Campus Network Design

(Engineering Faculty & Workshops)

Course Name:
computer network

Submitted by:
Rowaida Abdel Nasser Hassan

Supervised by:

Dr. Ahmed Magdy

Faculty of Engineering
[Suez Canal University]
Department of Computer and Control Engineering

Academic Year: 2024 / 2025

Date of Submission:
Jun 2025

INTRODUCTION:

The Faculty of Engineering supports students and staff across various engineering and computing departments. Each member of staff has a (PC), while students have access to PCs in dedicated computer labs.

Create a network topology with the main components to support the following:

- **MAIN OBJECTIVES:**

  The main objectives of a Faculty of Engineering Network design are to provide efficient and reliable communication between devices on the college, while also providing security and management of the network. Some of the specific objectives that a college network design may aim to achieve include:

  o **Scalability:** The ability to easily add new devices and users to the network without disrupting existing communication.

  o **Performance:** Providing fast and reliable communication between devices, with minimal delays and data loss.

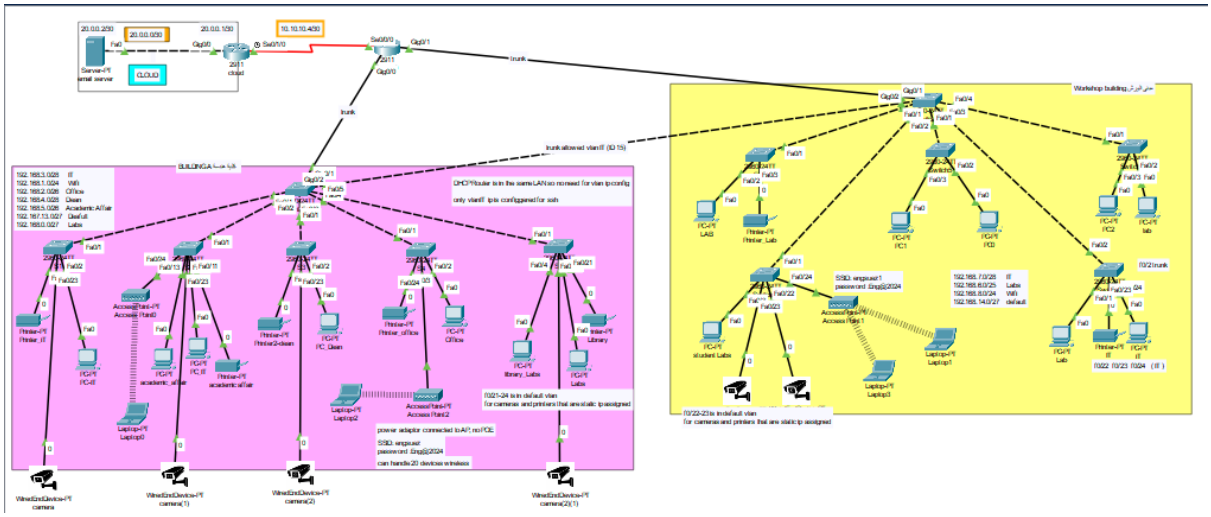
  o **Security:** Protecting the network and its users from unauthorized access.

COMPONENTS USED:

- Two Routers(Main-Router & Cloud-Router)
- Access Layer Switches
- PC's, printers & cameras (End devices)
- Email server
-

METHODOLOGY:

a-Create a network topology with the main components to support the following;



College Building (BUILDING A):

The college building is organized into four main levels, each dedicated to specific administrative, academic, and technical functions, with network segmentation implemented through VLANs for enhanced security and traffic management.

- **Basement**: **Academic affair staff department and Library.**
  - Their network connections are separated by configuring each department into its own VLAN. This ensures better network management, enhanced security, and optimized traffic control within the Faculty of Engineering's network infrastructure .

- **Ground Floor:** Academic affair staff, IT departments Security Office and Lecture Halls.
  - Their network connections are separated by configuring each department into its own VLAN; While IT has the access to all departments networks.

- **First Floor:** Administrative Offices, Heads of Departments' Offices and Lecture Halls.
  - Their network connections are separated by configuring each department into its own VLAN.
- **Scond Floor:** Heads of Departments' Offices, Lecture Halls.
  - Their network connections are separated by configuring each department into its own VLAN.

Workshop Building (BUILDING B**):**

The Workshop Building is designed to support the practical and technical needs of students, with a focus on providing resources for hands-on learning and computer-based activities.

Fourth Floor:

- Four student computer Laboratories:
  - All four computer Laboratories share the same VLAN, ensuring streamlined communication and resource sharing between the labs

b. You will be expected to configure the core devices and few end devices to provide end-to-end connectivity and access to the internet servers .

- Each department is expected to be on its own separate IP network.
- The switches should be configured with appropriate VLANs and security settings.
- The end devices will be expected to acquire dynamic IP addresses from a router-based DHCP server.

TECHNOLOGIES IMPLEMENTED:

