



Nottingham Trent University

Department Of Computer Science
COMP40461 - Coursework April 2025

Network and Cloud Security

By

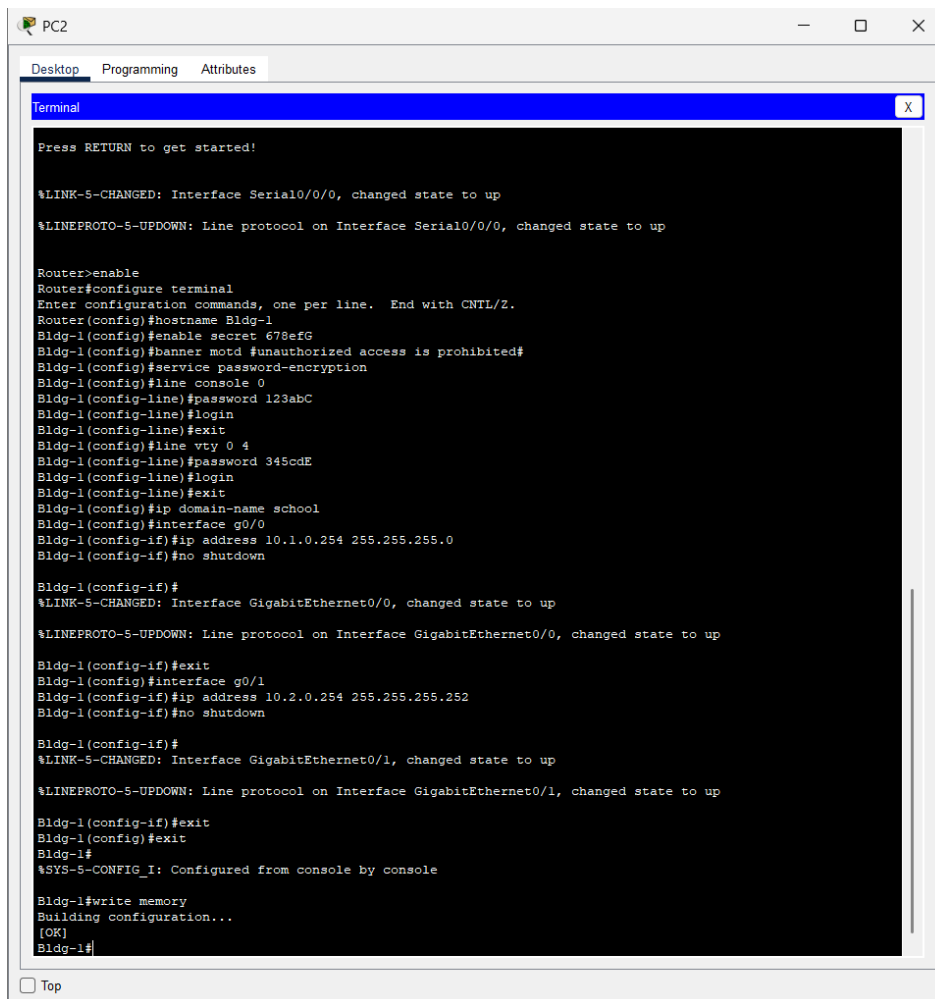
Karunakar Reddy Machupalli – N1334679

Task 1 - Network Design.....	3
Section A: Implementation Steps	3
Basic Router Configuration (Bldg-1) & LAN Interface Configuration	3
FL-1 Switch Remote Management & SSH Configuration on FL-1	4
W-1 Wireless Device Configuration	5
Host Configuration.....	11
Section B: Verification and Troubleshooting	12
Router (Bldg-1) Verification.....	12
Switch (FL-1) Verification.....	14
Host and Wireless Connectivity Verification.....	16
Task 2 - Communicating in a Cyber World	18
Section A: Implementation Steps	18
Email Communication.....	19
FTP File Transfer	22
Telnet Access	22
SSH Access	23
Section B: Verification and Solutions	24
Send Email between Users	25
Upload Files using FTP	31
Remotely Access an Enterprise Router Using Telnet	33
Remotely Access an Enterprise Router Using SSH	36

Task 1 - Network Design

Section A: Implementation Steps

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



```
PC2
Desktop Programming Attributes
Terminal
Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bldg-1
Bldg-1(config)#enable secret 678efG
Bldg-1(config)#banner motd #Unauthorized access is prohibited#
Bldg-1(config)#service password-encryption
Bldg-1(config)#line console 0
Bldg-1(config-line)#password 123abC
Bldg-1(config-line)#login
Bldg-1(config-line)#exit
Bldg-1(config)#line vty 0 4
Bldg-1(config-line)#password 345cdE
Bldg-1(config-line)#login
Bldg-1(config-line)#exit
Bldg-1(config)#ip domain-name school
Bldg-1(config)#interface g0/0
Bldg-1(config-if)#ip address 10.1.0.254 255.255.255.0
Bldg-1(config-if)#no shutdown

Bldg-1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Bldg-1(config-if)#exit
Bldg-1(config)#interface g0/1
Bldg-1(config-if)#ip address 10.2.0.254 255.255.255.252
Bldg-1(config-if)#no shutdown

Bldg-1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

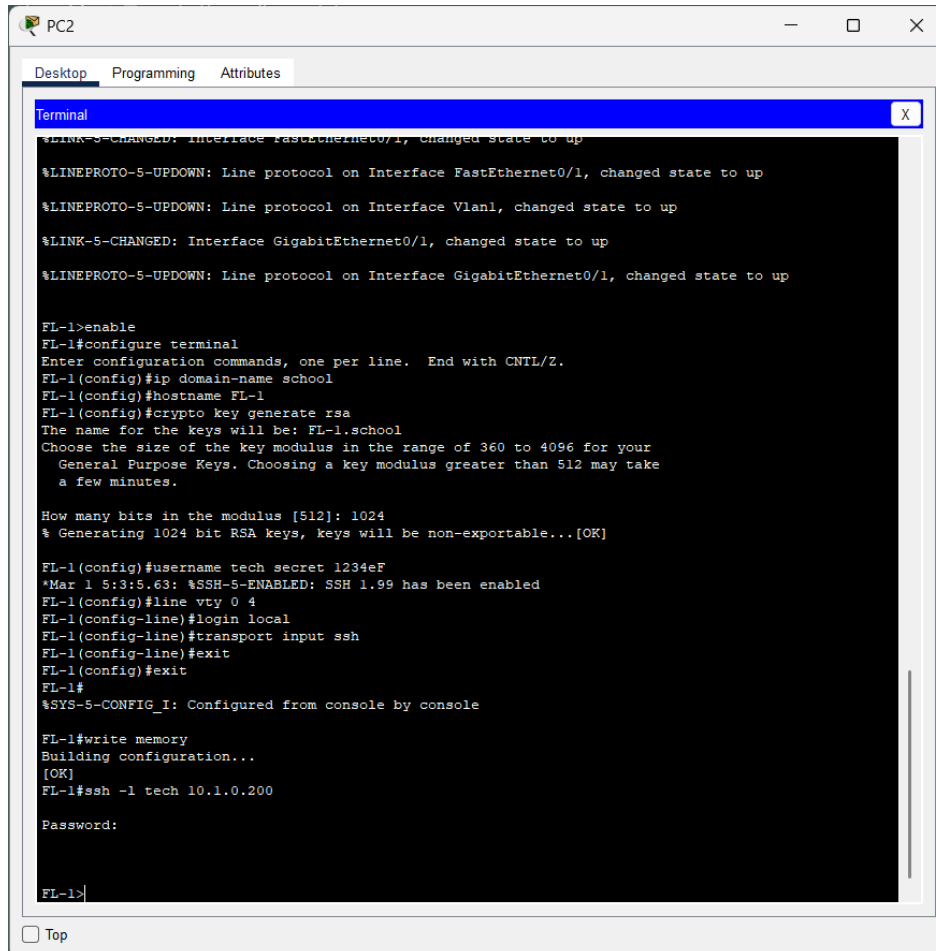
Bldg-1(config-if)#exit
Bldg-1(config)#exit
Bldg-1#
%SYS-5-CONFIG_I: Configured from console by console

Bldg-1#write memory
Building configuration...
[OK]
Bldg-1#
```

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` and activated with `no shutdown`, followed by interface `g0/1` with IP `10.2.0.254` and activated. After exiting interface configuration, the configuration was saved using `write memory`.

