Nottingham Trent University

Department Of Computer Science

COMP40461 - Coursework April 2025

Network and Cloud Security

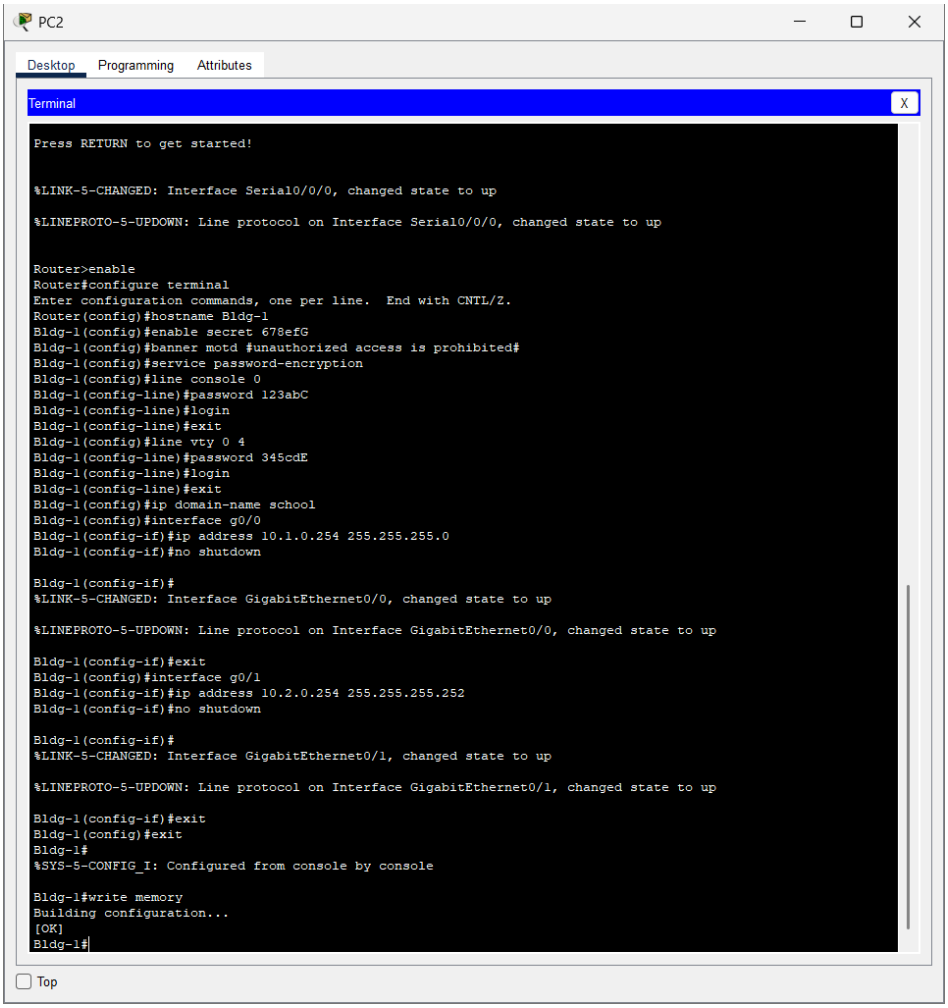
By

Karunakar Reddy Machupalli – N1334679

Task 1 - Network Design

Section A: Implementation Steps

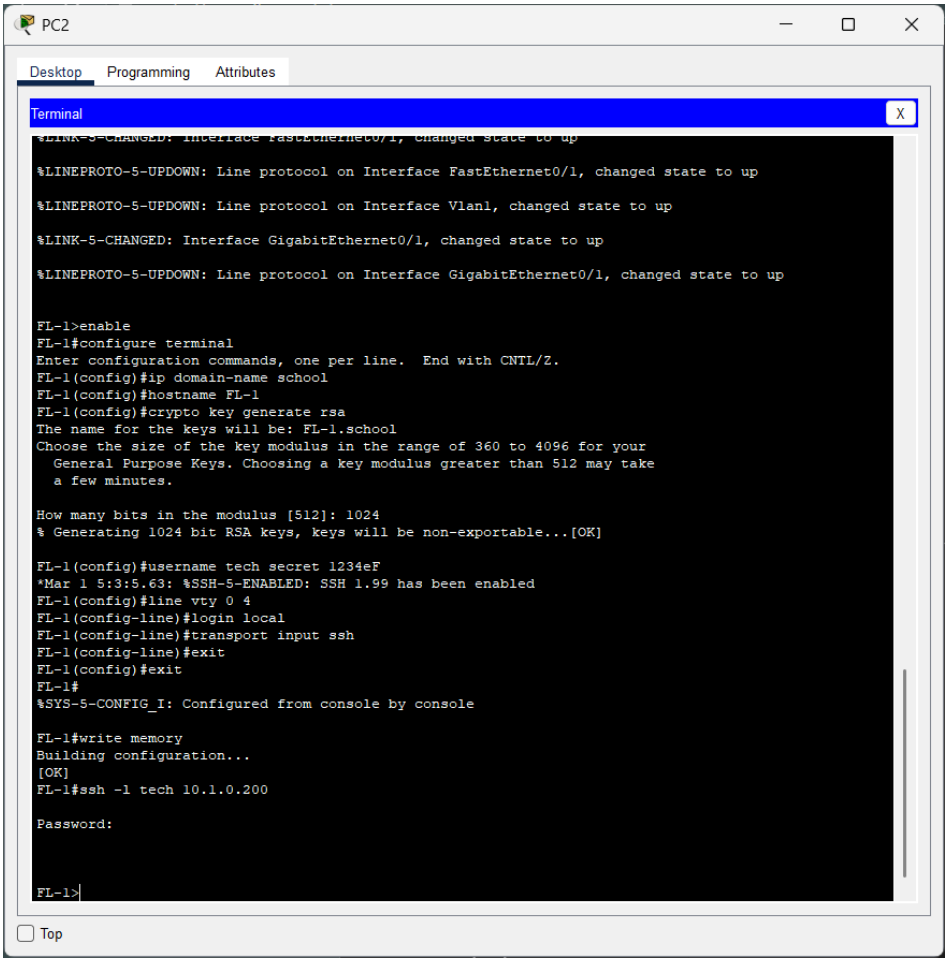
Basic Router Configuration (Bldg-1) & LAN Interface Configuration



To configure the Bldg-1 router, the session began in user EXEC mode and was elevated to privileged EXEC mode using the `enable` command. Configuration mode was accessed via `configure terminal`. The router

hostname was set with `hostname Bldg-1`, and the enable secret password was configured as `enable secret 678efG`. A message-of-the-day banner was added using `banner motd #unauthorized access is prohibited#`, and password encryption was enabled with `service password-encryption`. Console access was secured by entering `line console 0`, setting the password to `123abC`, enabling login with `login`, and exiting the line configuration. Virtual terminal lines were configured using `line vty 0 4`, with the password `345cdE` and login enabled. The domain name was set to `school` using `ip domain-name school`. The LAN interfaces were then configured: `interface g0/0` was assigned IP address `10.1.0.254 255.255.255.0` and activated with `no shutdown`, followed by `interface g0/1` with IP `10.2.0.254 255.255.255.252` and activated. After exiting interface configuration, the configuration was saved using `write memory`.

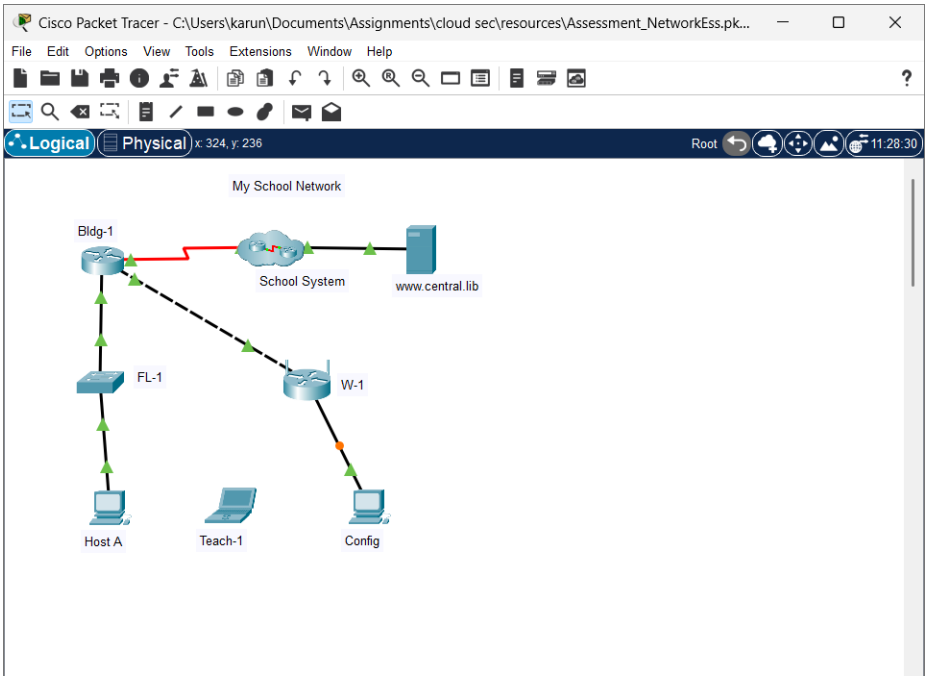
FL-1 Switch Remote Management & SSH Configuration on FL-1



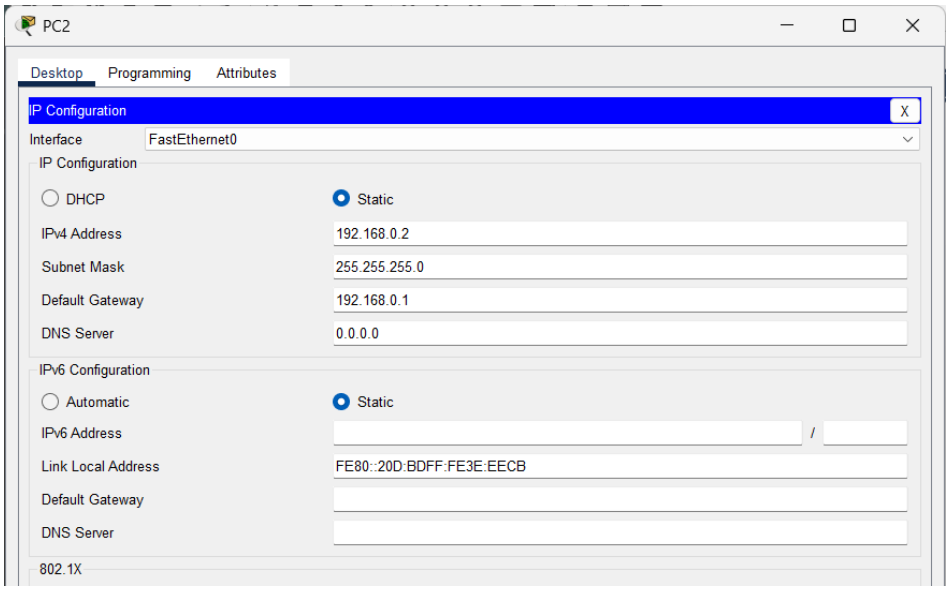
To configure the FL-1 switch for remote management and secure access, the session was initiated in privileged EXEC mode using `enable`, followed by entering global configuration mode with `configure`

`terminal`. The domain name was set using `ip domain-name school`, and the hostname was assigned as `FL-1`. RSA encryption keys were generated with `crypto key generate rsa`, specifying a 1024-bit modulus, which enabled SSH version 1.99. A local user account was created using `username tech secret 1234eF` for secure authentication. The virtual terminal lines were configured via `line vty 0 4`, enabling local login with `login local` and restricting remote access to SSH only using `transport input ssh`. For management interface setup, `interface vlan 1` was configured with IP address `10.1.0.200 255.255.255.0` and activated using `no shutdown`. The default gateway was set to `10.1.0.254` using `ip default-gateway`. Finally, the configuration was saved with `write memory`, and SSH connectivity was verified by initiating an SSH session to the switch using `ssh -l tech 10.1.0.200`.

