Project One Network Segmentation

William Pascoe

CYB-210: Computer Networking

Jamilah Telon

October 11, 2025

Project One Network Segmentation

We segmented the network by using 3 VLANs. VLAN 50 is the data VLAN. We are using this for workstations throughout the DMV. Next, we have VLAN 80 which is the video VLAN. This VLAN contains the camera s that we installed. The final VLAN that we are currently using is VLAN 70 which is the guest VLAN. This VLAN contains the WIFI router that guests can use to access the internet while they wait. There is a fourth VLAN, VLAN 150, that VLAN is a marked voice and is reserved for future use.

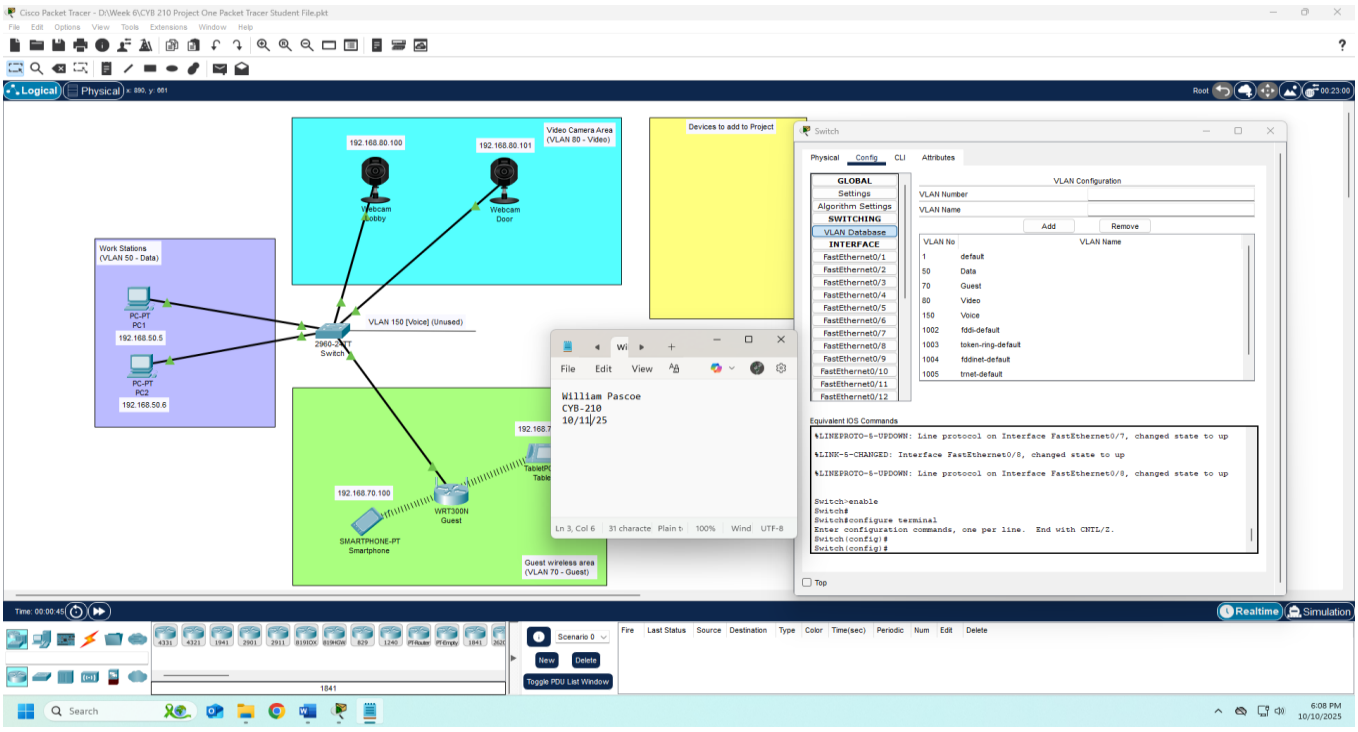
The video VLAN is segmented into its own VLAN and away from the others. This is done so that they can't be accessed though the guest WIFI in the event of a cyberattack. By placing them into their own subnet group we have the capability to add as many cameras as we need in the future. We can also set up protocols so that they can access through the workstation VLAN, VLAN 50, if we wanted certain accounts to have access to them at their workstations.

