DESIGNING A UNIVERSITY NETWORK USING PACKET TRACER

Dr. Tamer ElBatt

Marwan Eid – 900171885
Mohammed Abuelwafa - 900172603

The American University in Cairo
School of Sciences and Engineering
Department of Computer Science and Engineering
CSCE 331202 - Computer Networks
Fall 2020

Table of Contents

Table of Figures

Network Topology

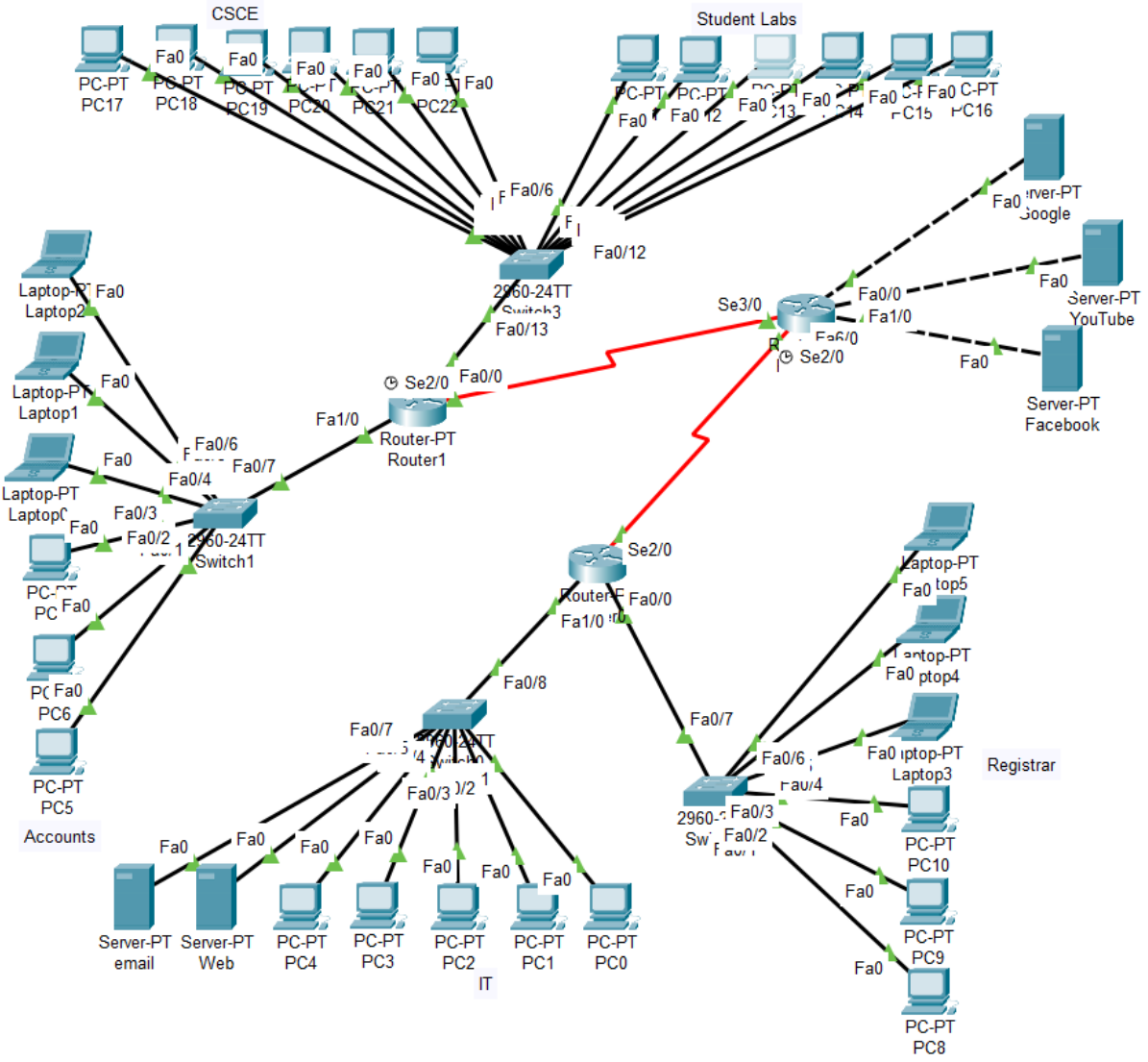

Figure 1

- The design of the university network is shown in Figure 1. The four departments along with the Engineering & Computer science school, (CSCE), are divided into five standalone networks.
- The two departments, CSCE and students' labs, are physically connected to the same LAN through Switch 3; however, they are divided logically into two virtual LANs (VLANs), VLAN 2 and VLAN 3.
- The subnet mask used throughout the network is 255.255.255.224 (/27), while that for the serial ports and for the servers is 255.255.255.128 (/25), i.e. the ISP router links.
- The serial ports used to connect the ISP router with router 0 and router 1 use a class A network IP addresses, 10.0.0.0 and 11.0.0.0, to resemble a network with many hosts.
- The structure of the network is as follows:
    - The network is connected through three main routers:
        - Router 0 connects the IT department with network IP address 172.16.1.0 and the registrar department with network IP address is 172.16.3.0. The IT department supports two services: the web server

and the email server; service is represented through pinging, i.e. not the actual email service.