1. Creating a network topology using Cisco Packet Tracer.

2. Hierarchical Network Design.

3. Connecting Networking devices with Correct cabling.

4. Creating VLANs and assigning ports VLAN numbers.

5. Subnetting and IP Addressing.

6. Configuring Inter-VLAN Routing (Router on a stick).

7. Configuring DHCP Server (Router as the DHCP Server).

8. Configuring SSH for secure Remote access.

9. End-Device Configurations.

10. Test and Verifying Network Communication.

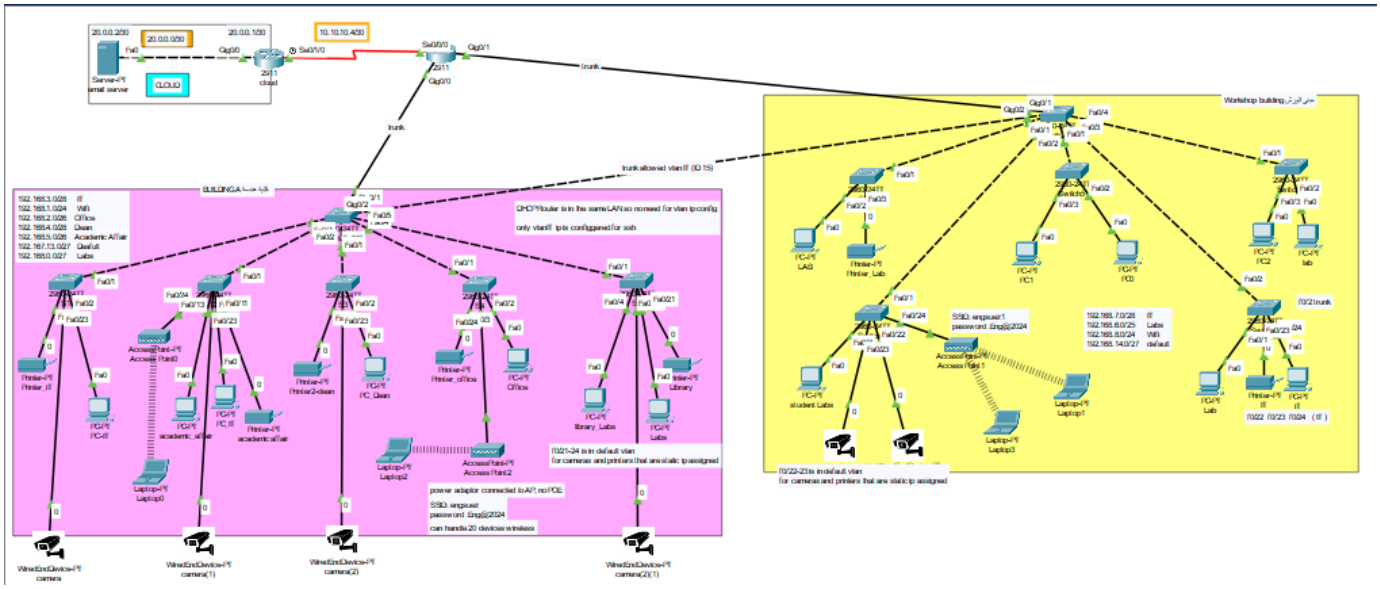
1. Procedure For Creating A Hierarchical Network Topology:

First of all we have to open Cisco Packet Tracer and then we have to do work in the workspace for creating a network topology.

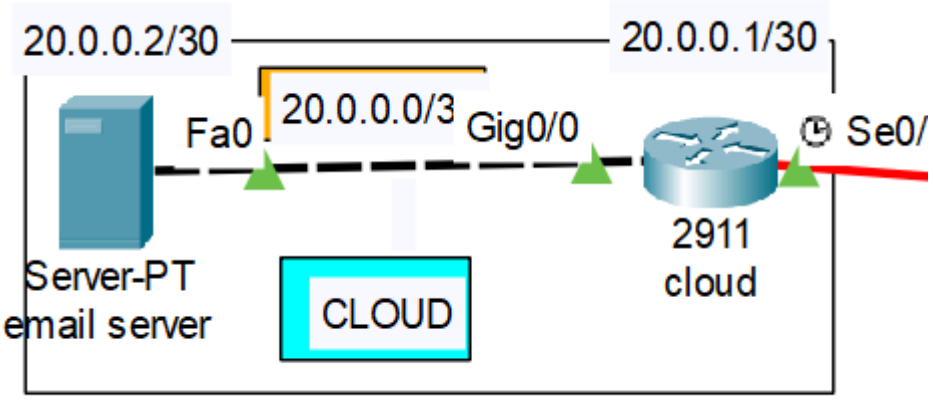
As we have to build hierarchical model for creating network topology. We have Core, distribution & Access layers at hierarchical model.

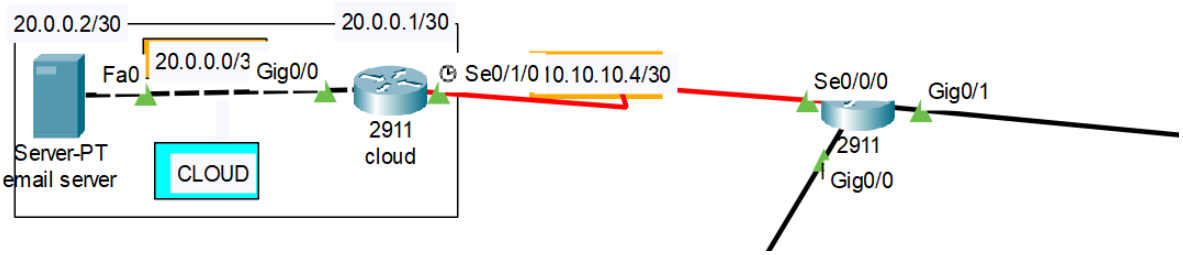
- **Core Layer:** Use a router to manage inter-VLAN routing and connect to external networks (Cloud/Email Server).
- **Distribution Layer:** Layer 2 switch for interconnecting access switches and managing VLANs.
- **Access Layer:** Use Layer 2 switches to connect end devices like PCs, laptops, printers, and access points and for VLAN management and inter-switch trunking.

Now we have to 1st drag a Router to the workspace and then drag L2 switch to connect all other switches in one switch to can connect them to router in one interface and then we have to drag access layer switches in the Floors of the building. At last we have to connect the End-devices with Access layer Switches as shown in the below screenshot;



In the same way we have to create a cloud building also and then we have to connect Cloud_Router to the Main router as shown below;