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



```

PC2
Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

FL-1>enable
FL-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FL-1(config)#ip domain-name school
FL-1(config)#hostname FL-1
FL-1(config)#crypto key generate rsa
The name for the keys will be: FL-1.school
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

FL-1(config)#username tech secret 1234eF
*Mar 1 5:3:5.63: %SSH-5-ENABLED: SSH 1.99 has been enabled
FL-1(config)#line vty 0 4
FL-1(config-line)#login local
FL-1(config-line)#transport input ssh
FL-1(config-line)#exit
FL-1(config)#exit
FL-1#
%SYS-5-CONFIG_I: Configured from console by console

FL-1#write memory
Building configuration...
[OK]
FL-1#ssh -l tech 10.1.0.200

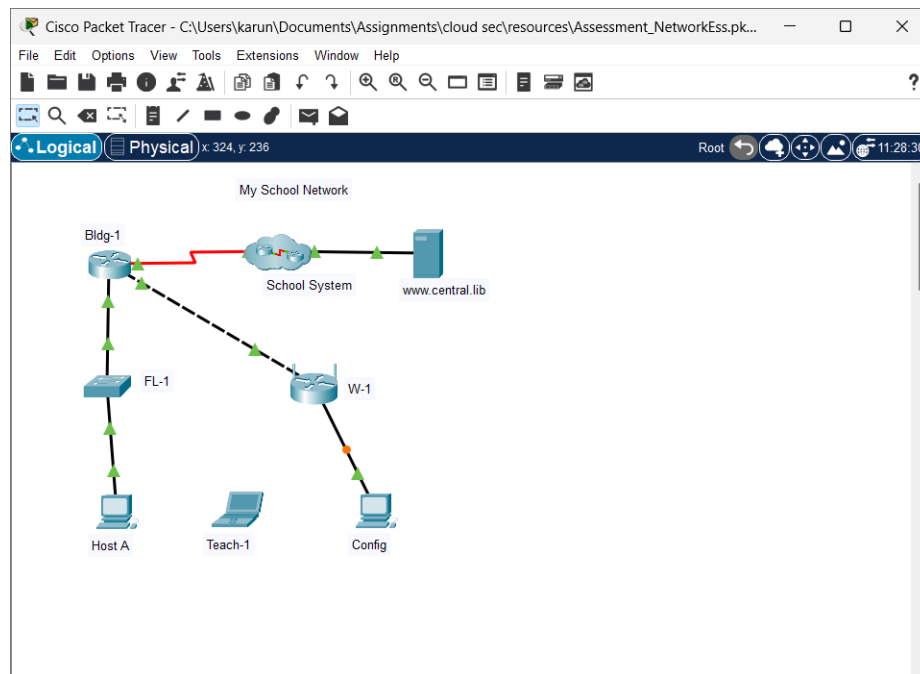
Password:

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



PC2

Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.0.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.0.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

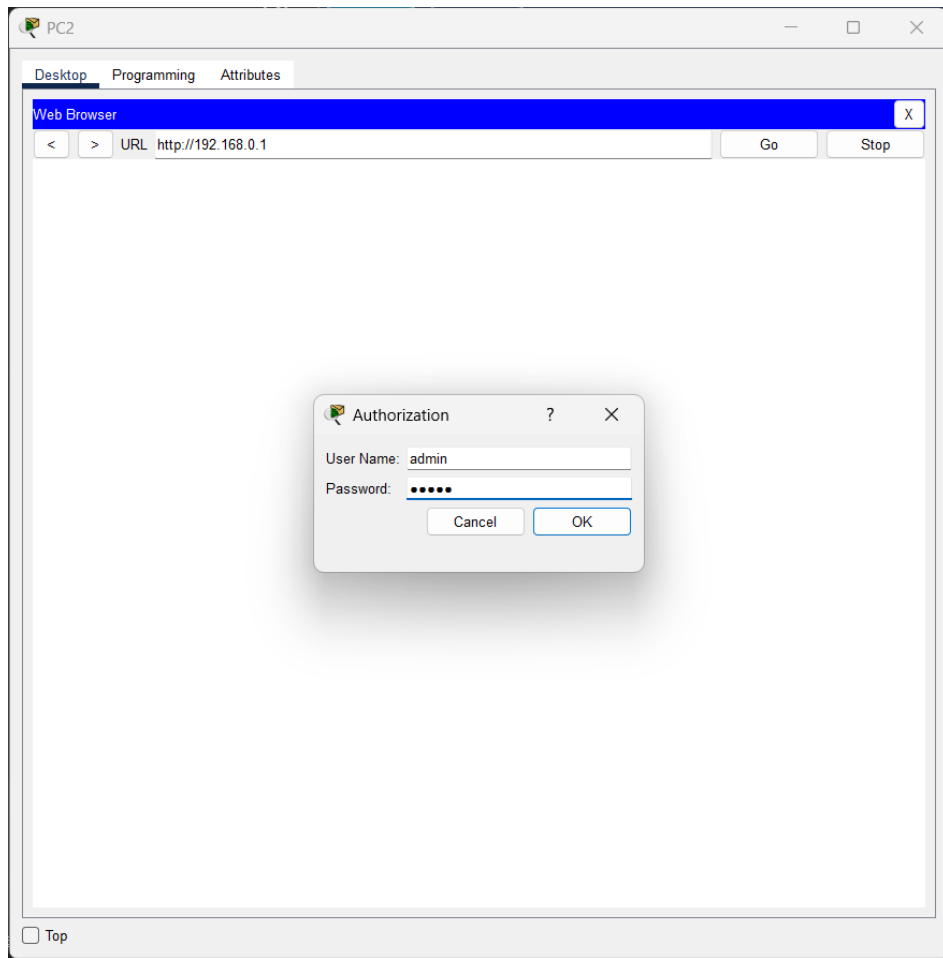
IPv6 Address /

Link Local Address FE80::20D:BDFE:FE3E:EECB

Default Gateway

DNS Server

802.1X



PC2

Desktop Programming Attributes

Web Browser

< > URL: http://192.168.0.1 Go Stop

Wireless Tri-Band Home Router

Firmware V

Setup Setup Wireless Security Access Restrictions Applications & Gaming Administration HomeRouter
Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Static IP

Help...

Internet IP Address: 10 . 2 . 0 . 253
Subnet Mask: 255 . 255 . 255 . 252
Default Gateway: 10 . 2 . 0 . 254
DNS 1: 198 . 51 . 100 . 5
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

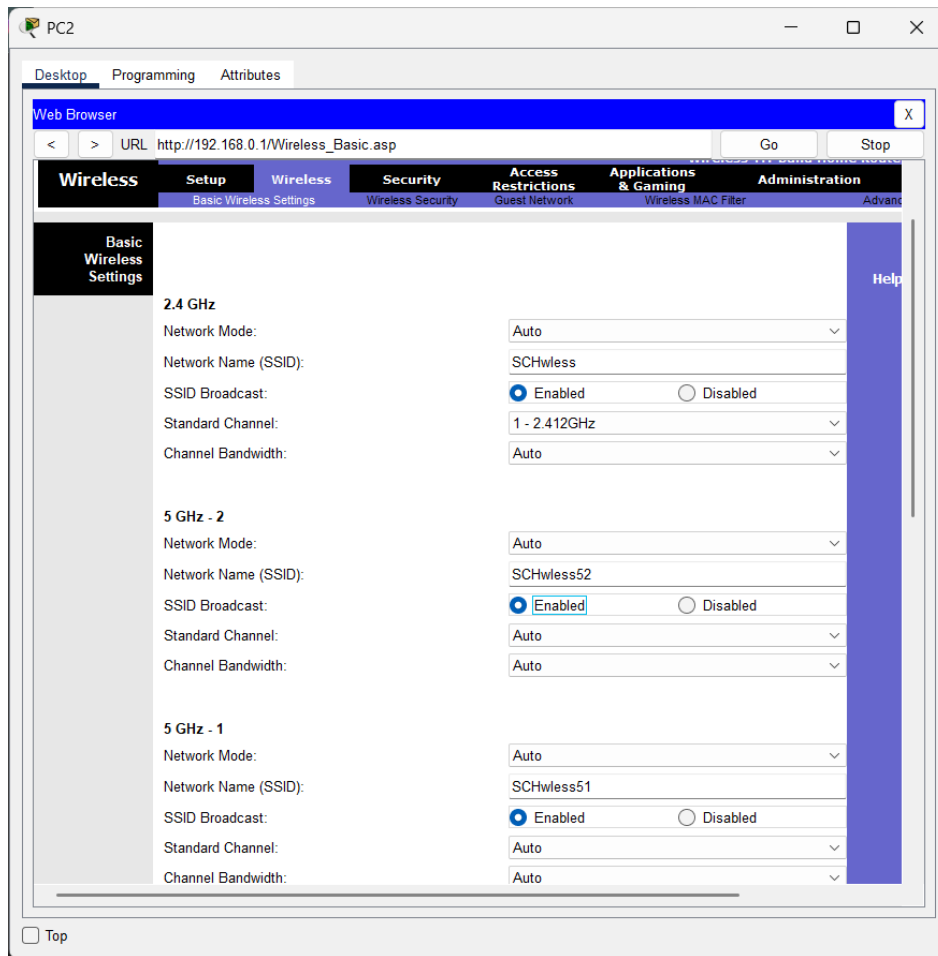
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU: Size: 1500

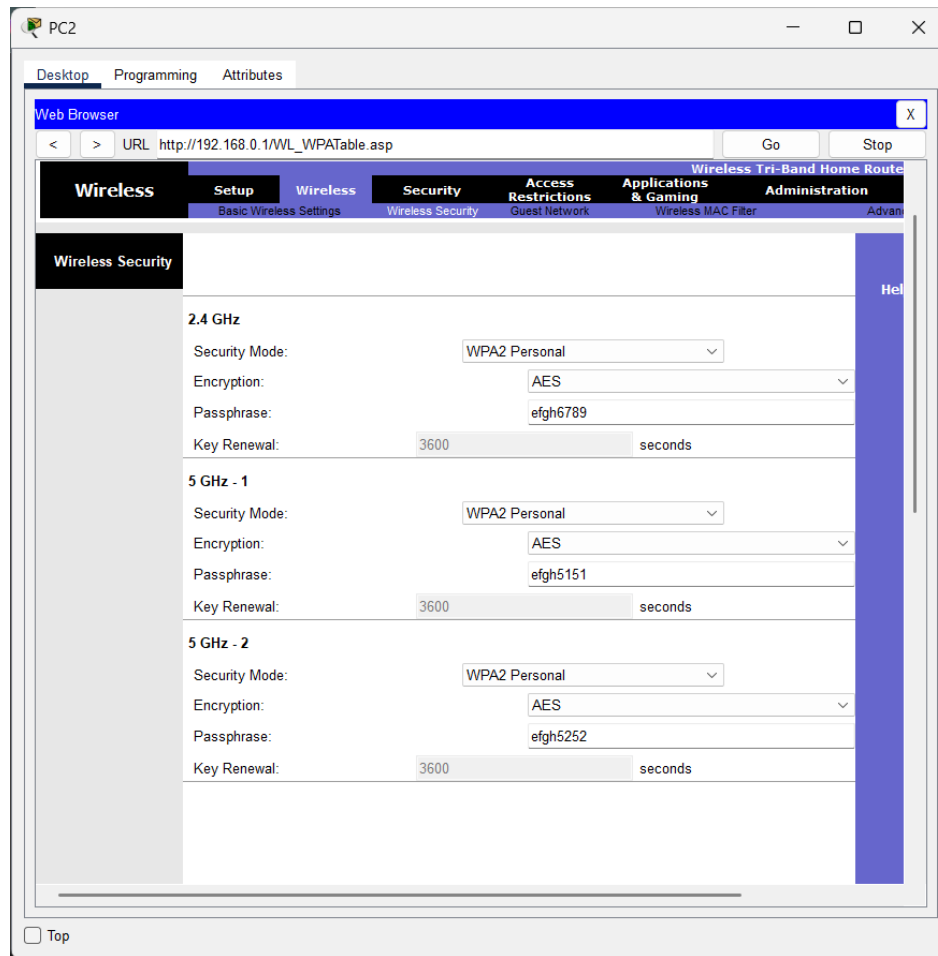
Network Setup

Router IP
IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255.255.255.252

DHCP Server Settings
DHCP Server: ☒ Enabled ☐ Disabled
Start IP Address: 192.168.0.1
Maximum number of Users: 1
IP Address Range: 192.168.0.1 - 1
DHCP Reservation

☐ Top





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

PC1

Desktop

Programming

Attributes

IP Configuration

X

InterfaceFastEthernet0

IP Configuration

☐ DHCP

☒ Static

IPv4 Address10.1.0.5

Subnet Mask255.255.255.0

Default Gateway10.1.0.254

DNS Server198.51.100.5

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address /

Link Local AddressFE80::260:3EFF:FE63:3919

Default Gateway

DNS Server

802.1X

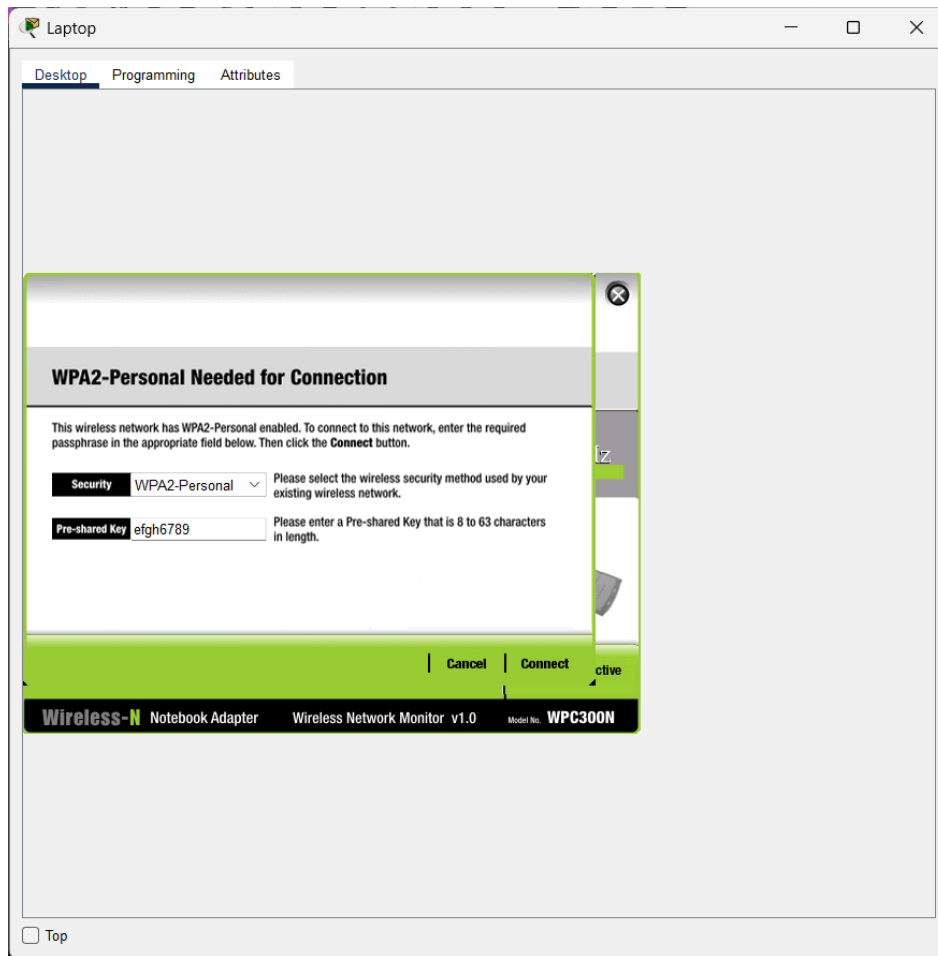
☐ Use 802.1X Security

AuthenticationMD5

Username

Password

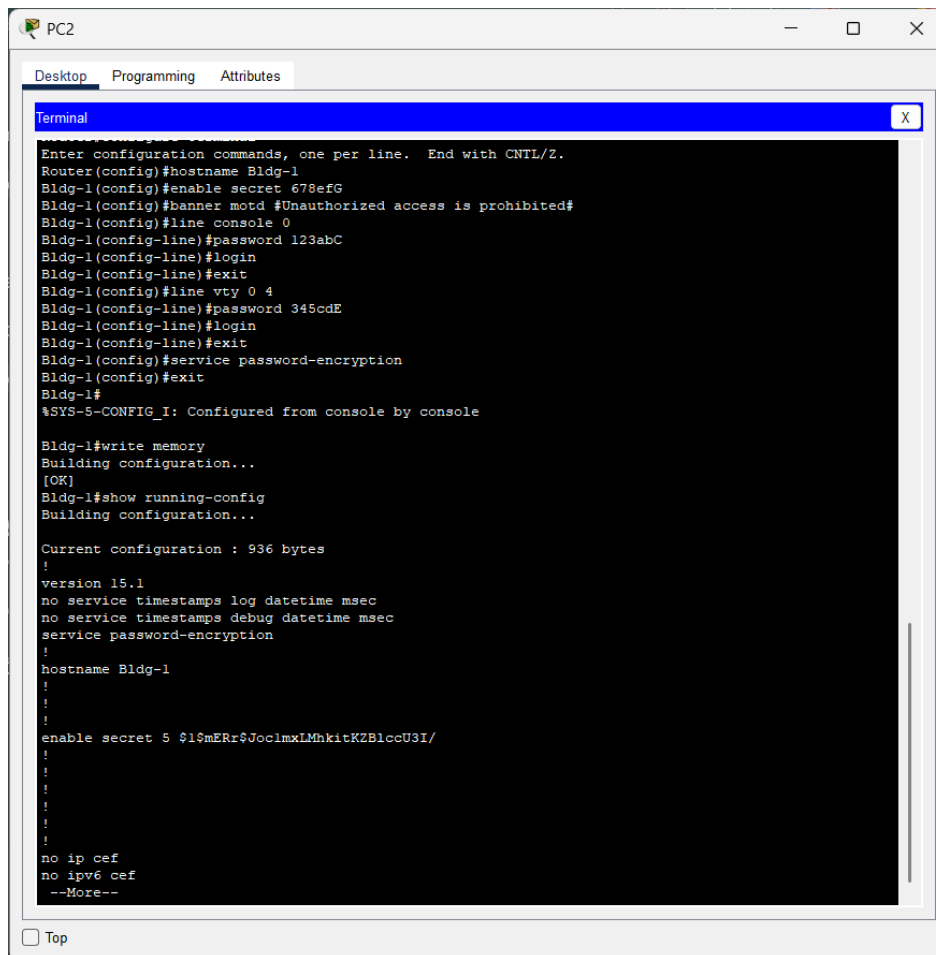
☐ Top



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



The image shows a window titled "PC2" with three tabs: "Desktop", "Programming", and "Attributes". The "Terminal" tab is active, displaying a Cisco IOS configuration session. The user enters various commands to configure a router named "Bldg-1", including setting the hostname, enabling secret passwords, configuring MOTD banners, and setting console and vty lines with passwords. The configuration is saved to memory, and the running configuration is displayed, showing the current configuration size and the full configuration text.

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bldg-1
Bldg-1(config)#enable secret 678efG
Bldg-1(config)#banner motd #Unauthorized access is prohibited#
Bldg-1(config)#line console 0
Bldg-1(config-line)#password 123abC
Bldg-1(config-line)#login
Bldg-1(config-line)#exit
Bldg-1(config)#line vty 0 4
Bldg-1(config-line)#password 345cdE
Bldg-1(config-line)#login
Bldg-1(config-line)#exit
Bldg-1(config)#service password-encryption
Bldg-1(config)#exit
Bldg-1#
%SYS-5-CONFIG_I: Configured from console by console

Bldg-1#write memory
Building configuration...
[OK]
Bldg-1#show running-config
Building configuration...

Current configuration : 936 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Bldg-1
!
!
enable secret 5 $1$mERr$Joc1mxLMhkitKZBlccU3I/
!
!
!
no ip cef
no ipv6 cef
--More--
```

