

Cisco Packet Tracer Network Design with Wireless Access Points

Documentation

I used 11 different IP addresses

The building network connections:

- 192.168.1.0
- 192.168.2.0
- 192.168.3.0
- 192.168.4.0
- 192.168.5.0

For the router connections:

- 192.168.6.0
- 192.168.7.0
- 192.168.8.0
- 192.168.9.0
- 192.168.10.0

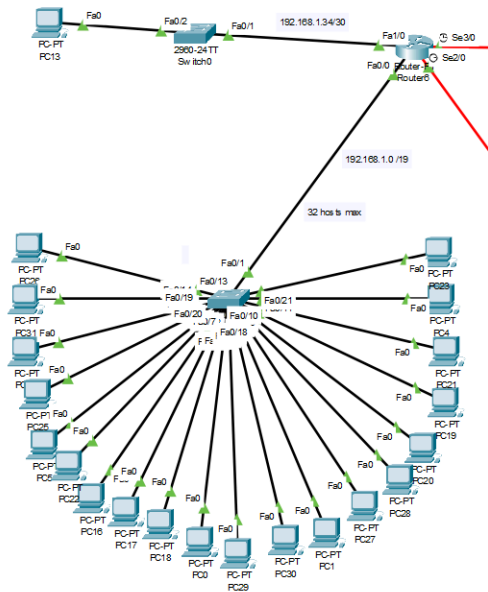
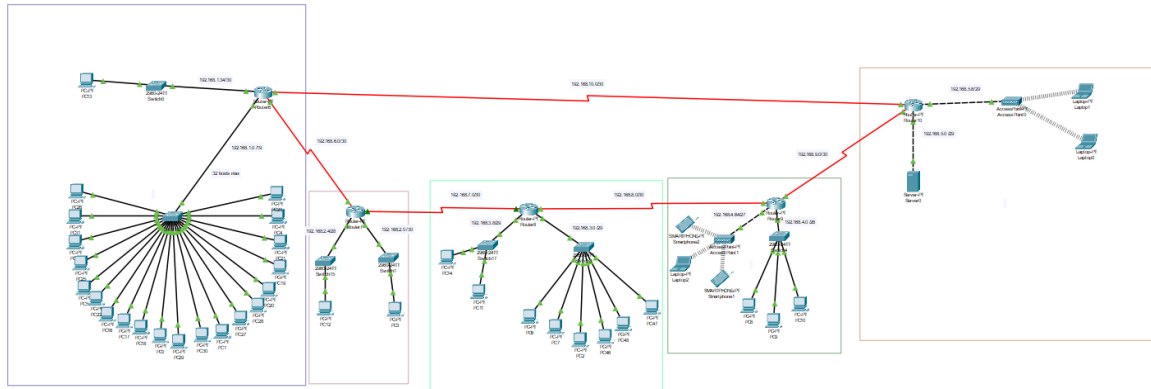
I utilized a Class C private IP address range to accommodate the network's growth and allow for efficient subnetting. Each building was assigned a unique subnet, while additional subnets were allocated for servers, wireless access points, and inter-building connections. I used the DHCP to dynamically assign IP addresses to various or newly connected devices.

I selected switches for local connectivity within each building due to their robust features and scalability. Routers were chosen for interconnecting buildings and implementing dynamic routing protocols to facilitate efficient packet forwarding. I added a firewall through a server in one of the networks to enforce security policies and protect the network perimeter.

Wireless access points were configured with WPA2 encryption and SSID broadcast disabled to enhance security. Each access point was assigned a unique SSID and VLAN to segregate wireless traffic and enforce network policies.