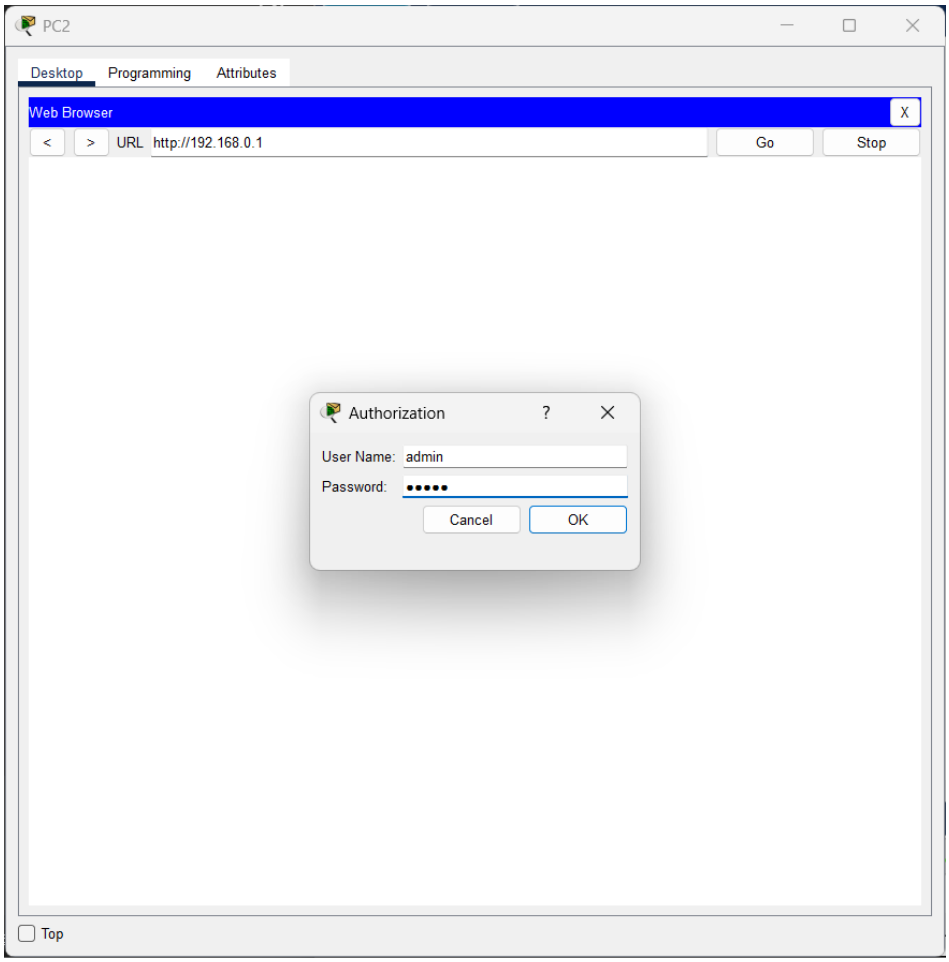
W-1 Wireless Device Configuration



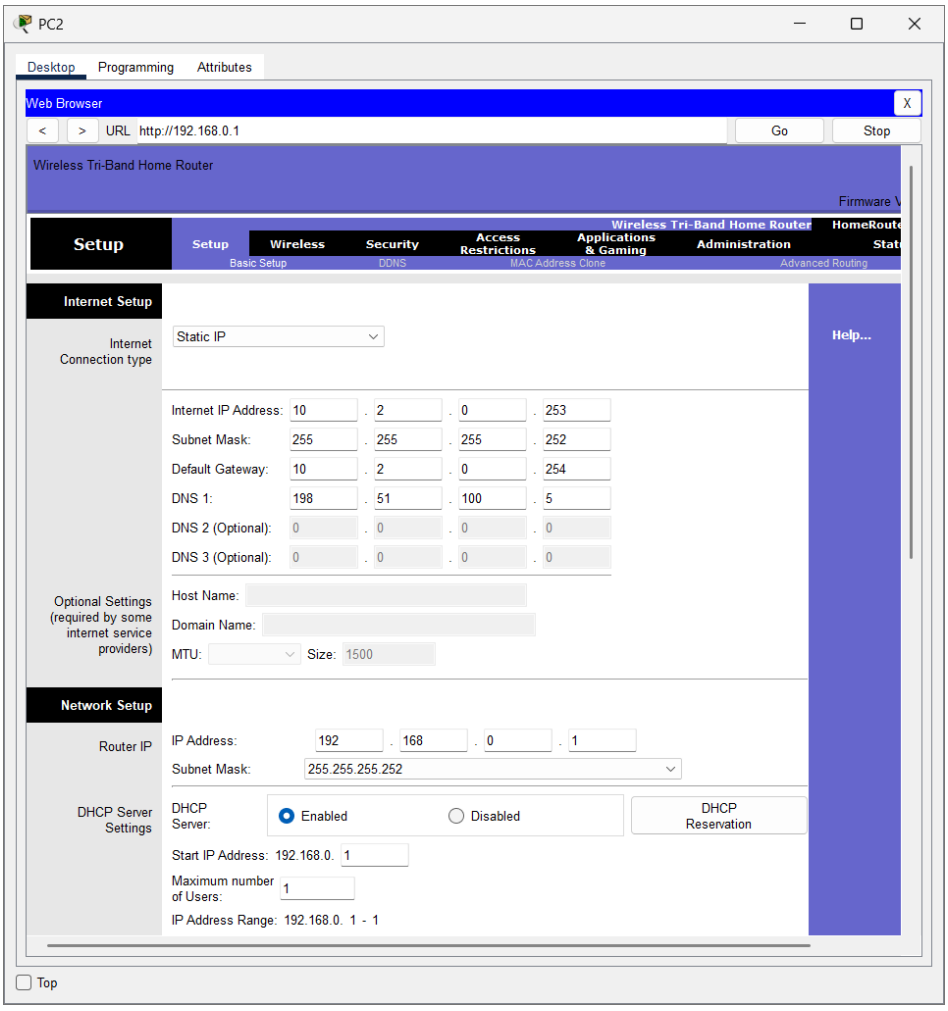
Karunakar Reddy Machupalli - N1334679



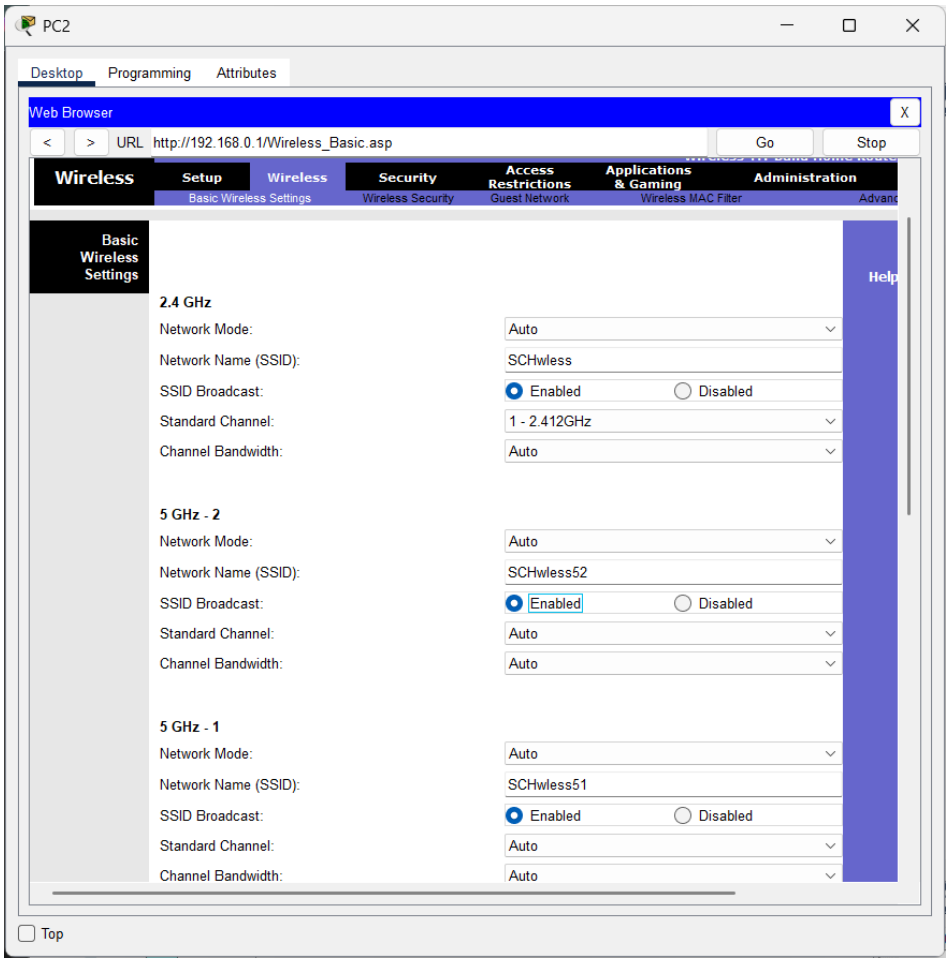
Karunakar Reddy Machupalli - N1334679

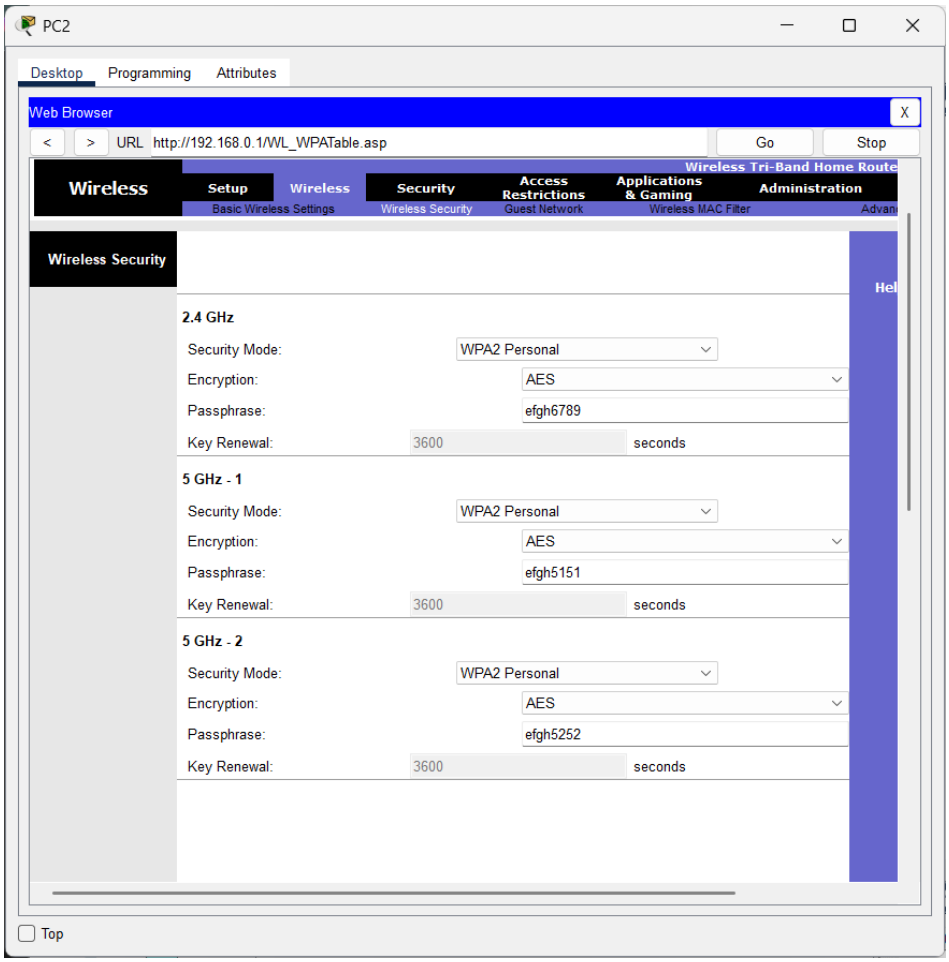


Karunakar Reddy Machupalli - N1334679



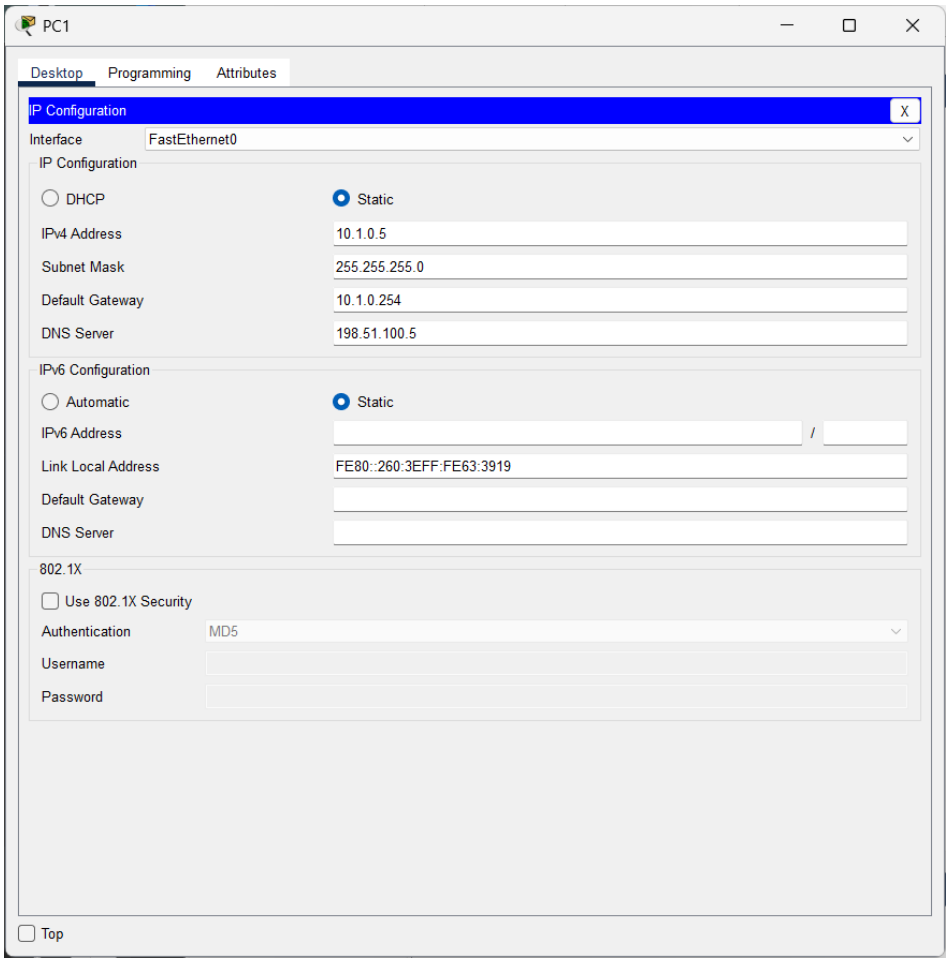
Karunakar Reddy Machupalli - N1334679

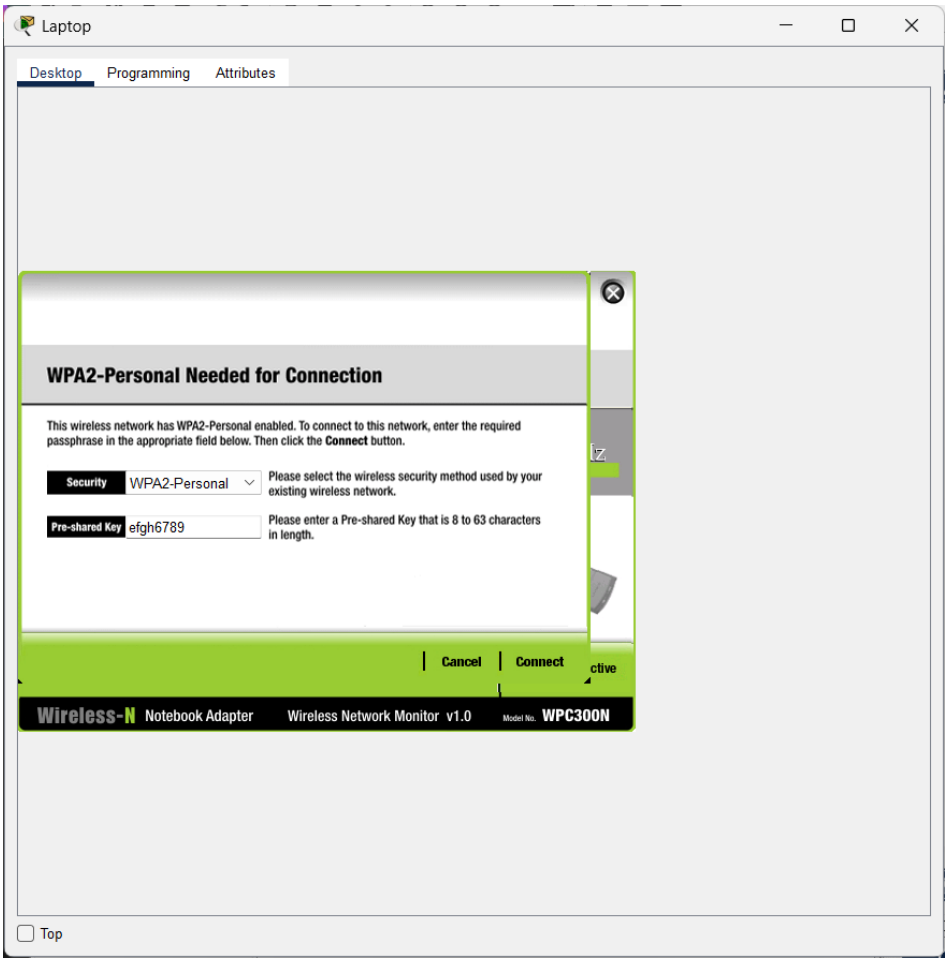




A host PC was connected to the W-1 wireless router via a console connection to perform the initial configuration. The PC was manually configured with a static IP address of `192.168.0.2`, a subnet mask of `255.255.255.0`, and a default gateway of `192.168.0.1`. The DNS server was left as `0.0.0.0`. Using this configuration, the router's web interface was accessed through a browser by navigating to `http://192.168.0.1`. The Internet interface was set to use a static IP configuration with the IP address `10.2.0.253`, subnet mask `255.255.255.252`, and default gateway `10.2.0.254`. The primary DNS server was configured as `198.51.100.5`. The router's internal IP was set to `192.168.0.1`, and DHCP was enabled with a start IP address of `192.168.0.1` and a maximum of 1 user. For wireless connectivity, three SSIDs were configured: `SCHwless` for 2.4 GHz, `SCHwless51` for 5 GHz-1, and `SCHwless52` for 5 GHz-2. All networks use WPA2 Personal Security with AES encryption. The passphrases were `efgh6789` for SCHwless, `efgh5151` for SCHwless51, and `efgh5252` for SCHwless52.

