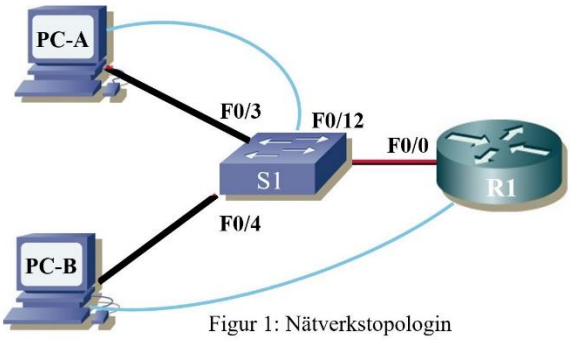
Kommunikationsnät
(Nätverkslabb 1)

Yasir Riyadh (KTH 2022)

Step 1 - Connect cables

a) The first step would have been "Start by connecting all the cables according to the topology above and turn on the power of the router and the switch." but due to the ongoing pandemic, the teachers have connected all the cables in the cross-connection room. It is possible to look into the cross-connection room if it is vacant!



Figur 1: Nätverkstopologin

Tabell 1: Namn och nätverksadresser till de olika nätverksenheterna

Enhet	Interface	IP-adress	Subnetmask	Default
R1	F0/0.1	192.168.1.1	255.255.255.0	N/A
	F0/0.10	192.168.10.1	255.255.255.0	N/A
	F0/0.20	192.168.20.1	255.255.255.0	N/A
S1	VLAN1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1

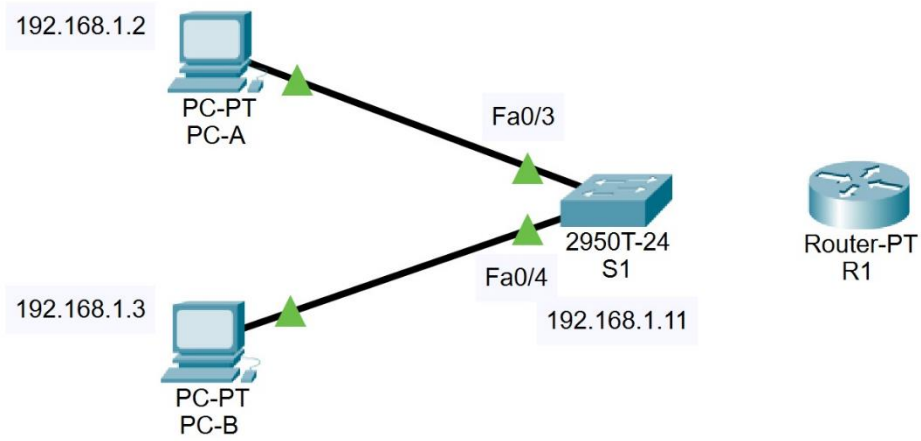
Step 2 - Configure the network settings on the computers

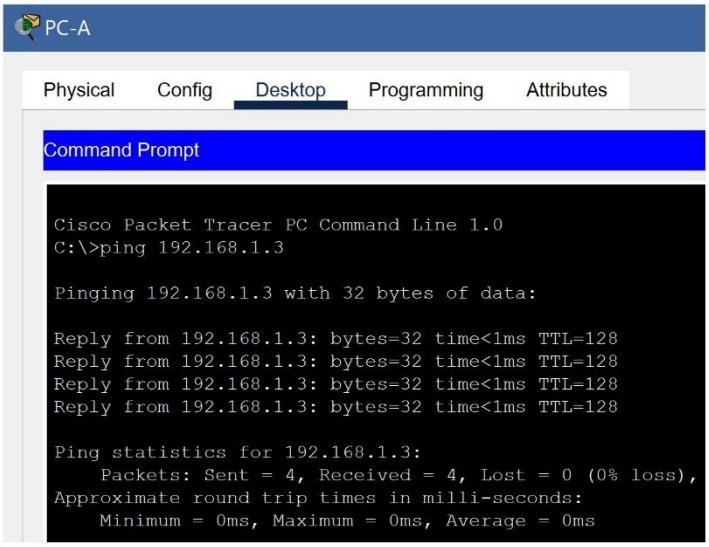
a) Configure the IP address, subnet mask and default gateway on the computers (PC-A and PC-B) according to the table on page 2.
Click Start on the computer and then select Settings -> Network & Internet -> Change adapter options -> Ethernet. Right-click on the Ethernet icon and select Properties, Internet Protocol Version 4 (TCP / IPV4) and then PROPERTIES, Fill in the IP address, subnet mask and default gateway.

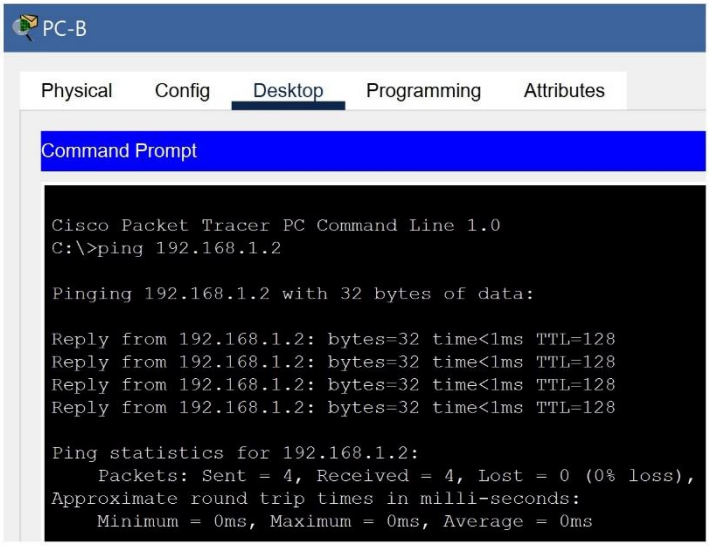
b) When the configuration of the computers is complete, it is important to test so that the network basically works. The Ping command in the command prompt on your computer is a useful tool for testing your network connection.

c) Test that PC-A accesses PC-B with the command from the previous step.

This should work, do not do so, check configuration again. (No need to move on to the next step if this does not work.)







