POLITECHNIKA ŚWIĘTOKRZYSKA

LABORATORIUM CYBERBEZPIECZEŃSTWO

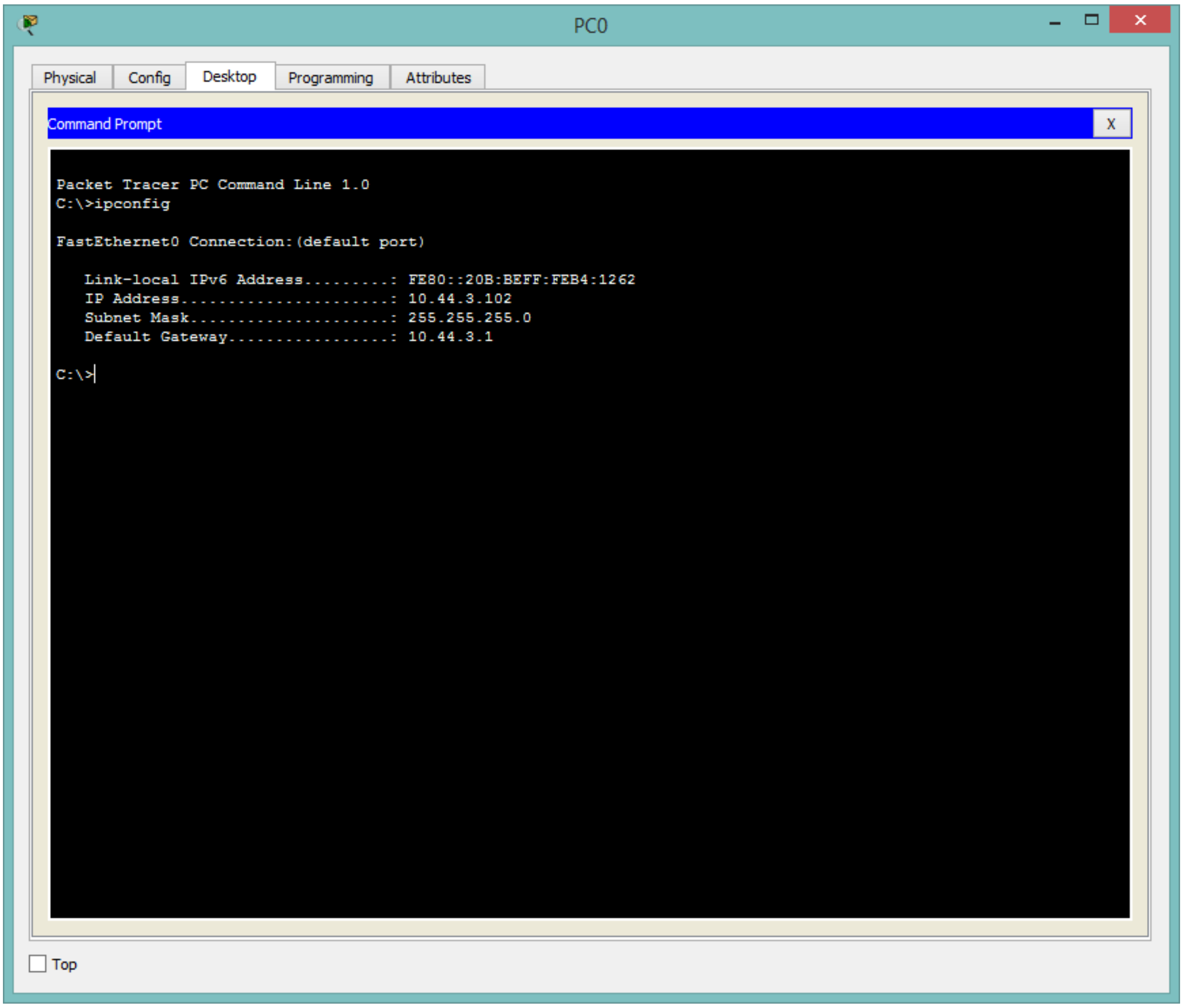
Numer ćwiczenia: 5	**Temat ćwiczenia:** WEP/WPA2 PSK/WPA2 RADIUS	Damian Zdyb
Data wykonania: 13.12.2018	**Data oddania do sprawdzenia:** 15.12.2018	**Ocena:**

Part 1: Configure WEP for Healthcare at Home

Step 1: Setup the Wireless SSID.

a. Click the **Healthcare at Home** site and click **PC0**.

b. Select **Desktop** tab. Click **Command Prompt**. At the prompt, enter **ipconfig**.



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

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::20B:BEFF:FEB4:1262
   IP Address......................: 10.44.3.102
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.3.1

C:\>
```

Adres IP bramki to główny adres routera. Mając do niego dostęp (login i hasło) mamy możliwość skonfigurować router.

