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

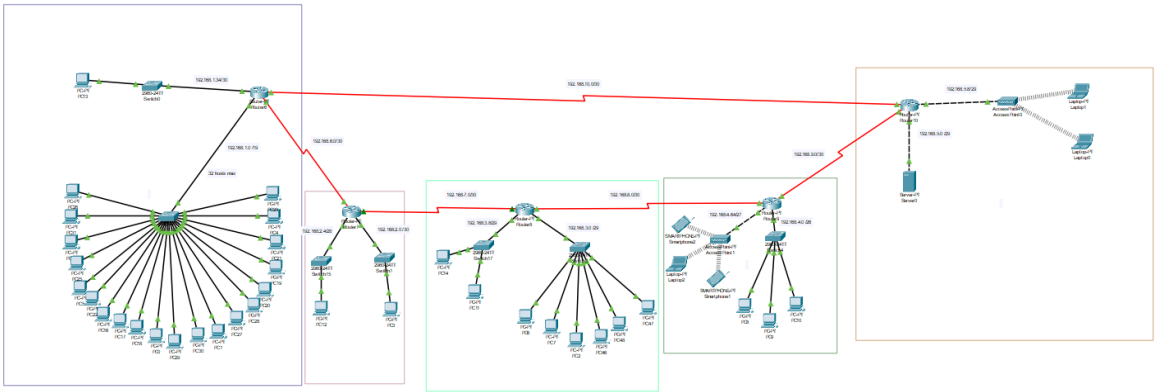
I utilized a Class C private IP address range to accommodate the network's growth and allow for efficient subnetting. Each building was assigned a unique subnet, while additional subnets were allocated for servers, wireless access points, and inter-building connections. I used the DHCP to dynamically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

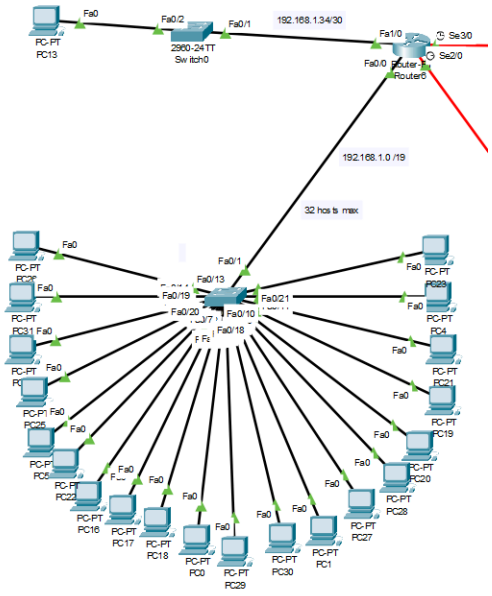
I selected switches for local connectivity within each building due to their robust features and scalability. Routers were chosen for interconnecting buildings and implementing dynamic routing protocols to facilitate efficient packet forwarding. I added a firewall through a server in one of the networks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

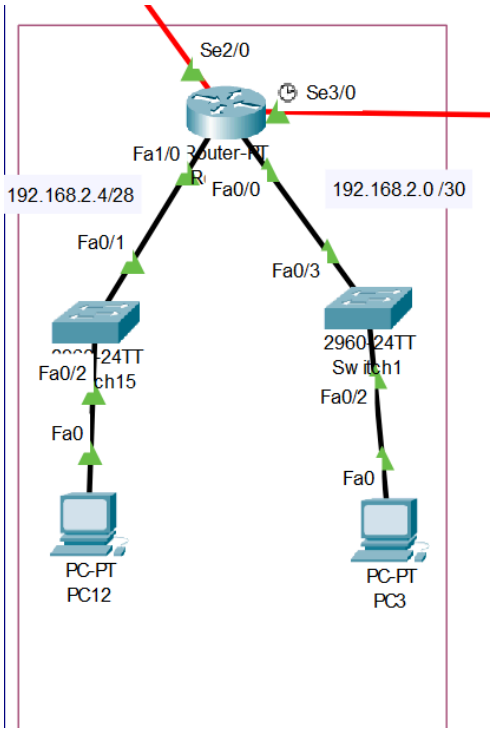
Each building has a router and 2 switches, and each network has two subnets.



