Packet Tracer – Communicating in a Cyber World

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Email/DNS Server	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
NTP/AAA Server	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ
File Backup Server	10.44.2.254	N/A	255.255.255.0	Gotham Healthcare Branch

Objectives

Part 1: Send Email between Users

Part 2: Upload and Download Files using FTP

Part 3: Remotely Access an Enterprise Router using Telnet

Part 4: Remotely Access an Enterprise Router using SSH

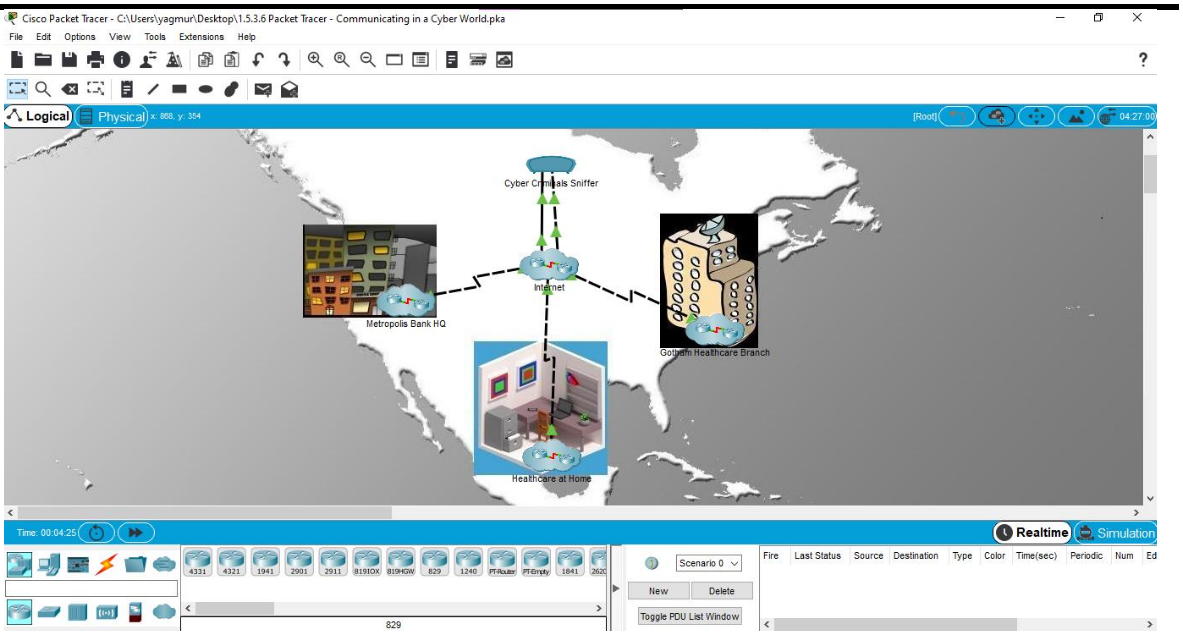
Background

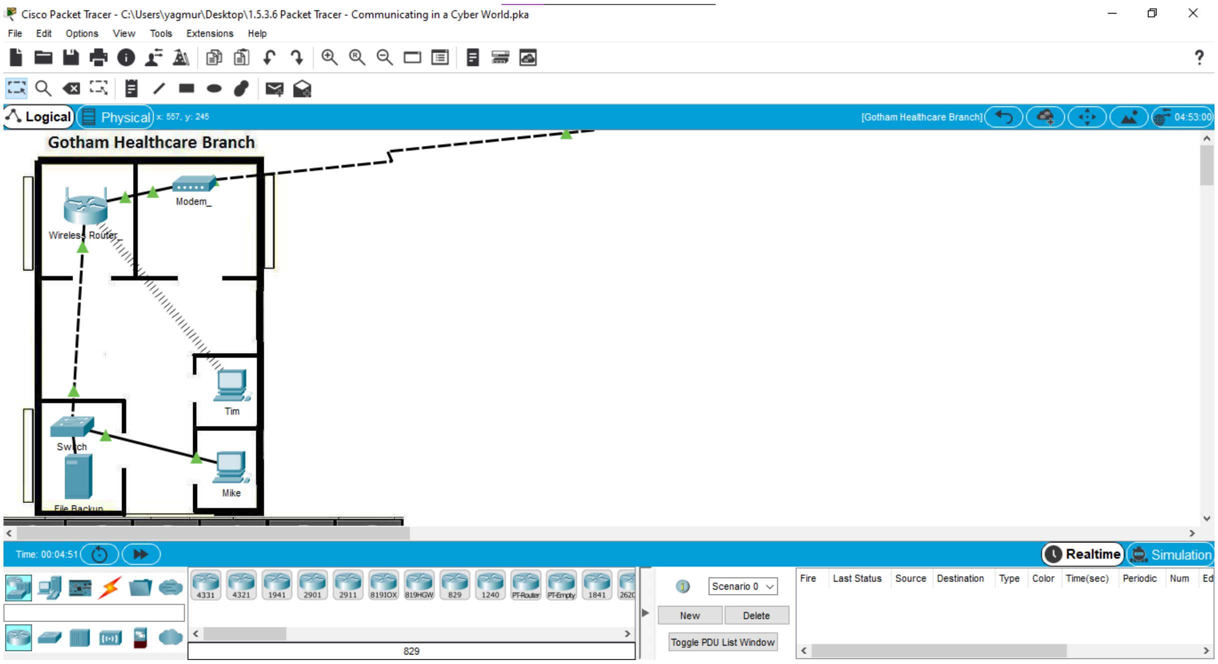
In this activity, you will communicate across remote networks using common network services. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to connect to both servers and other client devices.

Part 1: Send Email between Users

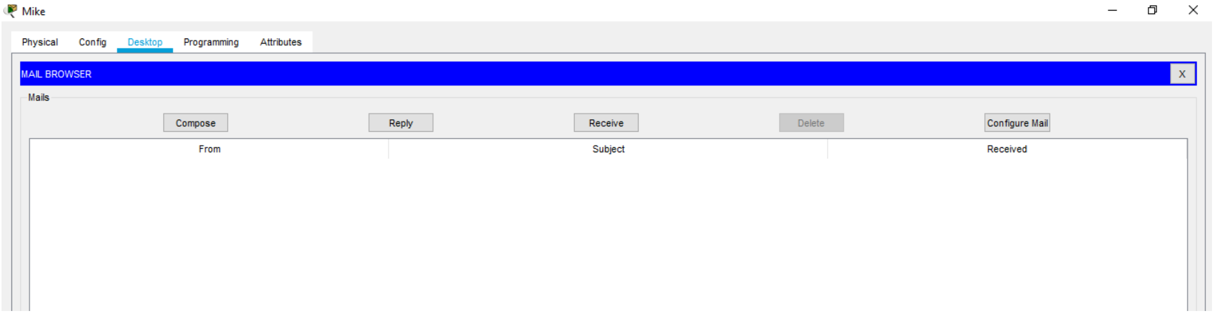
Step 1: Access the email client on Mike’s PC.

a. Click the **Gotham Healthcare Branch** site and then click the PC **Mike**.


Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 868, y: 354
[Root]
04:27:00
Cyber Criminals Sniffer
Internet
Metropolis Bank HQ
Gotham Healthcare Branch
Healthcare at Home
Time: 00:04:25
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
829
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed


Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 557, y: 245
[Gotham Healthcare Branch]
04:53:00
Gotham Healthcare Branch
Modem_
Wireless Router
Tim
Switch
Mike
File Backup
Time: 00:04:51
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
829
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed

b. Click the **Desktop** tab and then click **Email**.



Step 2: Send an email to Sally.

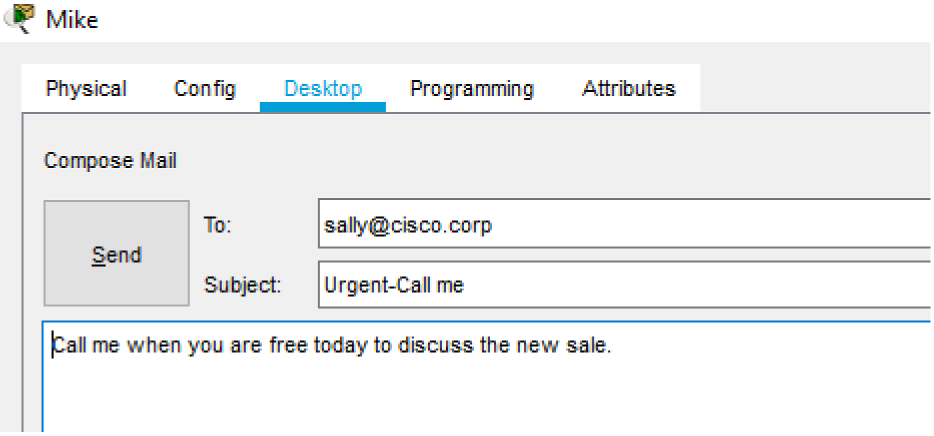
a. Create an email by clicking the **Compose** button.

b. In the **To:** field, enter the email sally@cisco.corp

In the **Subject:** field, enter the string of text “**Urgent- Call me**”.