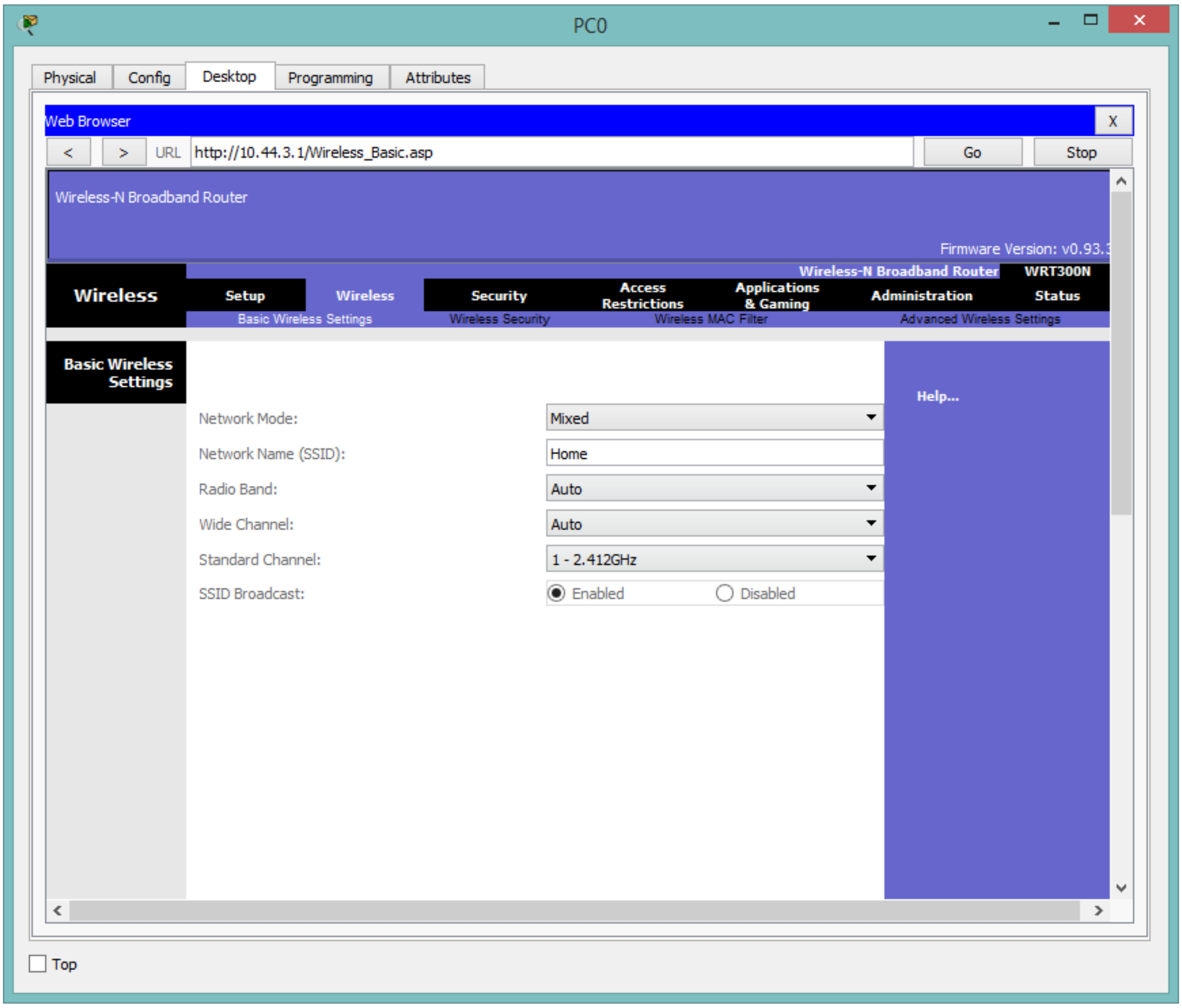
c. Navigate to the **Web Browser** and enter the IP address for the default gateway. Enter **admin** as the username and password when prompted. Click **OK**.

d. The **Wireless Router** is the default gateway for this network. Click **Wireless** tab.

e. Change the **SSID** from **DefaultWIFI** to **Home**.

f. Set the SSID to **Broadcast**.

g. Click **Save Settings**. Click **Continue**.



