Tony Schofield’s Final Project!!

Project Overview:

Students will use the mid-term project as a foundation to build upon this network. The main focus of the final project is security. The project will explore methods to secure incoming and outgoing packets coming to the router, as well as a technique to enhance security for switch port access.

Instructions:

This final project weighs 40% towards the total grade.

Each student must individually present the project. During the presentation, the camera must be turned on, and the student should also present his/her ID. Failure to do so will result in a mark of 0.

For the project presentation, students need to select a time slot that aligns with their availability from the sheet provided by your instructor.

The presentation should not exceed a maximum of 10 minutes.

You will be presenting your documentation and demonstrating your project, and the instructor may ask questions if necessary.

Document all the steps and attach a separate Packet Tracer file for each completed task.

**Deadline to submit the documentation is Thursday July 27, 11 PM (Toronto’s time)**

**Deadline to present the project is Friday July 28, 11 PM (Toronto’s time)**

* NOTE! 0.0.0..255 WILDCARD.

0.0.0.255 is called Wildcard mask. If you create an ACL to permit traffic from the IP range 192.168.10.0 to 192.168.100.255. The subnet mask for this IP range is 255.255.255.0 (or /24 in CIDR notation). The corresponding wildcard mask would be: 11111111.11111111.11111111.00000000 In decimal notation, this is: 0.0.0.255 In the ACL rule, you would use this wildcard mask to indicate that the last octet of the IP address is not important (can be any value), and only the first three octets need to match the given range.

Task 1- ACLs Access Control Lists

*Access Control Lists (ACLs) are a powerful feature used in Cisco routers to control the flow of network traffic based on specified criteria. ACLs act as filters that permit or deny packets as they pass through the router's interfaces. By implementing ACLs, network administrators can enhance security, control network traffic, and optimize network performance.*

In the final network product built for the mid-term project, all the devices in different VLANs can ping each other. However, in this task, you are required to use ACLs to limit this connectivity between these VLANs. The objective of this task is to block the connection from VLAN20 (students) to VLAN100 (Critical devices) and allow VLAN10(faculty\_Staff) to connect to VLAN100. In this task a Standard ACL (Access Control List) is used which is a type of access control list used in Cisco devices to filter network traffic based **only on the source IP address**.

This in blue did not work for me because of the IN command – OUT worked for me, both server and students were able to still see each other with the IN being added.

Step1: Configure the VLAN Access Control List (ACL)

1. In the router, enter global configuration mode
2. Create and configure the VLAN Access Control List (ACL) with the provided rules:

a. Deny traffic from VLAN20 (192.168.20.0/24) to VLAN100 (192.168.100.0/24): access-list 20 deny 192.168.20.0 0.0.0.255

b. Allow traffic from all other networks to access VLAN100:

access-list 20 permit any

1. Apply the ACL to the interface carrying VLAN100 (gigabitEthernet0/1.100):

a. Enter interface configuration mode by typing:

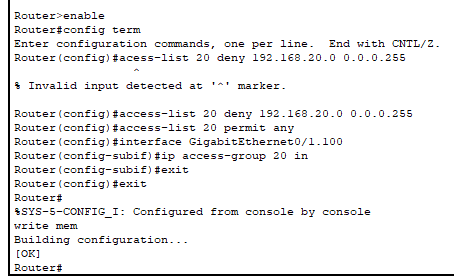
interface gigabitEthernet0/1.100

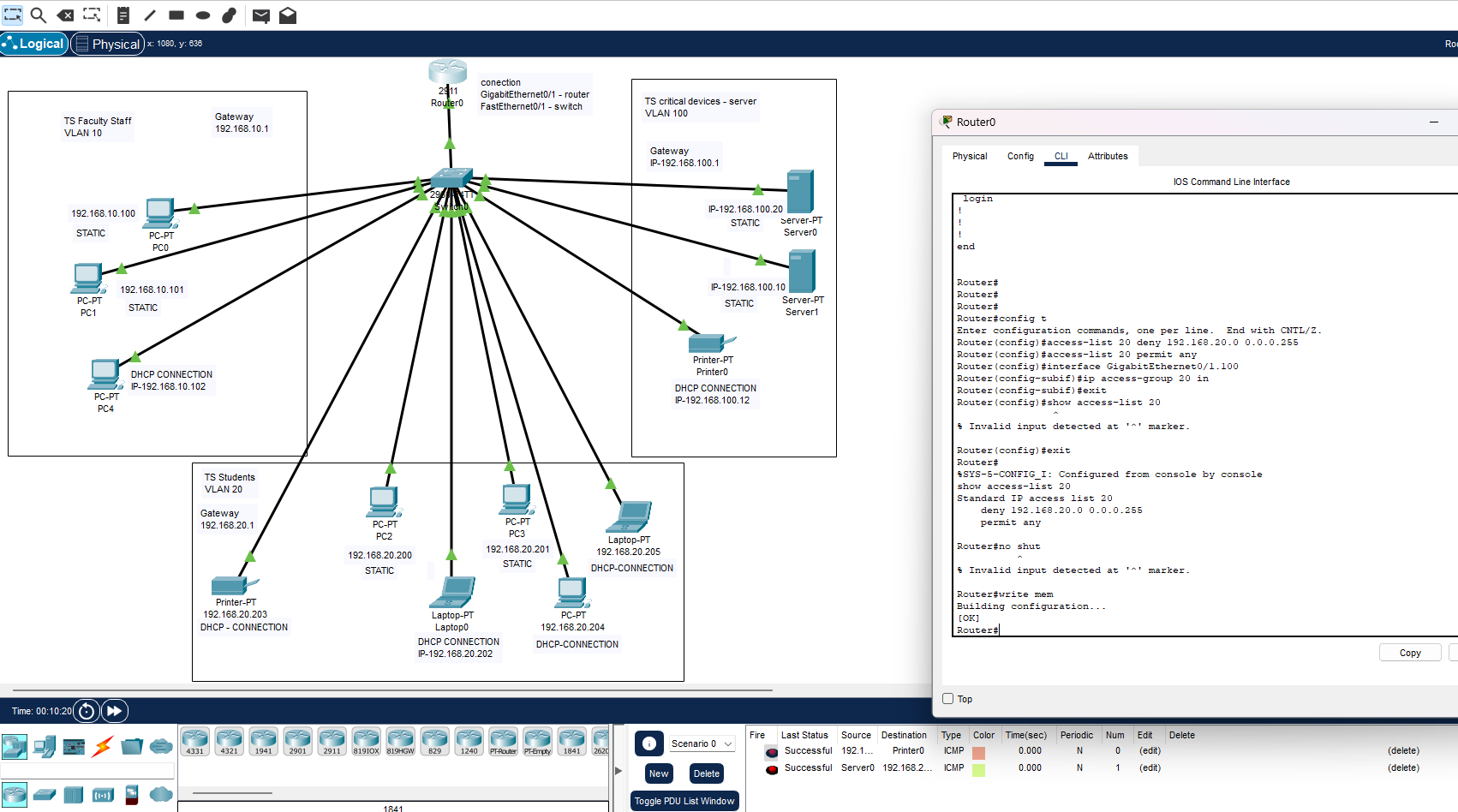
b. Apply the ACL to VLAN100 interface inbound traffic (in):

ip access-group 20 in

1. Verify that ACL is added by typing:

show access-list 20





Step1: Configure the VLAN Access Control List (ACL)

In the router, enter global configuration mode

Create and configure the VLAN Access Control List (ACL) with the provided rules:

1. Deny traffic from VLAN20 (192.168.20.0/24) to VLAN100 (192.168.100.0/24): access-list 20 deny 192.168.20.0 0.0.0.255
2. Allow traffic from all other networks to access VLAN100:

access-list 20 permit any

Apply the ACL to the interface carrying VLAN100 (gigabitEthernet0/1.100):

1. Enter interface configuration mode by typing:

interface gigabitEthernet0/1.100

1. Apply the ACL to the interface outbound (out) by typing the following command:

ip access-group 20 out

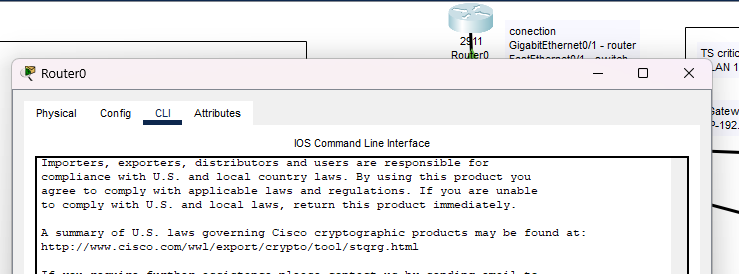
1. Verify that ACL is added by typing:

show access-list 20

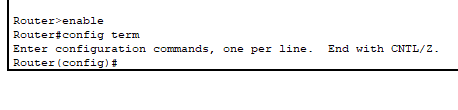
To do the step for TASK 1 in extended above follow these instructions,

TASK 1 STEPS =

1. Open the router by double clicking it, and then selecting the cli tab

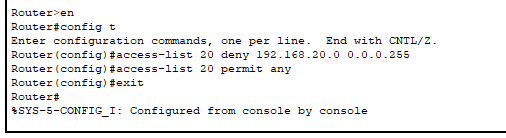


1. Type the command, enable then config term to enable configuration mode.



Now to deny traffic from VLAN 20 we need to create and configure a VLAN Access Control List or ACL. By typing the following commands,

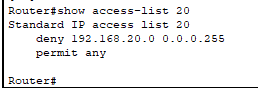
1. access-list 20 deny 192.168.20.0 0.0.0.255
2. access-list 20 permit any
3. then type the command, exit to bring us back to the config command.



