Lab3. Internetwork Operating System (IOS) and Packet Tracer

TA 施羿廷 (ytshih)
credit to 林揚哲 (linyz)

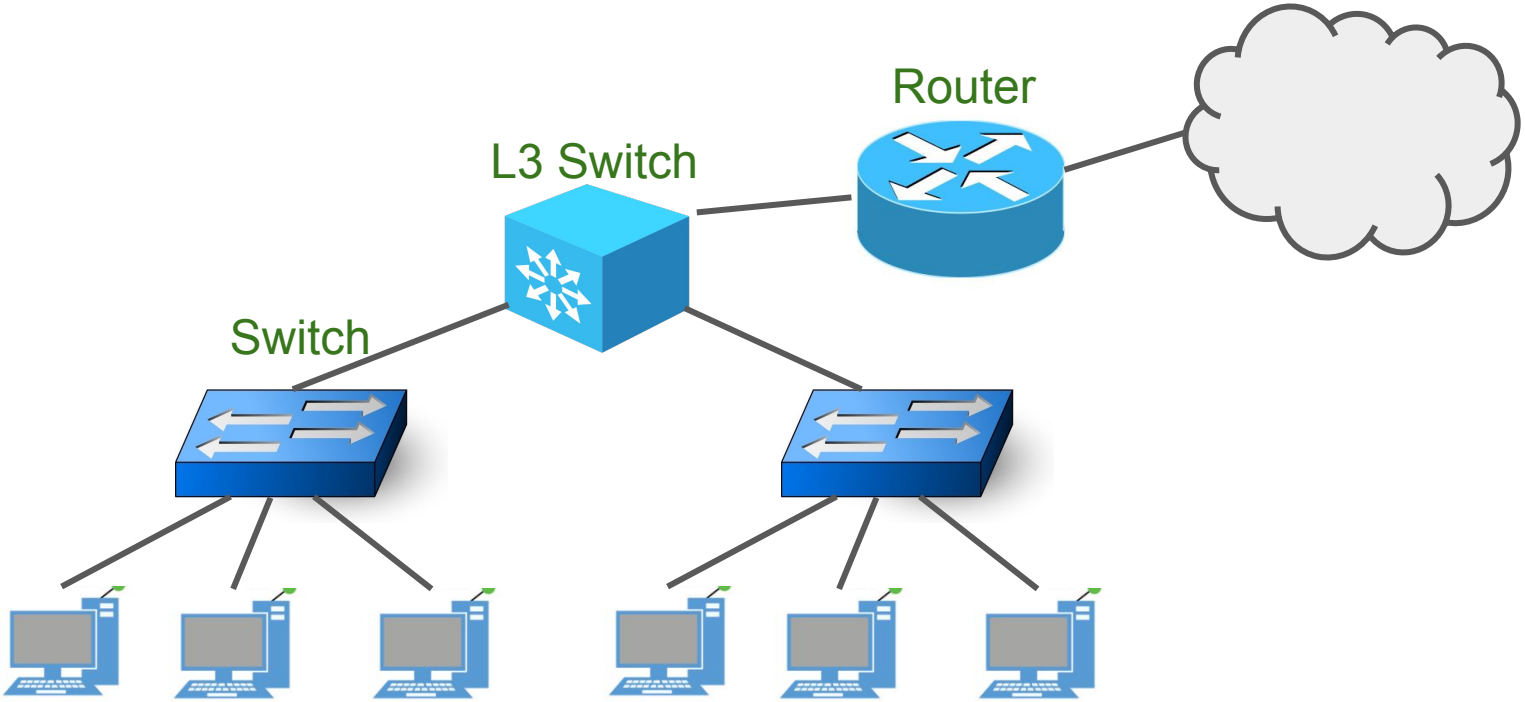
Outline

- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Outline

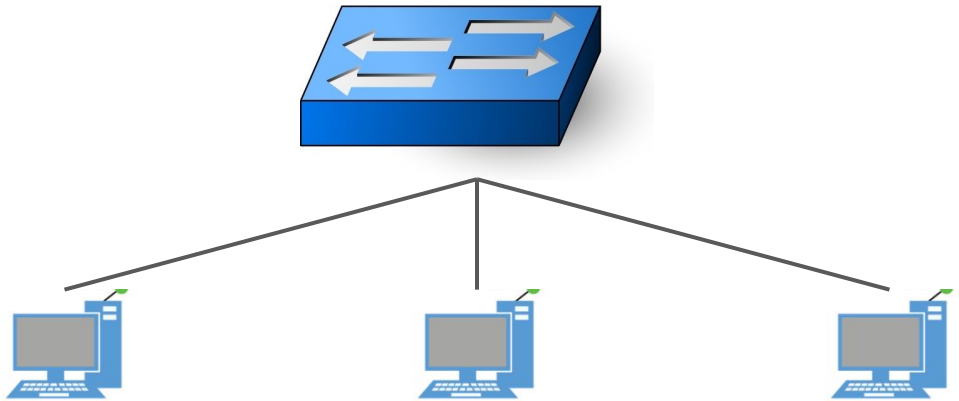
- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Simple Switch and Router topology



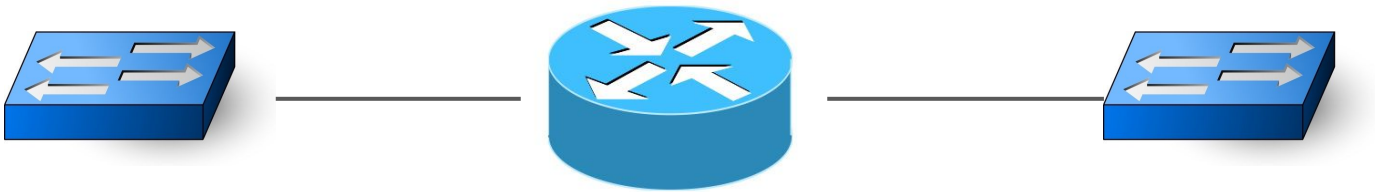
What is a Switch

- Connects multiple computers together within a network
- Operate at Data Link Layer (L2)
- Designed with multiple ports (usually more than 24 ports)



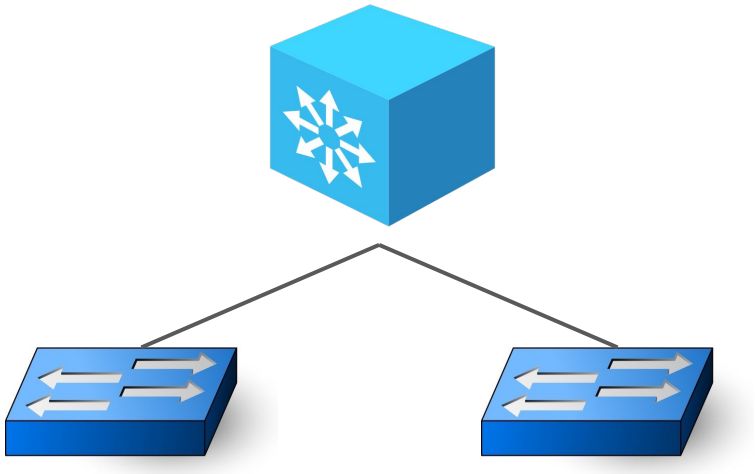
What is a Router

- Connect two or more logical subnets together
- Operate at Network Layer (L3)