URL http://10.44.3.1/Wireless_Basic.asp

Network Mode:	Mixed
Network Name (SSID):	Home
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	● Enabled ○ Disabled

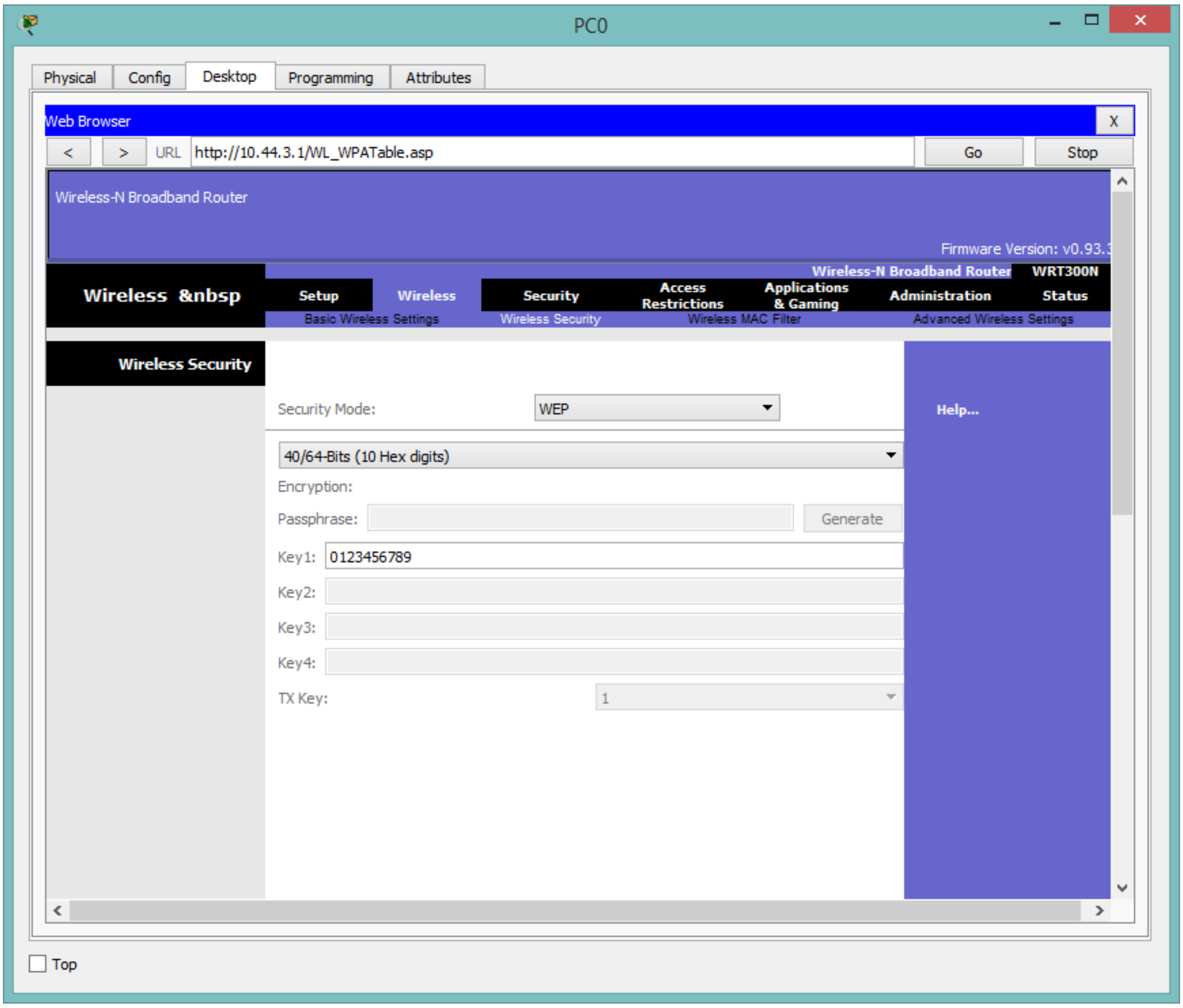
Step 2: Setup Wireless Security.

a. Within the Wireless Router, click **Wireless** > **Wireless Security**.

b. Click the drop down menu and set the Security Mode to **WEP**.

c. Keep the encryption option set to 40/64-bits and enter the key **0123456789** as Key 1.

d. Click **Save Settings**. Click **Continue**.



URL: http://10.44.3.1/WL_WPATable.asp

Security Mode: WEP

40/64-Bits (10 Hex digits)

Encryption:

Passphrase:

Key1: 0123456789

Key2:

Key3:

Key4:

TX Key: 1

□ Top

WEP jest najbardziej popularnym sposobem zabezpieczenia sieci bezprzewodowych ale jest również najsłabszym, najgorszym i najbardziej podatnym na ataki standardem, jaki możemy wybrać.

Step 3: Connect the Clients.

