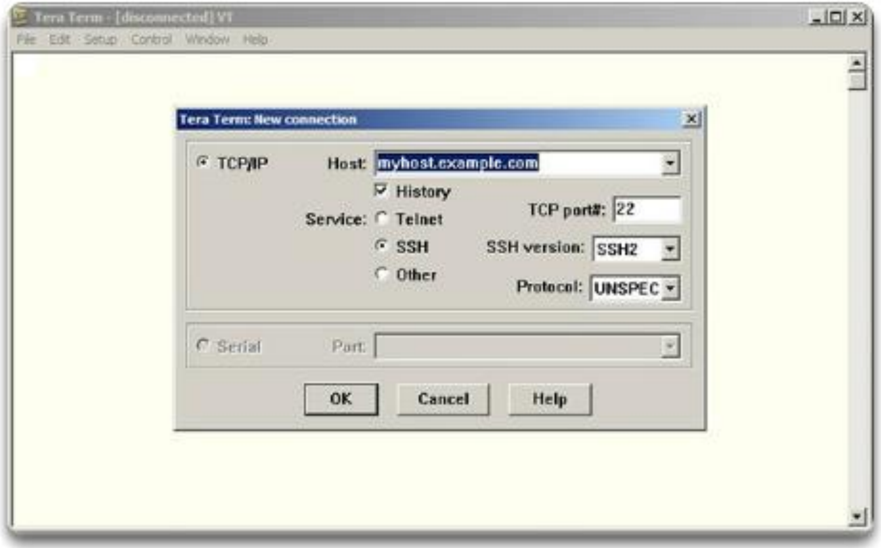
- The three most common ways to access the IOS are:
  - **Console port –** Out-of-band serial port used primarily for management purposes such as the initial configuration of the router.
  - **Secure Shell (SSH) -** Inband method for remotely and securely establishing a CLI session over a network. User authentication, passwords, and commands sent over the network are encrypted. As a best practice, use SSH instead of Telnet whenever possible.
  - **Telnet** – Inband interfaces remotely establishing a CLI session through a virtual interface, over a network. User authentication, passwords, and commands are sent over the network in plaintext.

Note: The AUX port is an on older method of establishing a CLI session remotely via a telephone dialup connection using a modem.

Terminal Emulation Program

- Regardless of access method, a terminal emulation program will be required. Popular terminal emulation programs include PuTTY, Tera Term, SecureCRT, and OS X Terminal.

Tera Term


Tera Term - [disconnected] VT
File Edit Setup Control Window Help
Tera Term: New connection
OK
Cancel
Help

● TCP/IP Host: myhost.example.com

☑ History

Service: ○ Telnet ● SSH ○ Other

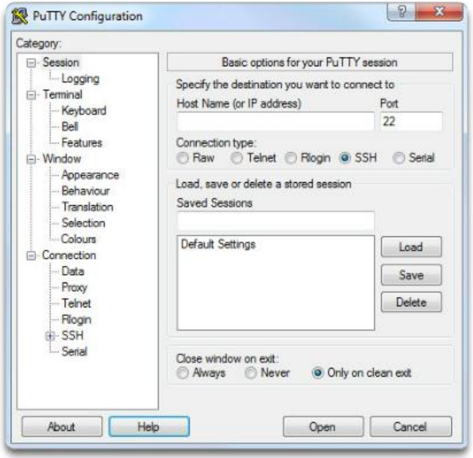
TCP port#: 22

SSH version: SSH2

Protocol: UNSPEC

○ Serial Port:

PuTTY



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

22

Connection type:

○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

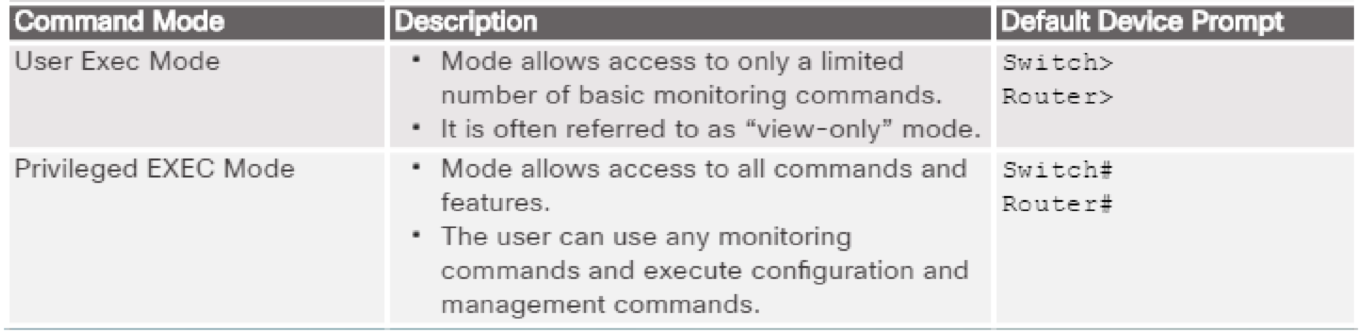
Saved Sessions

Default Settings

Close window on exit:

○ Always ○ Never ● Only on clean exit

Primary Command Modes



Command Mode	Description	Default Device Prompt

User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands.
	• It is often referred to as "view-only" mode.
		`Switch>`
		`Router>`

Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

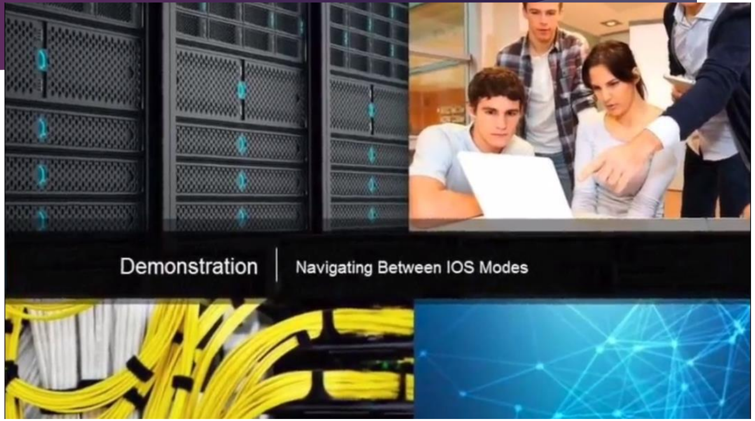
Configuration Command Modes

- The primary configuration mode is called **global configuration** or simply, **global config**.
  - Use the **configure terminal** command to access.
  - Changes made affect the operation of the device.

- Specific sub configuration modes can be accessed from global configuration mode. Each of these modes allows the configuration of a particular part or function of the IOS device.
  - **Interface mode** - to configure one of the network interfaces.
  - **Line mode** - to configure the console, AUX, Telnet, or SSH access.

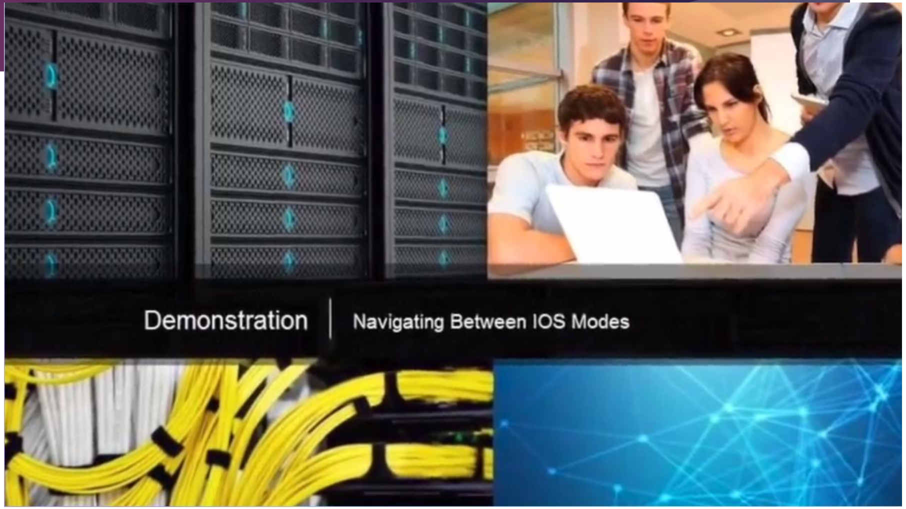
Navigate Between IOS Modes

- Various commands are used to move in and out of command prompts:
  - To move from user EXEC mode to privileged EXEC mode, use the **enable** command.
  - Use return to user EXEC mode, use the **disable** command.
- Various methods can be used to exit / quit configuration modes:
  - **exit** - Used to move from a specific mode to the previous more general mode, such as from interface mode to global config.
  - **end** - Can be used to exit out of global configuration mode regardless of which configuration mode you are in.
  - **^z** - Works the same as **end**.