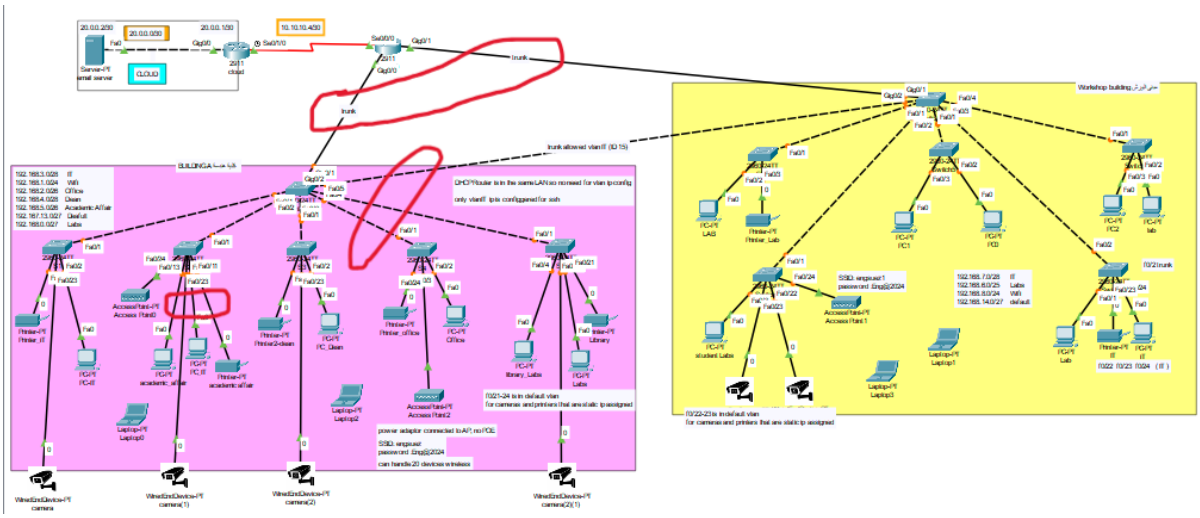

20.0.0.2/30
20.0.0.1/30
Fa0
20.0.0.0/3
Gig0/0
Se0/
Server-PT
email server
CLOUD
2911
cloud


20.0.0.2/30
20.0.0.1/30
Fa0
20.0.0.0/3
Gig0/0
Se0/1/0
10.10.10.4/30
Se0/0/0
Gig0/1
Server-PT
email server
CLOUD
2911
cloud
2911
Gig0/0

2. Procedure For Connecting Networking Devices With Correct Cabling:

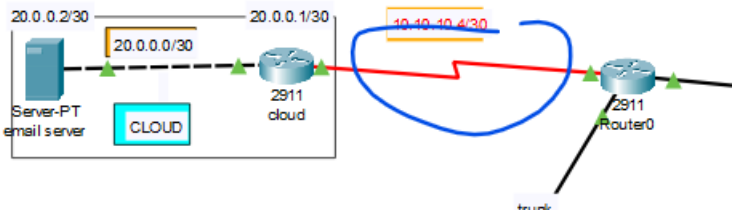
we have to choose proper cables for proper connection, as for different devices connectivity

- **Router to Switch (Router-on-a-Stick):**
  For different devices connectivity we have to use a **Copper Straight Through Ethernet cable** to connect the router's GigabitEthernet port to the switch's trunk port.
- **Switch to Switch (Trunk Links):**
  For same devices we have to use a **Copper-Cross Over Cable**

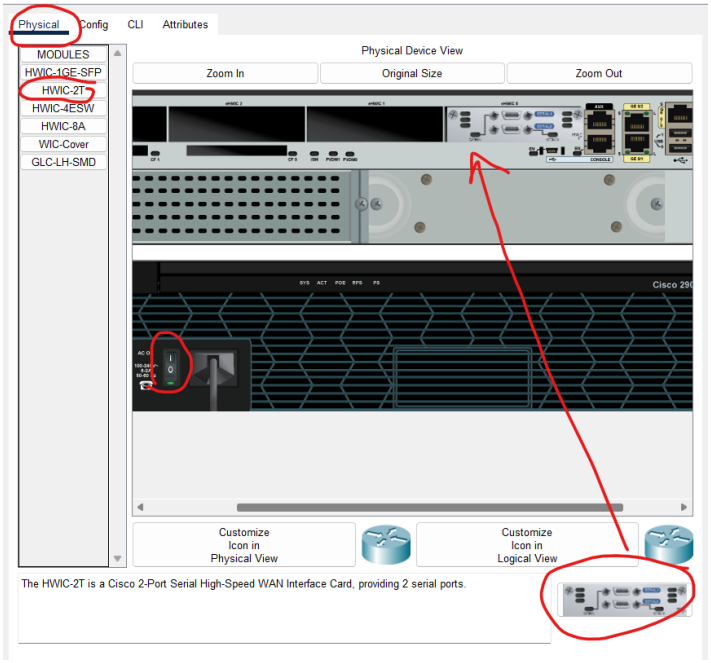


- **End Devices to Switches:**
  Use straight-through Ethernet cables to connect PCs, laptops, printers, and access points to the switches.

- **Cloud Connection:**
  Now we have to connect this Main-Router to the cloud for external connectivity serially using serial link (e.g., Se0/0/0).



For serially connecting Routers, we have to first add a HWIC-2T port to each Router as shown below;



Now we have to Configures INTERFACES serially,by doing so we have to type commands in the CLI of the routers as shown in the below screenshot;

```
Main_Router>
Main_Router>en
Main_Router#
Main_Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Main_Router(config)#interface s0/0/0
Main_Router(config-if)#clock rate 64000
Main_Router(config-if)#
Main_Router(config-if)#
Main_Router(config-if)#
```

3. Procedure For Creating VLANs And Assigning Ports VLAN Numbers:

Now we have to create VLAN for each department as shown in the below screenshots;

- **BUILDIN A:**
- **VLAN Creation:**

  Use the vlan command to create VLANs on switches.

```
vlan 15
name IT
vlan 30
name Students_Labs
vlan 40
name Wifi
vlan 50
name Academic_Affair
vlan 60
name Office
vlan 80
name Dean
```

- **Assign VLANs to Ports of Access Layer Switch:**

  Use the switchport access vlan command to assign VLANs to switch ports

```
S1_F1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1_F1(config)#interface range fa0/2-10
S1_F1(config-if-range)#switchport mode access
S1_F1(config-if-range)#switchport access vlan 15
S1_F1(config-if-range)#
```