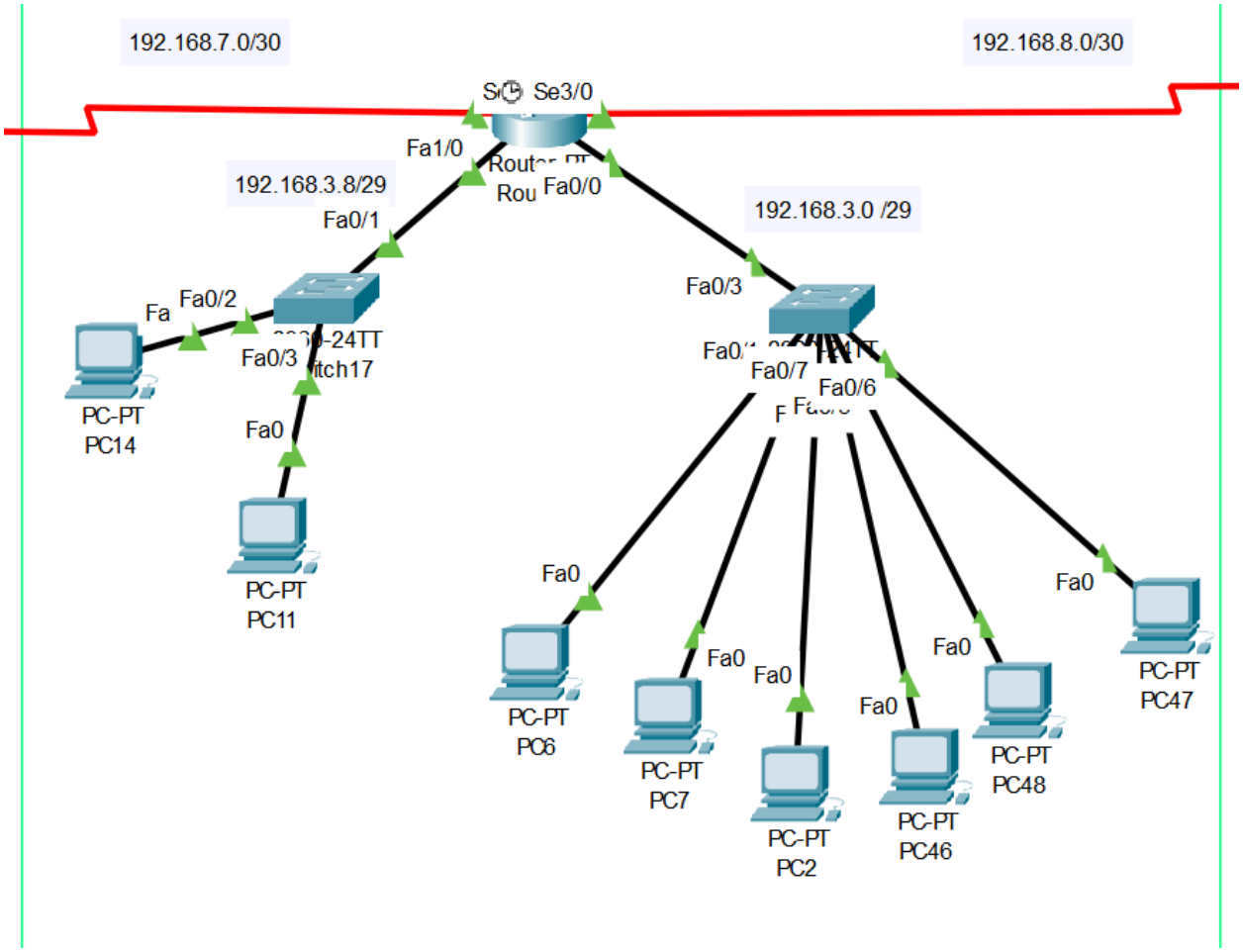


In the above network, there are two subnets. One being 192.168.1.0/19 and the other being 192.168.1.34/30. Each of them has 192.168.1.1 and 192.168.1.35 as the router ip address respectively.

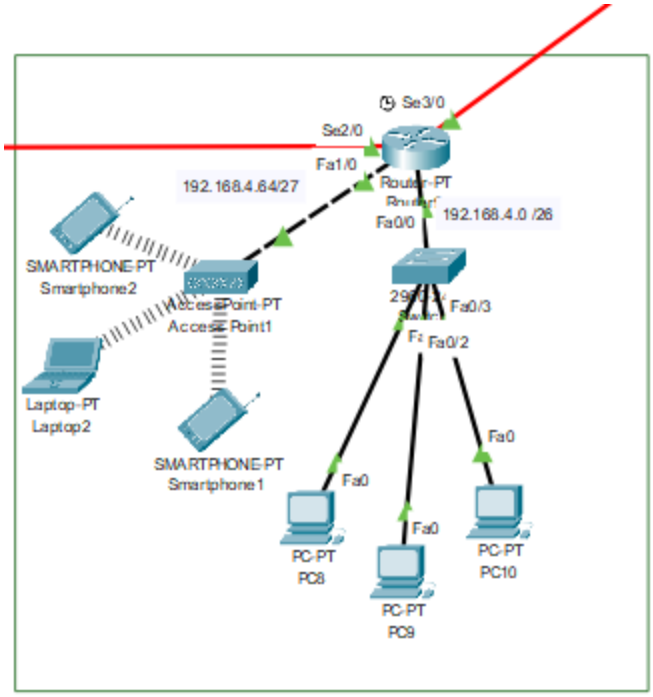
The router is also the DHCP server and dynamically assigns IP addresses to any device that connects to the network. But, in the 192.168.1.0/19 subnet, if I try to add another device to the subnet, it wouldn't allow me due to the max number of hosts being met. This is the same as all the other networks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