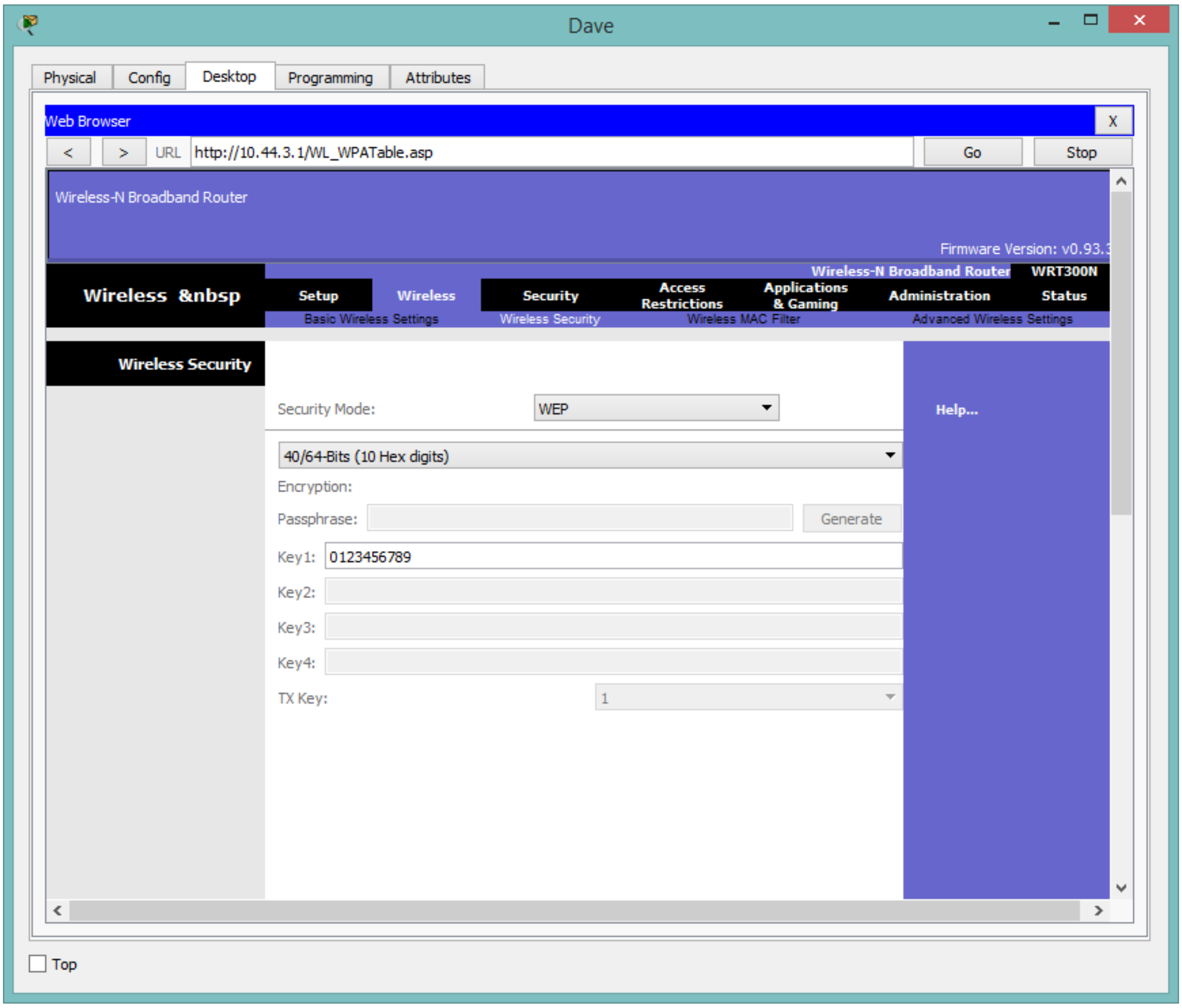
a. Within the **Healthcare at Home** site, click **Dave’s** Laptop.

b. Click the **Desktop** tab and click **PC Wireless**.

c. Click the **Connect** tab and click **Refresh**.

d. Select the Wireless Network Name of **Home** and click **Connect**.

e. Enter the key **0123456789** as WEP Key 1 and click **Connect**.



URL http://10.44.3.1/WL_WPATable.asp

Wireless Security

Security Mode: WEP

40/64-Bits (10 Hex digits)

Encryption:

Passphrase:

Key1: 0123456789

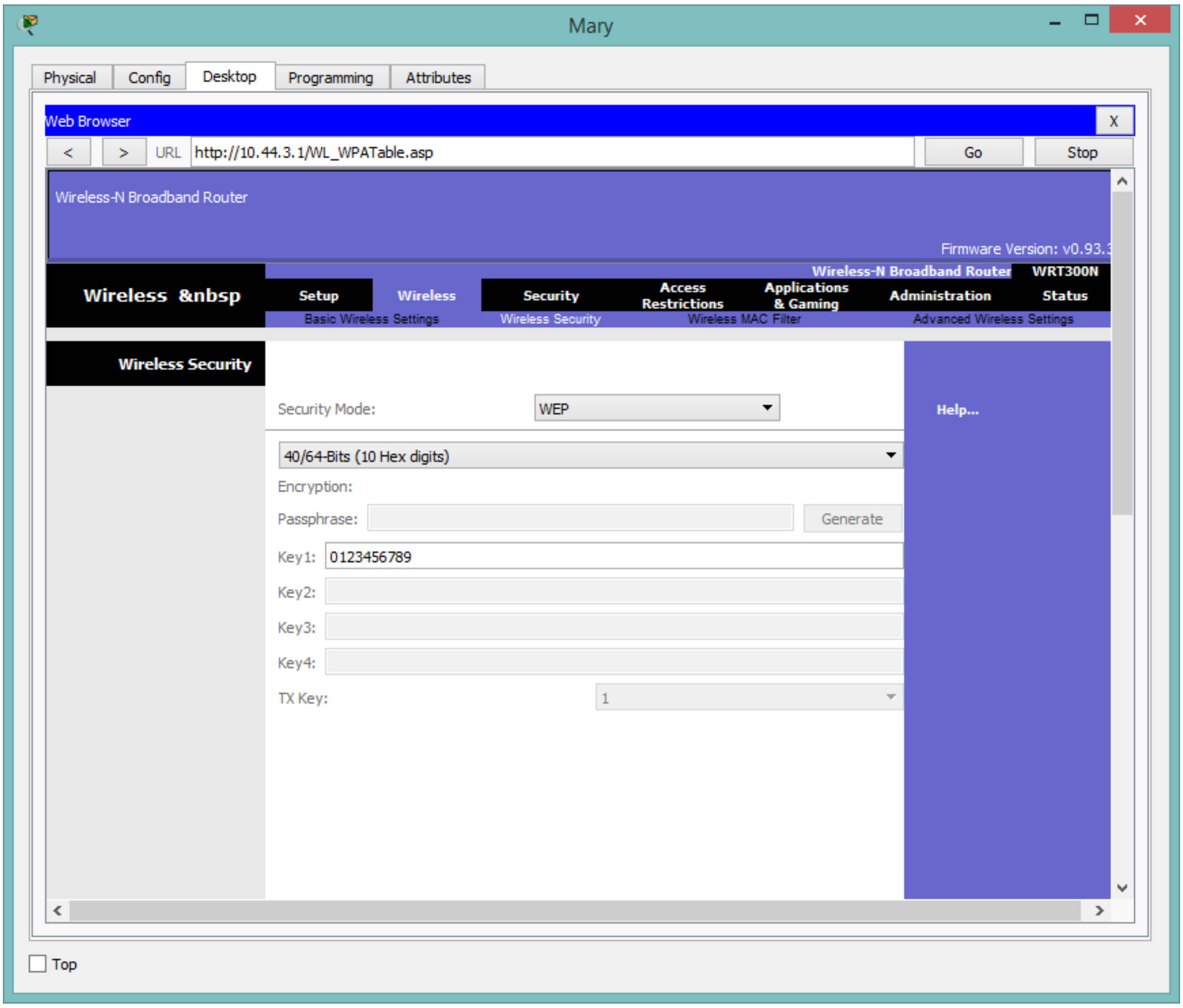
Key2:

Key3:

Key4:

TX Key: 1

a. Repeat steps **a - e** for **Mary's** Laptop.



URL: http://10.44.3.1/WL_WPATable.asp

