EC4060 – COMPUTER AND DATA NETWORK

INDEPENDENT LEARNING AND IMPLEMENTATION ASSIGNMENT

BANDARA H.G.T.D.

2022/E/048

GROUP CG04

SEMESTER 04

2025/02/02

* Requirements Given

**Objective:** Apply the principles of network design to create and simulate a functional network infrastructure for an institution with multiple branches.

**Scenario**: The Engineering Faculty consists of 5 academic departments (Civil, Mechanical, EEE, Computer, and Interdisciplinary Studies) and 1 Administration Section, requiring a scalable and secure network.

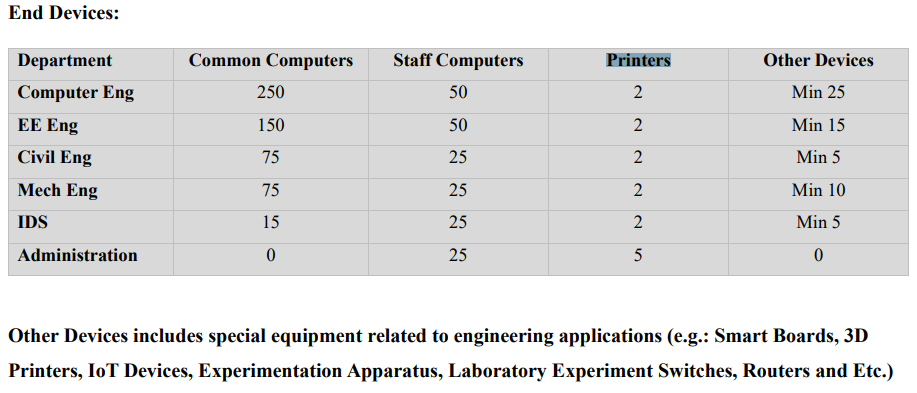
**Task:** The student is tasked with designing and simulating this network while ensuring:

* + Unique subnet allocation for each section.
  + • Identification of subnet information, including subnet mask, usable host range,
  + and broadcast address.
  + • Scalability to accommodate at least 30% future growth in each section.

**Categorization of Devices :** Separate devices for staff and students within each department.

**Common Devices**: Include department-specific printers and shared devices accessible only by staff.

**Central CCTV System: :** A unified subnet for CCTV cameras covering all departments.



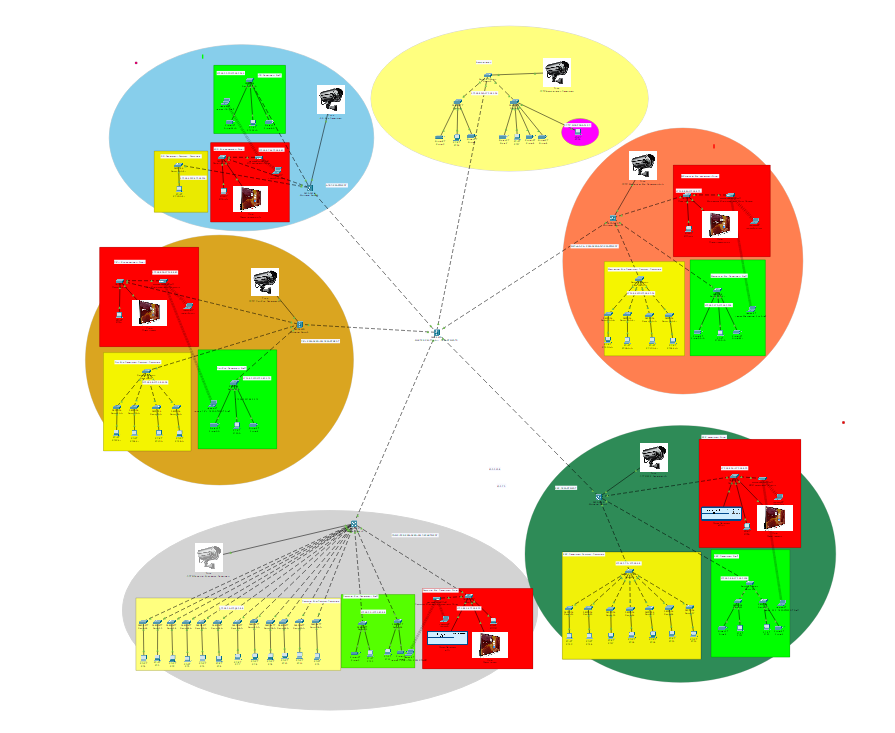
**SUBNETTING CALCULATIONS WITH TABLES FOR EACH SUBNET**

**TABLE 01: THE TABLE OF VLAN ID AND USABLE IP RANGE**

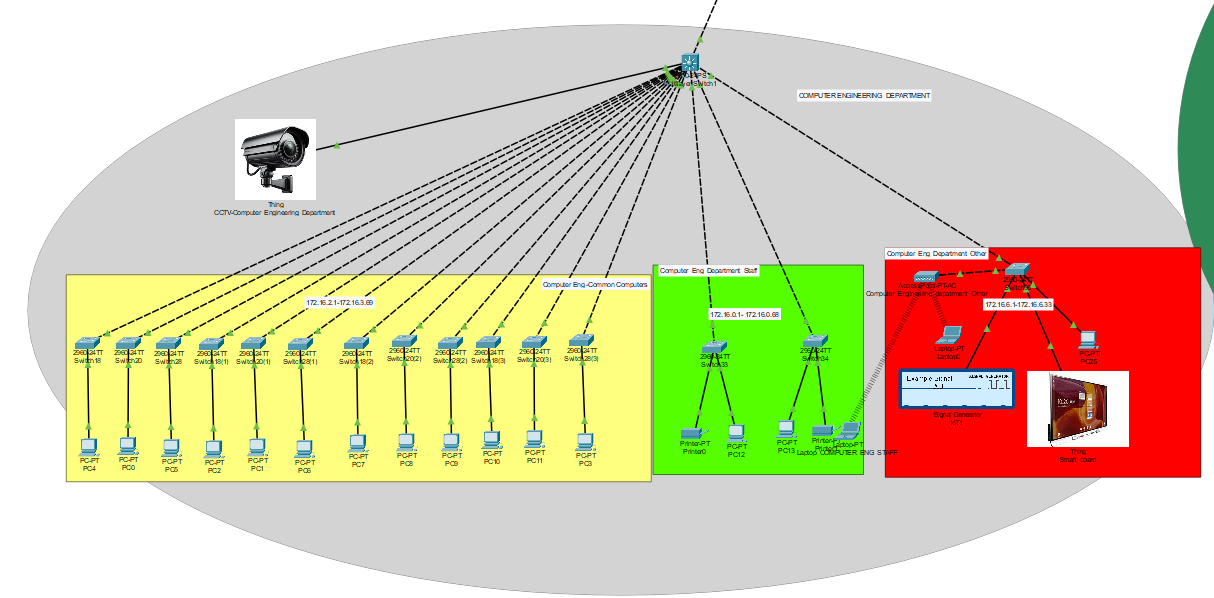
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VLAN-ID | Department | Category | Current | After 30% Growth | Subnet | Usable Range | Broadcast |
| 100 | | Computer | Staff & Printers | 52 | 68 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 100 | Electrical | Staff & Printers | 52 | 68 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 100 | Civil | Staff & Printers | 27 | 35 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 100 | Mechanical | Staff & Printers | 27 | 35 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 100 | IDS | Staff & Printers | 27 | 35 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 100 | Administration | Staff & Printers | 30 | 39 | 172.16.0.0/23 | 172.16.0.1 - 172.16.1.254 | 172.16.1.255 |
| 200 | Computer | Common Computers | 250 | 325 | 172.16.2.0/22 | 172.16.2.1 - 172.16.5.254 | 172.16.5.255 |
| 200 | Electrical | Common Computers | 150 | 195 | 172.16.2.0/22 | 172.16.2.1 - 172.16.5.254 | 172.16.5.255 |
| 200 | Civil | Common Computers | 75 | 98 | 172.16.2.0/22 | 172.16.2.1 - 172.16.5.254 | 172.16.5.255 |
| 200 | Mechanical | Common Computers | 75 | 98 | 172.16.2.0/22 | 172.16.2.1 - 172.16.5.254 | 172.16.5.255 |
| 200 | IDS | Common Computers | 15 | 20 | 172.16.2.0/22 | 172.16.2.1 - 172.16.5.254 | 172.16.5.255 |
| 300 | Computer | Other Devices | 25 | 33 | 172.16.6.0/25 | 172.16.6.1 - 172.16.6.126 | 172.16.6.127 |
| 300 | Electrical | Other Devices | 15 | 20 | 172.16.6.0/25 | 172.16.6.1 - 172.16.6.126 | 172.16.6.127 |
| 300 | Civil | Other Devices | 5 | 7 | 172.16.6.0/25 | 172.16.6.1 - 172.16.6.126 | 172.16.6.127 |
| 300 | Mechanical | Other Devices | 10 | 13 | 172.16.6.0/25 | 172.16.6.1 - 172.16.6.126 | 172.16.6.127 |
| 300 | IDS | Other Devices | 5 | 7 | 172.16.6.0/25 | 172.16.6.1 - 172.16.6.126 | 172.16.6.127 |
| 400 | All Departments | CCTV | 40 | 52 | 172.16.6.128/26 | 172.16.6.129 - 172.16.6.190 | 172.16.6.191 |