What is a Layer 3 Switch

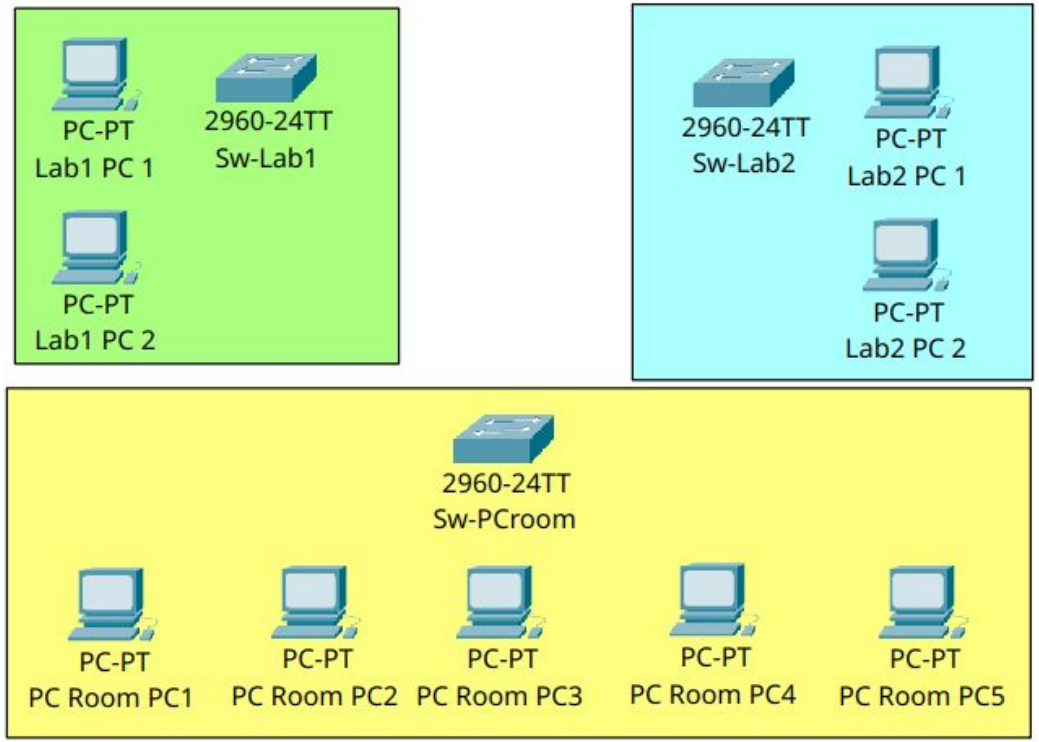
- Focus on vlan and simple IGP(Interior gateway protocol) funtionality
- Operate at both Data Link Layer (L2) and Network Layer (L3)



Scenario

- You are a newbie network administrator, and you found 3 switches.
- You have to manage the network of the company.
  - 1 PC room, with 5 PC.
  - 2 Labs, 2 PCs each.
  - The PCs should be able to connect to each other.

Lab 3 Scenario



Outline

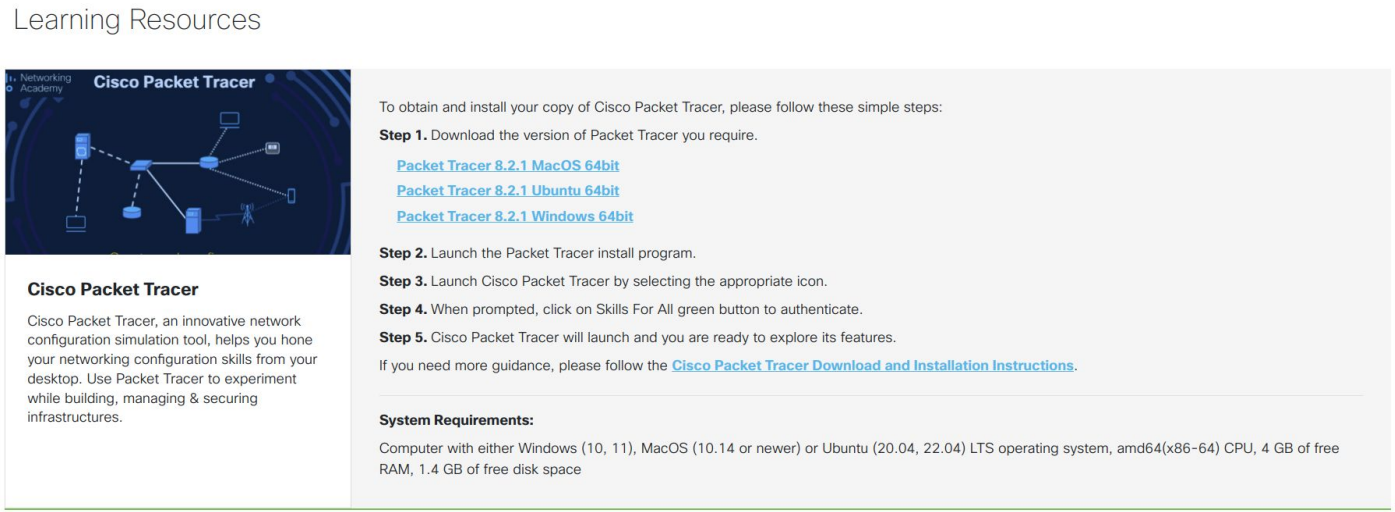
- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

What is Cisco Packet Tracer?

- Networking technology teaching and learning software developed by Cisco Networking Academy
- Create virtual networks and experiment on them
- Allow instructors to easily teach and demonstrate complex technical concepts and networking systems design

Download Packet Tracer

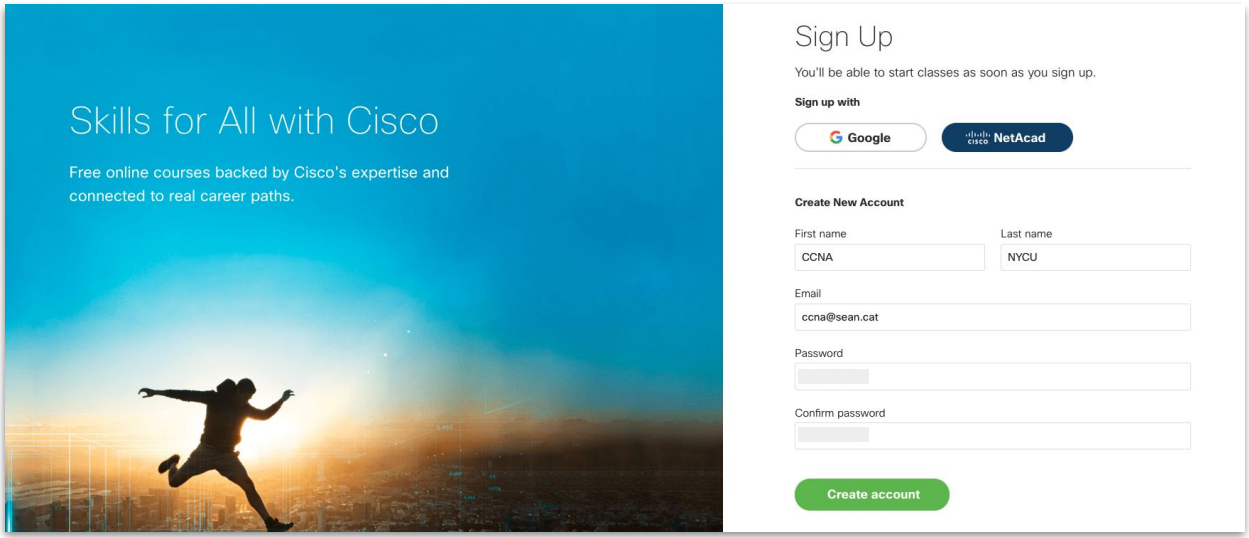
- You need an account to download Cisco Packet Tracer.
- Click top-right icon to sign-up.



https://skillsforall.com/resources/lab-downloads

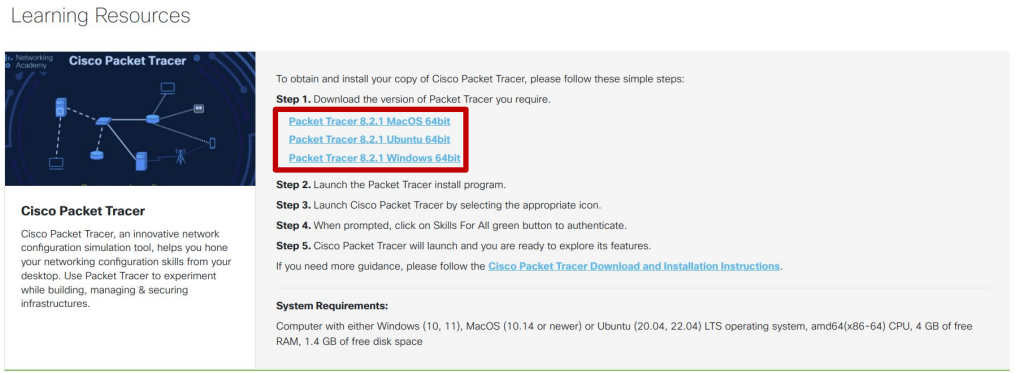
Download Packet Tracer

- Fill-in your own information to create an account.
- Please remember your password, you may need it for on-site midterm exam.

