CAREER EPISODE:3

INTRODUCTION:

CE 3.1 During my [redacted], I worked on the assessment task on "[redacted]", in [redacted] I researched, implemented, monitored, tested and finalized cybersecurity operations in simulated telecom network environment.

BACKGROUND:

CE 3.2 As part of my Diploma, I worked on Evaluate an organization's compliance with cybersecurity standards and law assessment, where I undertook a simulated case study based on organizational cybersecurity incident scenarios where confidential data had been compromised due to multiple security threats; malware, work propagation, DDoS attacks, leaked credentials and internal hacking. I evaluated the existing cybersecurity operations of the organization by reviewing log management, threat detection and monitoring processes to identify weaknesses and gaps. I analyzed the compliance needs of organization against cybersecurity standards and documented required updates like firewall policy enhancements, vulnerability patching, system updates and app security improvements. I then implemented network security controls in a simulated lab environment using Cisco packet tracer by configuring firewall protections, network segmentation, secure administrative access, DHCP allocation, static IP assignments, endpoint security authentication mechanisms. I finally tested and assessed the implemented security controls, updated the cybersecurity operations on the basis of performance outcomes and documented the final security strategy to enhance network protection, reliability and incident response capability.

REPORTING HIERARCHY:

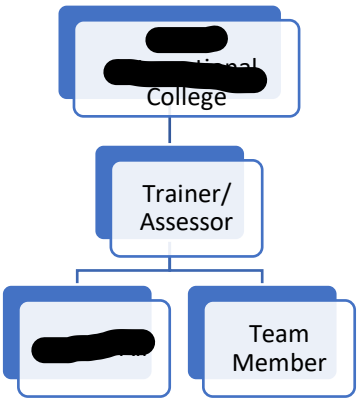


Figure 1: Hierarchy

PERSONAL ENGINEERING ACTIVITIES:

Analysis of Network Security Architecture:

CE 3.3 During this task, I analyzed how security is integrated into telecom network planning and design. I identified the operational needs to secure segmented telecom networks; subnet isolation, controlled routing and secure device communication. I assessed how network security needs; firewall configuration, access control restrictions and DHCP management support secure data flow and service reliability in various network segments. I analyzed how implementing network segmentation helps isolate traffic between user groups and reduce unauthorized access risks. I also defined objectives for network security by assigning roles, establishing monitoring points and ensuring secure communication between routers, switches and end devices.

Implementation of Incident Response & Network Access Controls:

CE 3.4 I developed an incident response plan for handling network security events. I defined the scope of incident management as per the network infrastructure components; routers, switches and end devices. I identified critical network assets; admin PCs, server, interfaces and communication links that needed protection. I assigned response roles and documented escalation procedures to handle network incidents affecting the connectivity, routing or device access. I implemented network security controls; firewall rules, access control restrictions, DHCP limitations and secure remote administration through Telnet for controlled network management. I configured administrative access restrictions so that only authorized systems could access router and switch configuration interfaces, supporting secure network functions and reducing exposure of critical telecom infrastructure.

Testing & Validation of Network Security Controls:

CE 3.5 For assessing effectiveness of implemented network security controls, I applied and analyzed testing techniques. I performed connectivity and segmentation validation test using ping to check that devices in same subnet could communicate while inter subnet communication remained restricted, confirming network isolation. I tested firewall configuration and access control rules by checking restricted access to router GUI and switch telnet interfaces for only authorized administrative devices to perform configuration tasks. I analyzed DHCP behavior for controlled IP allocation and assessed how limiting address pools enhances network protection against unauthorized device access. I reviewed the effectiveness of simulated attack scenarios by evaluating how network segmentation and ACL configurations prevent lateral movement between network segments for secure and reliable operation.

Implementation of Cybersecurity Operations:

CE 3.6 I worked on a simulated organizational case study, where I established and analyzed the existing network security architecture of the organization to find the weaknesses affecting telecom network security and service continuity. I analyzed the existing network topology, device connectivity and security controls to assess their effectiveness in maintaining service continuity and controlling data flow. I reviewed the system inventories, network resources and user activities to find gaps, network vulnerabilities as well as infrastructure vulnerabilities. This analysis helped me identify that although the organization had basic threat detection mechanisms; firewall and antivirus tools, it lacked an asset management process, formal cybersecurity policies and repeatable review procedure. I assessed the impact of security incidents; internal hacking, malware infections and unauthorized access on network availability, operational reliability and confidential data protection.

CE 3.7 Based on my analysis, I then found and documented the enhancements required to enhance network security. I proposed system updates for operating systems, software, firmware and critical apps to reduce vulnerabilities caused by outdated systems. I reviewed firewall considerations and developed updated traffic filtering rules for traffic filtering and network perimeter defense. I identified security weaknesses needing vulnerability patching and suggested patch management to enhance consistency. I analyzed major service disruption threats including malware on client workstations, worm propagation across the network, distributed denial of service attacks and leaked user credentials. I assessed how these incidents could impact telecom network performance, communication reliability and data confidentiality. Based on this, I documented mitigation measures including network segmentation, access control, multi factor authentication, stronger password policies and DDoS traffic filtering.

CE 3.8 I used Cisco packet tracer to configure and test firewall security operations in a simulated network environment. I configured firewall rules, router administrative access restriction, switch telnet access controls and secure wireless authentication to protect network resources and control communication paths. I tested network segmentation by performing connectivity validation for that dices within same subnet to communicate while communication between various subnets remains restricted as per the configured policy. I restricted DHCP address allocation to control endpoint access and reduce the risks of excessive unauthorized connections affecting network stability. I checked secure remote management by testing telnet access to confirm that only authorized admin devices could establish switch management sessions. It strengthened my practical skills in network security planning, cyber threat analysis, firewall configuration, incident response documentation and telecom network protection.

Implementation & Testing of Cybersecurity Operations:

CE 3.9 I implemented organizational security operations in simulated IT laboratory environment by installing and configuring security and simulation tools; Cisco packet tracer and endpoint security apps; Cisco secure endpoint, FireEye, sentinleOne and Sophos. I documented the installation process and checked software compatibility with the system needs, including network connectivity, browser support and operating system readiness. Through this, I established the needed software environment for implementing and monitoring cybersecurity operations within the network simulation scenario. I configured the network security using Cisco packet tracer by developing a network topology divided into 2 subnets; 192.168.100.0/24 and 10.0.0.0/8, to enhance traffic control and network segmentation. I configured DHCP services to automatically assign IP addresses to student laboratory systems while assigning static IP addresses to devices; administrator system and printers for reliable communication. I implemented firewall configuration to control inbound and outbound traffic and restrict communication between various subnets based on security needs. I configured secure admin access by allowing only the admin workstation to access the router configuration interface and implemented remote switch access using Telnet with authentication controls. I configured wireless security by enabling SSID broadcasting, applied wireless authentication and secured access through password protection for controlled wireless connectivity.