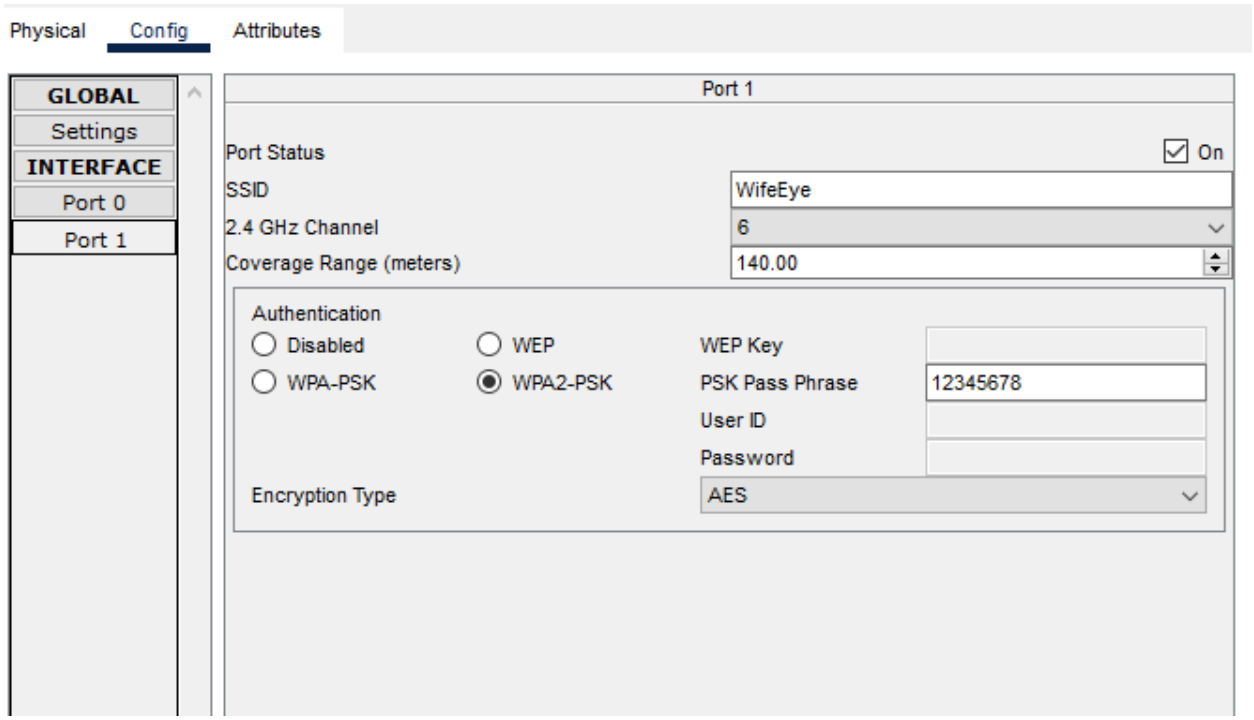
The network above contains two subnets, 192.168.2.0/30 and 192.168.2.4/28. Both of them only allow a maximum of one host. The IP address range of the 192.168.2.4/28 subnets starts from where the other subnet ends. 192.168.2.1 to 192.168.2.2 being the IP address range and 192.168.2.3 being the broadcast 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.



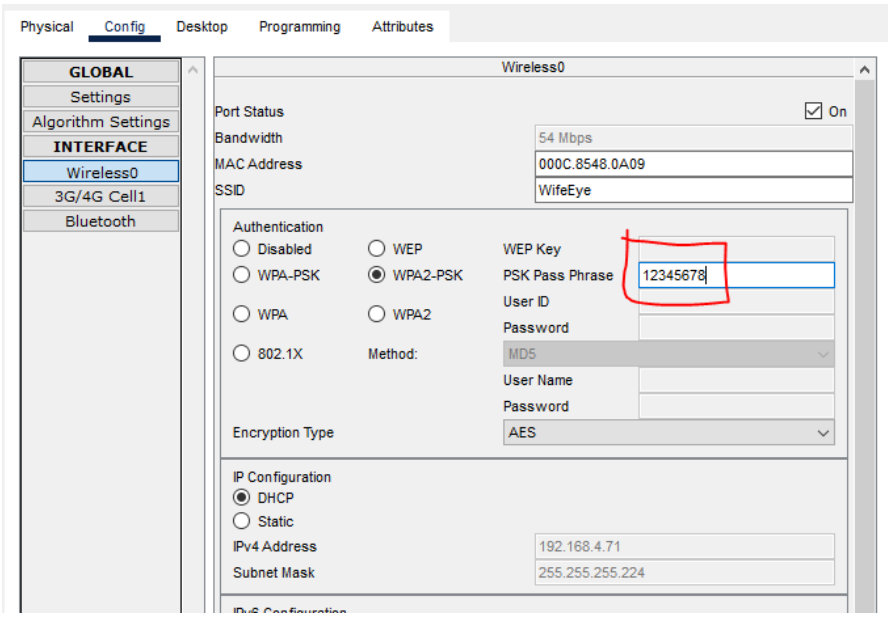
The network above contains two subnets, 192.168.3.0/30 and 192.168.3.8/29. Both of them only allow a maximum of one host. The router IP address of the 192.168.3.0/29 network is 192.168.3.1 with the range of 192.168.3.1 to 192.168.3.5, with 192.168.3.6 being the broadcast's IP address, and 192.168.3.9,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



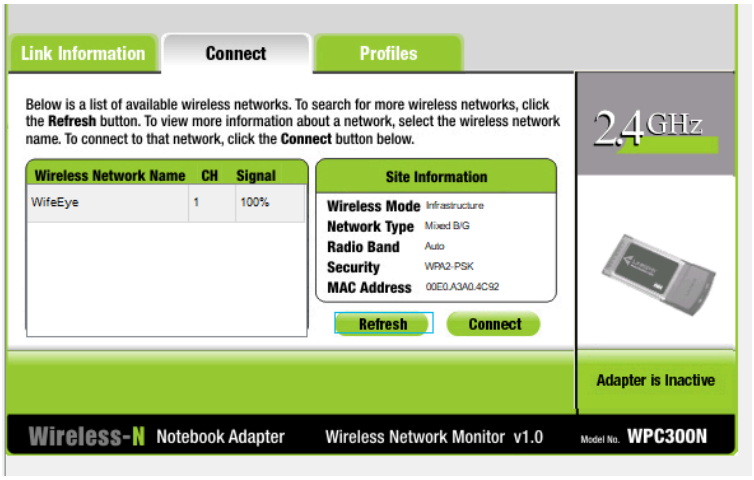
This network has two subnets. One of the subnets has a wireless device as the main connection point.