- Router 1 connects the accounts department with network IP address 172.16.2.0 and the two logically connected networks, CSCE with network IP address 172.16.5.0 and students' labs with network IP address 172.16.4.0.
- The ISP router connects the three servers that represent the internet in our topology to the network through routers 0 and 1.
    - The Google server has an IP address of 8.8.8.8 and a default gateway of 8.8.8.1.
    - The YouTube server has an IP address of 2.2.2.2 and a default gateway of 2.2.2.1.
    - The Facebook server has an IP address of 3.3.3.2 and a default gateway of 3.3.3.1.

Network Protocols

- The network addressing protocol used is IPv4.
- Two protocols, RIP v2 and static routing, were used for routing throughout the network, where RIP v2 was implemented to dynamically route the network, while some links were routed using static routing to enforce those routes.
- Routing information for router 0, router 1, and the ISP router is shown in figure 2, 3, and 4, respectively.

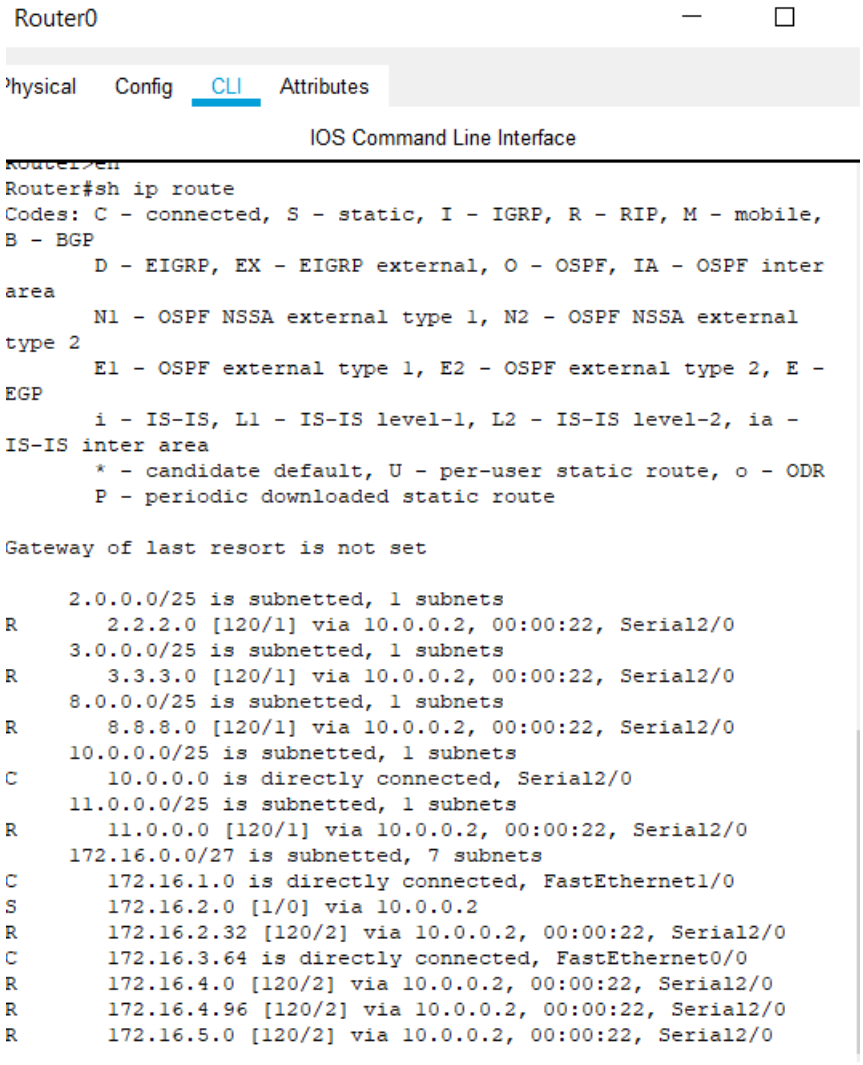

Figure 2

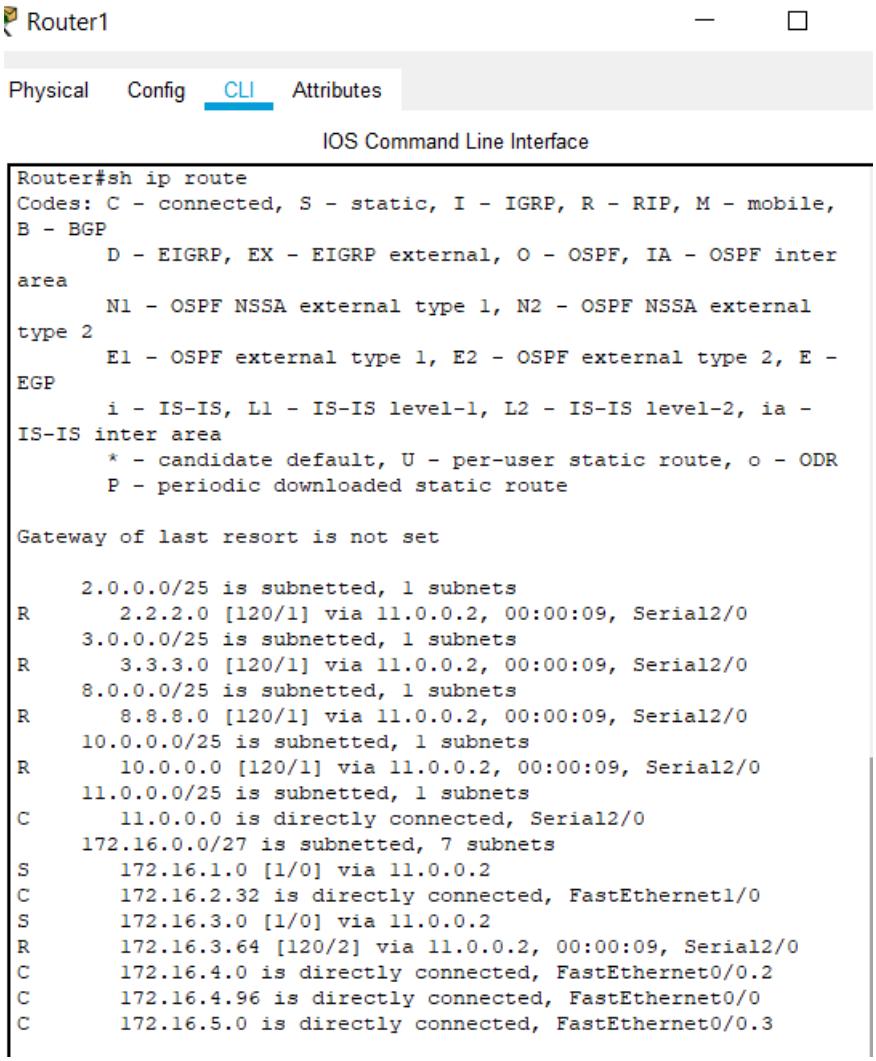
Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
2.0.0.0/25 is subnetted, 1 subnets
R 2.2.2.0 [120/1] via 11.0.0.2, 00:00:09, Serial2/0
3.0.0.0/25 is subnetted, 1 subnets
R 3.3.3.0 [120/1] via 11.0.0.2, 00:00:09, Serial2/0
8.0.0.0/25 is subnetted, 1 subnets
R 8.8.8.0 [120/1] via 11.0.0.2, 00:00:09, Serial2/0
10.0.0.0/25 is subnetted, 1 subnets
R 10.0.0.0 [120/1] via 11.0.0.2, 00:00:09, Serial2/0
11.0.0.0/25 is subnetted, 1 subnets
C 11.0.0.0 is directly connected, Serial2/0
172.16.0.0/27 is subnetted, 7 subnets
S 172.16.1.0 [1/0] via 11.0.0.2
C 172.16.2.32 is directly connected, FastEthernet1/0
S 172.16.3.0 [1/0] via 11.0.0.2
R 172.16.3.64 [120/2] via 11.0.0.2, 00:00:09, Serial2/0
C 172.16.4.0 is directly connected, FastEthernet0/0.2
C 172.16.4.96 is directly connected, FastEthernet0/0
C 172.16.5.0 is directly connected, FastEthernet0/0.3