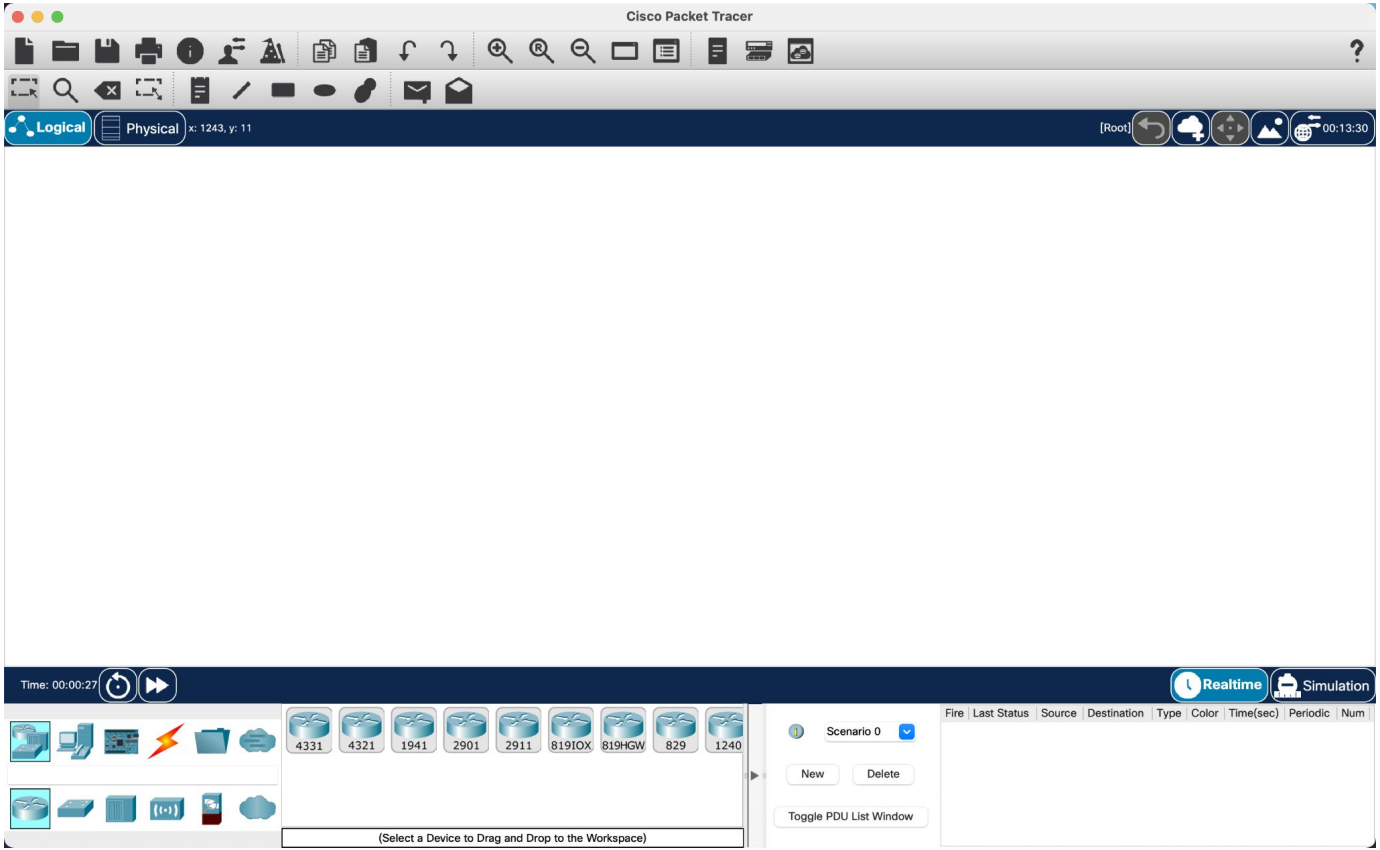


Download Packet Tracer

- Current version is 8.2.1.
- Using any version earlier than this might cause problems to your homework project.



Download Packet Tracer

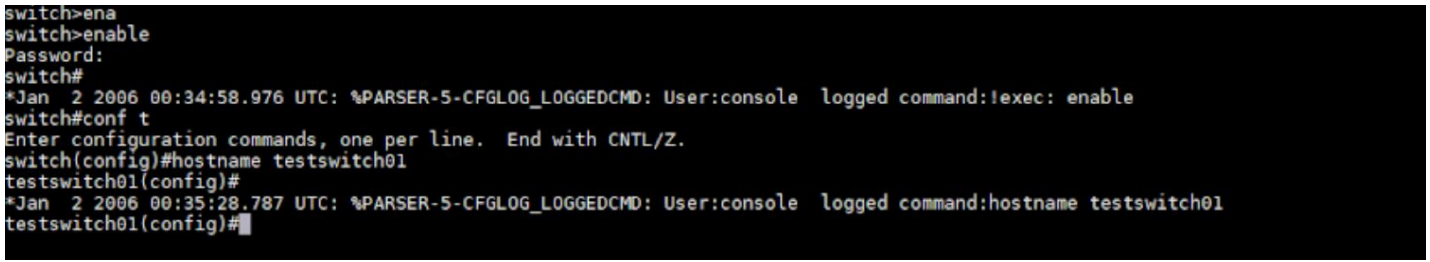


Outline

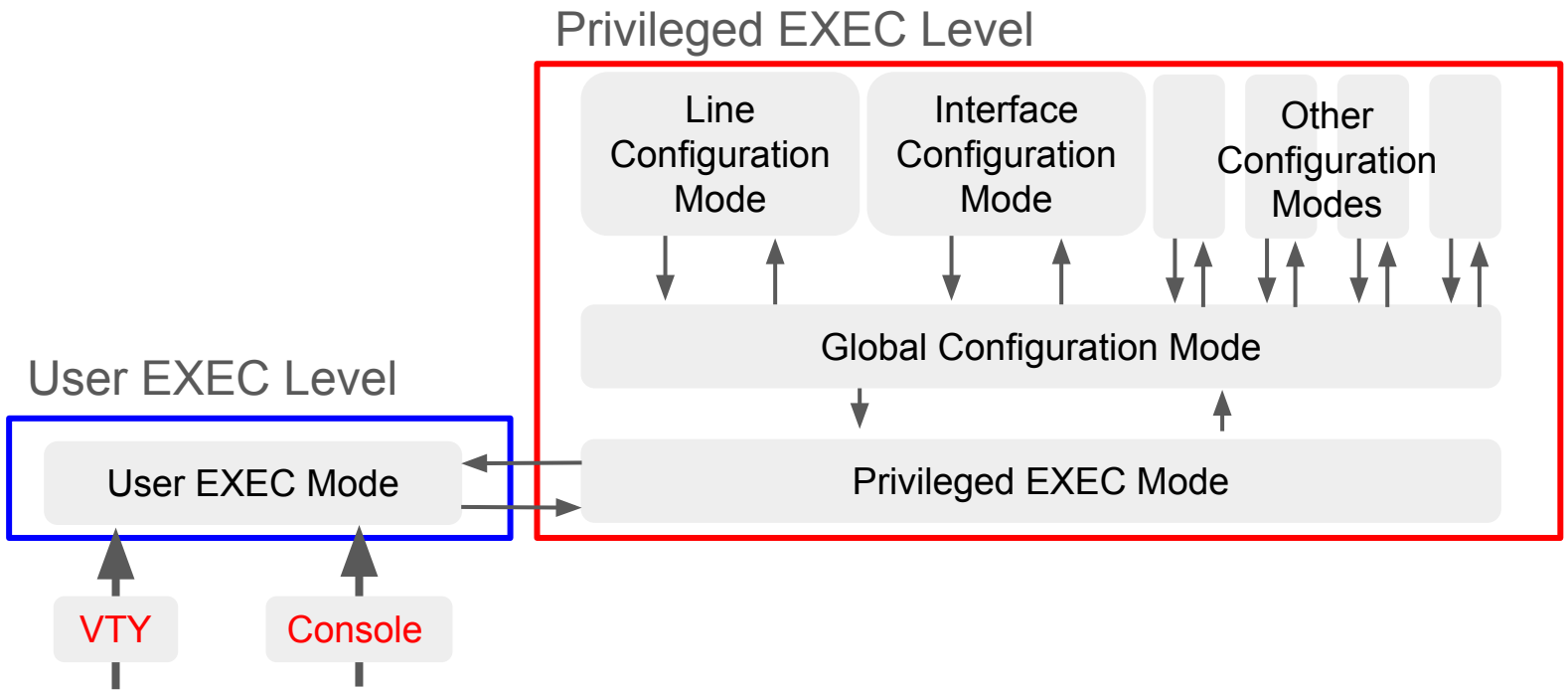
- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Purpose of IOS