In the **Message** section, enter. “**Call me when you are free today to discuss the new sale.**”

c. Click the **Send** button to transmit the email.



To: sally@cisco.corp

Subject: Urgent-Call me

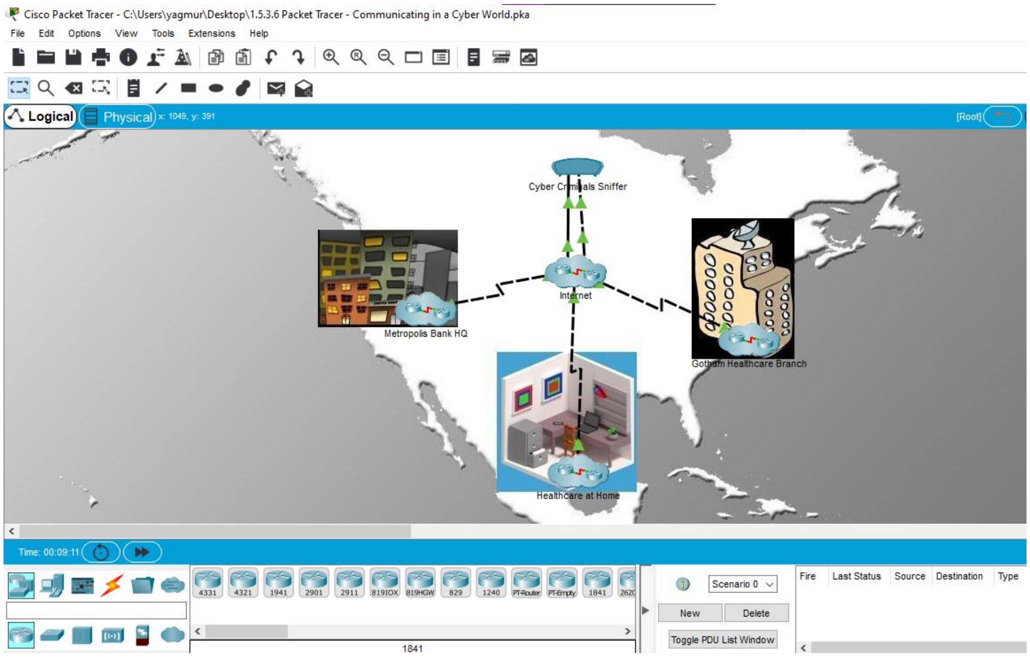
Call me when you are free today to discuss the new sale.

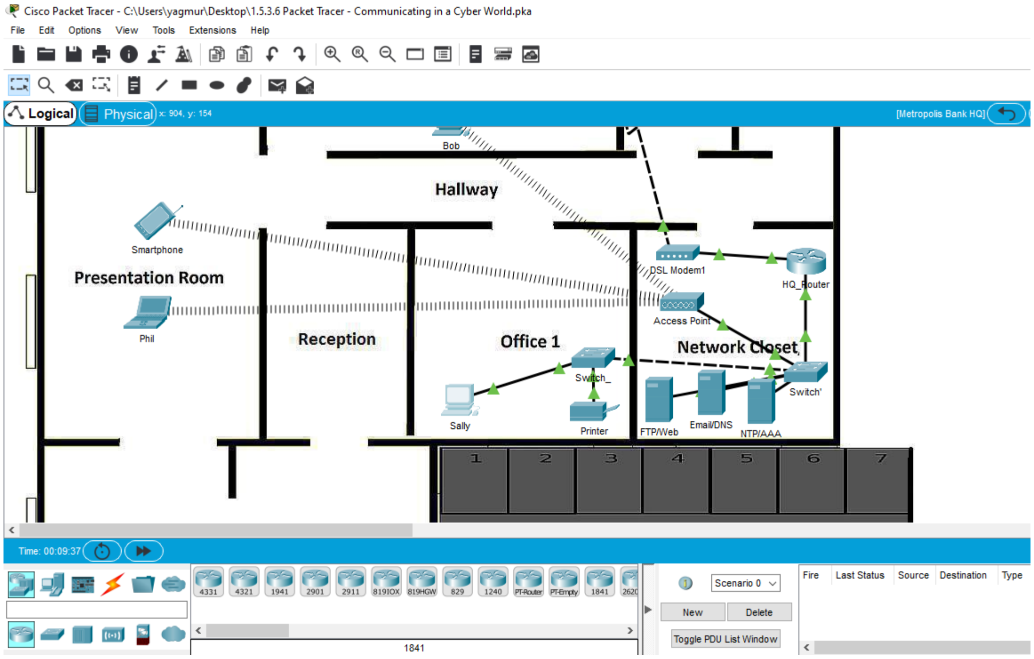
What protocol was used to send the email to the email server?

STMTP

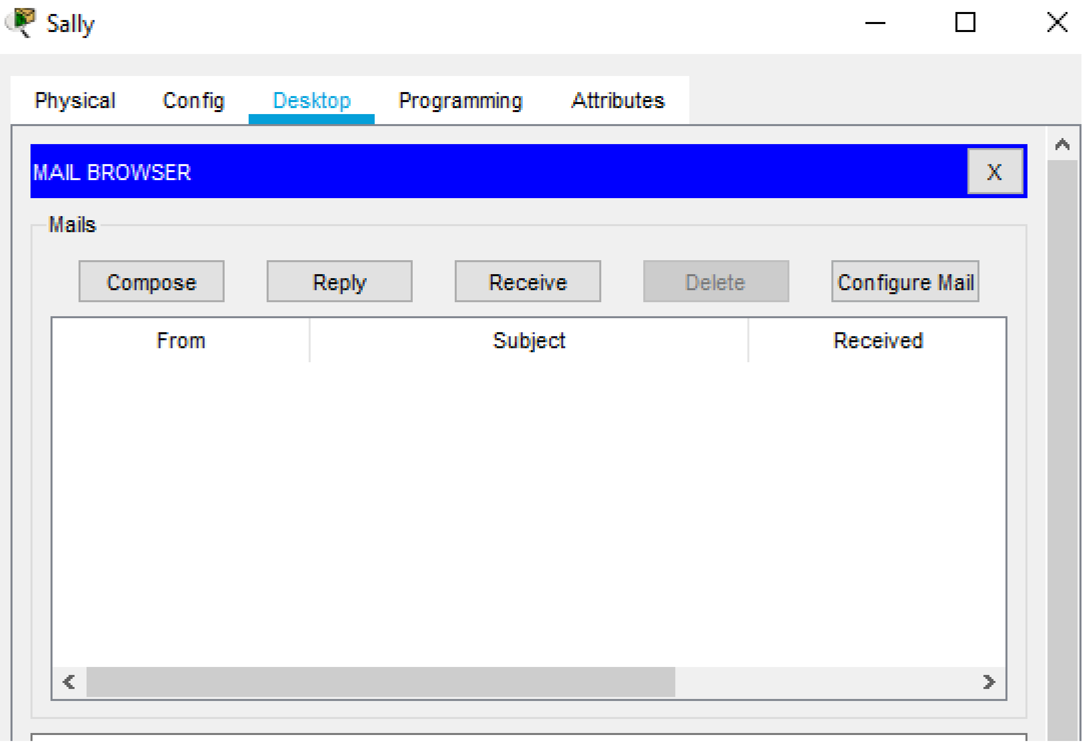
Step 3: Have Sally check her email.

a. Enter the **Metropolis Bank HQ** site and then click the PC **Sally**.