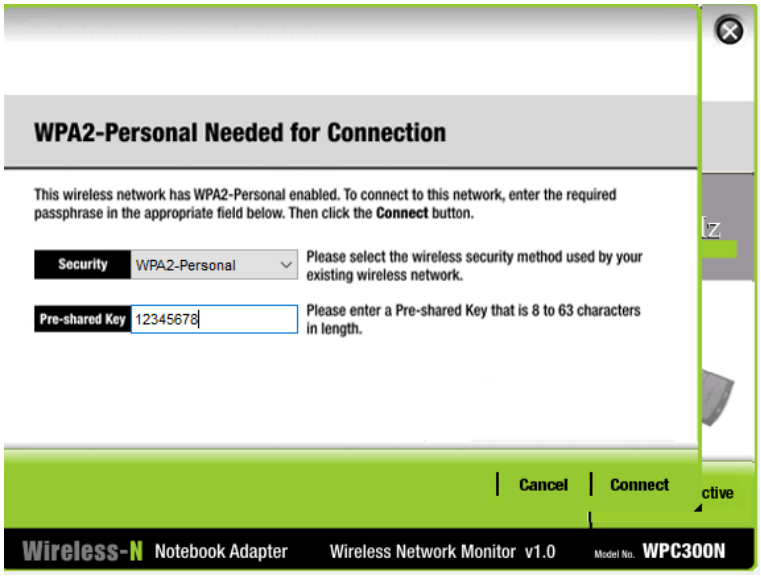


I used the WPA2 security protocol to protect the wireless network.

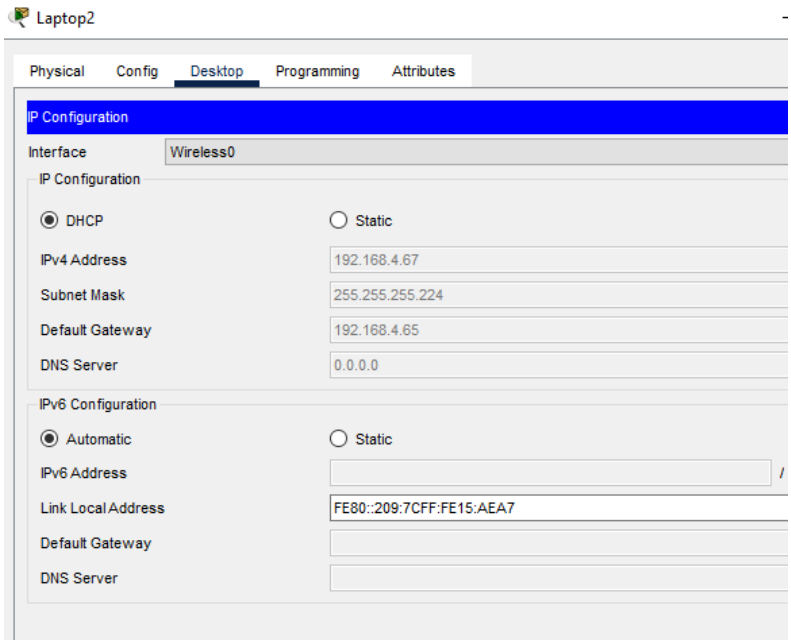


On mobile phones, I have to provide the password of the wireless device before it can connect to it.