☐ Top

```

PC2
Desktop Programming Attributes
Terminal
Bldg-1#
Bldg-1(config)#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bldg-1(config)#interface GigabitEthernet0/0
Bldg-1(config-if)#ip address 10.1.0.254 255.255.255.0
Bldg-1(config-if)#no shutdown

Bldg-1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Bldg-1(config-if)#exit
Bldg-1(config)#interface GigabitEthernet0/1
Bldg-1(config-if)#ip address 10.2.0.254 255.255.255.252
Bldg-1(config-if)#no shutdown

Bldg-1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Bldg-1(config-if)#exit
Bldg-1(config)#exit
Bldg-1#
%SYS-5-CONFIG_I: Configured from console by console

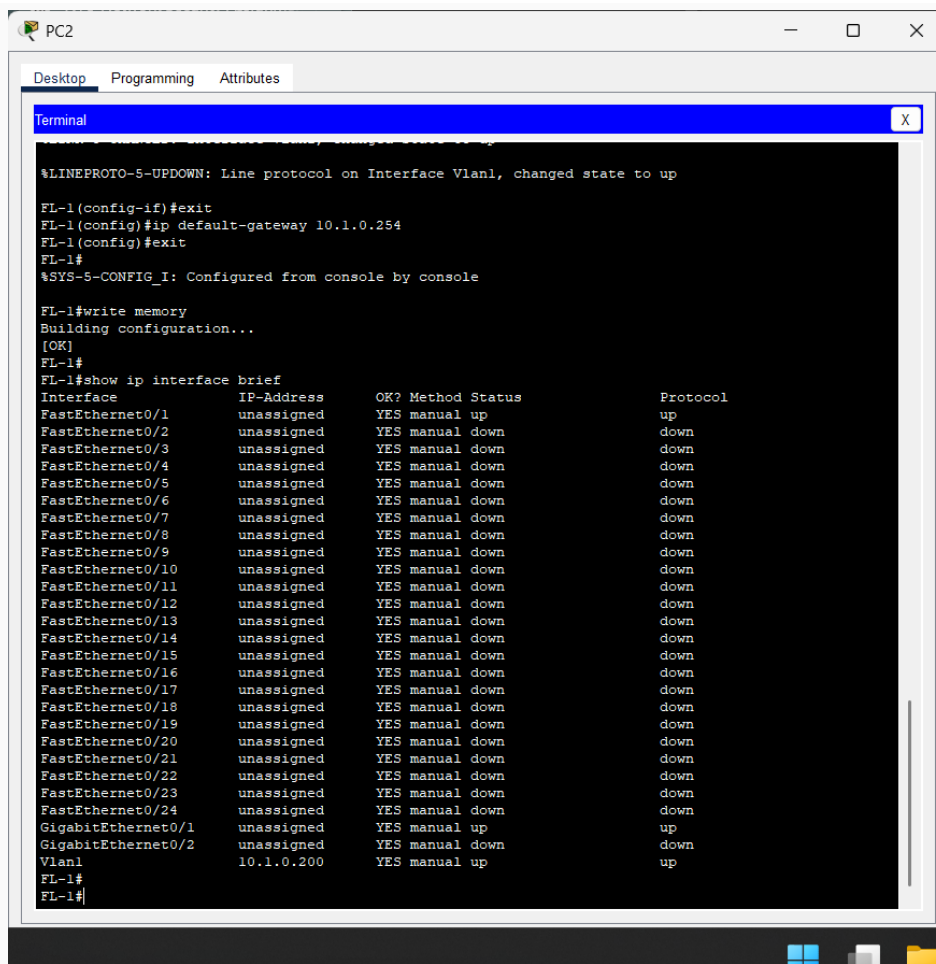
Bldg-1#write memory
Building configuration...
[OK]
Bldg-1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  10.1.0.254      YES manual up          up
GigabitEthernet0/1  10.2.0.254      YES manual up          up
Serial0/0/0       203.0.113.2     YES manual up          up
Serial0/0/1       unassigned      YES unset  administratively down down
Vlan1            unassigned      YES unset  administratively down down

Bldg-1#
Bldg-1#
Bldg-1#
Bldg-1#
Bldg-1#
Bldg-1#
Bldg-1#
Bldg-1#

```

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



The screenshot shows a terminal window titled 'PC2' with tabs for 'Desktop', 'Programming', and 'Attributes'. The 'Terminal' tab is active, displaying a series of commands and their outputs. The commands include setting the line protocol state, exiting configuration mode, setting a default gateway, writing the configuration to memory, and displaying a brief summary of all interfaces.