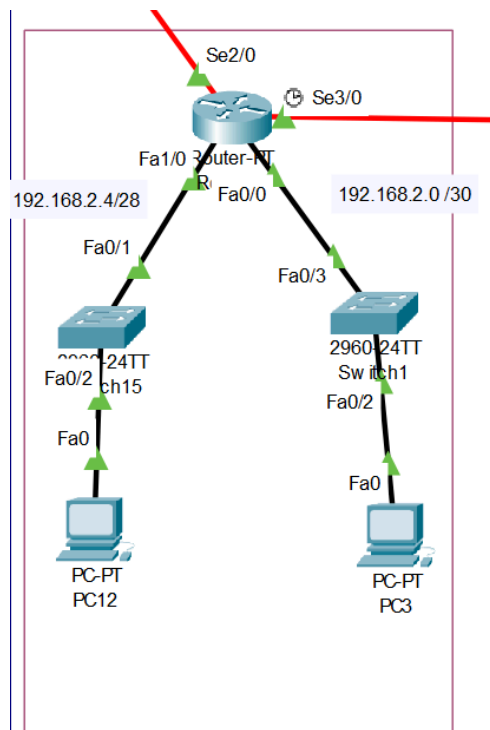
Detailed Documentation

Each building has a router and 2 switches, and each network has two subnets.