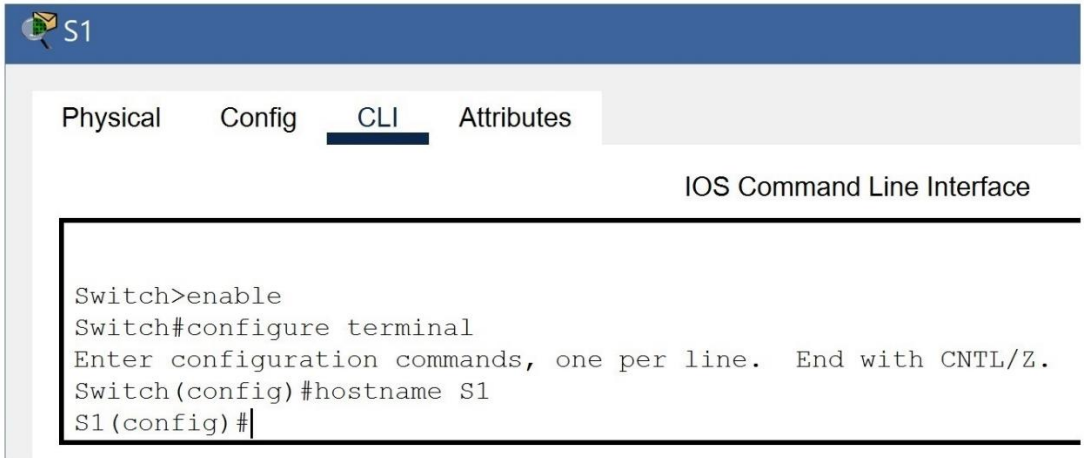
Step 3 - Configure the switch

The switch needs an IP address to be configured and monitored remotely. The configuration takes place in the switch's IOS (operating system) and has a command-interpreter-like design. Easy for those who know it, but a big question mark for the beginner. The model is based on the fact that there are different levels for different settings. When you start and log in to your router or switch, you are now at the lowest IOS mode level. This can be seen at the router / switch prompt. When you are at this level, the prompt has the following appearance: **Router>** We should not do anything there so we do not need to touch it. To get to the intermediate level, type **enable** and then return. Then the prompt will change from **Router>** to **Router #** Then you know that you are in the right position. If you want to go back to the previous level, write **exit**. If we got it right (without problems) then you can check the settings with the command **show running-config** which can be written in short form: **sh run**. At this level we can not change any settings but we have to navigate to the next level called Global configuration mode. To get to this level we need to type the command **configure terminal**. The same command can be written in short form **conf t**. Now the prompt should be changed to **Router (config) #**. Telnet and SSH are the two most common methods of remote configuration. However, Telnet is not a secure protocol. All information sent between the connected devices is sent in clear text and password and other sensitive information can then be read by a packet sniffer (in our case the program Wireshark). During the lab, the Wireshark program will be used to analyze data traffic. However, the switch initially has no IP address and then only needs to be configured via a terminal program. In our case, the **TeraTerm** program that you find on the desktop of your computer.

a) Start the TeraTerm program and if it is not already preselected, select **Serial** and the port labeled **USB-Serial CH340**.
b) After the switch has started, you answer **NO** to the question "Would you like to enter the initial… ..". If you do not see anything happening on the terminal, you may need to press the **Enter** button to wake the device.
c) Now enter the command to go to **privileged EXEC mode** on the switch
d) And then enter the command to go to **global configuration mode**.
e) Set the name of the switch to **S1**

F1 Vilket kommando används för att sätta namn(hostname) på en enhet(Cisco router eller Switch)?

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```



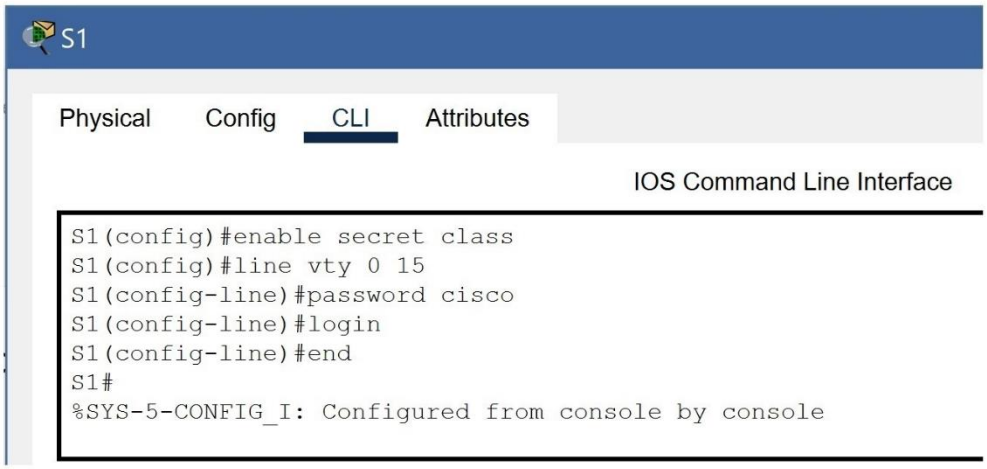
Before you can configure the switch S1 remotely, you must set a password and assign the switch IP address. The IP address of the switch will be assigned to the VLAN 1 interface.

a. Assign the **class** password on the switch to reach the privileged EXEC mode access level.

S1 (config) # enable secret class

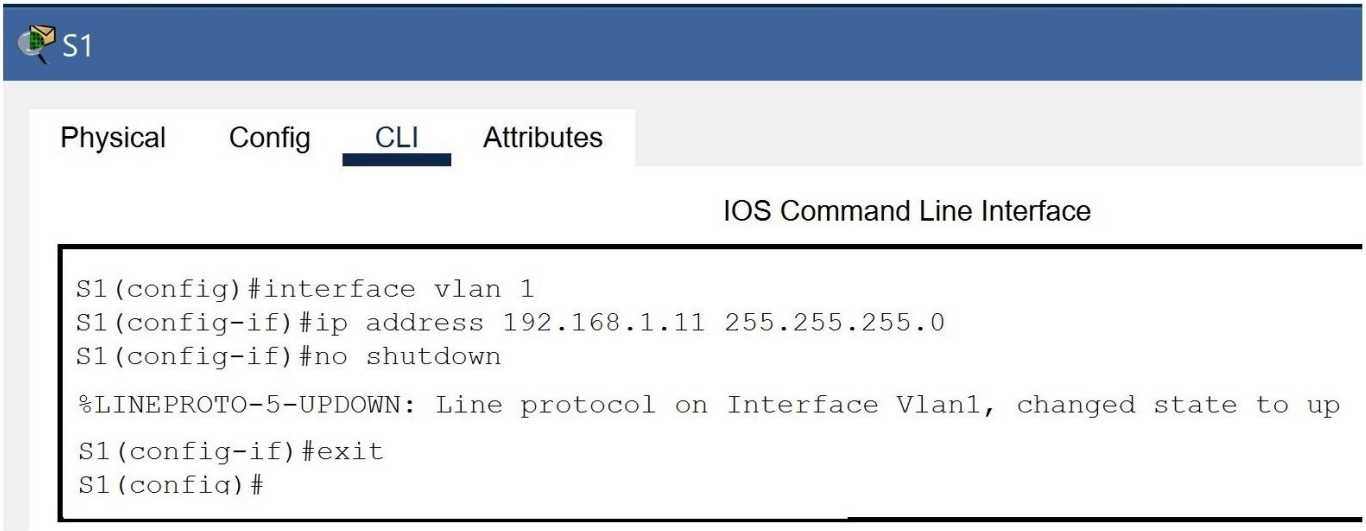
b. Also configure the virtual terminal (VTY) service to allow Telnet connections (for remote configuration) to the switch. (**line vty 0 15** means that a total of 16 simultaneous active connections)

S1 (config) # line vty 0 15
S1 (config-line) # password cisco
S1 (config-line) # login
S1 (config-line) # end



c. Now we need to put an IP address on interface **VLAN 1** to be able to communicate with the switch over the network

S1 (config) # interface vlan 1
% LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
S1 (config-if) # ip address 192.168.1.11 255.255.255.0
S1 (config-if) # no shutdown
S1 (config-if) # exit
S1 (config) #



d. With the following command, you can see the current configuration of the switch