**TABLE 02: THE STARTING AND END IP FOR EACH DEPARTMENT AND SUBNET MASK**

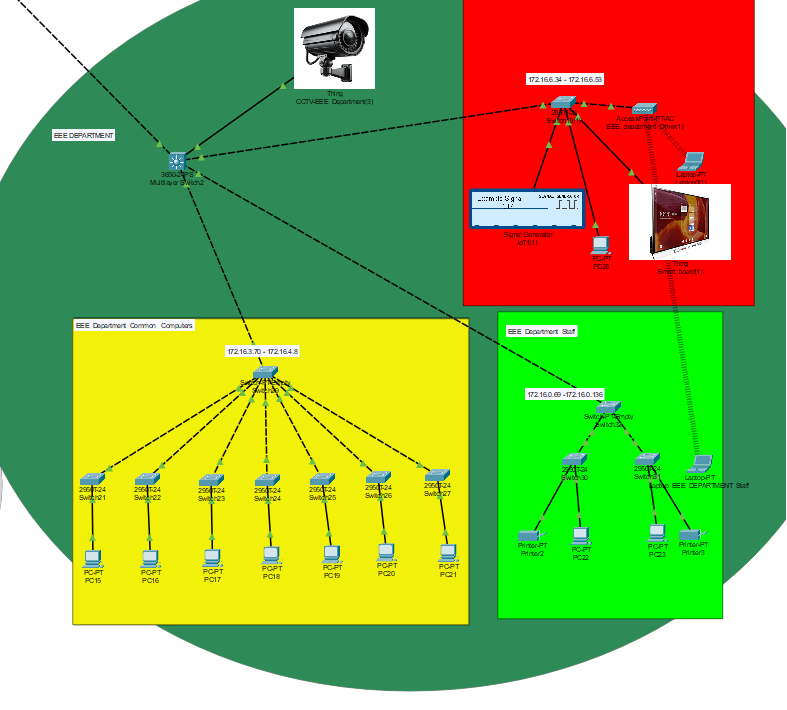
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VLAN | Department | Section | Subnet | Start IP | End IP | Total IPs | Subnet Mask |
| 200 | Computer | Common Computers | 172.16.2.0/23 | 172.16.2.1 | 172.16.3.69 | 325 | 255.255.252.0 |
| 200 | Electrical | Common Computers | 172.16.3.70/24 | 172.16.3.70 | 172.16.4.8 | 195 | 255.255.252.0 |
| 200 | Civil | Common Computers | 172.16.4.9/25 | 172.16.4.9 | 172.16.4.106 | 98 | 255.255.252.0 |
| 200 | Mechanical | Common Computers | 172.16.4.107/25 | 172.16.4.107 | 172.16.4.204 | 98 | 255.255.252.0 |
| 200 | IDS | Common Computers | 172.16.4.205/27 | 172.16.4.205 | 172.16.4.224 | 20 | 255.255.252.0 |
| 100 | Computer | Staff & Printers | 172.16.0.1/26 | 172.16.0.1 | 172.16.0.68 | 68 | 255.255.254.0 |
| 100 | Electrical | Staff & Printers | 172.16.0.69/26 | 172.16.0.69 | 172.16.0.136 | 68 | 255.255.254.0 |
| 100 | Civil | Staff & Printers | 172.16.0.137/26 | 172.16.0.137 | 172.16.0.171 | 35 | 255.255.254.0 |
| 100 | Mechanical | Staff & Printers | 172.16.0.172/26 | 172.16.0.172 | 172.16.0.206 | 35 | 255.255.254.0 |
| 100 | IDS | Staff & Printers | 172.16.0.207/26 | 172.16.0.207 | 172.16.0.241 | 35 | 255.255.254.0 |
| 100 | Administration | Staff & Printers | 172.16.0.242/26 | 172.16.0.242 | 172.16.1.24 | 39 | 255.255.254.0 |
| 300 | Computer | Other Devices | 172.16.6.1/26 | 172.16.6.1 | 172.16.6.33 | 33 | 255.255.255.128 |
| 300 | Electrical | Other Devices | 172.16.6.34/27 | 172.16.6.34 | 172.16.6.53 | 20 | 255.255.255.128 |
| 300 | Civil | Other Devices | 172.16.6.54/28 | 172.16.6.54 | 172.16.6.60 | 7 | 255.255.255.128 |
| 300 | Mechanical | Other Devices | 172.16.6.61/28 | 172.16.6.61 | 172.16.6.73 | 13 | 255.255.255.128 |
| 300 | IDS | Other Devices | 172.16.6.74/28 | 172.16.6.74 | 172.16.6.80 | 7 | 255.255.255.128 |
| 400 | All Departments | CCTV | 172.16.6.128/26 | 172.16.6.129 | 172.16.6.180 | 52 | 255.255.255.192 |

