LAB 3: Network Access, Security and VLANs

Contents

Introduction to LAB 3

In Module 3, you have learned about the benefits of VLANs. In the following lab, you will put this into practice – you will create VLANs, assign devices to them and test the connectivity inside a VLAN and between VLANs. You will configure e telnet access and will practice a password reset procedure. Finally, you will extend the VLANs which you created to a larger domain. You will observe how each of the networks (VLANs) can be extended to another switch but in the same time the security remains and no packets will be forwarded from one VLAN to another.

Exercise 1: Create VLANs, Assign ports and Test connectivity

1. Open <u>Cisco Packet Tracer</u> and add the following devices in the topology:
   - One switch (2960)
   - Four PCs (Generic)
   - One router (2911)
2. The PC numbers start from 0 but it will be easier for this task to change their numbers/names to start with 1. Change them as follows:
   a. Change the name of **PC3** to **PC4** (in the <u>Config</u> tab -> <u>Display Name</u>)
   b. Change the name of **PC2** to **PC3**
   c. Change the name of **PC1** to **PC2**
   d. Change the name of **PC0** to **PC1**

Now the end devices are named PC1, PC2, PC3 and PC4

3. Connect them as per the screenshot below:
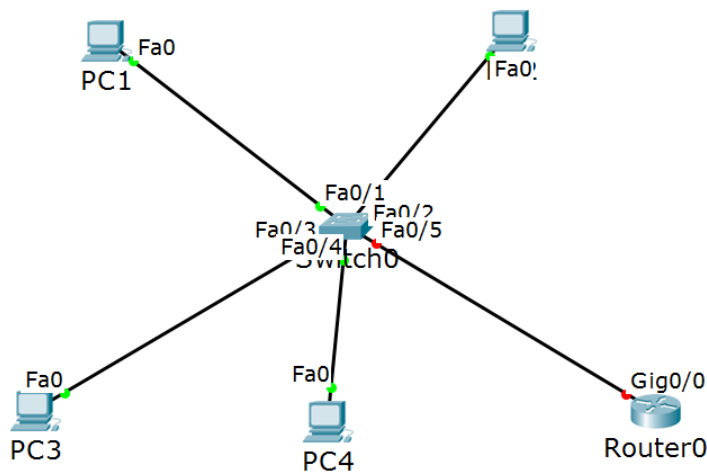
Note that Fa0/1 goes to PC1, Fa0/2 goes to PC2, Fa0/3 goes to PC3, Fa0/4 goes to PC4 and Fa0/5 goes to the router (So connect first PC1, etc. and lastly the router)

4. We will create two VLANs – VLAN 5 and VLAN 6. VLAN 5 will be associated with Fa0/1 and Fa0/2 (PC1 and PC2) and VLAN6 will be associated with Fa0/3, Fa0/4 and Fa0/5 (PC3, PC4 and the router)

- Open the CLI of the switch
- Navigate to global configuration mode (type **enable** and then **configure terminal**)
- Create the VLANs - type **vlan 5**, exit to global config mode again and type **vlan 6**. Type **exit** again.
- Associate the ports. Type the following commands:
    - interface fa0/1
    - switchport mode access
    - switchport access vlan 5
    - interface fa0/2
    - switchport mode access
    - switchport access vlan 5
    - interface fa0/3

- o switchport mode access
- o switchport access vlan 6
- o interface fa0/4
- o switchport mode access
- o switchport access vlan 6
- o interface fa0/5
- o switchport mode access
- o switchport access vlan 6
- o go to privileged exec mode (type **end**) and save the configuration by typing **write memory**

5. You will associate VLAN 5 with the network 10.5.5.0/24 and VLAN 6 with the network 10.6.6.0/24. If it is easier for you, you can color your topology and put informational text about the VLAN separation and the IP networks as per the screenshot below
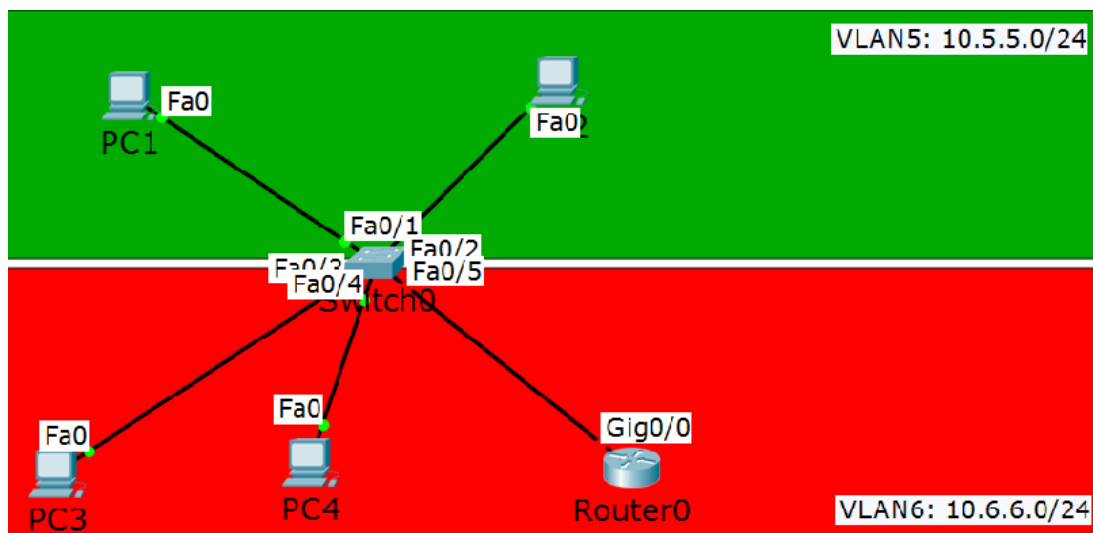
6. Assign the following addresses:

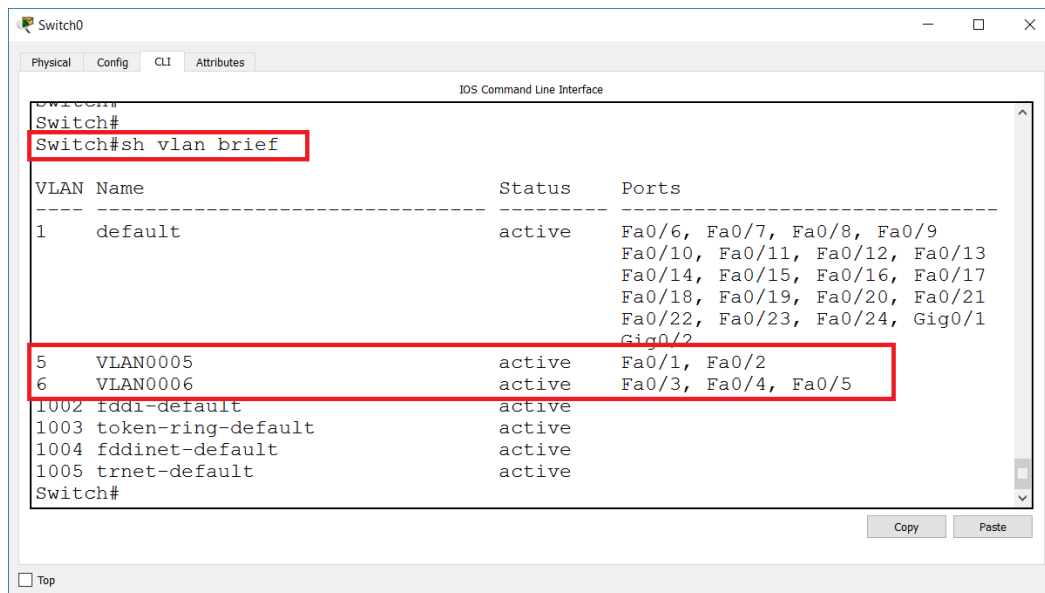| Device/Port	IP Address/Mask	Belongs to (informational only)
PC1/Fa0	10.5.5.1/24	Vlan 5

PC2/Fa0	10.5.5.2/24	Vlan 5
PC3/Fa0	10.6.6.1/24	Vlan 6
PC4/Fa0	10.6.6.2/24	Vlan 6
Router0/Gig0/0	10.6.6.3/24	Vlan 6

- To assign IP addresses on the PCs, go to the Config tab -> FastEthernet0
- To assign IP address on the Router, do the following:
  - Open the CLI and on the <u>Continue with configuration dialog? [yes/no]:</u> screen, answer **no**
  - Type **enable**
  - Type **configure terminal**
  - Type **interface gig0/0**
  - Type **ip address 10.6.6.3 255.255.255.0**
  - Type **no shut** to enable the interface (by default it is disabled)
  - Type **end** to go to privileged exec mode and type **write memory** to save your configuration
7. Change the <u>hostname</u> of the router by typing **hostname *Name*_Router0** from global configuration mode where for *Name* put your name. Save the configuration again - either type <u>**do** write memory</u> from the global configuration mode or exit to privileged exec and type **write memory**
8. Test the connectivity inside VLAN 5
   Open the CLI of PC1 (<u>Desktop</u> -> <u>Command Prompt</u>) and ping PC2 (10.5.5.2). Optionally, you can also ping PC1 (10.5.5.1) from PC2.

   Both pings should succeed since the devices are in the same VLAN and the same IP subnet!

9. Test the connectivity inside VLAN 6
   Open the CLI of PC3 and ping the other devices:
   - Ping PC4 (10.6.6.2)
   - Ping Router0 (10.6.6.3)

Again, the pings should succeed since the three devices belong to the same VLAN and the same IP network (subnet)

NOTE: If your pings are not successful, check your IP addresses and switch configuration. One useful troubleshooting command on the switch is **show vlan brief** where you can see the vlan to port associations. In the screenshot below they are correct