Host Configuration



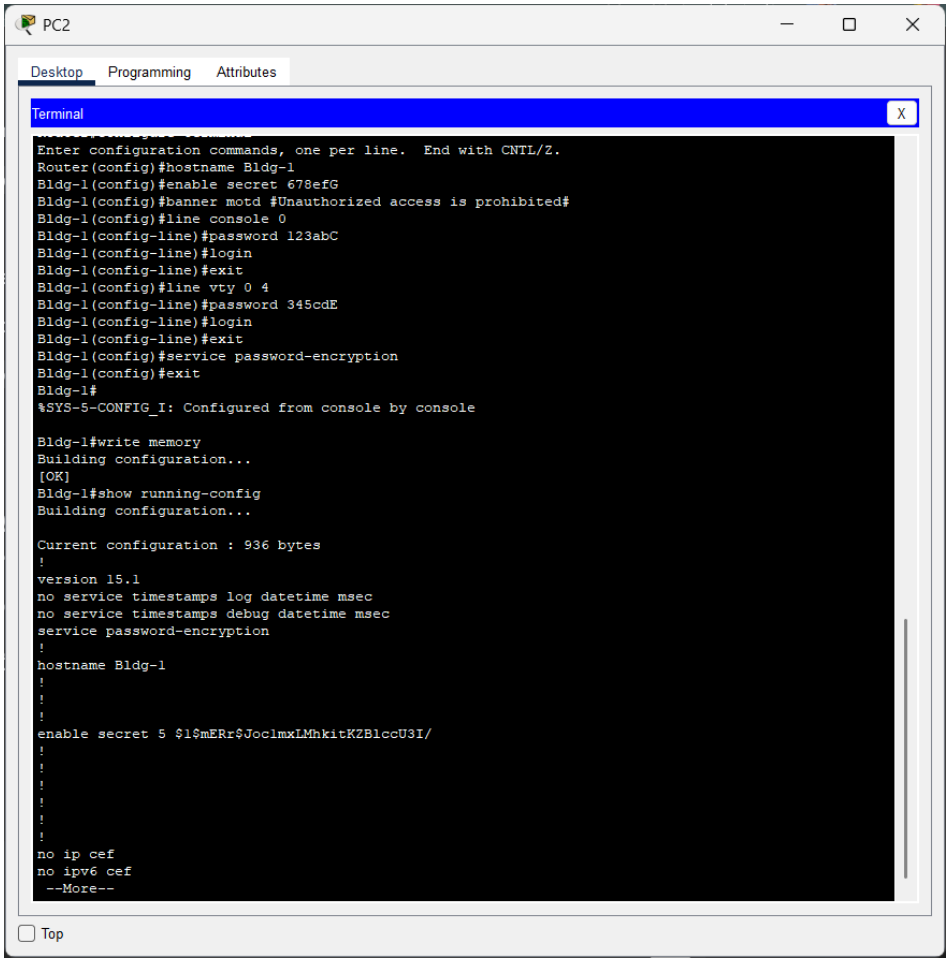


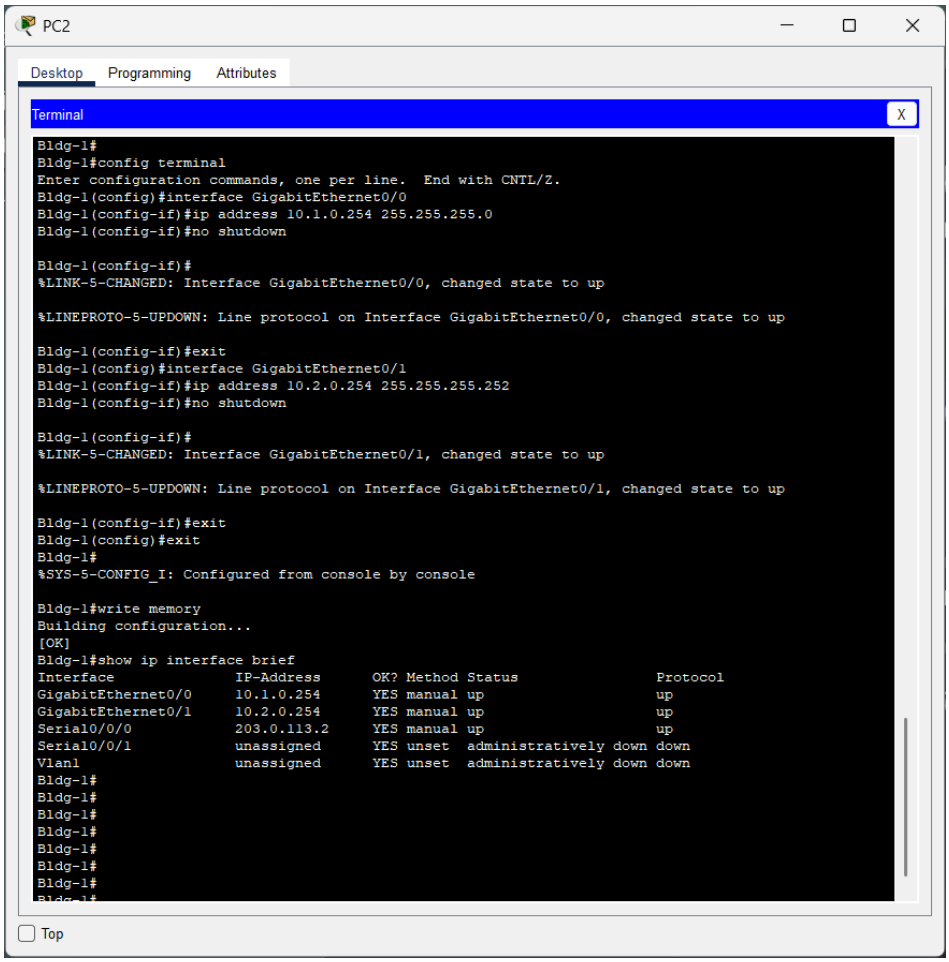
Host A was configured with a static IP address of `10.1.0.5`, a subnet mask of `255.255.255.0`, a default gateway of `10.1.0.254`, and a DNS server set to `198.51.100.5`. After configuring the network settings, the host successfully connected to the wireless network named **SCHwless**, which uses **WPA2-Personal** security. The connection was authenticated using the pre-shared key `efgh6789`, confirming successful wireless connectivity and access to the internal network and internet services.

Section B: Verification and Troubleshooting

Router (Bldg-1) Verification

Karunakar Reddy Machupalli - N1334679

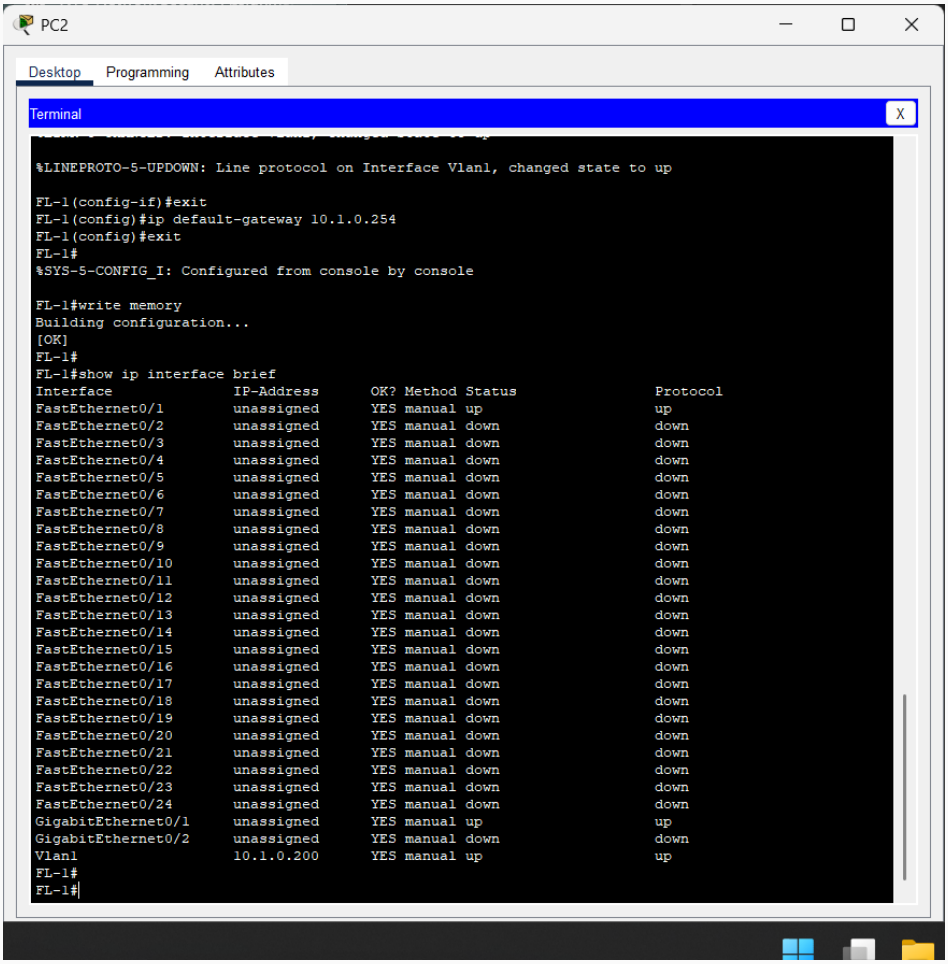


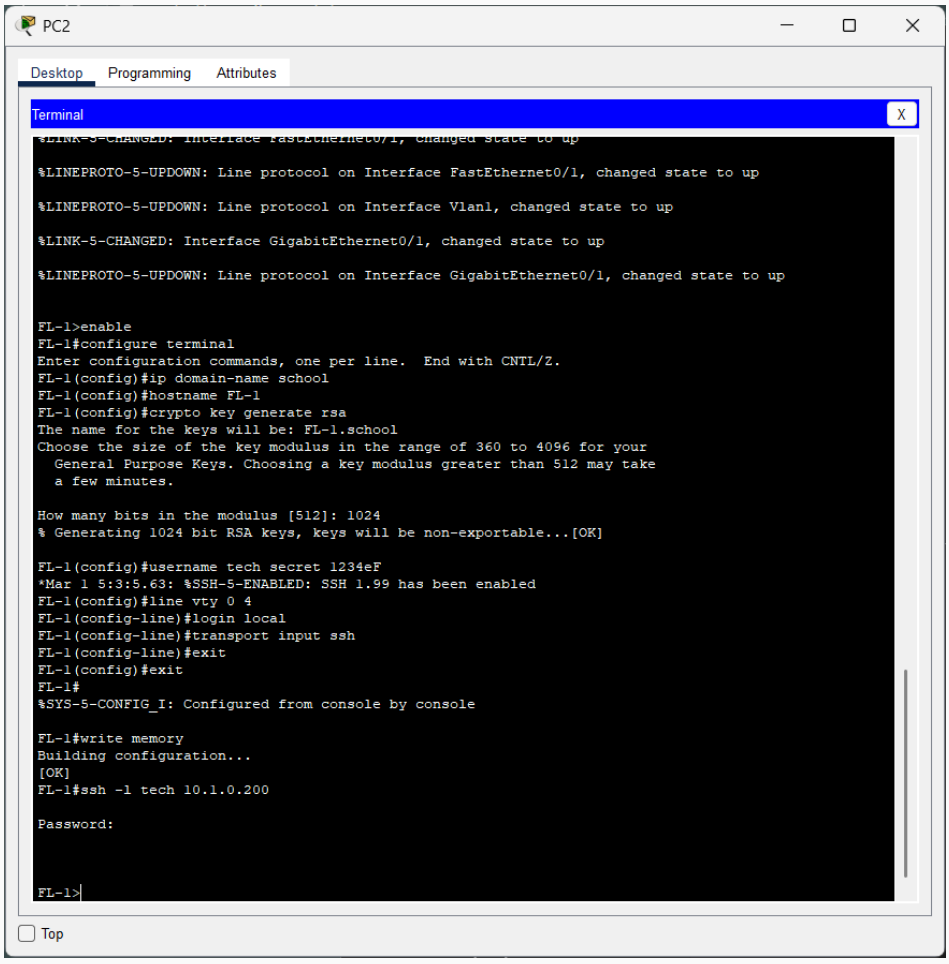


To verify the configuration of the Bldg-1 router, the `show running-config` command was used. The output confirmed that the hostname is correctly set to `Bldg-1`, the `enable secret` password is encrypted, and `service password-encryption` is enabled. The configuration also shows that both `CEF` and `IPv6 CEF` are disabled, which is acceptable for this setup. Next, the `show ip interface brief` command was executed to verify interface status. The output confirmed that both `GigabitEthernet0/0` and `GigabitEthernet0/1` are assigned the correct IP addresses (`10.1.0.254` and `10.2.0.254`, respectively), and both interfaces are in an **up/up** state, indicating they are active and functioning properly.