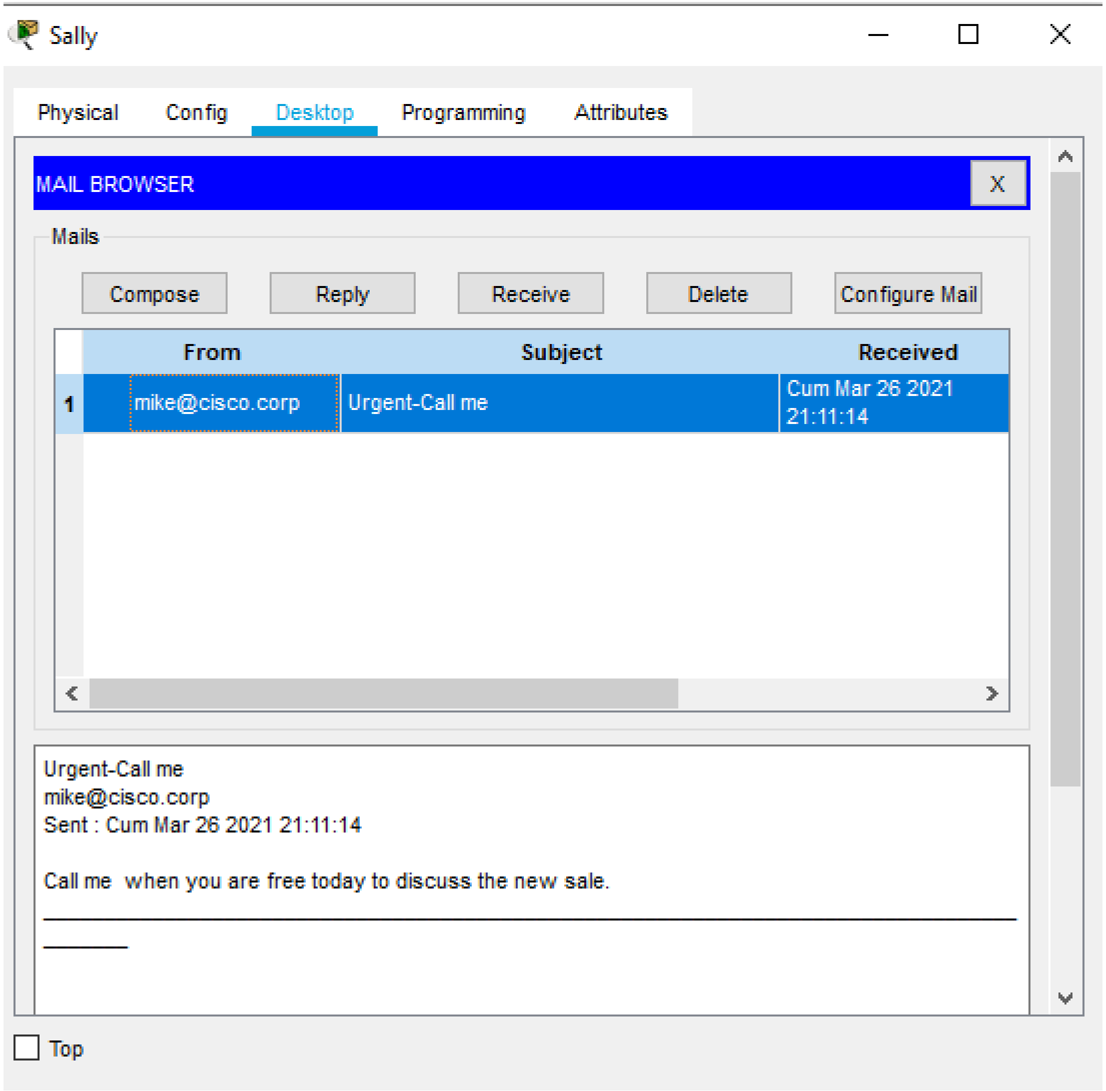




b. Click the **Desktop** tab and then click **Email**.



c. Click the **Receive** button to retrieve the email sent from Mike.



	From	Subject	Received
1	mike@cisco.corp	Urgent-Call me	Cum Mar 26 2021 21:11:14

Urgent-Call me
mike@cisco.corp
Sent : Cum Mar 26 2021 21:11:14

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

What protocol was used to retrieve the email from the email server?

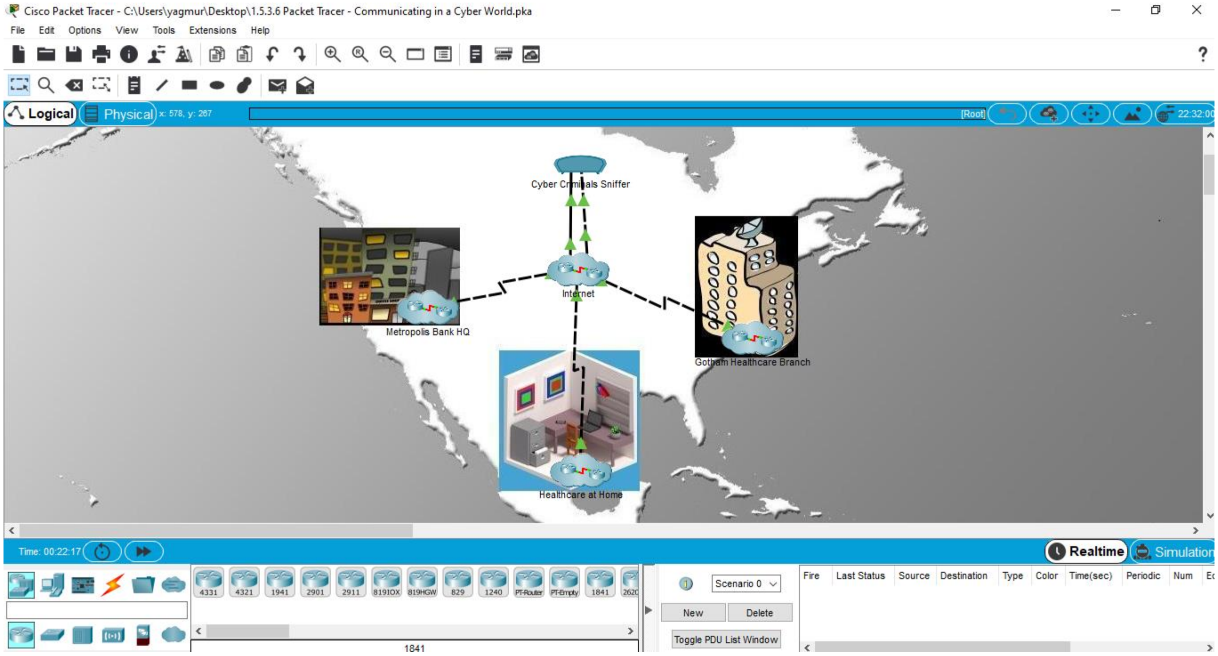
POP

Part 2: Upload Files using FTP

Step 1: Set the packet sniffer to capture traffic on the correct port.

a. Enter the geographic (root) view to see all three remote sites.

b. Click the **Cyber Criminals Sniffer**.

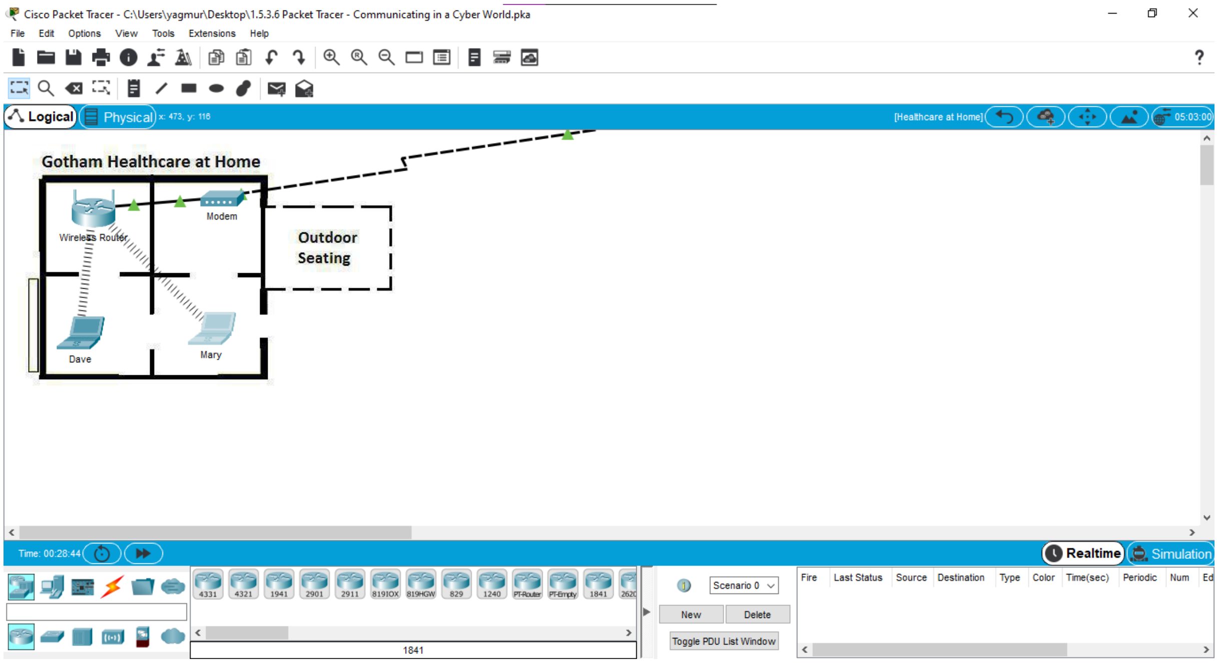

Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 578, y: 287
[Root]
22:32:00
Cyber Criminals Sniffer
Internet
Metropolis Bank HQ
Gotham Healthcare Branch
Healthcare at Home
Time: 00:22:17
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
1841
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed

c. Click **Port1** to capture packets on this port.