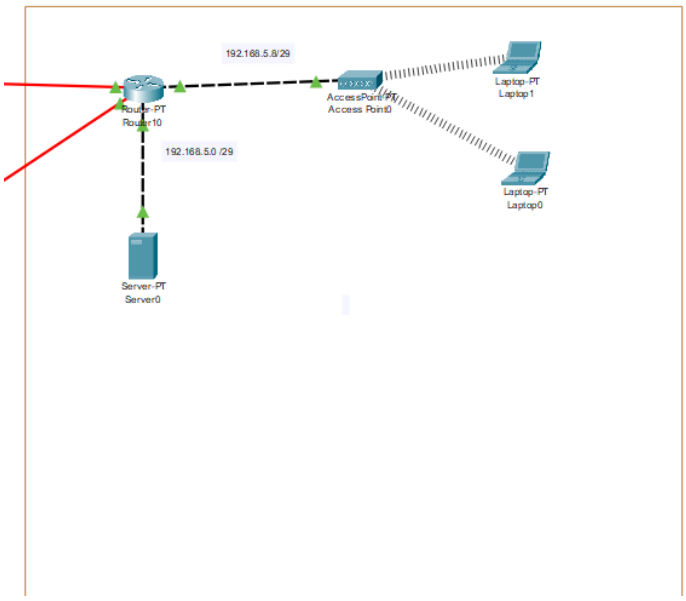




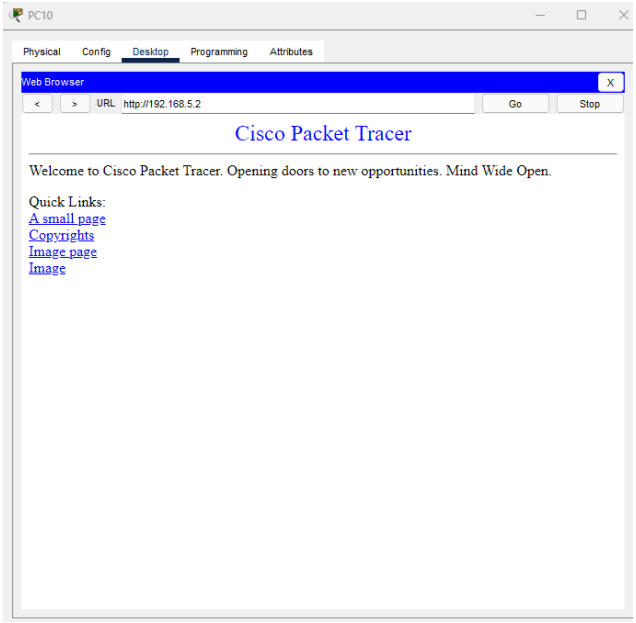
The same applies for the laptop.



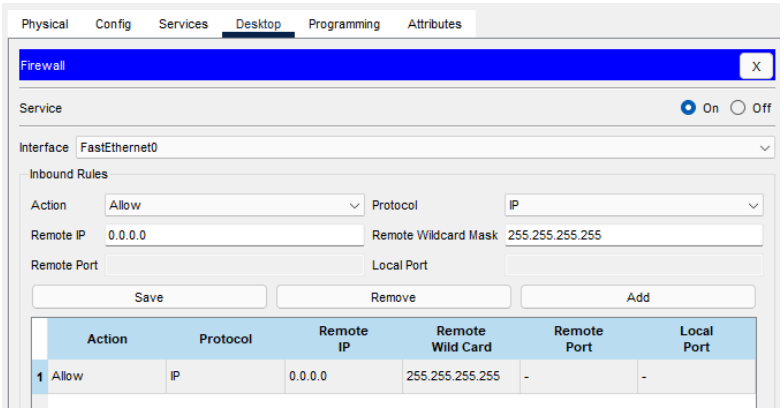
Each of them will then be assigned a unique IP address afterwards.



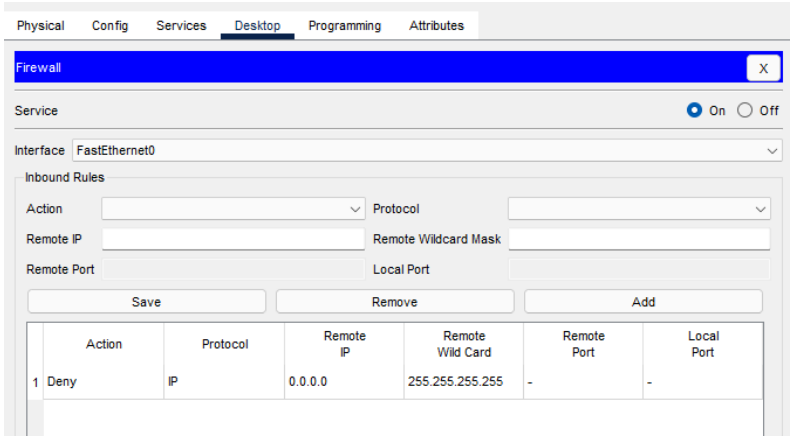
This network contains two subnets. One is wireless, the other is wired. On the wired network, a server is present for hosting applications.



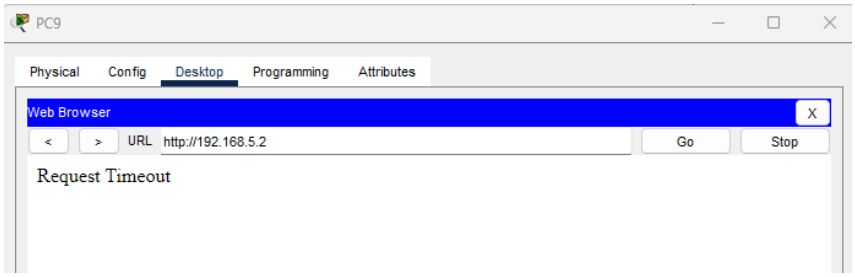
The server can be accessed from any PC, Laptop, or Mobile Phone on the entire network.