Switch (FL-1) Verification

Karunakar Reddy Machupalli - N1334679

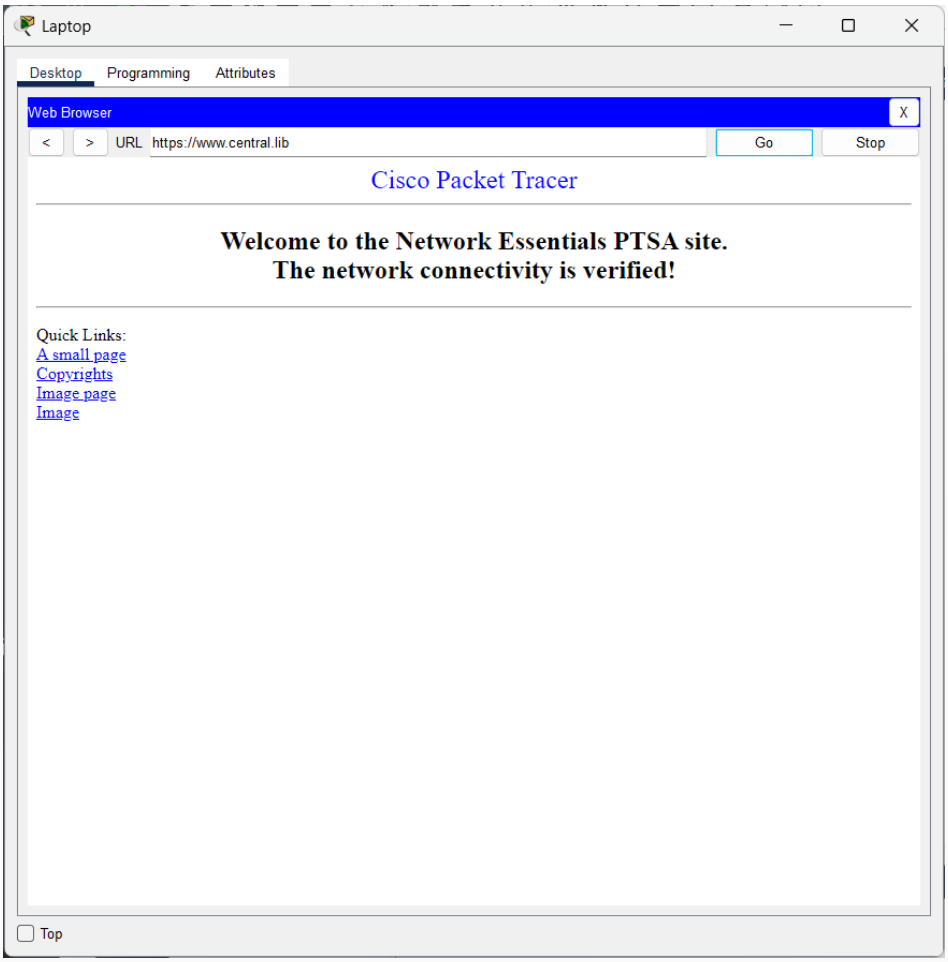


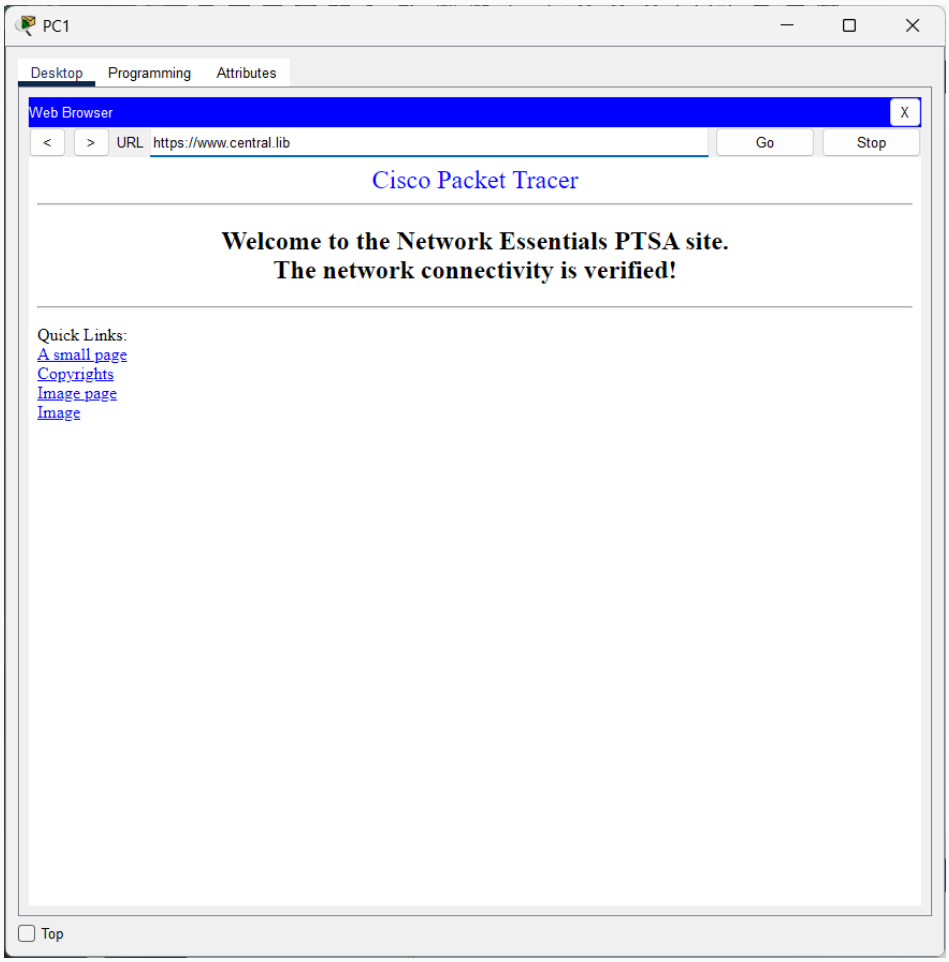


To verify the configuration of the FL-1 switch, the `show ip interface brief` command was executed. The output confirmed that **VLAN 1** is assigned the IP address `10.1.0.200` and is in an **up/up** state, indicating that the management interface is active and reachable. To test secure remote access, an SSH session was initiated using the command `ssh -l tech 10.1.0.200`. The connection was successful, confirming that SSH is properly configured, the user `tech` is authenticated, and the switch is accessible remotely over the network.

Host and Wireless Connectivity Verification

Karunakar Reddy Machupalli - N1334679



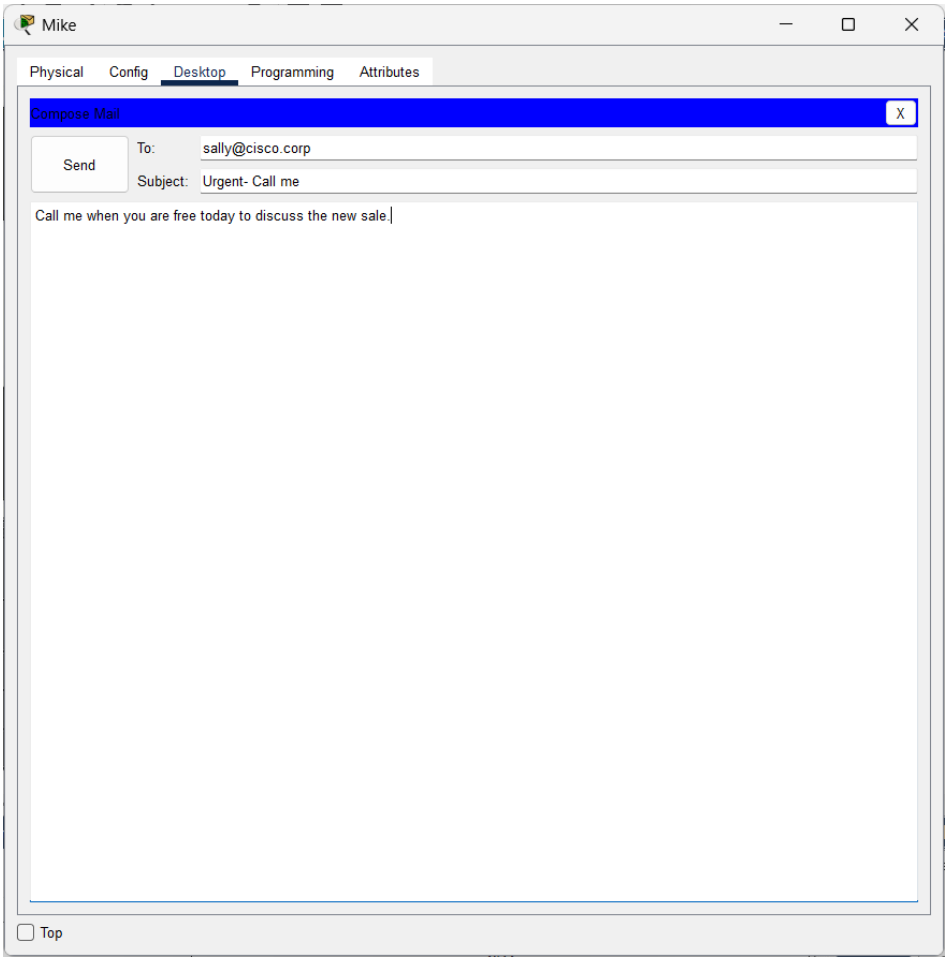


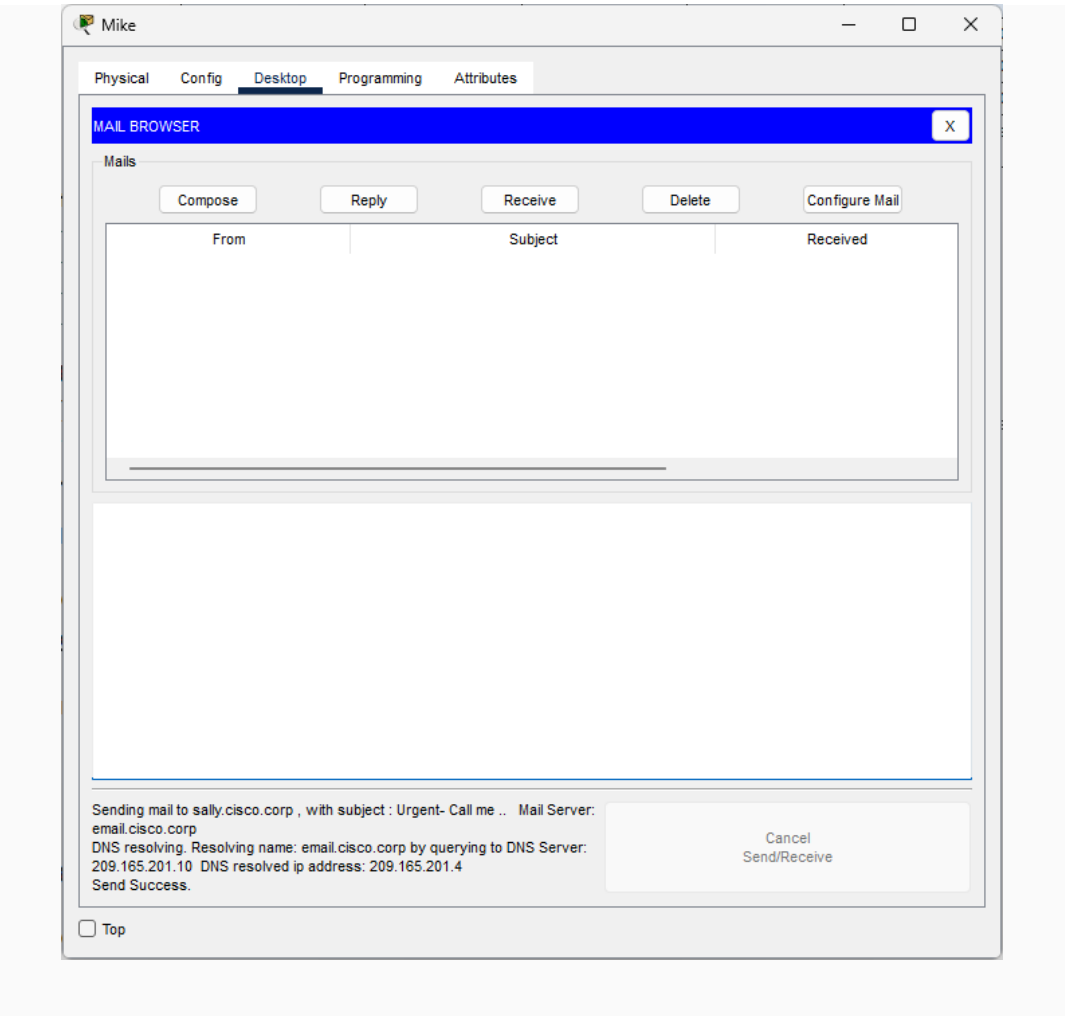
To confirm full network functionality, both the wired PC (Host A) and the wireless laptop (Teach-1) were tested for connectivity. Each device was configured with the appropriate IP settings and successfully connected to the network. Using a web browser, both devices accessed the internal website at `https://www.central.lib`, which loaded correctly and displayed the confirmation message: "*Welcome to the Network Essentials PTSA site. The network connectivity is verified!*" This confirms that routing, DNS resolution, and wireless connectivity are all functioning as expected across the network.