10. Test the connectivity between the VLANs
    Open the CLI of PC1 and try to ping the devices in VLAN 6 – PC3 (10.6.6.1), PC4 (10.6.6.2) and Router0 (10.6.6.3). The Ping should fail. Why?
11. (Optional) Try to bypass the VLAN security
    To do this, you will change the IP address of PC1. Assign an IP address of network 10.6.6.0/24 to PC1. For example, 10.6.6.10/24. Now try to ping again a device in VLAN 6 – PC3 (10.6.6.1). Did the ping succeed?
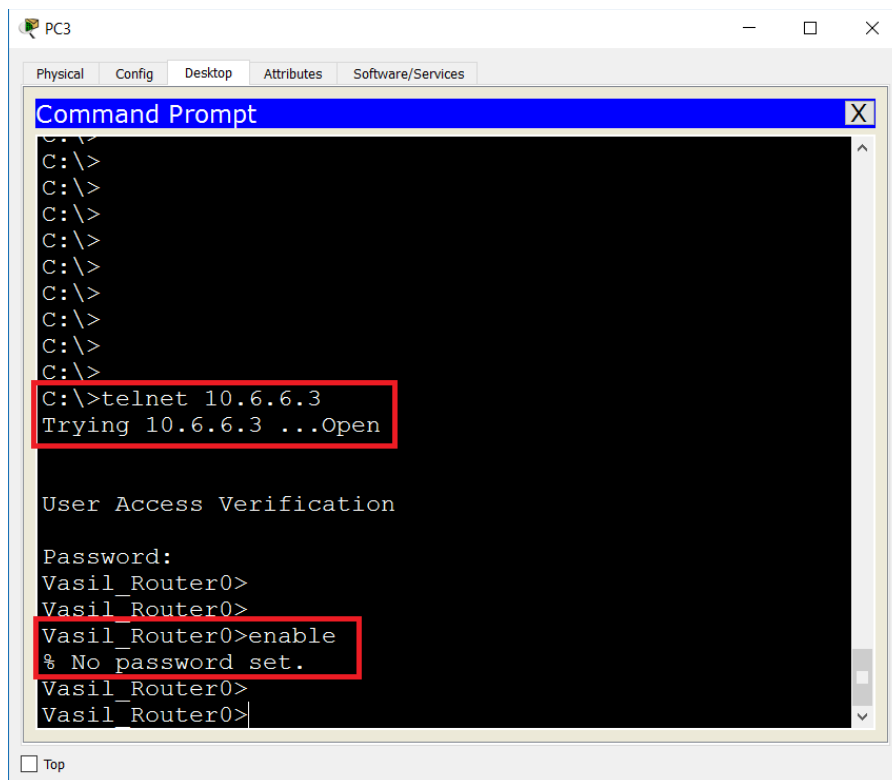   The ping should fail although PC1 and PC3 belong to the same IP network. The reason is that the switch isolates them at a lower OSI layer, layer 2 – they still belong to two different VLANs!

    Now, return the old address of PC1 – 10.5.5.1/24

Exercise 2: Configure Telnet

In this exercise, you will configure and test Telnet connectivity from PC3 (telnet client) to Router0 (Telnet server)

1. Login to the CLI of Router0 (*Name*_Router0). Go to the privileged exec mode (**enable** -> **conf t**) and
2. Enter the telnet (and ssh) configuration mode by typing **line vty 0 15**
3. Set a password. Type **password SoftUni** (case sensitive)
4. Go to the CLI of PC3 and establish a Telnet connection to the router: **telnet 10.6.6.3**. Enter the password that you configured in the previous step (SoftUni). Was the telnet successful? It should succeed. Now, from the telnet session, try to enter to the privileged exec mode. Type **enable**. It will refuse going to this mode because an <u>enable</u> password for the privileged exec mode has not been set
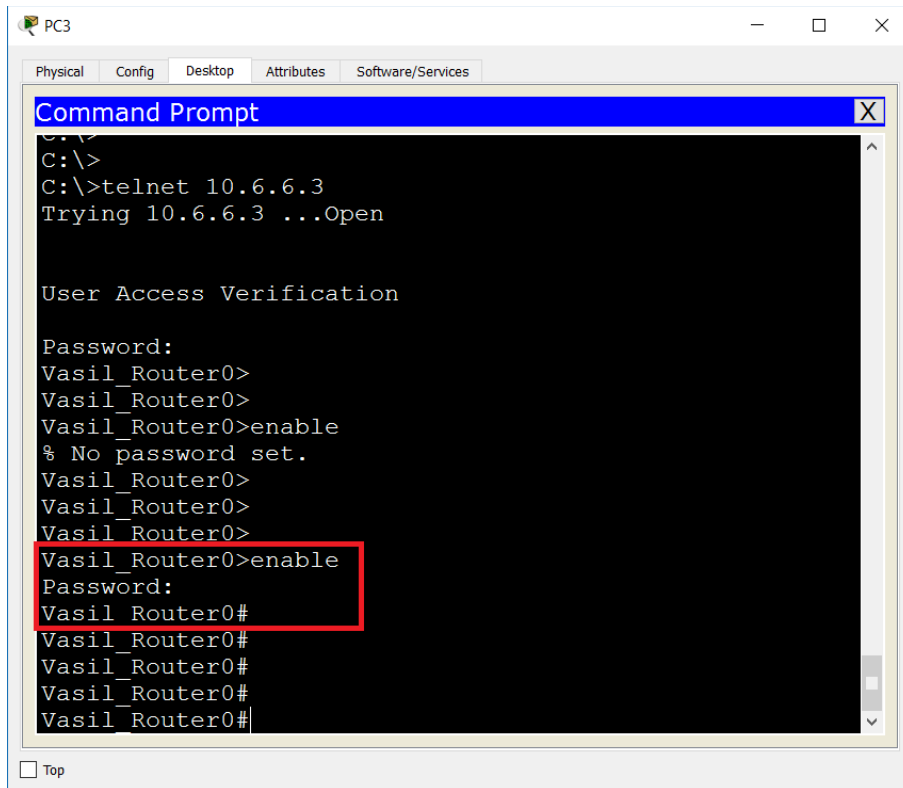
5. Go back in the CLI of the router. From the global configuration mode, type **enable secret 123**
6. Repeat the logon attempt from PC3. If you are disconnected, type again **telnet 10.6.6.3** and enter **SoftUni** as a password. Then type **enable** end use **123** as password to enter the privileged exec mode. It should now succeed and you should be in control of the remote router


7. Save your router configuration either from the Router itself or from the Telnet session where you are already in with read/write privileges. To save, type either **write memory** or **copy running-config startup-config** (and confirm the destination filename)

Exercise 3: Password Reset

In this exercise, we will pretend that you have forgotten your enable secret for the router (and you just have saved your configuration) and you have to reset it to a new one: **456**

You can either attach a PC with a console cable for the purposes of this password reset task or simply use the simulated router prompt which is provided from the Cisco Packet Tracer software (when you click on the router and go to the CLI tab). We will use the first option here since it is closer to the real world where you have to use a console connection.