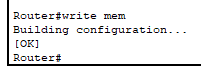
1. Then type the command, interface GigabitEthernet0/1.100
2. Then type the command, ip access-group 20 out



1. Now type exit then press the return key
2. Follow step 9 again.
3. Then type, show access-list 20 to show the access list.

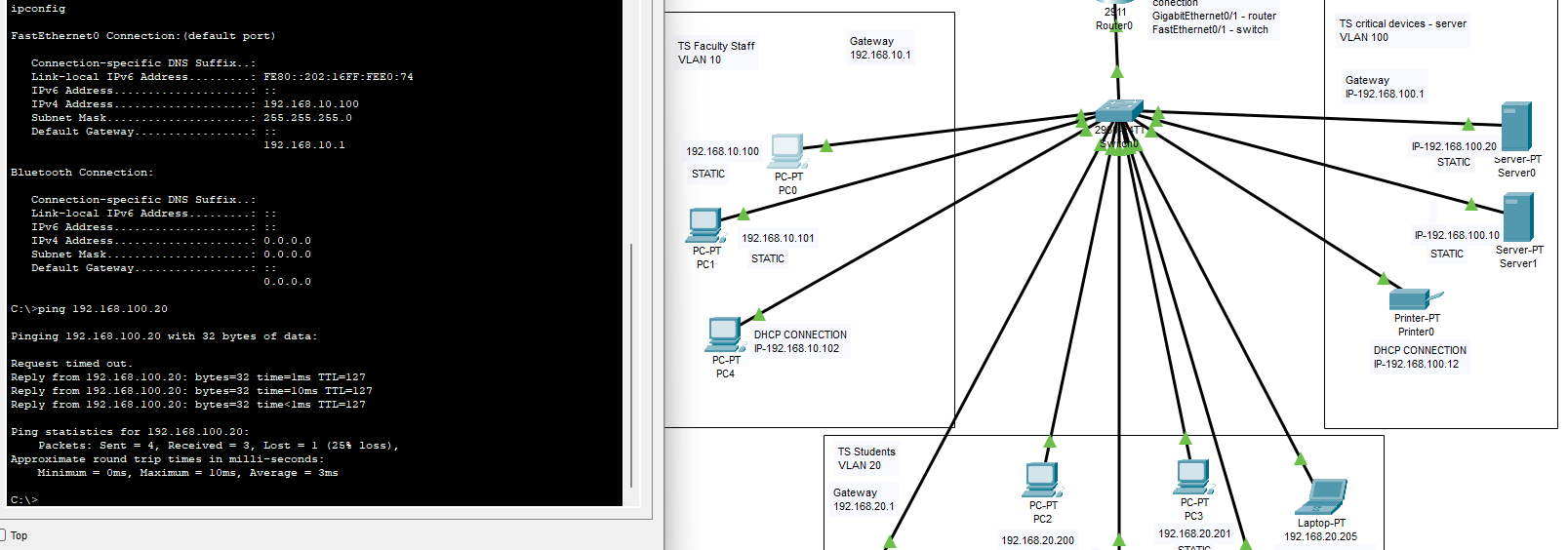


1. Now we will type exit
2. And then the command, write mem – to write it to the memory



Now we shall ping 192.168.100.20 SERVER from CLIENT 192.168.10.100 and from server to faculty client.

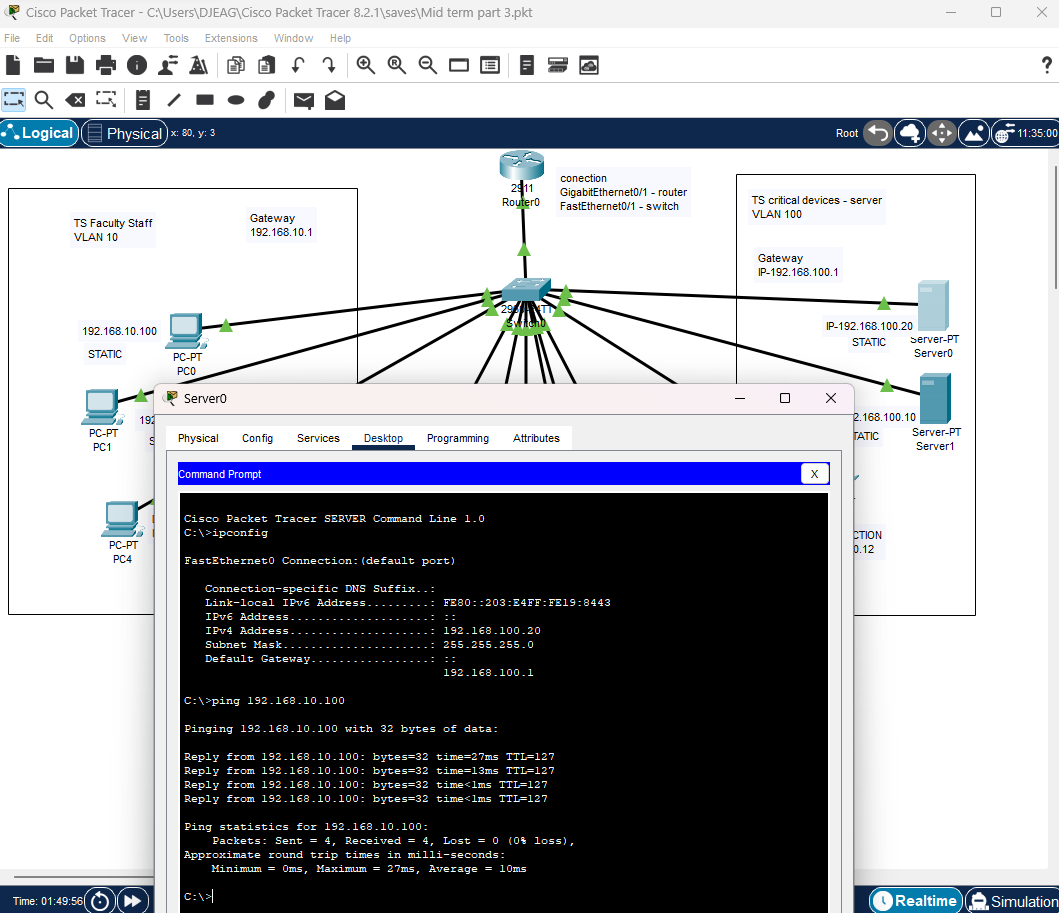
1. Open up command prompt on client and type ping 192.168.100.20



