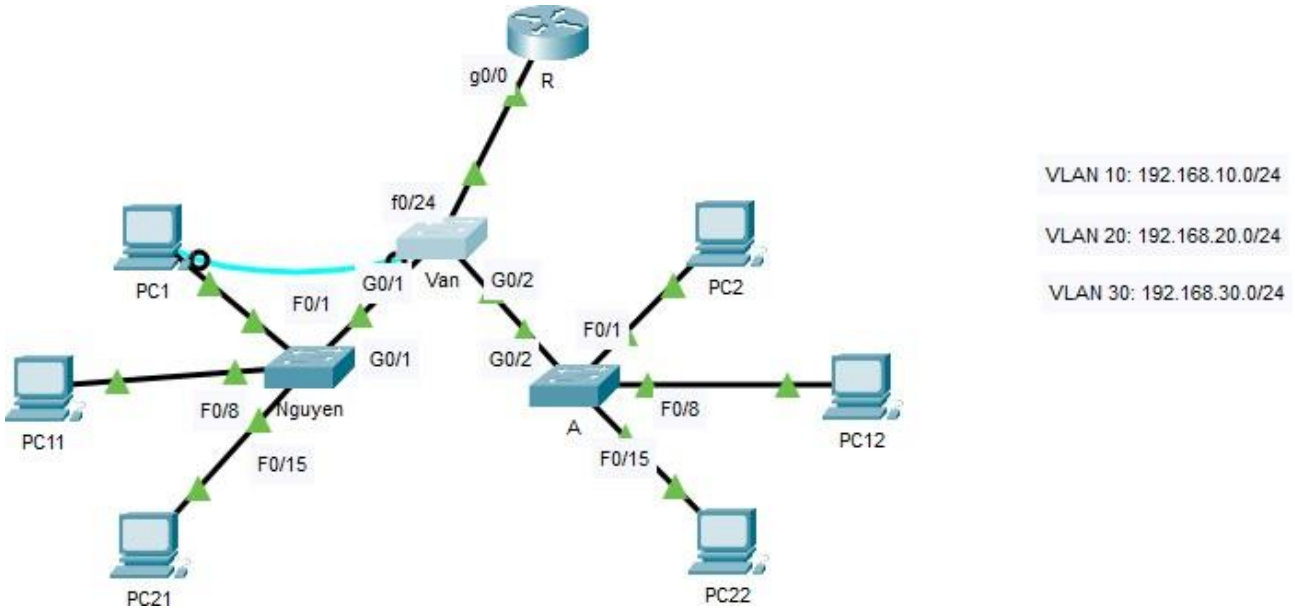
Configuring VLANs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	192.168.10.2	255.255.255.0	10
PC2	NIC	192.168.10.3	255.255.255.0	10
S1	VLAN 10	192.168.10.252	255.255.255.0	10
S2	VLAN 10	192.168.10.253	255.255.255.0	10
S3	VLAN 10	192.168.10.254	255.255.255.0	10
R	G0/0.10	192.168.10.1	255.255.255.0	10
…				
PC11	NIC	192.168.20.11	255.255.255.0	20
PC12	NIC	192.168.20.12	255.255.255.0	20
R	G0/0.20	192.168.20.1	255.255.255.0	20
…..				
PC21	NIC	192.168.30.21	255.255.255.0	30
PC22	NIC	192.168.30.22	255.255.255.0	30
R	G0/0.30	192.168.30.1	255.255.255.0	30
…				

Objectives

Part 1: Basic Switch Configuration

Part 2: VLANs Configuration

Part 3: Trunks Configuration

Part 4: Inter-VLAN Routing

Background

VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

Part 1: Switch Configuration

1. Switch Configuration from PC1:

Step 1: Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the light blue Console cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling from it.

c. Click **PC1**. A window displays an option for an RS-232 connection.

d. Drag the other end of the console connection to the S1 switch and click the switch to access the connection list.

e. Select the **Console** port to complete the connection.

Step 2: Establish a terminal session with S1.

a. Click **PC1** and then select the **Desktop** tab.

b. Click the **Terminal** application icon. Verify that the Port Configuration default settings are correct.

What is the setting for bits per second? 9600

c. Click **OK**.

d. The screen that appears may have several messages displayed. Somewhere on the screen there should be a `Press RETURN to get started!` message. Press ENTER.

2. Verify the Default Switch Configuration

Step 3: Enter privileged EXEC mode.

You can access all switch commands from privileged EXEC mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

Enter privileged EXEC mode by entering the **enable** command:

```
Switch> enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 4: Examine the current switch configuration.

a. Enter the **show running-config** command.

```
Switch# show running-config
```

b. Answer the following questions:

1) How many FastEthernet interfaces does the switch have? 24

2) How many Gigabit Ethernet interfaces does the switch have? 2

3) What is the range of values shown for the vty lines? 0 15

4) Which command will display the current contents of non-volatile random-access memory (NVRAM)?
show startup-configuration

5) Why does the switch respond with `startup-config is not present`?
Nó hiển thị thông báo này vì tệp cấu hình không được lưu vào NVRAM. Hiện tại nó chỉ nằm trong RAM

3. Create a Basic Switch Configuration

Step 5: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

```
Switch# configure terminal
Switch(config)# hostname MidName
S1(config)# exit
S1#
```

Step 6: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **tdmu**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password tdmu
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Why is the **login** command required?
Để quá trình kiểm tra mật khẩu hoạt động, nó yêu cầu cả lệnh đăng nhập và mật khẩu

Step 7: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 8: Secure privileged mode access.

Set the **enable** password to **cisco**. This password protects access to privileged mode.

Note: The **0** in **cisco** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password cisco
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 9: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

```
User Access Verification
Password:
```

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

```
S1# show running-config
```

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 10: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **ittdmu**.