Figure 3

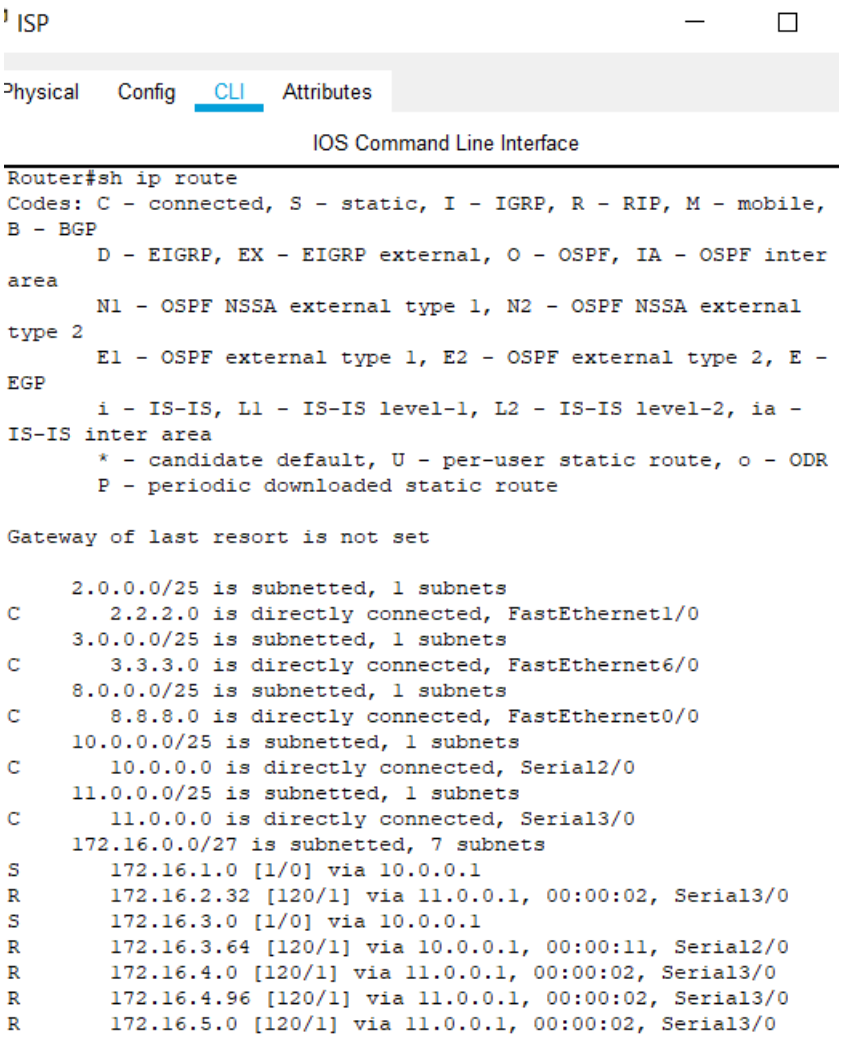

Figure 4

- NAT protocol could have been used to translate the public class A IP address to the private IP address; however, we depended only on routing information.

Addressing Table

Table 1 shows the addressing table for the university network.

Table 5

Addressing Table				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
PC0	NIC	172.16.1.2	255.255.255.224	172.16.1.1
PC1	NIC	172.16.1.3	255.255.255.224	172.16.1.1
PC2	NIC	172.16.1.4	255.255.255.224	172.16.1.1
PC3	NIC	172.16.1.5	255.255.255.224	172.16.1.1
PC4	NIC	172.16.1.6	255.255.255.224	172.16.1.1
Web Server	NIC	172.16.1.7	255.255.255.224	172.16.1.1
Email Server	NIC	172.16.1.8	255.255.255.224	172.16.1.1
Router0	F0/0	172.16.3.65	255.255.255.224	N/A
	F1/0	172.16.1.1	255.255.255.224	N/A
	Se2/0	10.0.0.1	255.255.255.128	N/A
PC5	NIC	172.16.2.34	255.255.255.224	172.16.2.33
PC6	NIC	172.16.2.35	255.255.255.224	172.16.2.33
PC7	NIC	172.16.2.36	255.255.255.224	172.16.2.33
Laptop0	NIC	172.16.2.37	255.255.255.224	172.16.2.33
Laptop1	NIC	172.16.2.38	255.255.255.224	172.16.2.33
Laptop2	NIC	172.16.2.39	255.255.255.224	172.16.2.33
Router1	F0/0	172.16.4.97	255.255.255.224	N/A
	F0/0.2	172.16.4.1	255.255.255.224	N/A
	F0/0.3	172.16.5.1	255.255.255.224	N/A
	F1/0	172.16.2.33	255.255.255.224	N/A
	Se2/0	11.0.0.1	255.255.255.128	N/A
PC8	NIC	172.16.3.66	255.255.255.224	172.16.3.65
PC9	NIC	172.16.3.67	255.255.255.224	172.16.3.65
PC10	NIC	172.16.3.68	255.255.255.224	172.16.3.65
Laptop3	NIC	172.16.3.69	255.255.255.224	172.16.3.65
Laptop4	NIC	172.16.3.70	255.255.255.224	172.16.3.65
Laptop5	NIC	172.16.3.71	255.255.255.224	172.16.3.65
PC11	NIC	172.16.4.2	255.255.255.224	172.16.4.1
PC12	NIC	172.16.4.3	255.255.255.224	172.16.4.1
PC13	NIC	172.16.4.4	255.255.255.224	172.16.4.1
PC14	NIC	172.16.4.5	255.255.255.224	172.16.4.1
PC15	NIC	172.16.4.6	255.255.255.224	172.16.4.1
PC16	NIC	172.16.4.7	255.255.255.224	172.16.4.1
PC17	NIC	172.16.5.2	255.255.255.224	172.16.5.1
PC18	NIC	172.16.5.3	255.255.255.224	172.16.5.1
PC19	NIC	172.16.5.4	255.255.255.224	172.16.5.1
PC20	NIC	172.16.5.5	255.255.255.224	172.16.5.1
PC21	NIC	172.16.5.6	255.255.255.224	172.16.5.1
PC22	NIC	172.16.5.7	255.255.255.224	172.16.5.1
Switch3	VLAN2	172.16.4.1	255.255.255.224	172.16.4.97
	VLAN3	172.16.5.1	255.255.255.224	172.16.4.97