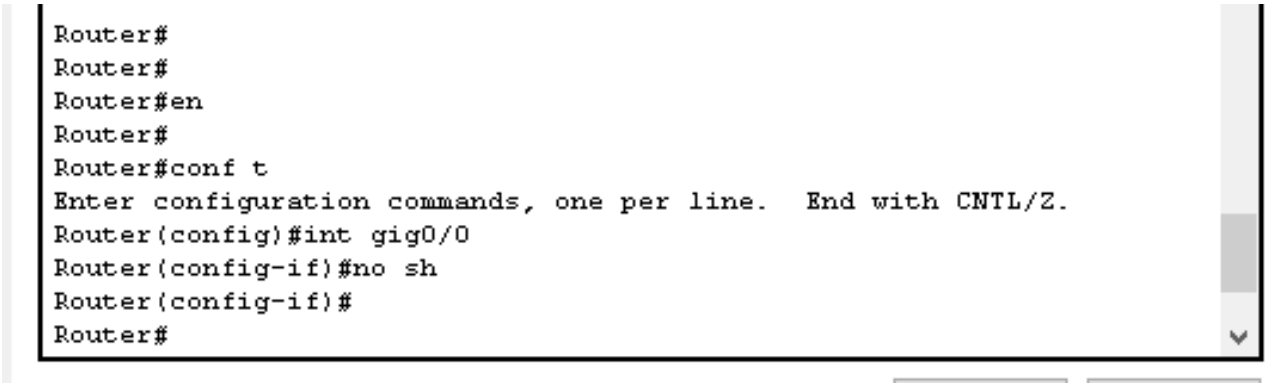
  As we saw in the above screenshot we had configured VLAN 15 in switch 1 in building A for the IT successfully. In the same way we have to do configurations for all the VLANS of all the departments in Building A & B.

```
Sl_Fl#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
15   IT                               active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
30   student_labs                     active
40   wifi                             active
50   academic_affair                  active
60   office                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
80   dean                             active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

4. Procedure for Configuration of different devices:

By default all the interfaces of the Routers are OFF so we have to Turn it ON, for this we have to do proper configuration

Now we have to enter commands in CLI to turn ON various interfaces of the Routers.



5. Procedure For Configuring The One Interface Of The L2 Switch (“Distribution switch”) To The Router’s Interface(“Main_Router”):

Procedure For Configuring The One Interface Of The L2 Switch To The Router’s interface we have to type the command in the below screenshot;

- **Distribution Layer Switches:**
  Configure trunk ports for VLAN propagation to access switches:

- Building A:

```
vlan 15
name IT
vlan 30
name Students_Labs
vlan 40
name Wifi
vlan 50
name Academic_Affair
vlan 60
name Office
vlan 80
name Dean
```

Connect the router’s GigabitEthernet port to the switch’s trunk port. Configure the switch port for trunking:

```
ST1(config)#
ST1(config)#
ST1(config)#
ST1(config)#interface g0/1
ST1(config-if)#switchport mode trunk
ST1(config-if)#switchport trunk allowed vlan 15,30,40,60,80,50
ST1(config-if)#
ST1(config-if)#
```

- As we saw in the above screenshot we had configured The One Interface Of The L2 Switch To The Router's interface.
- In the same way we have to do configuration for switch 2 "ST2" in Building B.

6. Procedure For Assigning IP Addresses To All The Interfaces Of The Routers & Also Configuring Inter-VLAN Routing:

- Enable Router-on-a-Stick inter-VLAN routing on the router using subinterfaces:
- Building A:

192.168.3.0/28	IT
192.168.1.0/24	Wifi
192.168.2.0/26	Office
192.168.4.0/28	dean
192.168.5.0/26	academic affair

1st we are going to assign IP addresses to the interfaces of the Router, so for this we have to go to the Router's CLI and type the command to configure IP to that particular interface as shown below;

For Main_Router:

```
Main_Router(config)#
Main_Router(config)#interface s0/0/0
Main_Router(config-if)#ip address 10.10.10.5 255.255.255.252
Main_Router(config-if)#no sh
Main_Router(config-if)#
Main_Router(config-if)#
Main_Router(config-if)#
```

Copy Paste

For Cloud_Router:

```
Router(config)#
Router(config)#int s0/1/0
Router(config-if)#ip address 10.10.10.6 255.255.255.252
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Copy Paste

Cloud/External Interface:

- Assign an IP for external routing:

```
Router>EN
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 20.0.0.1 255.255.255.252
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

Copy Paste

Inter-VLAN Routing Configuration

We have to do inter-Vlan Routing for all those interfaces which are connected to the VLAN's through Switches.

- Assign IP addresses to router sub interfaces for each VLAN:

```
Main_Router(config)#interface g0/0.15
Main_Router(config-subif)#encapsulation dot1Q 15
Main_Router(config-subif)#ip address 192.168.3.1 255.255.255.240
Main_Router(config-subif)#
Main_Router(config-subif)#
```

7. Configuring SSH for secure Remote access.

The following commands were executed to enhance the security of remote access to the router using SSH:

1- Enable Password Encryption:

To encrypt all plaintext passwords stored in the router's configuration file. It helps protect sensitive information by preventing unauthorized access to plain passwords.

2- Configure Login Block Parameters:

Add a security mechanism to block login attempts for 120 seconds if there are 3 failed login attempts within 60 seconds. It helps mitigate brute-force attacks by limiting the number of login attempts

3-Access the VTY Lines (Virtual Terminal Lines 0 to 4:

Access the configuration mode for virtual terminal lines 0 to 4, which are used for remote access via protocols such as SSH or Telnet.

4-Set an Idle Timeout for VTY Lines:

This sets an idle timeout for VTY lines. If a session remains idle for 2 minutes and 30 seconds, the session will automatically terminate. This reduces the risk of unauthorized access if the session is left open.

5-Restrict Access to SSH Only:

To limit remote access to the router through SSH only, disabling less secure protocols like Telnet. SSH encrypts all data, providing a secure method for remote communication.