```
S1# config t
S1(config)# enable secret ittdmu
```

```
S1(config)# exit
S1#
```

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 11: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

Note: You can abbreviate **show running-config** as

```
S1# show run
```

b. What is displayed for the **enable secret** password? _____

c. Why is the **enable secret** password displayed differently from what we configured?

_____

_____

Step 12: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain.

_____

_____

4. Configure a MOTD Banner

Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

```
S1# config t
S1(config)# banner motd "This is Switch Middle Name"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

1) When will this banner be displayed?

_____

_____

2) Why should every switch have a MOTD banner?

_____

_____

_____

_____

5. Save Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

Step 2: Save the configuration file.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

```
S1# copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]
```

What is the shortest, abbreviated version of the **copy running-config startup-config** command? _____

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM? _____

Are all the changes that were entered recorded in the file? _____

6. Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **FisrtName**

b. Protect access to the console using the **tdmu** password.

c. Configure an enable password of **cisco** and an enable secret password of **ittdmu**.

d. Configure a message to those logging into the switch with the following message:

```
Authorized access only. Unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law.
```

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

7. Configure S3

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **LastName**

b. Protect access to the console using the **tdmu** password.

c. Configure an enable password of **cisco** and an enable secret password of **ittdmu**.

d. Configure a message to those logging into the switch with the following message:

```
Authorized access only. Unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law.
```

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

Part 2: VLAN Configuration

1. View the Default VLAN Configuration

Step 1: Display the current VLANs.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.

Step 2: Configure IP on PCs (ip for earch PC in Addressing Table)

Step 3: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same network.

- PC1 can ping PC2
- PC11 can ping PC12
- PC21 can ping PC22

Pings to PCs in other networks fail.

What benefit will configuring VLANs provide to the current configuration?

_____

_____

2. Configure VLANs

Step 4: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

- VLAN 10: Faculty
- VLAN 20: Students
- VLAN 30: Guest
- VLAN 99: Management (Native)

S1(config)#vlan 10

S1(config-vlan)#name Faculty

Step 5: Verify the VLAN configuration.

Which command will only display the VLAN name, status, and associated ports on a switch?

_____

Step 6: Create the VLANs on S2 and S3.

Using the same commands from Step 1, create and name the same VLANs on S2 and S3.

Step 7: Verify the VLAN configuration.

3. Assign VLANs to Ports

Step 8: Assign VLANs to the active ports on S2, S3.

Assign the VLANs to the following ports:

- VLAN 10: Fast Ethernet 0/1-7
- VLAN 20: Fast Ethernet 0/8-14
- VLAN 30: Fast Ethernet 0/15-21
- VLAN 99: Fast Ethernet 0/22-24

S2(config)#int f0/1 (int rang f0/1-7)
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10

4. Configure IP for VLAN 10 on Switchs

Step 1: Configure IP for VLAN 10 on Switchs (ip for earch Switch in Addressing Table)

S1(config-if)#int vlan 10

S1(config-if)#ip add 192.168.10.252 255.255.255.0

S1(config-if)# exit

S1(config)#ip default-gateway 192.168.10.1

Step 2: Verify connectivity from PCs in VLAN10 to Switchs.

- PC1 can ping S1
- PC1 can ping S2
- PC1 can ping S3

Part 3: Configure Trunks

Step 1: Configure trunking on Switchs and use VLAN 99 as the native VLAN.

a. Configure G0/1, G0/2, f0/24 interfaces on S1 for trunking.

S1(config-if)#int g0/1

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
```

b. Configure VLAN 99 as the native VLAN for G0/1, G0/2 and f0/24 interfaces on **S1**.

The trunk port takes about a minute to become active due to Spanning Tree. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2
(99), with S3 GigabitEthernet0/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(99), with S2 GigabitEthernet0/1 (1).
```

c. Configure G0/1, interfaces on S2 for trunking. Configure VLAN 99 as the native VLAN for G0/1 on S2.

d. Configure G0/2, interfaces on S3 for trunking. Configure VLAN 99 as the native VLAN for G0/2 on S3.

Step 2: Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to cross the trunk?

_____

Step 3: Verify configurations on S2 and S3.

e. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.

f. Use the **show vlan** command to display information regarding configured VLANs. Why is port G0/2 on S2 no longer assigned to VLAN 1?

_____

Part 4: Inter-VLAN Routing

1. Test Connectivity Without Inter-VLAN Routing

Step 1: Ping between PC1 and PC11.

Because the two PCs are on separate networks and **R** is not configured, the ping fails.

Step 2: Switch to Simulation mode to monitor pings.

a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC11**. Notice how the ping never leaves **PC1**. What process failed and why?

_____

2. Configure Subinterfaces

Step 3: Configure subinterfaces on R using the 802.1Q encapsulation.

a. Create the subinterface G0/0.10.

- Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.

```
Router(config)#int g0/0
Router(config-if)#no sh
Router(config-if)#int g0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.10.1 255.255.255.0
Router(config-subif)#no sh
```

- Refer to the **Address Table** and assign the correct IP address to the subinterface.

b. Repeat for the G0/0.20, G0/0.30 and g0/0.99 subinterface.

Step 4: Verify Configuration.

a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated with.

b. Enable the G0/0 interface. Verify that the subinterfaces are now active.

3. Test Connectivity with Inter-VLAN Routing

Step 5: Ping between PC1 and PC2.

……..

Step 6: Ping between PC1 and PC12.

……..

Step 7: Ping between PC1 and PC22

……..