Security Mode: WEP

40/64-Bits (10 Hex digits)

Encryption:

Passphrase:

Key1: 0123456789

Key2:

Key3:

Key4:

TX Key: 1

Part 2: Configure WPA2 PSK for Gotham Healthcare Branch

Step 1: Setup the Wireless SSID.

a. Click the **Gotham Healthcare Branch** site and click **PC1**.

b. Select **Desktop** tab. Click **Command Prompt**. At the prompt, enter **ipconfig**.

Record the IP address for the default gateway:

c. Navigate to the **Web Browser** and enter the IP address for the default gateway. Enter **admin** as the username and password when prompted. Click **OK**.

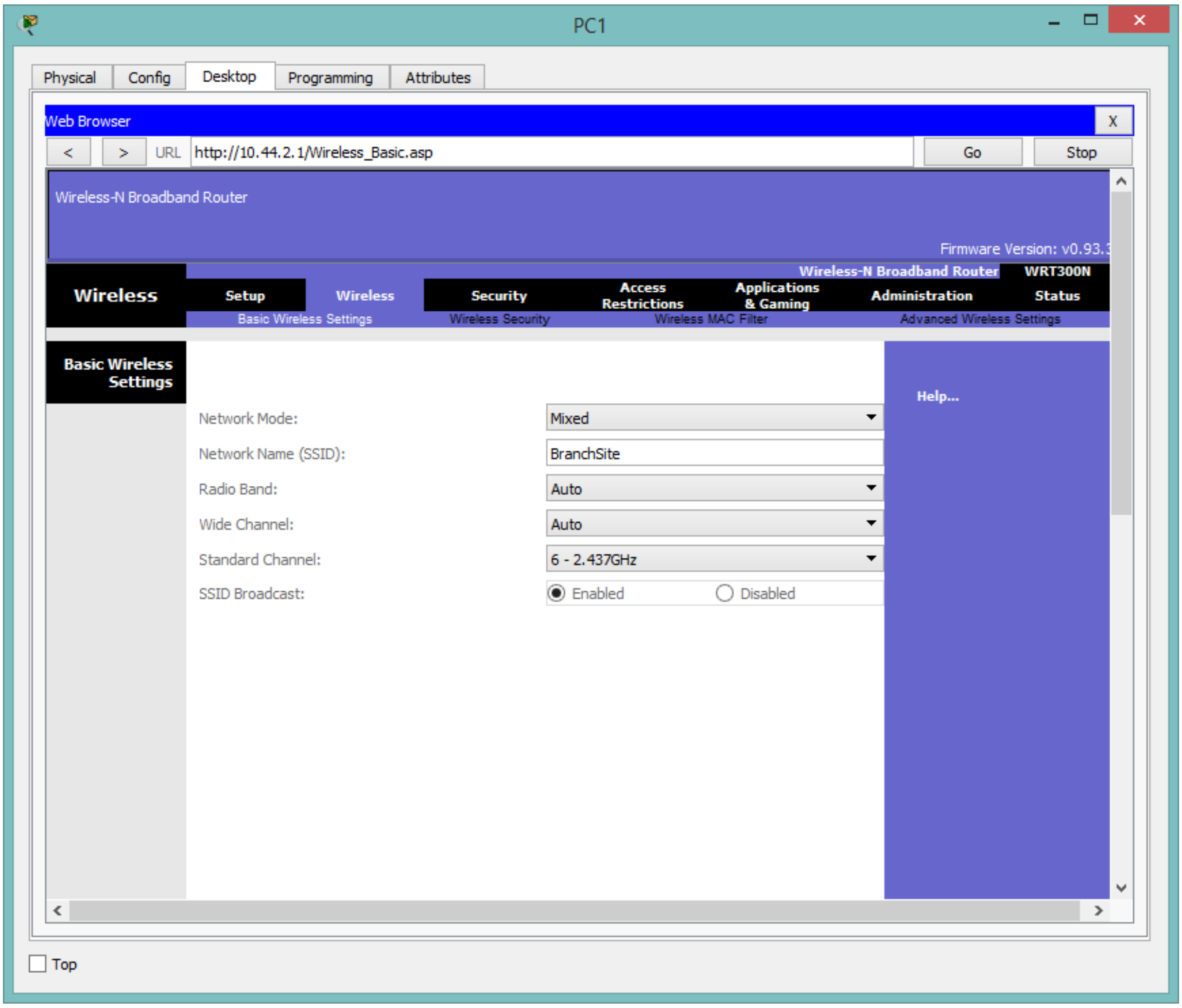
d. Click **Wireless** tab.