Success we can ping the server from the faculty client

Now open up command prompt on the server and ping the faculty client,

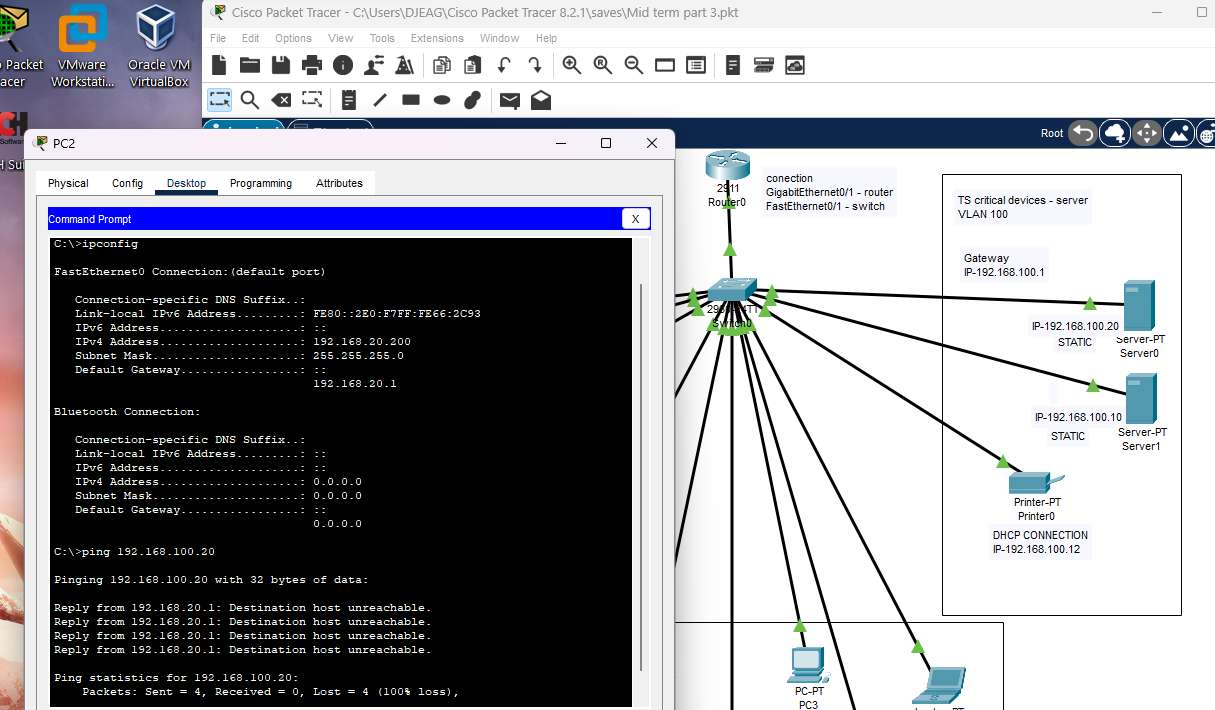
1. type, ping 192.168.10.100



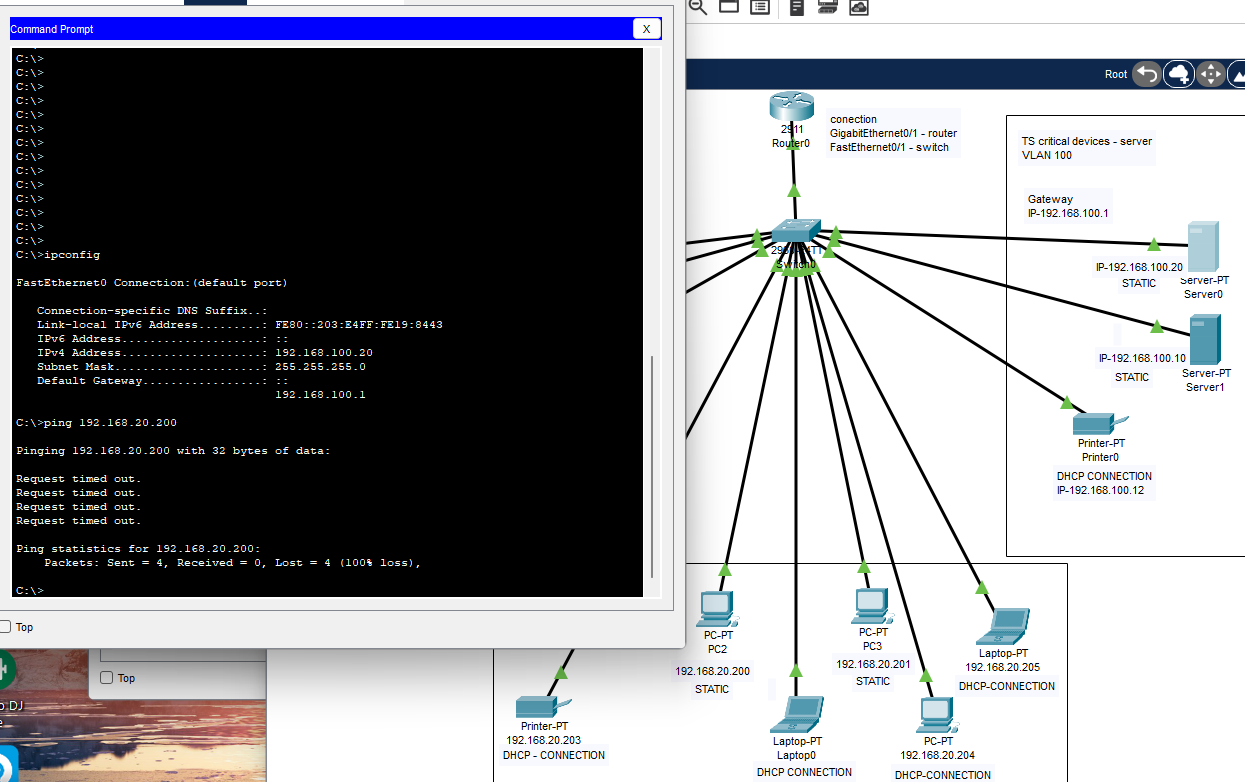
GREAT SUCCESS we can ping and see the client from the server

Now to ping the server 192.168.100.20 from the student room VLAN20 192.168.20.200 and vice a versa

1. Open up command prompt on student client 192.168.20.200 and type, ping 192.168.100.20



1. Open up command prompt on server 192.168.100.20 and type, ping 192.168.100.20



As you can see from pictures in step 16 and 17, access has now been blocked in both directions!

Task 1 P.T File standard

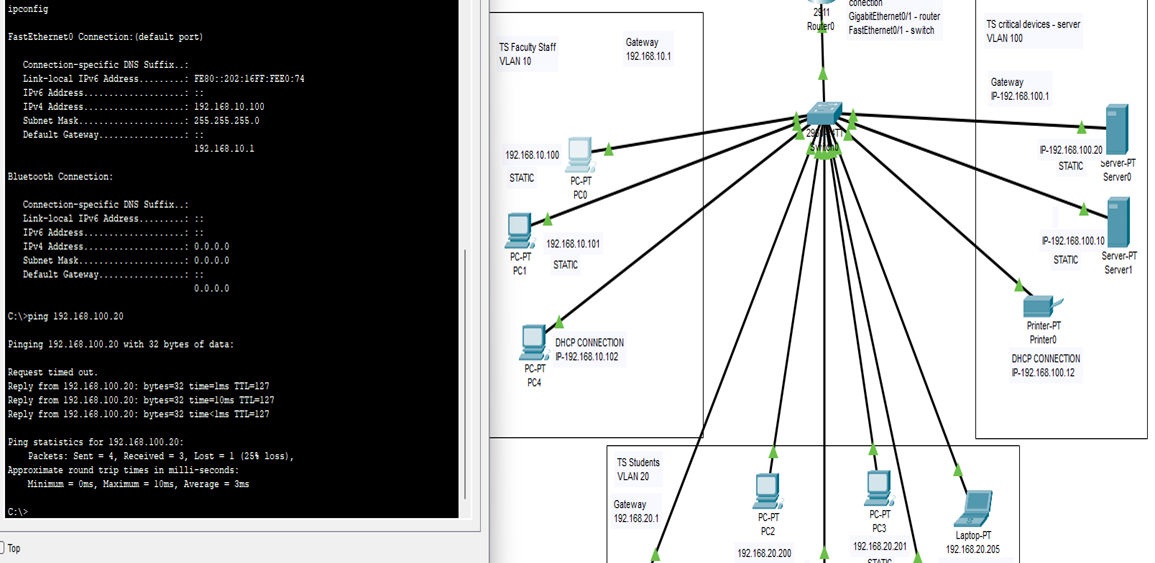


Step 2: Test Connectivity

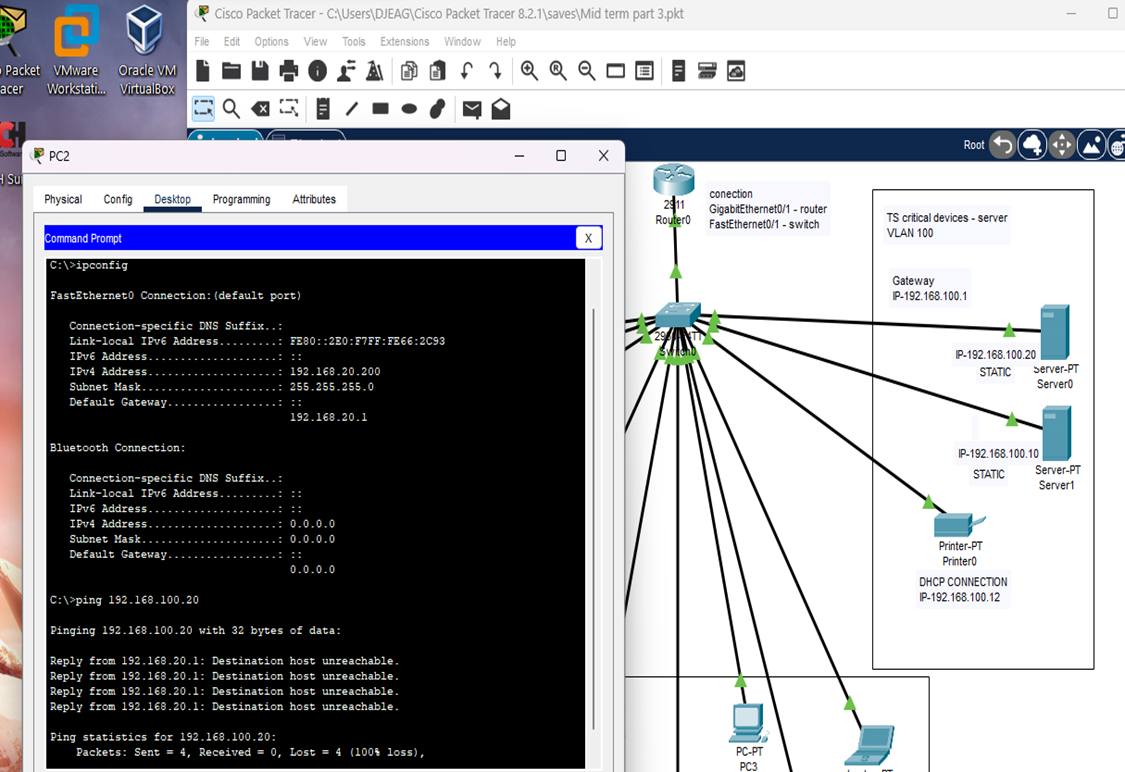
(SEE ABOVE FOR COMPLETION AND PACKET TRACER FILE)

Verify the ACL configuration by performing the following tests:

a. From any device in VLAN10 (Faculty\_Staff), ping any device in VLAN100 (Critical Devices). Observe that the pings are successful, as traffic from VLAN10 to VLAN100 is allowed by the ACL.