- A CLI-based network operating system on a switch or router that enables an user to:
  - Run CLI-based network programs
  - View output on a monitor
- Cisco networking devices run particular versions of the Cisco IOS
  - The IOS version is dependent on the type of device being used and the required features
  - While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set to obtain additional capabilities.



IOS - User Levels and Command Modes



Reference: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm

IOS - User Levels

As a security feature, the Cisco IOS software **separates management access** into the following two primary command modes:

- **User EXEC Level**
  - It allows only a limited number of basic monitoring commands
  - Any commands that might change the configuration is not allowed
  - The **user EXEC mode** is identified by the CLI prompt that ends with **>**
- **Privileged EXEC Level**
  - You can access **all the command modes**.
  - The **privileged EXEC mode** is identified by the prompt ending with **#**

IOS - Configuration Command Modes

- To configure the device, the user must enter **Global Configuration Mode**, which is commonly called global config mode
- From **global config mode**, configuration changes are made globally
  - **Global configuration mode** is identified by a prompt that ends with `(config)#`
  - i.e. `Switch(config)#`
- From global config mode, the user can enter different **sub-configuration modes**
  - **Sub-configuration modes** allows the configuration of a particular part
  - Two common sub-configuration modes include:
    - **Line Configuration Mode** - Used to configure console, SSH, Telnet access.
    - **Interface Configuration Mode** - Used to configure a switch port or router network interface.

Navigate Between IOS Modes

Move between **User EXEC Mode** and **Privileged EXEC Mode**

```
switch> enable
switch# disable
switch>
```

Move between **Privileged EXEC Mode** and **Global Configuration Mode**

```
switch# configure terminal
switch(config)# exit
switch#
```

Navigate Between IOS Modes

Move from **any sub-configuration mode** to **Privileged EXEC mode**

```
switch(config-line)# end
switch#
```

```
switch(config-line)# Ctrl+Z
switch#
```

From one sub-configuration mode to another can be moved directly

```
switch(config-line)# interface vlan 1
switch(config-if)#
```

Navigate Between IOS Modes

`exit` can be used to move from any mode to its parent mode.

```
switch(config-line)# exit
switch(config)#
```

```
switch(config-if)# exit
switch(config)#
```

```
switch(config)# exit
switch#
```

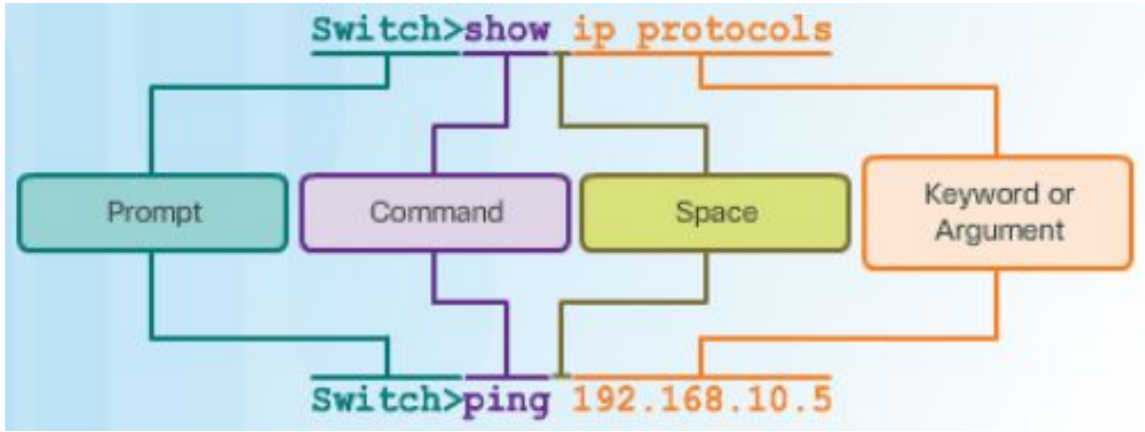
```
switch# exit
switch con0 is now available
press RETURN to get started.
```

Outline

- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Basic IOS Command Structure

- Each IOS command has a specific format or syntax and can only be executed in the appropriate mode
- The general syntax for a command is the command followed by any appropriate keywords and arguments.
  - **Keyword** - a specific parameter defined in the operating system (in the figure, ip protocols)
  - **Argument** - a value or variable defined by the user (in the figure, `192.168.10.5`)



Basic Configuration for Switch

- Generally speaking, your switch will work out of the box with no configuration.
- However, it will do nothing other than making your devices to be able to access each other.
    - Some other configurations might be needed to provide basic protection.

conventions

Bold	type exactly as shown.
Italic	replace with appropriate argument.
[brackets]	any or all arguments within [ ] are optional.
{braces}	all arguments within [ ] are necessary.

IOS - Commands and Keywords Shortening

- Commands and keywords can be shortened to the minimum number of characters that identify a unique selection
  - 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**
  - The **terminal** keyword can be shortened to **t** because terminal is the only keyword available in command configure.

```
switch# conf t
switch(config)#
```

```
switch# con t
% Ambiguous command: "con t"
```

IOS - Hotkeys

?	List available commands
Tab	Autocomplete & Check if the current command viable
Ctrl + Z	Return to Privileged EXEC Mode
Ctrl + Shift + 6	Cancel Cisco IOS Process
Up Arrow / Down Arrow	Allows user to scroll through former commands.

```
Switch>hello
Translating "hello"...domain server (255.255.255.255) % Name lookup aborted
Switch>
```

Save the Running Configuration File

- There are two system files that store the device configuration:
  - **startup-config**
    - Stored in Non-volatile Random Access Memory (NVRAM)
    - Contains all of the commands that will be used by the device upon reboot
    - NVRAM does not lose its contents when the device is powered off or restarted
  - **running-config**
    - Stored in Random Access Memory (RAM)
    - 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

```
switch# copy running-config startup-config
```

Configure Hostnames

Edit hostname

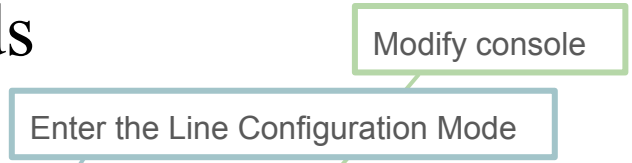
```
switch# configure terminal
switch(config)# hostname SW-EC1f
SW-EC1f(config)#
```

- Remember to save in Privileged EXEC Mode after configuring.
- Add **no** in front of any command will remove that command.
  - e.g. switch(config)# **no hostname** *SW-EC1f*

Secure Device Access

- Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device
  - Console Access password
    - Password for Switch console port access
  - Privileged EXEC Access password
    - **enable** password for entering Privileged EXEC from User EXEC Mode
- Other tasks
  - Encrypt all passwords
  - Provide legal notification

Configure Passwords



Console Access password

```
SW-EC1f(config)# line console 0
SW-EC1f(config-line)# password passwd1
SW-EC1f(config-line)# login
SW-EC1f(config-line)# exit
SW-EC1f(config)#
```