Border Router	Se2/0	10.0.0.2	255.255.255.224	N/A
	Se3/0	11.0.0.2	255.255.255.224	N/A
	F0/0	1.1.1.1	255.255.255.128	N/A
	F1/0	2.2.2.1	255.255.255.128	N/A
	F6/0	3.3.3.1	255.255.255.128	N/A
Google	NIC	8.8.8.2	255.255.255.128	8.8.8.1
YouTube	NIC	2.2.2.2	255.255.255.128	2.2.2.1
Facebook	NIC	3.3.3.2	255.255.255.128	3.3.3.1

Requirements Discussion

VLANs

- As aforementioned, the CSCE and students' labs departments are implemented as virtual LANs, where both are physically connected through a switch, switch 3, but are logically divided into VLAN 2, Students' labs department, and VLAN 3, CSCE department.
- Broadcasts sent by one host are received only by hosts with the same VLAN ID. Hence, VLANs would be useful where users can be grouped together according to their need for network communication, regardless of their actual physical locations.
- Configuration of VLANs was implemented as follows:
  On switch 3:
  - Switch#enable
  - Switch#config terminal
  - Switch(config)#vlan 2
  - Switch(config-vlan)#name Students
  - Switch(config-vlan)#vlan 3
  - Switch(config-vlan)#name CSCE
  - Switch(config-if)#int range fa0/7-12
  - Switch(config-if-range)#switchport mode access
  - Switch(config-if-range)#switchport access vlan 2
  - Switch(config-if-range)#exit
  - Switch(config-if)#int range fa0/1-6
  - Switch(config-if-range)#switchport mode access
  - Switch(config-if-range)#switchport access vlan 3
  - Switch(config-if-range)#exit
  - Switch(config-if)#int f0/13
  - Switch(config-if)#switchport mode trunk
  - Switch(config-if)#exit

  On router 1:

  - Router>enable
  - Router#config terminal
  - Router(config)#int fa0/0
  - Router(config-if)#no shutdown
  - Router(config-if)#int fa0/0.2
  - Router(config-subif)#encapsulation dot1q 2
  - Router(config-subif)#ip add 172.16.4.1 255.255.255.224
  - Router(config-subif)#int fa0/0.3
  - Router(config-subif)#encapsulation dot1q 3
  - Router(config-subif)#ip add 172.16.5.1 255.255.255.224
  - Router(config-subif)#exit
  - Router(config)#exit

Access Lists

- Access lists are used to prevent access for certain networks or end hosts.
- There are two types of access lists: standard access lists and extended access lists. Both types are used to filter traffic coming into or leaving an interface, whereas extended access lists are used to specify different types of traffic such as ICMP, TCP, or UDP.
- Standard access lists were used to control the accessibility of our university network as follows:
    - The CSCE department is denied access to Facebook as follows:
      On the ISP router:
        - Router#config terminal
        - Router(config)#access-list 10 deny 172.16.5.0 0.0.0.31
        - Router(config)#access-list 10 permit any
        - Router(config)#int fa6/0
        - Router(config-if)#ip access-group 10 out
        - Router(config-if)#exit
        - Router(config)#exit
    - Students labs department is denied access to YouTube and Facebook as follows:
      On the ISP router:
        - Router#config terminal
        - Router(config)#access-list 10 deny 172.16.4.0 0.0.0.31
        - Router(config)#access-list 10 permit any
        - Router(config)#int fa1/0
        - Router(config-if)#ip access-group 10 out
        - Router(config-if)#exit
        - Router(config)#exit
        - Router(config)#int fa6/0
        - Router(config-if)#ip access-group 10 out
        - Router(config-if)#exit
        - Router(config)#exit
    - Students labs department is denied access to the accounts department as follows:
      On the router 1:
        - Router#config terminal
        - Router(config)#access-list 10 deny 172.16.4.0 0.0.0.31
        - Router(config)#access-list 10 permit any
        - Router(config)#int fa1/0
        - Router(config-if)#ip access-group 10 out
        - Router(config-if)#exit
        - Router(config)#exit
    - Students labs department is denied access to the IT department as follows:
      On the router 0:
        - Router#config terminal
        - Router(config)#access-list 10 deny 172.16.4.0 0.0.0.31
        - Router(config)#access-list 10 permit any

- Router(config)#int fa1/0
- Router(config-if)#ip access-group 10 out
- Router(config-if)#exit
- Router(config)#exit

Access Validation

- Figures 6 below shows that students labs hosts are denied access to the accounts department.