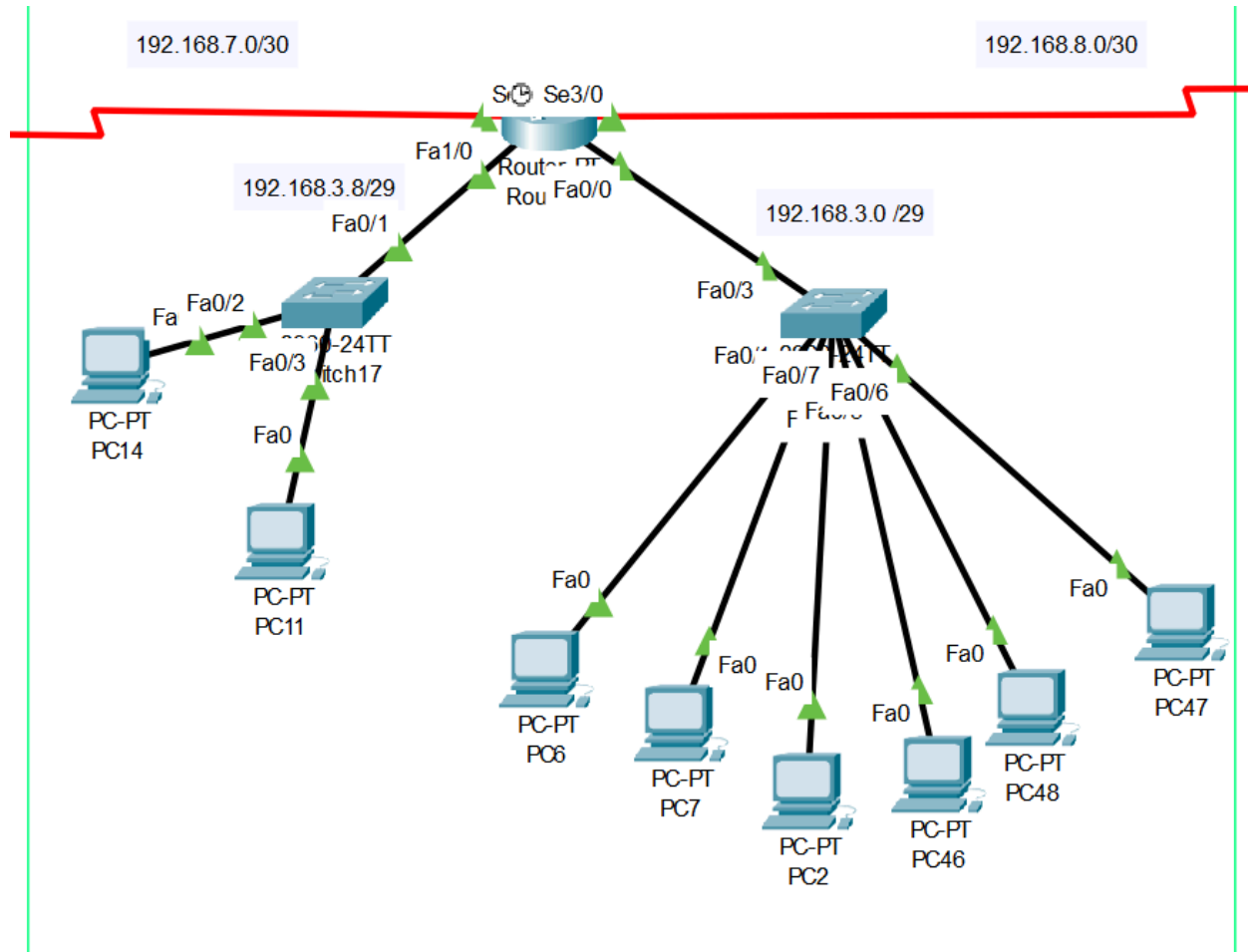


In the above network, there are two subnets. One being 192.168.1.0/19 and the other being 192.168.1.34/30. Each of them has 192.168.1.1 and 192.168.1.35 as the router ip address respectively.

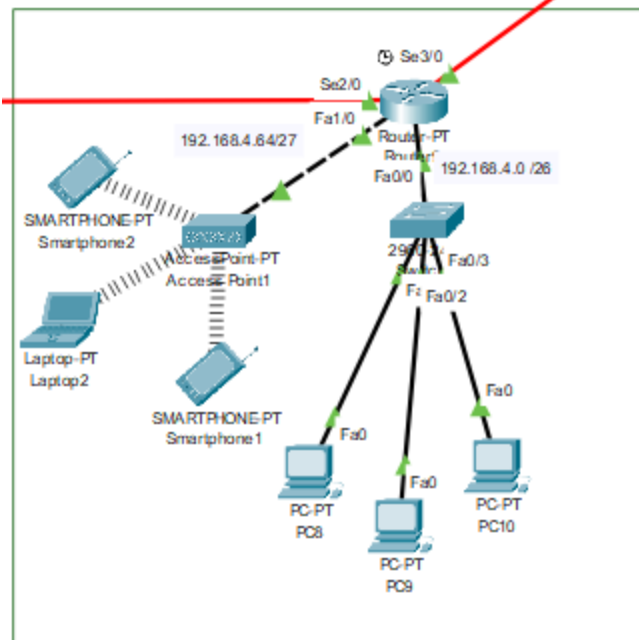
The router is also the DHCP server and dynamically assigns IP addresses to any device that connects to the network. But, in the 192.168.1.0/19 subnet, if I try to add another device to the subnet, it wouldn't allow me due to the max number of hosts being met. This is the same as all the other networks due to subnetting.



The network above contains two subnets, 192.168.2.0/30 and 192.168.2.4/28. Both of them only allow a maximum of one host. The IP address range of the 192.168.2.4/28 subnets starts from where the other subnet ends. 192.168.2.1 to 192.168.2.2 being the IP address range and 192.168.2.3 being the broadcast IP of the previous subnet. The 198.168.2.4/28 network has a router with an IP address of 192.168.2.5/28, which dynamically assigns an IP address to the host.



The network above contains two subnets, 192.168.3.0/30 and 192.168.3.8/29. Both of them only allow a maximum of one host. The router IP address of the 192.168.3.0/29 network is 192.168.3.1 with the range of 192.168.3.1 to 192.168.3.5, with 192.168.3.6 being the broadcast's IP address, and 192.168.3.9, with a range of 192.168.3.9 to 192.168.3.14, broadcast being 192.168.3.15, for the other.



This network has two subnets. One of the subnets has a wireless device as the main connection point.

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID WifeEye

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase 12345678

User ID

Password

Encryption Type AES

I used the WPA2 security protocol to protect the wireless network.

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

3G/4G Cell1

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 54 Mbps

MAC Address 000C.8548.0A09

SSID WifeEye

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase 12345678

User ID

Password

Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.4.71

Subnet Mask 255.255.255.224

On mobile phones, I have to provide the password of the wireless device before it can connect to it.

Link Information

Connect

Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
WifeEye	1	100%

Site Information

Wireless Mode

Infrastructure

Network Type

Mixed B/G

Radio Band

Auto

Security

WPA2-PSK


MAC Address

00E0.A3A0.4C52

Refresh

Connect

2.4GHz



Adapter is Inactive

Wireless-N Notebook Adapter

Wireless Network Monitor v1.0

Model No. WPC300N

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security

WPA2-Personal

Please select the wireless security method used by your existing wireless network.