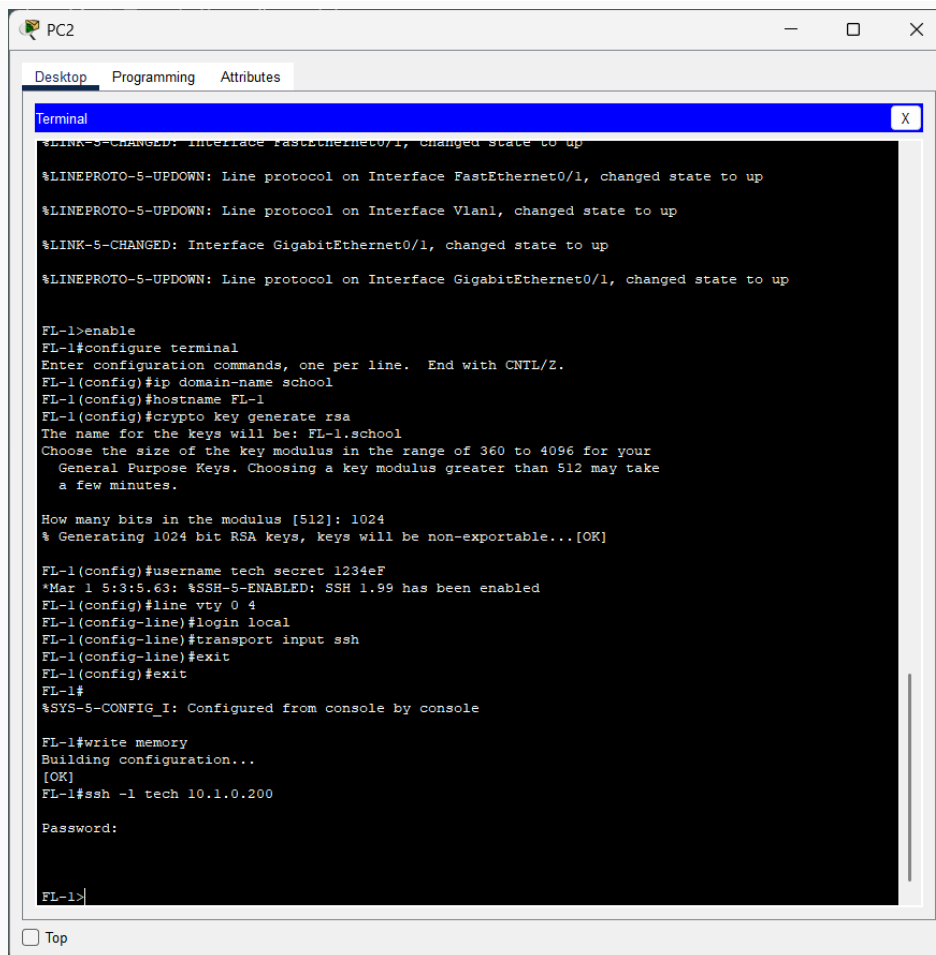
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

FL-1(config-if)#exit
FL-1(config)#ip default-gateway 10.1.0.254
FL-1(config)#exit
FL-1#
%SYS-5-CONFIG_I: Configured from console by console

FL-1#write memory
Building configuration...
[OK]
FL-1#
FL-1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	down	down
FastEthernet0/3	unassigned	YES	manual	down	down
FastEthernet0/4	unassigned	YES	manual	down	down
FastEthernet0/5	unassigned	YES	manual	down	down
FastEthernet0/6	unassigned	YES	manual	down	down
FastEthernet0/7	unassigned	YES	manual	down	down
FastEthernet0/8	unassigned	YES	manual	down	down
FastEthernet0/9	unassigned	YES	manual	down	down
FastEthernet0/10	unassigned	YES	manual	down	down
FastEthernet0/11	unassigned	YES	manual	down	down
FastEthernet0/12	unassigned	YES	manual	down	down
FastEthernet0/13	unassigned	YES	manual	down	down
FastEthernet0/14	unassigned	YES	manual	down	down
FastEthernet0/15	unassigned	YES	manual	down	down
FastEthernet0/16	unassigned	YES	manual	down	down
FastEthernet0/17	unassigned	YES	manual	down	down
FastEthernet0/18	unassigned	YES	manual	down	down
FastEthernet0/19	unassigned	YES	manual	down	down
FastEthernet0/20	unassigned	YES	manual	down	down
FastEthernet0/21	unassigned	YES	manual	down	down
FastEthernet0/22	unassigned	YES	manual	down	down
FastEthernet0/23	unassigned	YES	manual	down	down
FastEthernet0/24	unassigned	YES	manual	down	down
GigabitEthernet0/1	unassigned	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	manual	down	down
Vlan1	10.1.0.200	YES	manual	up	up

```
FL-1#
FL-1#
```



```
PC2
Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

FL-1>enable
FL-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FL-1(config)#ip domain-name school
FL-1(config)#hostname FL-1
FL-1(config)#crypto key generate rsa
The name for the keys will be: FL-1.school
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

FL-1(config)#username tech secret 1234eF
*Mar 1 5:3:5.63: %SSH-5-ENABLED: SSH 1.99 has been enabled
FL-1(config)#line vty 0 4
FL-1(config-line)#login local
FL-1(config-line)#transport input ssh
FL-1(config-line)#exit
FL-1(config)#exit
FL-1#
%SYS-5-CONFIG_I: Configured from console by console

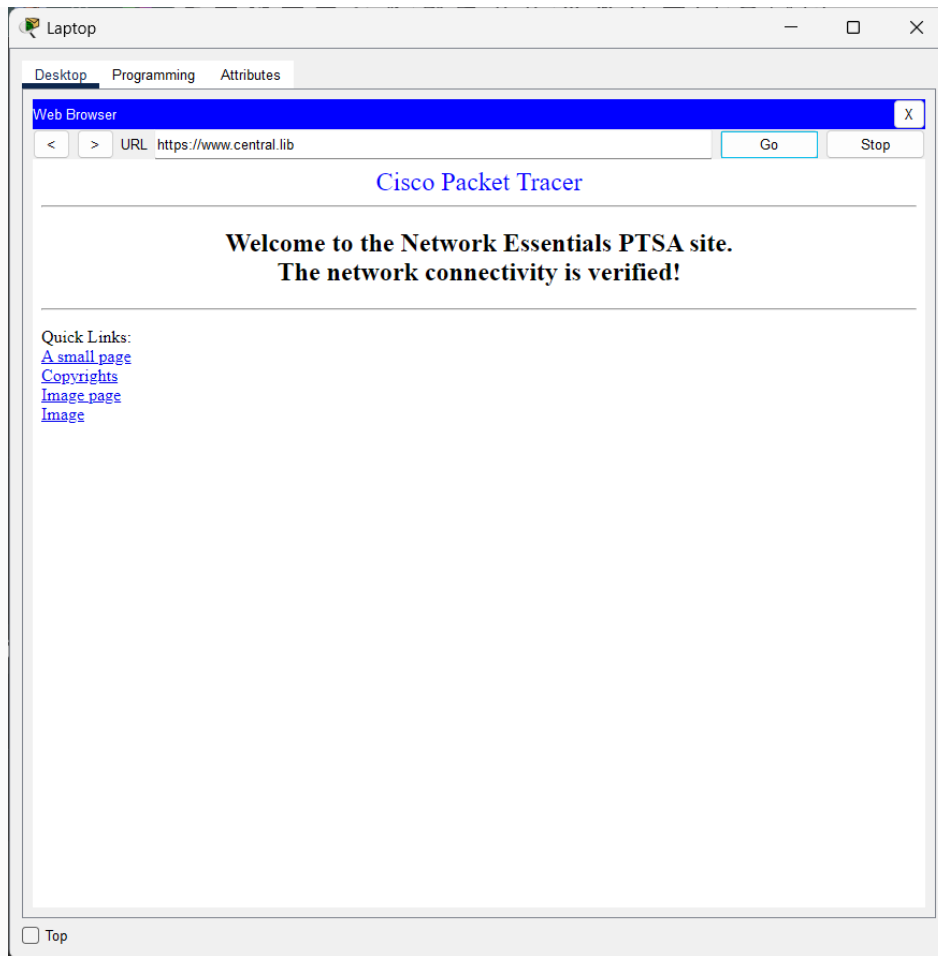
FL-1#write memory
Building configuration...
[OK]
FL-1#ssh -l tech 10.1.0.200

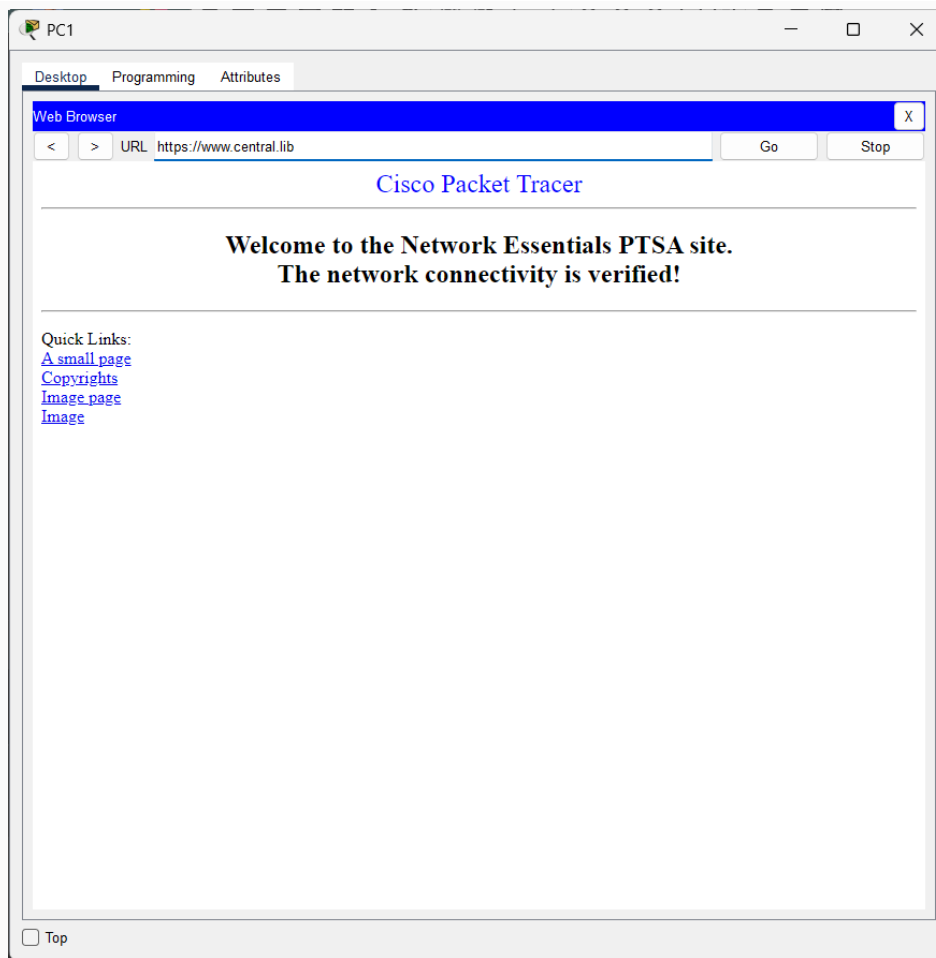
Password:

FL-1>
```