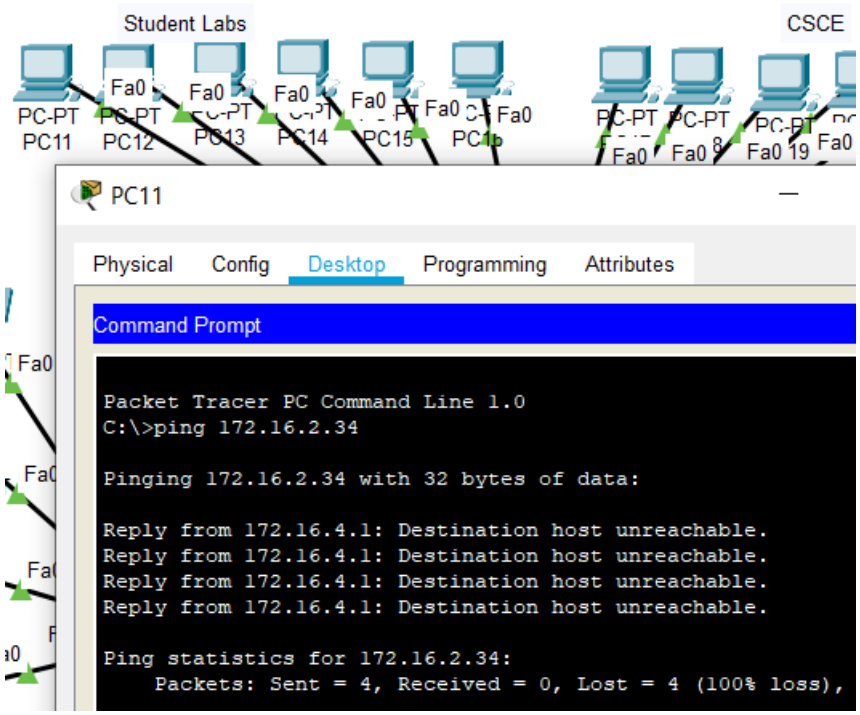

Figure 6

- Figure 7 below shows that accounts hosts are permitted to access the students' labs department. However, the request timeout output shown below is because the ICMP reply packet is denied access to the accounts hosts since it is coming from a restricted network, i.e. students' labs department.
- One possible solution for this is to use an extended access list for the ICMP protocol.

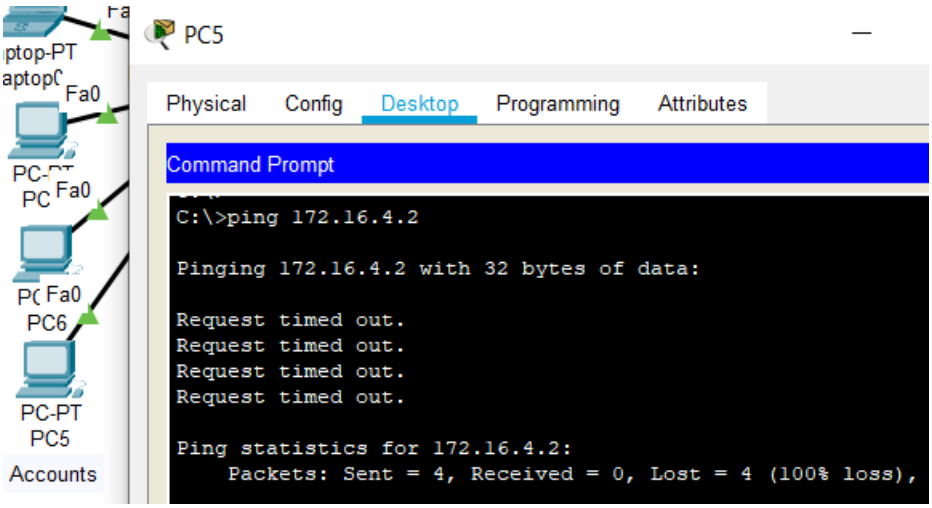

Figure 7

Request timeout Simulation

- Step 1: Packet is sent from an accounts department host and received by a student lab host.