**TOPOLOGY DIAGRAM**

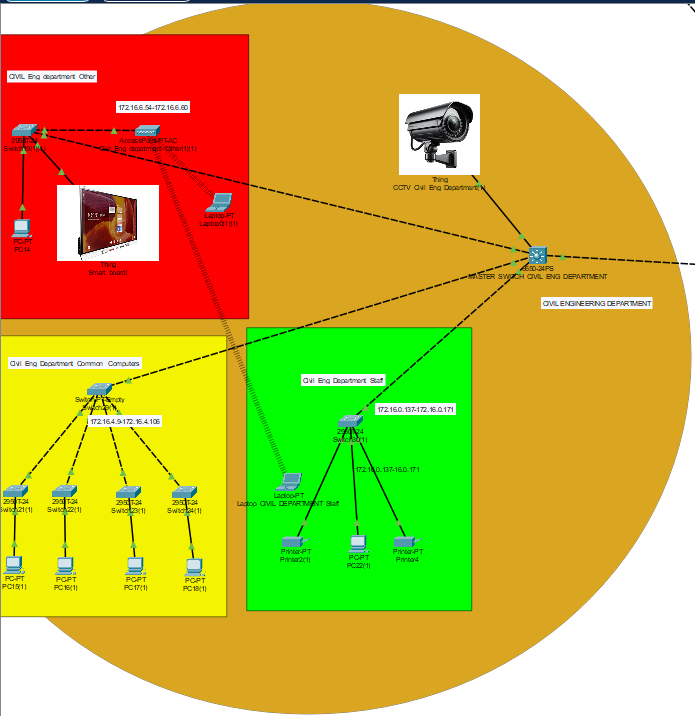
**FIGURE 01: THE FULL NETWORK DIAGRAM**



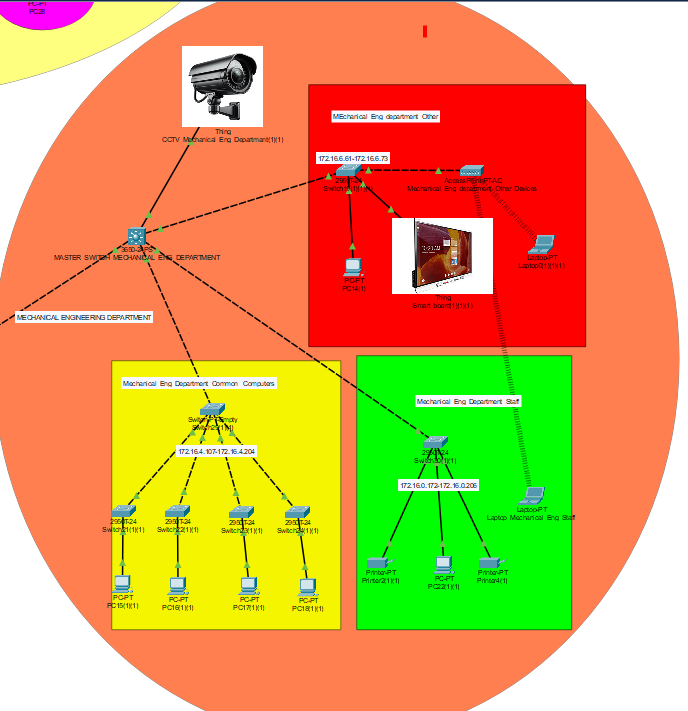
**FIGURE 02: THE NETWORK DIAGRAM OF COMPUTER ENGINEERING DEPARTMENT**



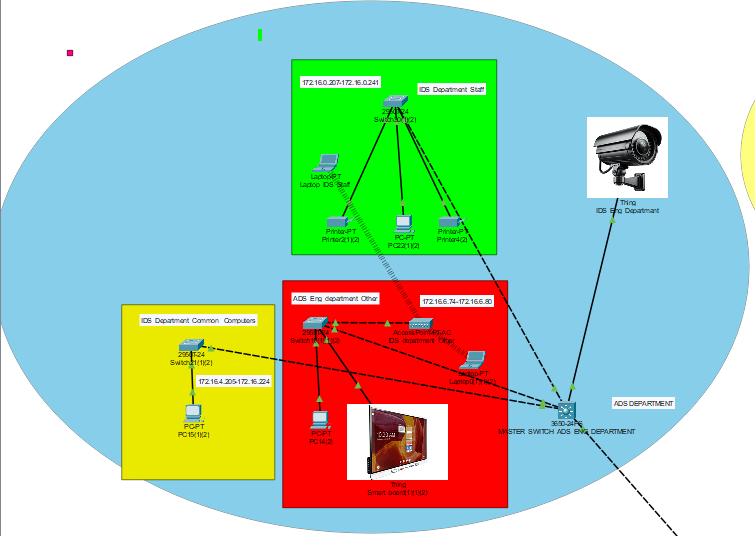
**FIGURE 03: THE NETWORK DIAGRAM OF EEE DEPARTMENT**