S1 # show running

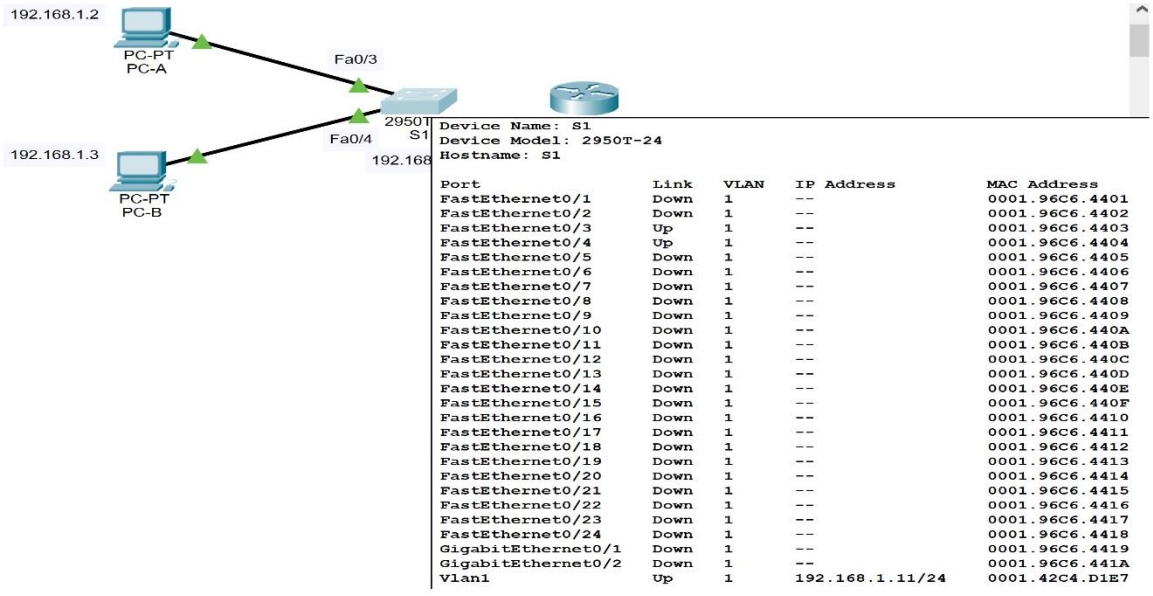
S1

Physical Config CLI Attributes

IOS Command Line Interface

```
S1#show running
Building configuration...
Current configuration : 1171 bytes
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname S1
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
!
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

e. How many interfaces does the switch have? **3 up (Fa0/3, Fa0/4, VLAN1)**



Step 4 - Level of security?

In this part, the security of the communication between the computer and the switch must be examined when the switch is configured remotely over Telnet. Sending encrypted information, especially passwords, is very important, as it is quite easy to intercept data traffic, especially in an unencrypted wireless network. The goal of this step is to find out the password to the switch m.h.a. program wireshark.

a) Start Wireshark on the computer where the network program Telnet is intended to run to log in and communicate with the switch. Start with Wireshark by selecting **Capture-> Options** in Wireshark. Then select **Ethernet** and then **start**.

a) To start a connection to the switch with the Telnet program, select in the **TeraTerm : File -> New Connection -> TCP / IP** and then enter the IP address of the switch. Make sure Telnet is checked in the This should work box, if not, check the connection and configuration again. (No need to move on to the next step if this does not work.)

b) Now enter the password **cisco** in Telnet and press the Enter button. Stop recording packets in Wireshark and locate packets sent **from** the computer **to** the **TELNET** switch. Each keystroke (ie each character) on the Telnet terminal is sent as a separate packet to the switch.

Select the different TELNET packages in Wireshark and look at the data load named with TELNET (in the lower half of the screen) to find out the password. You may need to expand **Telnet** by clicking the> sign next to it. Can you see in the packages what the password is?

c) Shut down the Telnet session with the exit command and return to communication with the switch via the console cable.