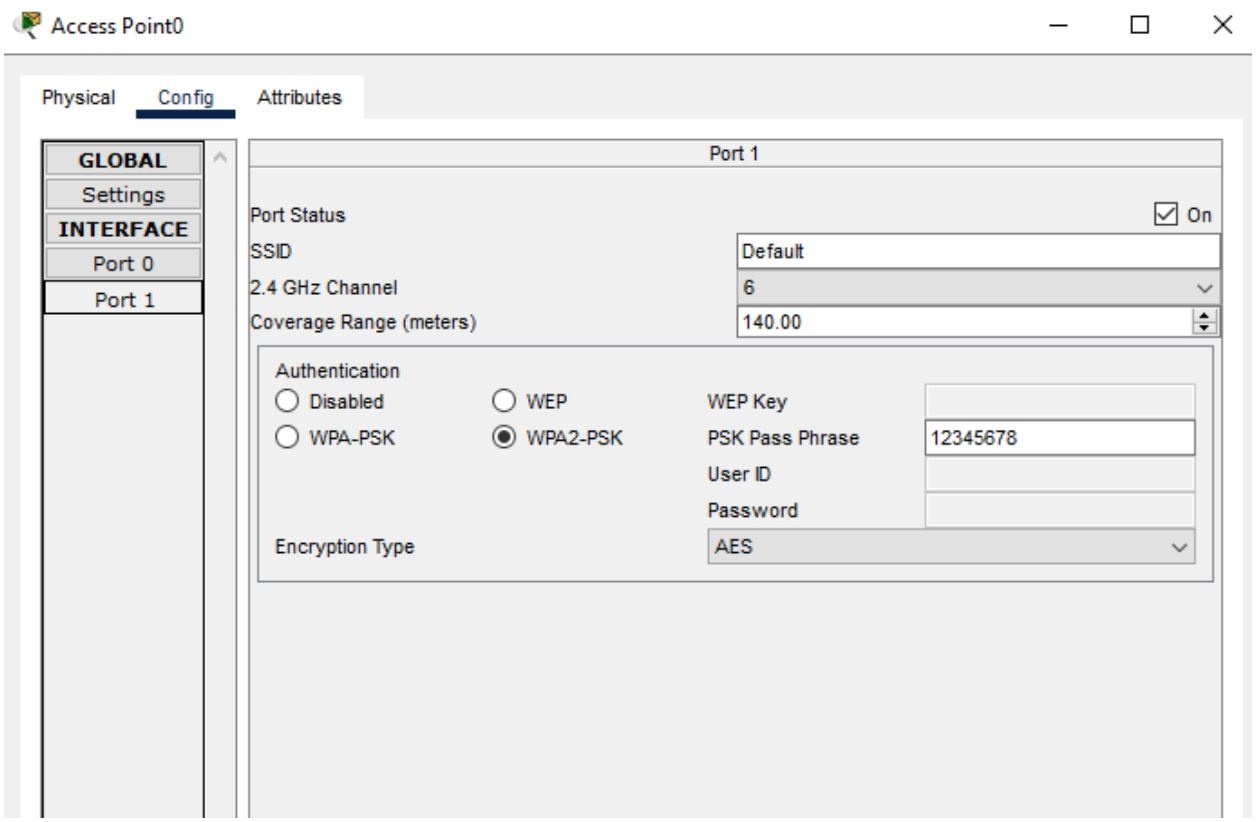
Using the firewall, I gave every device on the network access to the server.



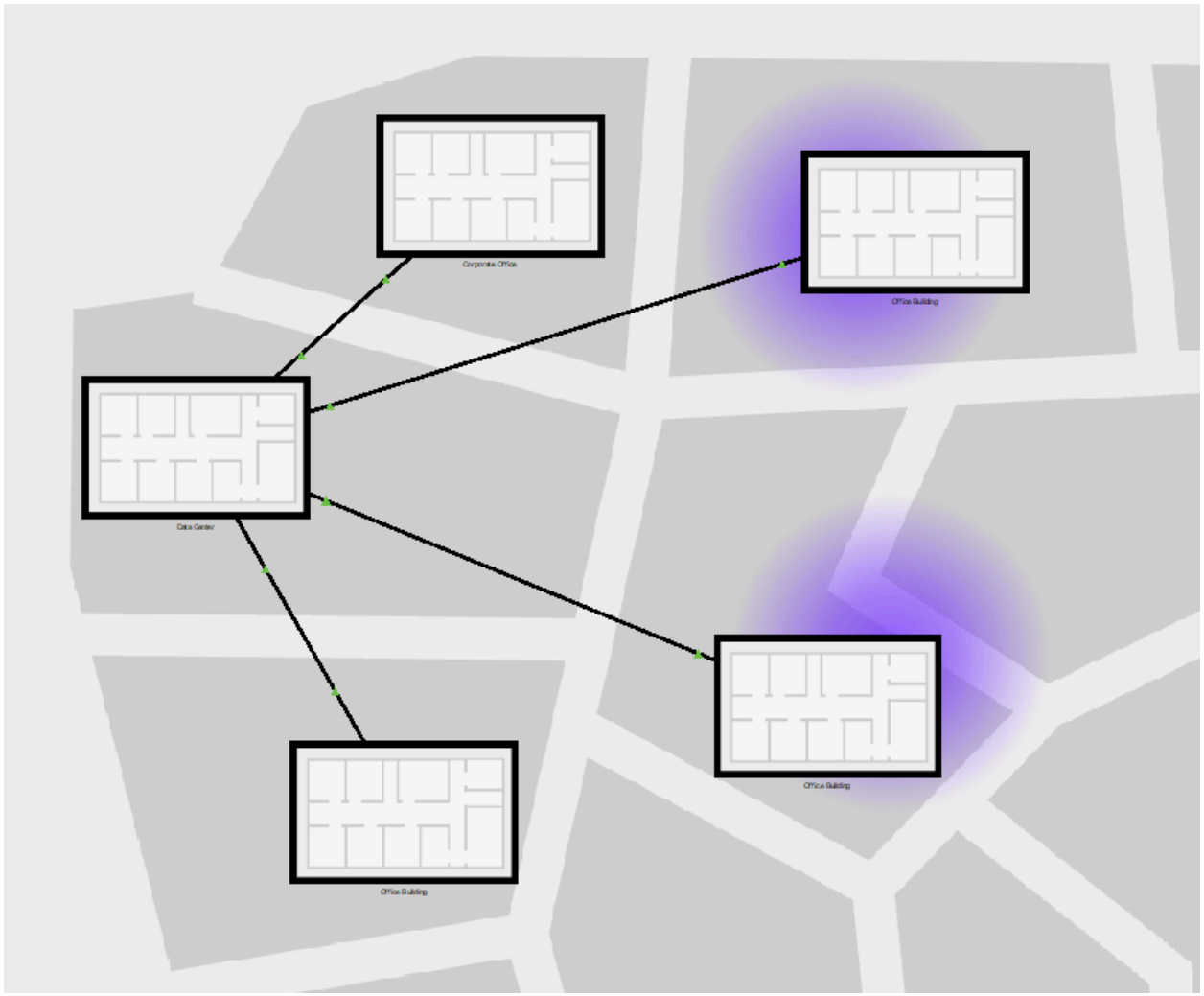
And when it is changed from “Allow” to “Deny”,