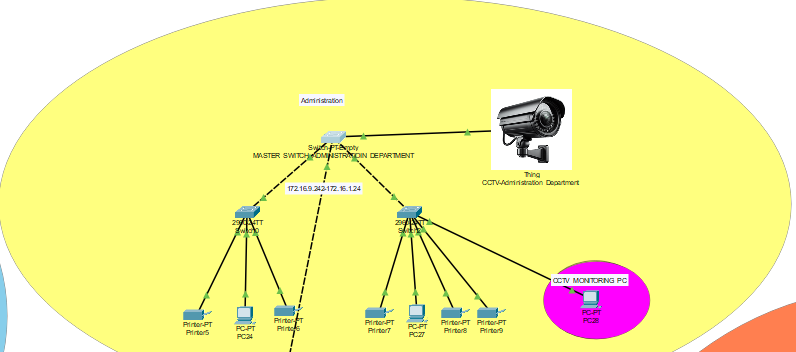
**FIGURE 04: THE NETWORK DIAGRAM OF CIVIL ENGINEERING DEPARTMENT**



**FIGURE 05: THE NETWORK DIAGRAM OF MECHANICAL ENGINEERING DEPARTMENT**

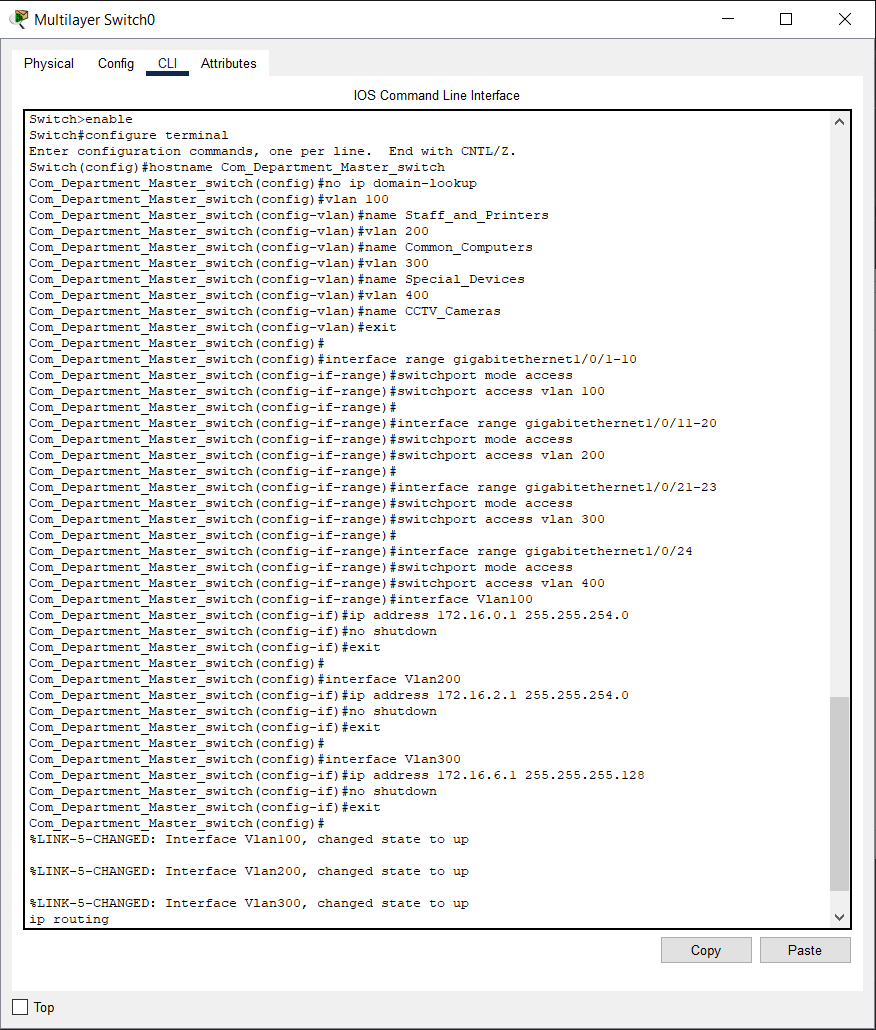
****

**FIGURE 06: THE NETWORK DIAGRAM OF ADS ENGINEERING DEPARTMENT**



**FIGURE 07: THE NETWORK DIAGRAM ADMINISTRATION DEPARTMENT**

**CONFIGURATION SCRIPTS**

****

**FIGURE 08: CONFIGURE MASTER SWITCH IN COMPUTER ENGINEERING DEPARTMENT**

**The configuring code for the master switch in Computer Engineering Department**

enable

configure terminal

hostname Com\_Department\_Master\_switch

no ip domain-lookup

vlan 100

name Staff\_and\_Printers