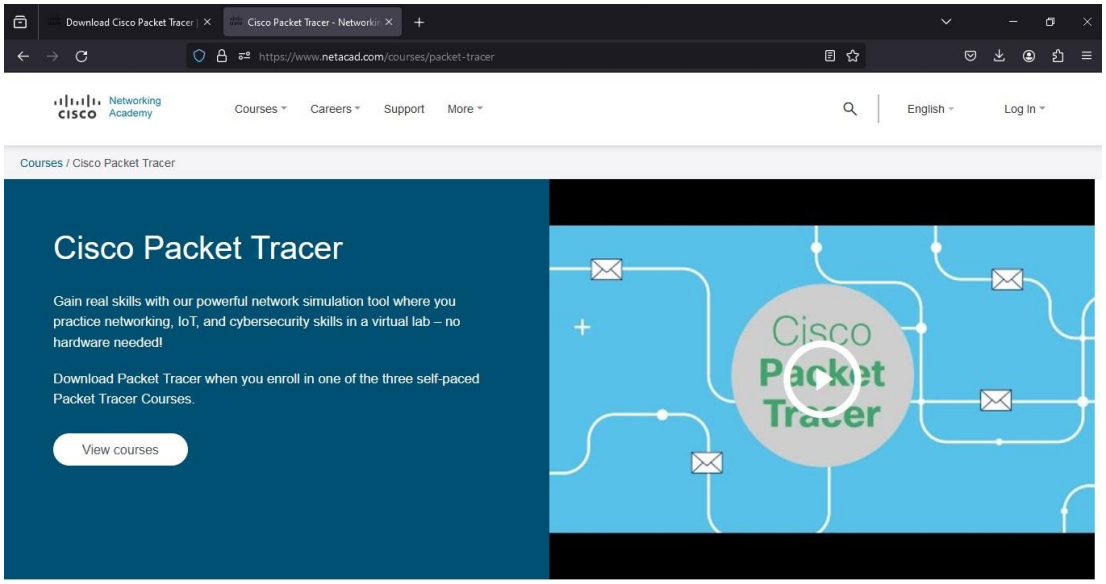


Figure 2: Cisco packet tracer website

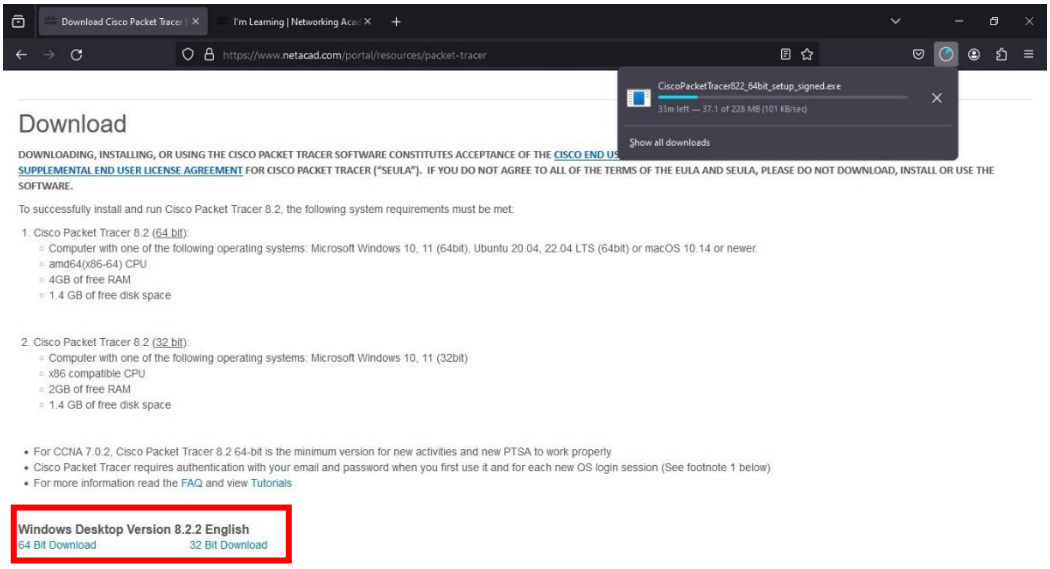


Figure 3: Downloading Cisco packet tracer

Figure 4: Running the installer

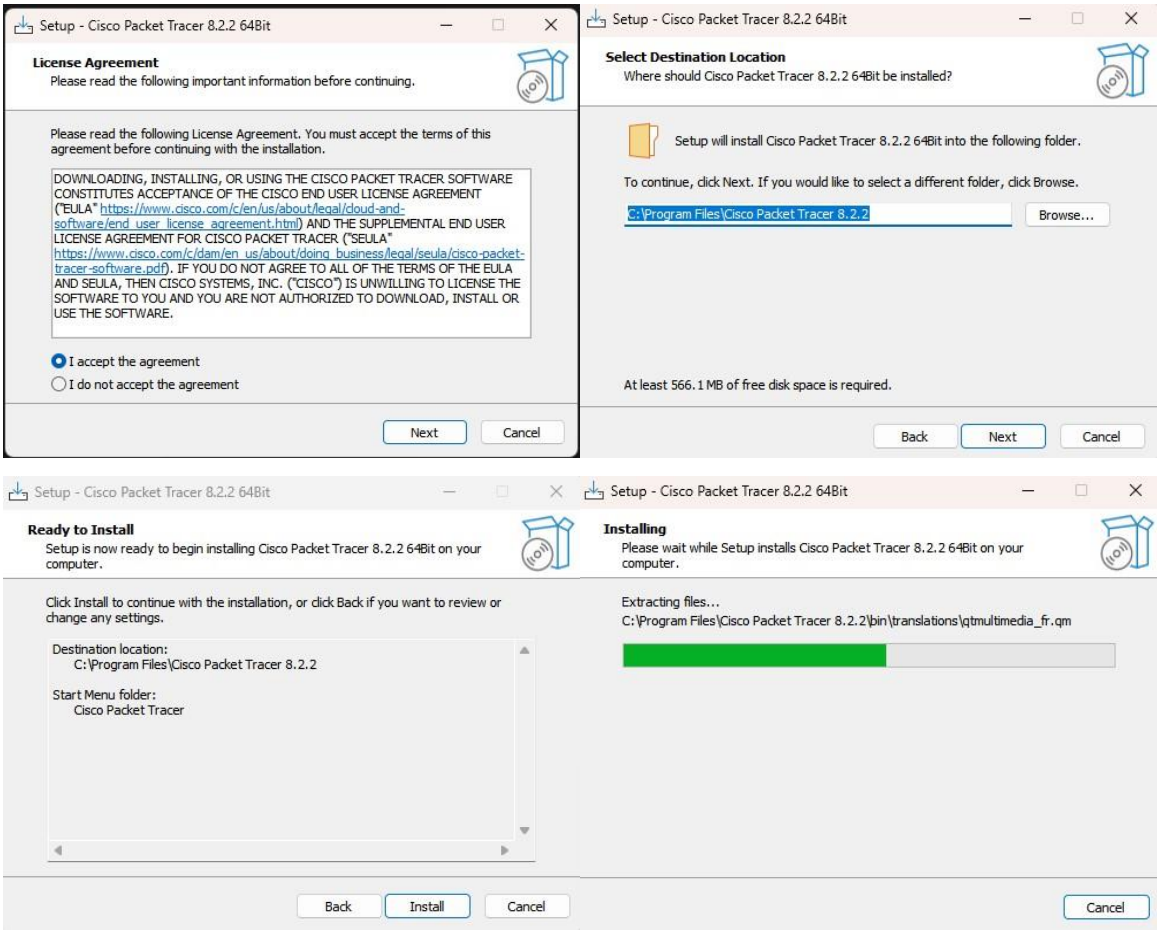


Figure 5: Accepting license agreement and proceeding with installation

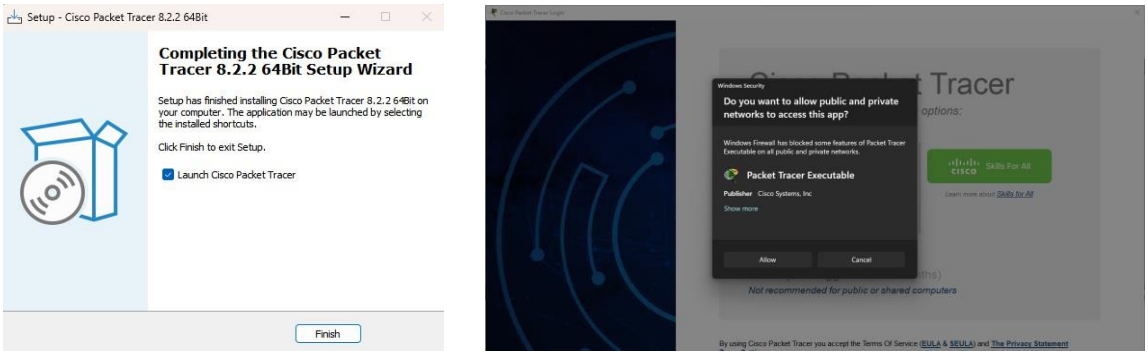
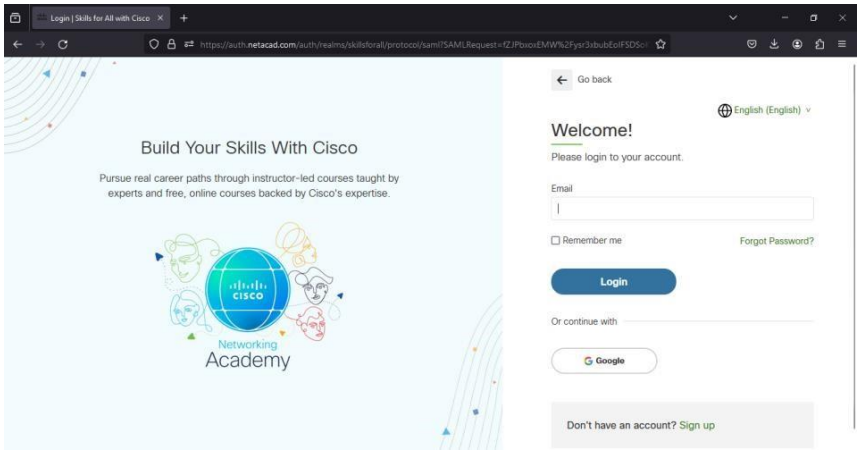


Figure 6: Launching and allowing windows security network access



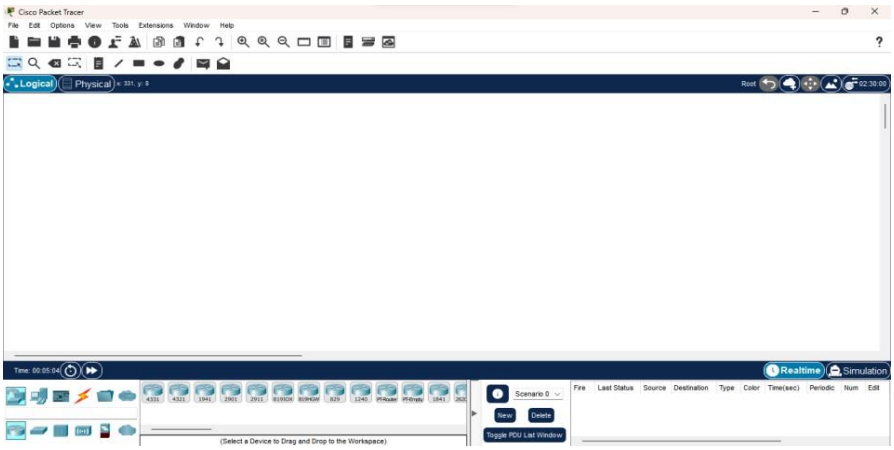


Figure 7: Signing in

CE 3.10 To enhance security and incident response capability, I performed antivirus scanning using built-in Windows defender and reviewed Windows firewall configurations to detect and prevent malware threats. I monitored endpoint tasks and analyzed abnormal traffic patterns, unauthorized access attempts and unusual endpoint behavior to detect security incidents and support timely threat response. I implemented 2-factor authentication to enhance account security and reduce unauthorized access risks. To reduce DDoS exposure, I configured and restricted DHCP pool to control device allocation and prevent excessive unauthorized connections. I also segmented the network into separate LANs to restrict the spread of worms and malware between devices. This implementation, enhanced my skills in network security configuration, endpoint protection, access control implementation, firewall management and telecom network security.

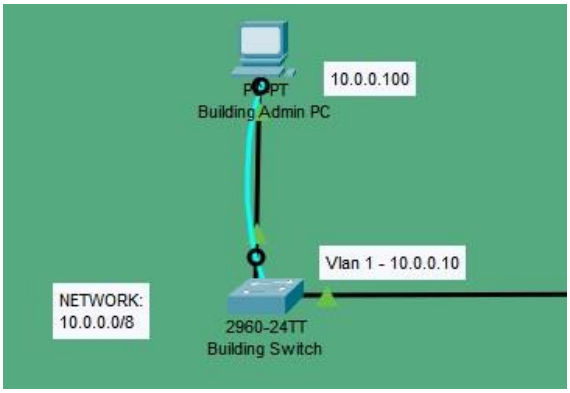


Figure 8: Connecting PC and switch using console cable

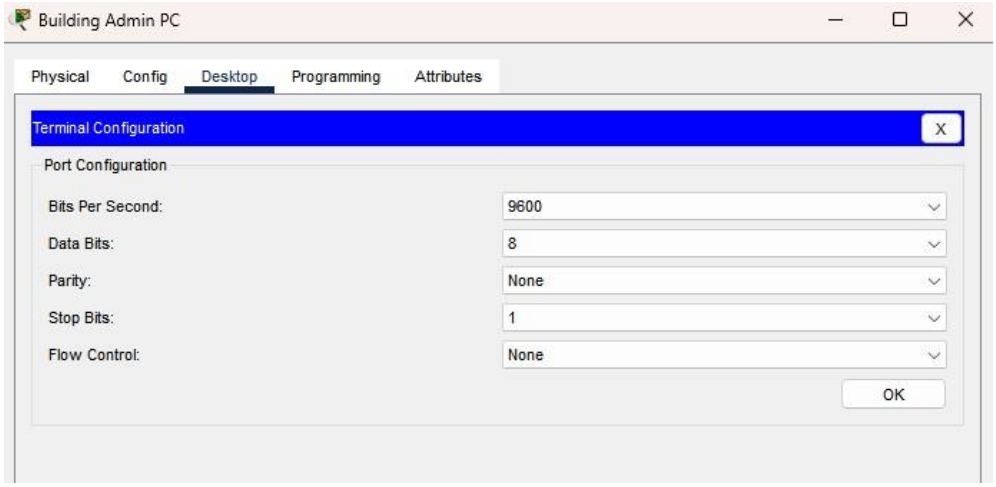


Figure 9: Accessing switch using terminal configuration

```
Switch(config)#
Switch(config)#hostname BuildingSwitch
BuildingSwitch(config)#enable secret #50Grenfell
BuildingSwitch(config)#banner motd ^
Enter TEXT message.  End with the character '^'.

UNAUTHORIZED ACCESS IS RESTRICTED!

^

BuildingSwitch(config)#
```

Figure 10: Applying configuration

```
BuildingSwitch(config)#
BuildingSwitch(config)#interface vlan 1
BuildingSwitch(config-if)#ip address 10.0.0.10 255.0.0.0
BuildingSwitch(config-if)#no shutdown

BuildingSwitch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

BuildingSwitch(config-if)#exit
BuildingSwitch(config)#
```

Figure 11: Assigning IP address for VLAN 1

```
BuildingSwitch(config)#
BuildingSwitch(config)#line vty 0 4
BuildingSwitch(config-line)#password #Telnet50Grenfell
BuildingSwitch(config-line)#login
BuildingSwitch(config-line)#exit
BuildingSwitch(config)#
```