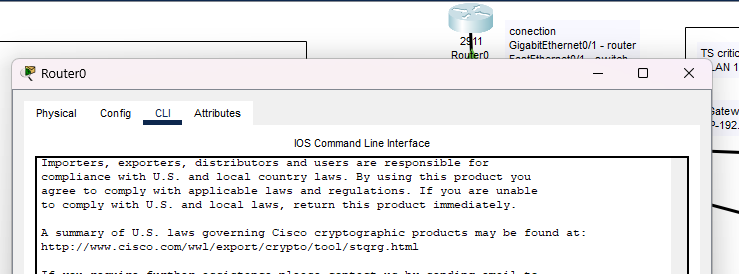
b. From any device in VLAN20 (Students), ping any device in VLAN100 (Critical Devices). Confirm that the pings are unsuccessful, as traffic from VLAN20 to VLAN100 is denied by the ACL.



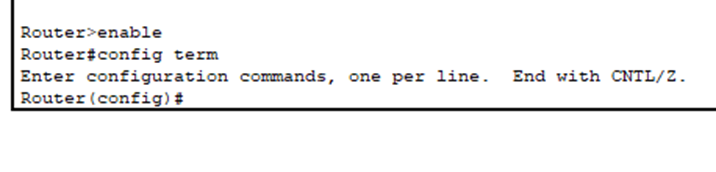
Challenge tasks: Conduct your research on how to complete the following challenge task and document all the steps:

Challenge 1: Deny ICMP echo requests (ping) from VLAN20 to VLAN10.

1. Open the router by double clicking it, and then selecting the cli tab



1. Type the command, enable then config term to enable configuration mode.



1. now we will type the following commands one at a time,

access-list 101 deny icmp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 echo

interface gigabitEthernet0/1.20

ip access-group 101 ? ( incase you forget what is available, or an option to select from)

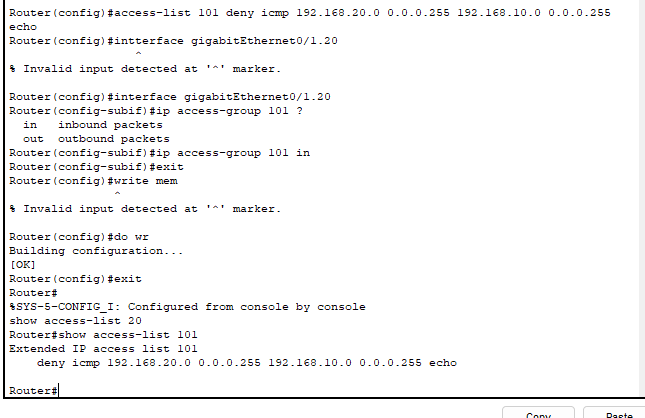
in

exit

do wr (this saves in the command structure, write or write mem is for when you are in config root)

exit

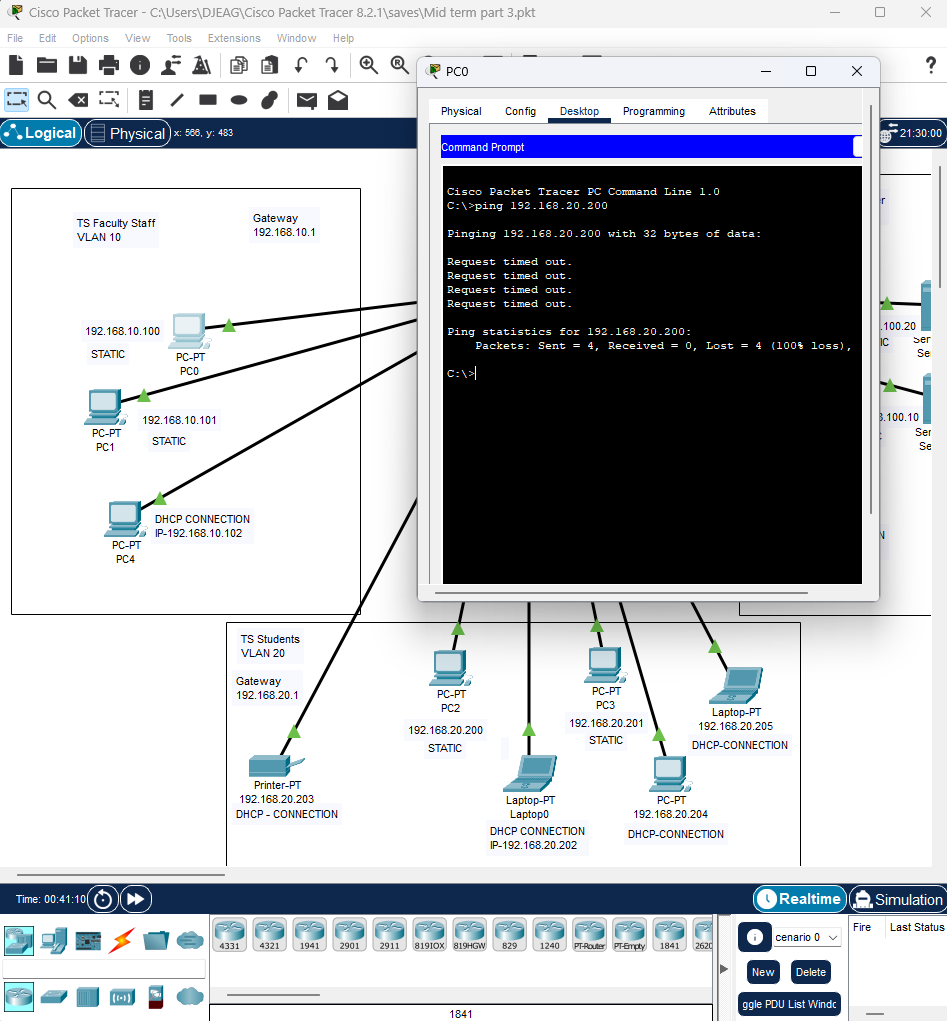
show access-list 20



As you can see, our VLAN20 & VLAN10 are set to deny, blocking traffic to each other.