Privileged EXEC Access password

```
SW-EC1f(config)# enable password passwd2
```

Encrypt Passwords

- The startup-config and running-config files display **password** in plaintext
  - This is a security threat since anyone can see the passwords used if they have access to these files.
- To encrypt passwords, use the **service password-encryption** global config command
  - The command applies weak encryption (Vigenère cipher) to all unencrypted passwords
  - This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network
  - The purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.
  - **It cannot provide any security at all**

```
SW-EC1f(config)# service password-encryption
```

Configure Users and their Secrets

- Create a user and set its secret
  - Secret is same with password
  - But it stores the result of MD5 hash function instead

```
SW-EC1f(config)# username user secret passwd3
SW-EC1f(config)# line console 0
SW-EC1f(config-line)# login local
SW-EC1f(config-line)# exit
SW-EC1f(config)#
```

```
SW-EC1f(config)# enable secret passwd4
```

Banner Messages

Although requiring passwords is one way to keep unauthorized personnel out of a network, it is vital to provide a method for declaring that only authorized personnel should attempt to gain entry into the device

```
SW-EC1f(config)# banner motd !
helloworld hellloflvksdflsdk!
SW-EC1f(config)#
```

The Delimiter can be any character, being used to mark the start and end of message.

Verify and Monitor Solution

- The Cisco IOS **show** commands are some of the most useful troubleshooting and verification tools included the Cisco IOS
  - Taking advantage of a large variety of options and sub-options, the show command can be used to narrow down and display information about practically any specific aspect of IOS

```
SW-EC1f# show running-config
SW-EC1f# show statup-config
SW-EC1f# show interfaces
SW-EC1f# show arp
SW-EC1f# show version
```

Command Output Redirection

- The output of a **show** command can be filtered or redirected to a file.
- Redirection is available using a **pipe (|)** character after **any show command**, combined with the following keywords:

`begin`	Begins unfiltered output of the show command with the first line that contains the regular expression.
`exclude`	Displays output lines that do not contain the regular expression.
`include`	Displays output lines that contain the regular expression.
`section`	Filter a section of output

Command Output Redirection - Examples

```
Switch# show running-config | section username
username ccna secret 5 $1$mERr$Bok4KDfVutXOJolNq009M/
Switch# show running-config | section line
line con 0
  login local
line vty 0 4
  login
line vty 5 15
  login
end
Switch#
```

Cisco Discovery Protocol (CDP)

- A Cisco proprietary protocol
- Collect directly connected neighbor device information
  - hardware, software, device name, …
- Show all neighbors

```
Sw-Lab1# show cdp neighbors
```

- Show details of one neighbor

```
Sw-Lab1# show cdp entry Device-ID
```

Cisco Discovery Protocol (CDP)

- Disable CDP globally

```
Sw-Lab1(config)# no cdp run
```

- Disable CDP for an interface

```
Sw-Lab1(config)# interface fastEthernet 0/1
Sw-Lab1(config-if)# no cdp enable
```

Link Layer Discovery Protocol (LLDP)

- IEEE standard protocol
- Similar to CDP
- Not enabled by default

```
Sw-Lab1(config)# lldp run
```

or

```
Sw-Lab1(config)# interface fastEthernet 0/1
Sw-Lab1(config-if)# lldp receive
Sw-Lab1(config-if)# lldp transmit
```

Link Layer Discovery Protocol (LLDP)

- Show lldp neighbors

```
Sw-Lab1# show lldp neighbors
```

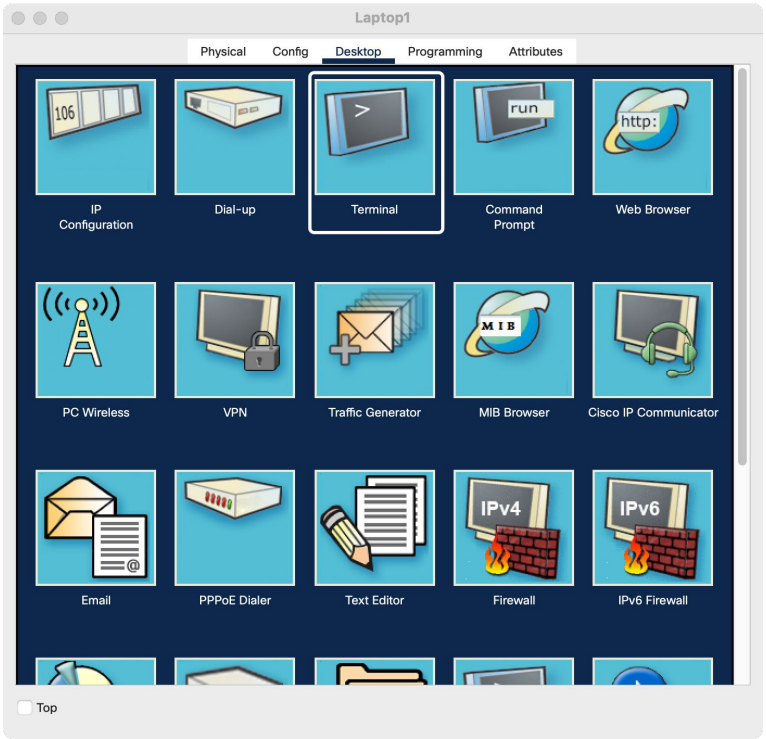
Command Review

```
switch> enable
switch# conf term
switch(config)# hostname SW-EC1f
SW-EC1f(config)# enable secret passwd1
SW-EC1f(config)# username user secret passwd2
SW-EC1f(config)# line console 0
SW-EC1f(config-line)# login local
SW-EC1f(config-line)# exit
SW-EC1f(config)# banner motd !
helloworld hellloflvksdflsdk!
SW-EC1f(config)# exit
SW-EC1f# cop runn start
```

Outline

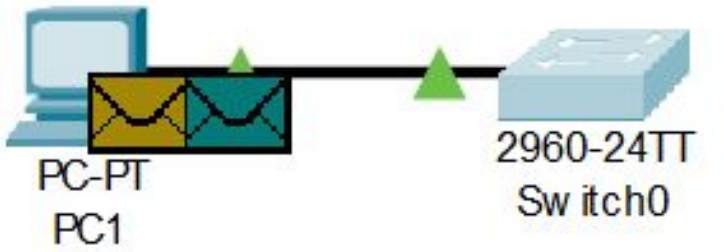
- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Packet Tracer Functions - Console



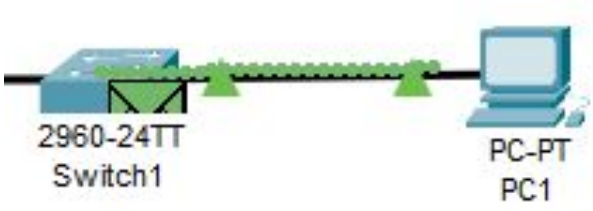
Packet Tracer Functions - Protocol Data Unit

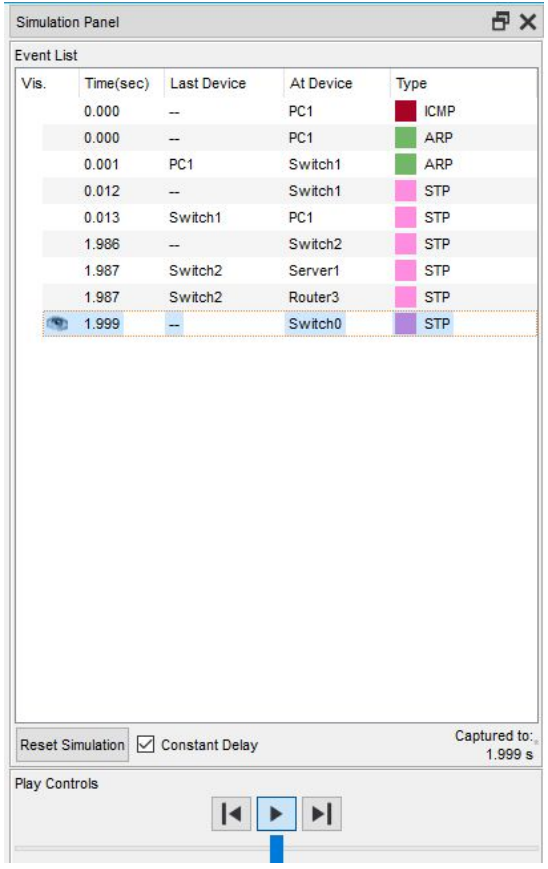
- Send a Protocol Data Unit (PDU) for test