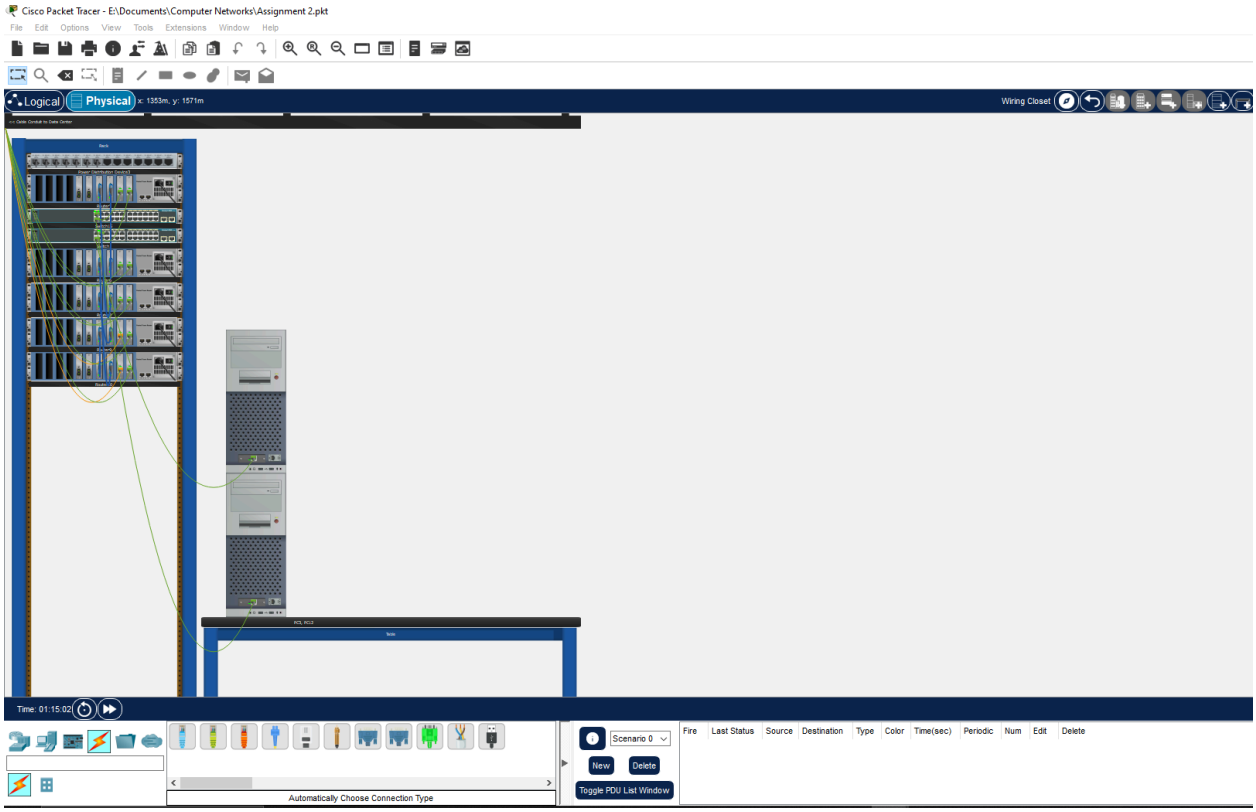
none of the devices can connect to the server.



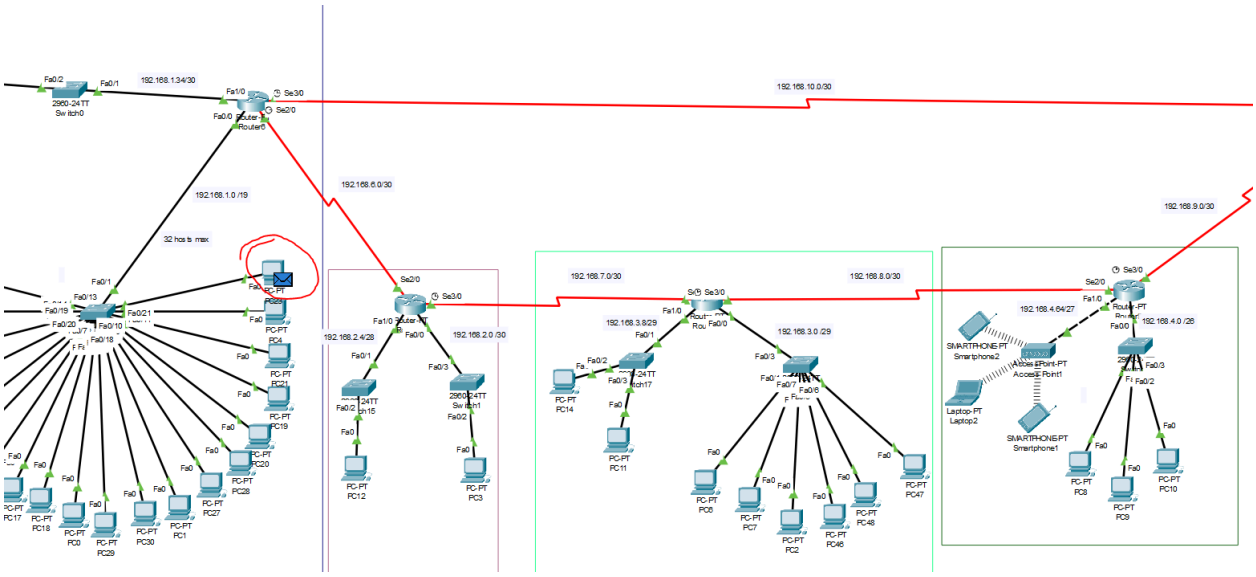
The wireless device on the other subnet (192.168.5.8/29) also uses the WPA2 security protocol and has an IP address of 192.168.5.9.