Now we shall check the ping

1. open up command prompt on pc0 and type ping 192.168.20.200

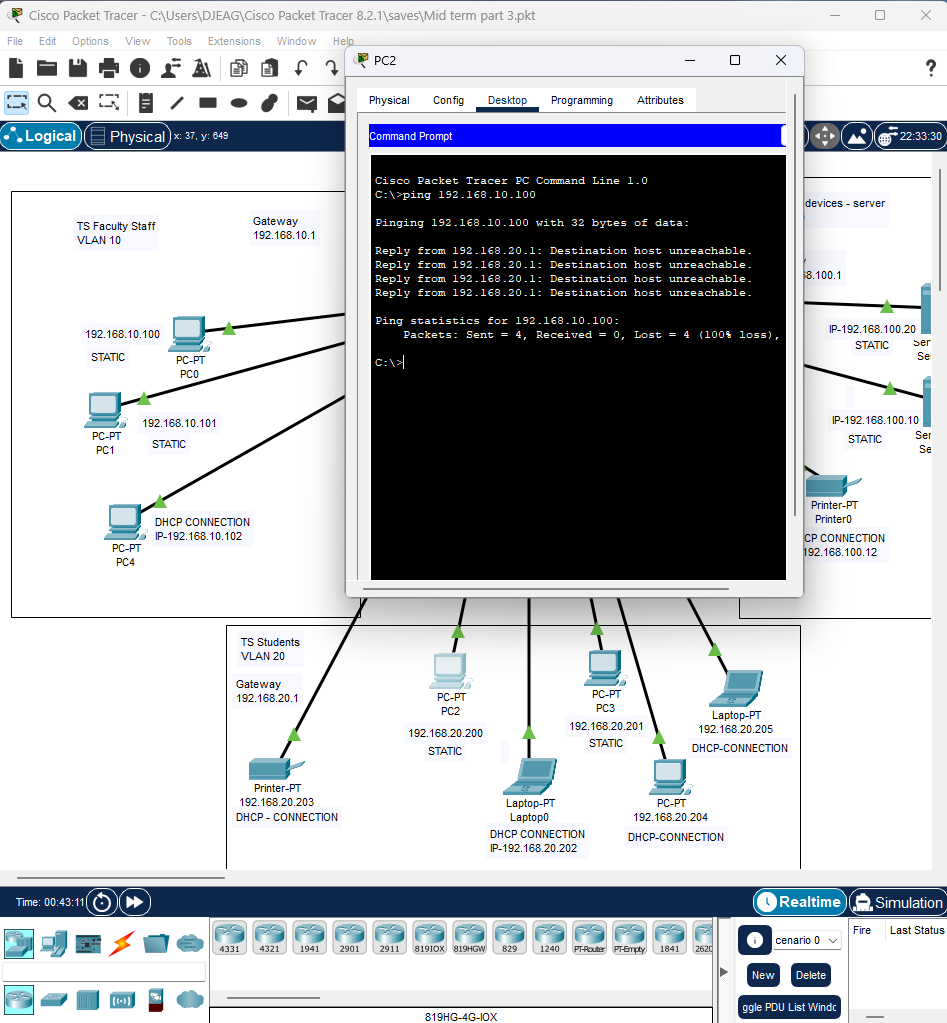


As you can see the faculty can not ping the students as it times out,

Now let us ping the faculty from the students,

1. open up command prompt from pc2 in the students and ping pc0 in the faculty room by typing the following command into command prompt

ping 192.168.10.100



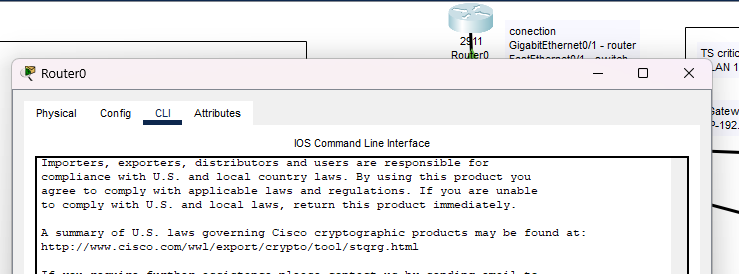
Great success, now they can not see each other

Challenge 1 P.T File.

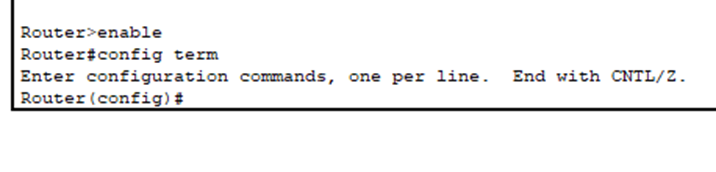


Challenge 2: Allow ONLY one device in VLAN 20 (Students) to access VLAN 100 (Critical Devices)

1. Open the router by double clicking it, and then selecting the cli tab

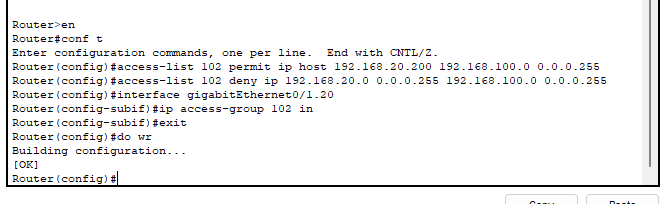


1. Type the command, enable then config term to enable configuration mode.



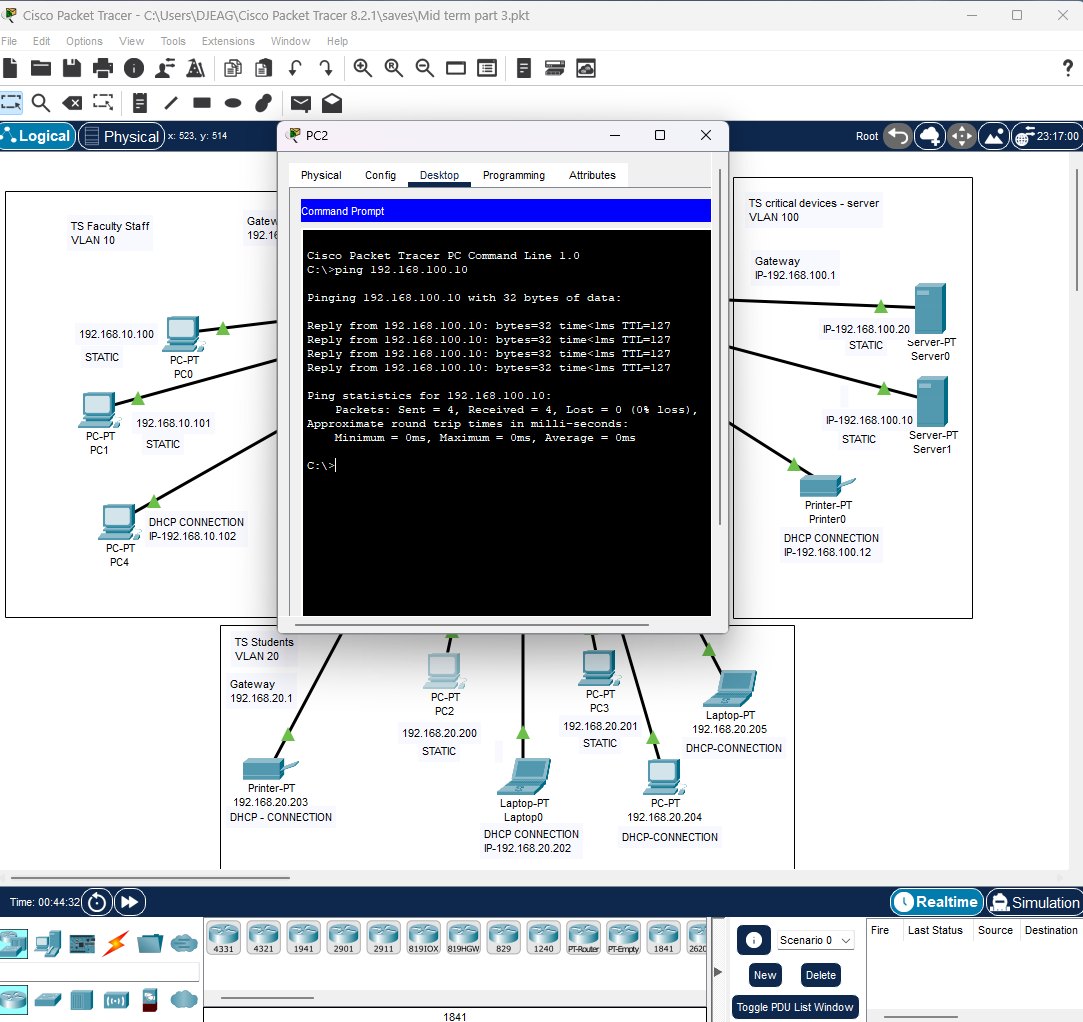
Then type the following commands 1 at a time,

1. access-list 102 permit ip host 192.168.20.200 192.168.100.0 0.0.0.255
2. access-list 102 deny ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255
3. interface gigabitEthernet0/1.20
4. ip access-group 102 in
5. exit
6. do wr