1. Add another PC to the topology, PC5 and connect it to the router with a console cable. Select RS 232 and Console options when you connect the PC5 and the Router0 respectively
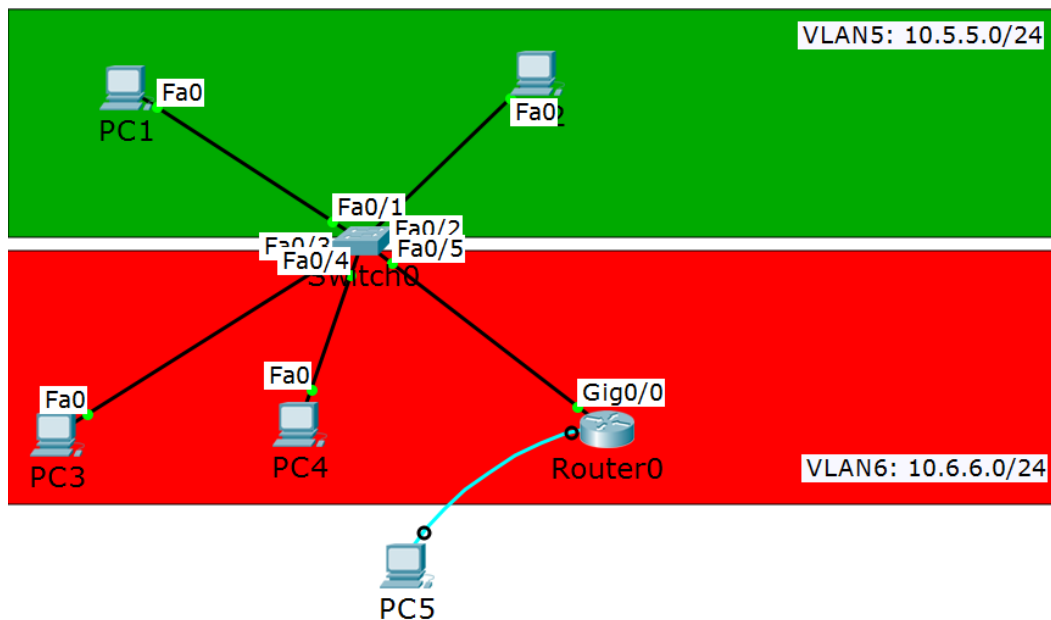
Note that PC5 does not belong to any VLAN, it is console connected to the router.

2. Open PC5, go to Desktop -> Terminal, accept the default terminal configuration settings and click OK
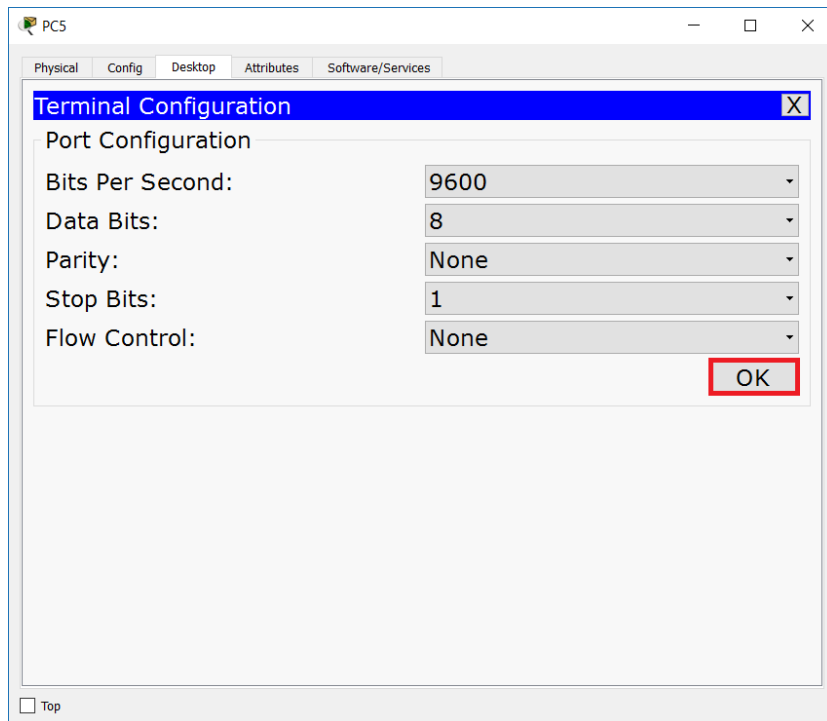
3. You should see the user exec mode now. If you are in another mode (like privileged exec or global configuration mode), go back to user exec (**exit**) because we want to pretend that we do not know the password

```
Vasil_Router0>
Vasil_Router0>
Vasil_Router0>enable
Password:
Password:
Password:
% Bad secrets

Vasil_Router0>
Vasil_Router0>
```