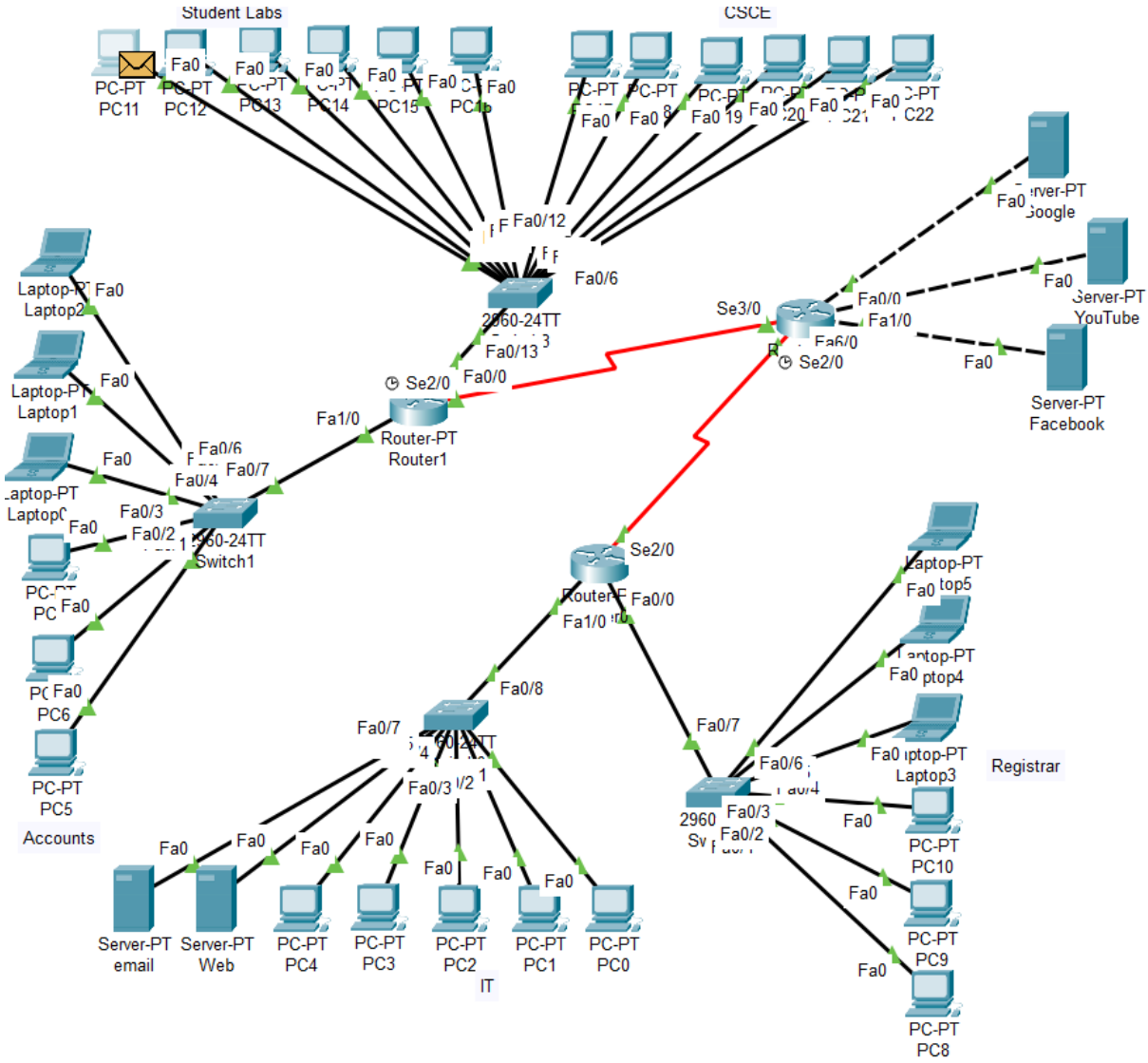

Figure 8

- Step 2: The reply packet is sent from the student lab host to the switch.