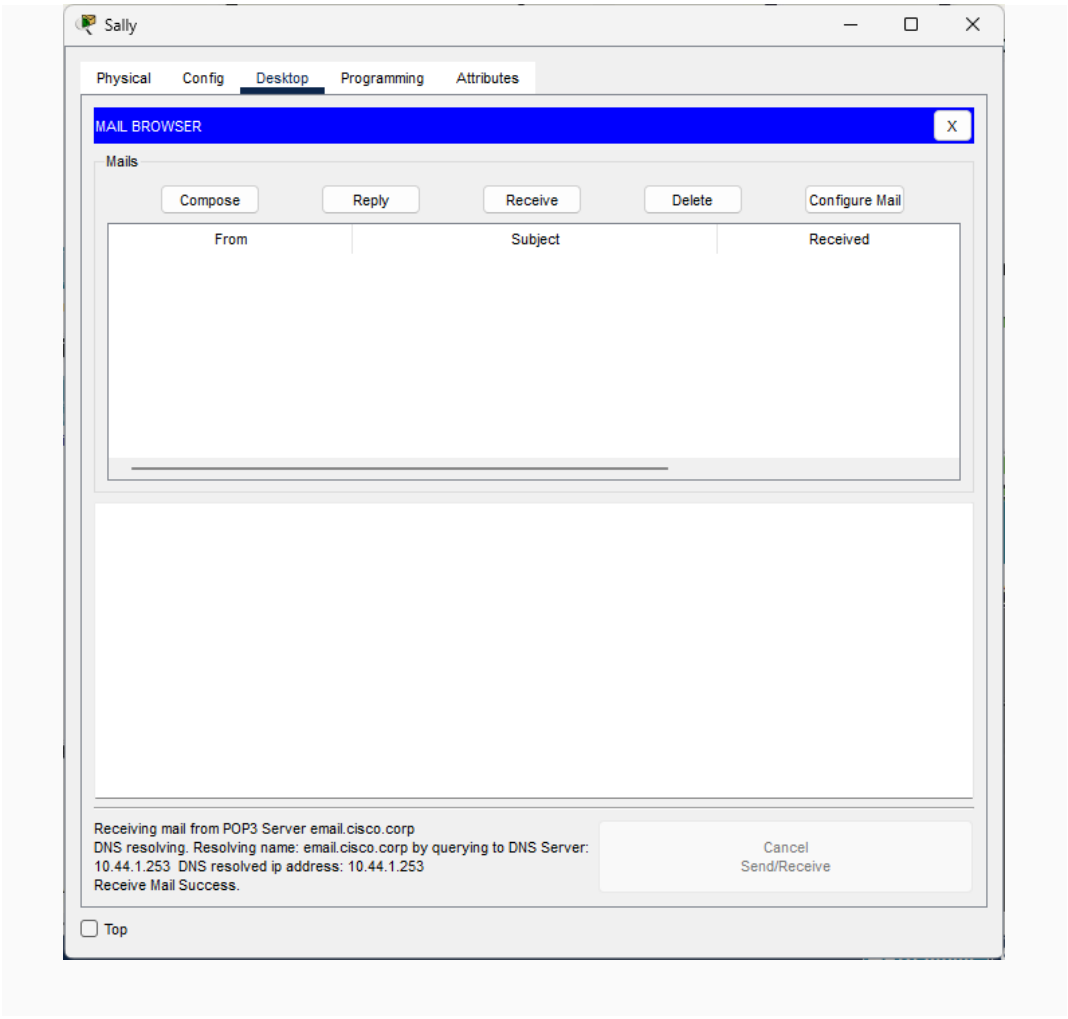
Task 2 - Communicating in a Cyber World

Section A: Implementation Steps

Email Communication

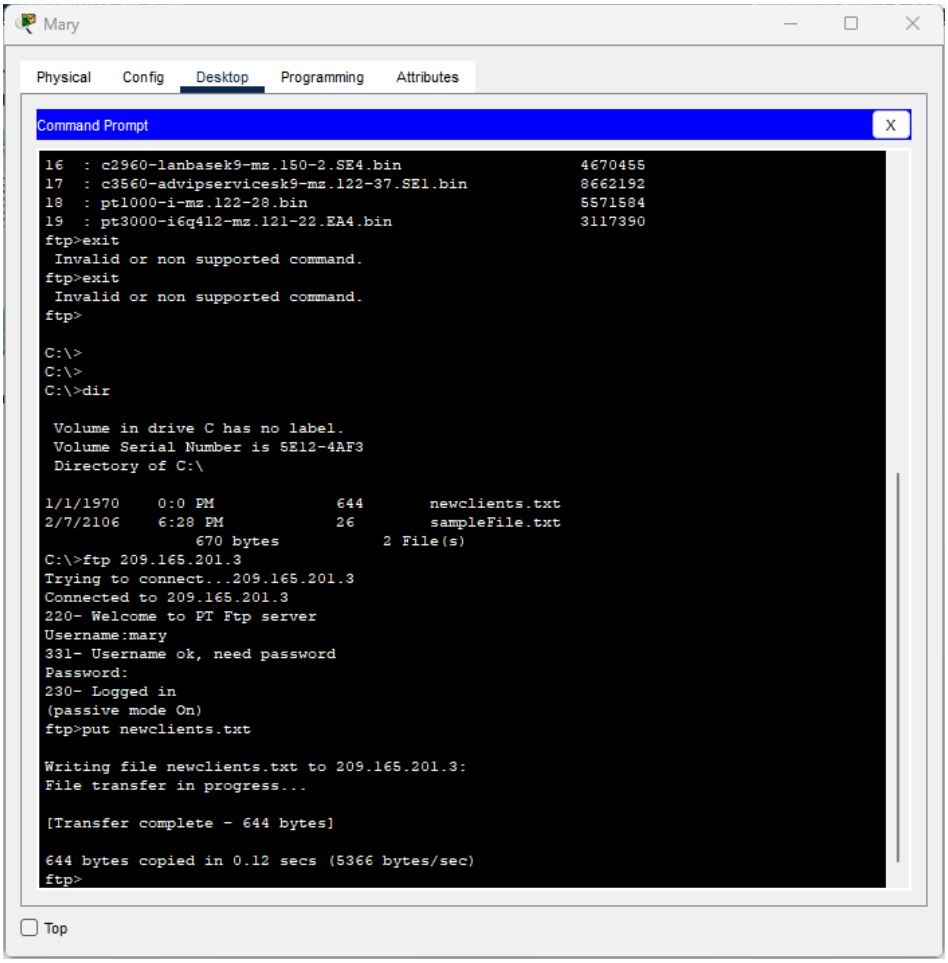



Mike
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
Sending mail to sally.cisco.corp , with subject : Urgent- Call me .. Mail Server: email.cisco.corp
DNS resolving. Resolving name: email.cisco.corp by querying to DNS Server: 209.165.201.10 DNS resolved ip address: 209.165.201.4
Send Success.
Cancel
Send/Receive
Top



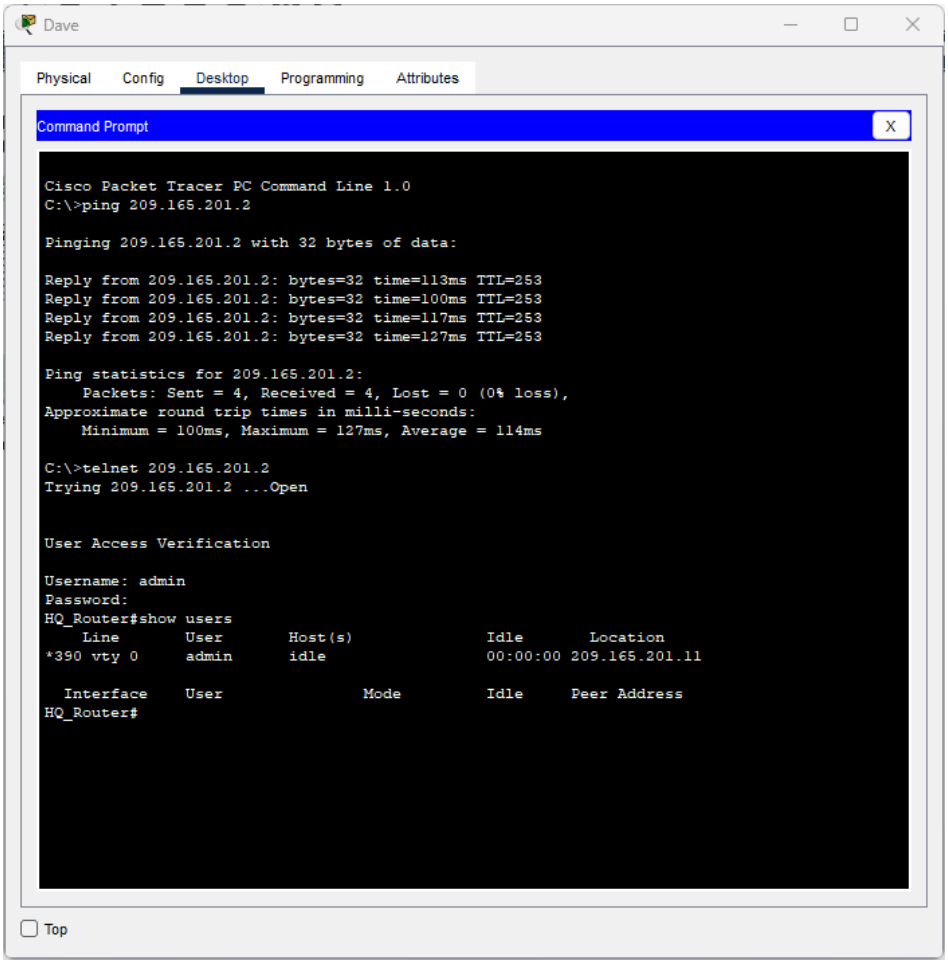
I initiated the email communication task by accessing the email software on Mike's PC at the Gotham Healthcare Branch. I wrote an email to Sally at Metropolis Bank HQ, using the recipient email ID sally@cisco.corp. The email's subject was "Urgent – Call me," and the content read, "Call me when you are free today to discuss the new sale." Upon selecting the submit button, the system commenced DNS resolution to translate the domain email.cisco.corp into an IP address. The external DNS server at 209.165.201.10 successfully resolved the domain and returned the IP address 209.165.201.4, corresponding to the mail server. This resolution allowed the email client to transmit the message to the server using the SMTP (Simple Mail Transfer Protocol). I transitioned to Sally's computer at the Metropolis Bank headquarters and launched the email program. Upon selecting the "Receive" button, the client re-initiated DNS resolution for email.cisco.corp, asking the internal DNS server at 10.44.1.253, which resolved the name to the identical internal mail server IP 10.44.1.253. The email client successfully retrieved the email over the POP3 (Post Office Protocol version 3) protocol. The process was successfully completed, confirming that both the transmission and reception of emails across network sites were completely operational. Consequently, the job illustrated the application of SMTP for transmitting email to the mail server and POP3 for retrieving email from the server.

FTP File Transfer



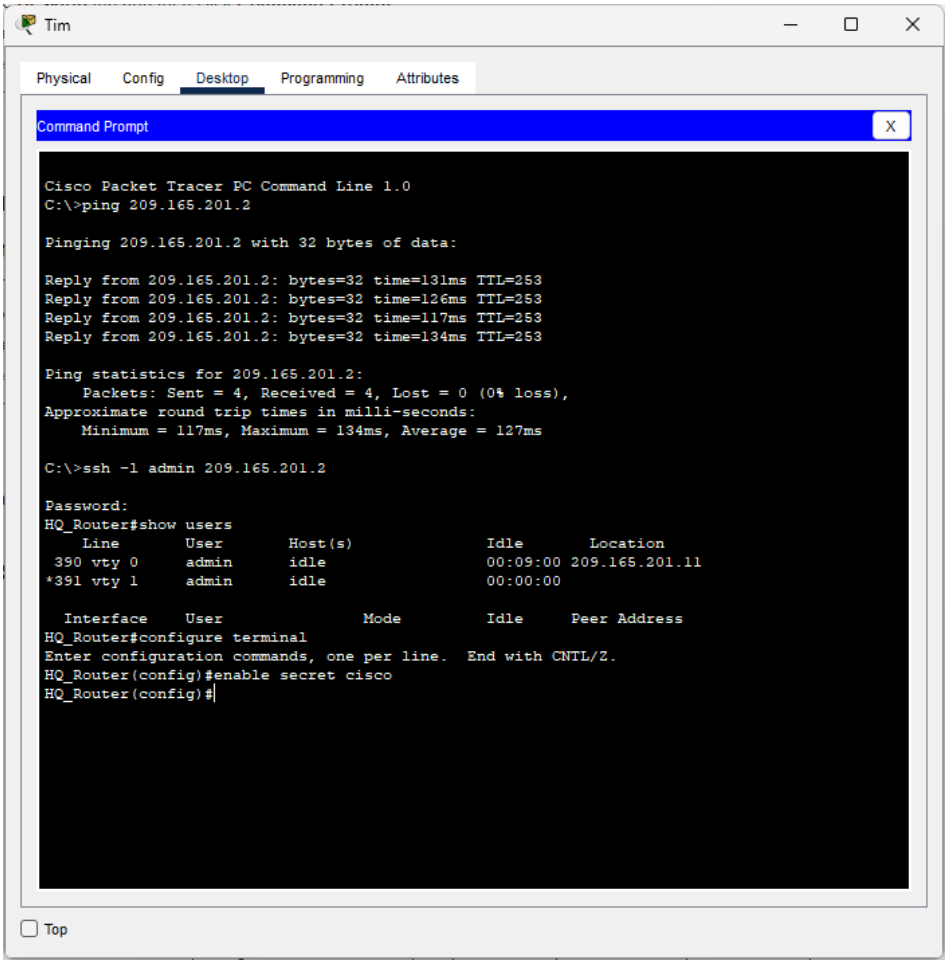
In this segment of the work, I utilized the command-line FTP program on Mary's PC, located at the Healthcare at Home site, to establish a connection with the enterprise FTP server hosted at Metropolis Bank HQ. The connection was established via the server's public IP address 209.165.201.3. After receiving a welcome prompt from the server, I authenticated using the credentials: username mary and password cisco123. Upon acceptance of the login and the session entering passive mode, I executed the command put newclients.txt, which transferred the file containing sensitive healthcare client information to the distant server. The transfer was executed successfully, verifying that the FTP service operated as anticipated. I employed a packet sniffer set up at the Cyber Criminals' node in the network to oversee this procedure. The intercepted packets disclosed unencrypted information, with login credentials and the name of the uploaded file clearly visible during transmission. This underscores the intrinsic vulnerability of FTP-based file transfers.