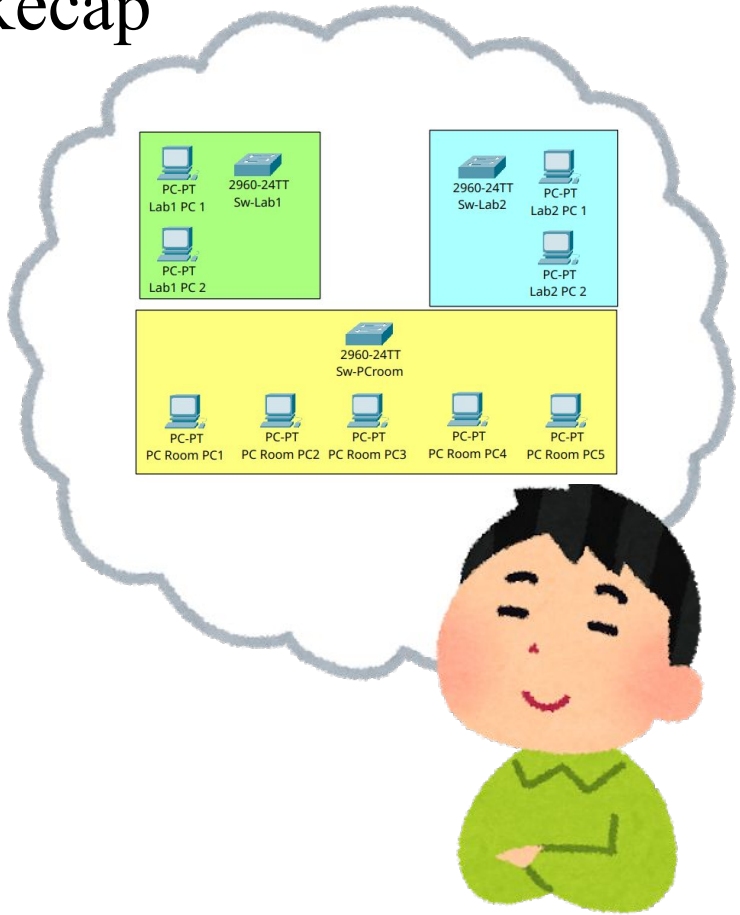
Packet Tracer Functions - Simulation

- Visualize the network traffic

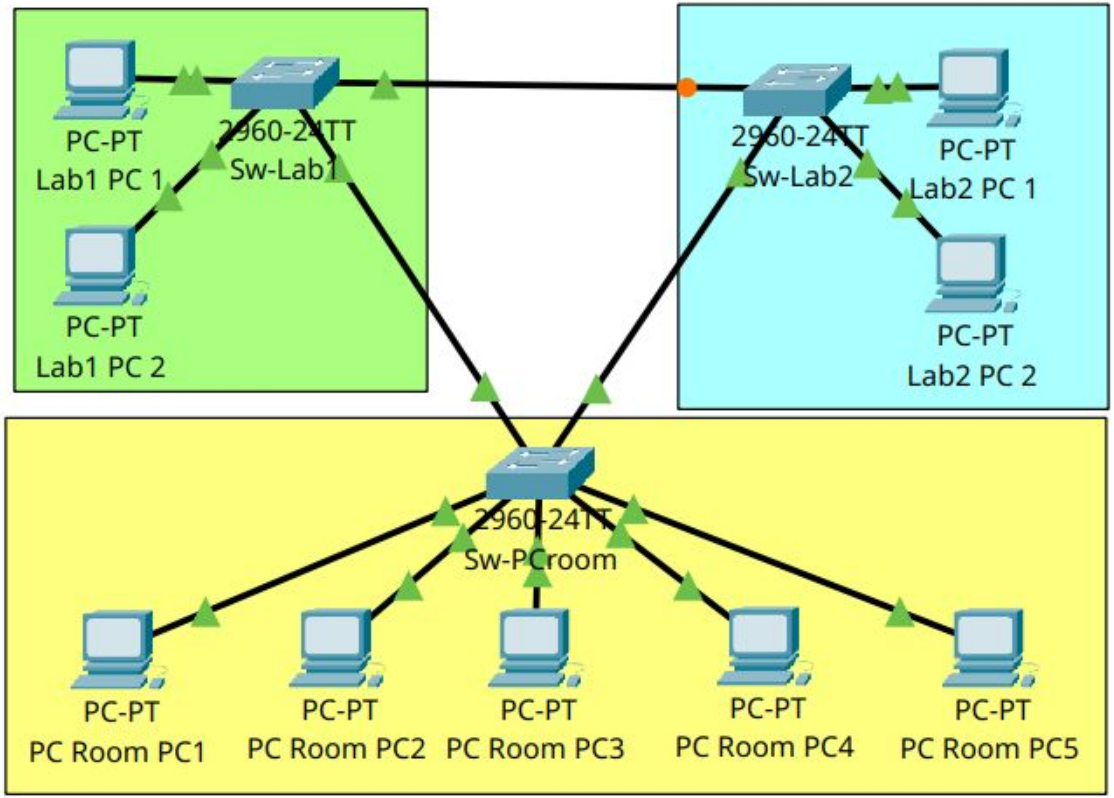




Lab3 Scenario Recap



Lab3 Solution



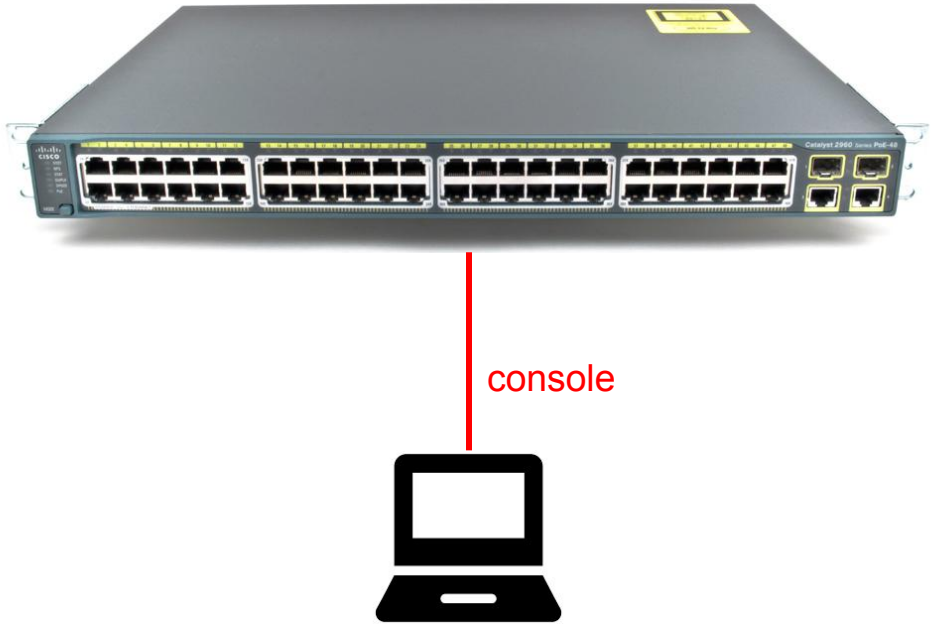
Lab Requirement

- Banner message should be set to **`This is my first project!`**
- There should be hostname on each switch.
  - `Sw-Lab1`
  - `Sw-Lab2`
  - `Sw-PCroom`
- Password **`class`** should be required for entering user EXEC mode.
  - Encrypted using weak encryption.
- Password **`nycu`** should be required for entering privileged EXEC mode.
  - Encrypted using MD5
- There should be a distinct IP on each PC, and is able to ping each other.
  - Lab1: `192.168.1.1/16 - 192.168.1.2/16`
  - Lab2: `192.168.2.1/16 - 192.168.2.2/16`
  - PCroom: `192.168.3.1/16  - 192.168.3.5/16`