F2 Telnet turns out to send passwords in plain text. What / what other / other protocol could you use to encrypt the connection between a router / switch and a computer when configuring it?

Secure Shell Protocol (SSH)

Step 5 - Implement port security

In this step, you will configure and verify port security on a switch. Port security allows you to restrict a port's incoming traffic by restricting the MAC addresses that may send traffic to the port. In this step, the task is to let the switch learn about the MAC address of the connected computer connected to a specific port on the switch. Should another device with a different MAC address connect to the switch on the same port, data traffic will not be allowed.

S1(config)# interface vlan 1

a) On switch S1, enable port security on Fast Ethernet ports 0/3 and 0/4 by entering the following commands

S1 (config) # interface range f0 / 3 - 4
S1 (config-if-range) # switchport mode access
S1 (config-if-range) # switchport port-security

b) Set the maximum value so that only one device can access the respective Fast Ethernet ports 0/3 and 0/4. That is, a device's MAC address is registered on the port that can then use it.

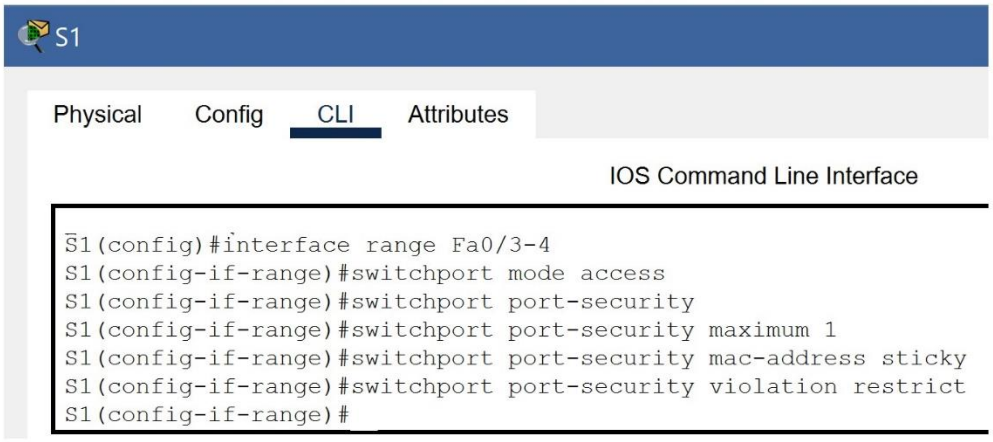
S1 (config-if-range) # switchport port-security maximum 1

c) Make sure that the Fast Ethernet ports on the switch learn the connected computer's MAC address "dynamically" and add it to the current configuration.

S1 (config-if-range) # switchport port-security mac-address sticky

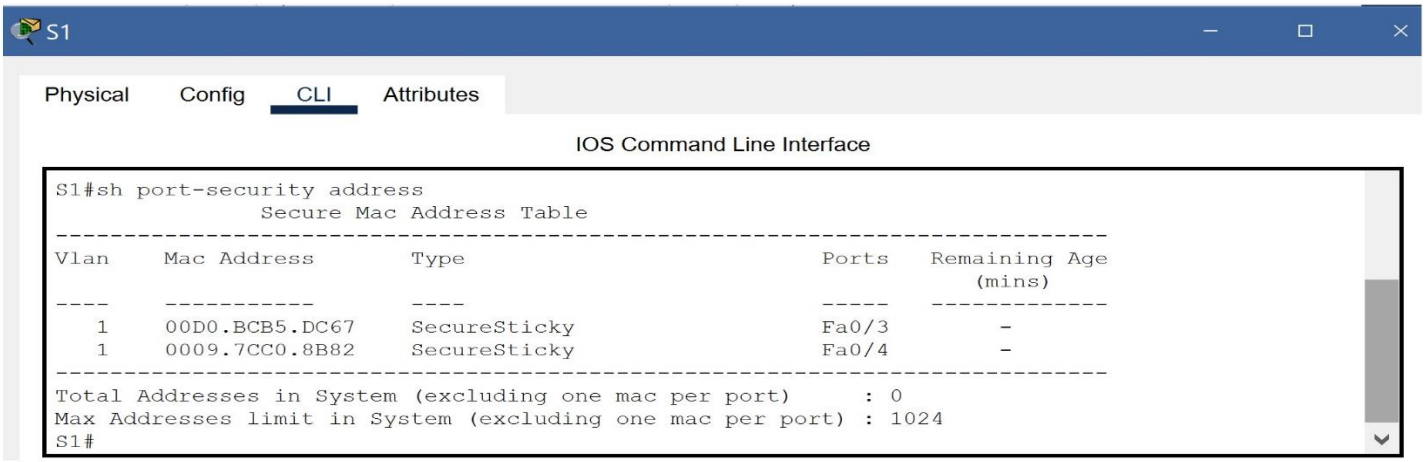
d) Set the violation mode so that the Fast Ethernet ports 0/3 and 0/4 are not deactivated when a violation occurs, but a message about the security violation is generated and data packets from the unknown source are discarded, ie all data traffic from the device with an unauthorized MAC address is thrown.

S1 (config-if-range) # switchport port-security violation restrict



e) Now use the show port-security address command to display the configuration information.

S1 # sh port-security address



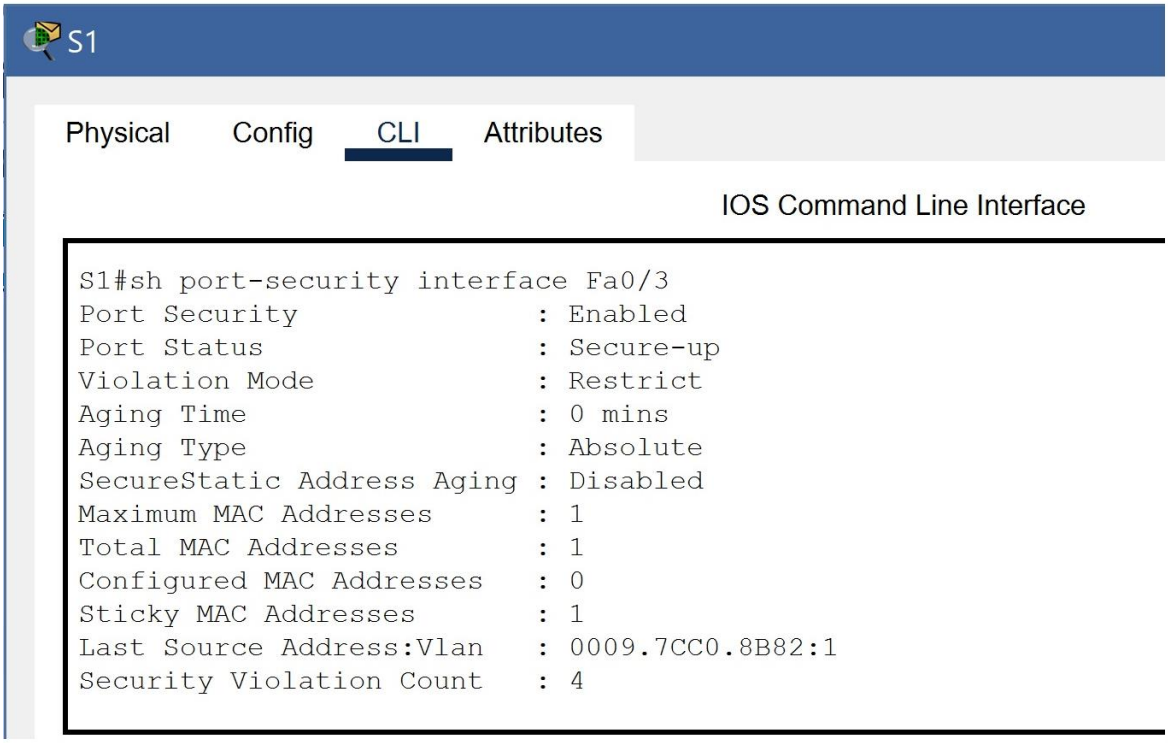
f) To create a breach, switch so that PC-A is connected to port F0 / 4 and PC-B is connected to port F0 / 3 on the switch. Now ping again from PC-B to PC-A. It should not work and generate a warning message on the switch that a violation has occurred