Figure 12: Setting up telnet connections

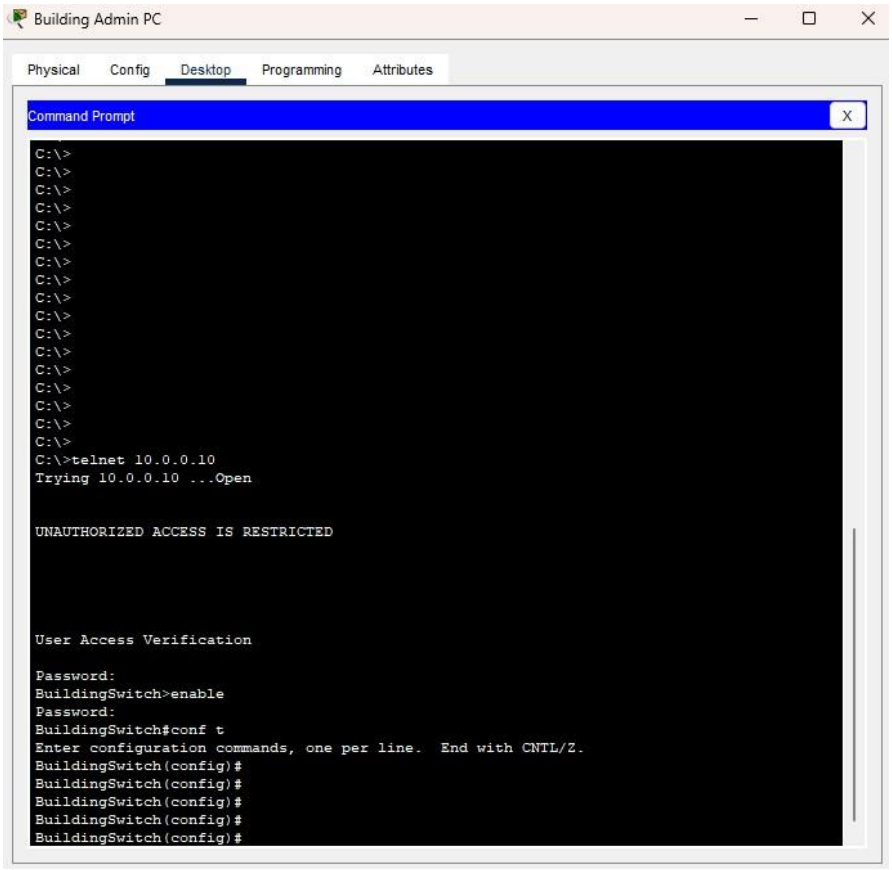


Figure 13: Accessing switch remotely using telnet

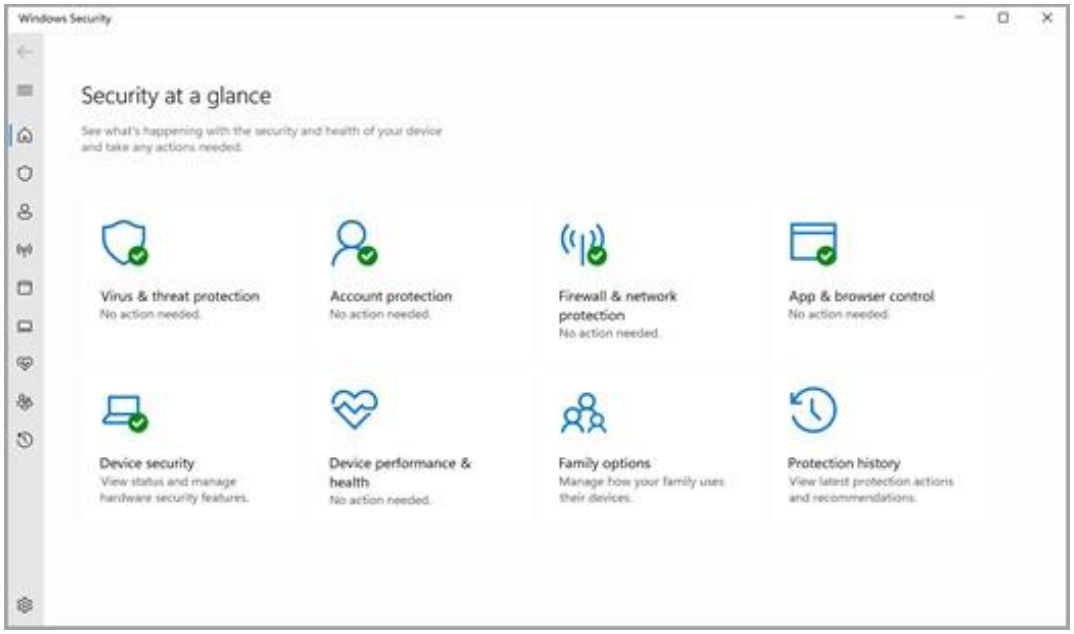


Figure 14: Preconfigured settings

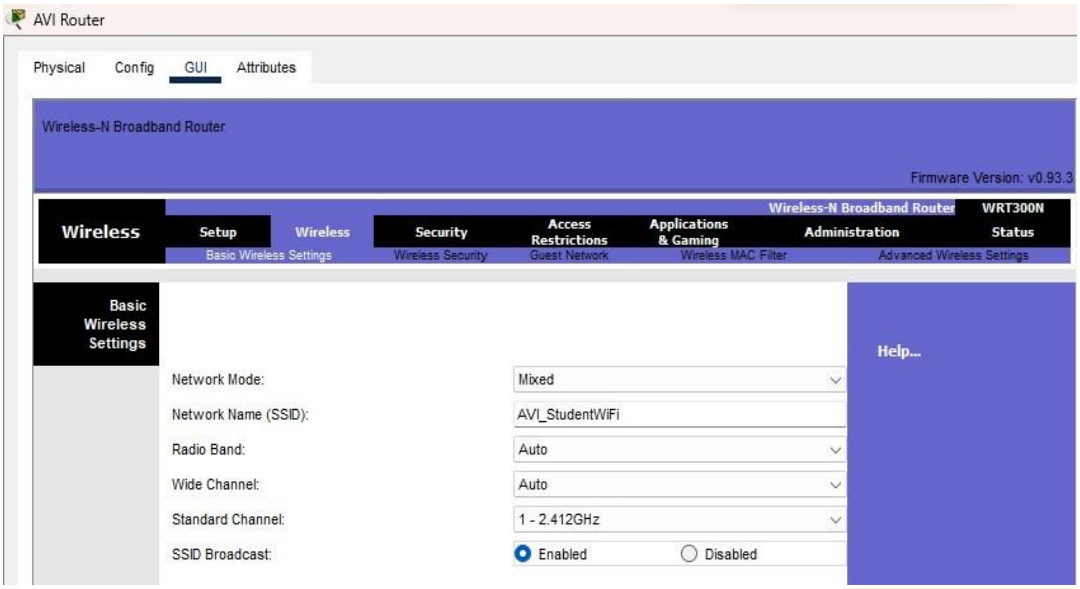


Figure 15: Enabling broadcast and inputting an SSID

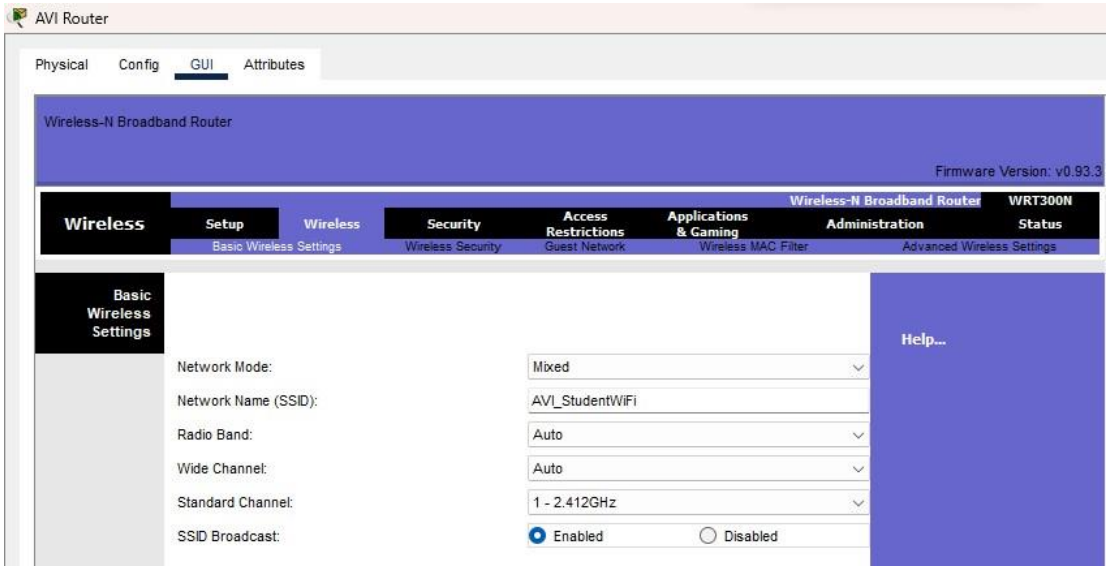


Figure 16: Selecting wireless security mode and assigning password

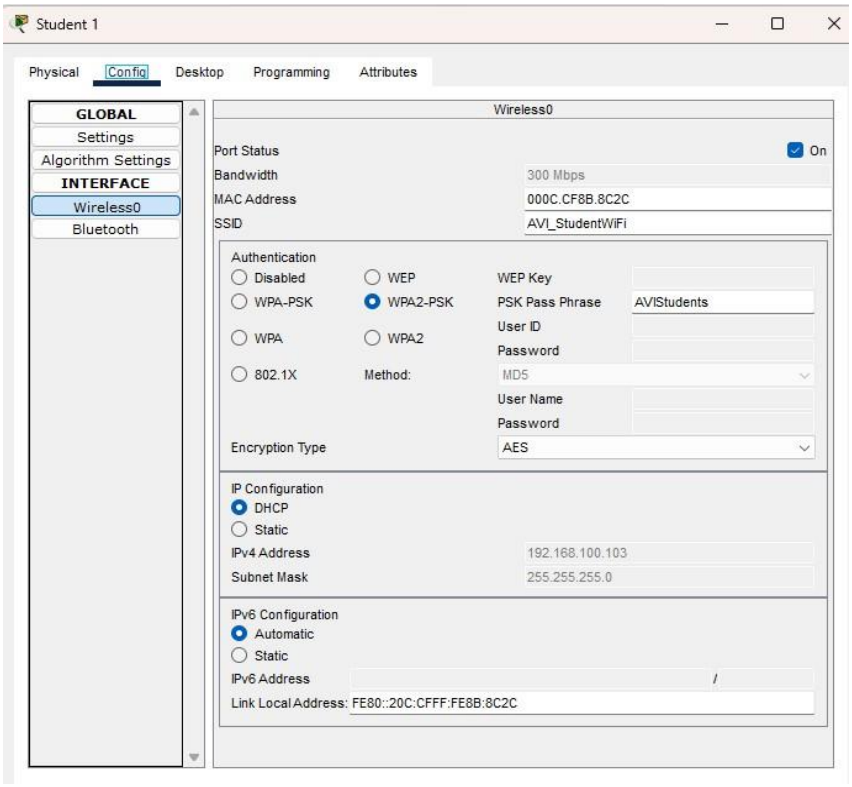


Figure 17: Connecting to Wi-Fi

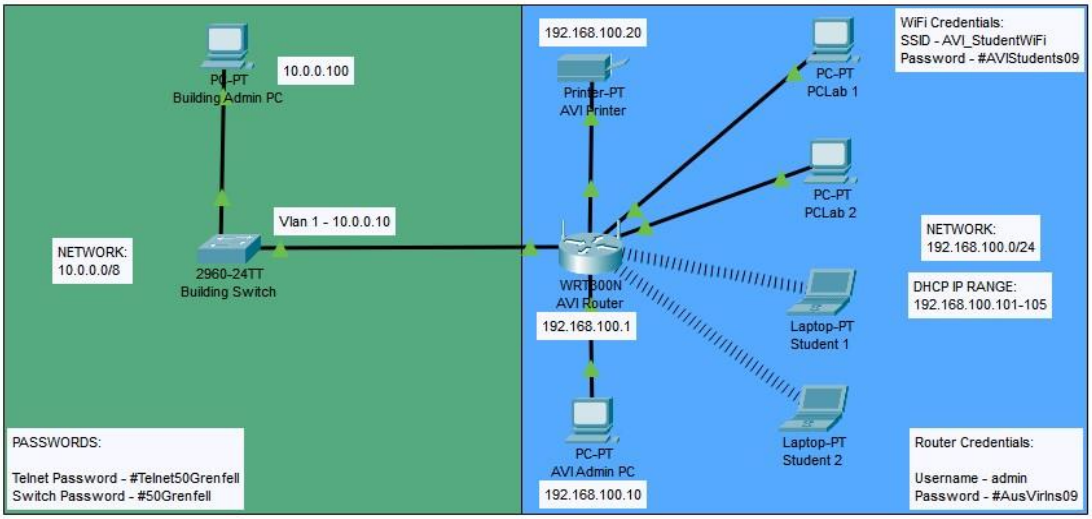


Figure 18: Network topology

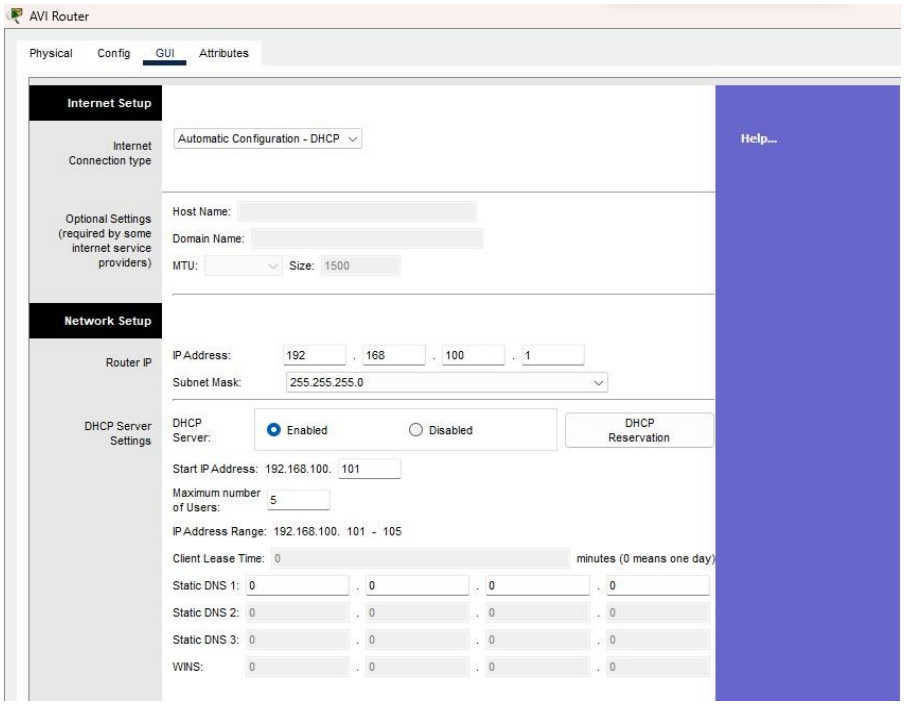


Figure 19: DHCP configuration- router

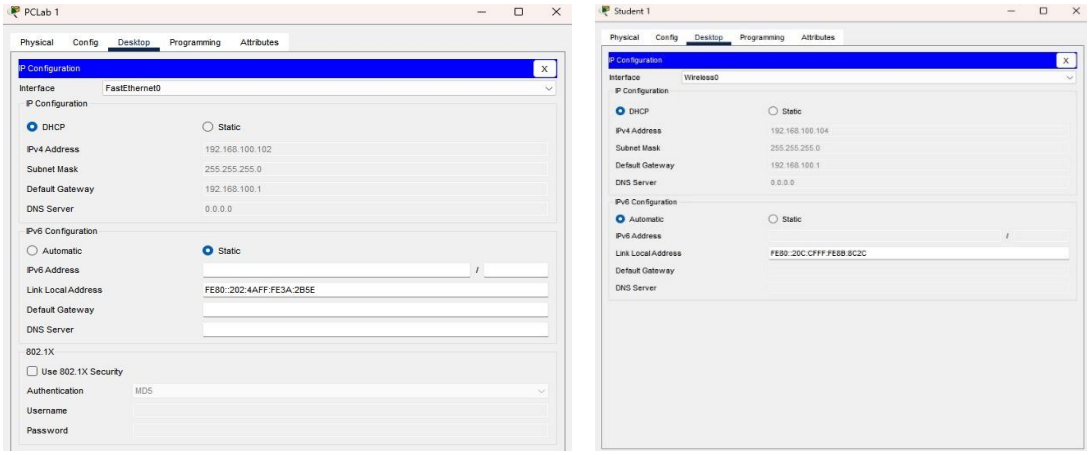


Figure 20: DHCP configuration-host

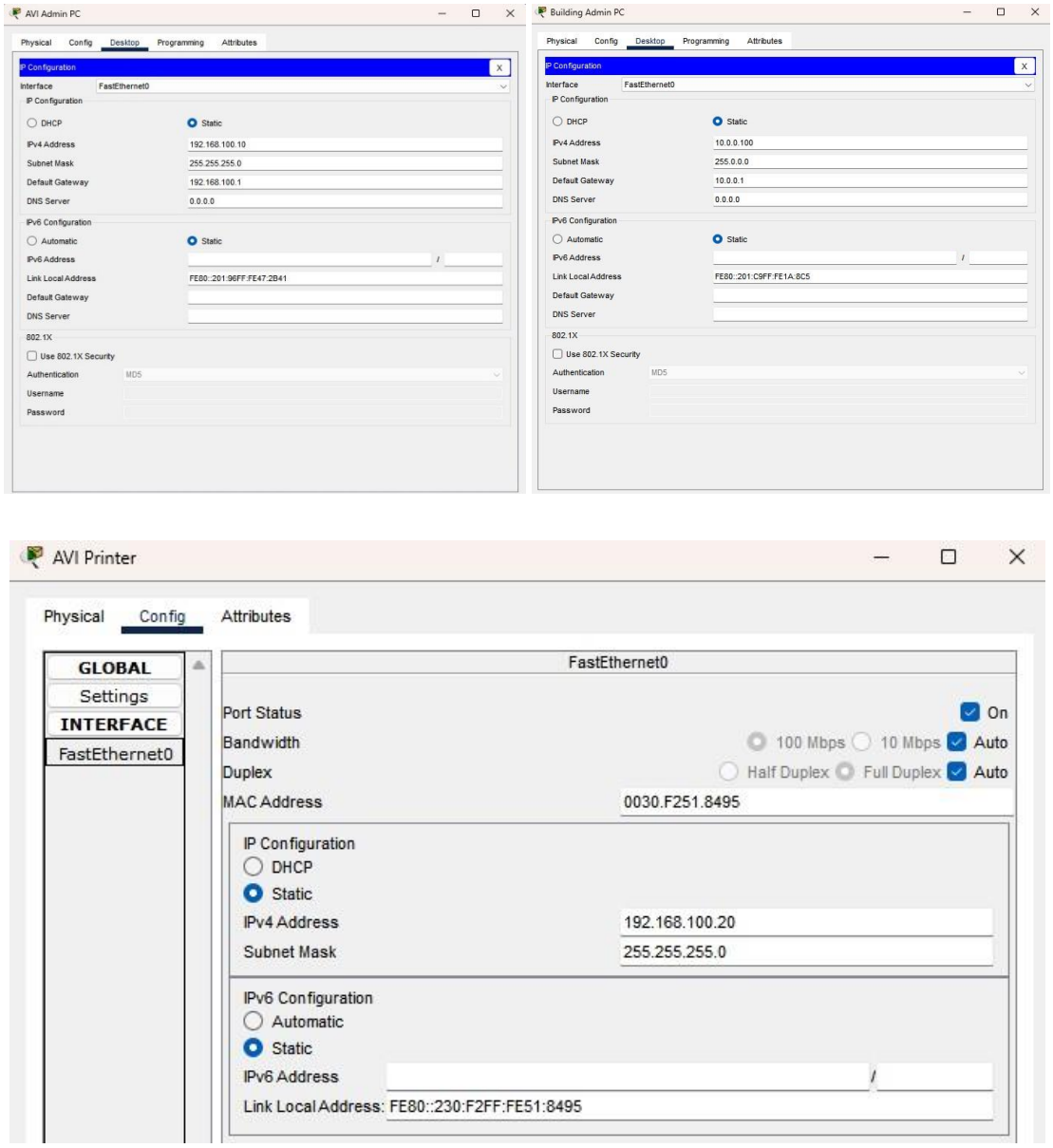


Figure 21: Static IP configuration- end hosts

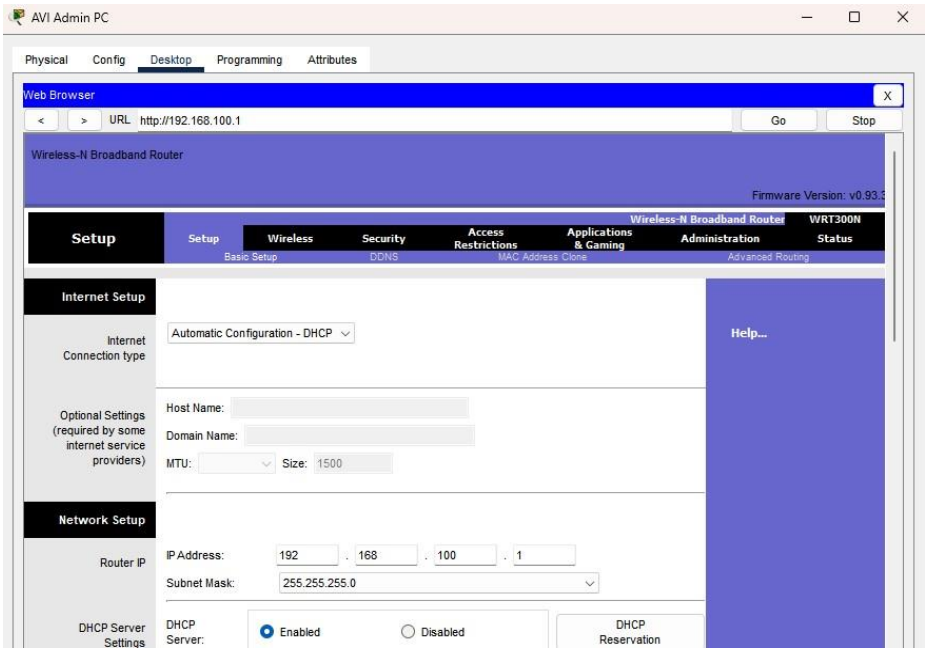


Figure 22: AVI router GUI access by AVI network admin

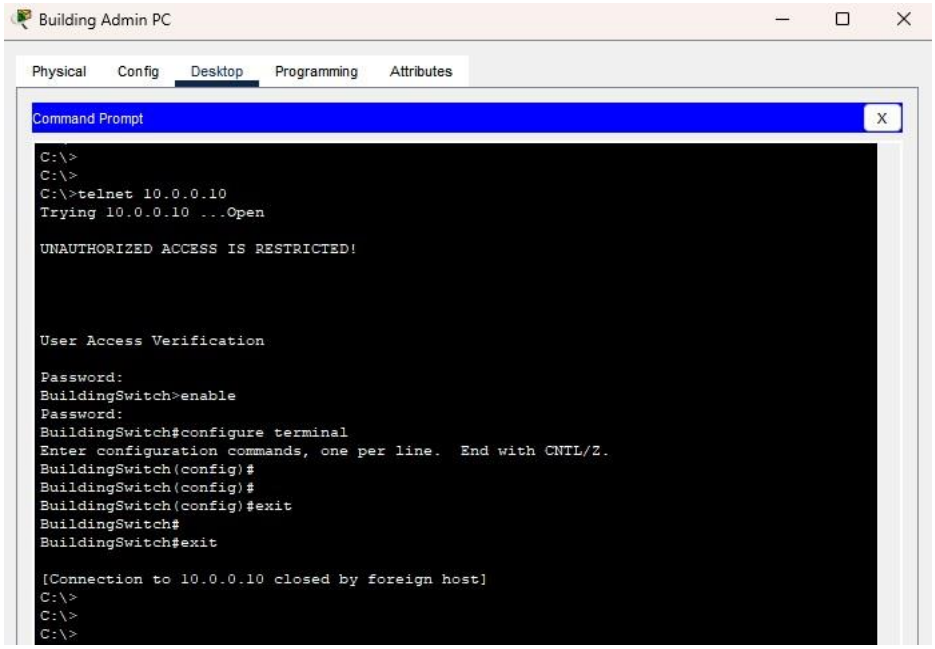


Figure 23: Building switch remote access

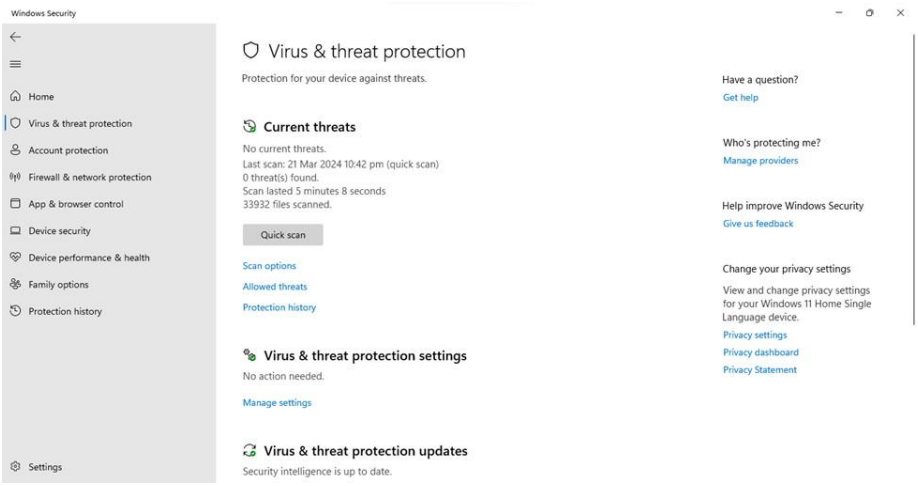


Figure 24: Executing antivirus software scan