vlan 200

name Common\_Computers

vlan 300

name Special\_Devices

vlan 400

name CCTV\_Cameras

exit

interface range gigabitethernet1/0/1-10

switchport mode access

switchport access vlan 100

interface range gigabitethernet1/0/11-20

switchport mode access

switchport access vlan 200

interface range gigabitethernet1/0/21-23

switchport mode access

switchport access vlan 300

interface range gigabitethernet1/0/24

switchport mode access

switchport access vlan 400

interface Vlan100

ip address 172.16.0.1 255.255.254.0

no shutdown

exit

interface Vlan200

ip address 172.16.2.1 255.255.254.0

no shutdown

exit

interface Vlan300

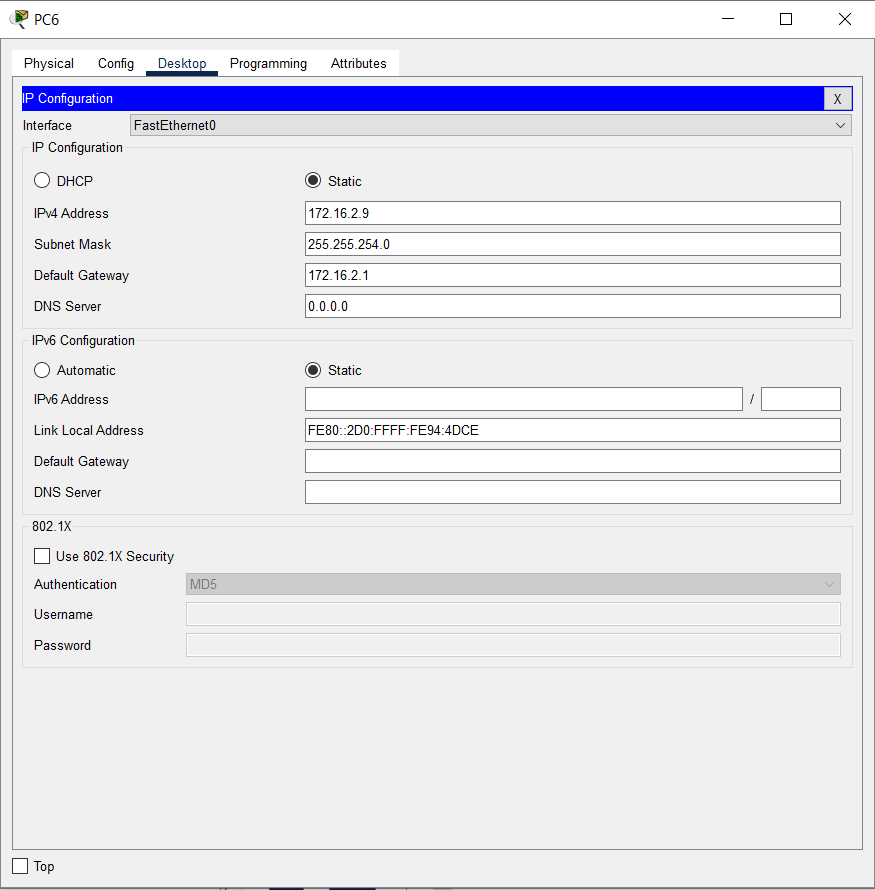