```
Main_Router(config)#service password-encryption
Main_Router(config)#login block-for 120 attempts 3 within 60
Main_Router(config)#line vty 0 4
Main_Router(config-line)#exec-timeout 2 30
Main_Router(config-line)#transport input ssh
Main_Router(config-line)#exit
```

8. Procedure for Configuring DHCP Server (Router as the DHCP Server):

DHCP Configuration in Packet Tracer:

As part of the network connection project in Packet Tracer, Configuring DHCP services on the router to enable dynamic IP address allocation across multiple VLANs. This setup simplifies network management by reducing manual IP assignment while ensuring specific devices like printers and cameras use static IPs through exclusion ranges.

VLAN and Subnet Allocation

The following VLANs were configured with corresponding IP subnets and subnet masks:

VLAN 15: 192.168.3.0/24 (Subnet Mask: 255.255.255.224)

VLAN 30: 192.168.0.0/27 (Subnet Mask: 255.255.255.224)

VLAN 40: 192.168.1.0/24 (Subnet Mask: 255.255.255.0)

VLAN 50: 192.168.5.0/26 (Subnet Mask: 255.255.255.192)

VLAN 60: 192.168.2.0/26 (Subnet Mask: 255.255.255.192)

VLAN 80: 192.168.4.0/26 (Subnet Mask: 255.255.255.240)

VLAN 1 (Default): 192.168.13.0/27 (Subnet Mask: 255.255.255.224)

IP Address Exclusions

To reserve specific IP addresses for devices requiring static configurations, the following address ranges were excluded from the DHCP pools:

VLAN 15: 192.168.3.1 - 192.168.3.7

VLAN 30: 192.168.0.1 - 192.168.0.10

VLAN 40: 192.168.1.1 - 192.168.1.10

VLAN 50: 192.168.5.1 - 192.168.5.10

VLAN 60: 192.168.2.1 - 192.168.2.10

VLAN 80: 192.168.4.1 - 192.168.4.4

Additionally, the following IP ranges outside of the defined VLANs were also excluded to reserve them for future static device configurations:

192.168.7.1 - 192.168.7.6

192.168.13.1 - 192.168.13.8

192.168.14.1 - 192.168.14.8

Now we have to configure DHCP_Server to the Router, to use Router as DHCP-Server.
By doing so we have to go to the CLI of the router and type command For DHCP-Server to be configured as shown below;

- **DHCP Pool Configuration:**
- Configure DHCP pools for each VLAN to dynamically assign IP addresses:

```
Main_Router(config)#
Main_Router(config)#
Main_Router(config)#
Main_Router(config)#ip dhcp pool VLAN30
Main_Router(dhcp-config)#network 192.168.0.0 255.255.255.224
Main_Router(dhcp-config)#default-router 192.168.0.1
Main_Router(dhcp-config)#dns-server 8.8.8.8
Main_Router(dhcp-config)#
Main_Router(dhcp-config)#
Main_Router(dhcp-config)#
Main_Router(dhcp-config)#
```

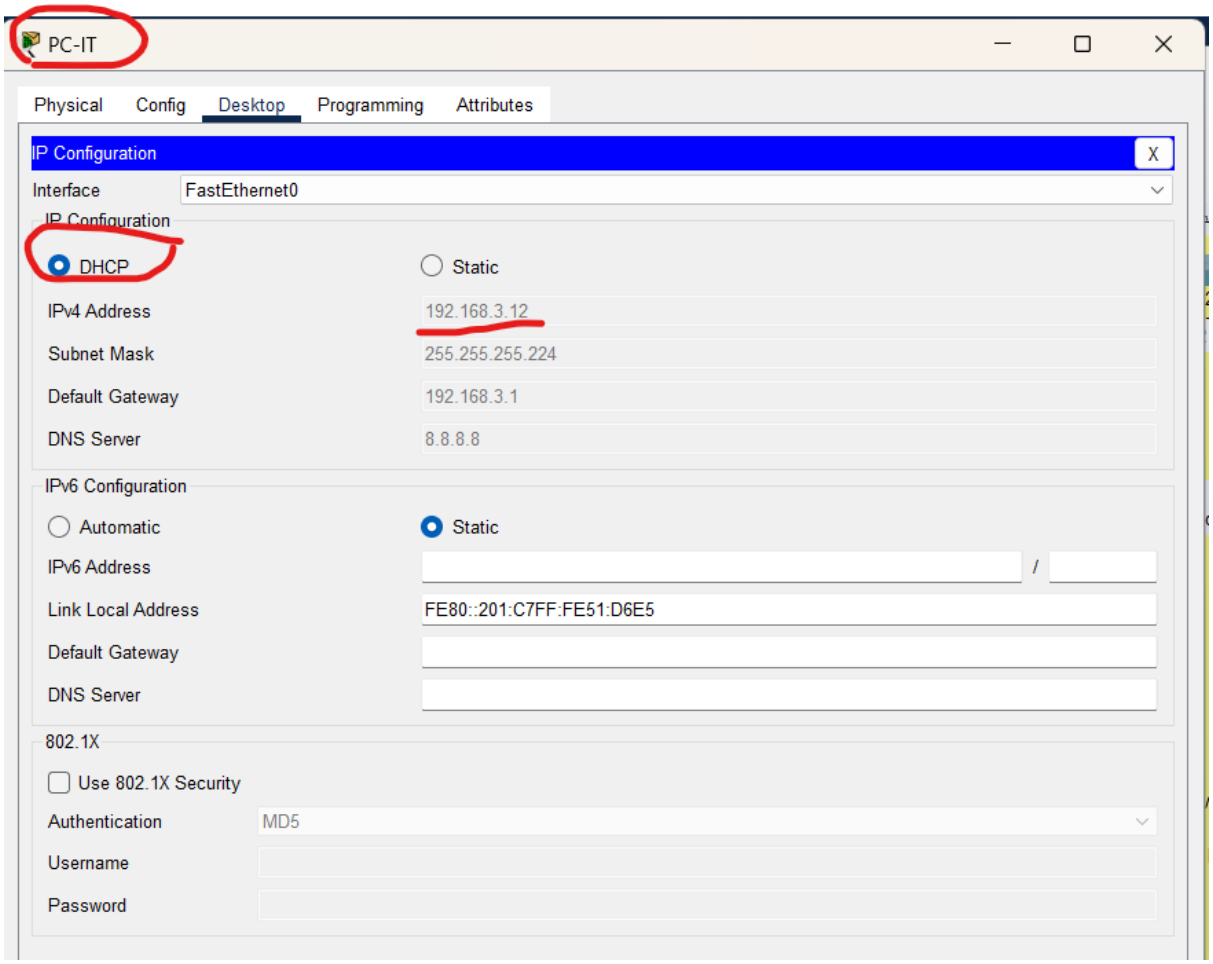
- **Exclude Reserved IPs:**

Exclude IP addresses reserved for static configuration:

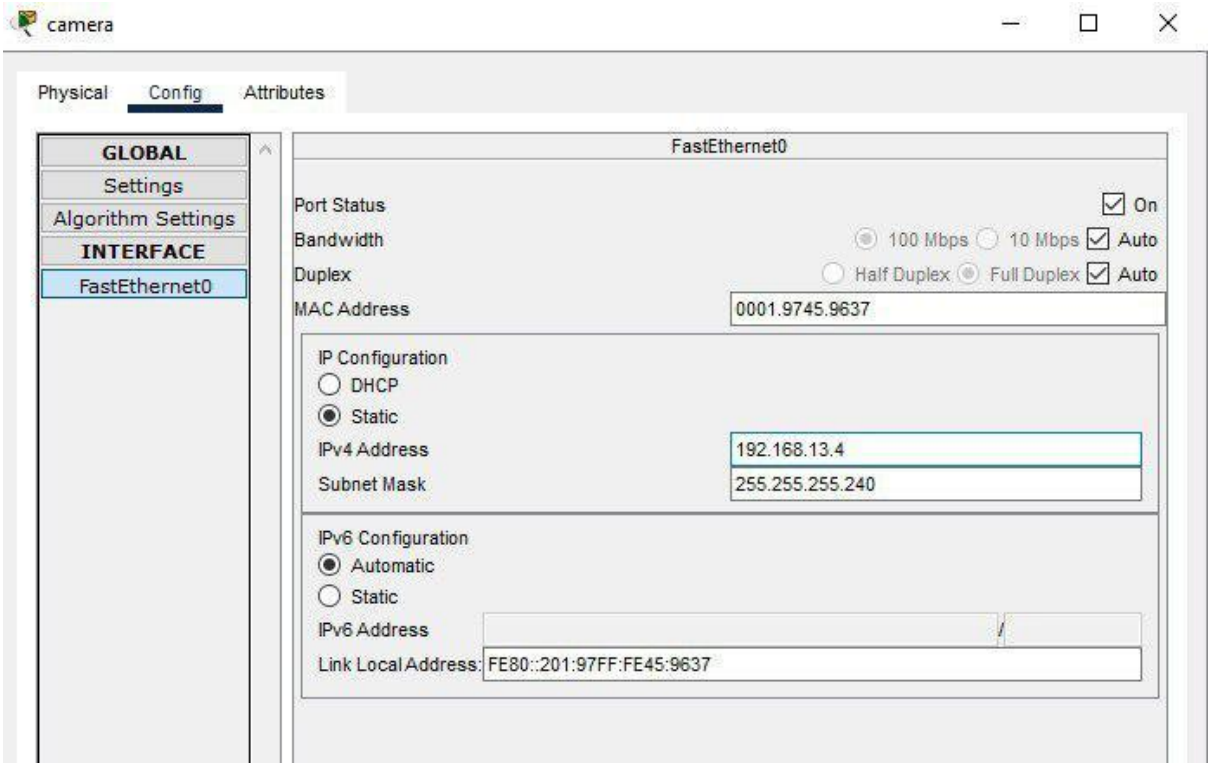
```
Main_Router(config)#
Main_Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Main_Router(config)#
```