e. Change the **SSID** from **DefaultWIFI** to **BranchSite**.

f. Change the Standard Channel to **6 – 2.437GHz**.

g. Set the SSID to **Broadcast**.

h. Click **Save Settings**. Click **Continue**.



URL: http://10.44.2.1/Wireless_Basic.asp

Network Mode: Mixed

Network Name (SSID): BranchSite

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 6 - 2.437GHz

SSID Broadcast: ● Enabled ○ Disabled

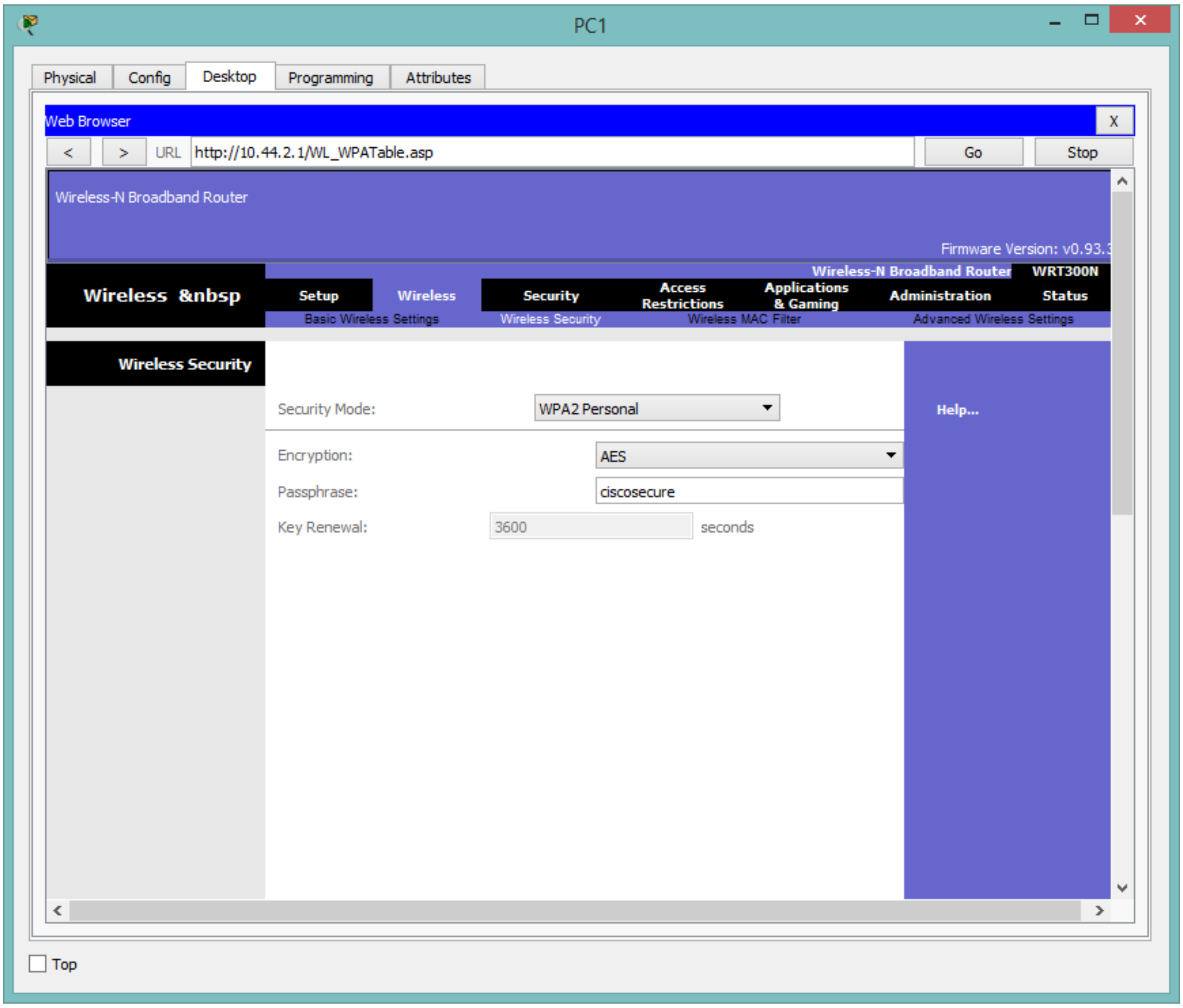
Step 2: Setup Wireless Security.