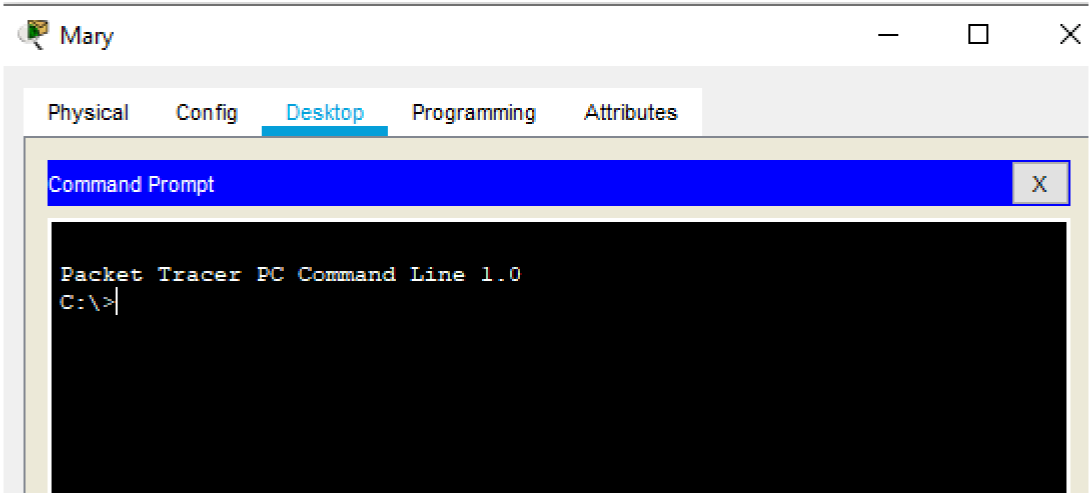
d. Leave the **Cyber Criminal Sniffer** open and visible for the rest of this part.

Step 2: Remotely connect to the FTP server.

e. Enter the **Healthcare at Home** site and then click the PC **Mary**.


Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 473, y: 116
[Healthcare at Home]
05:03:00
Gotham Healthcare at Home
Modem
Wireless Router
Outdoor Seating
Dave
Mary
Time: 00:28:44
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
1841
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed

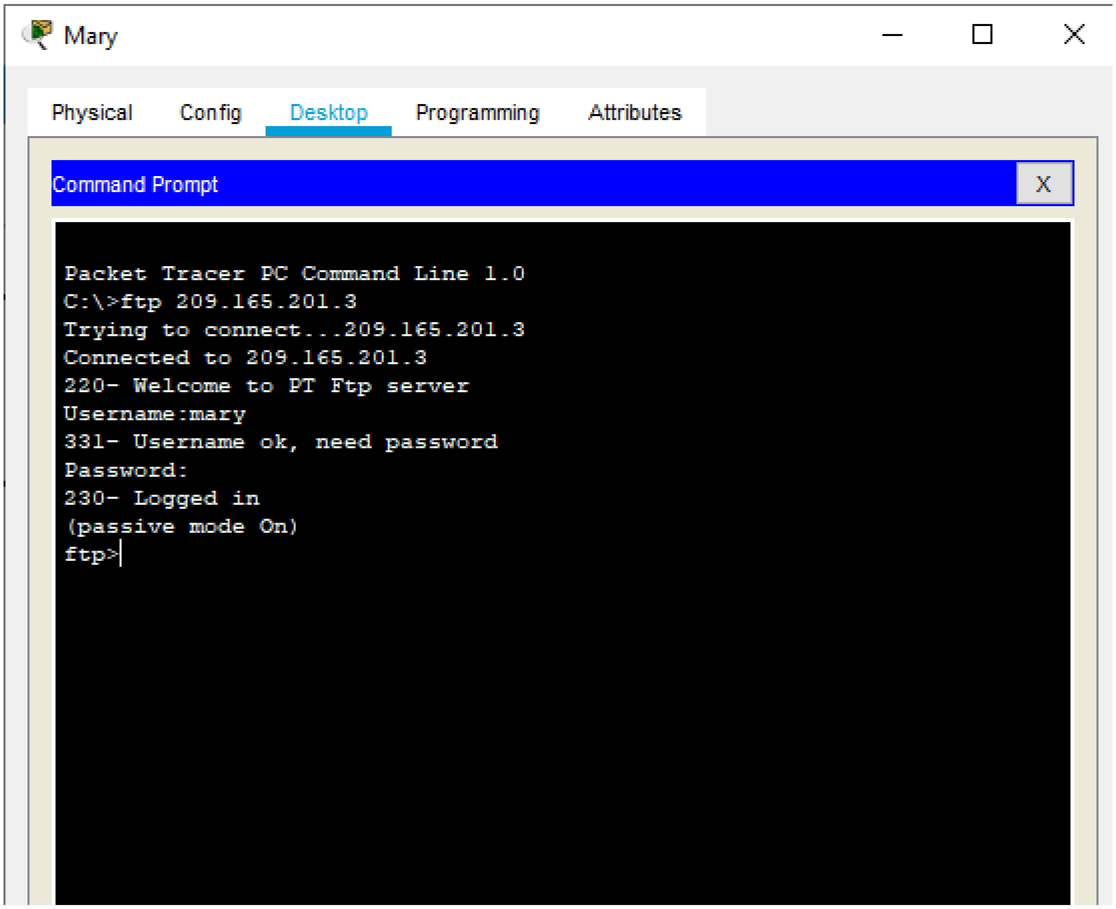
f. Click the **Desktop** tab and then click **Command Prompt**.



```
Packet Tracer PC Command Line 1.0
C:\>
```

g. Connect to the **FTP/Web** server at **Metropolis Bank HQ** by entering **ftp 209.165.201.3** in the command prompt.

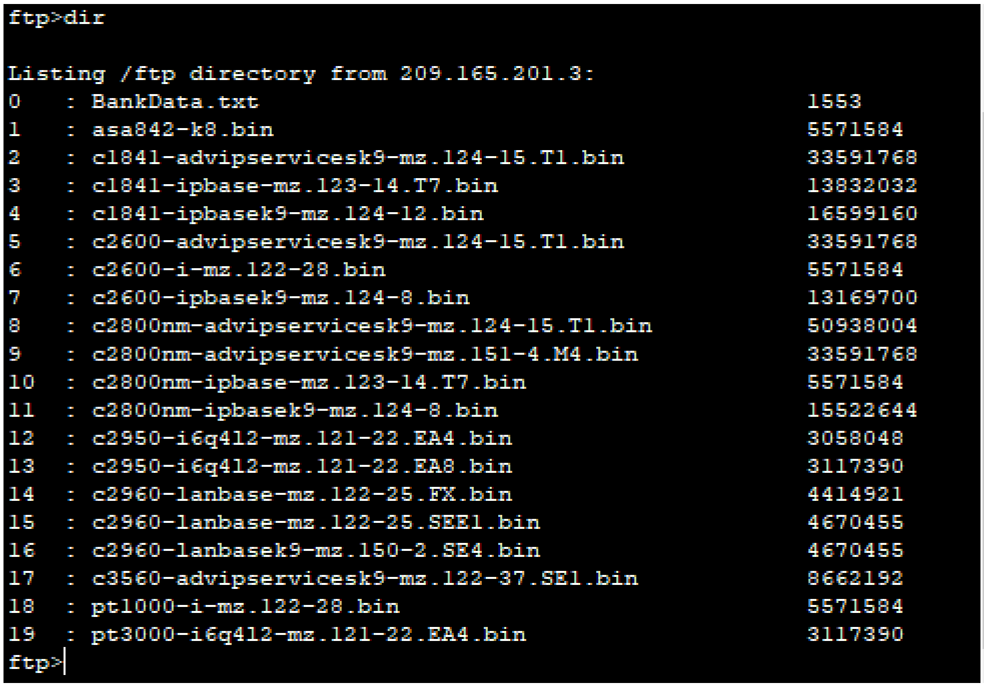
h. Enter the username of **mary** and a password of **cisco123**.



```
Packet Tracer PC Command Line 1.0
C:\>ftp 209.165.201.3
Trying to connect...209.165.201.3
Connected to 209.165.201.3
220- Welcome to PT Ftp server
Username:mary
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

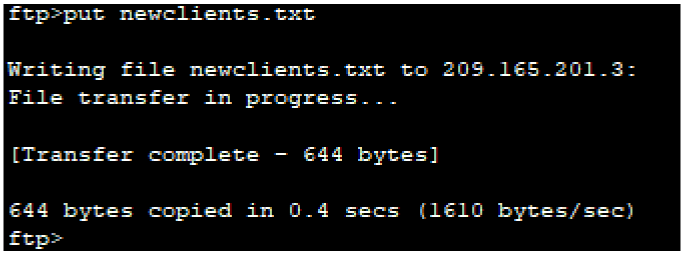
Step 3: Upload a file to the FTP server.

a. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the remote FTP server.



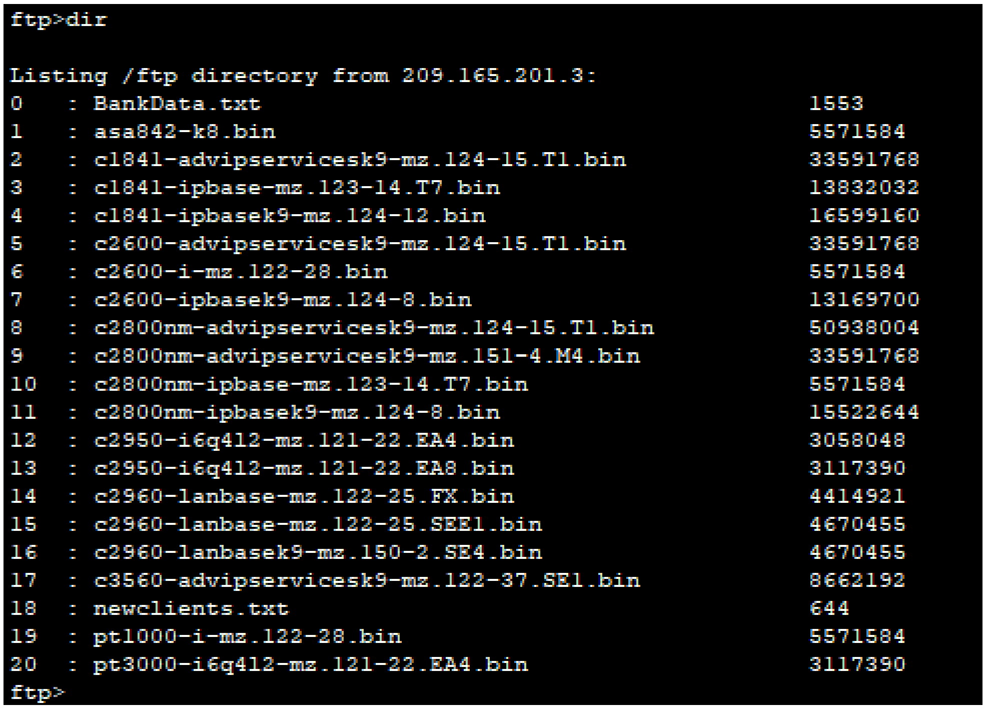
```
ftp>dir