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



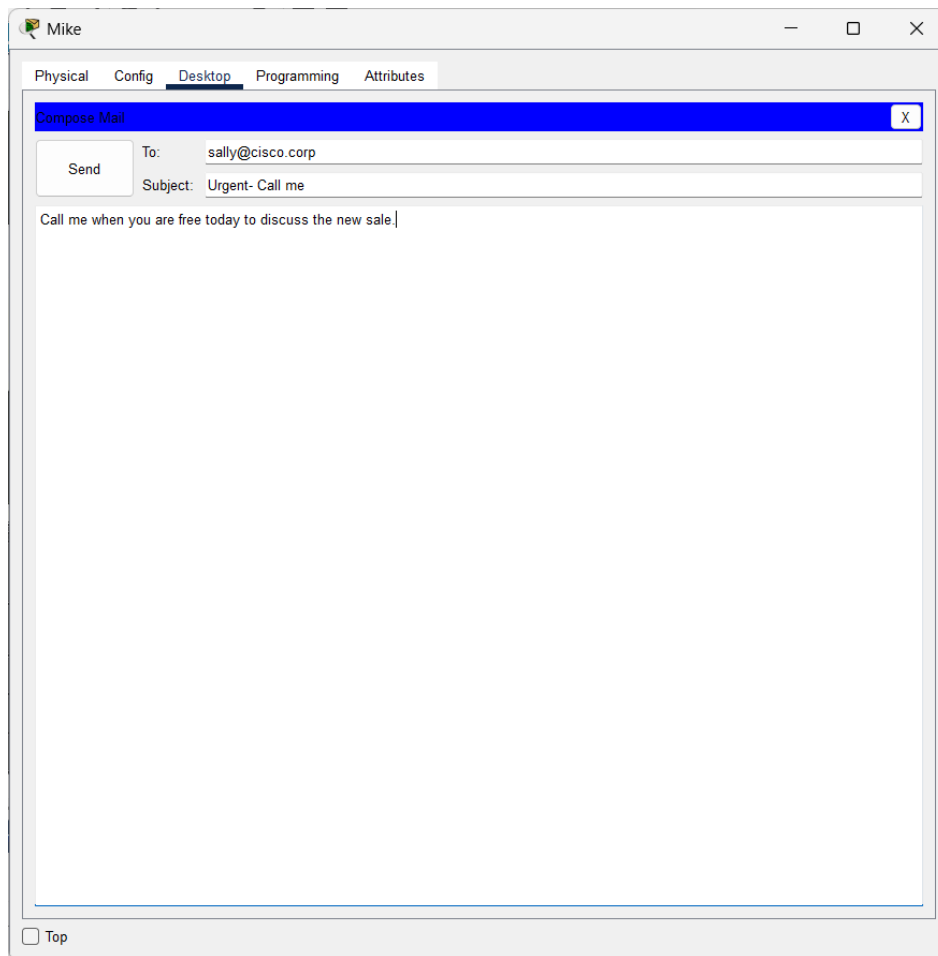


To confirm full network functionality, both the wired PC (Host A) and the wireless laptop (Teach-1) were tested for connectivity. Each device was configured with the appropriate IP settings and successfully connected to the network. Using a web browser, both devices accessed the internal website at `https://www.central.lib`, 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



The screenshot shows a Cisco IOS interface window titled "Mike". It features a tabbed menu at the top with "Physical", "Config", "Desktop" (selected), "Programming", and "Attributes". The "Compose Mail" window is open, displaying a "Send" button and fields for "To:" (sally@cisco.corp) and "Subject:" (Urgent- Call me). The email body contains the text "Call me when you are free today to discuss the new sale." and a "Top" link at the bottom left.

Mike

Physical Config **Desktop** Programming Attributes

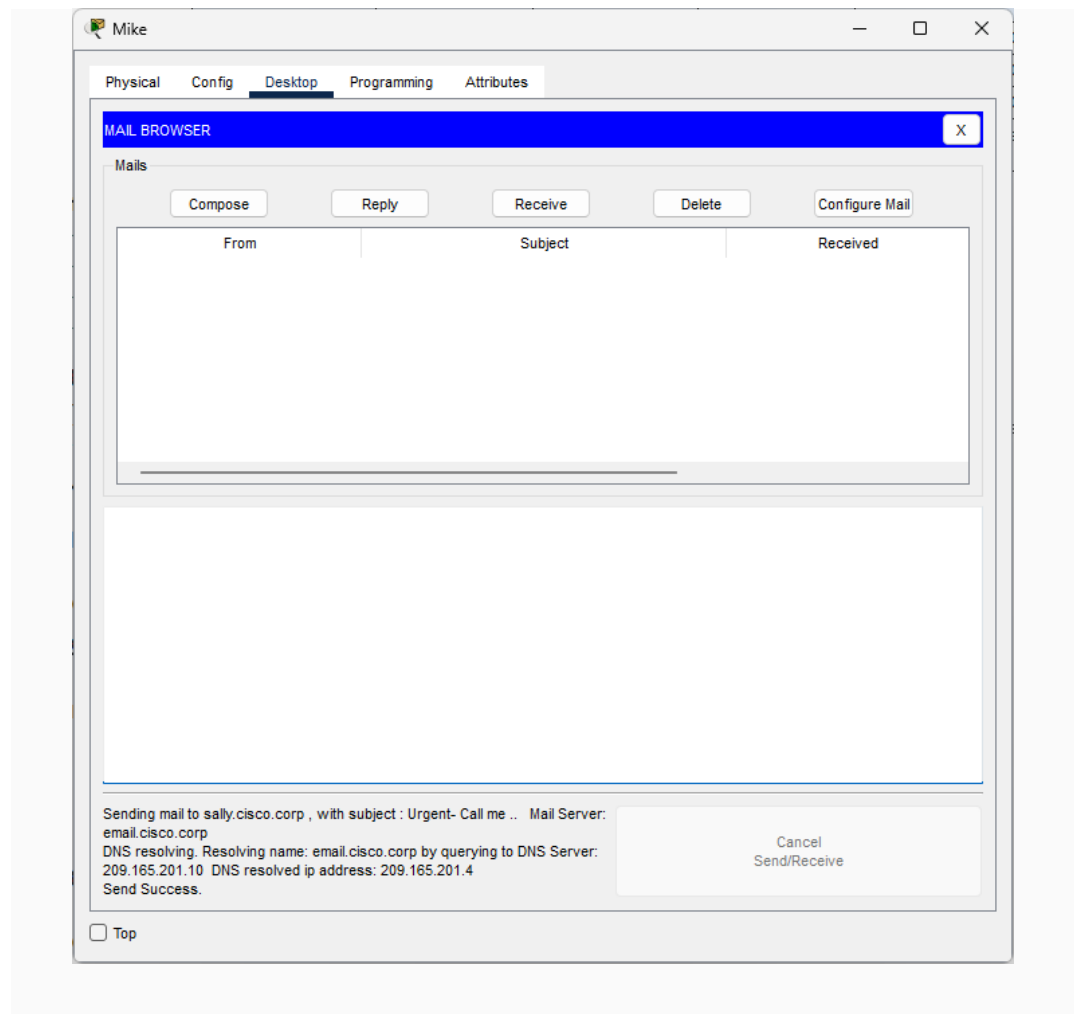
Compose Mail X

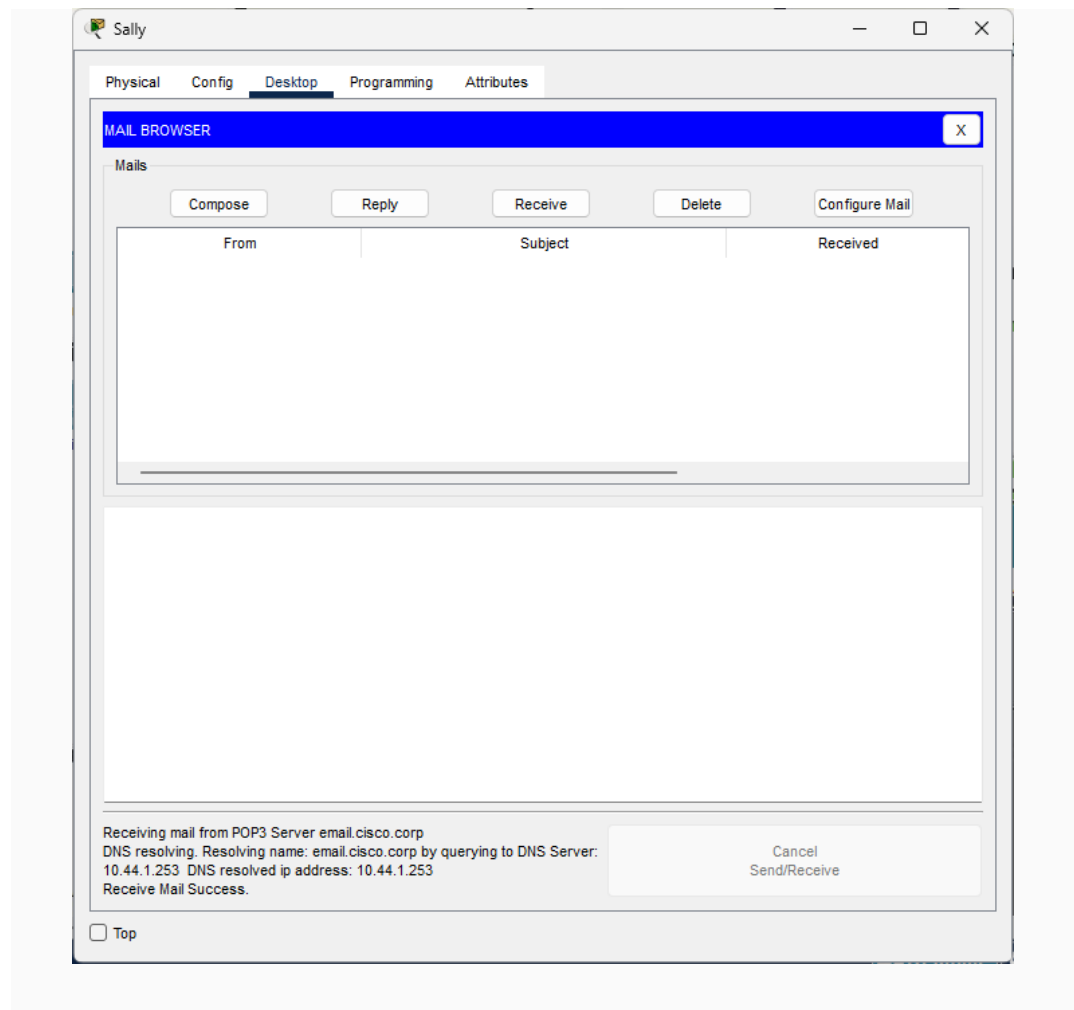
Send To: sally@cisco.corp

Subject: Urgent- Call me

Call me when you are free today to discuss the new sale.