Navigate Between IOS Modes (Cont.)

- The following provides an example of navigating between IOS modes:
  - Enter privileged EXEC mode using the **enable** command.
  - Enter global config mode using the **configure terminal** command.
  - Enter interface sub-config mode using the **interface fa0/1** command.
  - Exit out of each mode using the **exit** command.
  - The remainder of the configuration illustrates how you can exit a sub-config mode and return to privileged EXEC mode using either the **end** or **^Z** key combination.



Hot Keys and Shortcuts

- 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**.
  - An even shorter version of **con** will not work because more than one command begins with **con**.
  - Keywords can also be shortened.

Video Demonstration - Hotkeys and Shortcuts

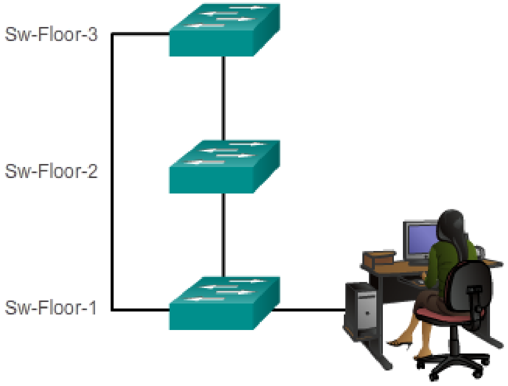
The IOS CLI support the following hotkeys:

- **Down Arrow** – Allows the user to scroll through command history.
- **Up Arrow** - Allows the user to scroll backward through commands.
- **Tab** - Completes the remainder of a partially entered command.
- **Ctrl-A** - Moves to the beginning of the line.
- **Ctrl-E** – Moves to the end of the line.
- **Ctrl-R** – Redisplays a line.
- **Ctrl-Z** – Exits the configuration mode and returns to user EXEC.
- **Ctrl-C** – Exits the configuration mode or aborts the current command.
- **Ctrl-Shift-6** – Allows the user to interrupt an IOS process (e.g., ping).

Device Names

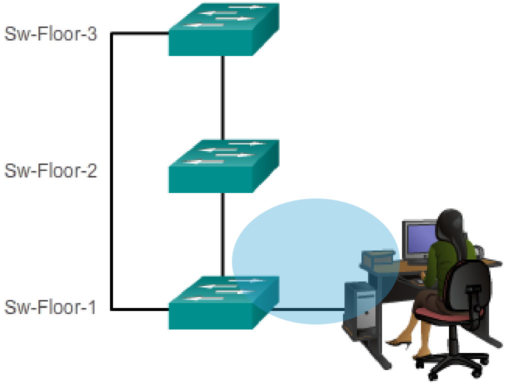
- The first step when configuring a switch is to assign it a unique device name, or hostname.
  - Hostnames appear in CLI prompts, can be used in various authentication processes between devices, and should be used on topology diagrams.
  - Without a hostname, network devices are difficult to identify for configuration purposes.

Hostnames enables an administrator to name a device making it easier to identify in a network.



Configure Hostnames

- Once the naming convention has been identified, the next step is to apply the names to the devices using the CLI .
- The **hostname** *name* global configuration command is used to assign a name.



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

Limit Access to Device Configurations

Configure Passwords

Securing User EXEC Mode	Description
`Switch(config)#` **line console 0**	Command enters line console configuration mode.
`Switch(config-line)#` **password** *password*	Command specifies the line console password.
`Switch(config-line)#` **login**	Command makes the switch require the password.

Securing Remote Access	Description
`Switch(config)#` **line vty 0 15**	Cisco switches typically support up to 16 incoming VTY lines numbered 0 to 15.
`Switch(config-line)#` **password** *password*	Command specifies the VTY line password.
`Switch(config-line)#` **login**	Command makes the switch require the password.

Limit Access to Device Configurations

Configure Passwords (Cont.)

Secure Privileged EXEC	Sw-Floor-1(config)# **enable secret class** Sw-Floor-1(config)# **exit** Sw-Floor-1# Sw-Floor-1# **disable** Sw-Floor-1> **enable** Password: Sw-Floor-1#
Securing User EXEC	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)# **exit** Sw-Floor-1(config)#
Securing Remote Access	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)#

Limit Access to Device Configurations

Encrypt Passwords

- The **startup-config** and **running-config** files display most passwords in plaintext. This is a security threat because anyone can see the passwords if they have access to these files.