```
S1#
00:21:13: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 5cf9.dde6.3e38 on port FastEthernet0/3.
```

The MAC address learned for a particular port on the switch no longer matches what it initially learned and thus will not accept any data packets from unknown MAC addresses that are not "set" for a particular port on the switch.

g) Show the port security violation for the port to which PC-B is connected on the switch.

S1 # sh port-security interface f0 / 3



h) With this simple method, you can increase security a little so that anyone can not connect. Switch back to PC-A connected to F0 / 3 and PC-B to F0 / 4. It should be possible to ping between the computers again. If you want to clear the learned MAC address, you can use the following command.

S1 # clear port-security all

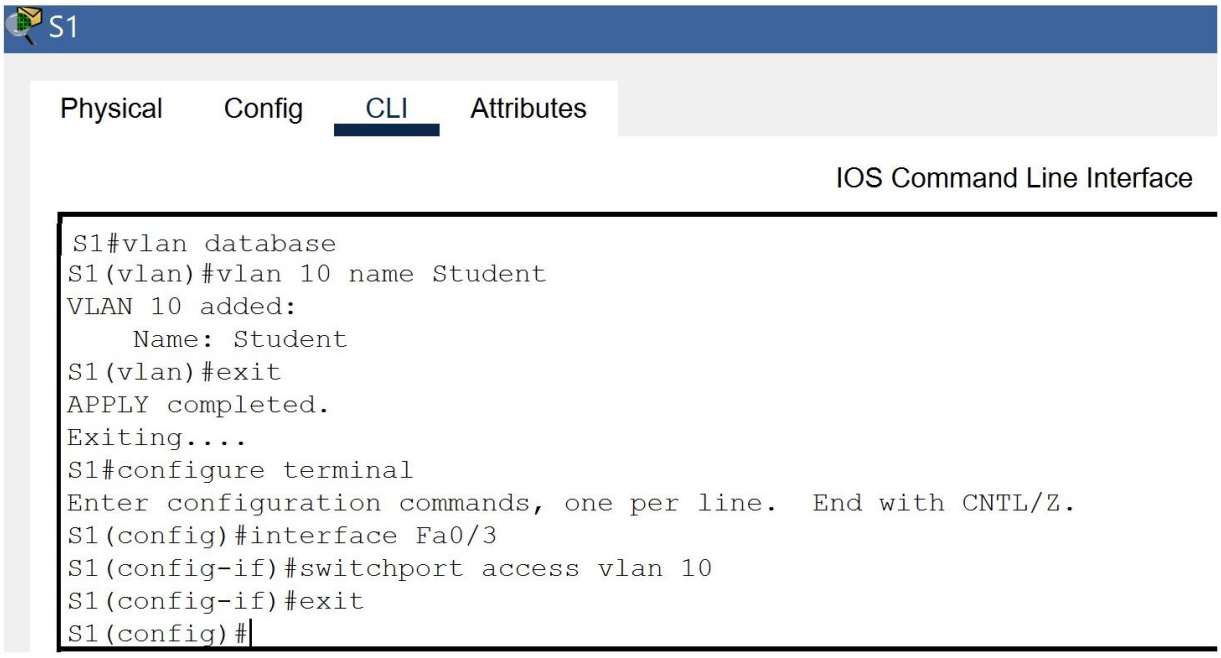
Step 6 - Create VLAN on switch S1

In step 6, you will create two different VLANs on the switch: first Student and then Faculty. You will then assign the specified VLAN to the correct interface on the switch. Feel free to use the show vlan command to verify your settings.

F3 What commands are used to assign a VLAN to an interface and specify how to name a VLAN?

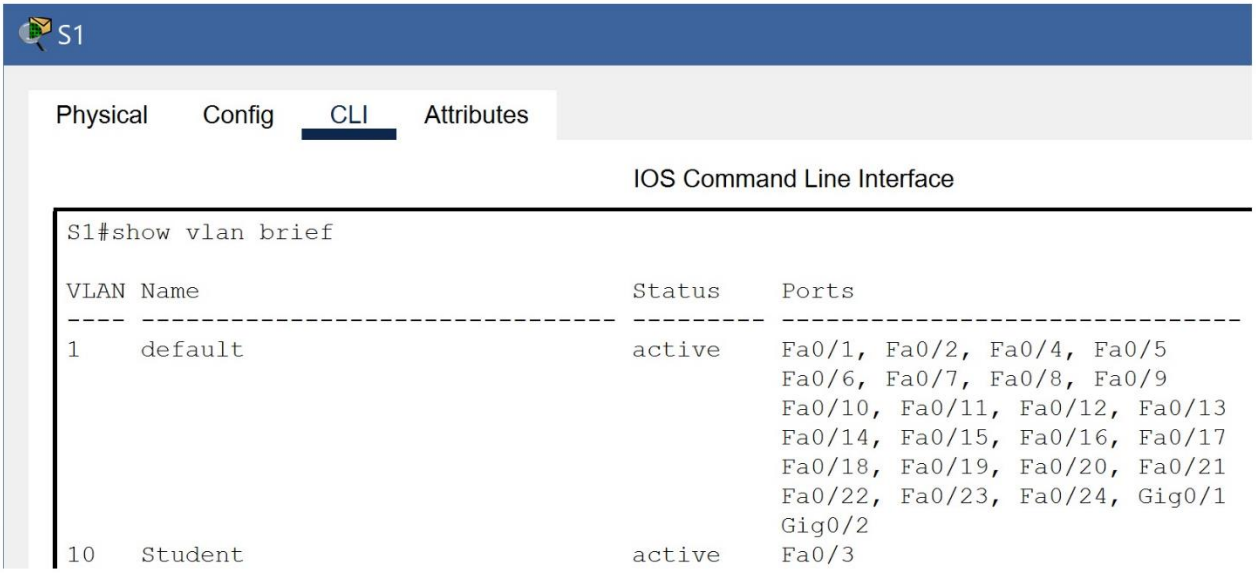
```
S1# vlan database
S1(vlan)# vlan 10 name Student
S1(vlan)# exit
S1# configure terminal
S1(config)# interface FastEthernet0/3
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
```

a) Create and name VLAN 10 for Student and configure the interface fastethernet0 / 3 and the fixed network 0/4 with the affiliation VLAN 10.



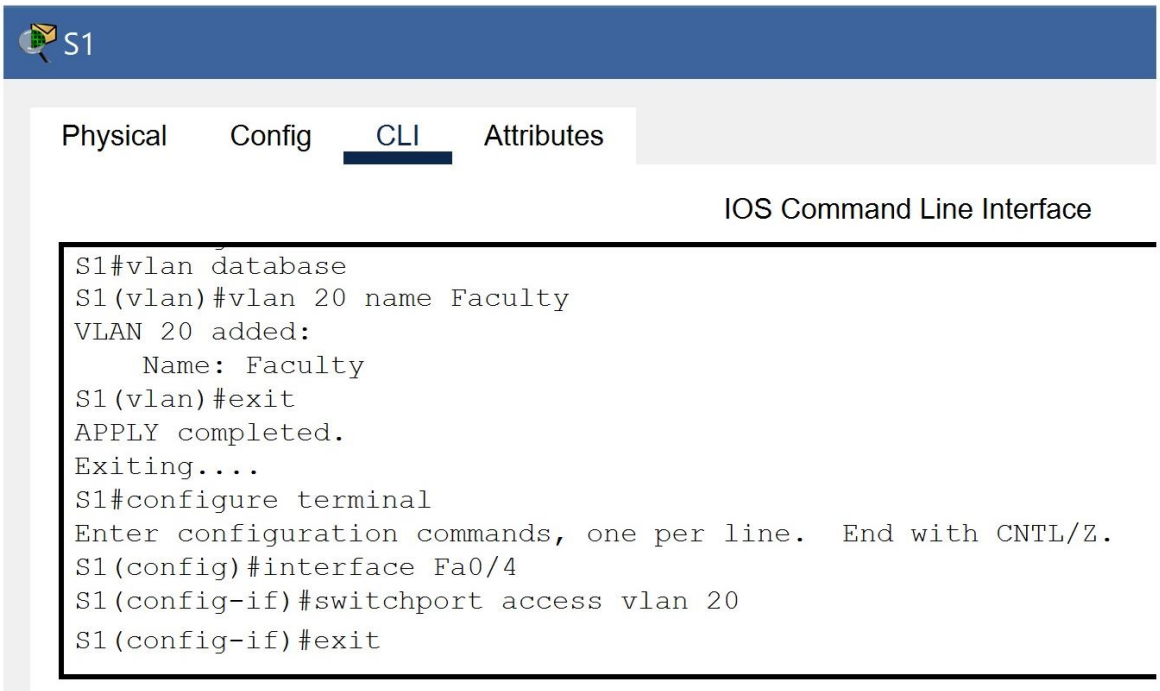
b) Enter the show vlan brief command to display the list of VLANs on S1.

S1 # show vlan brief



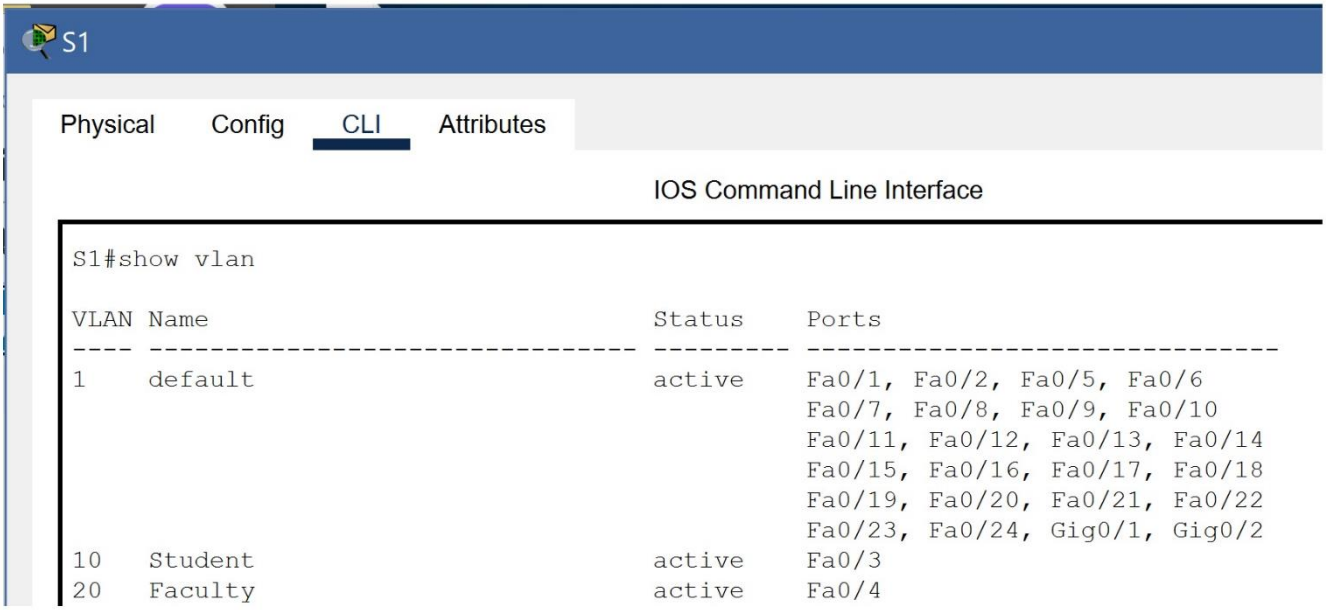
c) Test that PC-A accesses PC-B with the ping command on PC-A. This should work.

d) Also create VLAN 20, name the VLAN to Faculty and configure so that the interface fastethernet 0/4 belongs to VLAN 20.