Pre-shared Key

12345678

Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel

Connect

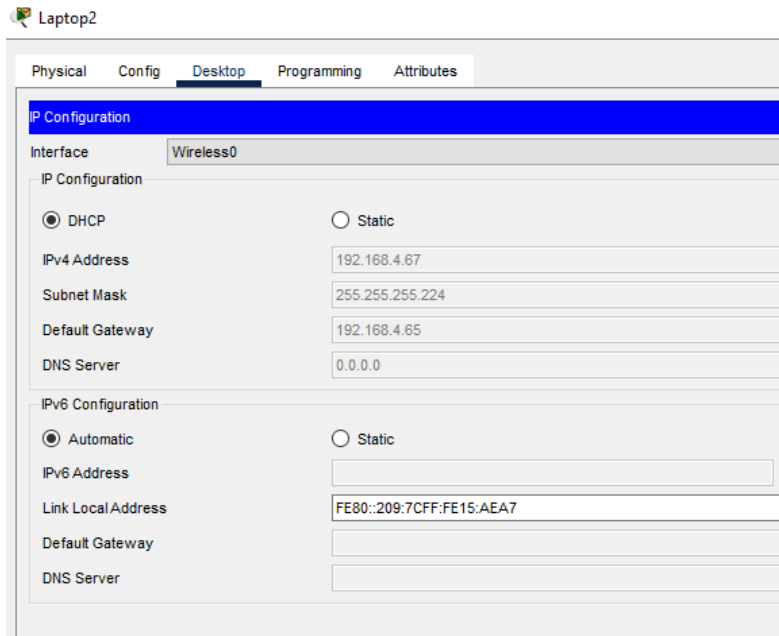
Active

Wireless-N Notebook Adapter

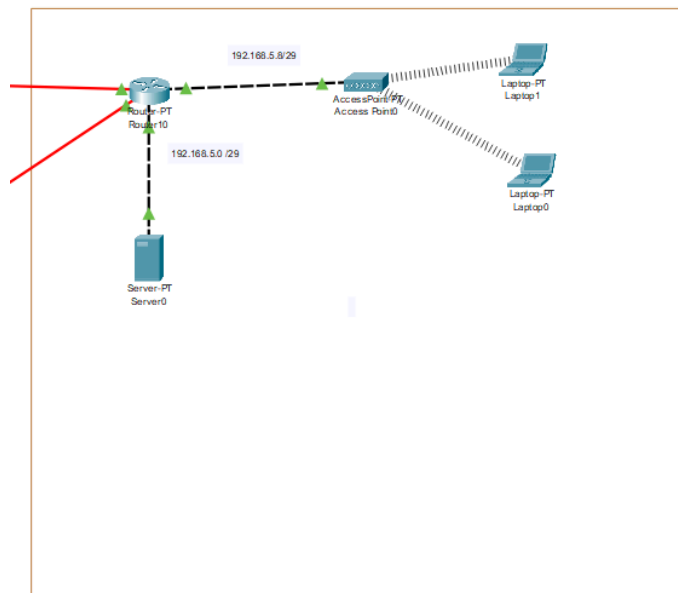
Wireless Network Monitor v1.0

Model No. WPC300N

The same applies for the laptop.



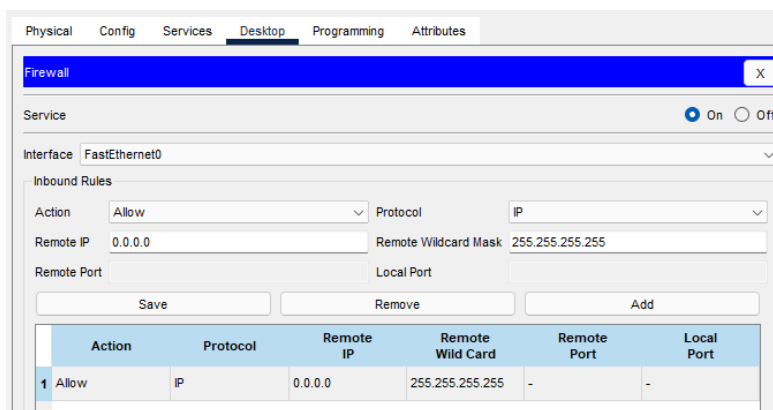
Each of them will then be assigned a unique IP address afterwards.