Listing /ftp directory from 209.165.201.3:
0   : BankData.txt                                       1553
1   : asa842-k8.bin                                      5571584
2   : c1841-advipservicesk9-mz.124-15.T1.bin             33591768
3   : c1841-ipbase-mz.123-14.T7.bin                      13832032
4   : c1841-ipbasek9-mz.124-12.bin                       16599160
5   : c2600-advipservicesk9-mz.124-15.T1.bin             33591768
6   : c2600-i-mz.122-28.bin                              5571584
7   : c2600-ipbasek9-mz.124-8.bin                        13169700
8   : c2800nm-advipservicesk9-mz.124-15.T1.bin           50938004
9   : c2800nm-advipservicesk9-mz.151-4.M4.bin            33591768
10  : c2800nm-ipbase-mz.123-14.T7.bin                    5571584
11  : c2800nm-ipbasek9-mz.124-8.bin                      15522644
12  : c2950-i6q4l2-mz.121-22.EA4.bin                     3058048
13  : c2950-i6q4l2-mz.121-22.EA8.bin                     3117390
14  : c2960-lanbase-mz.122-25.FX.bin                     4414921
15  : c2960-lanbase-mz.122-25.SEE1.bin                   4670455
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-i6q4l2-mz.121-22.EA4.bin                    3117390
ftp>
```

b. Mary has a file containing sensitive information regarding new healthcare client information. Upload the **newclients.txt** file to the FTP server by entering the command **put newclients.txt**.



```
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 0.4 secs (1610 bytes/sec)
ftp>
```

c. At the **ftp>** prompt, enter the command **dir** and verify the **newclients.txt** file is now on the FTP server.



```
ftp>dir

Listing /ftp directory from 209.165.201.3:
0    : BankData.txt                                         1553
1    : asa842-k8.bin                                        5571584
2    : c1841-advipservicesk9-mz.124-15.T1.bin               33591768
3    : c1841-ipbase-mz.123-14.T7.bin                        13832032
4    : c1841-ipbasek9-mz.124-12.bin                         16599160
5    : c2600-advipservicesk9-mz.124-15.T1.bin               33591768
6    : c2600-i-mz.122-28.bin                                5571584
7    : c2600-ipbasek9-mz.124-8.bin                          13169700
8    : c2800nm-advipservicesk9-mz.124-15.T1.bin             50938004
9    : c2800nm-advipservicesk9-mz.151-4.M4.bin              33591768
10   : c2800nm-ipbase-mz.123-14.T7.bin                      5571584
11   : c2800nm-ipbasek9-mz.124-8.bin                        15522644
12   : c2950-i6q4l2-mz.121-22.EA4.bin                       3058048
13   : c2950-i6q4l2-mz.121-22.EA8.bin                       3117390
14   : c2960-lanbase-mz.122-25.FX.bin                       4414921
15   : c2960-lanbase-mz.122-25.SEE1.bin                     4670455
16   : c2960-lanbasek9-mz.150-2.SE4.bin                     4670455
17   : c3560-advipservicesk9-mz.122-37.SE1.bin              8662192
18   : newclients.txt                                       644
19   : pt1000-i-mz.122-28.bin                               5571584
20   : pt3000-i6q4l2-mz.121-22.EA4.bin                      3117390
ftp>
```

Why is FTP considered an insecure protocol for moving files?

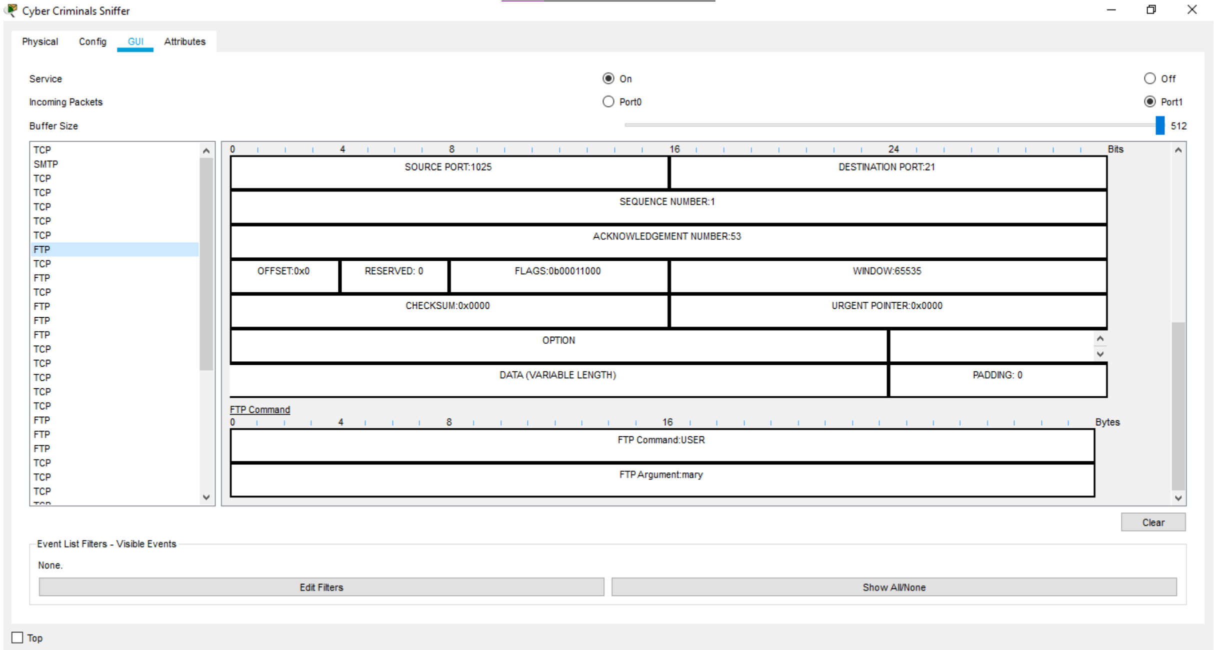
FTP does not provide encryption and all data is sent in clear text.

Step 4: Analyze the FTP traffic.

a. Enter the geographic (root) view to see all three remote sites.

b. Click the **Cyber Criminals Sniffer**.

c. Under the GUI tab on the left, click the 1st FTP packet available to select it. Then scroll down to the bottom of the window displayed on the right.



Cyber Criminals Sniffer

Service: ● On ○ Off
Incoming Packets: ○ Port0 ● Port1
Buffer Size: 512

SOURCE PORT:1025
DESTINATION PORT:21
SEQUENCE NUMBER:1
ACKNOWLEDGEMENT NUMBER:53
OFFSET:0x0
RESERVED: 0
FLAGS:0b00011000
WINDOW:65535
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0

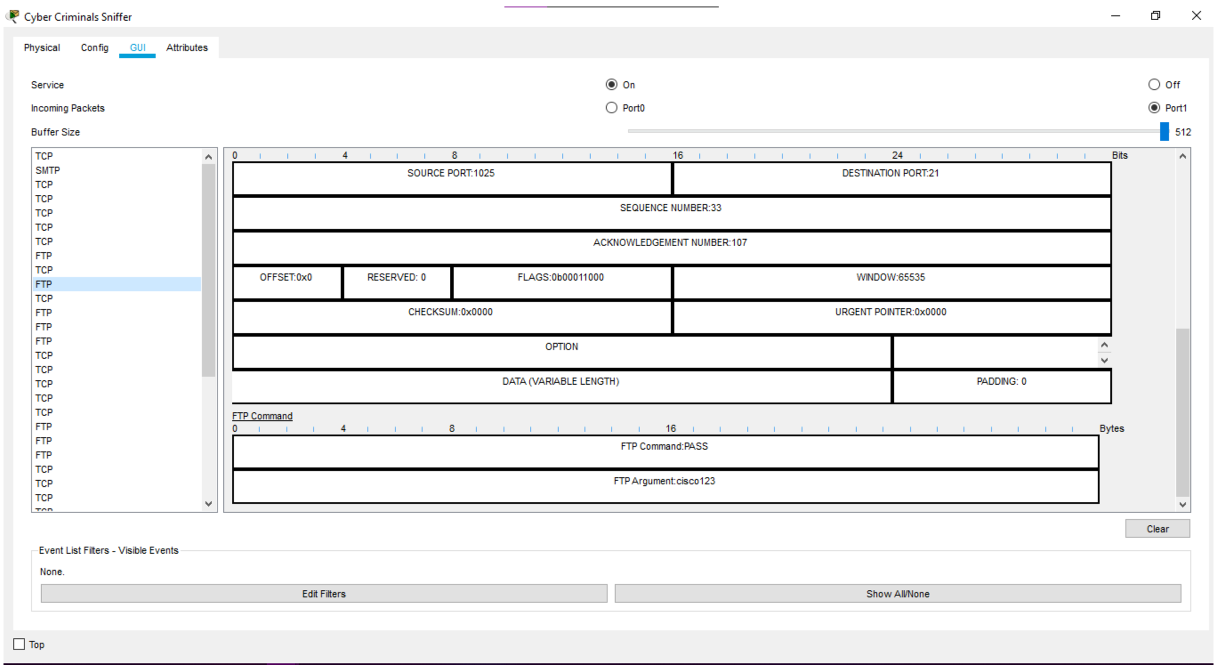
FTP Command
FTP Command:USER
FTP Argument:mary

Event List Filters - Visible Events
None.

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

The username used by the client to connect to the FTP server.

d. On the left, click the 2nd FTP packet available to select it. Then scroll down to the bottom of the window displayed on the right. Do this again for the 3rd FTP packet.



Cyber Criminals Sniffer

Physical | Config | GUI | Attributes

Service: ● On ○ Off
Incoming Packets: ○ Port0 ● Port1
Buffer Size: 512