Telnet Access



I utilized the command prompt on Dave's PC at the Healthcare at Home facility to execute remote administrative access via Telnet. I initially confirmed the connectivity to the remote corporate router at Metropolis Bank HQ by issuing a ping command to the router's public IP address 209.165.201.2. The router provided consistent responses, confirming the device's accessibility and the operability of the network path. I subsequently opened a Telnet session to the identical IP employing the telnet command. Upon connection, the system requested user authentication. I input the username admin and the password cisco123, which provided access to the router's command-line interface. This verified that remote CLI management was effectively implemented via Telnet. Upon logging in, I executed commands like display users, which confirmed the active Telnet session.

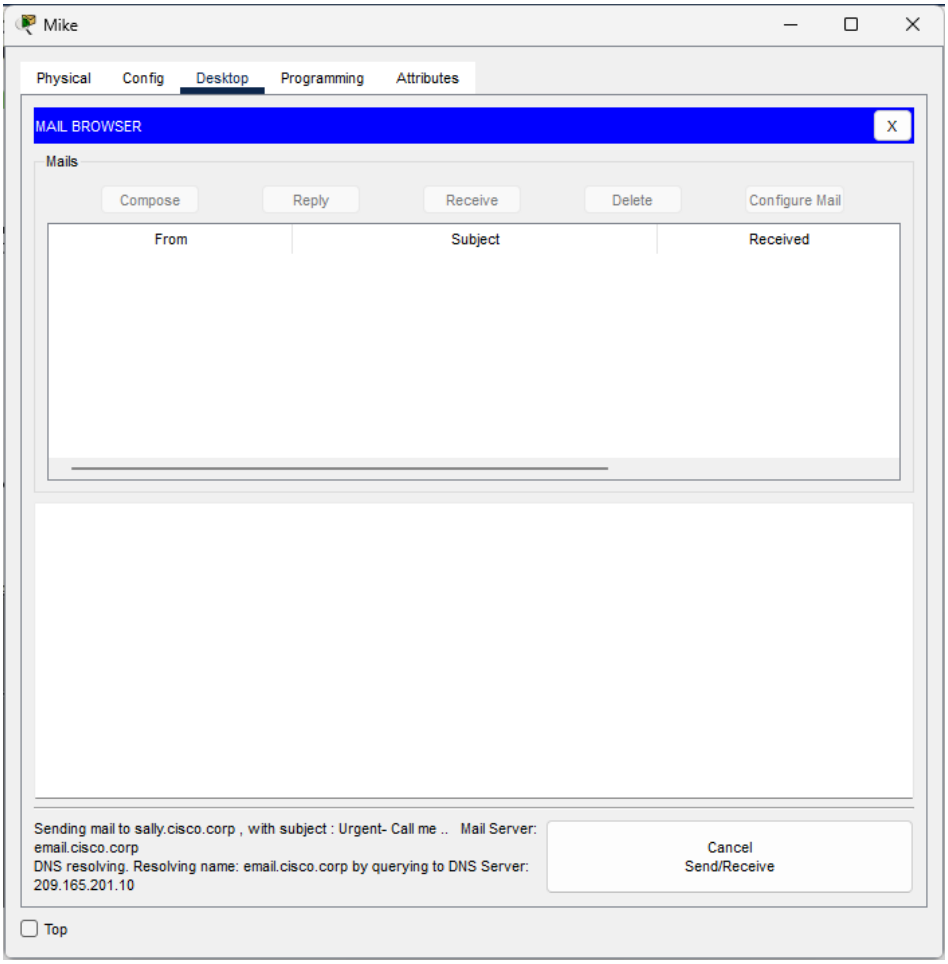
SSH Access



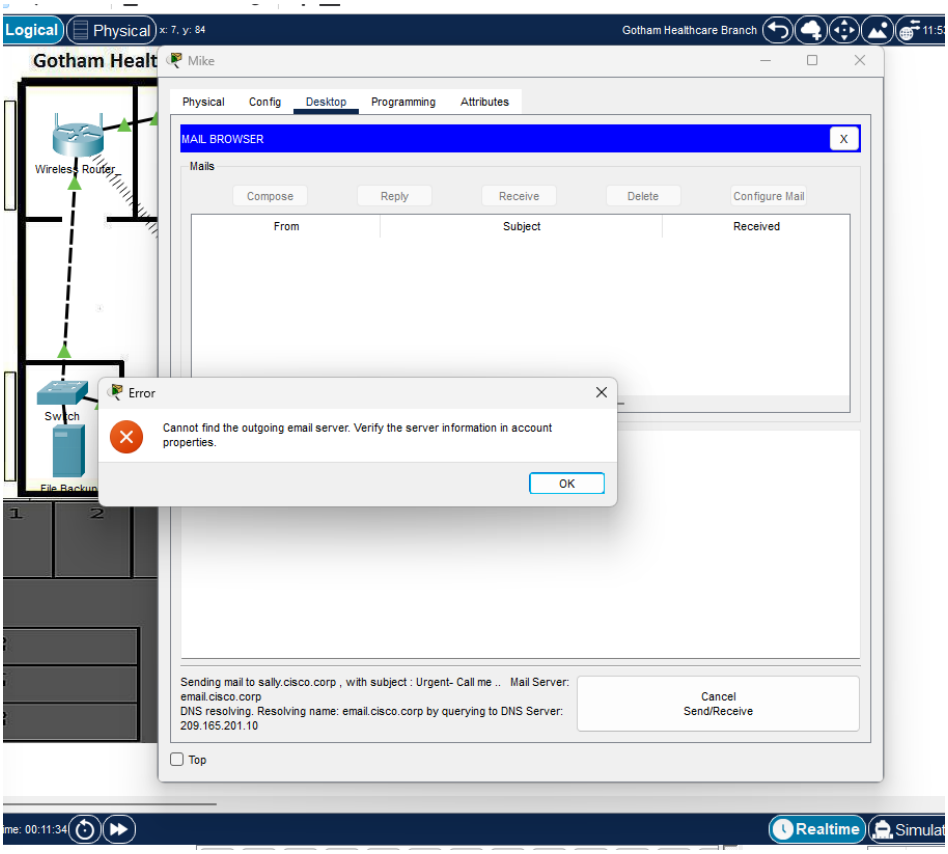
In the concluding phase of the work, I initiated a secure remote management session via SSH (Secure Shell). I initiated a ping from Tim's PC at the Gotham Healthcare Branch to the business router at Metropolis Bank HQ, utilizing the IP address 209.165.201.2. The router replied with all four packets, verifying that the target was accessible via the network. I subsequently commenced an SSH session with the command ssh -l admin 209.165.201.2. Upon inputting the password cisco123, I successfully accessed the router's command-line interface. Upon establishing the connection, I used the command show users, which revealed active remote connections via virtual terminal (vty) lines, indicating that the username admin was logged in, so validating an active SSH session. I accessed global configuration mode by entering configure terminal and established a privileged mode password with the command enable secret cisco. This configuration step guarantees that administrative access to the router is safeguarded by a secure, encrypted password in subsequent sessions.