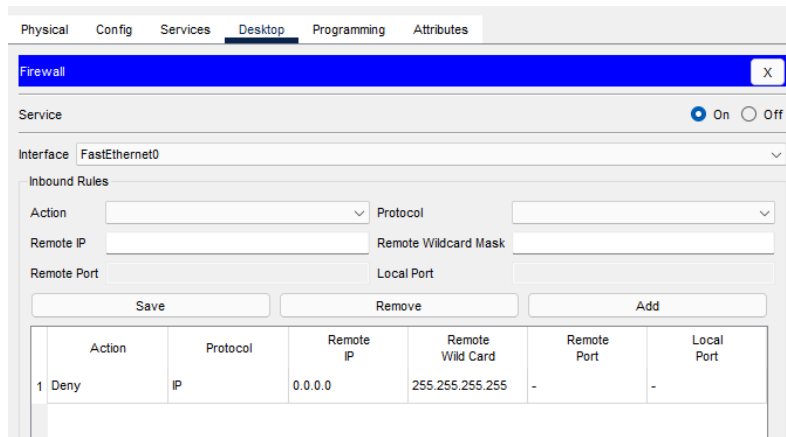
This network contains two subnets. One is wireless, the other is wired. On the wired network, a server is present for hosting applications.



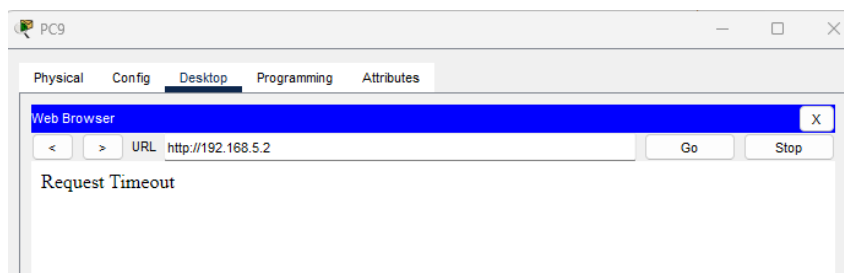
The server can be accessed from any PC, Laptop, or Mobile Phone on the entire network.



Using the firewall, I gave every device on the network access to the server.



And when it is changed from “Allow” to “Deny”,



none of the devices can connect to the server.