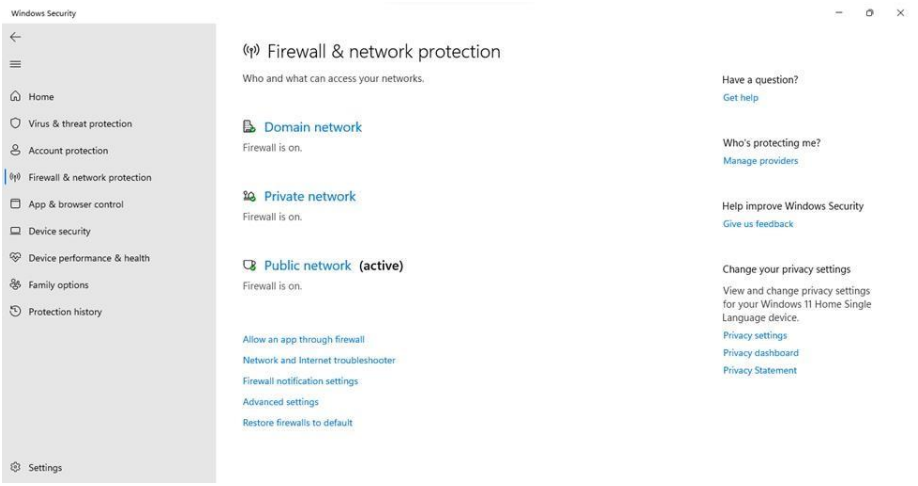


Figure 25: Checking configuration of windows firewall

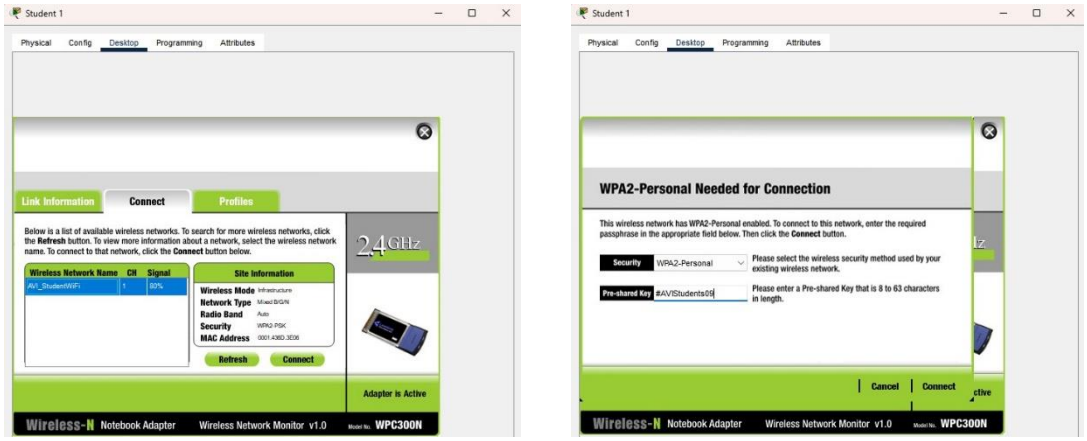


Figure 26: Adding authentication when connecting the end devices to network

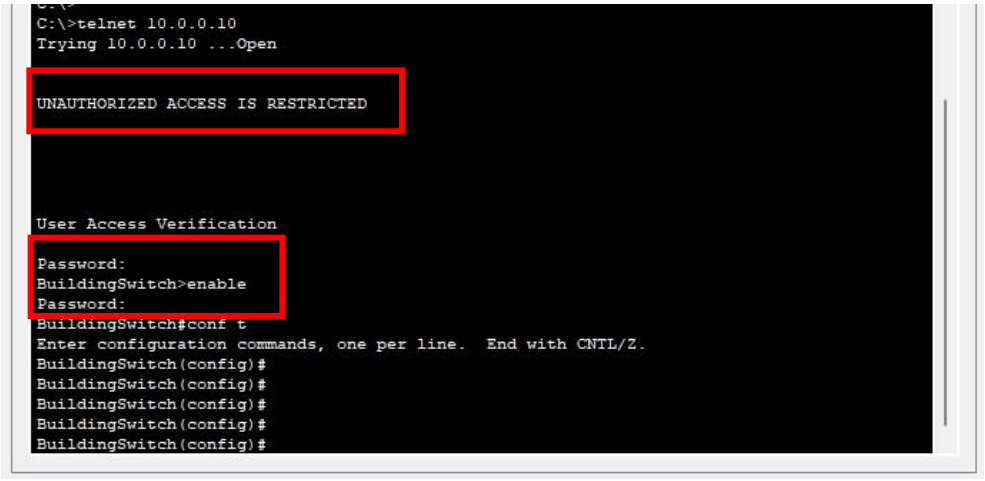


Figure 27: 2-factor authentication to access switch remotely

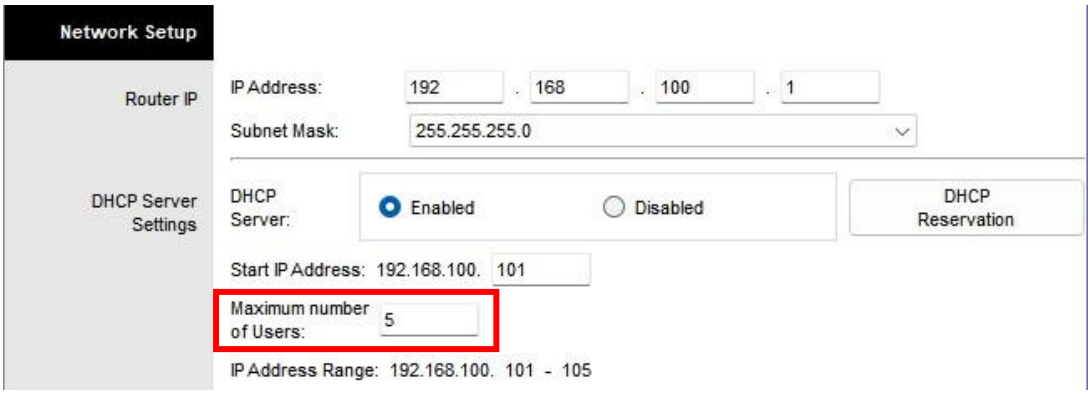


Figure 28: Configuring limited DHCP pool to reduce DDoS attack risks

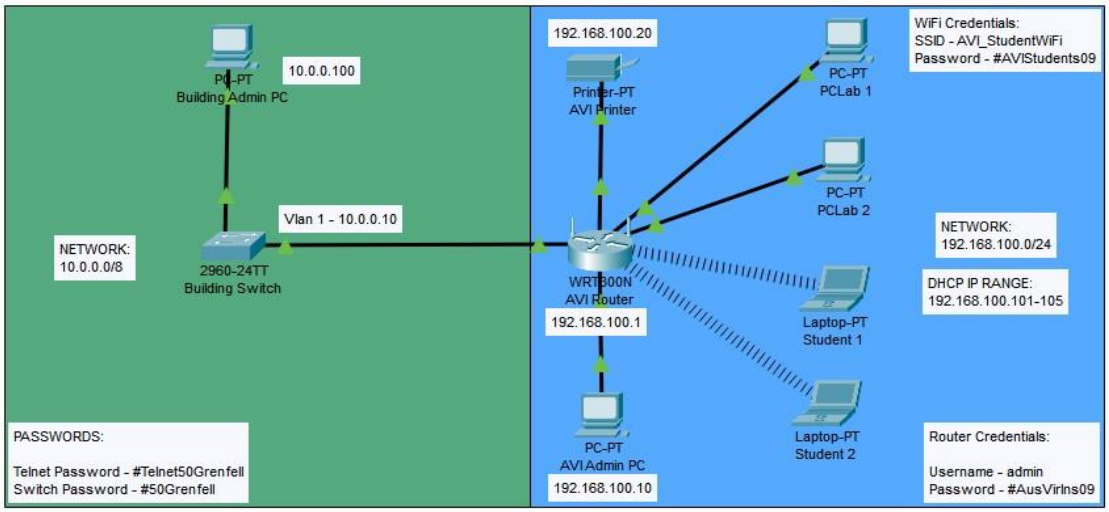


Figure 29: Dividing network into separate LANs

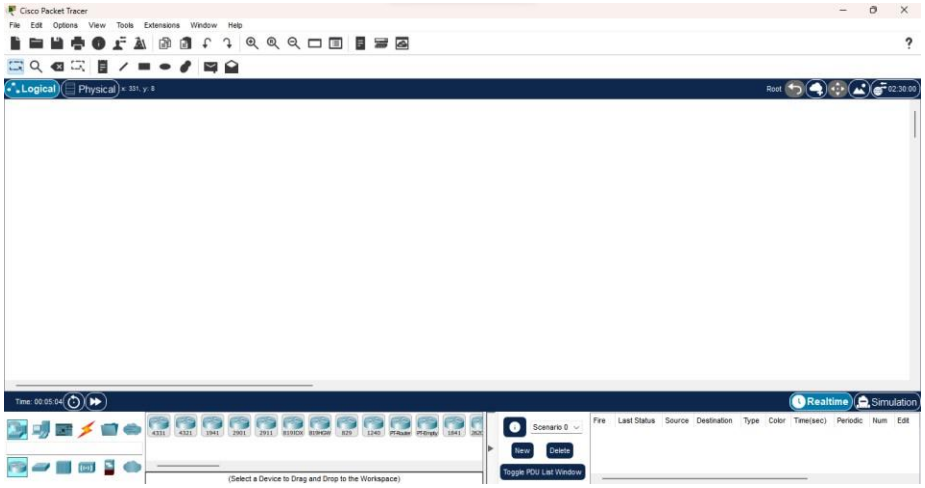


Figure 30: Cisco packet tracer

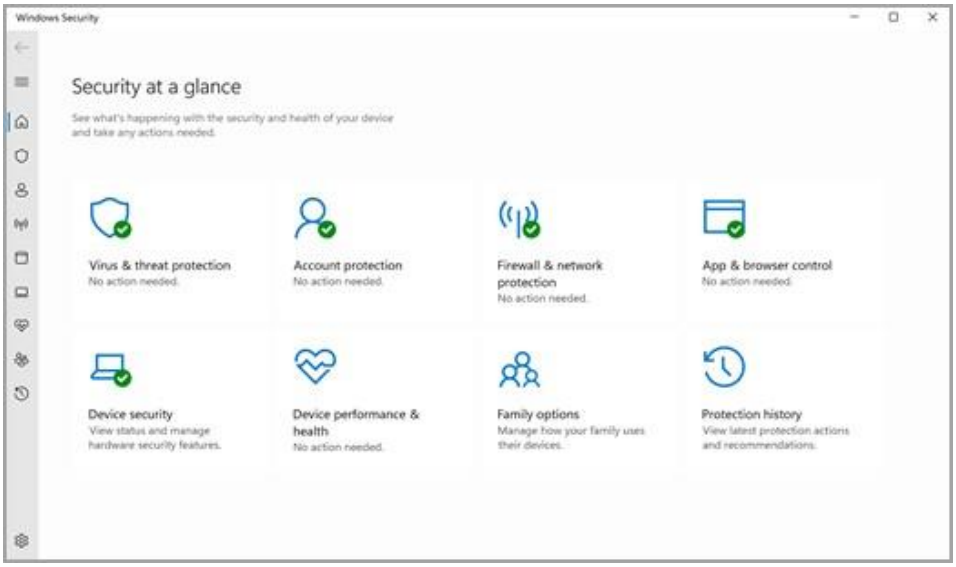


Figure 31: Windows defender and windows firewall

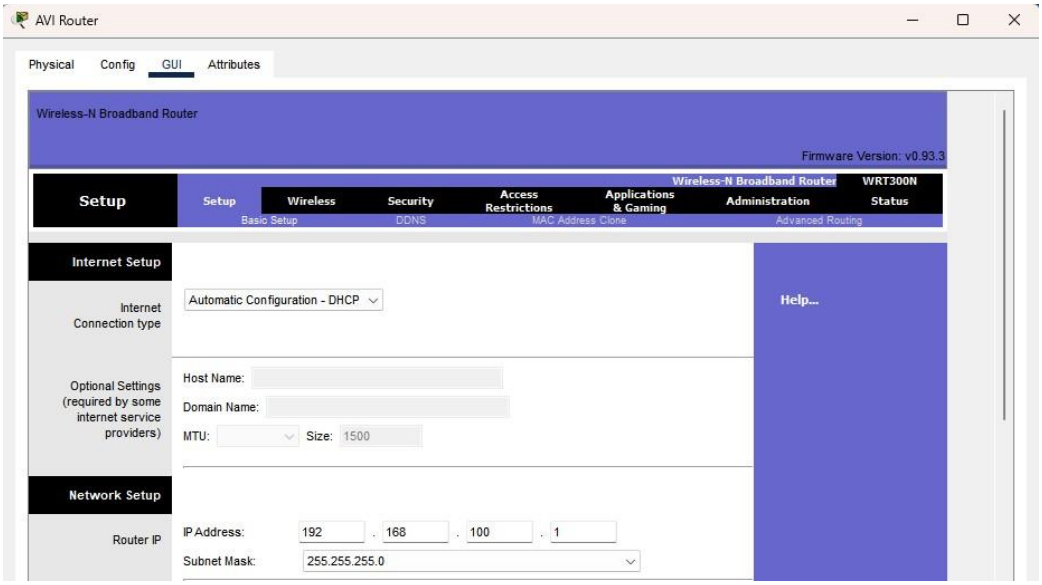


Figure 32: Wireless router and GUI

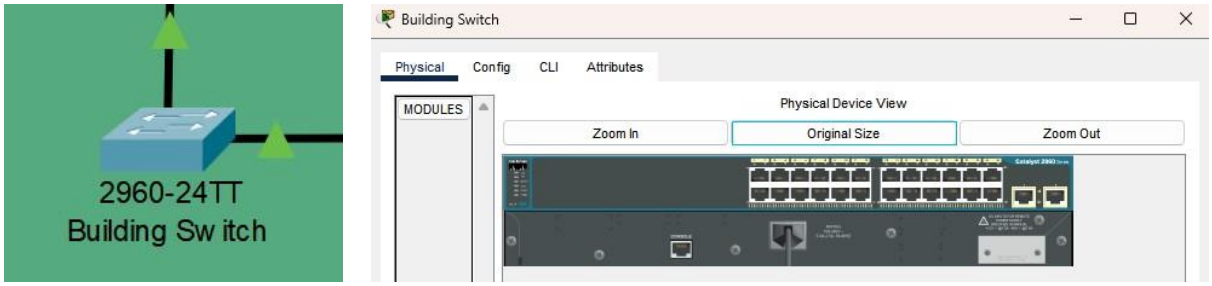


Figure 33: Switch – Cisco 296024TT

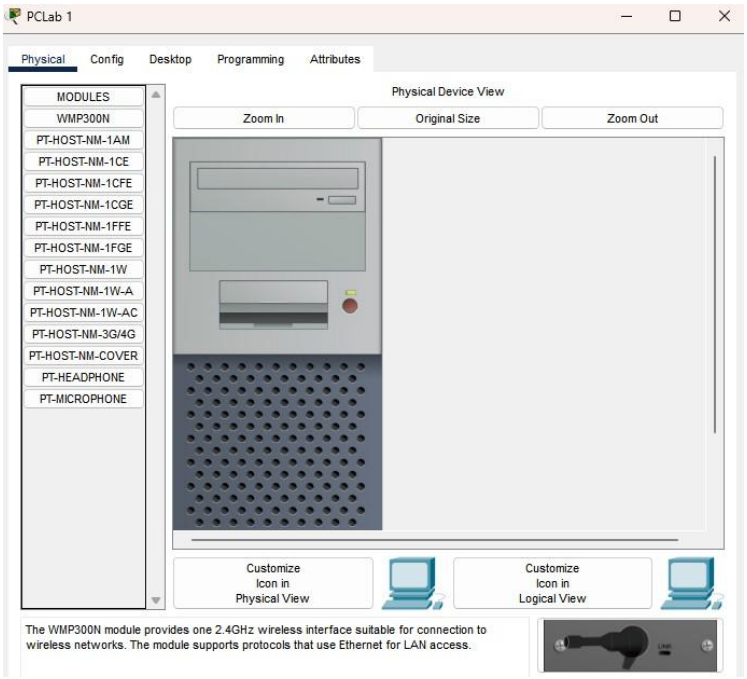


Figure 34: PC-PT

Figure 35: Laptop-PT

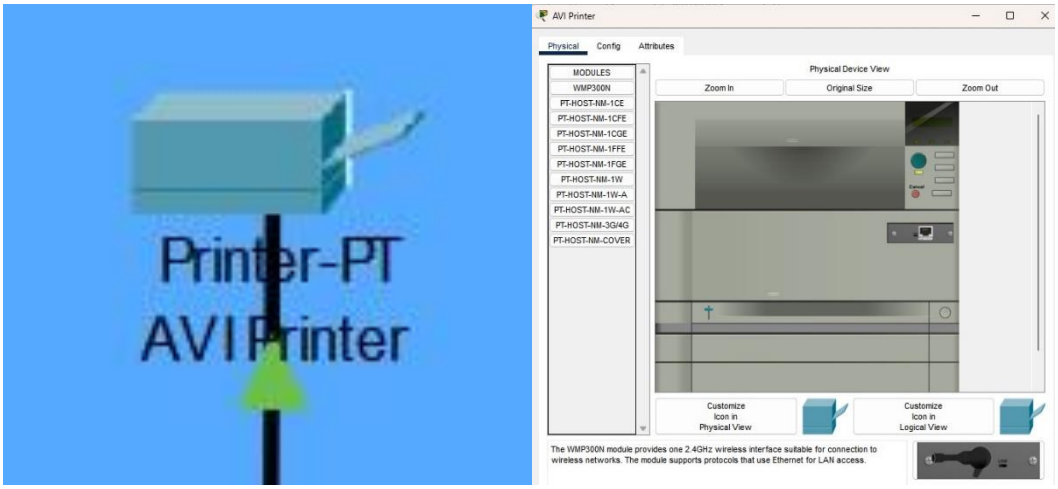


Figure 36: Printer-PT

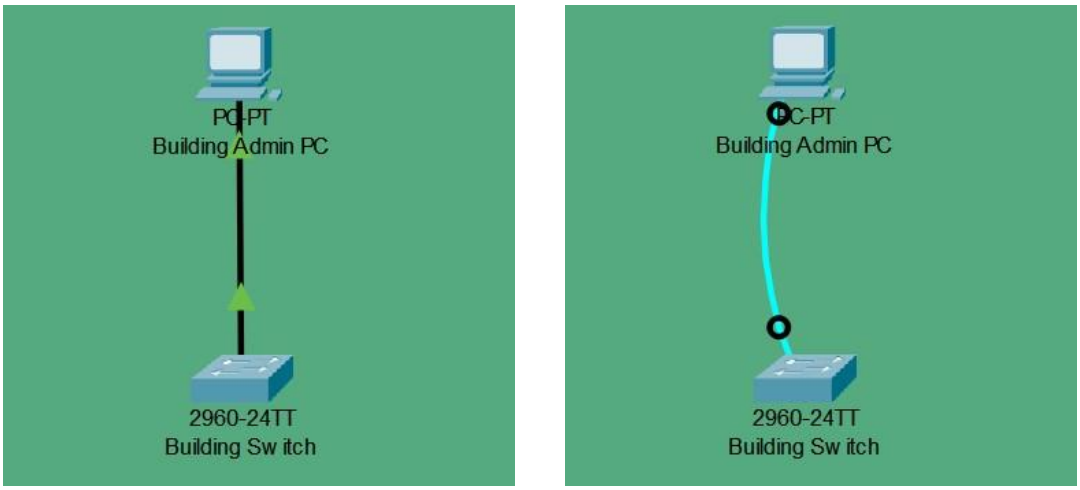


Figure 37: UTP copper straight; through cable and console cable

Testing & Finalization of Cybersecurity Operations:

CE 3.11 In the final part of my task, I tested the processes of the implemented cybersecurity controls to check their effectiveness and alignment with the network security needs of the simulated telecom environment. I conducted connectivity testing using ICMP ping commands to check communication paths between end devices, routers and switches. Through the ping test outcomes, I checked that devices within the same subnet could communicate successfully, while communication between various subnets remained restricted as per the configured segmentation policy. It confirmed that the subnetting structure and access restrictions were functioning correctly for network isolation and reducing the risks of lateral threat movement. I tested router administrative access controls by checking that only the designated admin workstation could access the router graphical configuration interface. All

other devices although reachable through basic connectivity testing, remained restricted from configuration access.