4. Go to Router0 -> Physical tab and then Shutdown the router from the button
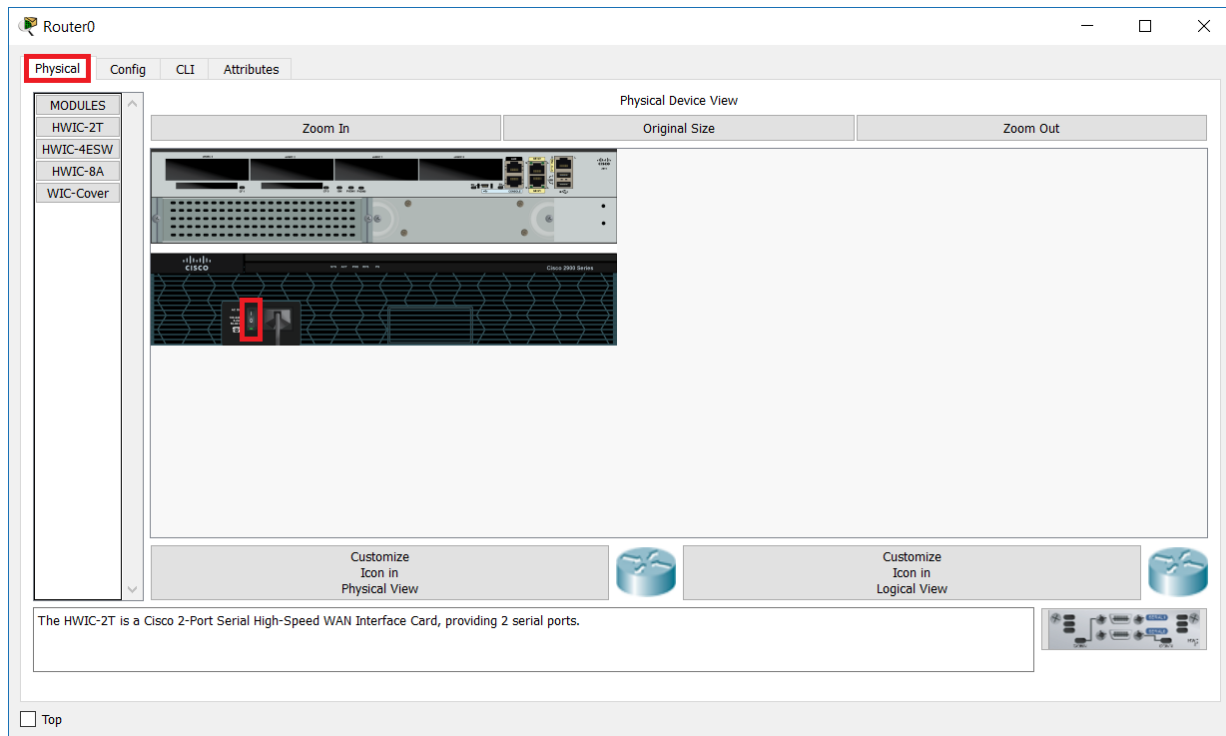
5. Prepare to power on the router using the same button. After you power it on, you have to be quick with the break sequence key combination from the terminal software in PC5. Click again to power on, switch to PC5 and press **CTR+SHIFT+F6+C** simultaneously to interrupt the normal boot and to go to the <u>rommon 1 ></u> prompt (if this combination does not work, try with **CTR+Pause**)

```
PC5                                                    —  □  ×

 Physical   Config   Desktop   Attributes   Software/Services

 Terminal                                                    X

 Press RETURN to get started.




 System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
 Technical Support: http://www.cisco.com/techsupport
 Copyright (c) 2010 by cisco Systems, Inc.
 Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
 CISCO2911/K9 platform with 524288 Kbytes of main memory
 Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

 Readonly ROMMON initialized

 program load complete, entry point: 0x80803000, size: 0x1b340
 program load complete, entry point: 0x80803000, size: 0x1b340

 IOS Image Load Test
 _____
 Digitally Signed Release Software
 program load complete, entry point: 0x81000000, size: 0x3bcd3d8
 Self decompressing the image :
 ###################
 monitor: command "boot" aborted due to user interrupt
 rommon 1 >

 □ Top
```
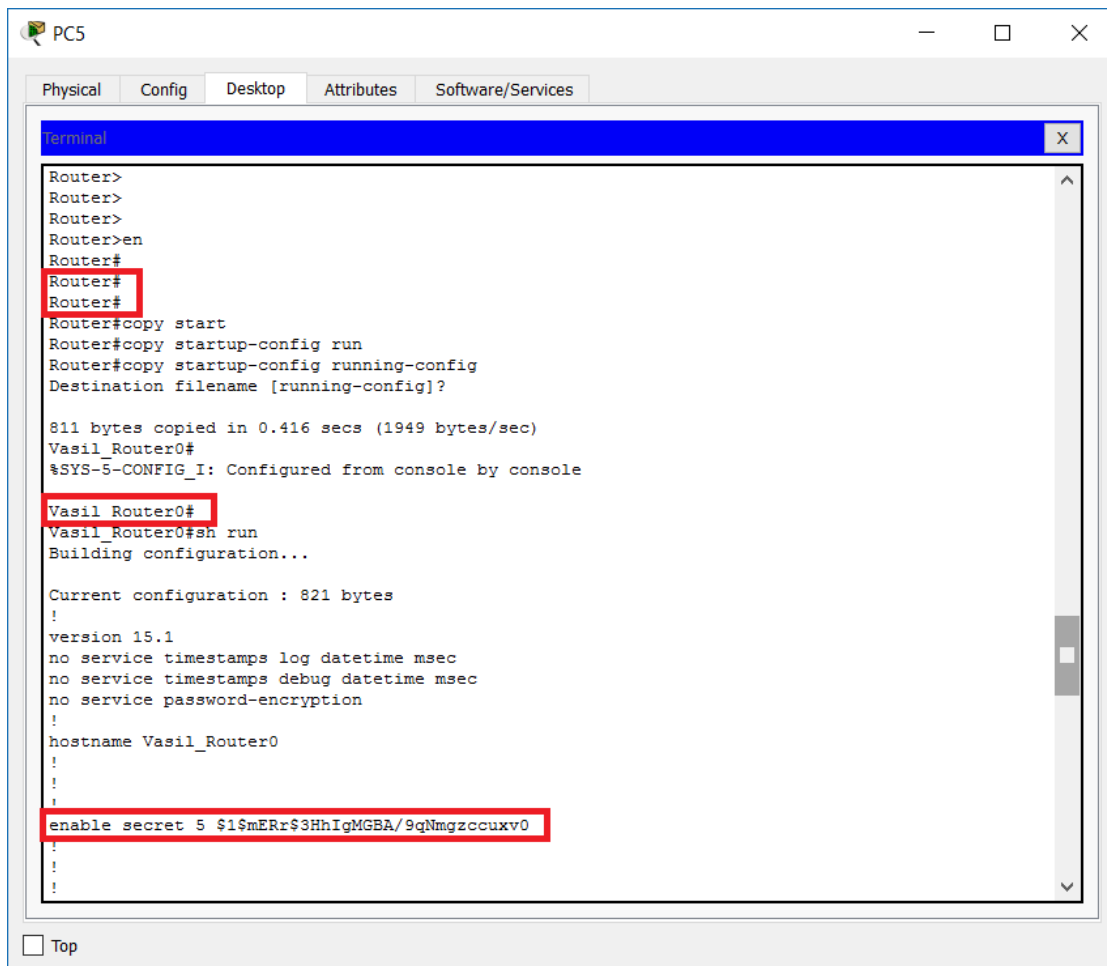
NOTE: If you missed it, repeat steps 4 and 5.