a. Within the wireless router, click on **Wireless** > **Wireless Security**.

b. Click the drop down menu and set the Security Mode to **WPA2 Personal**.

c. Keep the encryption option set to **AES** and enter the passphrase **ciscosecure**.

d. Click **Save Settings**. Click **Continue**.



URL: http://10.44.2.1/WL_WPATable.asp

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: ciscosecure

Key Renewal: 3600 seconds

Step 3: Connect the Clients.

a. Within the **Gotham Healthcare Branch** site, click **Tim's** computer.

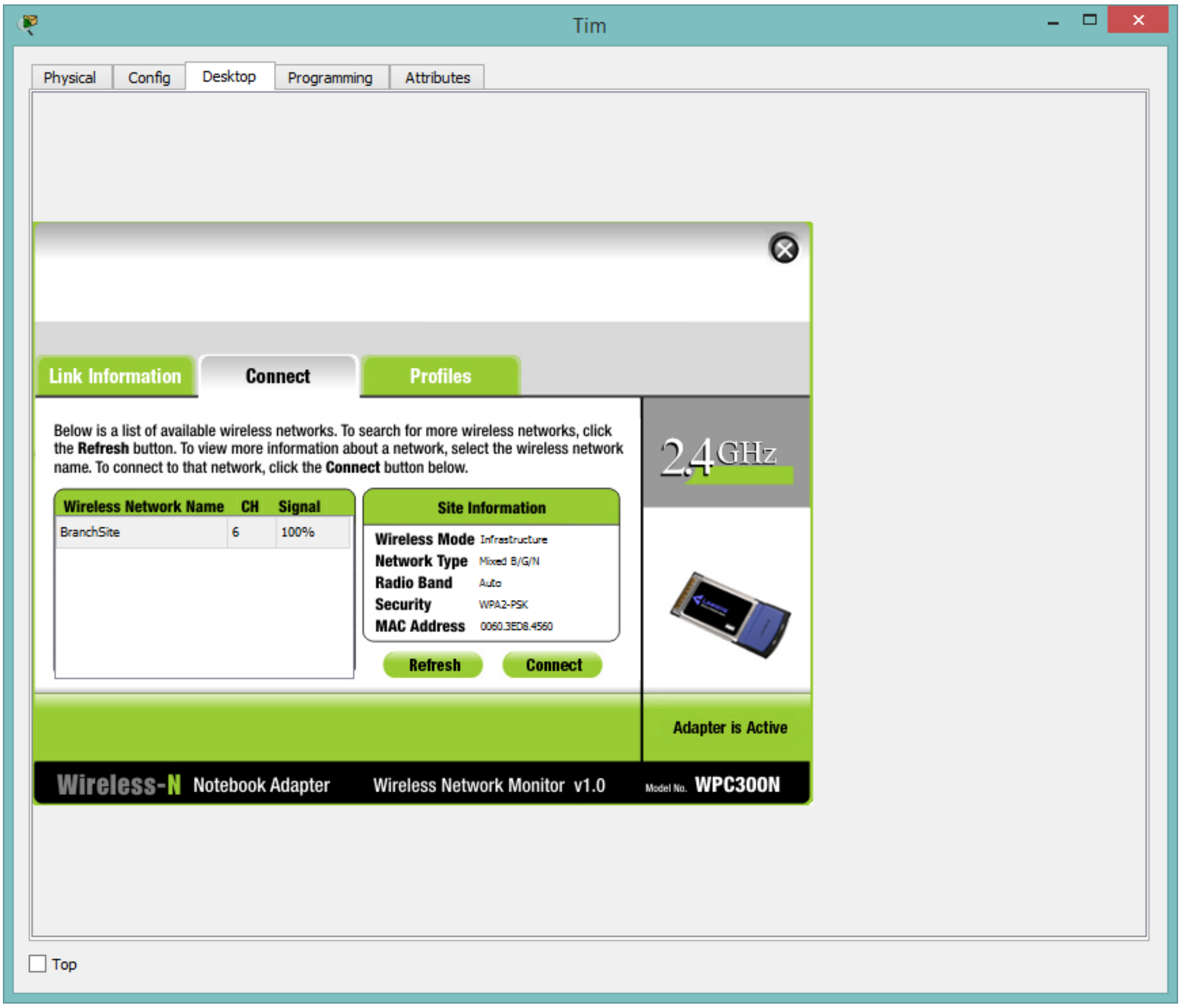
b. Click the **Desktop** tab and click on **PC Wireless**.

c. Click the **Connect** tab and click **Refresh**.