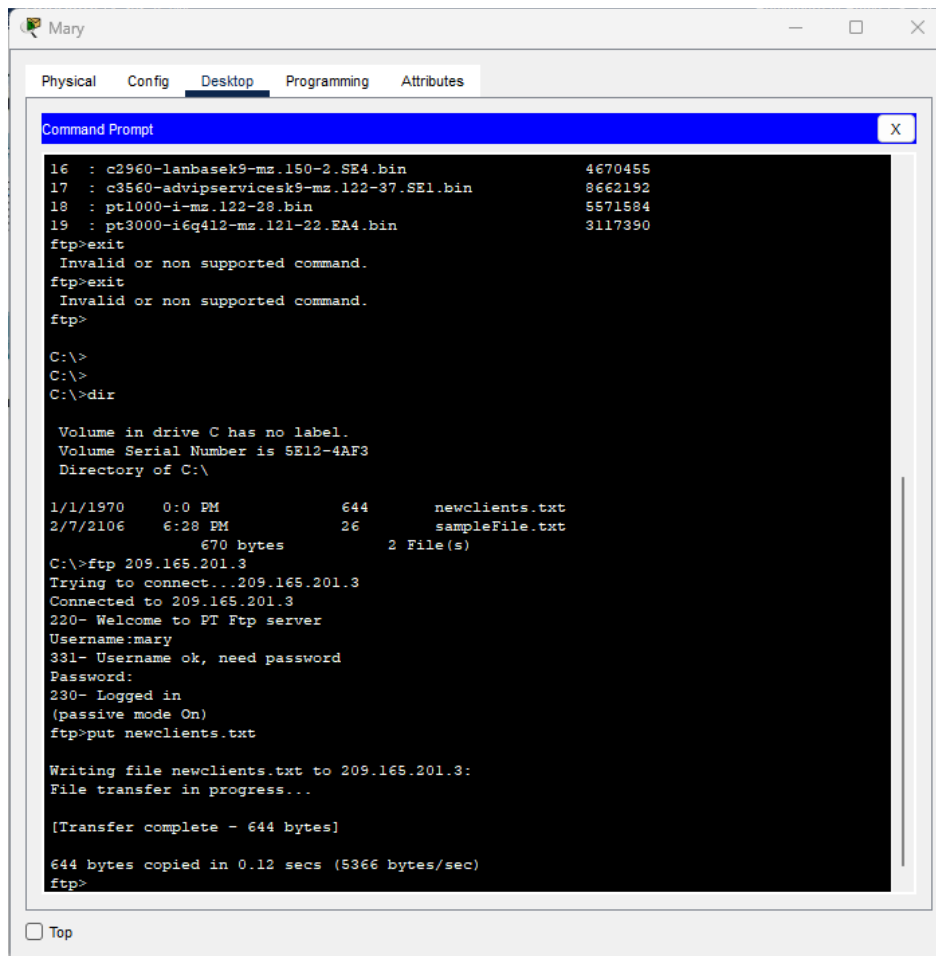
☐ Top





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



```
16 : c2960-lanbasek9-mz.150-2.SE4.bin          4670455
17 : c3560-advipservicesk9-mz.122-37.SE1.bin    8662192
18 : pt1000-i-mz.122-28.bin                     5571584
19 : pt3000-i6q412-mz.121-22.EA4.bin            3117390
ftp>exit
Invalid or non supported command.
ftp>exit
Invalid or non supported command.
ftp>

C:\>
C:\>
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970    0:0 PM             644      newclients.txt
2/7/2106    6:28 PM             26      sampleFile.txt
               670 bytes          2 File(s)
C:\>ftp 209.165.201.3
Trying to connect...209.165.201.3
Connected to 209.165.201.3
220- Welcome to FT Ftp server
Username:mary
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put newclients.txt

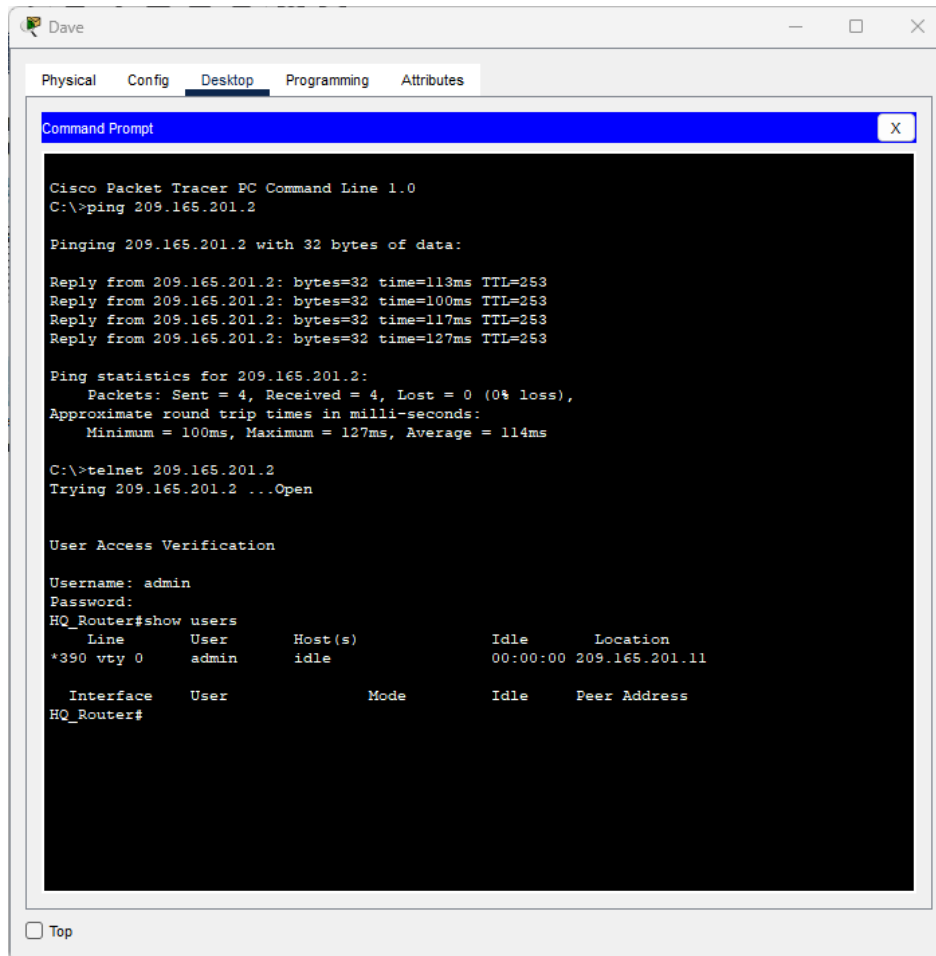
Writing file newclients.txt to 209.165.201.3:
File transfer in progress...

[Transfer complete - 644 bytes]

644 bytes copied in 0.12 secs (5366 bytes/sec)
ftp>
```

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



The screenshot shows a 'Command Prompt' window within a 'Dave' PC environment in Cisco Packet Tracer. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=113ms TTL=253
Reply from 209.165.201.2: bytes=32 time=100ms TTL=253
Reply from 209.165.201.2: bytes=32 time=117ms TTL=253
Reply from 209.165.201.2: bytes=32 time=127ms TTL=253

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 100ms, Maximum = 127ms, Average = 114ms

C:\>telnet 209.165.201.2
Trying 209.165.201.2 ...Open

User Access Verification

Username: admin
Password:
HQ_Router#show users
```

Line	User	Host(s)	Idle	Location
*390 vty 0	admin	idle	00:00:00	209.165.201.11

```

  Interface  User      Mode      Idle      Peer Address
HQ_Router#
```

At the bottom of the window, there is a 'Top' button.

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

The screenshot shows a 'Tim' window with a 'Command Prompt' tab. The command prompt displays the following text:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=131ms TTL=253
Reply from 209.165.201.2: bytes=32 time=126ms TTL=253
Reply from 209.165.201.2: bytes=32 time=117ms TTL=253
Reply from 209.165.201.2: bytes=32 time=134ms TTL=253

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 117ms, Maximum = 134ms, Average = 127ms

C:\>ssh -l admin 209.165.201.2

Password:
HQ_Router#show users
   Line    User      Host(s)      Idle      Location
  390 vty 0   admin     idle        00:09:00  209.165.201.11
 *391 vty 1   admin     idle        00:00:00
HQ_Router#
HQ_Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ_Router(config)#enable secret cisco
HQ_Router(config)#

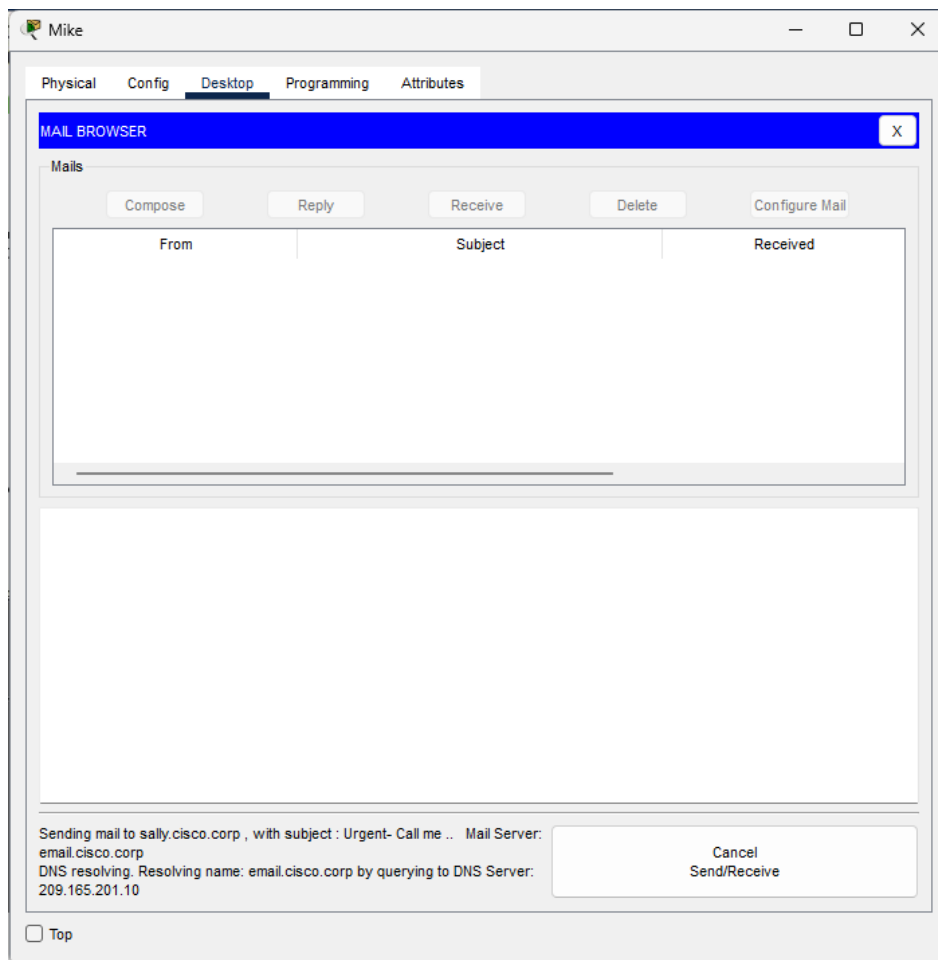
```