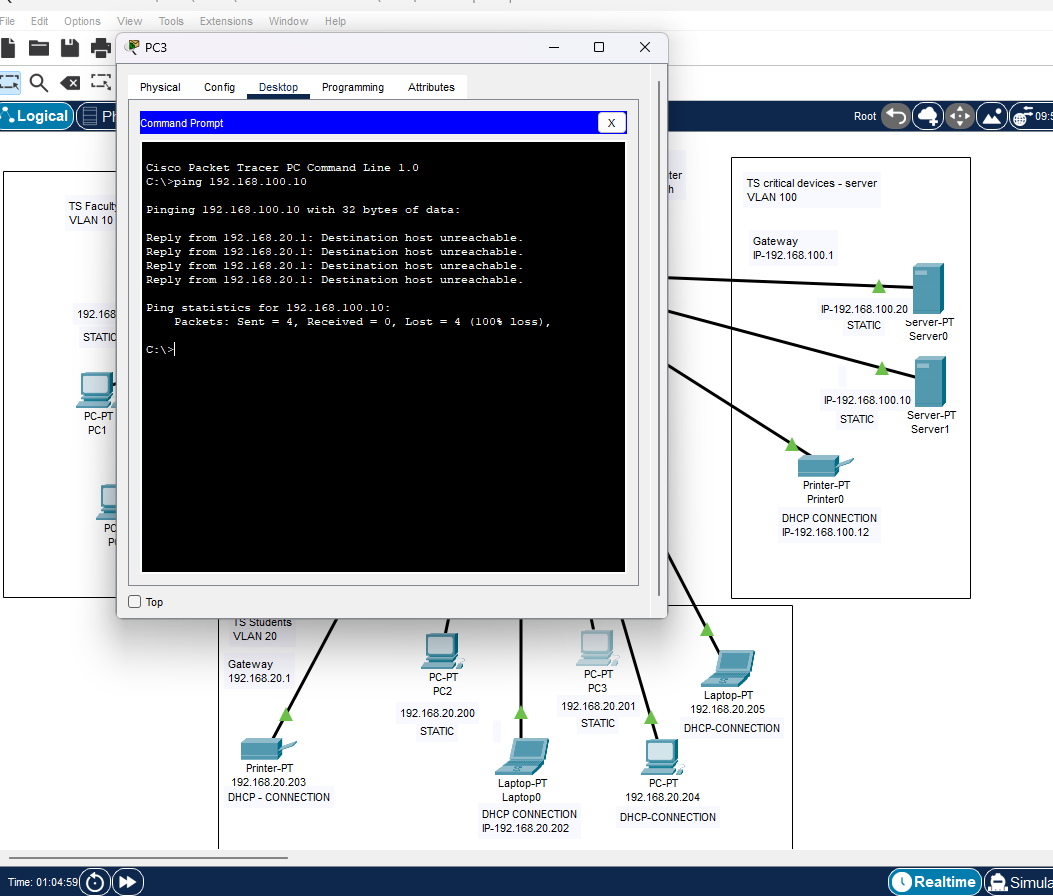
Now we will ping from pc2 to server 1

Bring up the command prompt for pc2 and type – ping 192.168.100.20

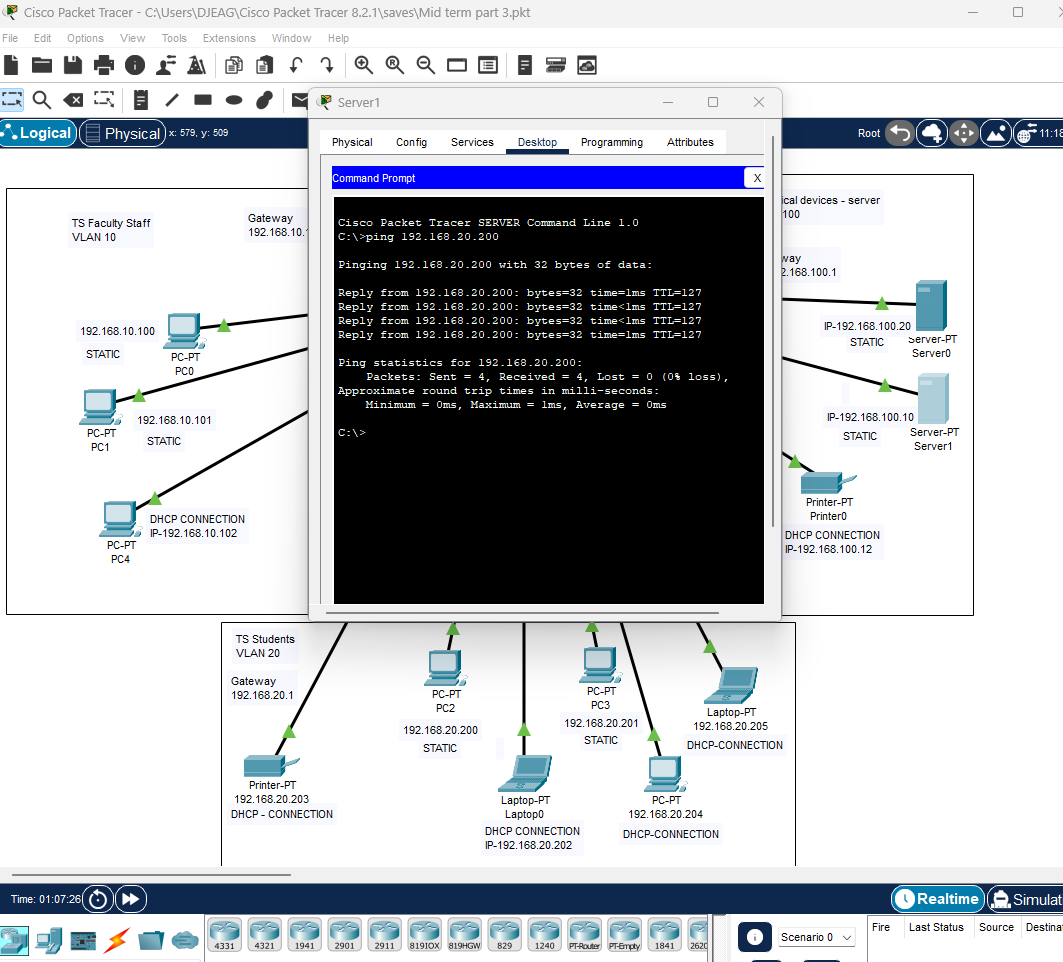


GREAT SUCCESS! Now we will ping from pc3 to server

So now open command prompt on pc3 and type – ping 192.168.100.10



Now just one more screen shot from server to pc1 to make sure that it can see both ways,



GREAT SUCCESS!!

Challenge 2 P.T File,



Task 2- Switch Port Security

Port security is a network security feature that is implemented on switches to control and restrict access to the network by unauthorized devices. It helps prevent unauthorized users from connecting to a network through switch ports by allowing administrators to define and enforce specific security policies.

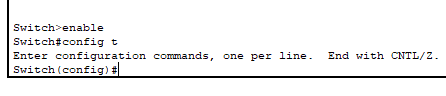
Follow these steps to secure the port to which Server1 is connected (assuming it is connected to port fa0/6). The restriction is based on Server1's MAC address. Applying port security to a specific port will prevent unauthorized access and ensure that only the designated device can connect to that specified port.

Using the switchport mode access command (which was not added to the instruction list) is a basic setup on network switches that can improve network security by managing who can connect, dividing traffic into different groups, limiting the impact of security issues, and stopping specific attacks. However, it's crucial to use other security methods together with switchport mode access to create a strong cybersecurity plan for your network.

IN THE SWITCH! DO THE FOLLOWING STEPS!!

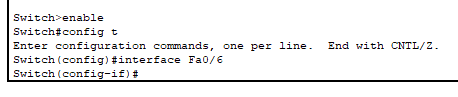
1. Enter Global Configuration Mode by using the following commands:

Enable then configure terminal

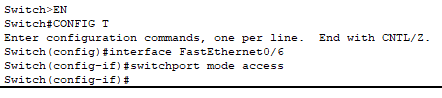


1. Select the Interface to Configure Choose the interface corresponding to the server port where you want to assign the MAC address. For example, if you want to configure interface Fa0/6, enter the following command:

interface Fa0/6

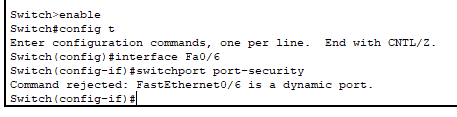


1. Type in the command, switchport mode access – if you do not type this you get and error code – command rejected: FastEthernet0/6 is a dynamic port



1. Enable port security on the selected interface using the following command:

switchport port-security

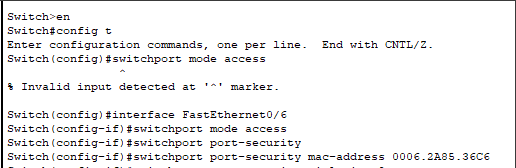


1. Assign the MAC address of the server device to the port using the following command:

switchport port-security mac-address <your mac address goes here>

FOR EXAMPLE:

switchport port-security mac-address 0006.2A85.36C6



Replace <MAC\_ADDRESS> with the actual MAC address of the server device you want to allow on this port.

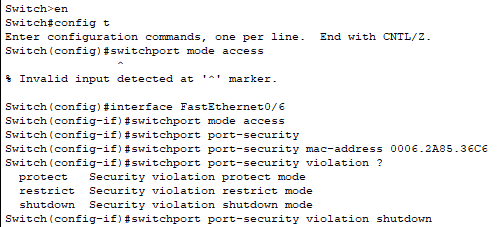
1. Specify the action that the switch should take when a violation occurs. For example, to shut down the port when a violation occurs, use the following command:

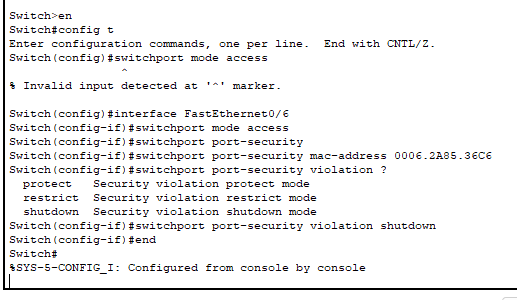
switchport port-security violation shutdown

Note: There are other violation modes available, such as restrict and protect.