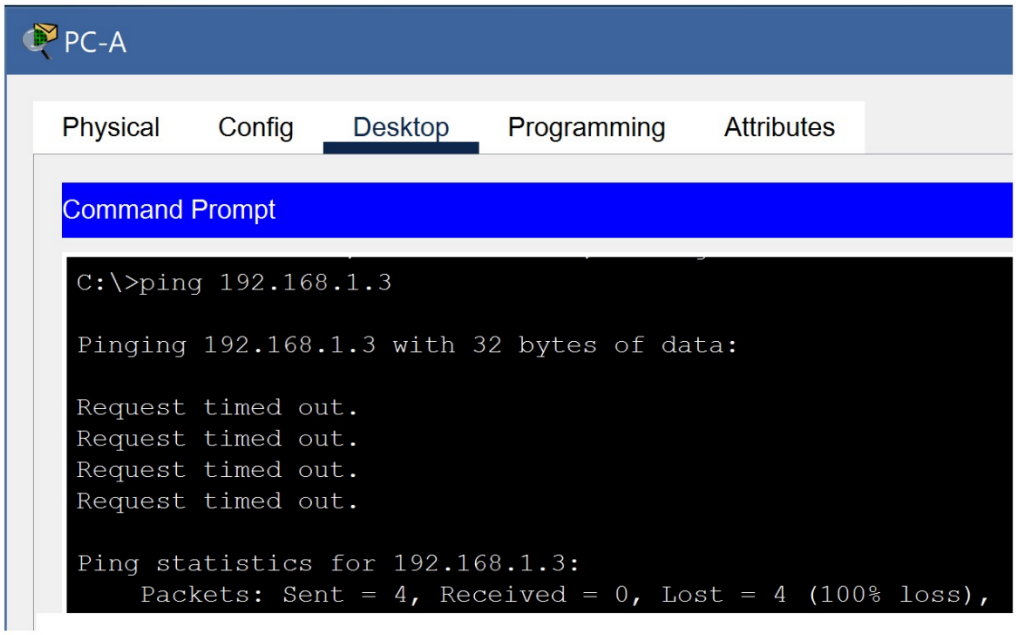


e) Enter the show vlan brief command to display the list of VLANs on S1.

S1 # show vlan



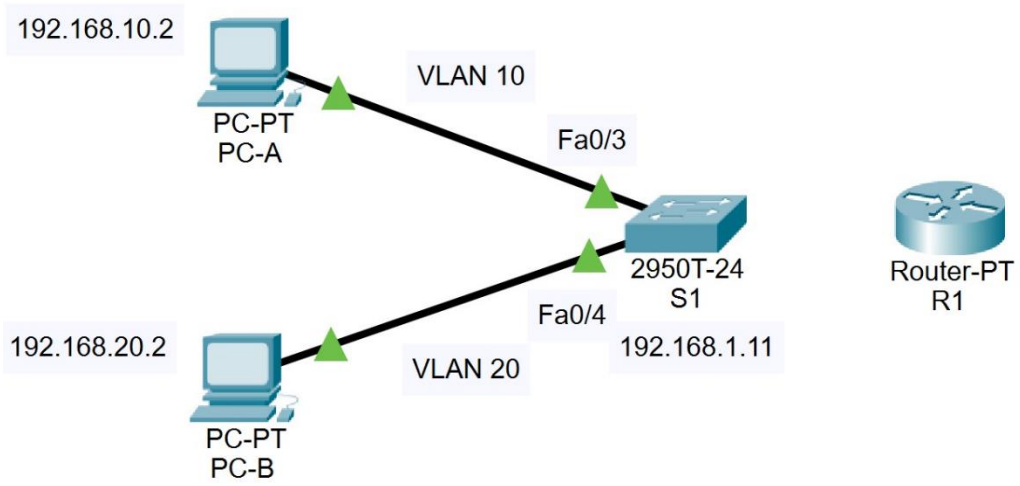
f) Now test again if PC-A can access PC-B with the command ping on PC-A. This should NOT work.



Now that we have moved PC-B to VLAN 20, ie changed the VLAN affiliation on port f0 / 4 to VLAN 20, ping should not work as PC-A and PC-B are connected on different VLANs (student and faculty) and the units can do not communicate between different VLANs. Time to get a network with two VLANs that can communicate with each other via a router.

All devices located on the same VLAN must belong to the same network address.
PC-A is connected to VLAN 10 and PC-B is connected to VLAN 20 and must then belong to different network addresses.
VLAN 10 belongs to the network address 192.168.10.0/24 and VLAN 20 to the network address 192.168.20.0/24. In the next step, both PC-A and PC-B will change the IP address so that they belong to the correct network address.

g) Change the address of PC-A to 192.168.10.2 and default gateway to 192.168.10.1 and PC-B to 192.168.20.2 and default gateway to 192.168.20.1. The subnet mask is the same as before 255.255.255.0. Note that the default gateway address is on the same network address as the computer.



Step 7 - Create Trunk on Switch

Trunks are connections between switches and / or routers that enable the switches to exchange information about any VLAN. By default, a trunk port belongs to all VLANs.

F4 In data communication, what is the Trunk method used for and describe the benefits of this technology.

Trunk provides VLAN identification for frames traveling between switches to support VLAN traffic

F5 A switch must also support what is called NATIVE VLAN. What is it intended to be used for?

NATIVE VLAN is VLAN into which traffic without a VLAN tag will be put when it's received on a trunk port

F6 What commands should be used to configure an interface to the trunk?