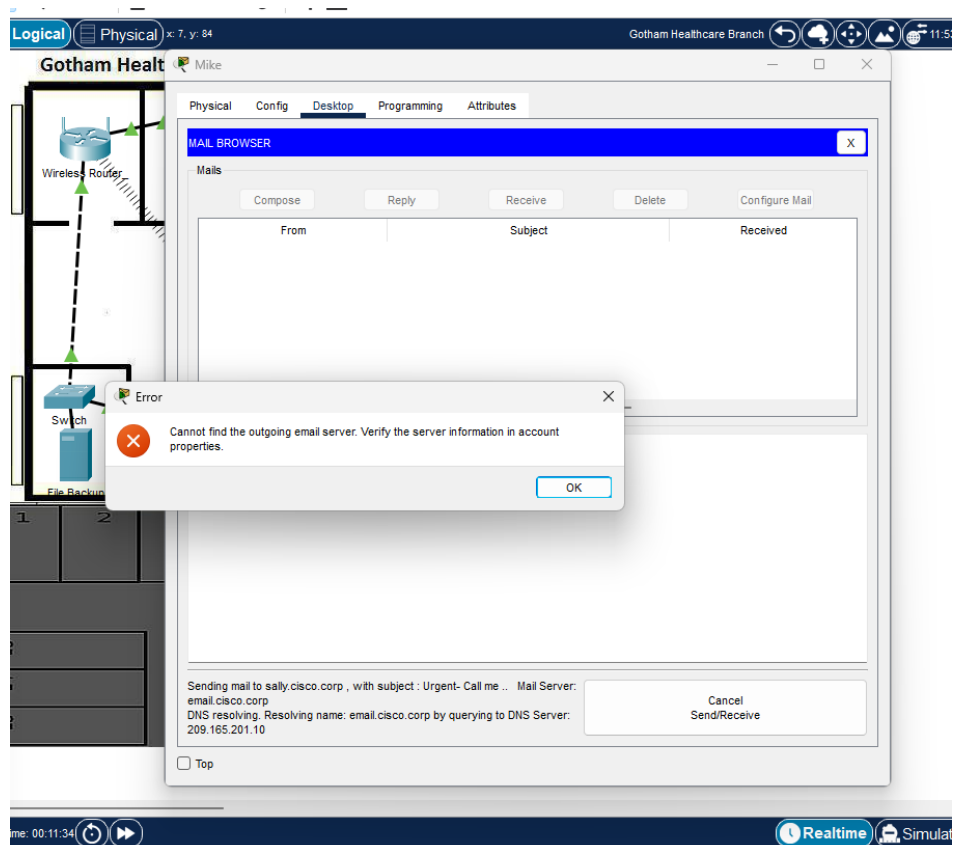
At the bottom of the window, there is a 'Top' button.

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





File Backup

Physical

Config

Services

Desktop

Programming

Attributes

IP Configuration

X

IP Configuration

DHCP

Static

IPv4 Address

10.44.2.254

Subnet Mask

255.255.255.0

Default Gateway

10.44.2.1

DNS Server

209.165.201.10

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::2D0:BCFF:FE14:4DA7

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication

MDS

Username

Password

Top

Mike

Physical

Config

Desktop

Programming

Attributes

IP Configuration

X

Interface

FastEthernet0

IP Configuration

DHCP

Static

IPv4 Address

10.44.2.10

Subnet Mask

255.255.255.0

Default Gateway

10.44.2.1

DNS Server

209.165.201.10

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::201:63FF:FE57:4D54

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication

MD5

Username

Password

Top

Email/DNS

Physical

Config

Services

Desktop

Programming

Attributes

IP Configuration

IP Configuration

DHCP

Static

IPv4 Address

10.44.1.253

Subnet Mask

255.255.255.0

Default Gateway

10.44.1.1

DNS Server

10.44.1.253

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::201:43FF:FEDA:ABB3

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication

MDS

Username

Password

Top

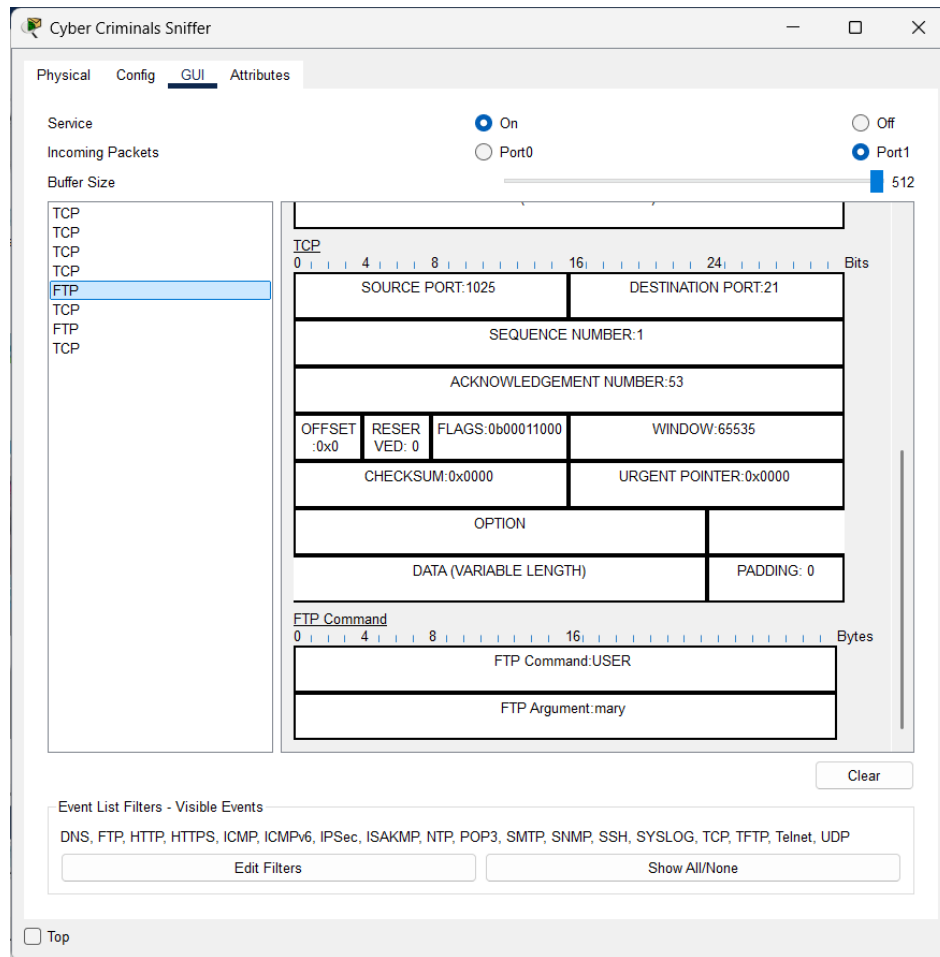
The screenshot shows a configuration window titled 'Sally' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying the 'IP Configuration' section. The interface is set to 'FastEthernet0'. Under 'IP Configuration', 'Static' is selected over 'DHCP'. The IPv4 settings are: IPv4 Address 10.44.1.11, Subnet Mask 255.255.255.0, Default Gateway 10.44.1.1, and DNS Server 10.44.1.253. Under 'IPv6 Configuration', 'Static' is selected over 'Automatic'. The IPv6 settings are: IPv6 Address (empty), Link Local Address FE80::2D0:D3FF:FEB0:C18E, Default Gateway (empty), and DNS Server (empty). The '802.1X' section has 'Use 802.1X Security' unchecked, 'Authentication' set to 'MD5', and 'Username' and 'Password' fields empty. A 'Top' button is at the bottom left.

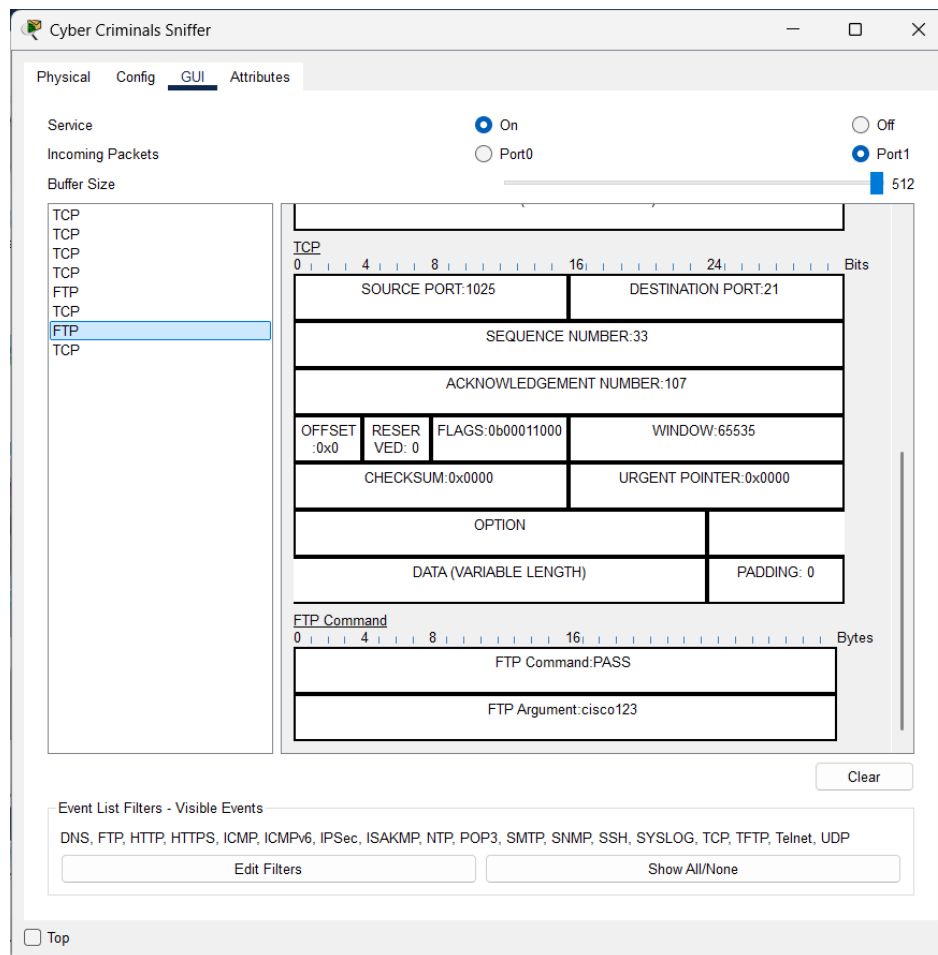
IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	10.44.1.11
Subnet Mask	255.255.255.0
Default Gateway	10.44.1.1
DNS Server	10.44.1.253
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::2D0:D3FF:FEB0:C18E
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