```
Main_Router#
Main_Router#
Main_Router#show running-config | include excluded-address
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp excluded-address 192.168.3.1 192.168.3.10
ip dhcp excluded-address 192.168.5.1 192.168.5.10
ip dhcp excluded-address 192.168.3.1 192.168.3.7
ip dhcp excluded-address 192.168.7.1 192.168.7.6
ip dhcp excluded-address 192.168.13.1 192.168.13.8
ip dhcp excluded-address 192.168.14.1 192.168.14.8
Main_Router#
Main_Router#
```

Now we can give Ips for all devices dynamically;



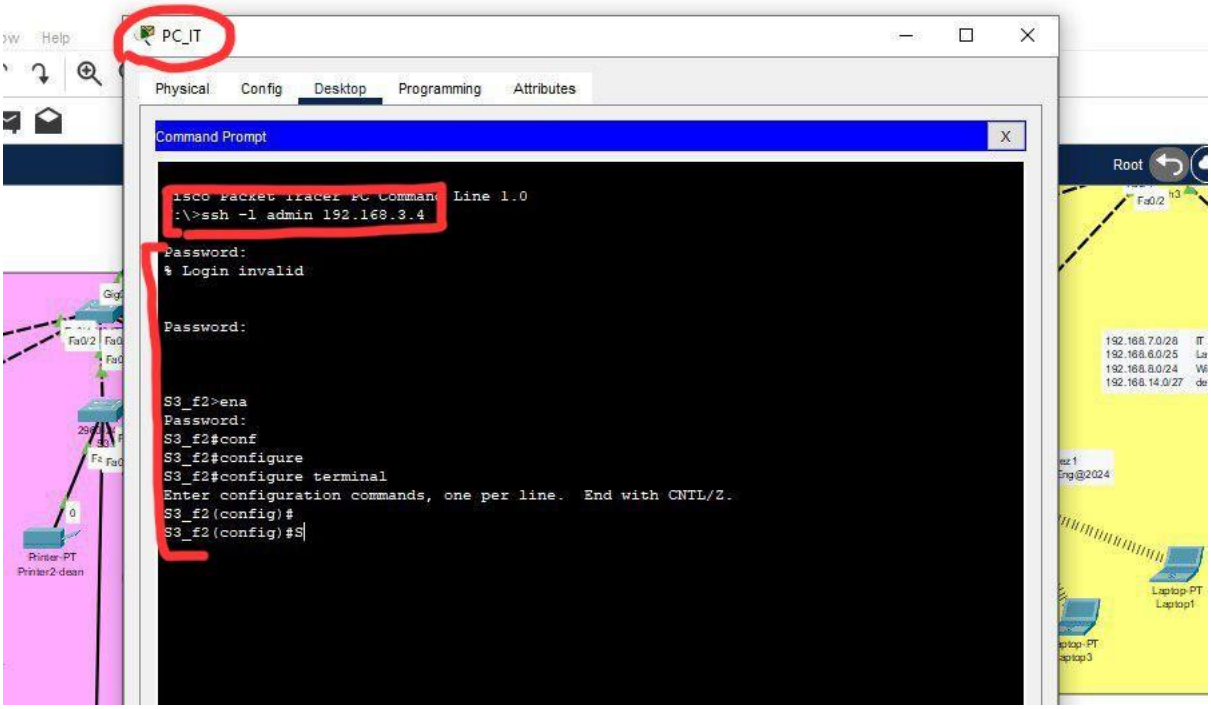
Also we can give Ips for Cameras and printers statically;
By using excluded IPs



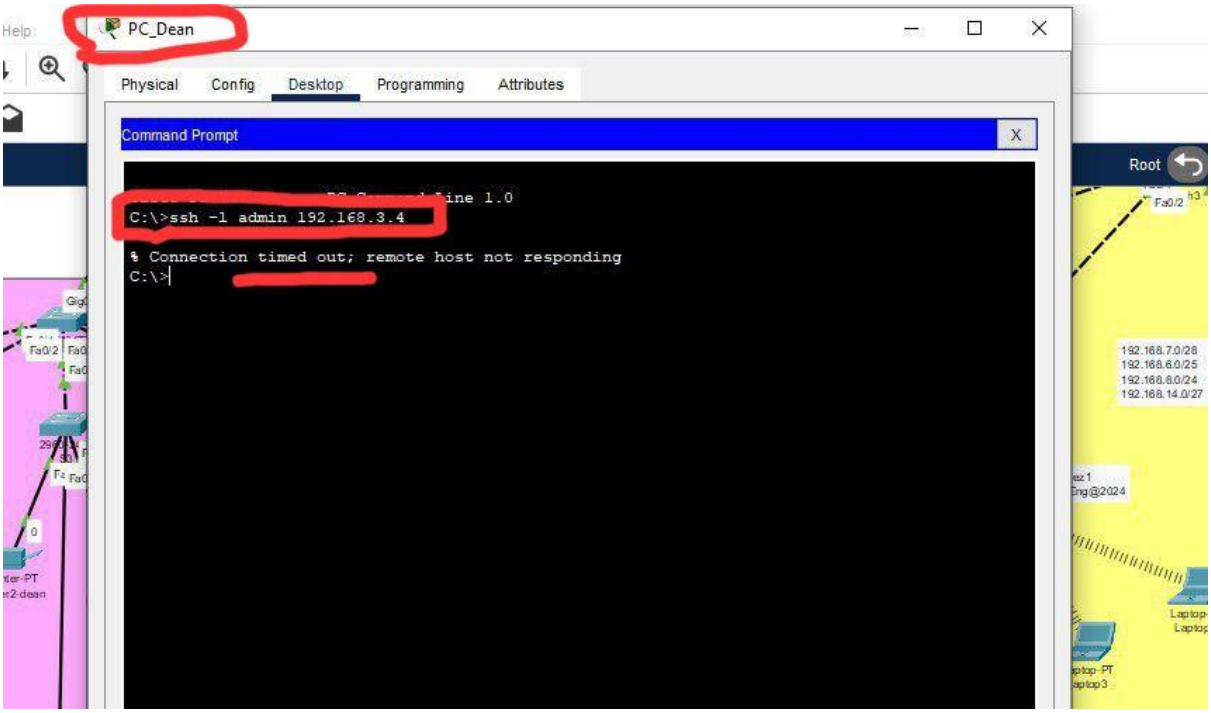
Switch IP Assignment and SSH Access Control

By assigning an IP address from the IT VLAN's IP range (192.168.3.0/27) to the switch interface VLAN 15. Specifically, when excluded the IP range 192.168.3.1 - 192.168.3.8 from DHCP allocation to ensure these addresses are reserved for static assignment to switches.

By implementing this configuration, only IT devices within the correct VLAN can establish SSH connections to the switch. Devices from other VLANs attempting to initiate SSH sessions will be denied access, enhancing network security by restricting management access to authorized IT devices only.



Here is Devices from other VLANs attempting to initiate SSH sessions will be denied access;



9. Testing and Verifying Network Communication:

- **Ping Tests:**

  Verify connectivity between PCs in the same VLAN.

  Test inter-VLAN connectivity using the router as a gateway.

- **Trunk Link Verification:**

  Verify trunk port status:

```
ST1>en
ST1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99
Fa0/4       on           802.1q         trunking      99
Fa0/5       on           802.1q         trunking      99
Gig0/1      on           802.1q         trunking      99
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
Fa0/4       1-1005
Fa0/5       1-1005
Gig0/1      1-1005
Gig0/2      15

Port        Vlans allowed and active in management domain
Fa0/1       1,15,30,40,50,60,80
Fa0/2       1,15,30,40,50,60,80
Fa0/3       1,15,30,40,50,60,80
 --More--
```

- **Routing Table Verification:**

  Check RIP routes:

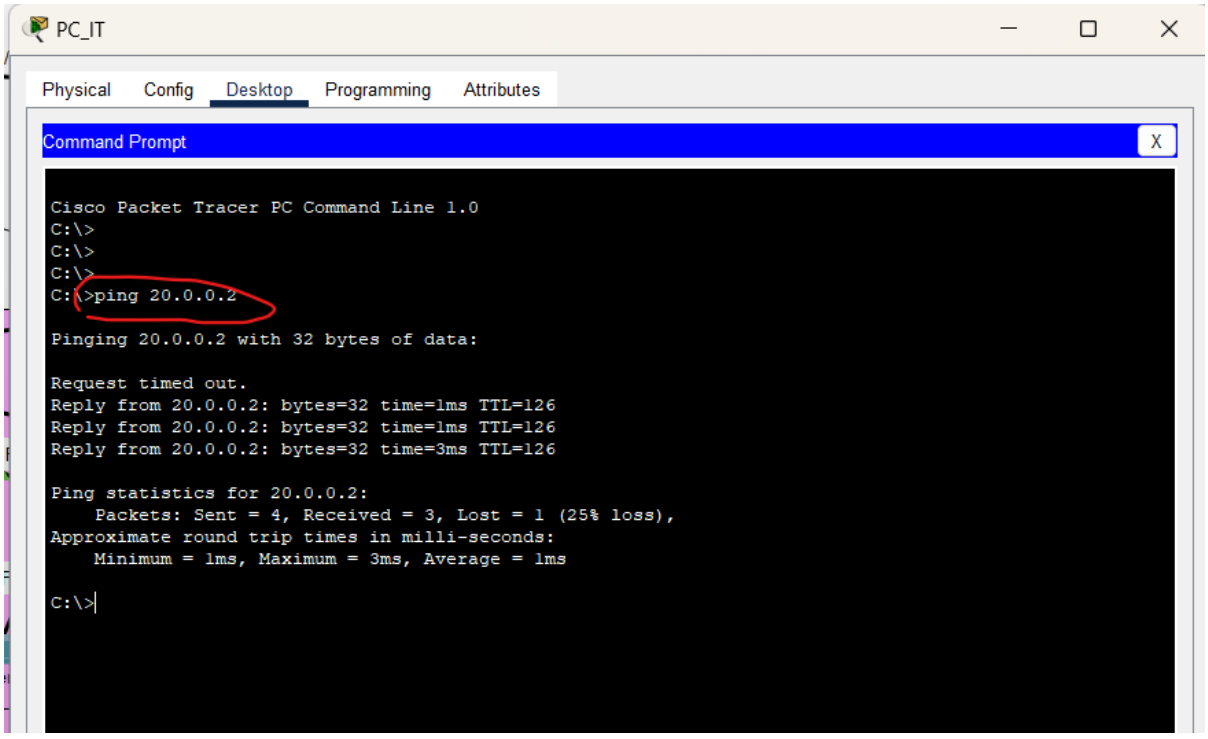
```
Main_Router#
Main_Router#
Main_Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 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 10.10.10.6 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.4/30 is directly connected, Serial0/0/0
L       10.10.10.5/32 is directly connected, Serial0/0/0
     20.0.0.0/30 is subnetted, 1 subnets
S       20.0.0.0/30 [1/0] via 10.10.10.6
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/27 is directly connected, GigabitEthernet0/0.30
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0.30
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0.40
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.40
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
 --More--
```

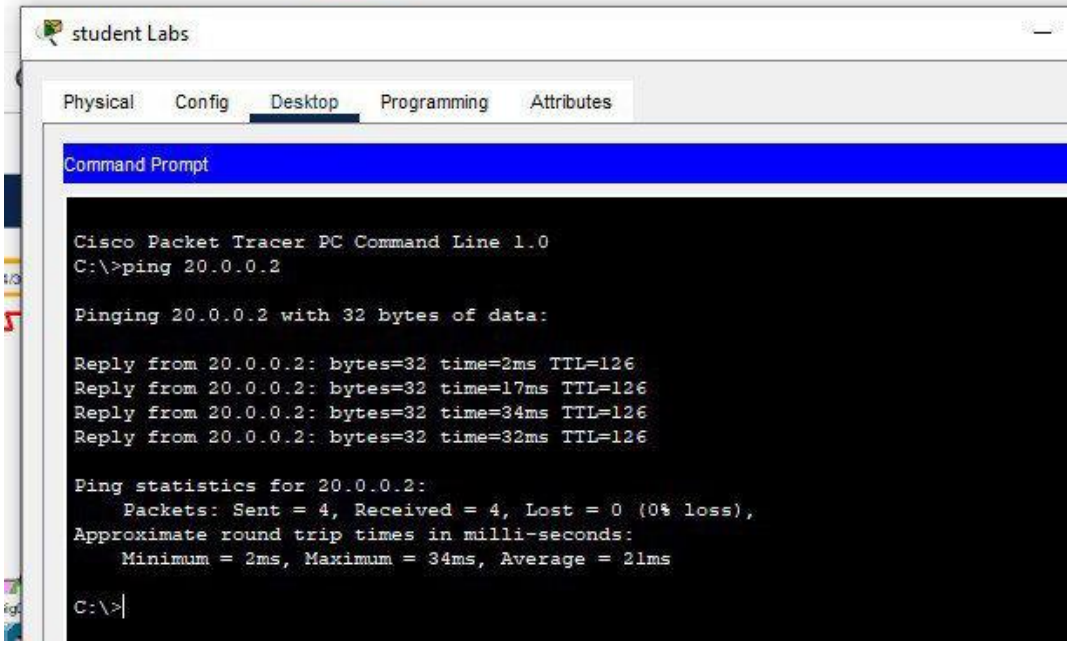
- **DHCP Verification:**
  Verify DHCP address allocation to client devices

```
Main_Router#
Main_Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.3.12     0001.C751.D6E5          --                      Automatic
192.168.3.13     000C.8541.9408          --                      Automatic
192.168.3.11     0002.4AC7.2C10          --                      Automatic
192.168.0.12     0004.9A95.D1B5          --                      Automatic
192.168.0.11     0090.0CED.3E9E          --                      Automatic
192.168.1.11     00D0.FF48.68DC          --                      Automatic
192.168.1.12     0001.976E.4627          --                      Automatic
192.168.2.11     00D0.FFC1.4545          --                      Automatic
192.168.4.2      0001.43A0.A874          --                      Automatic
192.168.3.12     0001.C751.D6E5          --                      Automatic
192.168.3.11     0002.4AC7.2C10          --                      Automatic
192.168.3.13     000C.8541.9408          --                      Automatic
192.168.6.2      0004.9A80.5901          --                      Automatic
192.168.6.5      00E0.F743.5B1E          --                      Automatic
192.168.6.4      0060.5CC2.99C1          --                      Automatic
192.168.6.3      0001.43D8.6003          --                      Automatic
192.168.6.6      0030.A36B.0048          --                      Automatic
192.168.6.7      0002.4ADA.BAA6          --                      Automatic
192.168.6.8      0050.0F84.7D9D          --                      Automatic
192.168.8.2      00E0.B02B.BCD4          --                      Automatic
 --More--
```

Copy Paste

- **Cloud Connectivity:**
  Test external connectivity using ping.
  On any router or PC that needs to test connectivity to the cloud server or external device.




student Labs
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.2
Pinging 20.0.0.2 with 32 bytes of data:
Reply from 20.0.0.2: bytes=32 time=2ms TTL=126
Reply from 20.0.0.2: bytes=32 time=17ms TTL=126
Reply from 20.0.0.2: bytes=32 time=34ms TTL=126
Reply from 20.0.0.2: bytes=32 time=32ms TTL=126
Ping statistics for 20.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 34ms, Average = 21ms
C:\>