ip address 172.16.6.1 255.255.255.128

no shutdown

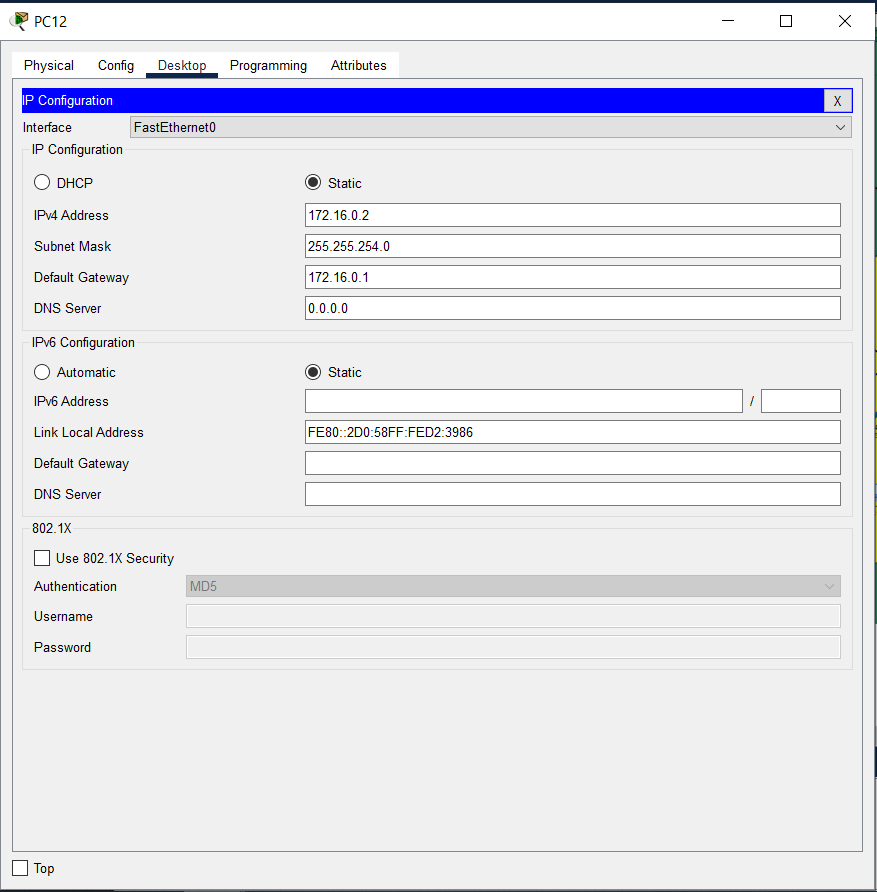
exit

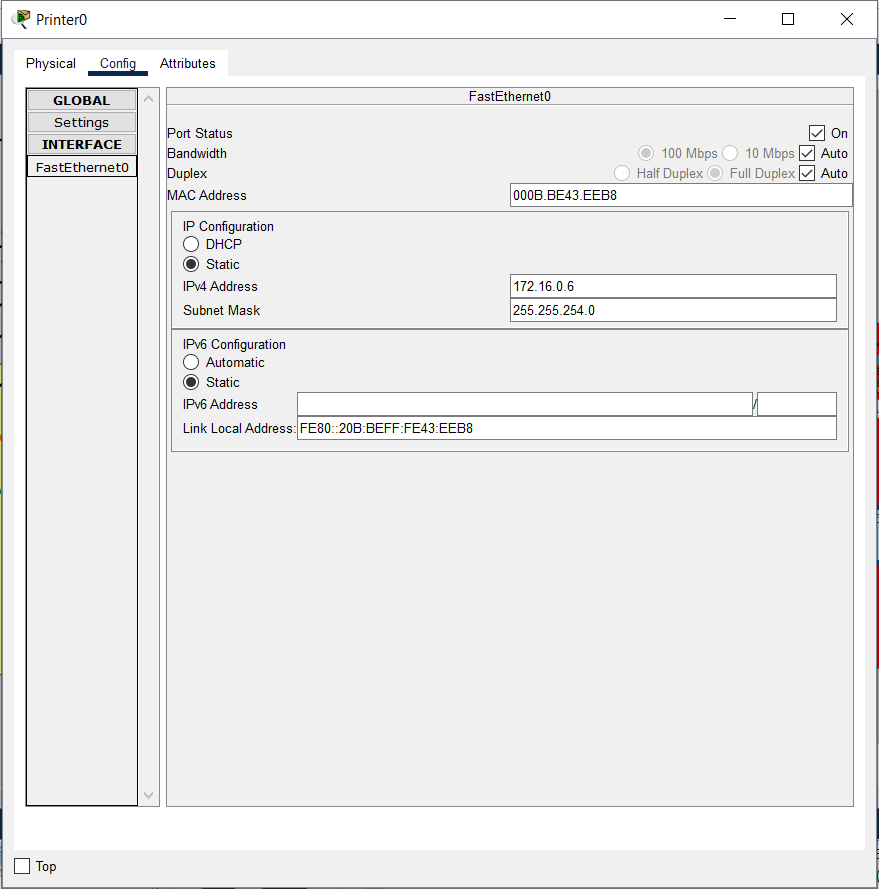
ip routing

end

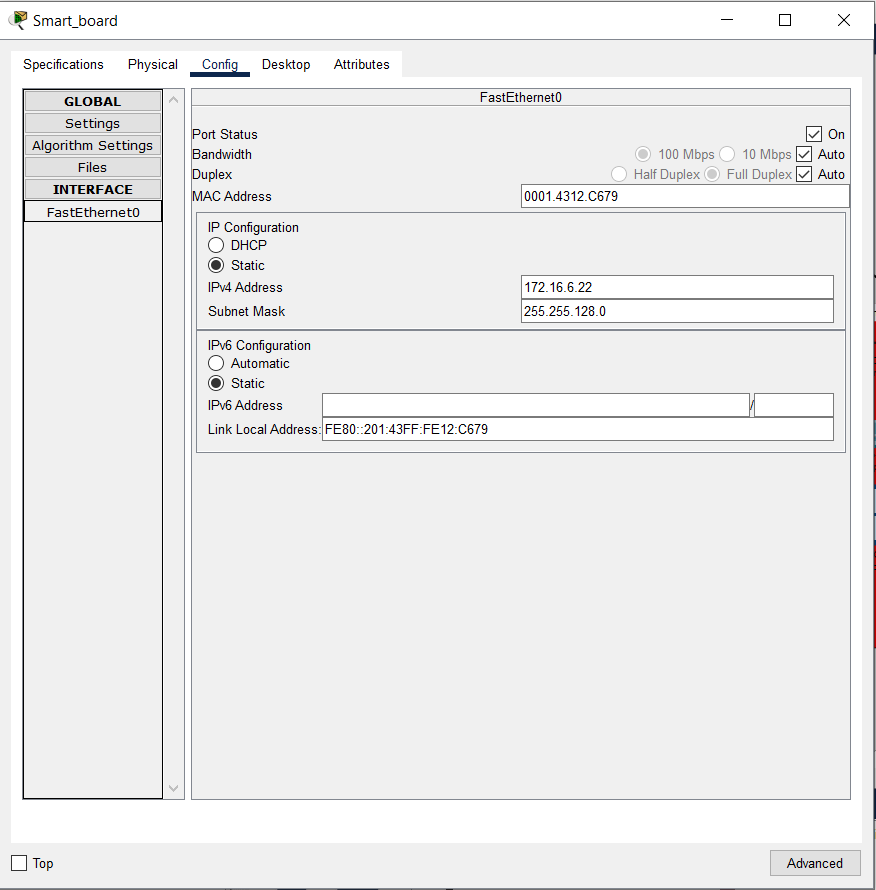
write memory

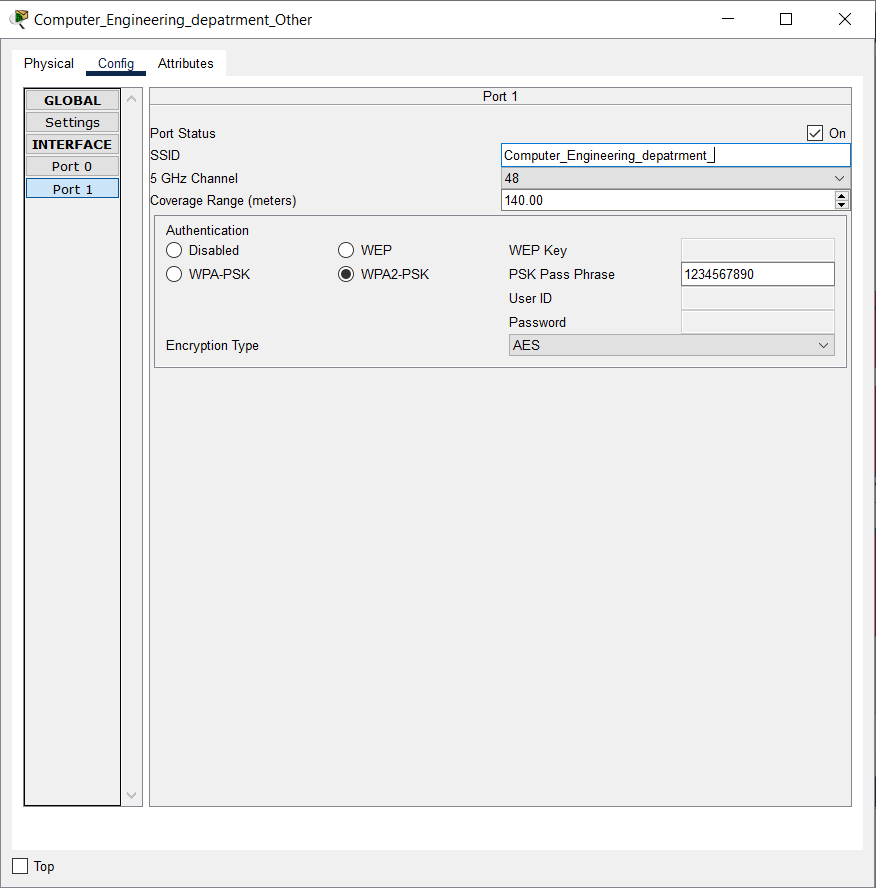
**FIGURE 09: CONFIGURE THE COMMON PC IN COMPUTER DEPARTMENT**



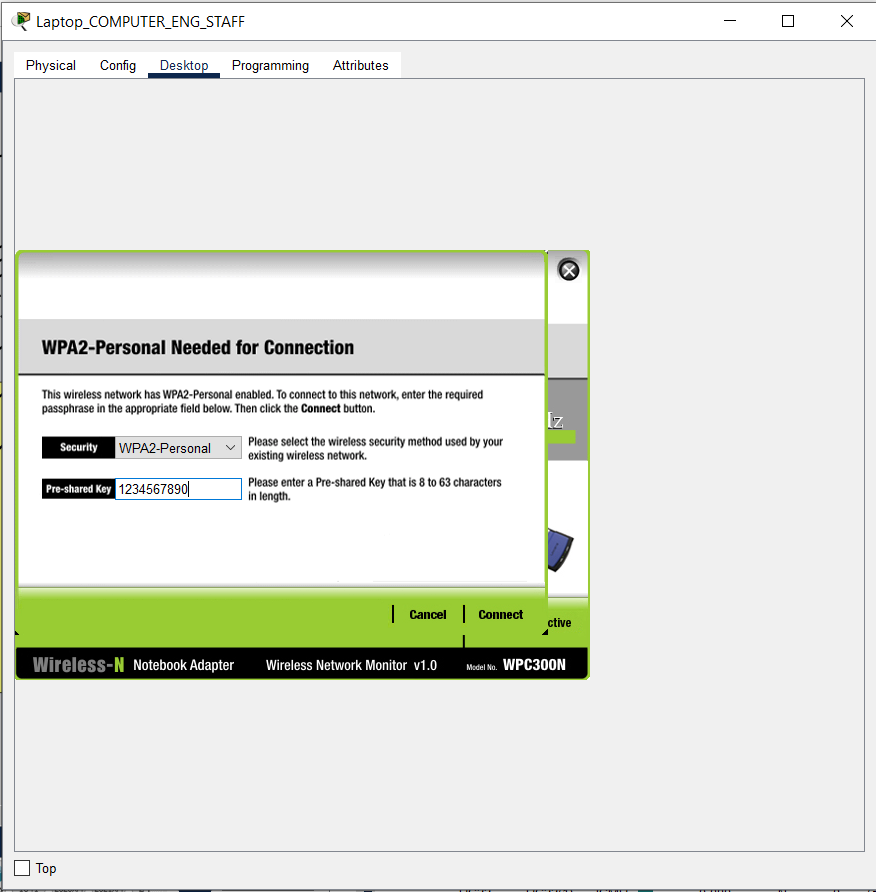
**FIGURE 10: CONFIGURE THE STAFF PC IN COMPUTER ENGINEERING DEPARTMENT**

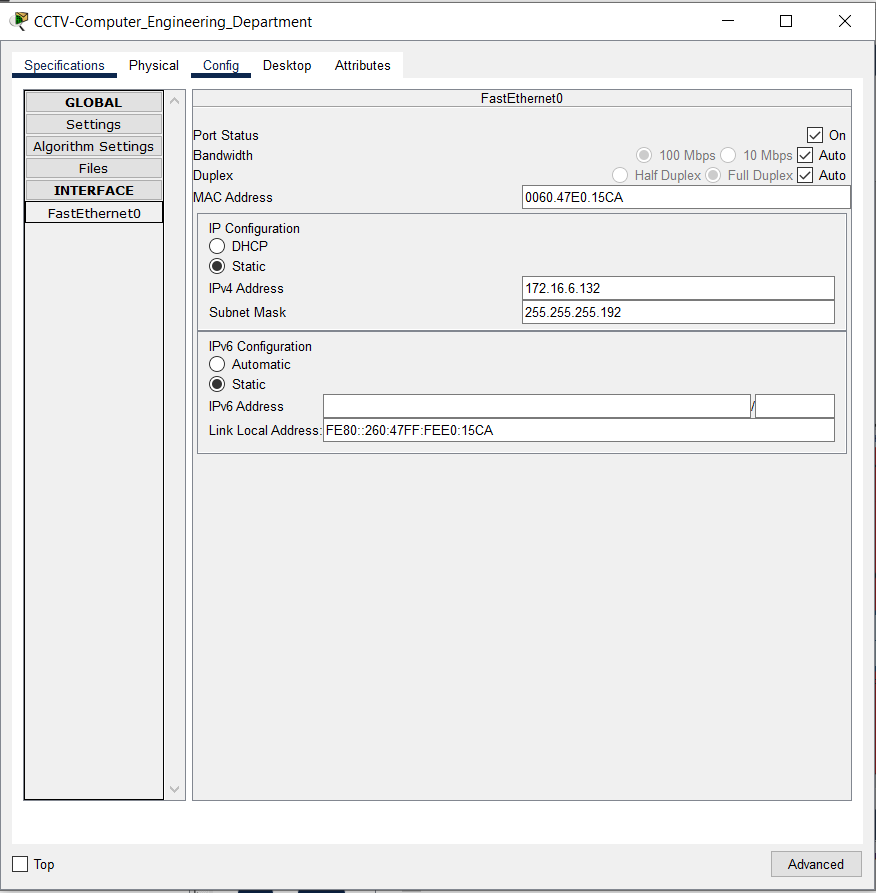
**FIGURE 11: CONFIGURE A PRINTER IN COMPUTER ENGINEERING DEPARTMENT**



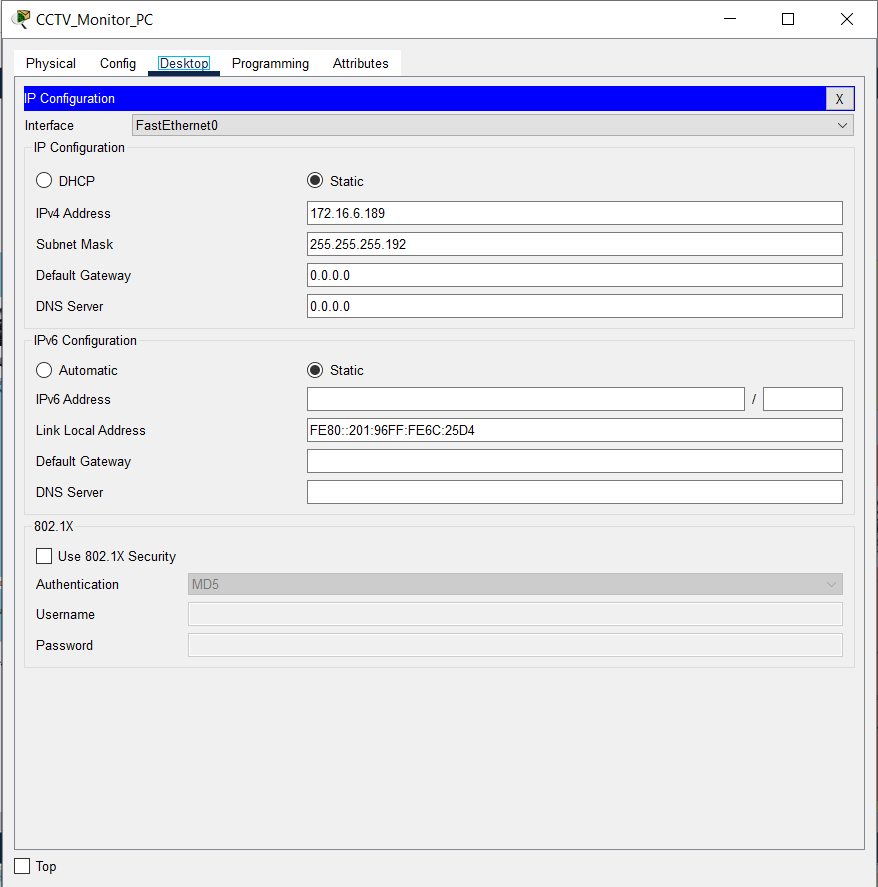
**FIGURE 12: CONFIGURE THE SMART BOARD (OTHER DEVICES) IN COMPUTER ENGINEERING DEPARTMENT**