```
TCP
SMTP
TCP
TCP
TCP
TCP
TCP
FTP
TCP
FTP
TCP
FTP
FTP
FTP
TCP
TCP
TCP
TCP
TCP
FTP
FTP
FTP
TCP
TCP
TCP
```

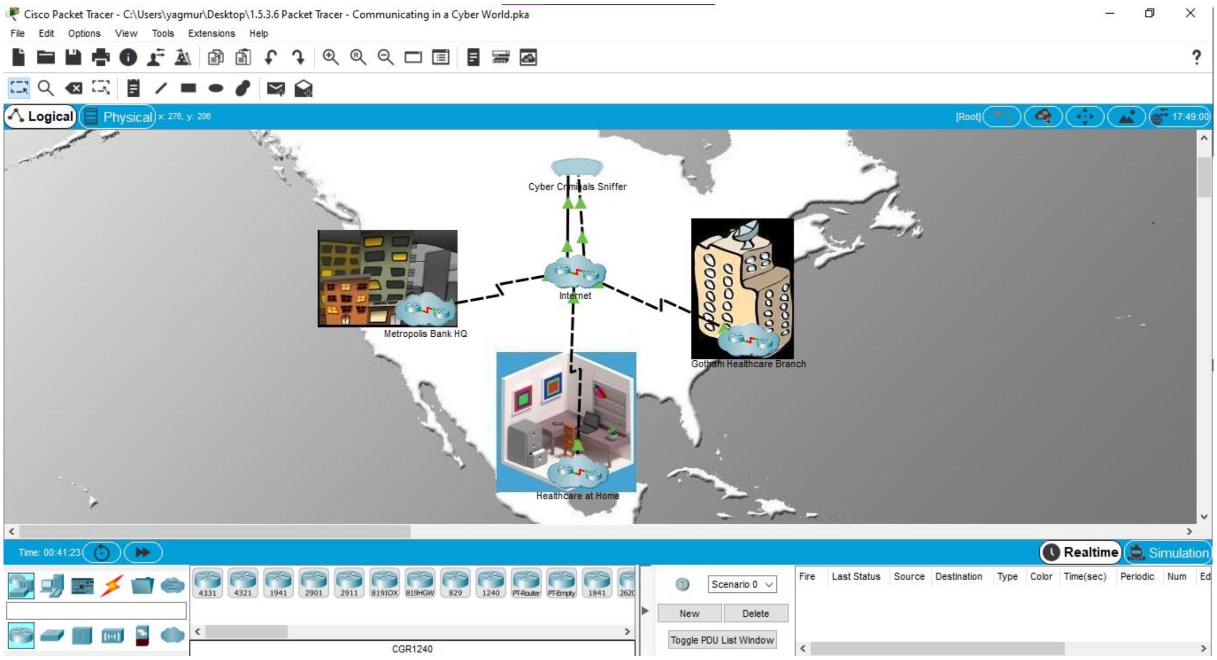
SOURCE PORT:1025			DESTINATION PORT:21
SEQUENCE NUMBER:33			
ACKNOWLEDGEMENT NUMBER:107			
OFFSET:0x0	RESERVED: 0	FLAGS:0b00011000	WINDOW:65535
CHECKSUM:0x0000			URGENT POINTER:0x0000
OPTION			
DATA (VARIABLE LENGTH)			PADDING: 0

FTP Command

FTP Command:PASS
FTP Argument:cisco123

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

The password used by the client to connect to the FTP server.

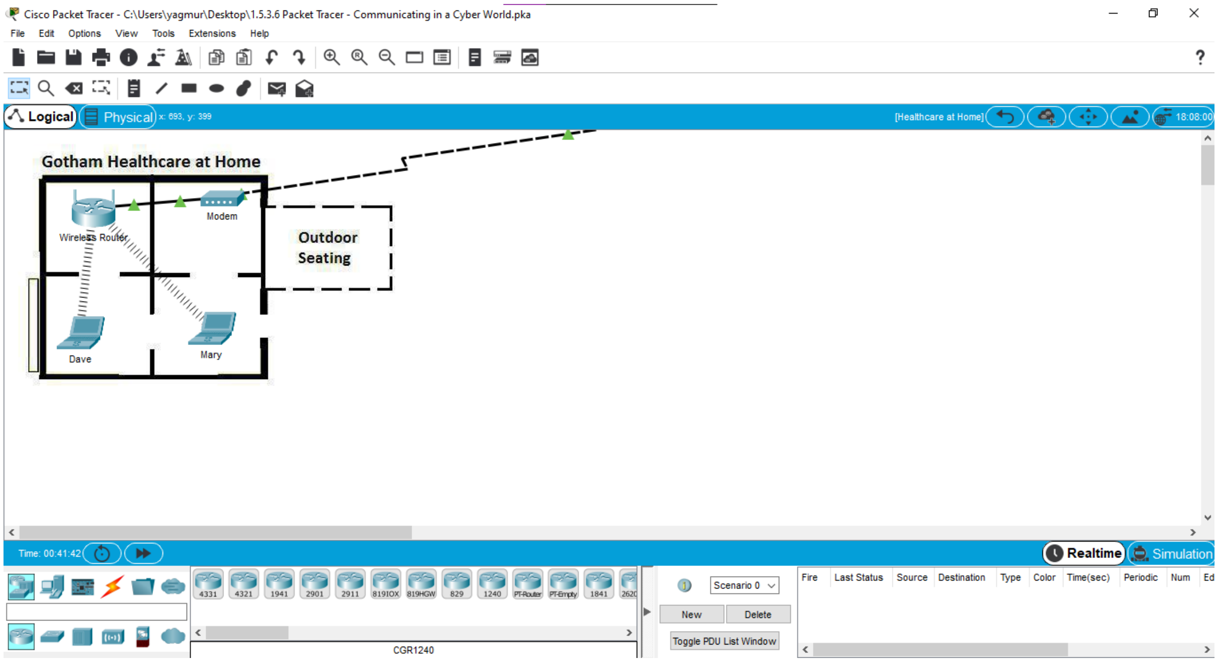


Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka

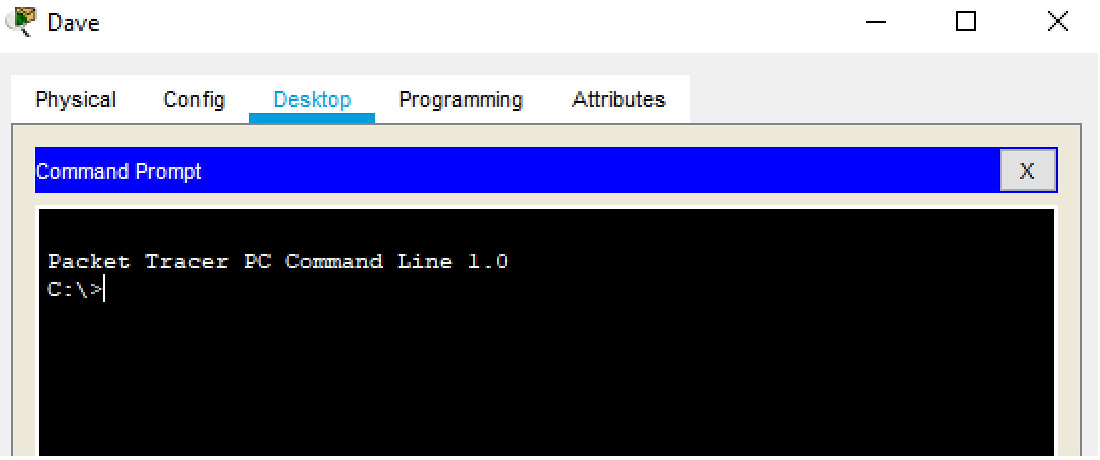
Part 3: Remotely Access an Enterprise Router Using Telnet

Step 1: Remotely connect to an enterprise router.

a. Enter the **Healthcare at Home** site and then click on the PC **Dave**.

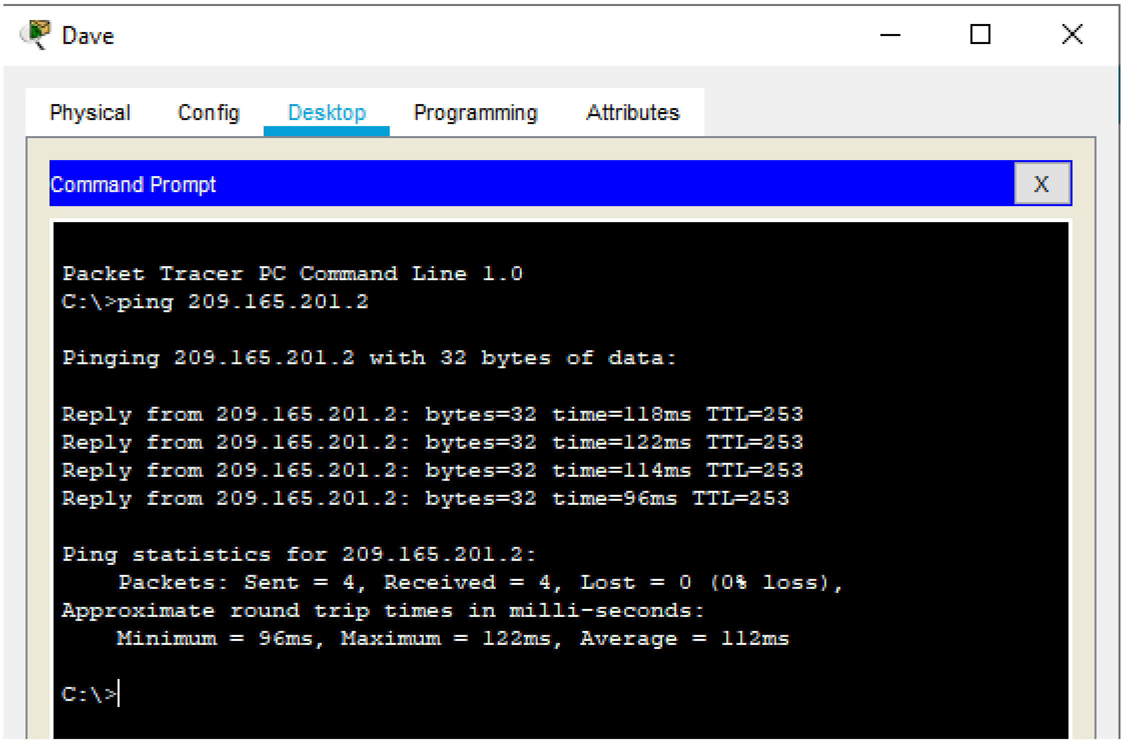

Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 693, y: 399
[Healthcare at Home]
18:08:00
Gotham Healthcare at Home
Wireless Router
Modem
Outdoor Seating
Dave
Mary
Time: 00:41:42
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
CGR1240
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed

b. Click the **Desktop** tab and then click **Command Prompt**.