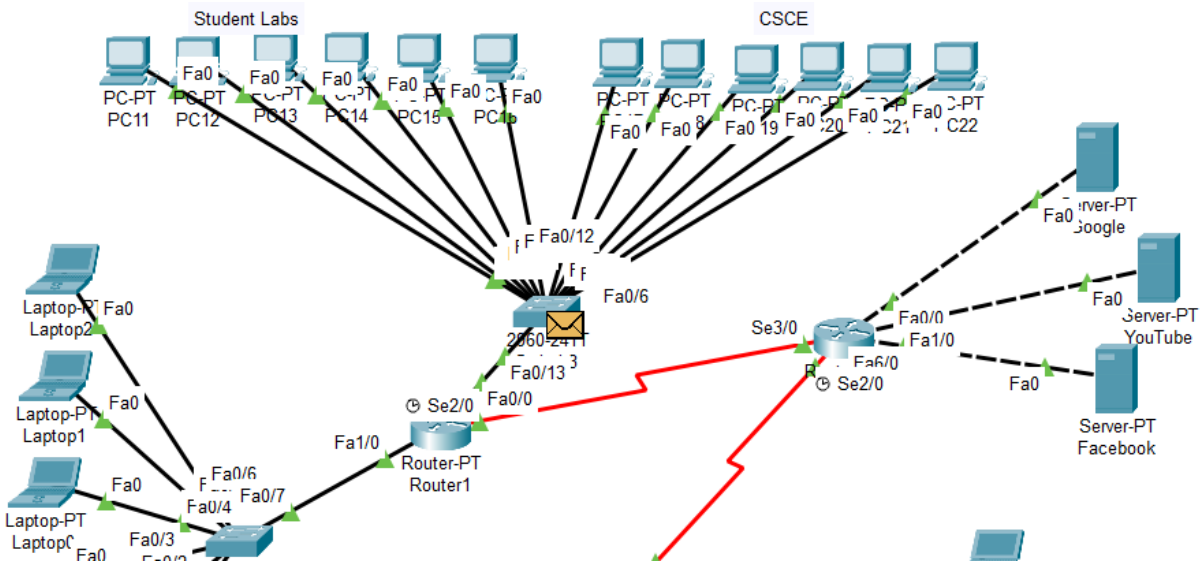

Figure 9

- Step 3: The reply packet is sent to router 1 but is denied access to network 172.16.2.0 on interface 1/0.

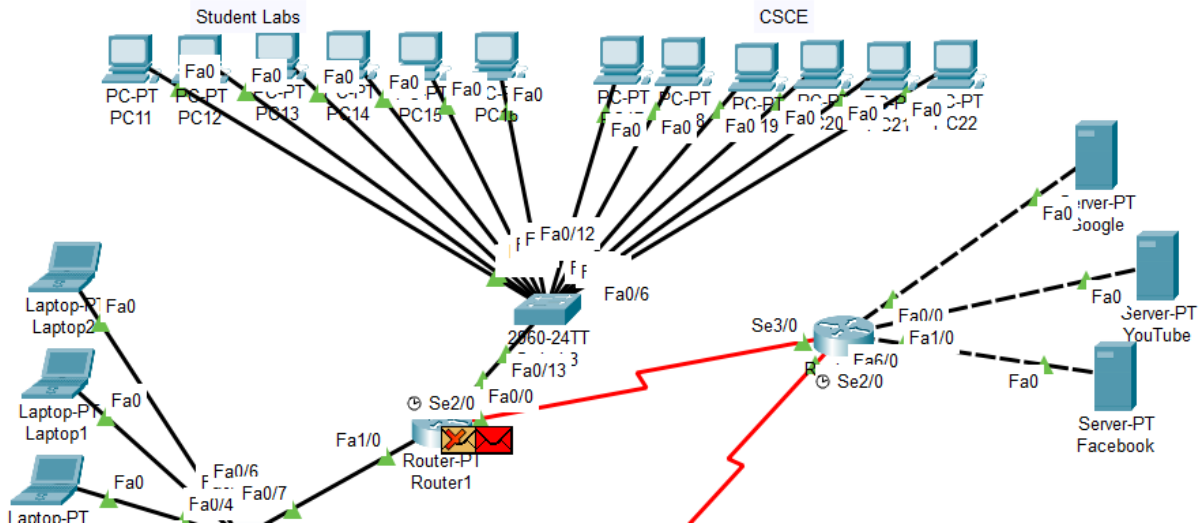

Figure 10

Answers of Questions

1. **Given that the student labs can access only Google, can we deny a host in a certain lab in the school of Eng. & CS access to Google because of an exam ? Justify your answer.**

- Yes, we can deny a host in deny a host in a certain lab in CSCE to access Google in some ways; one of which is using a standard access list as follows:
    - Assume that we have a host with IP address 172.16.5.2 and a subnet mask 255.255.255.224, and assuming that the gateway is interface Fa0/1, then by configuring the gateway's router with the following commands (given that the student labs can access only Google):
      Router1(config)# access-list 10 deny host 172.16.5.2
      Router1(config)# int fa0/1
      Router1(config-if)# ip access-group 10 in
      Router1(config-if)# exit
      Router1(config)# exit

  We have that this host is denied access on the router until it is permitted again.

2. **Assume you find a couple of configuration issues after saving the current configuration in the startup configuration. Thus, you make necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?**

- The configuration at the time of the last save would be restored to the device after the reload, since any changes made to the running configuration after it was last saved are lost.

3. **Why is it necessary to erase the startup configuration before reloading the router?**

- It is necessary to erase the startup configuration before reloading the router since erasing this file allows the router to return to its default configuration after it reloads. Hence, the startup configuration file is loaded into memory to be the running configuration after reloading the router.