**FIGURE 13: CONFIGURE THE OTHER DEVICES’ WI-FI IN COMPUTER ENGINEERING DEPARTMENT**

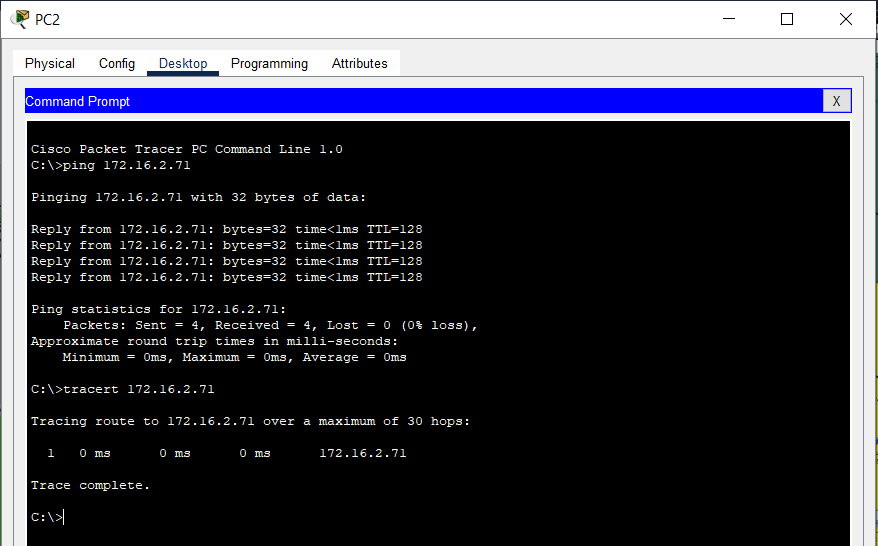


**FIGURE 14: CONNECT TO THE OTHER DEVICES’ WI-FI BY A STAFF LAPTOP IN COMPUTER ENGINEERING DEPARTMENT**

**FIGURE 15: CONFIGURE THE CCTV IN COMPUTER ENGINEERING DEPARTMENT**

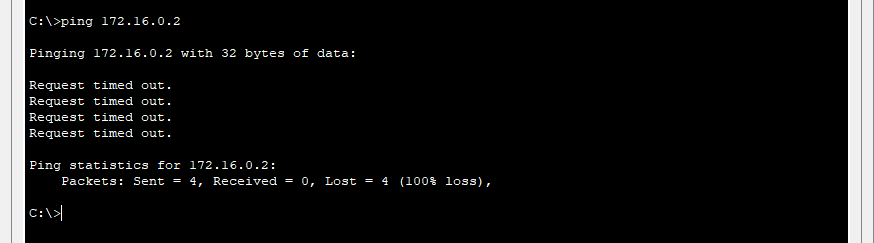


**FIGURE 16: CONFIGURE THE CCTV MONITOR PC IN ADMINISTRATION DEPARTMENT**

**SIMULATION RESULTS**

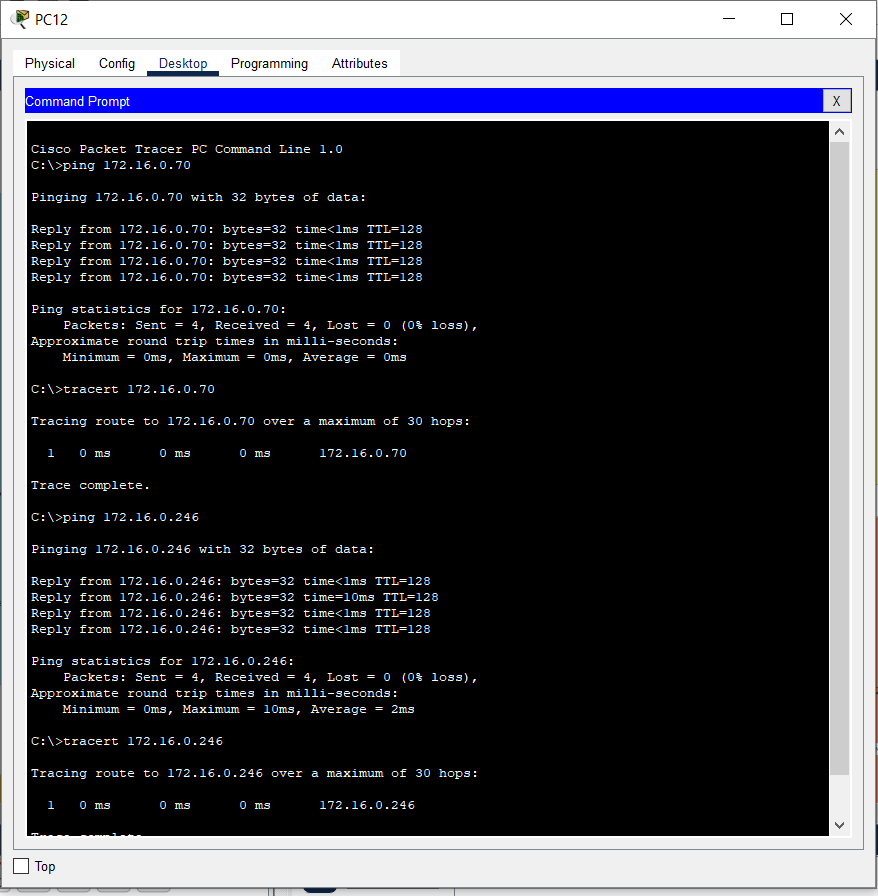
**FIGURE 17: PING AND TRACEROUTE TEST BETWEEN COMPUTER ENG AND EEE COMMON COMPUTERS**

**Note:** The common computers of the Computer Engineering Department and EEE department in same subnet and they only can access each other, and they can’t access staff, other devices and CCTV networks (for security purpose).



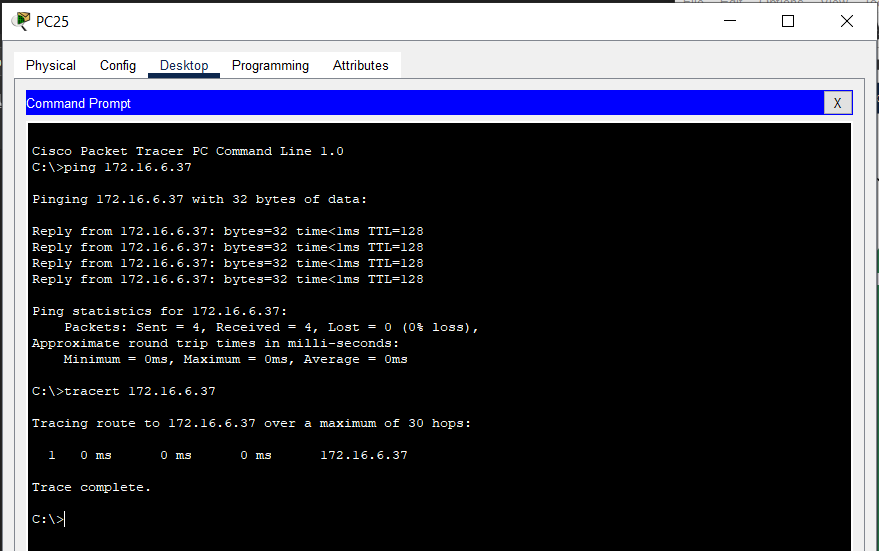
**FIGURE 18: PING TEST BETWEEN COMPUTER ENG COMMON COMPUTER AND STAFF COMPUTERS (STUDENT CAN’T** **ACCESS STAFF)**