CE 3.12 I performed telnet access testing on the network switch and checked that only the authorized building admin PC could establish a remote management session. I checked that systems outside the permitted network segment were unable to reach the switch via ICMP/ established telnet sessions. It confirmed that the access control configuration was properly implemented. On the basis of these outcomes, I then introduced network enhancement to increase operational stability. I assigned static IP addresses to critical admin systems and printers for stable connectivity and management reliability, while configuring DHCP pools for student laboratory devices and wireless users to support flexible and controlled IP allocation. It enhanced the efficiency of address management and supported telecom network planning. Following this, I updated the cybersecurity operations to enhance the network against previously identified incidents; malware infection, credential leakage, worm propagation and DDoS threats. I implemented authentication and encryption mechanisms across wireless access, router administration and switch remote access by configuring secure passwords and restricting unauthorized administrative access. I limited Telnet access lines to reduce simultaneous remote session exposure. I blocked DHCP assigned client devices from accessing the router management interface to enhance administrative security. I enabled automatic operating system updates and scheduled weekly antivirus scanning using Windows defender for endpoint protection and vulnerability management. I reviewed firewall configuration periodically and maintained network segmentation to separate operational traffic based on user roles and functions. At the end, I reviewed the complete security orchestration, automation and response strategy and documented the final cybersecurity framework. This testing and finalization process, enhanced my practical skills in network validation, security testing, access control verification and secure telecom network operation planning.

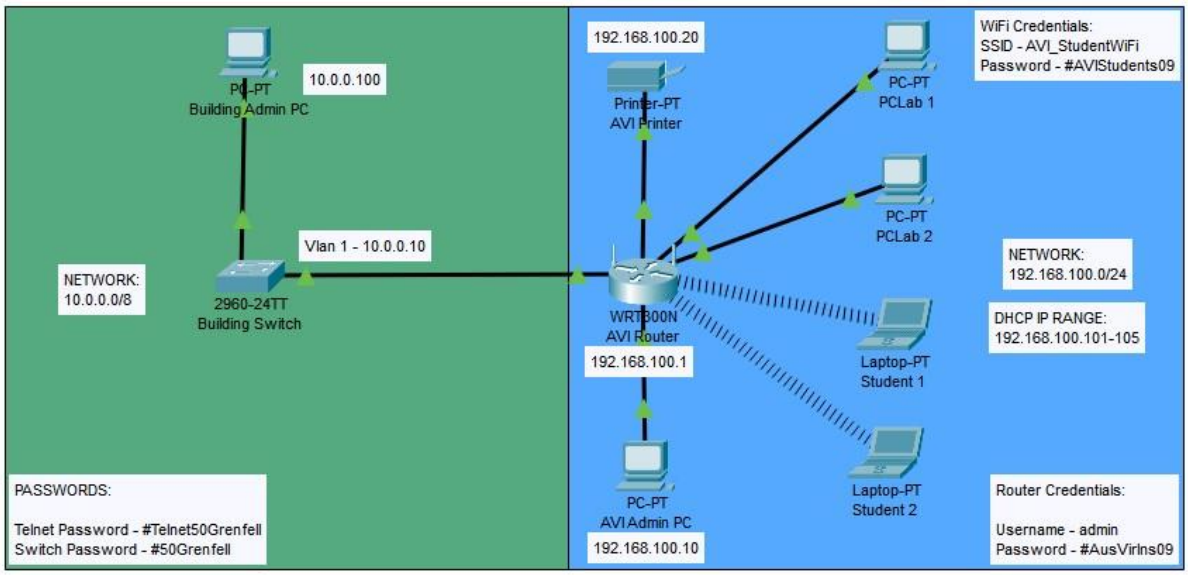


Figure 38: Network topology

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PCLab 1	PCLab 2	ICMP		0.000	N	0	(edit)
	Successful	PCLab 1	Student 1	ICMP		0.000	N	1	(edit)
	Successful	PCLab 1	Student 2	ICMP		0.000	N	2	(edit)
	Successful	PCLab 1	AVI Admin PC	ICMP		0.000	N	3	(edit)
	Successful	PCLab 1	AVI Printer	ICMP		0.000	N	4	(edit)
	Successful	PCLab 1	AVI Router	ICMP		0.000	N	5	(edit)
	Failed	PCLab 1	Building Admin PC	ICMP		0.000	N	6	(edit)
	Failed	PCLab 1	Building Switch	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PCLab 2	PCLab 1	ICMP		0.000	N	0	(edit)
	Successful	PCLab 2	Student 1	ICMP		0.000	N	1	(edit)
	Successful	PCLab 2	Student 2	ICMP		0.000	N	2	(edit)
	Successful	PCLab 2	AVI Admin PC	ICMP		0.000	N	3	(edit)
	Successful	PCLab 2	AVI Printer	ICMP		0.000	N	4	(edit)
	Successful	PCLab 2	AVI Router	ICMP		0.000	N	5	(edit)
	Failed	PCLab 2	Building Admin PC	ICMP		0.000	N	6	(edit)
	Failed	PCLab 2	Building Switch	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Student 1	PCLab 1	ICMP		0.000	N	0	(edit)
	Successful	Student 1	PCLab 2	ICMP		0.000	N	1	(edit)
	Successful	Student 1	Student 2	ICMP		0.000	N	2	(edit)
	Successful	Student 1	AVI Admin PC	ICMP		0.000	N	3	(edit)
	Successful	Student 1	AVI Printer	ICMP		0.000	N	4	(edit)
	Successful	Student 1	AVI Router	ICMP		0.000	N	5	(edit)
	Failed	Student 1	Building Admin PC	ICMP		0.000	N	6	(edit)
	Failed	Student 1	Building Switch	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Student 2	PCLab 1	ICMP		0.000	N	0	(edit)
	Successful	Student 2	PCLab 2	ICMP		0.000	N	1	(edit)
	Successful	Student 2	Student 1	ICMP		0.000	N	2	(edit)
	Successful	Student 2	AVI Admin PC	ICMP		0.000	N	3	(edit)
	Successful	Student 2	AVI Printer	ICMP		0.000	N	4	(edit)
	Successful	Student 2	AVI Router	ICMP		0.000	N	5	(edit)
	Failed	Student 2	Building Admin PC	ICMP		0.000	N	6	(edit)
	Failed	Student 2	Building Switch	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	AVI Admin PC	PCLab 1	ICMP		0.000	N	0	(edit)
	Successful	AVI Admin PC	PCLab 2	ICMP		0.000	N	1	(edit)
	Successful	AVI Admin PC	Student 1	ICMP		0.000	N	2	(edit)
	Successful	AVI Admin PC	Student 2	ICMP		0.000	N	3	(edit)
	Successful	AVI Admin PC	AVI Printer	ICMP		0.000	N	4	(edit)
	Successful	AVI Admin PC	AVI Router	ICMP		0.000	N	5	(edit)
	Failed	AVI Admin PC	Building Admin PC	ICMP		0.000	N	6	(edit)
	Failed	AVI Admin PC	Building Switch	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Building Admin PC	Building Switch	ICMP		0.000	N	0	(edit)
	Failed	Building Admin PC	AVI Router	ICMP		0.000	N	1	(edit)
	Failed	Building Admin PC	PCLab 1	ICMP		0.000	N	2	(edit)
	Failed	Building Admin PC	PCLab 2	ICMP		0.000	N	3	(edit)
	Failed	Building Admin PC	Student 1	ICMP		0.000	N	4	(edit)
	Failed	Building Admin PC	Student 2	ICMP		0.000	N	5	(edit)
	Failed	Building Admin PC	AVI Admin PC	ICMP		0.000	N	6	(edit)
	Failed	Building Admin PC	AVI Printer	ICMP		0.000	N	7	(edit)

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Building Admin PC	Building Switch	ICMP		0.000	N	0	(edit)
	Failed	Building Admin PC	AVI Router	ICMP		0.000	N	1	(edit)
	Failed	Building Admin PC	PCLab 1	ICMP		0.000	N	2	(edit)
	Failed	Building Admin PC	PCLab 2	ICMP		0.000	N	3	(edit)
	Failed	Building Admin PC	Student 1	ICMP		0.000	N	4	(edit)
	Failed	Building Admin PC	Student 2	ICMP		0.000	N	5	(edit)
	Failed	Building Admin PC	AVI Admin PC	ICMP		0.000	N	6	(edit)
	Failed	Building Admin PC	AVI Printer	ICMP		0.000	N	7	(edit)