- Use the **service password-encryption** global config command to encrypt all passwords.
  - The command applies weak encryption to all unencrypted passwords.
  - However, it does stop "shoulder surfing".

```
Sw-Floor-1(config)# service password-encryption
S1(config)# exit
S1# show running-config
<output omitted>
service password-encryption
!
hostname S1
!
enable secret 5
$1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
<Output omitted>
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login!
```

Limit Access to Device Configurations

Banner Messages

- Banners are messages that are displayed when someone attempts to gain access to a device. Banners are an important part of the legal process in the event that someone is prosecuted for breaking into a device.

  - Configured using the **banner motd** *delimiter message delimiter* command from global configuration mode. The delimiting character can be any character as long as it isunique and does not occur in the message (e.g., #$%^&*)

Limit Access to Device Configurations

Syntax Checker – Limiting Access to a Switch

Encrypt all passwords.

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

Secure the privileged EXEC access with the password Cla55.

```
Sw-Floor-1(config)# enable secret Cla55
Sw-Floor-1(config)#
```

Secure the console line. Use the password Cisc0 and allow login.

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password Cisc0
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# exit
Sw-Floor-1(config)#
```

Secure the first 16 VTY lines. Use the password Cisc0 and allow login.

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password Cisc0
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Save Configurations

Save the Running Configuration File

- Cisco devices use a **running configuration** file and a **startup configuration** file.

- Use the **copy running-config startup-config command** to save the running configuration.

Save Configurations

Alter the Running Configuration

- If configuration changes do not have the desired effect, they can be removed individually or the device can be rebooted to the last saved configuration using the **reload** privileged EXEC mode command.
  - The command restores the startup-config.
  - A prompt will appear to ask whether to save the changes. To discard the changes, enter **n** or **no.**

- Alternatively, if undesired changes were saved to the startup configuration, it may be necessary to clear all the configurations using the **erase startup-config** privileged EXEC mode command.

Configure IP Addressing

Switch Virtual Interface

- To remotely manage a switch, it must also be configured with an IP configuration:
  - However, a switch does not have a physical Ethernet interface that can be configured.
  - Instead, you must configure the VLAN 1 **switch virtual interface (SVI).**

- The VLAN 1 SVI <u>must</u> be configured with:
  - **IP address -** Uniquely identifies the switch on the network
  - **Subnet mask -** Identifies the network and host portion in the IP address
  - **Enabled -** Using the **no shutdown** command.

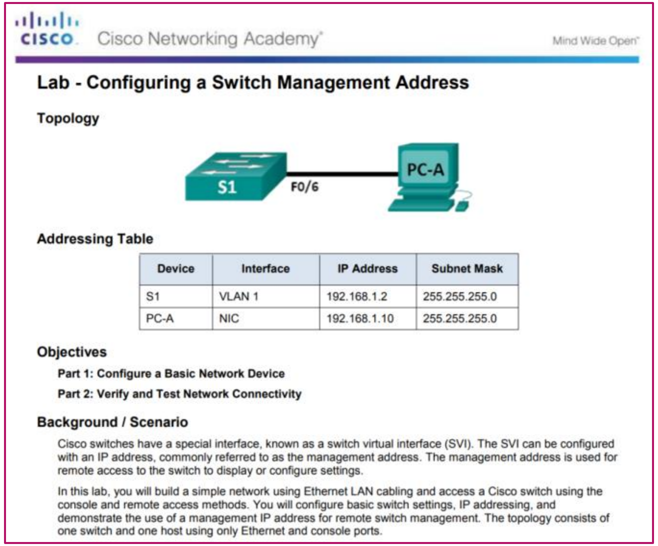
Verifying Connectivity

Interface Addressing Verification

- The IP configuration on a Windows host is verified using the **ipconfig** command.
- To verify the interfaces and address settings of intermediary devices like switches and routers, use the **show ip interface brief** privileged EXEC command.

Verifying Connectivity

Lab – Configuring a Switch Management Address



Cisco Networking Academy® Mind Wide Open™

Lab - Configuring a Switch Management Address

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0

Objectives

Part 1: Configure a Basic Network Device

Part 2: Verify and Test Network Connectivity

Background / Scenario

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings, IP addressing, and demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Thank You

cisco