**Note:** The common computers of the departments can’t access the staff network (For security reasons)



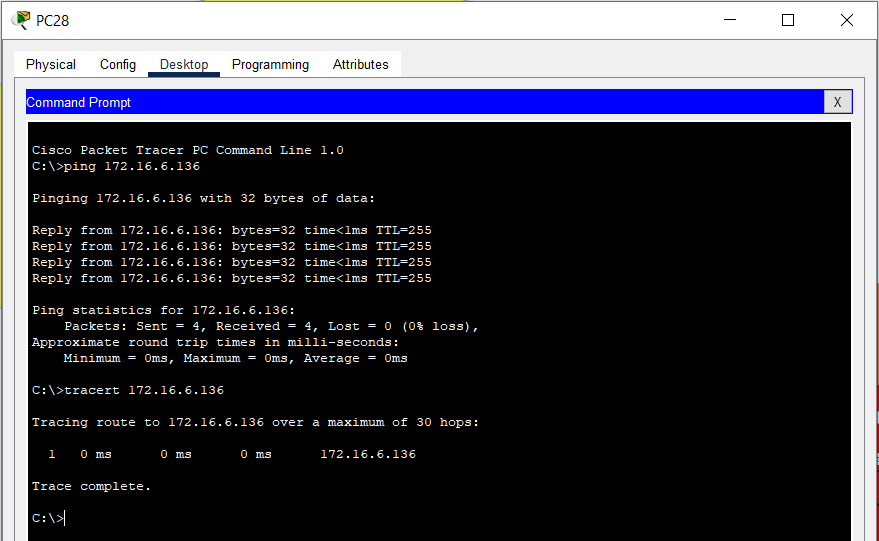
**FIGURE 19: PING AND TRACEROUTE TEST BETWEEN COMPUTER ENG STAFF AND EEE STAFF COMPUTERS AND THE ADMIN COMPUTERS**

**Note:** Staff computers in all departments are in same subnetwork and all staff members can access the staff network, and the all-staff members can access the printers also, and the administration also in staff subnetwork, then they also can access the Staff network. I put all staff computer network because if any printer down in any department they can get the print using another department, also he can get that print from administration building. And for the IOT devices I use Wi-Fi access for that devices and only special members in staff like Lectures and Instructors only have the access to that network. I use Passkey (1234567890) for connect that Other devices, and the special members only Know the passkey. I use this method because in Other Devices includes special equipment related to engineering applications and when the deal with such like valuable items they should have proper knowledge for working with them, That is the reason that items also have limited access for special staff members.

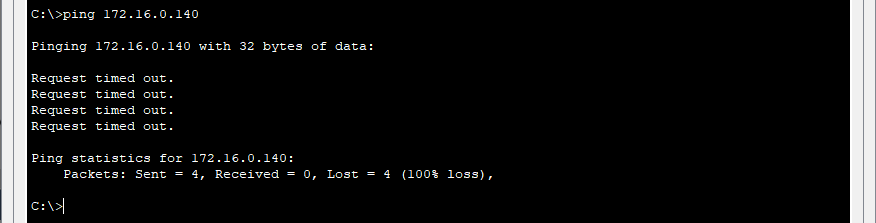


**FIGURE 20: PING AND TRACEROUTE TEST BETWEEN COMPUTER ENG OTHER DEVICES AND EEE OTHER DEVICES**

**Note:** The other-devices of all department in same sub network and they can access each other and limited access for special staff members for this devices because of security purpose. And for the IOT devices I use Wifi access for that devices and only special members in staff like Lectures and Instructors only have the access to that network. I use Passkey (1234567890) for connect that Other devices, and the special members only Know the passkey. I use this method because in Other Devices includes special equipment related to engineering applications and when the deal with such like valuable items they should have proper knowledge for working with them, That is the reason that items also have limited access for limited special staff members.



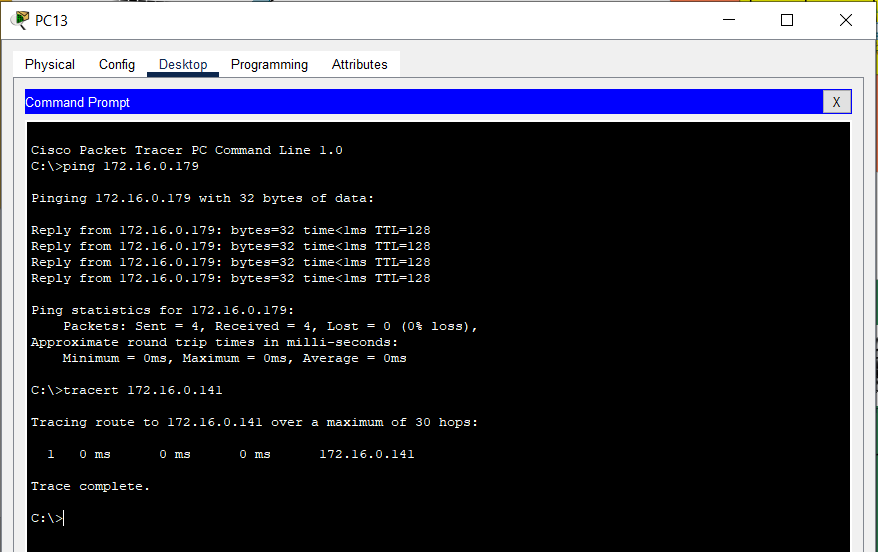
**FIGURE 21: PING AND TRACEROUTE TEST BETWEEN CCTV STATION IN ADMIN AND A CCTV (HAVE ACCESS)**

****

**FIGURE 22: PING AND TRACEROUTE TEST BETWEEN CCTV AND STAFF (EVEN STAFF MEMBERS ALSO DON’T HAVE ACCESS)**

**Note:** I designed the CCTV in another subnet and it only access by the CCTV network. I design this network and any other member can’t access this network even staff members. Only access this network by the special computer for monitor the CCTV devices placed in Administration department.

I designed this because of if staff members have access for this network all the staff members can access this network. If any person in network can change the data of this CCTV network. But in this design, only person who have special access only can access this network. Then we can ensure about the **security**.



**FIGURE 23: PING AND TRACEROUTE TEST BETWEEN COMPUTER ENG STAFF AND PRINTER IN CIVIL DEPARTMENT AND MECHANICAL DEPARTMENT**

**Note:** In this network diagram, any staff members have access to the all printers in all department, they also have access to the printers in the admin department. Because if any printer failure occurs in any department, they can use another printer in any other department. That method is more effective.

**SUMMARY OF ADDED DEVICES AND NETWORK PERFORMANCE**

In this network all **common computers** are in same subnet and each common computers can access another common computer, furthermore common computers in Computer Engineering and EEE department are in same subnet and they also can access more easily, I designed like that because in those two departments more have common practices and more same activities. In other department all the common computers are in same subnet and they also can access the subnet easily. Then any common computer don’t have access to staff , other, administration or CCTV network. I restrict them because considering about security reason.

And when the considering the **staff** subnet, I created a subnet for all the staff members in all departments and the **Administration department** also in that subnet . All the printers are connected to that staff subnet. Then the staff member can get the print from any department, if other printer fails in that department.

And when considering about the **Other Devices** all the other devices also in other subnet in all department, then all other devices can access each other. Furthermore, it also have limited access by the special staff members in each department. They can access the common devices subnet by WI-FI access point. The only staff member who has the passkey (1234567890) can access that network. And for Other devices I use Wi-Fi access for that devices and only special members in staff like Lectures and Instructors only have the access to that network. I use Passkey (1234567890) for connect those other devices, and the special members only Know the passkey. I use this method because in Other Devices includes special equipment related to engineering applications and when the deal with such like valuable items, they should have proper knowledge for working with them, that is the reason that items also have limited access for special staff members.

When the consider about the **CCTV** that is the network which need some additional security. Then in this network diagram CCTV belongs to another subnet. Then for security purpose that subnet only access by the special computer places in administration block. I separate CCTV subnet from staff network also, because if it gives access to the staff members all members in the staff subnet can access the CCTV network. When that is considering about security that is not acceptable. That is the reason all the CCTV in Other subnet that only access by Admin.

This designed was created for using minimal resources and better network performance.