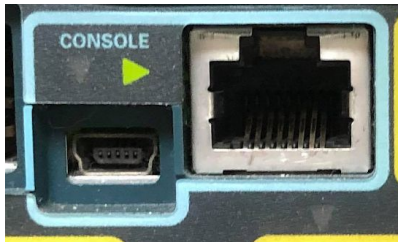
Outline

- Network Device Introduction
- Packet Tracer Introduction & Installation
- IOS Introduction
- Basic Setting of Switch
- Functions of Packet Tracer
- Try the Real Switch

Try the Real Switch



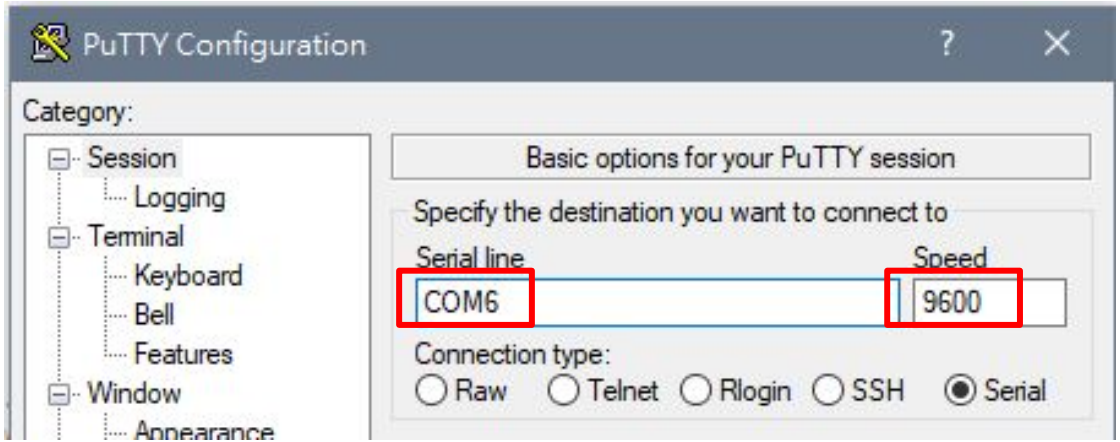
Try the Real Switch - Console

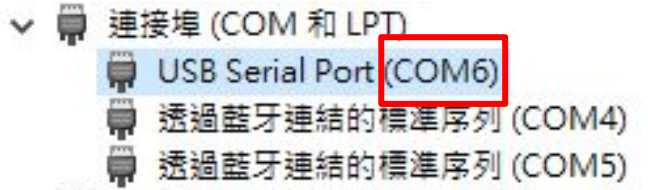


Try the Real Switch - Console

裝置管理員

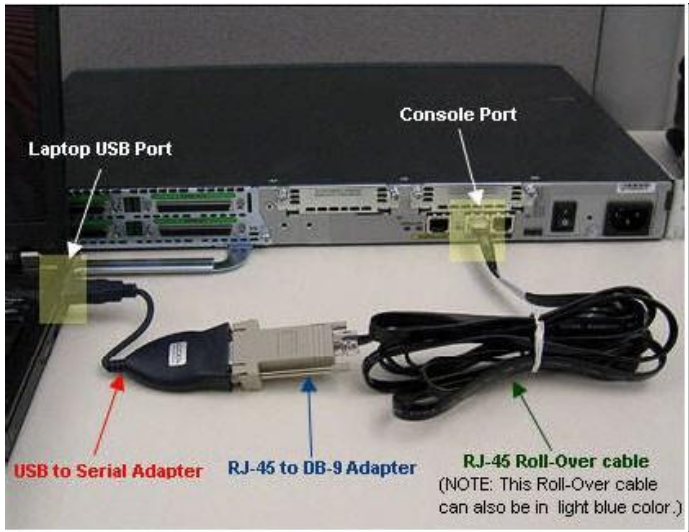
控制台

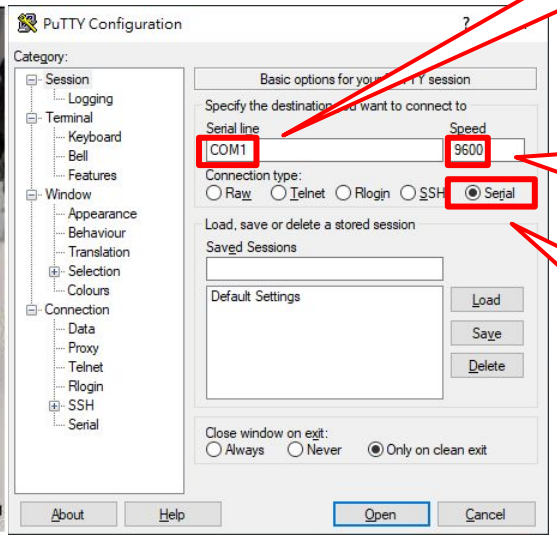




How to Access a Switch - Console

- Directly connect the ethernet cable to the console port on the switch.
  - No need to be able to access internet.
  - Filled in the transmission speed (bit rate) according to the brand and model.
    - e.g. 300, 1200, 2400, 9600, 115200, 19200 bit/s





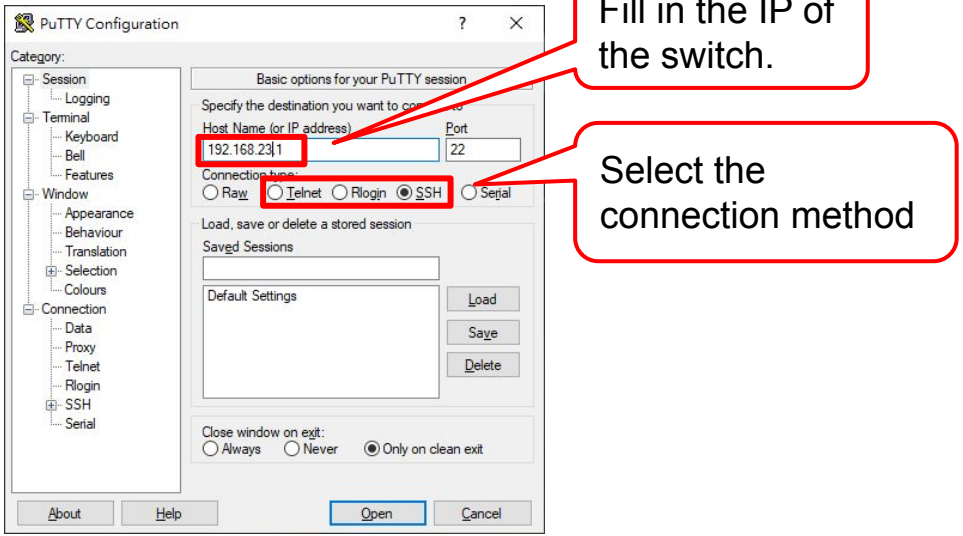
Select the connected interface

Fill in the transmission speed

Select Connection Type ‘Serial’

How to Access a Switch - VTY (Virtual Teletype Terminal)

- Connect to the administration interface by network connection.
  - The basic networking must be configured.
  - e.g. ssh, telnet



Try the Real Switch - Reset

- Unplug the power cord
- Plug in the power cord and immediately hold down the“MODE”button for a while

Try the Real Switch - Reset

- Mount flash file system

```
The system has been interrupted ...
...

switch: flash_init
```

- Show files

```
switch: dir flash:

Directory of flash:/
   13  drwx         192   Mar 01 1993 22:30:48  c2960-lanbase-mz.122-25.FX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat
```

Try the Real Switch - Reset

- Delete config.text and vlan.dat

```
switch: delete flash:config.text
switch: delete flash:vlan.dat
```

- Boot

```
switch: boot
...
Continue with the configuration dialog? [yes/no]:  N

Switch>
```

Try the Real Switch - SSH Configuration

- Set a Switched Virtual Interface (SVI) to switch

```
switch(config)# interface vlan 1
switch(config-if)# ip address 192.168.<Team-ID>.69 255.255.0.0
switch(config-if)# no shutdown
```