☐ Top

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





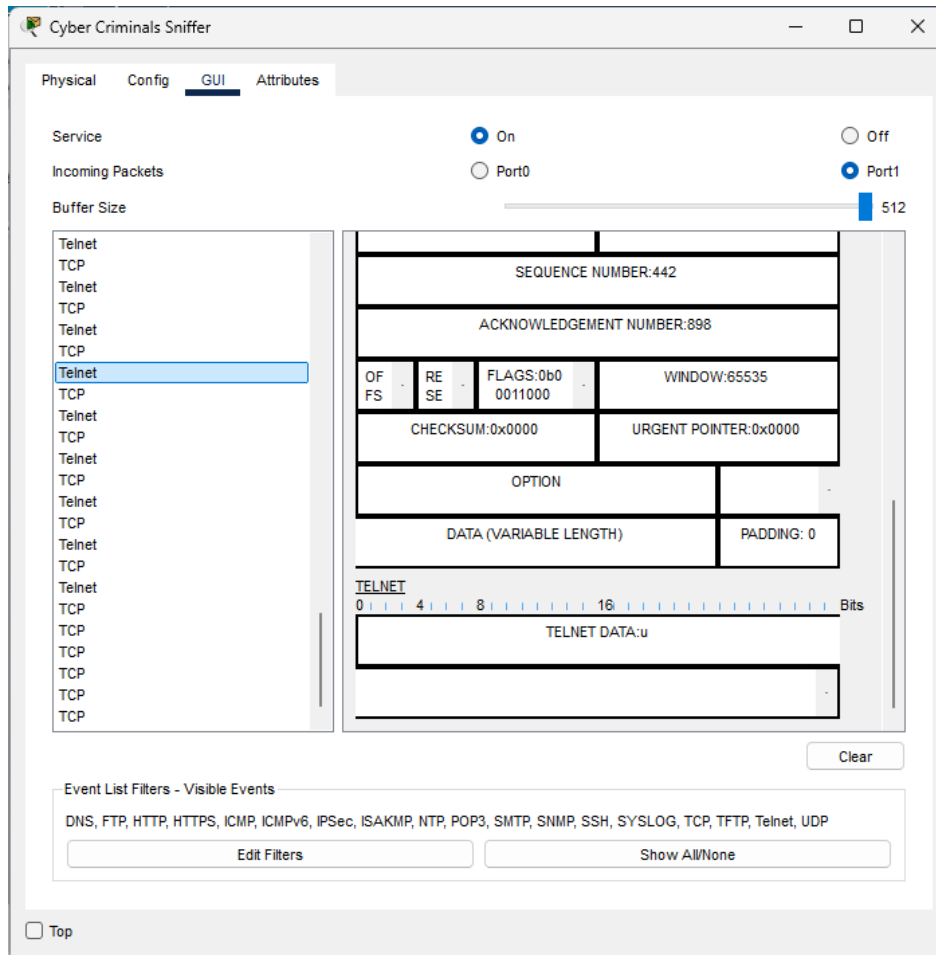
Why is FTP considered an insecure protocol for moving files?

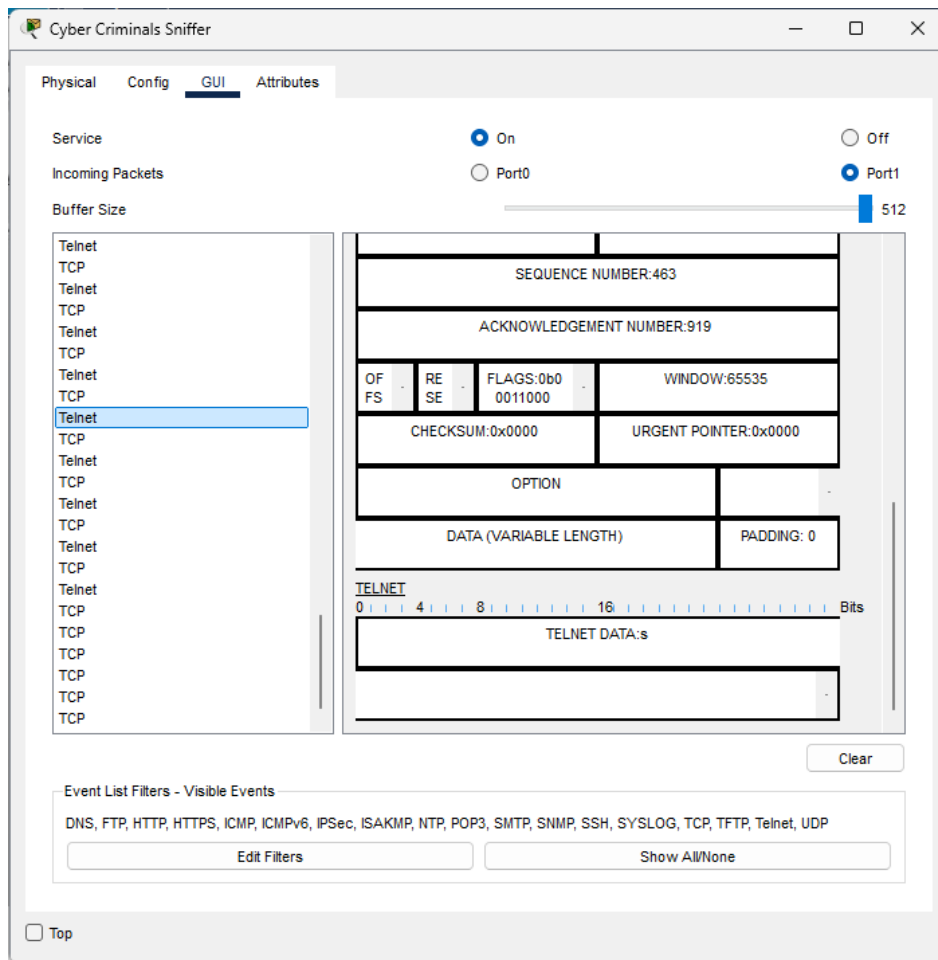
What information is displayed in clear text from the FTP header?

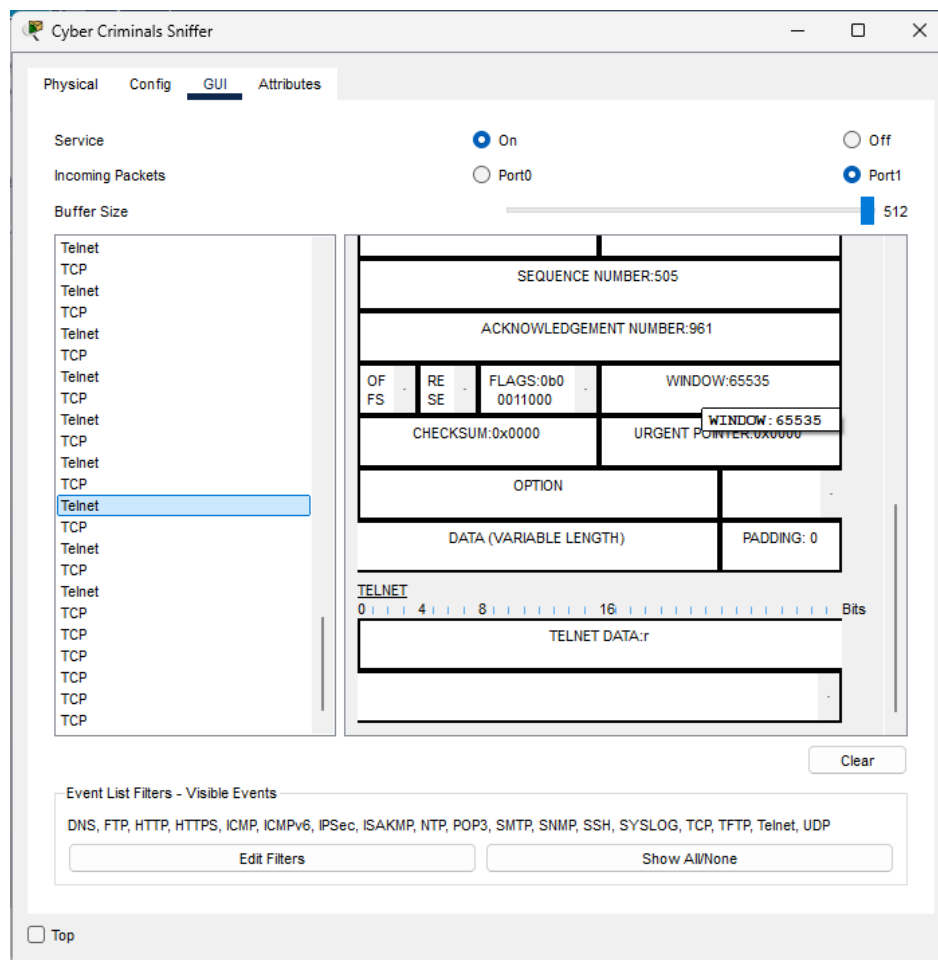
Besides the username, what other sensitive information is displayed in clear text from the FTP header?

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



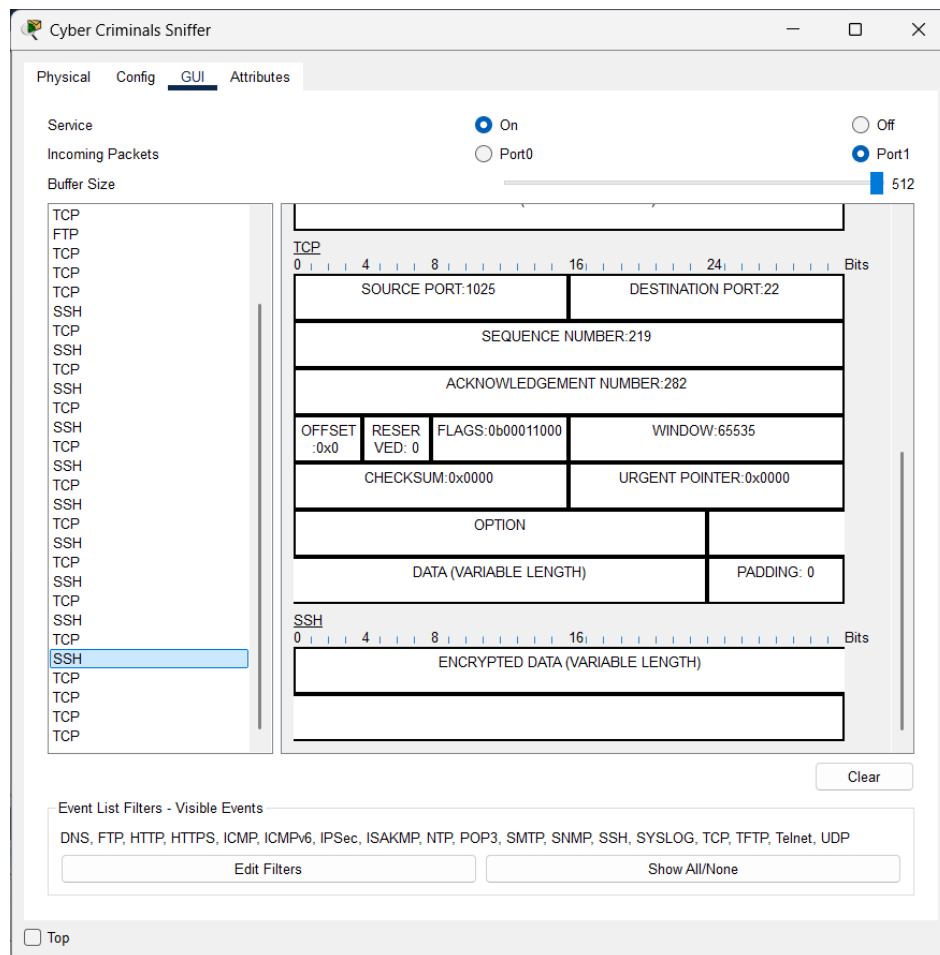




Why is Telnet considered an insecure protocol for remotely managing a device?

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.