Section B: Verification and Solutions

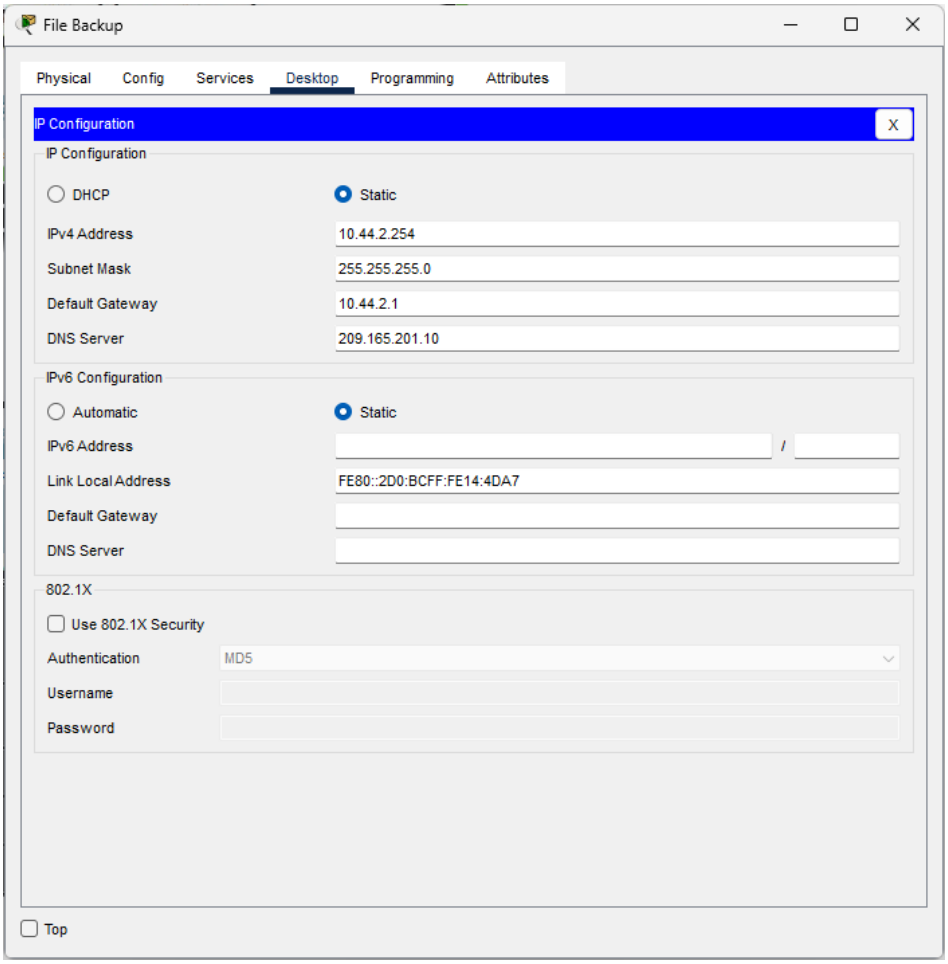
Send Email between Users



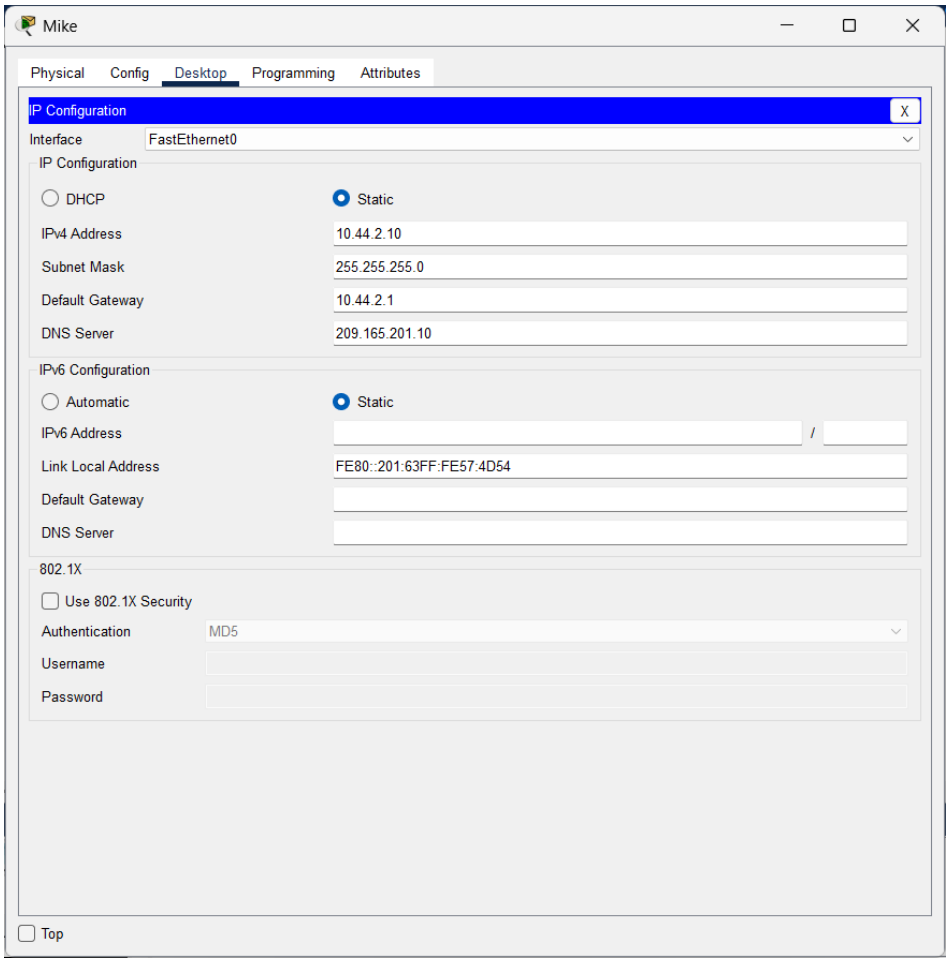
Karunakar Reddy Machupalli - N1334679



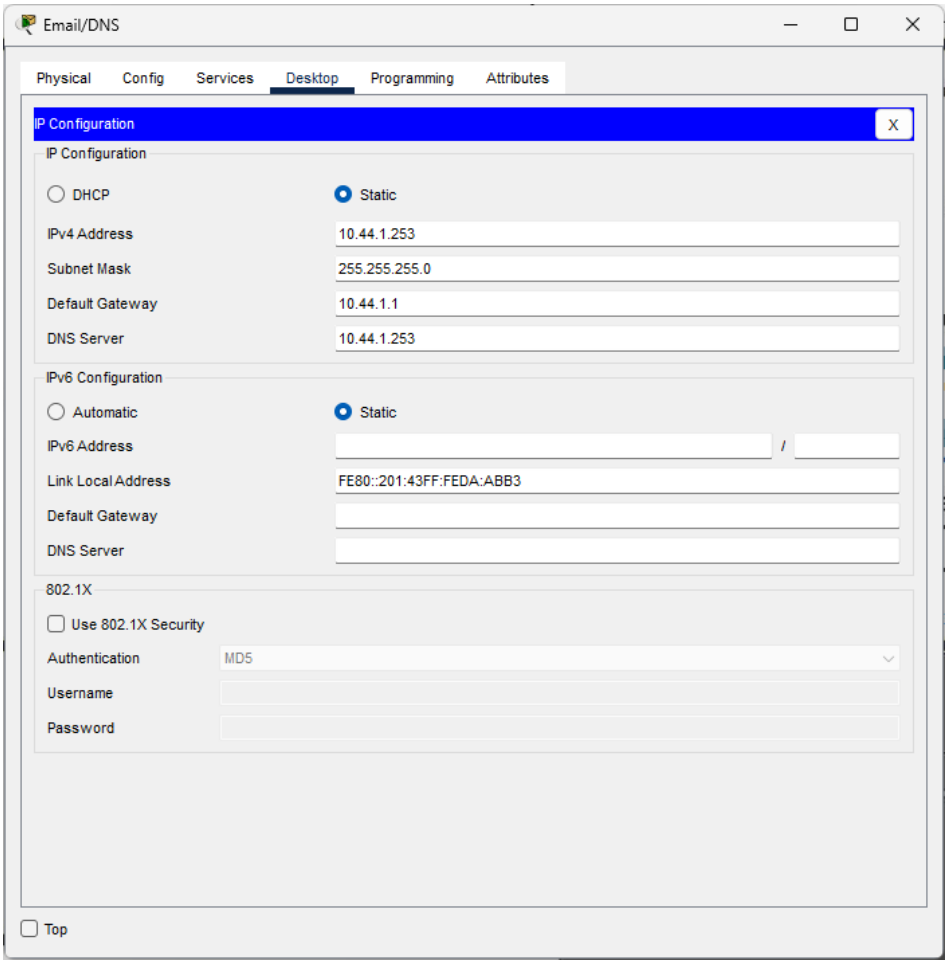
Karunakar Reddy Machupalli - N1334679

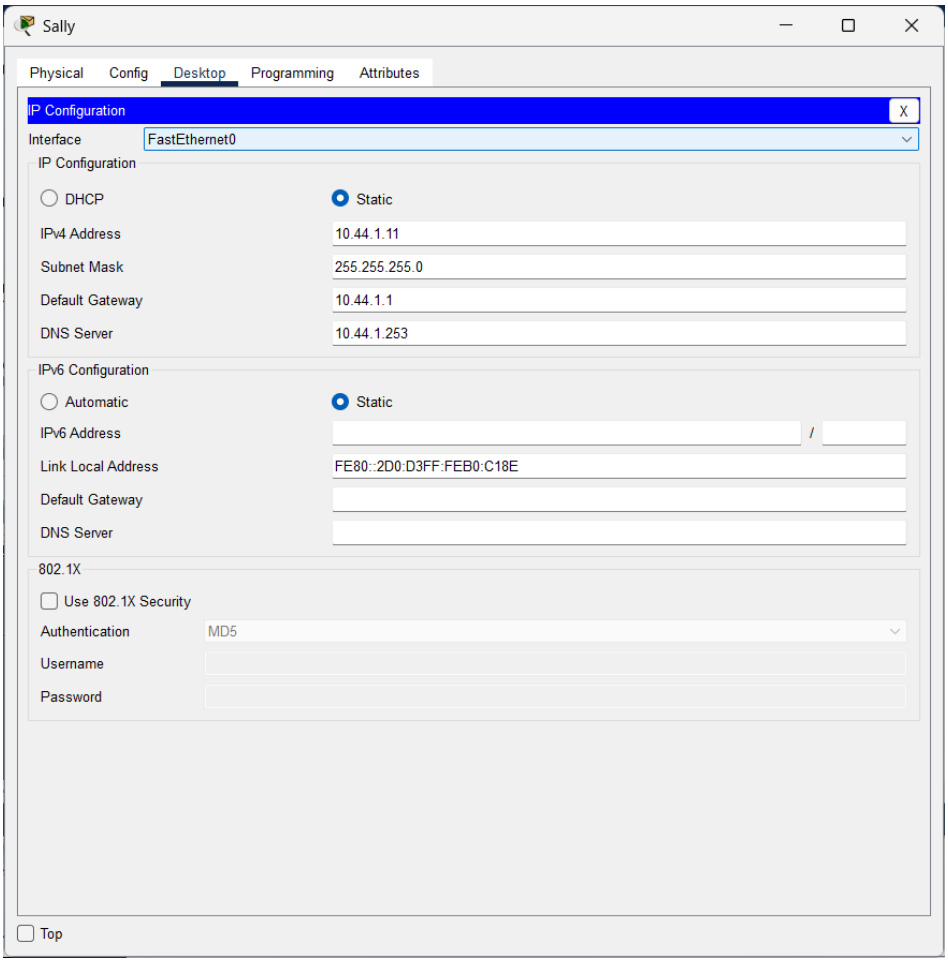


Karunakar Reddy Machupalli - N1334679



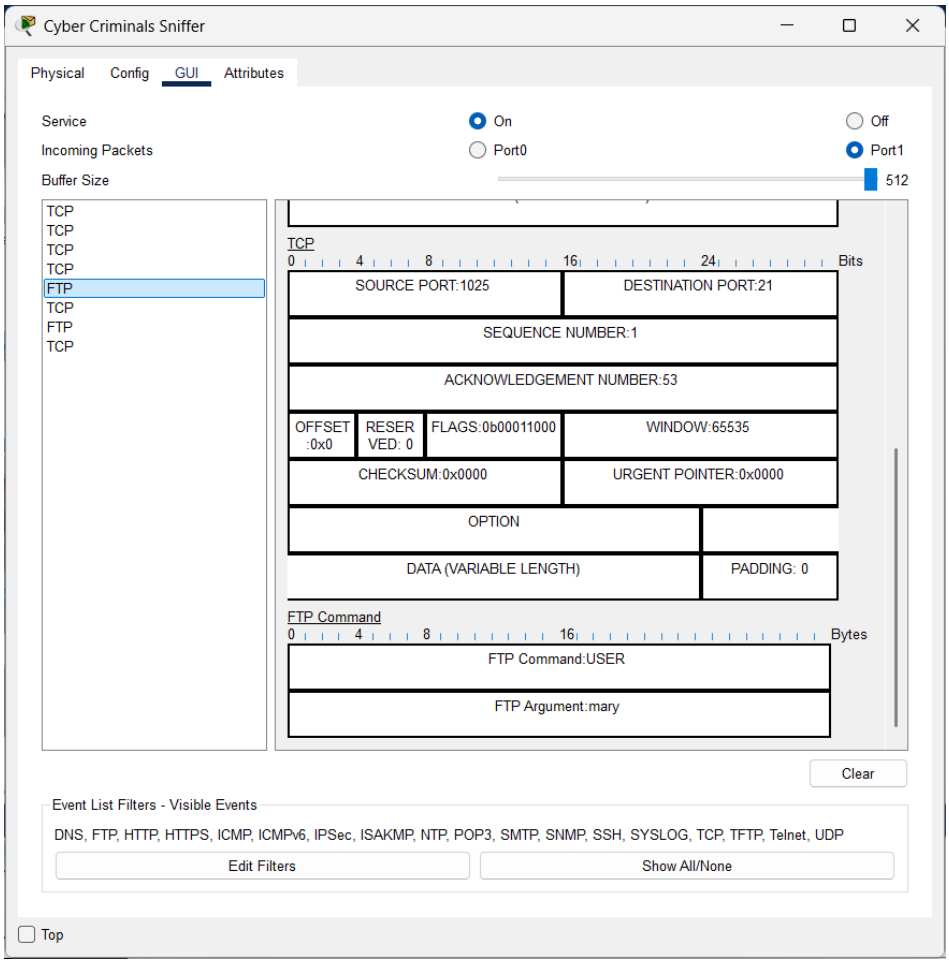
Karunakar Reddy Machupalli - N1334679

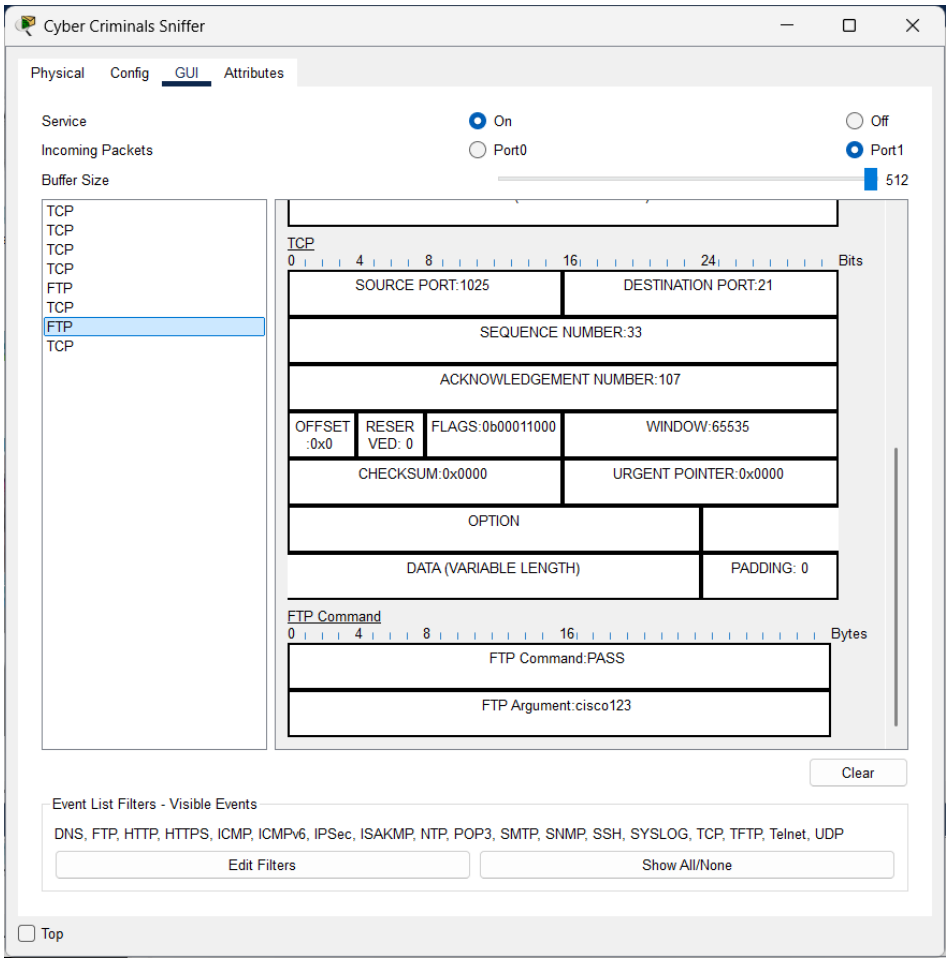




During the execution of Task 2, multiple difficulties were identified and methodically addressed through verification and troubleshooting methods. During the evaluation of email communication in Part 1, an error message was displayed indicating: "Cannot locate the outgoing email server." Confirm the server details in the account settings. This suggested that either the email client was unable to resolve the mail server's domain name or that the device was devoid of network connectivity. Upon inquiry, I found that Mike's PC lacked an allocated IP address and was configured to use an erroneous DNS server. I manually set Mike's PC with the static IPv4 address 10.44.2.10, subnet mask 255.255.255.0, default gateway 10.44.2.1, and DNS server 209.165.201.10, according to the specified addressing scheme. Likewise, Sally's computer at the Metropolis Bank headquarters was discovered to lack a suitable network configuration. Utilizing the foundational setup of the Email/DNS server, which possessed a static IP of 10.44.1.253, subnet mask 255.255.255.0, and a DNS server directed to itself (10.44.1.253), I allocated the IP address 10.44.1.11, subnet mask 255.255.255.0, gateway 10.44.1.1, and DNS server 10.44.1.253 to Sally's PC. The modifications reinstated network functionality and enabled DNS resolution to accurately translate the domain email.cisco.corp to the appropriate IP address. Upon completion, Mike successfully dispatched the email without issues, and Sally retrieved it via the POP3 protocol.

Upload Files using FTP





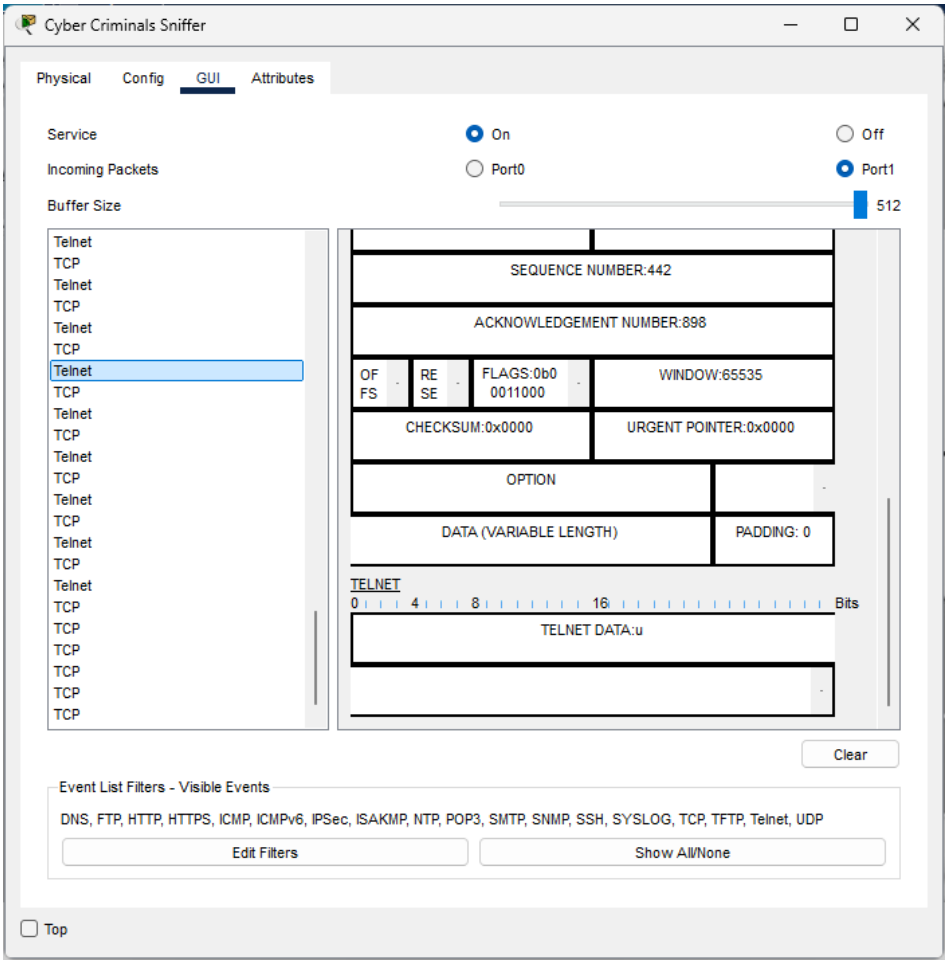
Why is FTP considered an insecure protocol for moving files?