Access Point0

Physical Config Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID Default

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

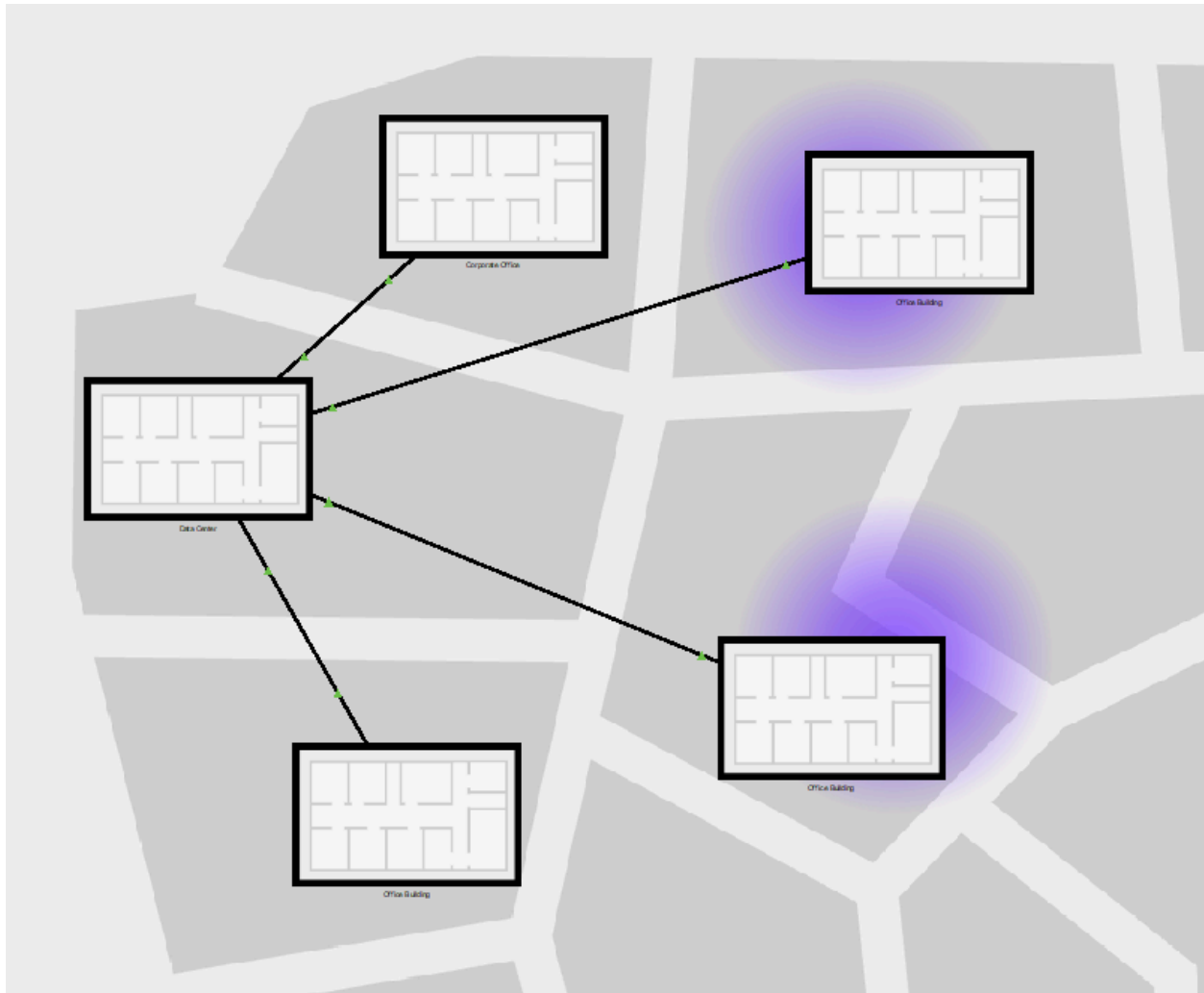
PSK Pass Phrase 12345678

User ID