```
Packet Tracer PC Command Line 1.0
C:\>
```

c. Ping the enterprise router using the command **ping 209.165.201.2** to verify reachability.

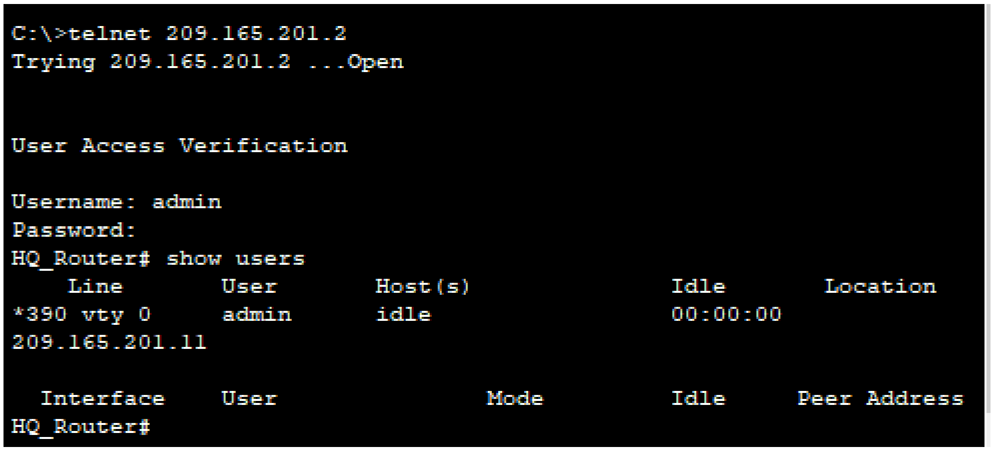


```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=118ms TTL=253
Reply from 209.165.201.2: bytes=32 time=122ms TTL=253
Reply from 209.165.201.2: bytes=32 time=114ms TTL=253
Reply from 209.165.201.2: bytes=32 time=96ms 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 = 96ms, Maximum = 122ms, Average = 112ms

C:\>
```

d. Use the command **telnet 209.165.201.2** to telnet to the IP address of the enterprise router.

e. Authenticate to the enterprise router with the username of **admin** and the password of **cisco123**.

f. Use the command **show users** to view the active Telnet connection to the enterprise router.