6. Type **?** to see the available commands. Note that one of them is <u>confreg</u>.
    Type **confreg 0x2142** and then **reset** to reboot the device

What is the meaning of this? The default configuration register setting is
0x2102 which instructs the device to read and load its configuration file from
the flash. When you change it to 0x2142, the device will boot bypassing its
configuration file. It is not deleted and is still in the flash, but we instruct the
device not to use it, because the password (which we do not know) is part of it.

7. After the reboot, observe that the router will prompt you <u>Continue with
    configuration dialog? [yes/no]:</u> since it loads without configuration. Answer
    with **no**

8. Type **enable**. You should NOT be asked for a password since this is a blank (default) configuration which does not include passwords

9. One more time, pay attention that the device is now without configuration. While in the privilege exec mode, you will load the configuration file in the RAM. Type **copy startup-config running-config** and confirm the destination filename. Now the old config should be loaded. To confirm this, please not the following:

   - The router name has changed – from the default **Router** to your previously configured and saved name **Name_Router0**
   - Type **show run** and note that the password (its hash) is in the running configuration! (You simply bypassed it)

10. And this is the trick for the password reset - you are now in a privileged exec mode, bypassing the enable secret password (with the confreg 0x2142

command), and you have privileges to either delete or change this password

11. Change the password to 456. To do this, go to global configuration mode (**conf t**) and type **enable secret 456**. Then, save your configuration by typing **do wr m** (the "do" is because you are in a different than privilege exec mode and "wr m" is abbreviated from "write memory")