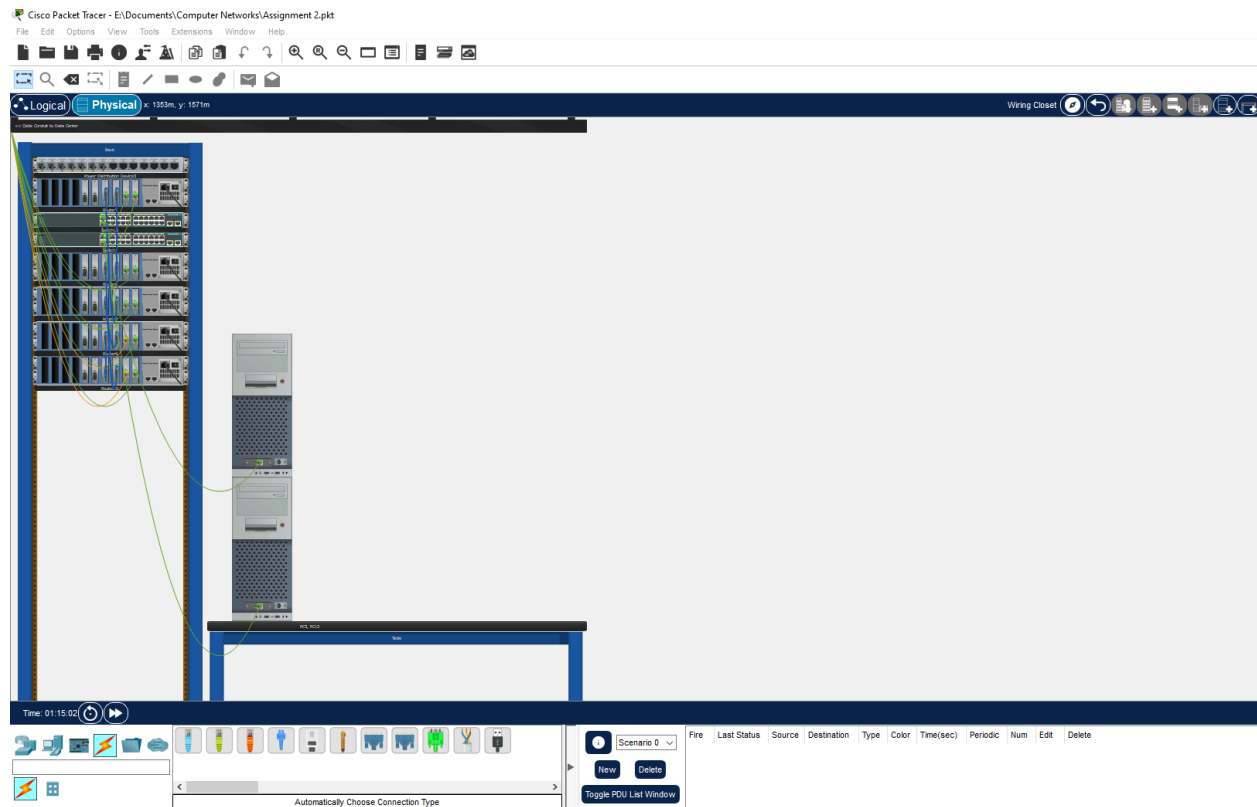
Password

Encryption Type AES

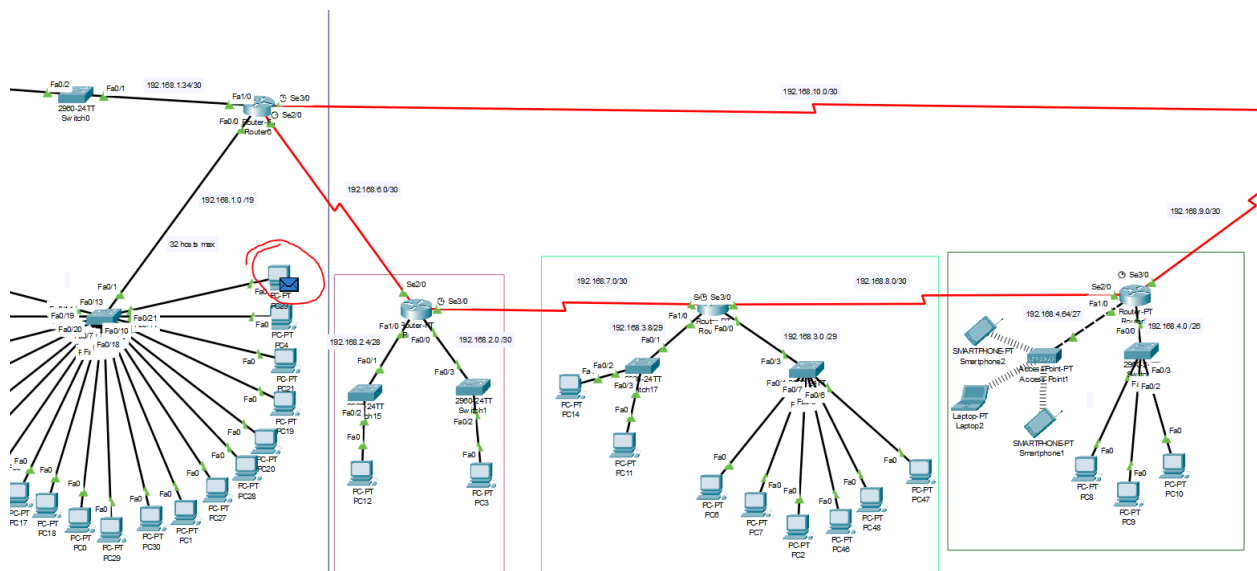
The wireless device on the other subnet (192.168.5.8/29) also uses the WPA2 security protocol and has an IP address of 192.168.5.9.