When creating the guest VLAN we did consider scalability. We gave it its own subnet and set of IP addresses. Even though we currently start the IP address at 100 we can modify it to a lower number, if need be, to allow more IP addresses to be used. Also, by having a short lease time of 4 hours we can ensure that the IP addresses are not tied up for long period of time after they are done being used. This will allow them to be recycled more often and increase the number of users. Another way that we have greater flexibility with the IP addresses is by setting up DHCP. This assigns the IP addresses dynamically so it will ensure that all the numbers in the range are being used as needed and then once a lease expires put that number back in the pool to be reassigned again. We disabled authentication and encryption for this WIFI router. This could be a security concern, but we have segmented it from the other devices on the network by

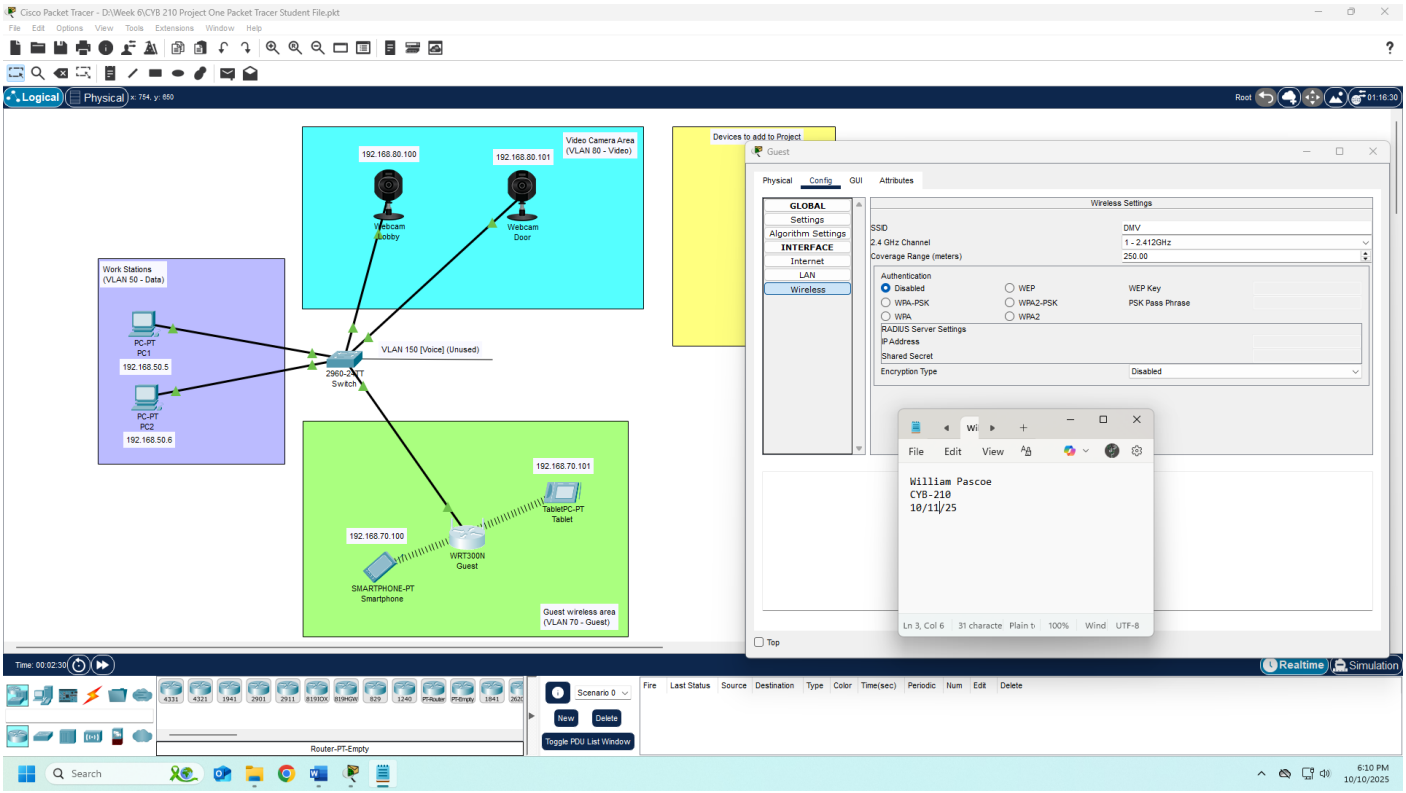
placing it in its own VLAN. The disabling of the authentication was done as more of a convenience to guests wanting to connect to the network.