12. Change back the configuration register to its default setting, 0x2102, instructing the device to load its configuration file from the flash memory on the next reboot. Type **config-register 0x2102** from the global config mode

```
!
line aux 0
!
line vty 0 4
 password SoftUni
 login
line vty 5 15
 password SoftUni
 login
!
!
!
end


Vasil_Router0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Vasil_Router0(config)#
Vasil_Router0(config)#
Vasil_Router0(config)#enable secret 456
Vasil_Router0(config)#
Vasil_Router0(config)#
Vasil_Router0(config)#do wr m
Building configuration...
[OK]
Vasil_Router0(config)#
Vasil_Router0(config)#
Vasil_Router0(config)#
Vasil_Router0(config)#confre
Vasil_Router0(config)#config
Vasil_Router0(config)#config-register ?
  WORD  Config register number
Vasil_Router0(config)#config-register 0x2102
Vasil_Router0(config)#
Vasil_Router0(config)#
```
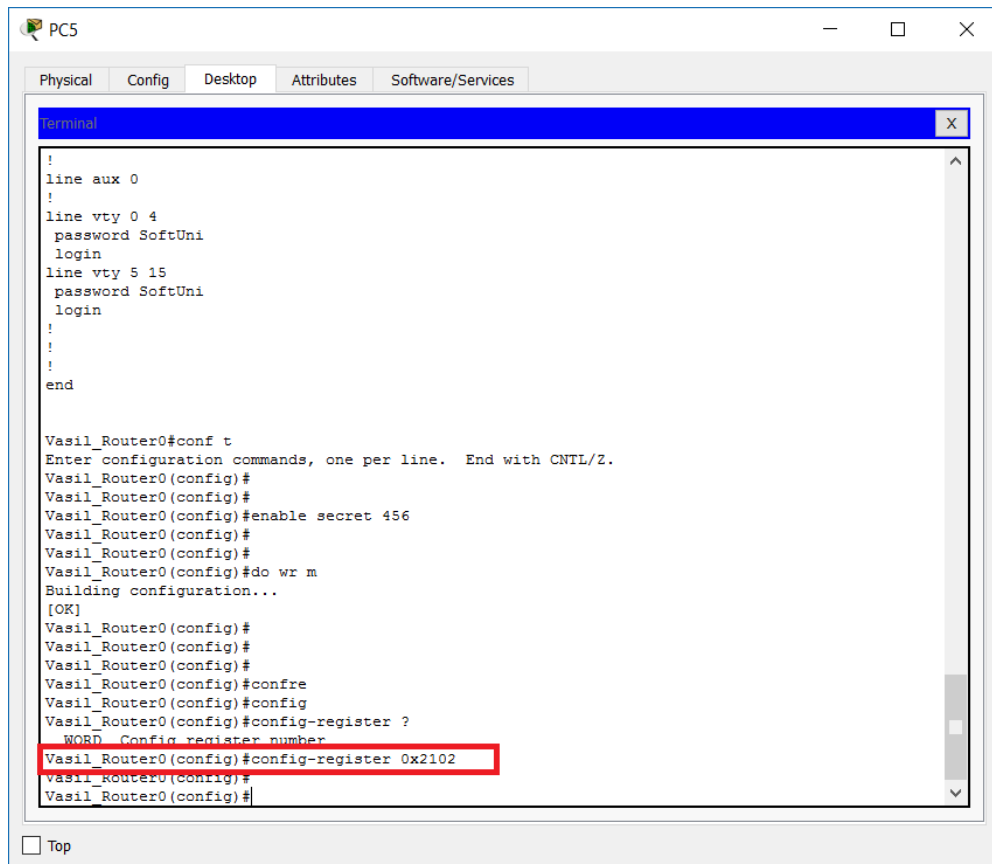
13. Optionally, you can check the configuration register setting by typing **show version** (or **do show version** if you are still in the global config mode). Notice the result

```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#    PID                   SN
-------------------------------------------------
*0         CISCO2911/K9          FTX1524B6W3


Technology Package License Information for Module:'c2900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current      Type            Next reboot
----------------------------------------------------------------
ipbase        ipbasek9     Permanent       ipbasek9
security      disable      None            None
uc            disable      None            None
data          disable      None            None

Configuration register is 0x2142 (will be 0x2102 at next reload)

Vasil_Router0(config)#
```

14. Reboot the router with the **reload** command
15. After the reboot, type **enable** and login with the new password **456**
   This confirms that the password has been successfully reset.
16. Delete the enable secret password. To do this, type **no enable secret** from global configuration mode. Save your config.

Exercise 4: Extend the broadcast domains (VLANs) with a trunk link

In Task 1, you created two VLANs and assigned access (untagged) ports to each of them. Now we want to extend these VLANs to another switch. For this purpose, you will use trunk between the switches.

1. Add three more devices in your topology: one switch (2960) and two end devices (Generic). Connect the end devices to the new switch (Switch1) and then connect the Switch1 to the other switch, Switch0. Either use the Auto

connection type or select the cables manually. Note that you have to use cross-over cable for the connection between the switches
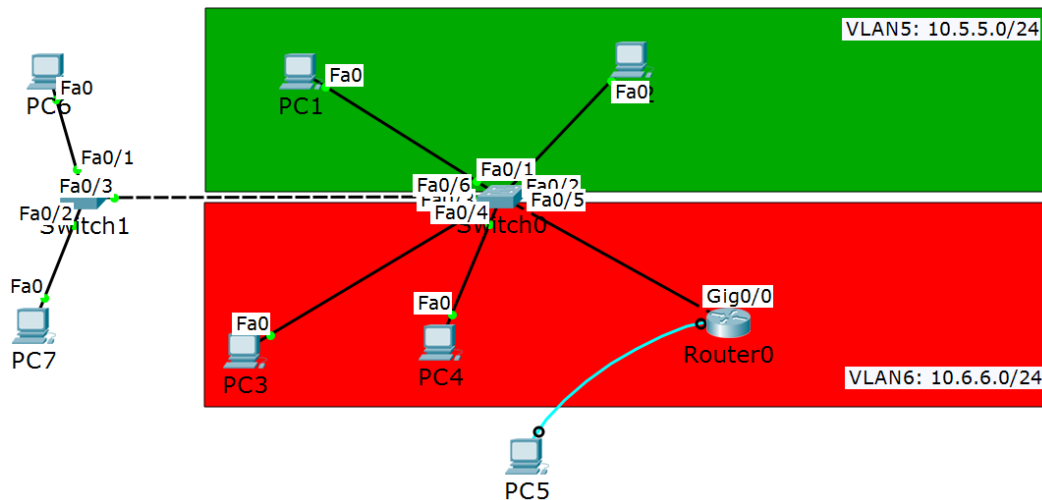
2. Now you will assign port Fa0/1 on Switch1 to VLAN5 and port Fa0/2 to VLAN6. This means that PC6 will belong to VLAN5 and PC7 – to VLAN6 Login to Switch1 and do the following:
   - Change the hostname to Switch1. Type **hostname Switch1** from global config mode
   - Create the VLANs - type **vlan 5**, exit to global config mode again and type **vlan 6**. Type **exit** again
   - Associate the ports in Switch1
     o interface fa0/1
     o switchport mode access
     o switchport access vlan 5
     o interface fa0/2
     o switchport mode access
     o switchport access vlan 6
     o interface fa0/3
     o switchport mode trunk