What information is displayed in clear text from the FTP header?

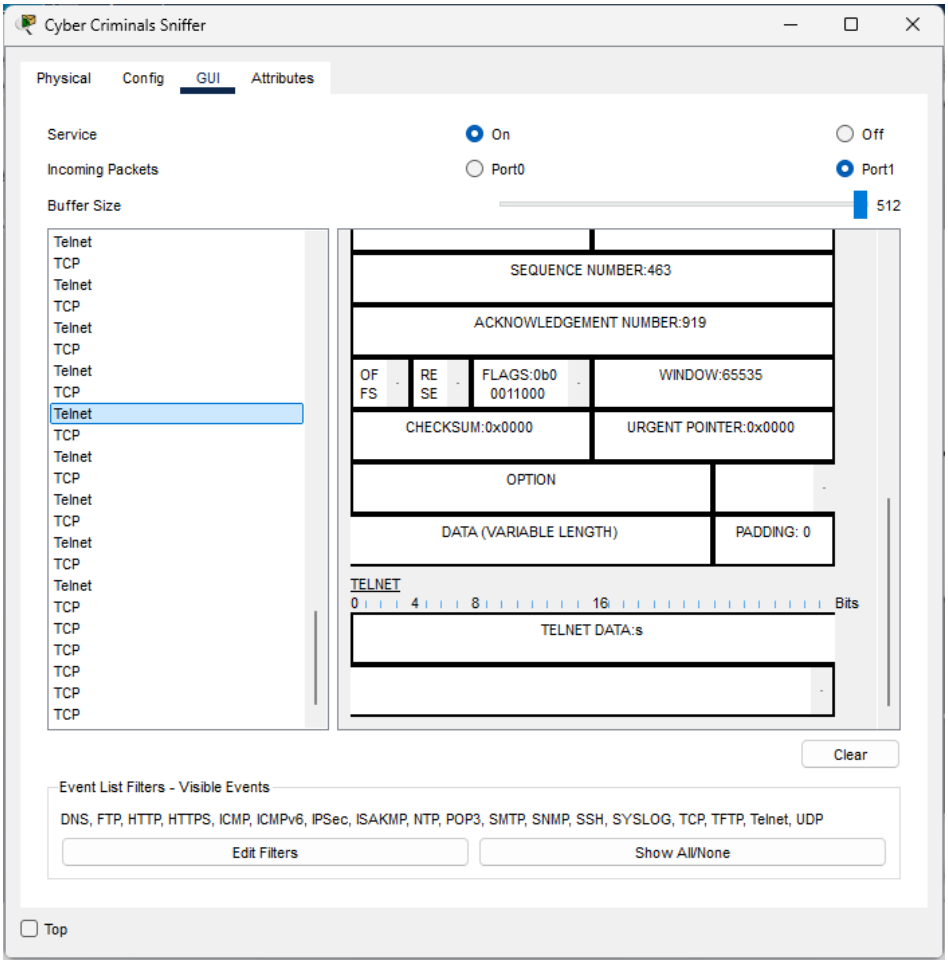
Besides the username, what other sensitive information is displayed in clear text from the FTP header?

During the FTP file upload task, I utilized Mary's PC at the Healthcare at Home site to transfer a confidential file titled newclients.txt to the FTP server at Metropolis Bank HQ. Upon successfully establishing a connection to the server via the command ftp 209.165.201.3, I authenticated using the credentials mary and cisco123. The file was successfully sent with the put command. To authenticate this procedure and assess its security, I employed the Cyber Criminals Sniffer tool connected to the network link. Upon examining the initial collected packets in simulation mode, I distinctly noted the FTP username and password transmitted in plaintext within the packet data. The initial packet displayed the USER command for mary, succeeded by the subsequent packet carrying the PASS cisco123. These findings underscore a significant vulnerability in the FTP protocol, as it lacks data encryption, allowing anyone with access to the network pathway to readily intercept login credentials and file information. Consequently, FTP is exceedingly insecure for the transmission of confidential or sensitive information, particularly across public or untrusted networks.

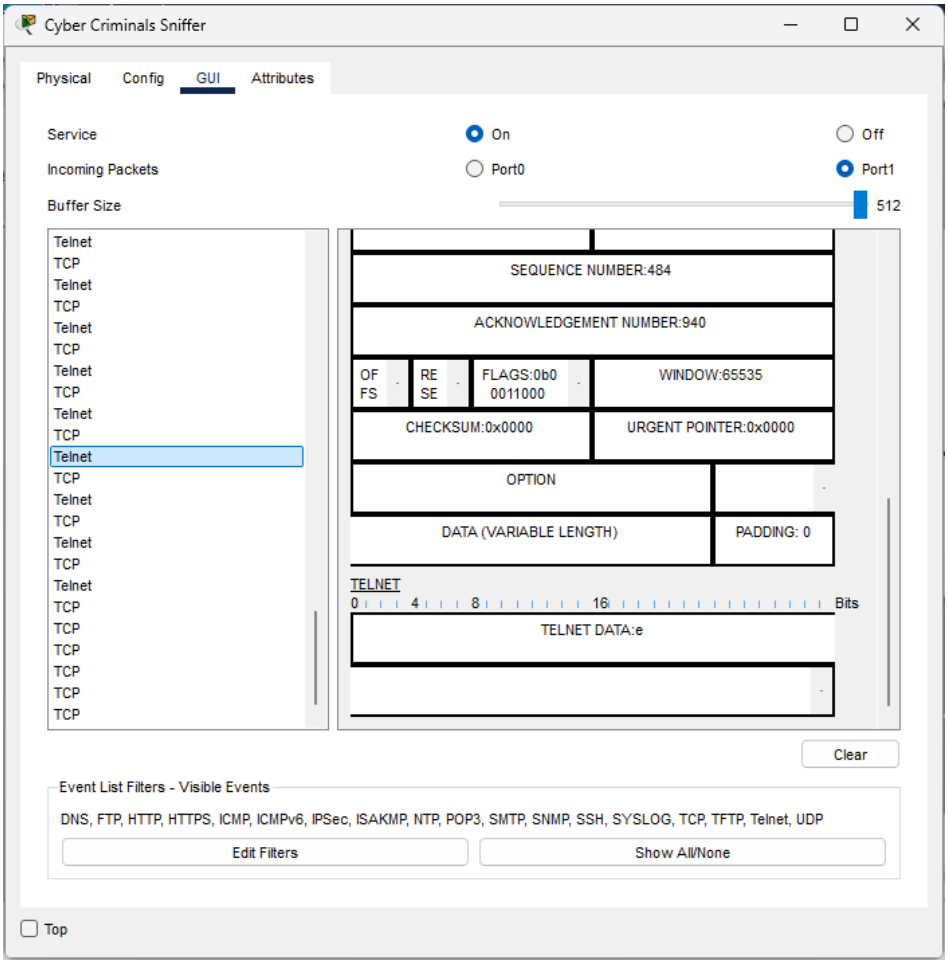
Remotely Access an Enterprise Router Using Telnet

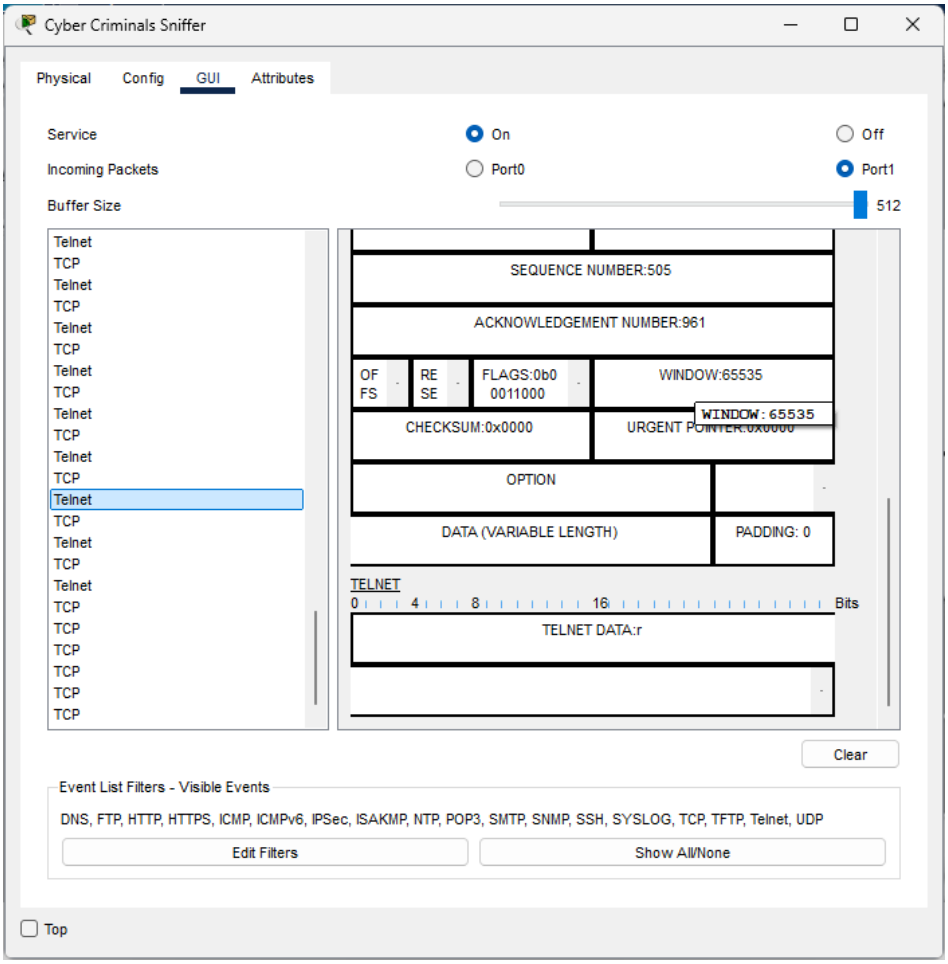


Karunakar Reddy Machupalli - N1334679



Karunakar Reddy Machupalli - N1334679

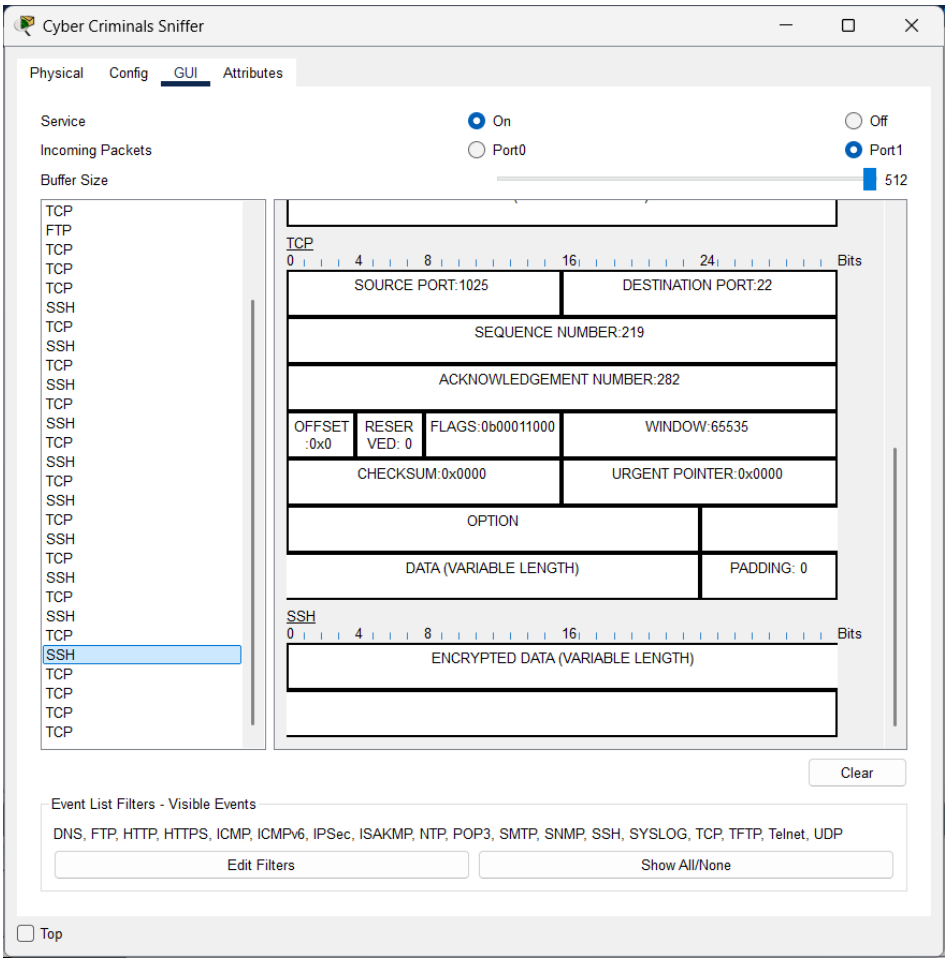




Why is Telnet considered an insecure protocol for remotely managing a device?

During the verification process for remote device management via Telnet, I assessed connectivity from Dave's PC at the Healthcare at Home branch to the business router situated at Metropolis Bank HQ. By executing the command ping 209.165.201.2, I verified successful connectivity with zero packet loss and minimal round-trip delay. Upon verifying that the path was unobstructed, I executed the command telnet 209.165.201.2 to commence a Telnet session. The gadget displayed a login box, to which I provided the credentials: username admin and password cisco123. Following successful authentication, I obtained command-line access to the router's interface. I analyzed Telnet's security by monitoring the flow with packet capture. The complete login sequence, comprising the username and password, was transmitted in plain text without encryption. This reveals a significant flaw in the architecture of Telnet. Any individual intercepting network traffic can access these credentials and obtain unauthorized entry to essential infrastructure.

Remotely Access an Enterprise Router Using SSH



Why is SSH considered a secure protocol for remotely managing a device?

In contrast to Telnet, SSH does not reveal user credentials or session commands during transmission. All data transmitted during the session is secured using encryption. SSH is an exceptionally secure way for remote device management, particularly in public or multi-branch networks where interception poses a problem.