In order to show these instead of the above code type in the following command,

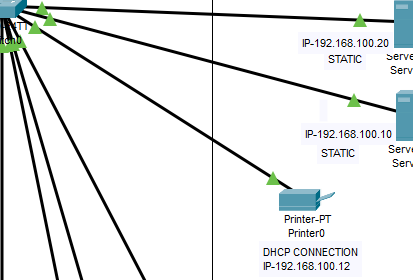
switchport port-security violation ?



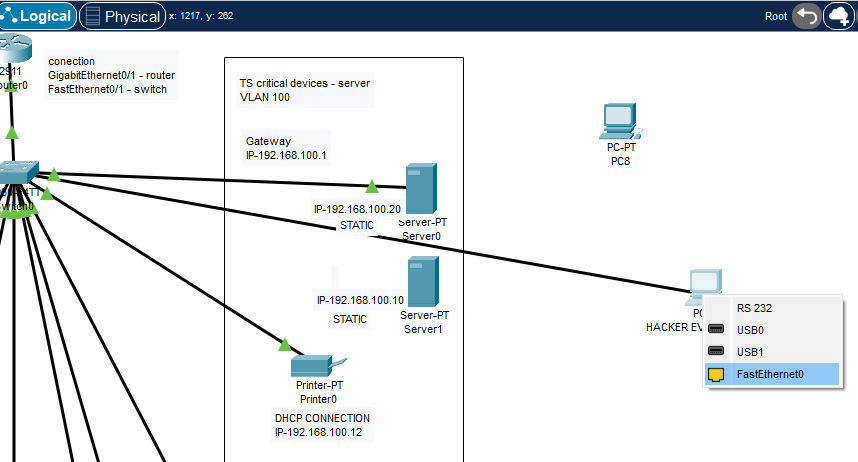


Test Unauthorized Connection, try connecting a device other than the server with the configured MAC address to the FastEthernet port (Fa0/6). Observe the switch's reaction when the unauthorized device is connected. The port should automatically shut down

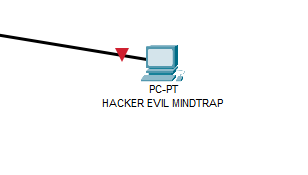
1. Ok so drag the cable from server 1 to your hacker machine, by clicking on the green icon closest to the server,



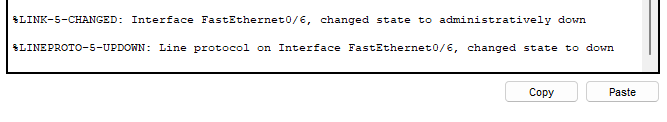
And dragging it to the hacker machine and connect to FastEthernet0



Connection will be green at first, but after some time it should go red like this

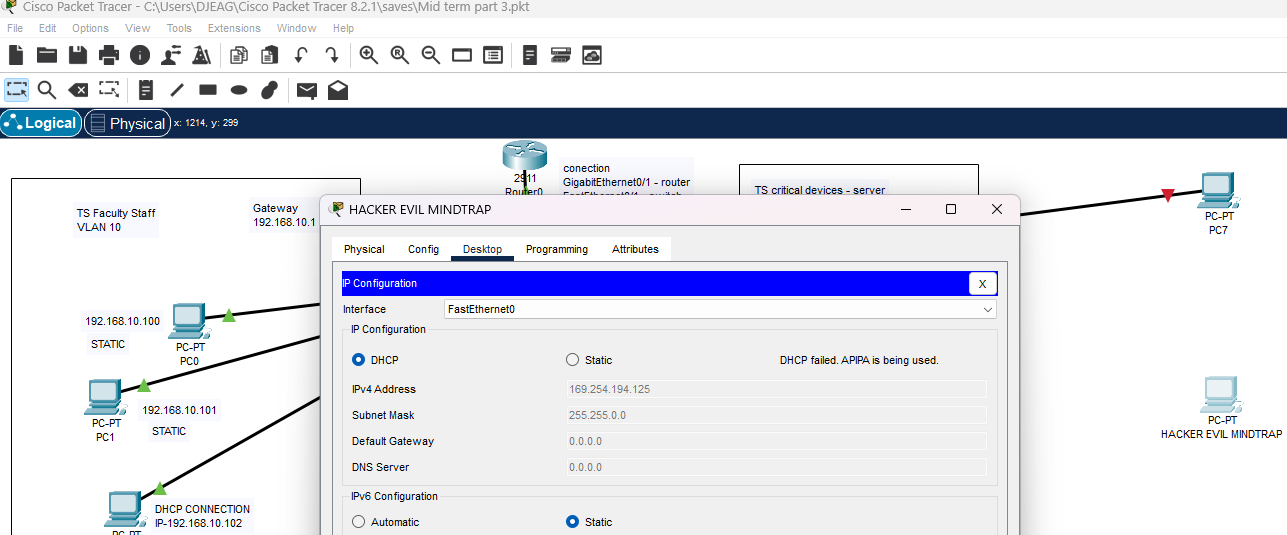


Now we will go into the switch and check the cli,

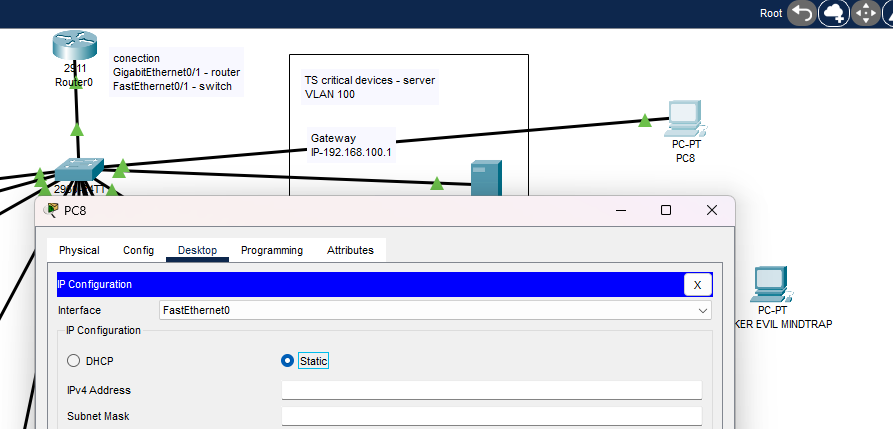


GREAT SUCCESS

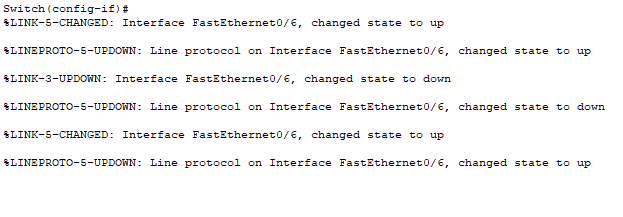
If For some reason your hacker machine is showing green and the administrative shutdown does not show in the switch cli, then that means the hackers machine is not actively connecting properly and you need to go to the hacker machine and go to desktop – ip config – and turn on dhcp, this needs to be turned on, on the hacker machine In order for P.T to register the active conection.



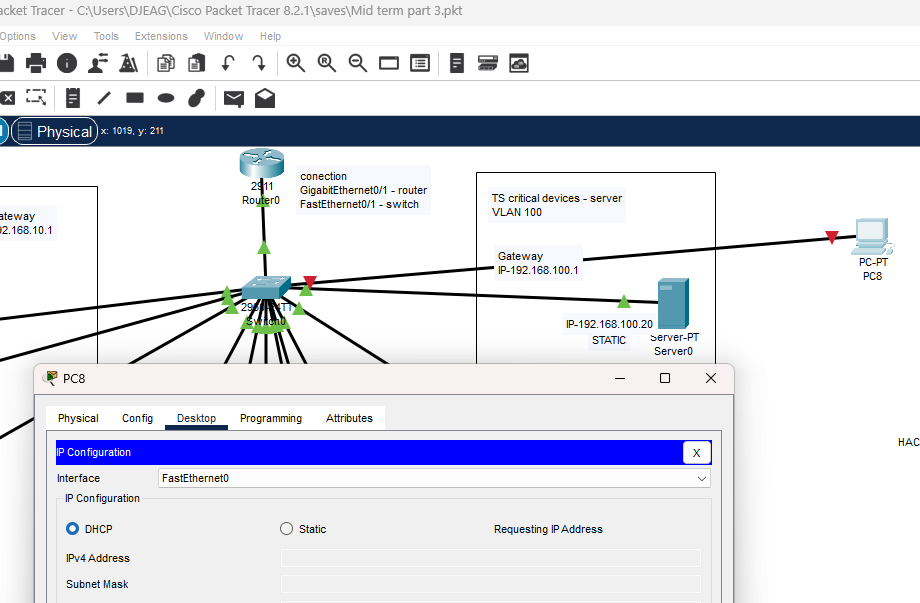
1. As you can see here that the line is still green for pc8 when the machine is in static mode,



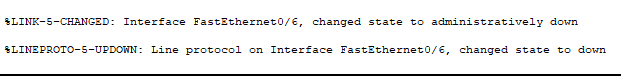
1. In the switch, nothing registers because the hacker’s machine is not asking correctly for the ip address.