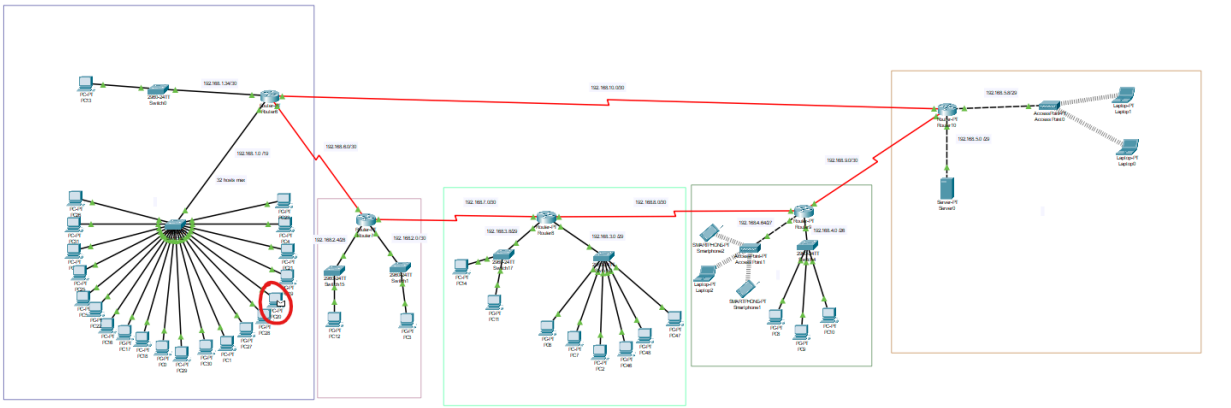


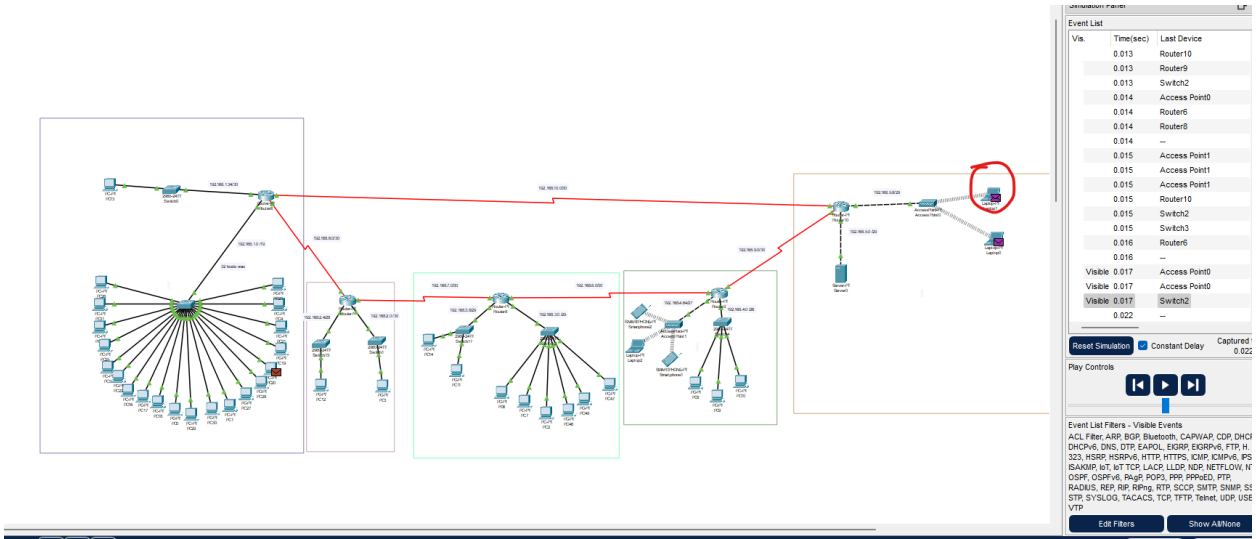
In the physical view, I added five buildings, each with their own network. One of the buildings is a data center where all the routers of each building are located.



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







Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC23	Laptop0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC21	PC10	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC25	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC6	Smartphone2	ICMP		0.000	N	3	(edit)	(delete)

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.