Figure 39: Ping results

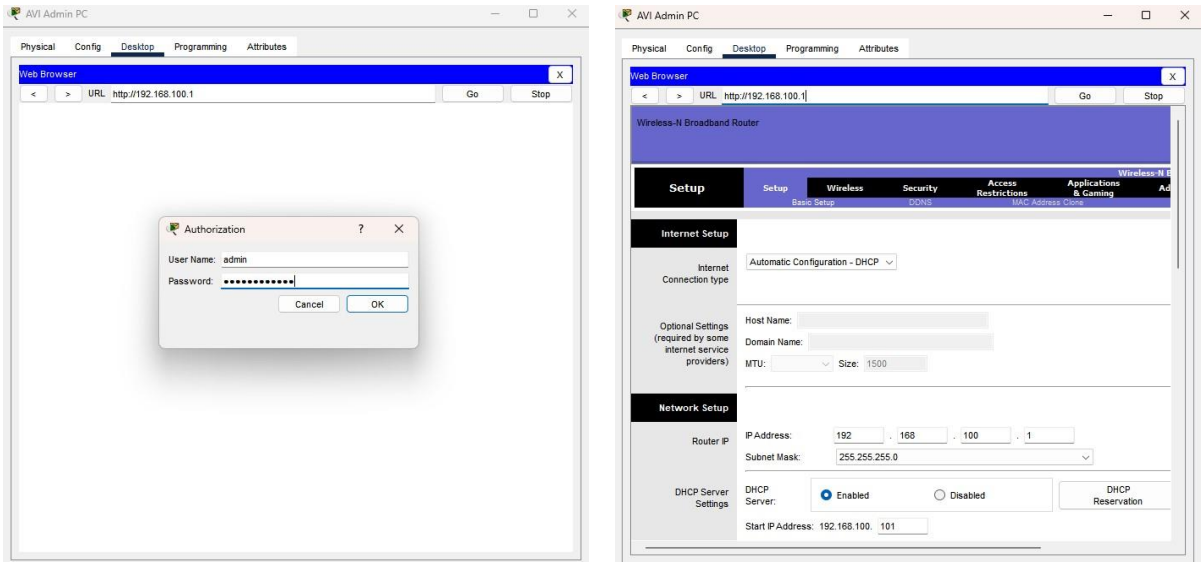


Figure 40: AVI admin PC-AVI router GUI configuration page test

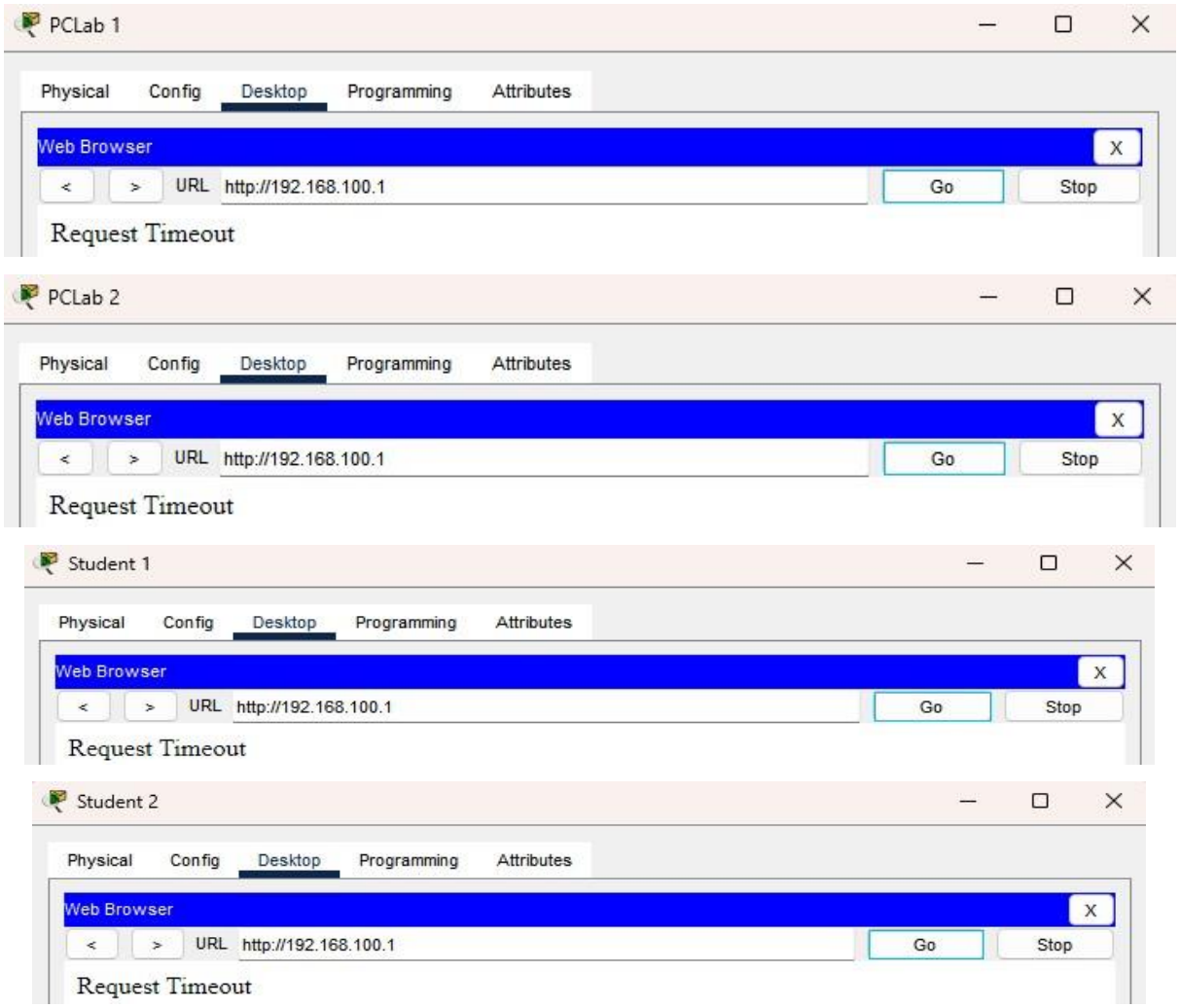


Figure 41: 192.168.100.0/24 devices-AVI router GUI configurations page test

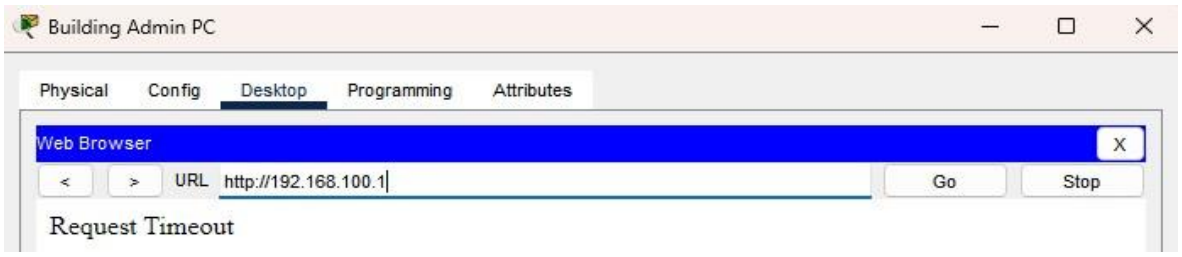


Figure 42: Building admin PC-AVI router GUI configuration page test

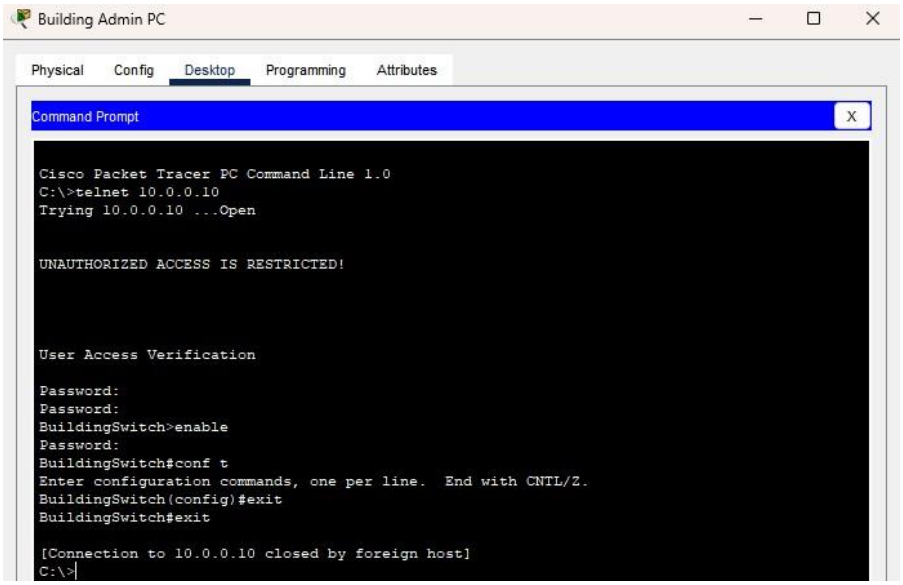


Figure 43: Building admin PC telnet test

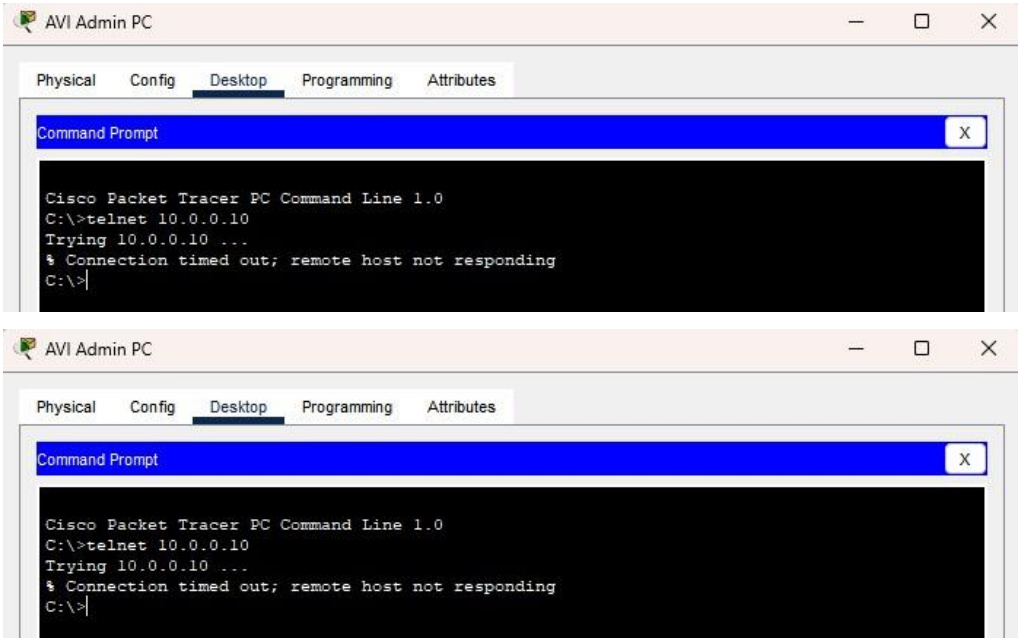
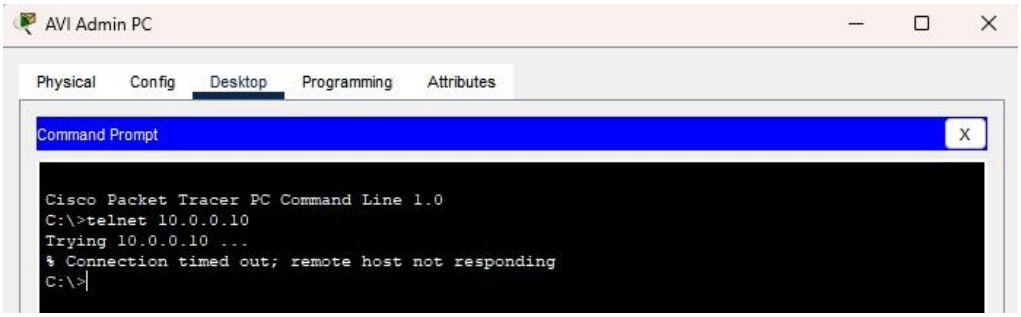