```
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#
```

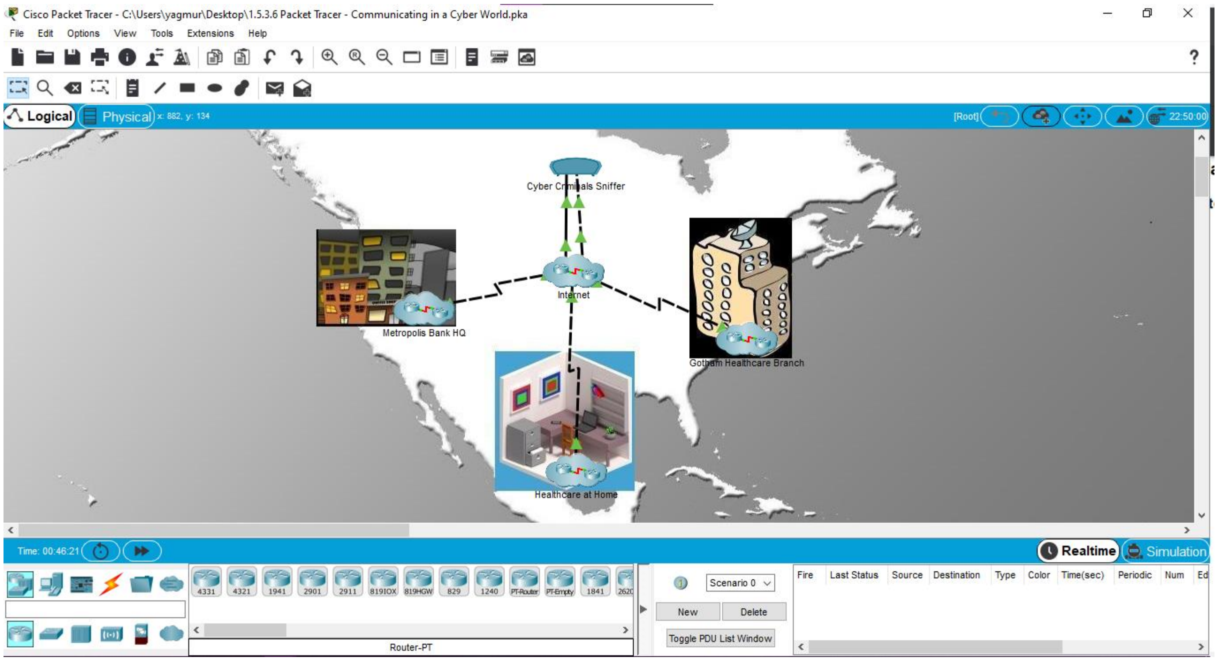
Why is Telnet considered an insecure protocol for remotely managing a device?

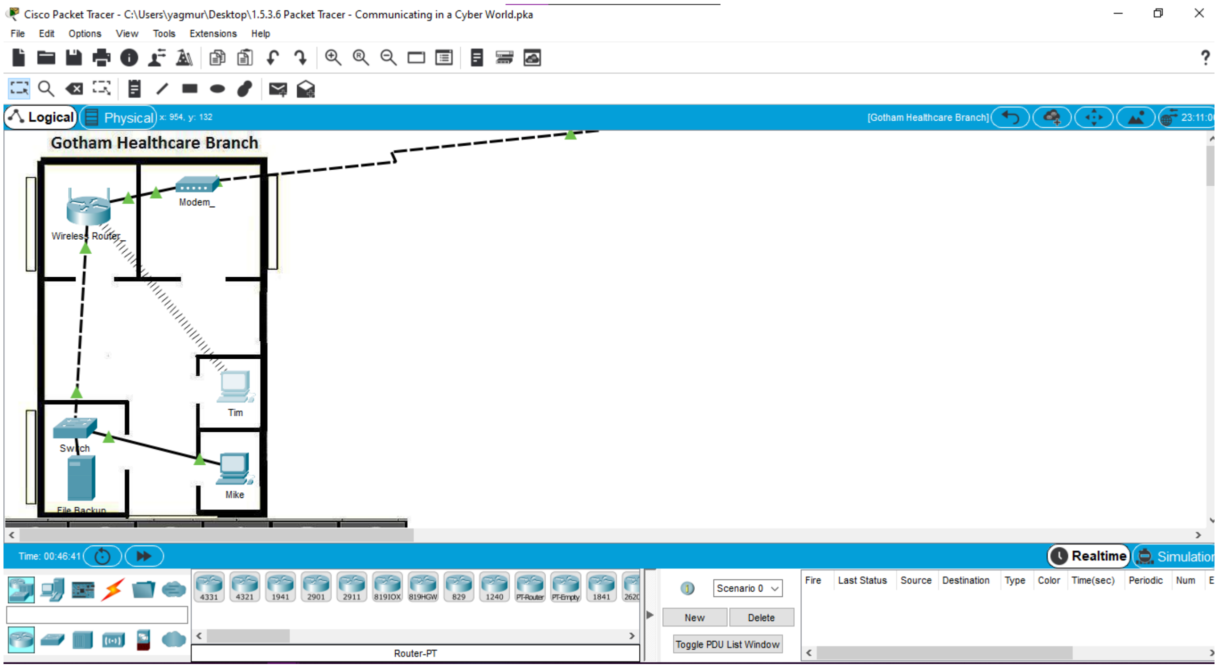
Telnet does not provide encryption and all data is sent in clear text.

Part 4: Remotely Access an Enterprise Router Using SSH

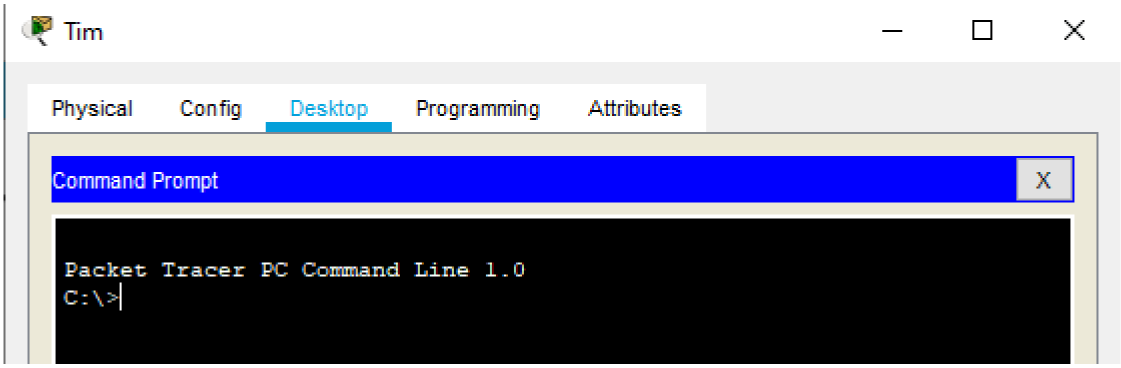
Step 1: Remotely connect to an enterprise router.

a. Enter the **Gotham Healthcare Branch** site and then click the PC **Tim**.


Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 882, y: 134
[Root]
22:50:00
Cyber Criminals Sniffer
Internet
Metropolis Bank HQ
Gotham Healthcare Branch
Healthcare at Home
Time: 00:46:21
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
Router-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed

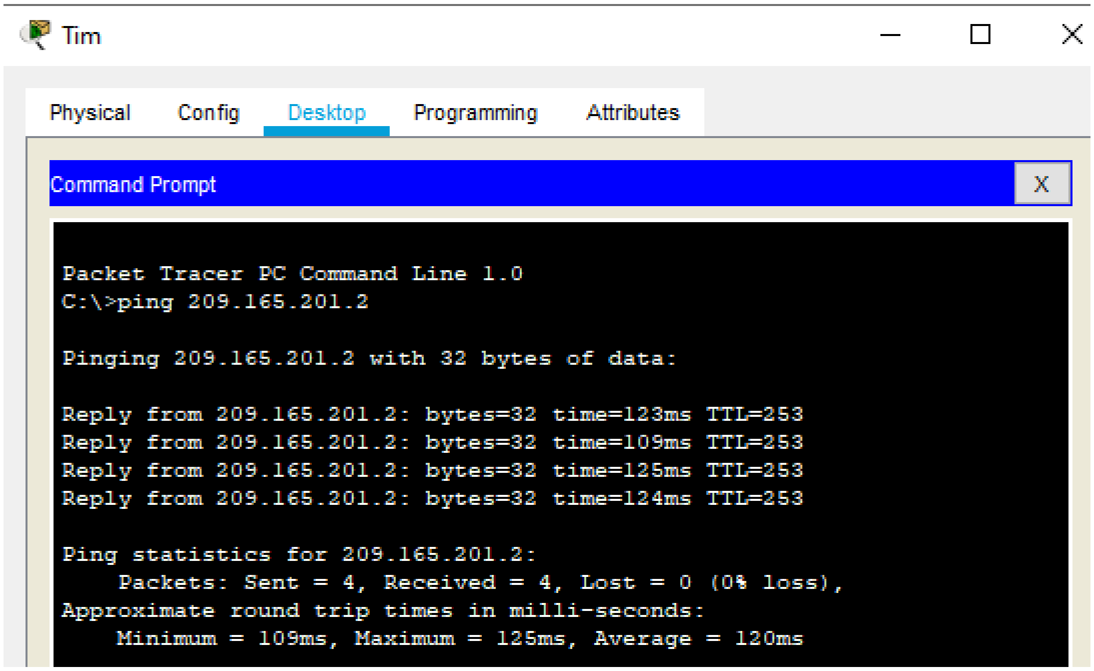

Cisco Packet Tracer - C:\Users\yagmur\Desktop\1.5.3.6 Packet Tracer - Communicating in a Cyber World.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 954, y: 132
[Gotham Healthcare Branch]
23:11:0
Gotham Healthcare Branch
Modem_
Wireless Router_
Tim
Switch
Mike
File Backup
Time: 00:46:41
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
Router-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num E

b. Click the **Desktop** tab and then click **Command Prompt**.



```
Packet Tracer PC Command Line 1.0
C:\>
```

c. Ping the enterprise router using the command **ping 209.165.201.2** to verify reachability.

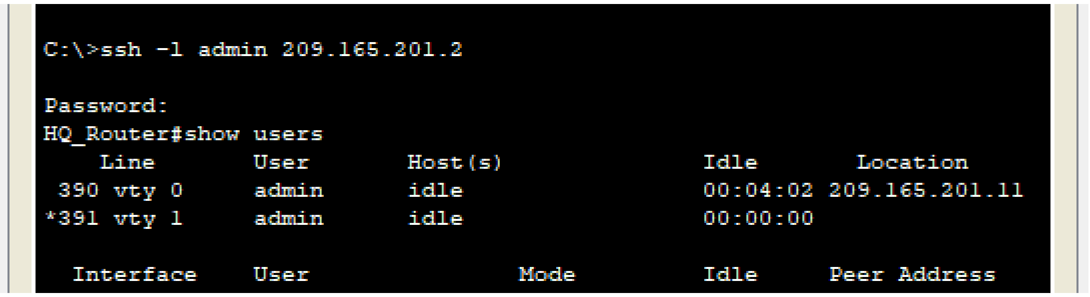


```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=123ms TTL=253
Reply from 209.165.201.2: bytes=32 time=109ms TTL=253
Reply from 209.165.201.2: bytes=32 time=125ms TTL=253
Reply from 209.165.201.2: bytes=32 time=124ms 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 = 109ms, Maximum = 125ms, Average = 120ms
```

d. Use the command **ssh -l admin 209.165.201.2** to SSH to the IP address of the enterprise router.

e. Authenticate to the enterprise router with the password of **cisco123**.

f. Use the command **show users** to view the active SSH connection to the enterprise router.



```
C:\>ssh -l admin 209.165.201.2

Password:
HQ_Router#show users
    Line       User       Host(s)              Idle       Location
 390 vty 0     admin      idle                 00:04:02 209.165.201.11
*391 vty 1     admin      idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
```

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

SSH provides encryption and all data is sent in a secure format.