```
S1# configure terminal
S1(config)# interface fa0/12
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

a) Konfigurera trunk på interface fastethernet 0/12 på switchen.

Step 8 - Configure the router with IP addresses

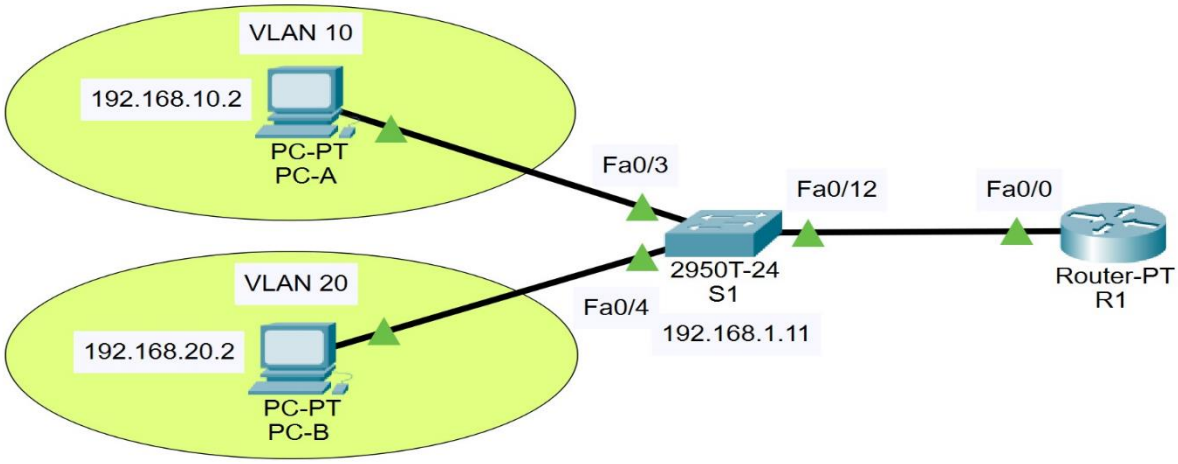
In step 8, you will configure R1 so that you can send data between different VLANs by creating so-called subinterface for each VLAN using a single physical interface. Each subinterface connected to a specific VLAN is assigned an IP address that belongs to that VLAN. This inter-VLAN method is called router-on-a-stick.
- On VLAN 1, we have the network 192.168.1.0/24 where the switch is connected.
- On VLAN 10, we have the network 192.168.10.0/24 where PC-A is connected.
- On VLAN 20, we have the network 192.168.20.0/24 where PC-B is connected.

To be able to configure the router, you also need to use a terminal program here. In our case TeraTerm. If it is not already pre-selected, select Serial in Tera Terms and the port labeled USB-Serial CH340.

a) Start the program and after the routers have started, answer NO to the question "Would you like to enter the initial… .." Sometimes the continuation question can come "Would you like to terminate autoinstall?" and there you answer YES.

b) Go first to the privileged EXEC mode configuration level and then to the global configuration mode. See the preparation information at the beginning for commands.

c) Configure the router named R1.



d) Create a subinterface on R1's Fastethernet 0/0 interface for VLAN 1 by entering the command interface f0 / 0.1 The number 1 (in the command interface f0 / 0.1) is a local numbering on the subinterface and has no connection to VLAN ID. For practical reasons, the subinterface may have the same number as the VLAN ID for easier identification. The number 1 (in the command "encapsulation dot1Q 1") indicates that this subinterface belongs to VLAN 1.

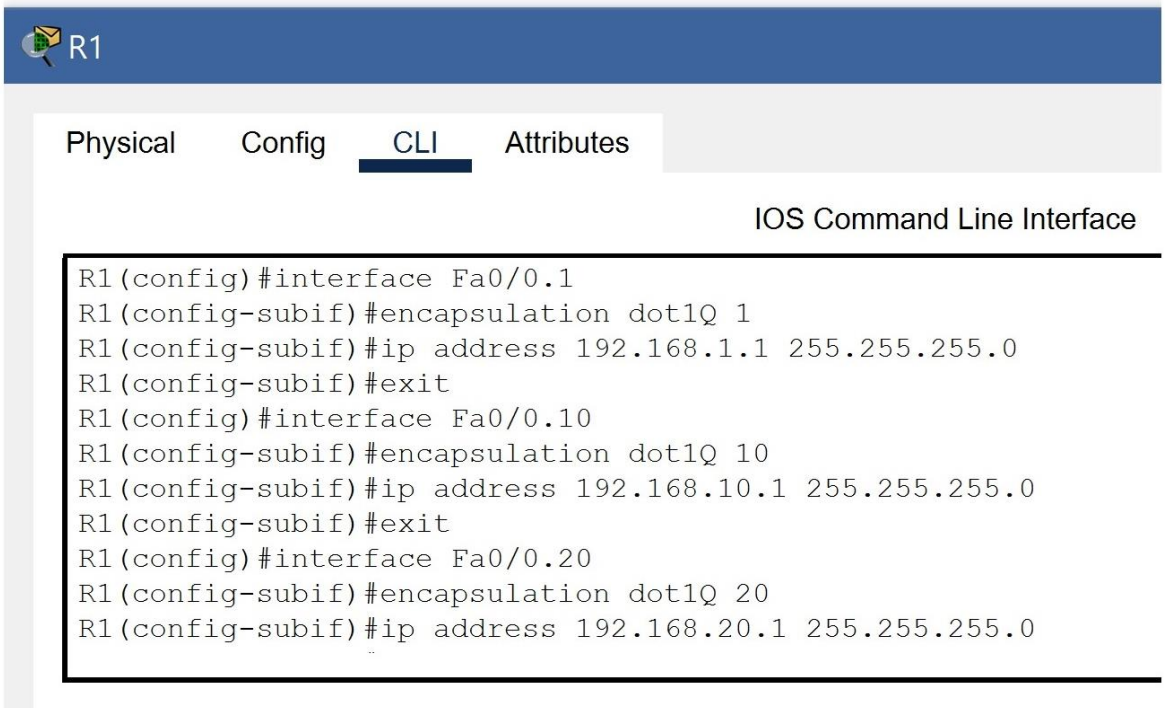
R1 (config) # interface f0 / 0.1
R1 (config-subif) # encapsulation dot1Q 1
R1 (config-subif) # ip address 192.168.1.1 255.255.255.0

e) Now add a VLAN 10 subinterface to the router.

R1 (config) # interface f0 / 0.10
R1 (config-subif) # encapsulation dot1Q 10
R1 (config-subif) # ip address 192.168.10.1 255.255.255.0

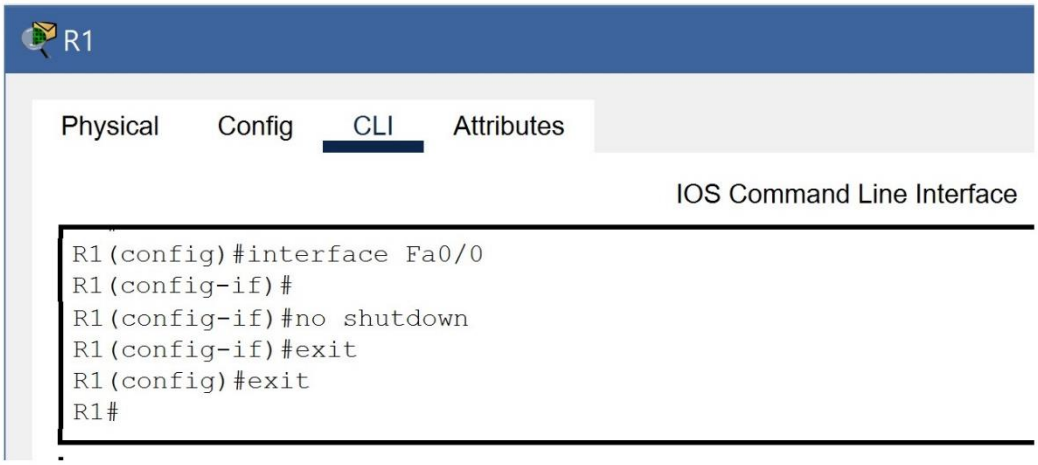
f) And another for subinterface VLAN 20 on the router's interface f0 / 0.20. See the previous step as an example and enter the correct IP address and VLAN ID

R1 (config) # interface f0 / 0.20
R1 (config-subif) # encapsulation dot1Q 20
R1 (config-subif) # ip address 192.168.20.1 255.255.255.0