     Note the last two commands: Interface fa0/3 is connected to the other switch and must carry all VLANs, that is why you configure it as a trunk
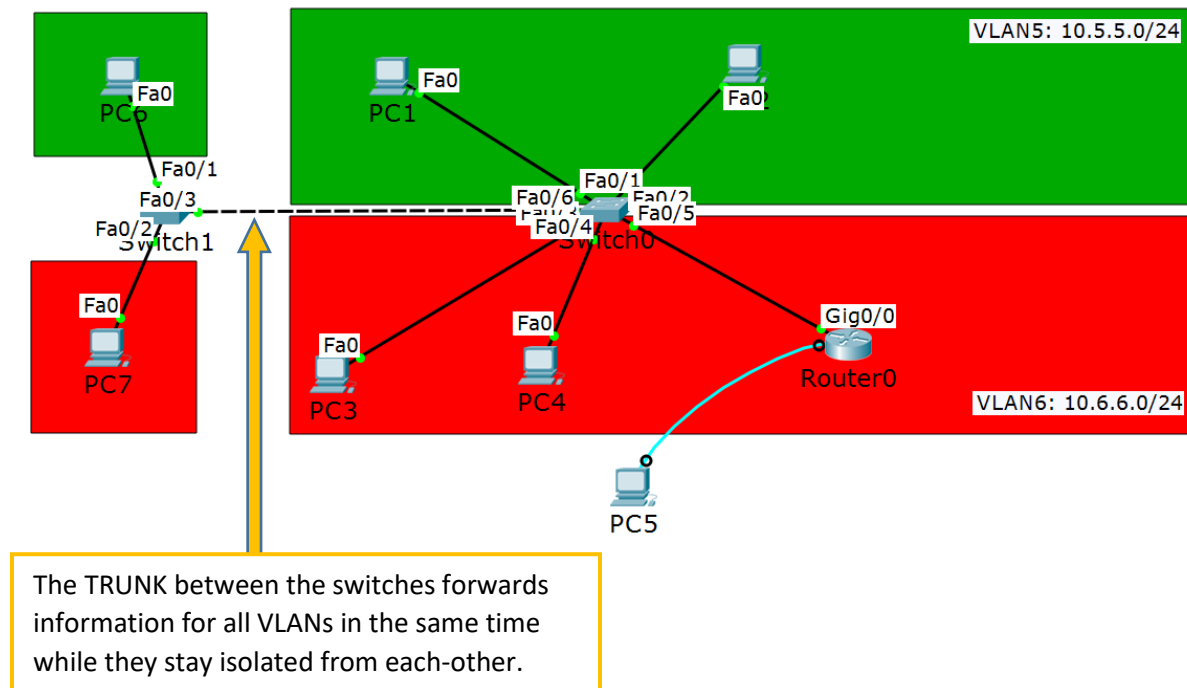
   - Associate the trunk port on Switch0

- o interface fa0/6 (from global config mode)
- o switchport mode trunk

3. Assign the following addresses

Device/Port	IP Address/Mask	Belongs to (informational only)
PC6/Fa0	10.5.5.5/24	Vlan 5
PC7/Fa0	10.6.6.6/24	Vlan 6

4. Now PC6 belongs to VLAN5 and PC7 belongs to VLAN6 and we still have two broadcast domains. The VLANs were extended across the switches because of the trunk

The TRUNK between the switches forwards information for all VLANs in the same time while they stay isolated from each-other.

5. Test the connectivity inside VLAN 5
   Open the CLI of PC6 (Desktop -> Command Prompt) and ping PC1 (10.5.5.1) and PC2 (10.5.5.2).

Both pings should succeed since the devices are in the same VLAN and the same IP subnet – although they are distributed between different switches, they still belong to the same virtual network.

6. Test the connectivity inside VLAN 6
Open the CLI of PC7 (<u>Desktop</u> -> <u>Command Prompt</u>) and ping PC3 (10.6.6.1), PC4 (10.6.6.2) and Router0 (10.6.6.3).

Again, all pings should succeed since the devices are in the same VLAN and the same IP subnet – although they are distributed between different switches, they still belong to the same virtual network.
In addition, you can try to telnet to the router (10.6.6.3) - it should succeed (with the password **SoftUni**). Now you should not be able to go to privileged exec mode since no password exist at the moment – you deleted it in Task 3, step 16.

NOTE: If you have troubles pinging and telnetting to the router, check if the interface GigabitEthernet0/0 is UP. To do it, type **show ip interface brief**. If it is disabled (administratively down), go to the interface configuration mode and type **no shutdown**. Check again the status and save the configuration.

7. Try to connect between the VLANs
Try to ping any PC in VLAN6 from VLAN5 and vice-versa. Also, try to telnet to Router0 from any device in VLAN5 (PC1, PC2 or PC6). These attempts will be unsuccessful. This is expected since the VLANs provide Layer 2 isolation and security.

If you want to connect between the VLANs, a Layer 3 device (Router or L3 Switch) is required to be configured to <u>route</u> between these different networks. This will be discussed in a later module of the training.

Exercise 5: Save your LAB

In later modules, you may need this topology and configurations, so it is better to save the whole LAB now. In the Packet Tracer, go to <u>File</u> -> <u>Save As...</u> and save it as LAB 3.pkt on your local disk.

You have completed LAB 3.