- Create a user

```
switch(config)# username username secret passwd
```

Try the Real Switch - SSH Configuration

- Configure hostname and domain name

```
switch(config)# hostname hostname
CCNA-01(config)# ip domain-name domain-name
```

- Configure RSA key pair

```
CCNA-01(config)# crypto key generate rsa
! Choose modulus length = 1024
```

Try the Real Switch - SSH Configuration

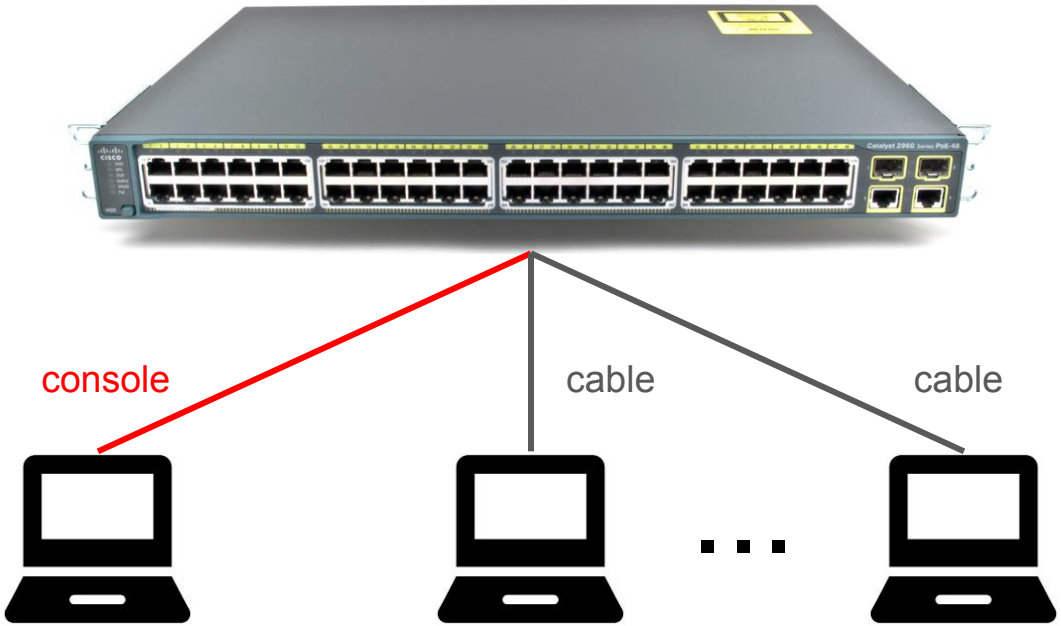
- Choose SSH version

```
CCNA-01(config)# ip ssh version 2
```

- Allow users to login by SSH
  - Allow SSH only and use user authentication

```
CCNA-01(config)# line vty 0 15
CCNA-01(config-line)# transport input ssh
CCNA-01(config-line)# login local
CCNA-01(config-line)# exit
```

Try the Real Switch - Cable



Try the Real Switch - Cable

1. Plug in the ethernet cable.
2. Set `192.168.<Team_ID>.x/16` on your laptop.
3. Gateway will not be used for now, set it to `192.168.<Team_ID>.254`

Try the Real Switch - SSH

- Ping to check connectivity
- Connect to the switch
  - Use PuTTY if you have
  - PowerShell / CMD: `C:\> ssh -l username 192.168.<Team-ID>.69`

Try the Real Switch - SSH issue

- Unable to negotiate with `x.x.x.x` port `22`: no matching cipher found

```
C:\> ssh -l username 192.168.<Team-ID>.69  -c cipher
```

- Their offer: diffie-hellman-group1-sha1
  - Create a file `C:\User\<username>\.ssh\config`
  - Copy the content below to it and save

```
HostKeyAlgorithms +ssh-rsa
PubkeyAcceptedKeyTypes +ssh-rsa
KexAlgorithms +diffie-hellman-group1-sha1
Ciphers +3des-cbc
```

Force Other Users to Logout

- Check current connections

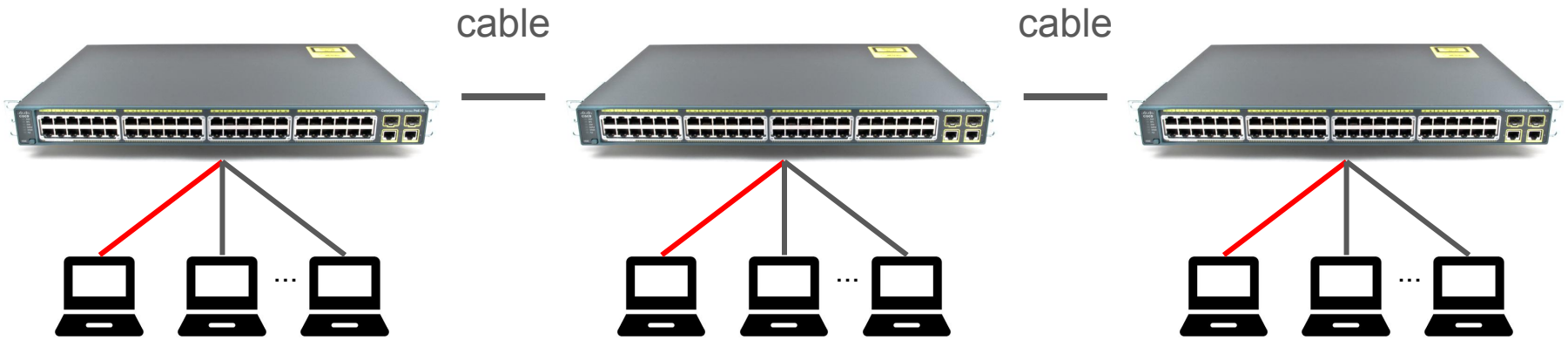
```
CCNA-01# show users
    Line       User   Host(s)        Idle       Location
* 0 con 0               idle          00:00:00
  2 vty 0     user2  idle          00:00:45
  3 vty 1     user3  idle          00:00:23
```

- Choose a lucky number and kick him/her out!

```
CCNA-01# clear line vty x
[confirm]
 [OK]
```

Try the Real Switch - Interconnection

- Connect to your neighbor team



Try the Real Switch - Interconnection

- Use CDP to check your neighbor(s)

```
CCNA-01# show cdp neighbors
CCNA-01# show cdp entry Device-ID
```

- Ping your neighbor(s)

```
CCNA-01# ping 192.168.x.y
```

- Use Wireshark to see what can be captured

Try the Real Switch - Password Recovery

- Set a password for console port and save

```
CCNA-01(config)# line console 0
CCNA-01(config-line)# password passwd
CCNA-01(config-line)# login
CCNA-01(config-line)# ^z
CCNA-01# copy running-config startup-config
```

- Forgot password...

Try the Real Switch - Password Recovery

- Unplug the power cord
- Plug in the power cord and immediately hold down the“MODE”button for a while

Try the Real Switch - Password Recovery

- Mount flash file system

```
The system has been interrupted ...
...

switch: flash_init
```

- Show files

```
switch: dir flash:

Directory of flash:/
   13  drwx         192   Mar 01 1993 22:30:48  c2960-lanbase-mz.122-25.FX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat
```

Try the Real Switch - Password Recovery

- Rename config.text

```
switch: rename flash:config.text flash:config.bak
```

- Boot

```
switch: boot
```

Try the Real Switch - Password Recovery

- Enter no to reject initial configuration dialog

```
In order to access the device manager, ...
...
Would you like to enter the initial configuration dialog?
[yes/no]: no

Switch>
```

- Restore config.text and running-config

```
Switch> enable
Switch# copy running-config startup-config
Switch# copy flash:config.bak flash:config.text
Switch# copy startup-config running-config
```

Try the Real Switch - Password Recovery

- Change the password

```
CCNA-01(config)# line console 0
CCNA-01(config-line)# password passwd
CCNA-01(config-line)# login
CCNA-01(config-line)# exit
CCNA-01(config)#
```

- Save to startup-config

```
CCNA-01# copy running-config startup-config
```

That’s all

- Feel free to ask any question.