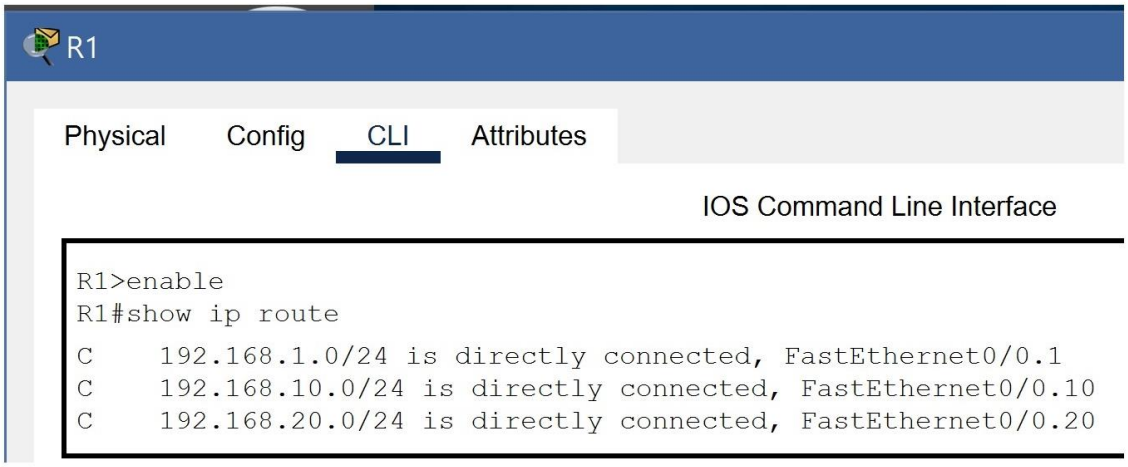
g) All interfaces on the router are shut down for security reasons and we need to activate the fast ethernet interface. Enter the commands below to activate the interface.

R1 (config) # interface f0 / 0
R1 (config-if) # no shutdown
R1 (config-if) # exit
R1 (config) # exit
R1 #

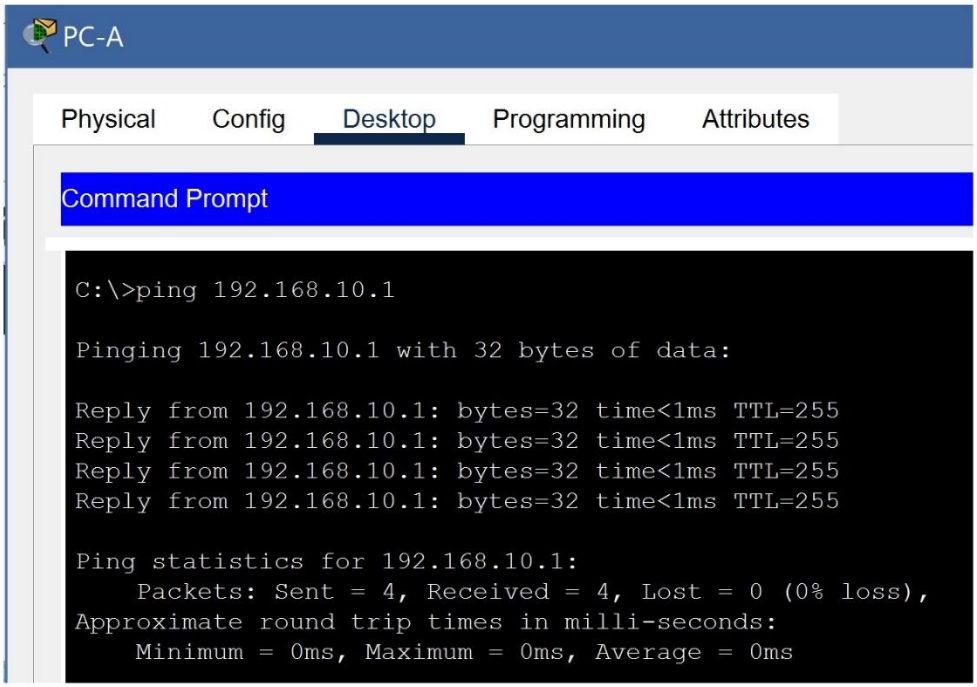


Step 9 - Final verification of the Inter-VLAN network

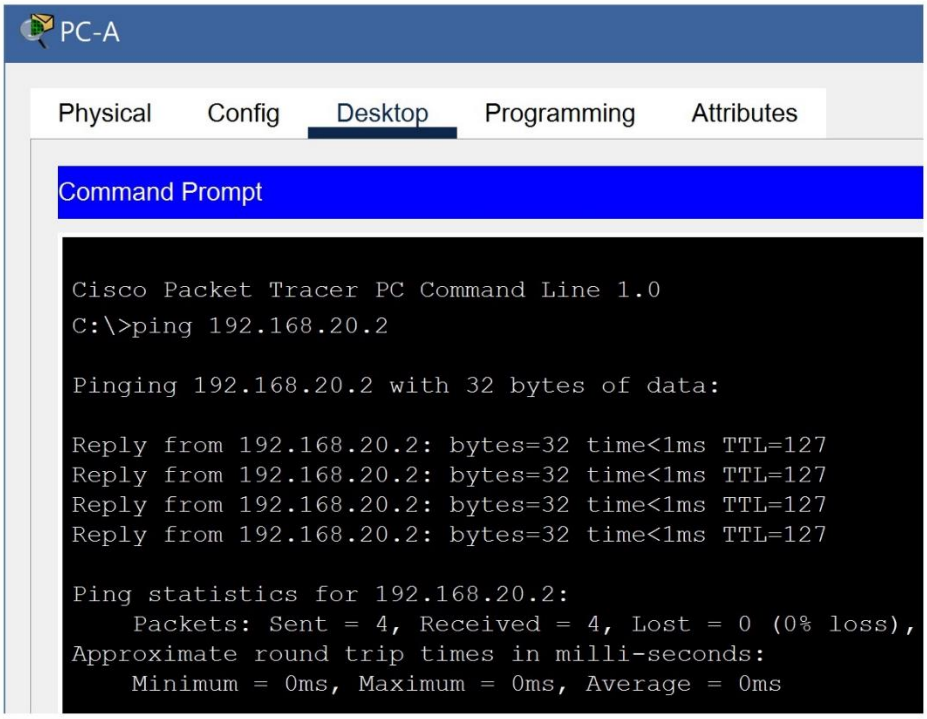
a) Enter the show ip route command on R1 to display the routing table. Which network addresses are shown in the table?

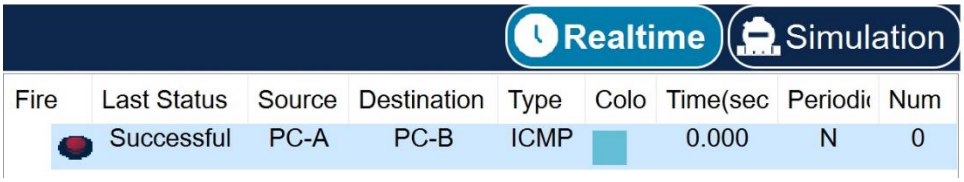


From PC-A, is it possible to ping the default gateway for VLAN 10? **Yes**



From PC-A, is it possible to ping PC-B? **Yes**





The above two points should work, if not, re-examine the connection and configuration.

b) Now start Wireshark in PC-A and ping ip the address 10.10.10.10 from PC-A. (10.10.10.10 is a made-up address that does not exist on the network.) What does ping respond to?

At Lab from PC-A: ping 10.10.10.10

What will be the result on PC-A in Wireshark? Do you see any response to the ping request packages sent from PC-A?