Screen Shots:

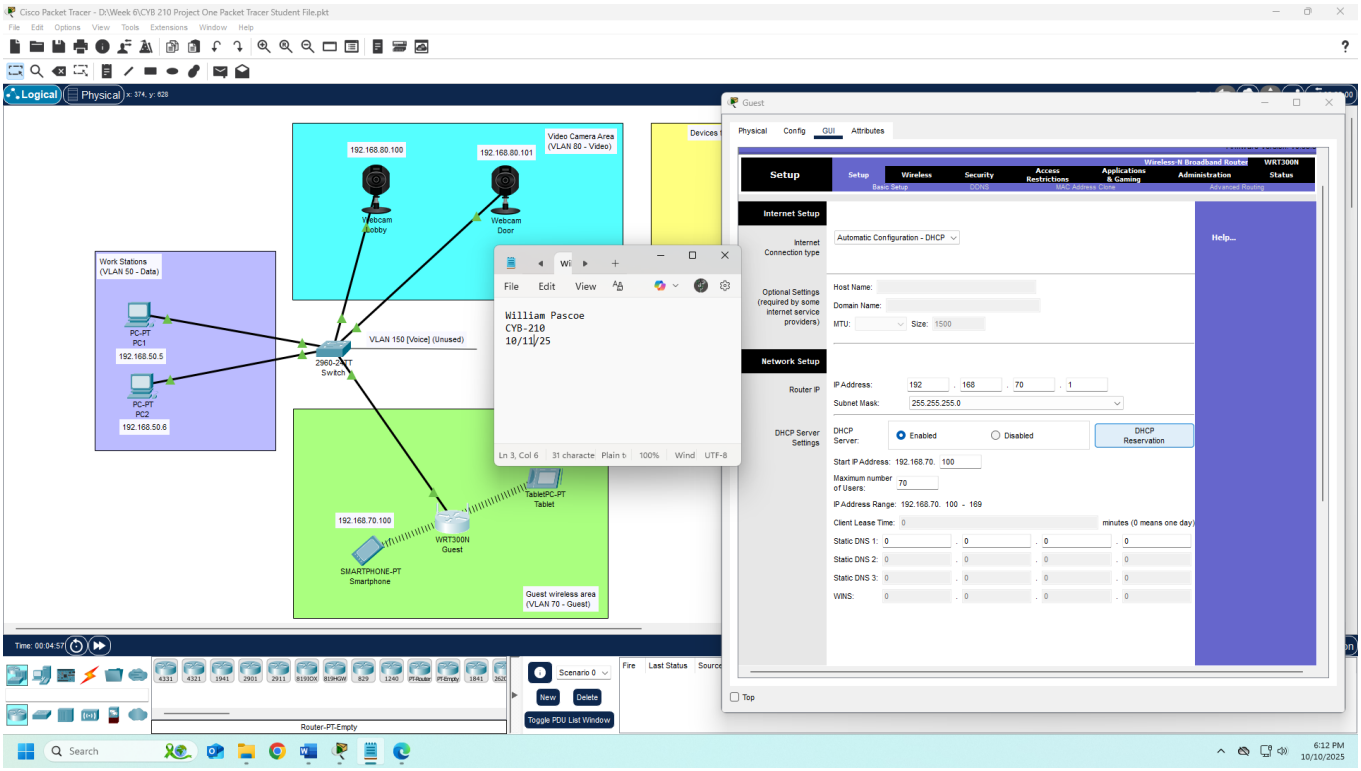
VLAN Table



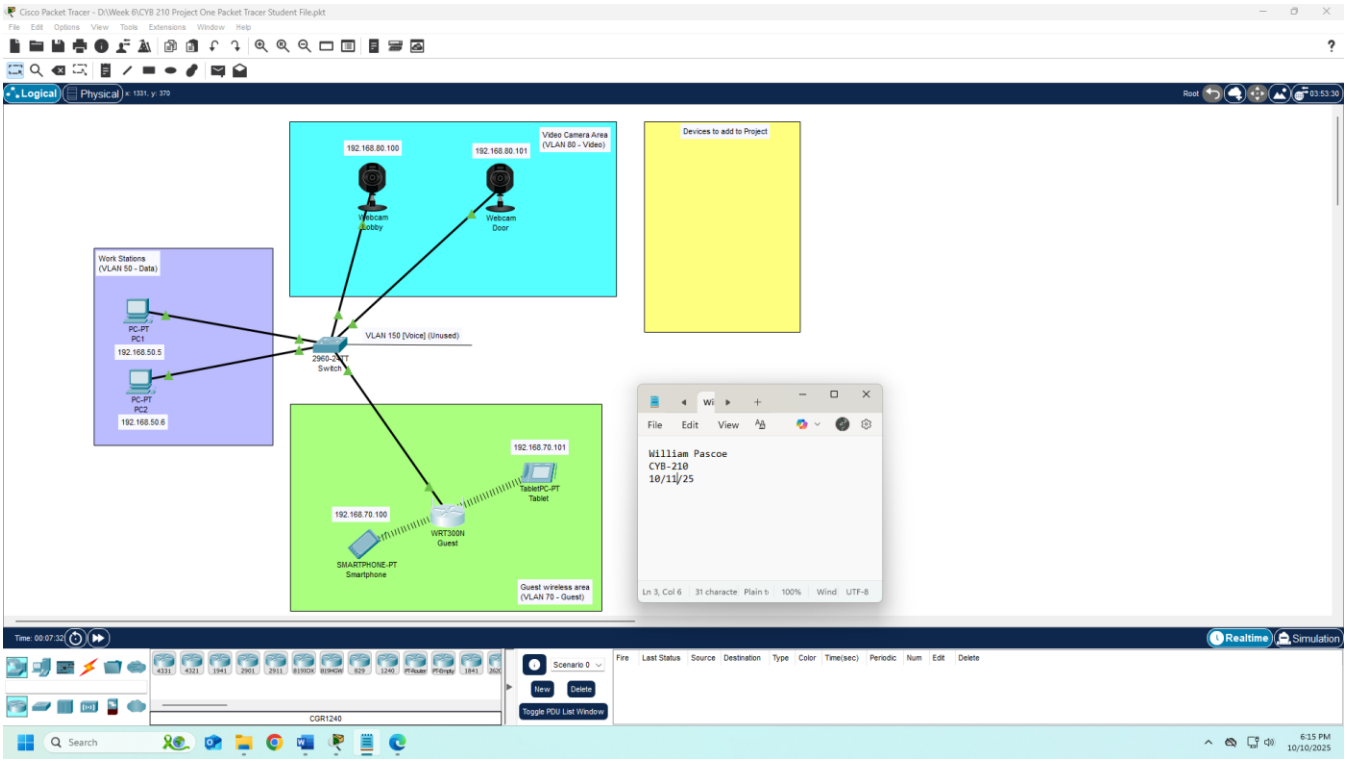
Wireless Router Settings



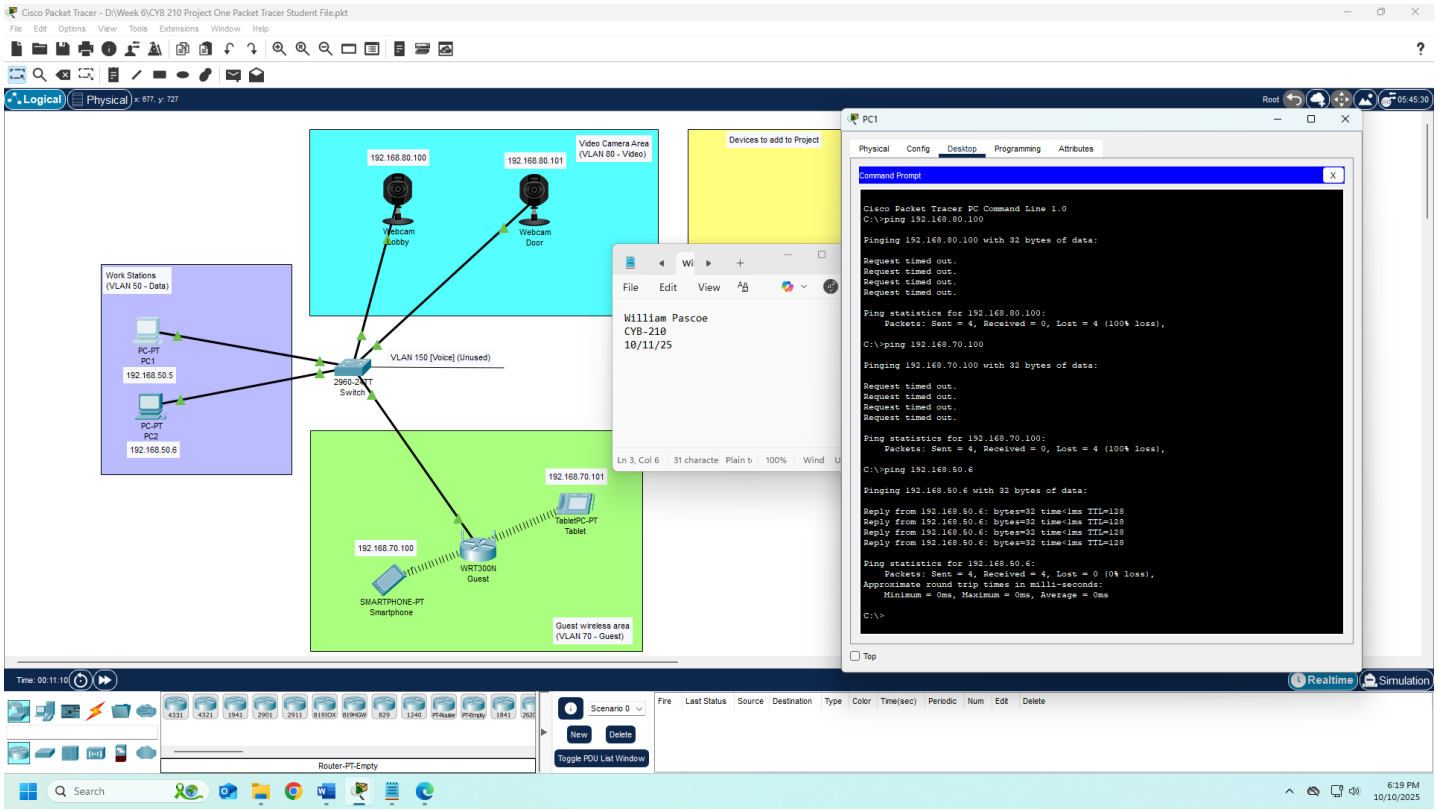
DHCP Setup



Network Diagram



Ping Tests


Cisco Packet Tracer - D:\Week 6\CYB 210 Project One Packet Tracer Student File.pkt
Logical
Physical
Video Camera Area (VLAN 80 - Video)
192.168.80.100
192.168.80.101
Webcam Lobby
Webcam Door
Devices to add to Project
Work Stations (VLAN 50 - Data)
PC-PT PC1
192.168.50.5
PC-PT PC2
192.168.50.6
VLAN 150 [Voice] (Unused)
2960-24TT Switch
192.168.70.101
TabletPC-PT Tablet
192.168.70.100
WRT300N Guest
SMARTPHONE-PT Smartphone
Guest wireless area (VLAN 70 - Guest)
PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.80.100
Pinging 192.168.80.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.80.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.70.100
Pinging 192.168.70.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.70.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.50.6
Pinging 192.168.50.6 with 32 bytes of data:
Reply from 192.168.50.6: bytes=32 time<1ms TTL=128
Reply from 192.168.50.6: bytes=32 time<1ms TTL=128
Reply from 192.168.50.6: bytes=32 time<1ms TTL=128
Reply from 192.168.50.6: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.50.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
William Pascoe
CYB-210
10/11/25
Realtime
Simulation
Router-PT-Empty
Scenario 0
New
Delete
Toggle PDU List Window
6:19 PM
10/10/2025