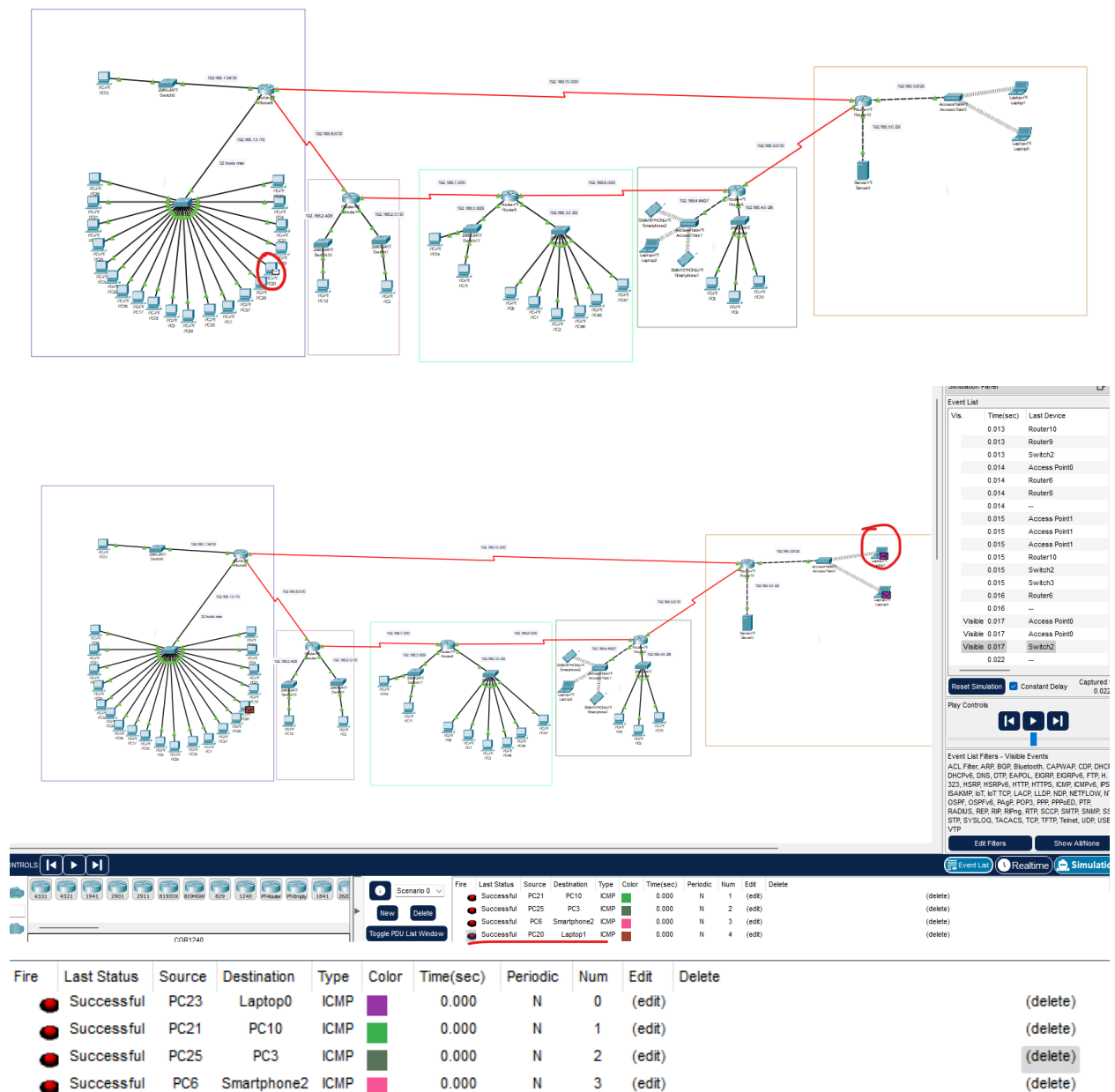


In the physical view, I added five buildings, each with their own network. One of the buildings is a data center where all the routers of each building are located.



The data center closet has all the routers stored in a rack.





Extensive testing was conducted to validate the functionality of the network design, including simulations, packet captures, and connectivity tests. Testing procedures were documented, and any issues or discrepancies were addressed and resolved promptly.

The network design successfully meets the requirements outlined in the assignment, providing scalable, secure, and efficient connectivity across the campus.