Figure 44: 192.168.100.0/24 Device Telnet Test



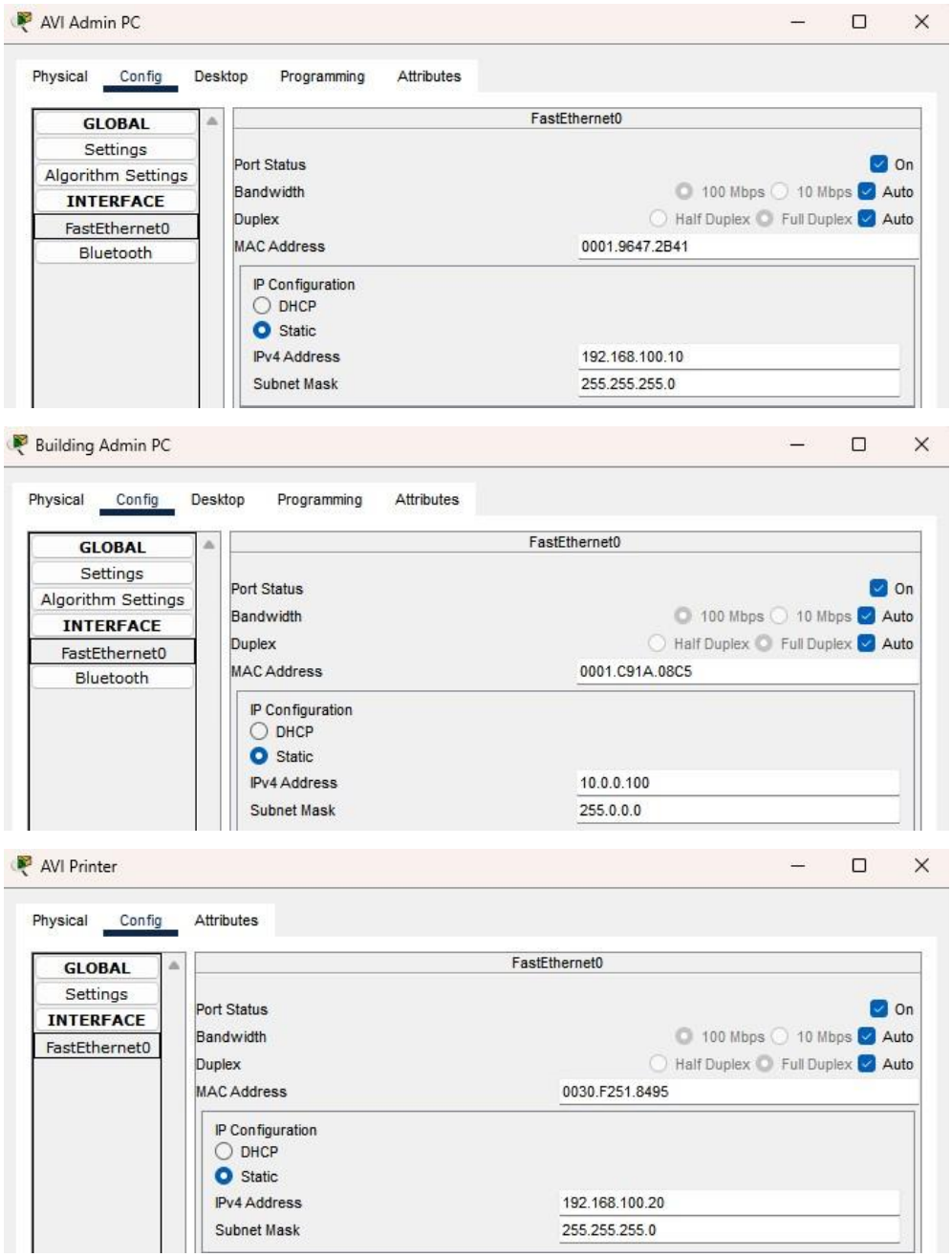


Figure 45: Assigning static IP addresses to admin PCs and network devices

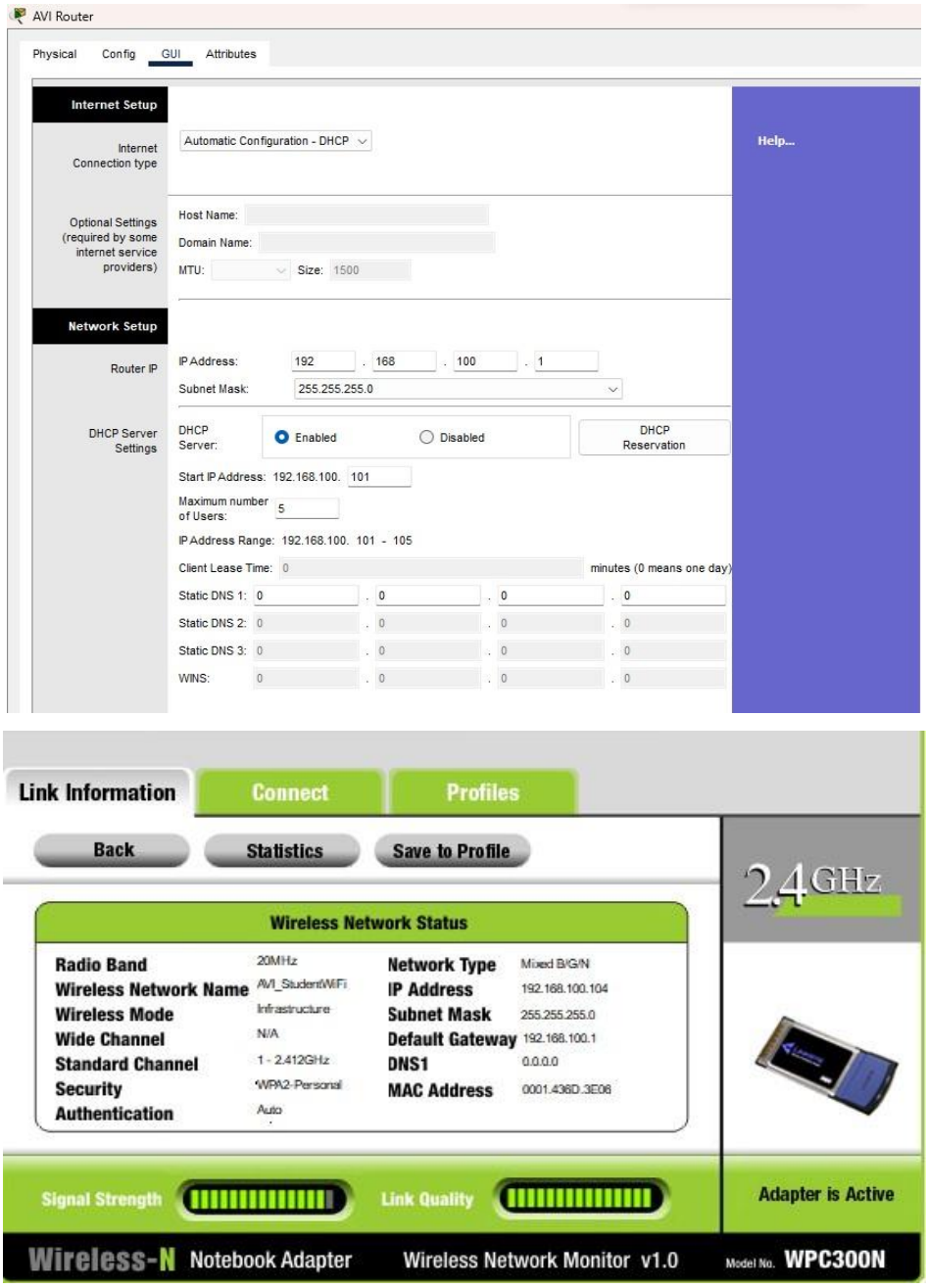


Figure 46: Creating DHCOP pool for end devices

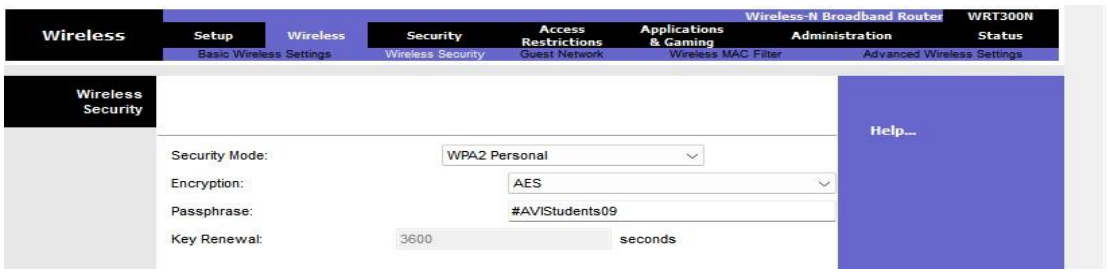


Figure 47: Student Wi-Fi

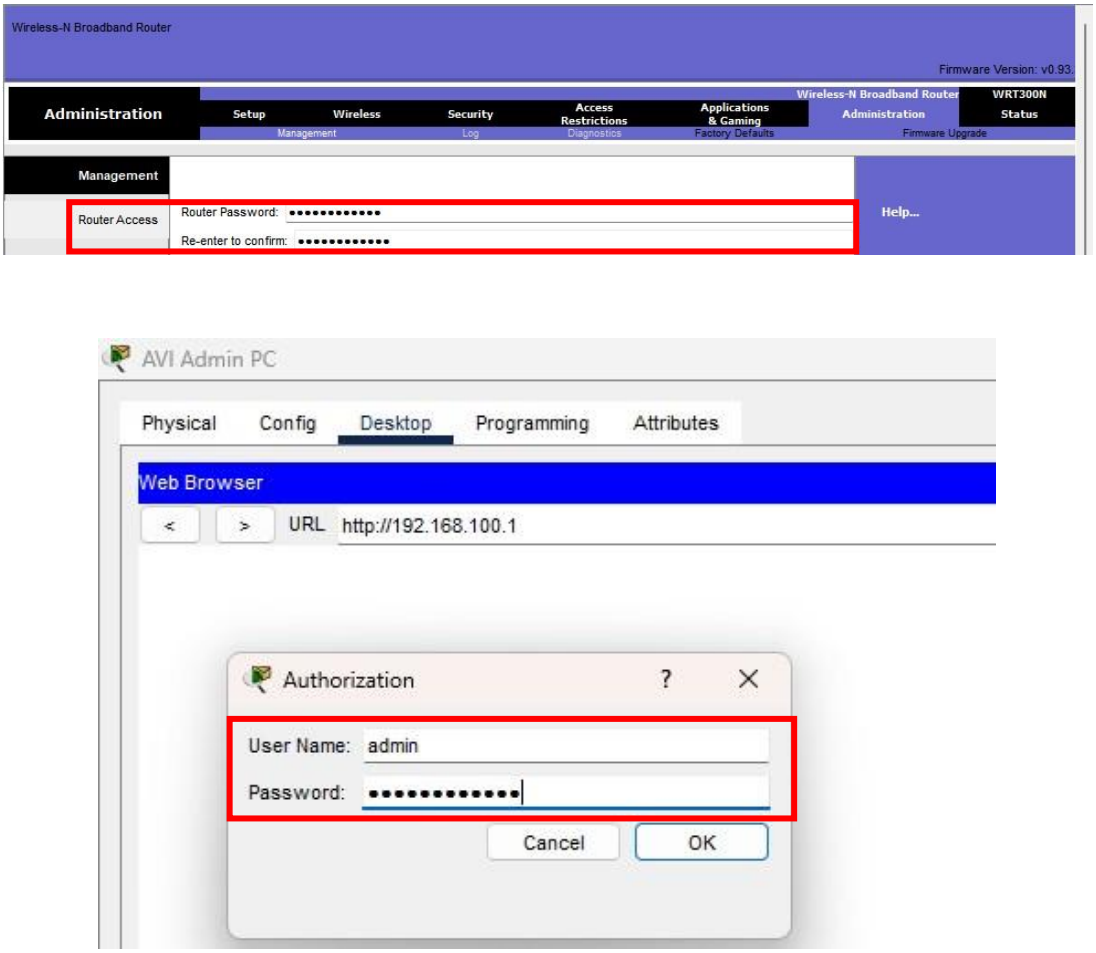


Figure 48: AVI router GUI configuration page

```
Switch(config)#
Switch(config)#hostname BuildingSwitch
BuildingSwitch(config)#enable secret #50Grenfell
BuildingSwitch(config)#banner motd ^
Enter TEXT message.  End with the character '^'.

UNAUTHORIZED ACCESS IS RESTRICTED!

^

BuildingSwitch(config)#
```

```
BuildingSwitch#
BuildingSwitch#show run
BuildingSwitch#show running-config
Building configuration...

Current configuration : 1226 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BuildingSwitch
!
enable secret 5 $1$mERr$DJgXvMvHZ27VWxeIw8mA00
!
```

Figure 49: Building switch

```
BuildingSwitch(config)#
BuildingSwitch(config)#line vty 0 4
BuildingSwitch(config-line)#password #Telnet50Grenfell
BuildingSwitch(config-line)#login
BuildingSwitch(config-line)#exit
BuildingSwitch(config)#
```

Figure 50: Telnet to building switch

```
BuildingSwitch(config)#
BuildingSwitch(config)#line vty 0 4
BuildingSwitch(config-line)#password #Telnet50Grenfell
BuildingSwitch(config-line)#login
BuildingSwitch(config-line)#exit
BuildingSwitch(config)#
```

Figure 51: Telnet lines

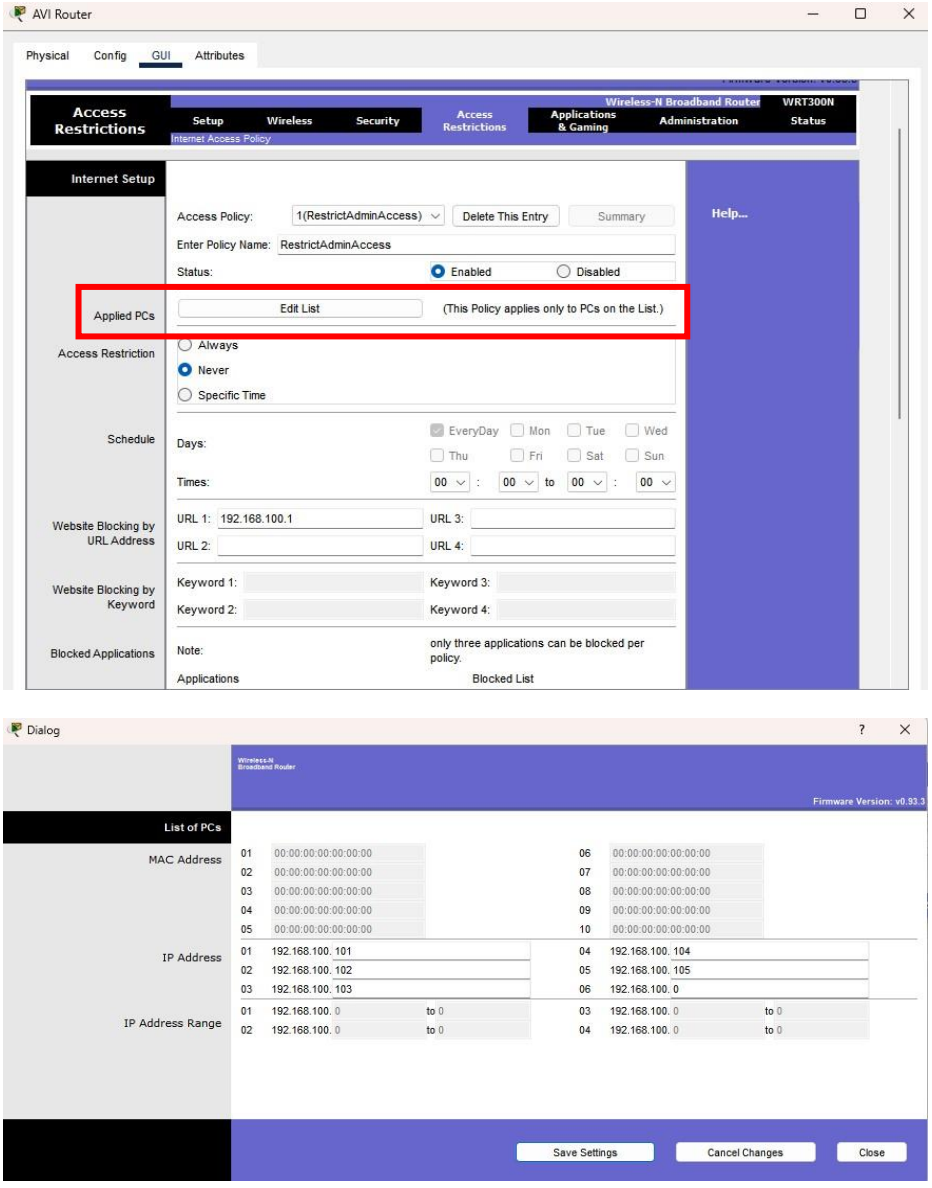


Figure 52: AVI router GUI configuration page restriction

Figure 53: Automatic windows updates

Challenges Faced & Project Management:

CE 3.13 I faced several issues and challenges while configuring the simulated network environment as well as implementing cybersecurity controls. At first, I faced difficulties in designing the subnet structure, configuring firewall rules correctly and restricting admin access without affecting normal network communication. I also faced challenges in analyzing threat scenarios; malware spread and DDoS behavior in the network simulation. To handle these, I reviewed the assessments needs, consulted technical resources and discussed implementation steps with my professor to check the configuration approach. I worked with my fellow student in the lab environment to complete the tasks. I had discussions with them to share observations and troubleshoot configuration errors. I divided the tasks into planning, implementation, testing and documentation stages, that helped me complete the tasks within the timelines while enhancing the accuracy of the final cybersecurity operations strategy.

SUMMARY

CE 3.14 As part of my diploma assessment, I simulated organizational case study where I evaluated, implemented, tested and finalized cybersecurity measures to enhance telecom network against threats. I analyzed the existing security operations of organization; log management, threat detection and monitoring. I identified operational weaknesses and documented required enhancements; firewall policy updates, vulnerability patching and system upgrades. Using Cisco packet tracer, I designed and configured a segmented network topology, implemented firewall controls, DHCP allocations, static IP configuration, secure administrative access, wireless security and endpoint protection measures; antivirus scanning and authentication controls. I tested network connectivity, access restrictions and remote management security via ping and Telnet tests, reviewed the effectiveness of implemented controls and updated the Cybersecurity strategy using security orchestration, automation and response principles to enhance incident response, network reliability and security. This assessment enhanced my skills in secure telecom network planning, cyber threat mitigation, access control implementation and security management.