1. However it turns red when I switch to dhcp mode because it is asking (requesting) an ip from the source, however because of the port-security settings we have in place, they can not access through that port because of the MAC-ADDRESS (computer id/fingerprint) does not match the original server.



1. And when we look In the switch cli, we get





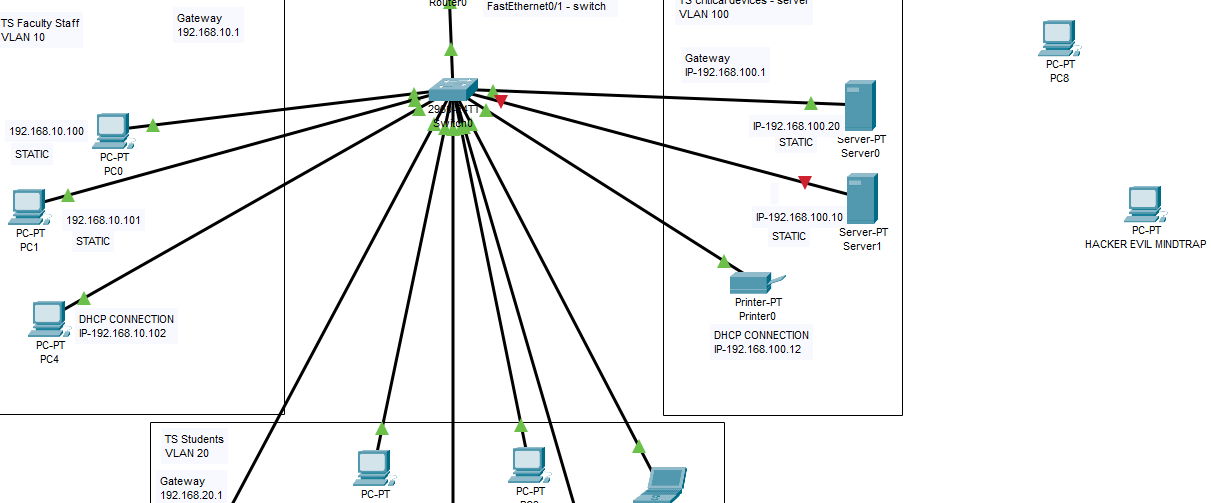
GREAT SUCCESS!!

Task 2 P.T File



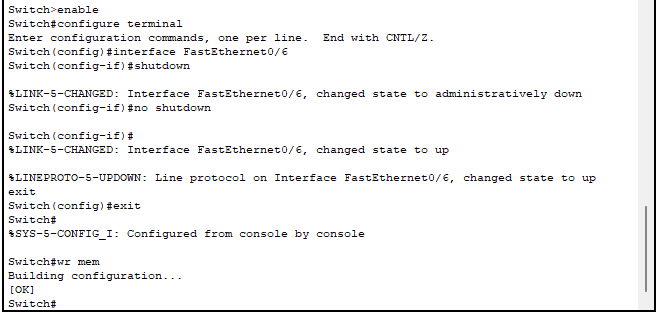
On a side note.

When a port gets terminated by the security protocol the line does not just reset itself,

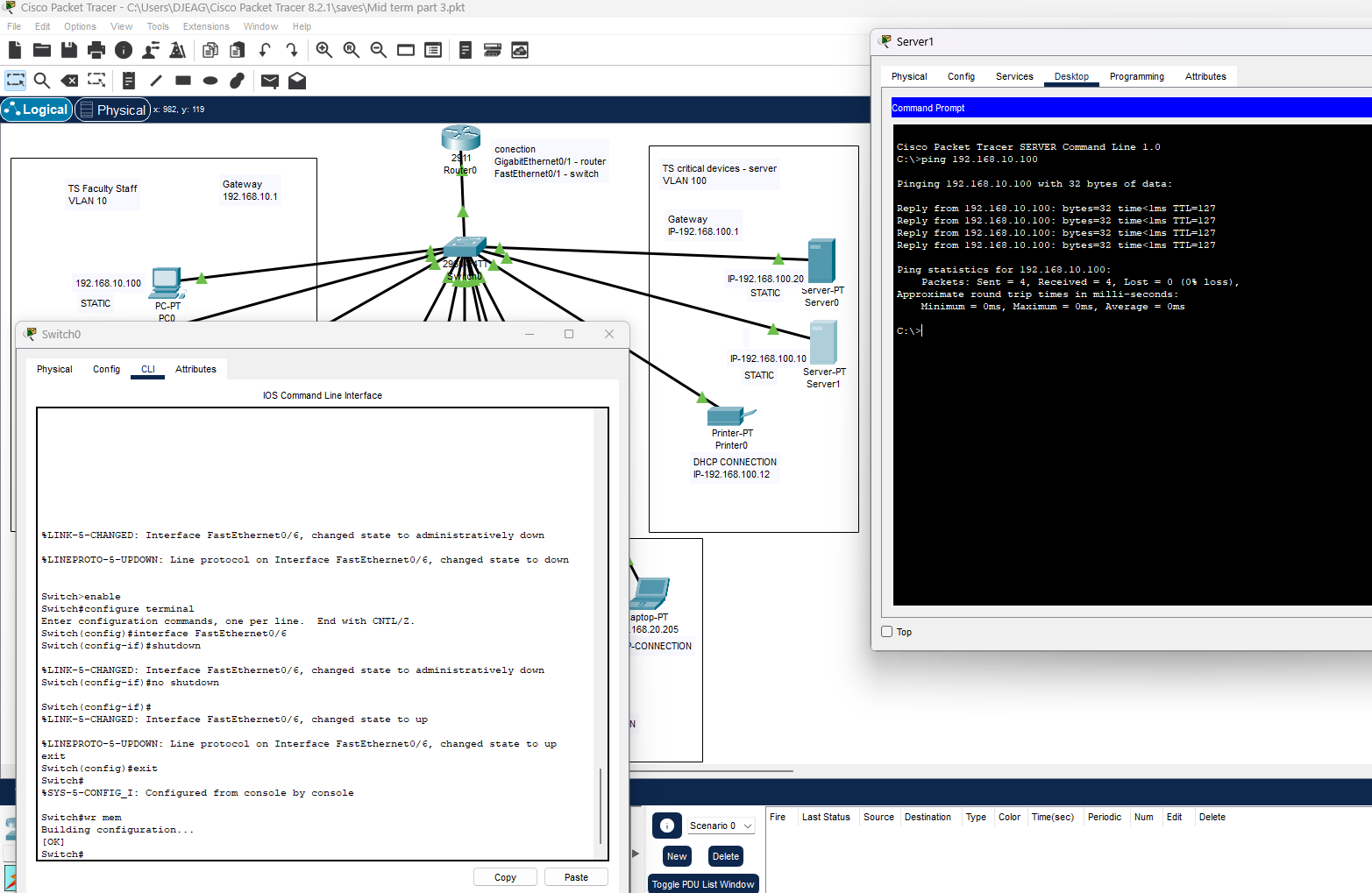


you have to go into the switch cli and type the following commands to reset the port, so that it can be used again.

1. Enable
2. Configure terminal
3. Interface FastEthernet0/6
4. Shutdown (this forces the conection to shutdown properly)
5. No shutdown
6. Exit
7. Exit
8. Write memory



And as you can see our server is green and connected again



Also, with regards to APIPA (Automatic Private IP Addressing)

APIPA enables devices to communicate within a local network even when no DHCP server is accessible. This feature is beneficial in small or isolated networks. However, it's important to understand that APIPA addresses cannot be used to communicate with devices on different networks. For full network connectivity, a DHCP server offering valid IP addresses must be present on the network.

**Marking guide**

|  |  |
| --- | --- |
| **TASKS** | **Mark** |
| Task 1 | 10 |
| Task 1-Challenge 1 | 6 |
| Task 1-Challenge 2 | 12 |
| Task 2 | 12 |
| **TOTAL SCORE** | **/40** |
|  |

Links

ACLs

<https://www.cbtnuggets.com/blog/certifications/cisco/networking-basics-how-to-configure-standard-acls-on-cisco-routers>

<https://www.youtube.com/watch?v=4PPUvRj2PvM>

<https://www.youtube.com/watch?v=XdBjnLppxB0>

<https://www.youtube.com/watch?v=FIVJUx1k3xA>

<https://www.youtube.com/watch?v=aSkv5-0S0ZM>

Port security

<https://www.youtube.com/watch?v=sD5SpnGBh64>