d. Select the Wireless Network Name of **BranchSite** and click the **Connect**.

e. Enter the Pre-shared Key **ciscosecure** and click **Connect**.

f. Repeat steps **a - e** for **Mike's** computer.



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
BranchSite	6	100%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	0060.3ED8.4560

Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. **WPC300N**

Part 3: Configure WPA2 RADIUS for Metropolis Bank HQ

Step 1: Setup the Wireless SSID.

a. Click the **Metropolis Bank HQ** site and click **Sally**.

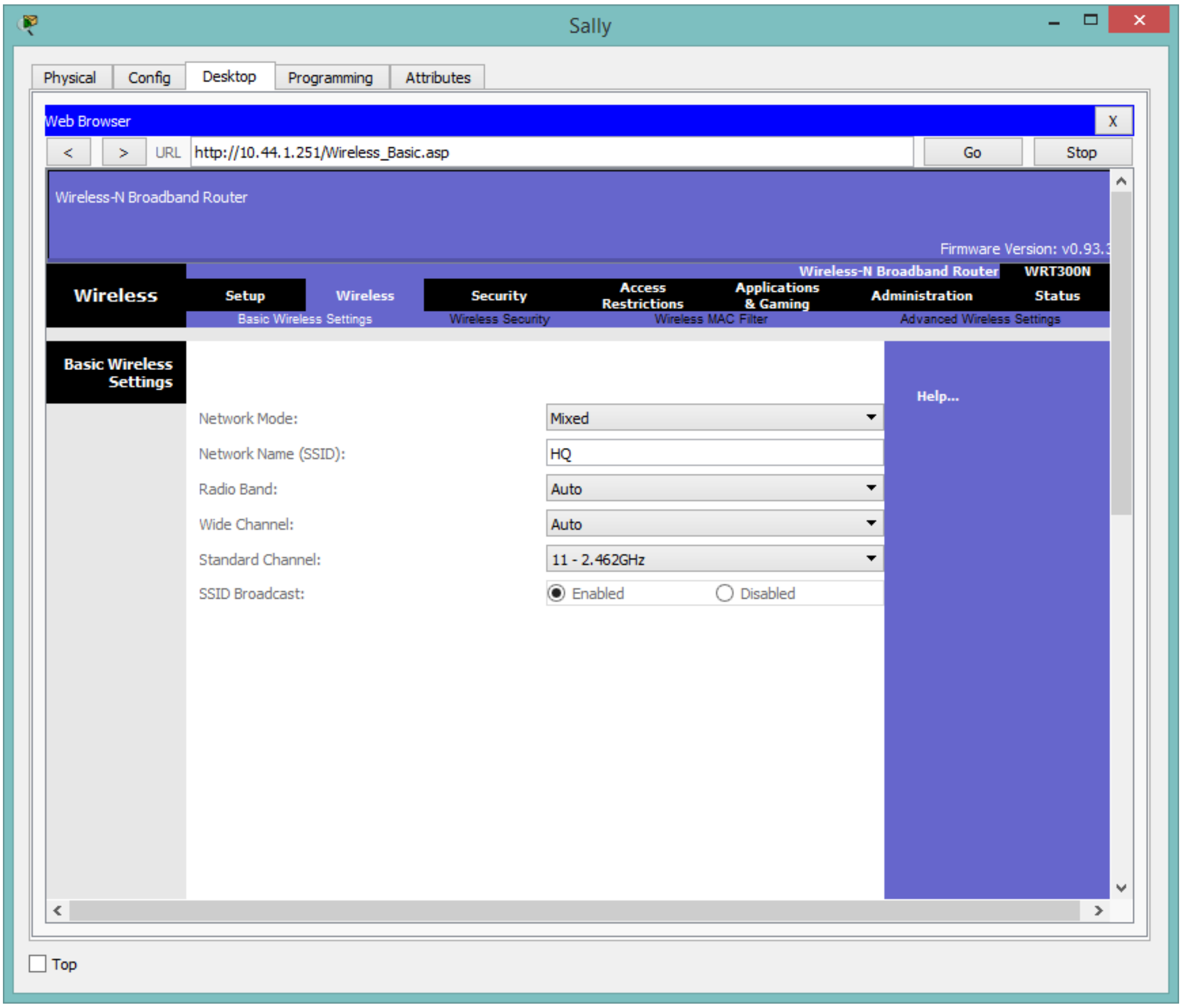
b. Navigate to the **Web Browser** and enter the IP address for the wireless router (**10.44.1.251**). Enter **admin** as the username and password when prompted. Click **OK**.

c. Click the **Wireless** tab. Change the **SSID** from **DefaultWIFI** to **HQ**.

d. Change the Standard Channel to **11 – 2.462GHz**.

e. Set the SSID to **Broadcast**.

f. Click **Save Settings**. Click **Continue**.



URL http://10.44.1.251/Wireless_Basic.asp

Network Mode: Mixed

Network Name (SSID): HQ

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 11 - 2.462GHz

SSID Broadcast: ● Enabled ○ Disabled

Step 2: Setup Wireless Security.

a. Within the **Wireless Router**, click on **Wireless** > **Wireless Security**.

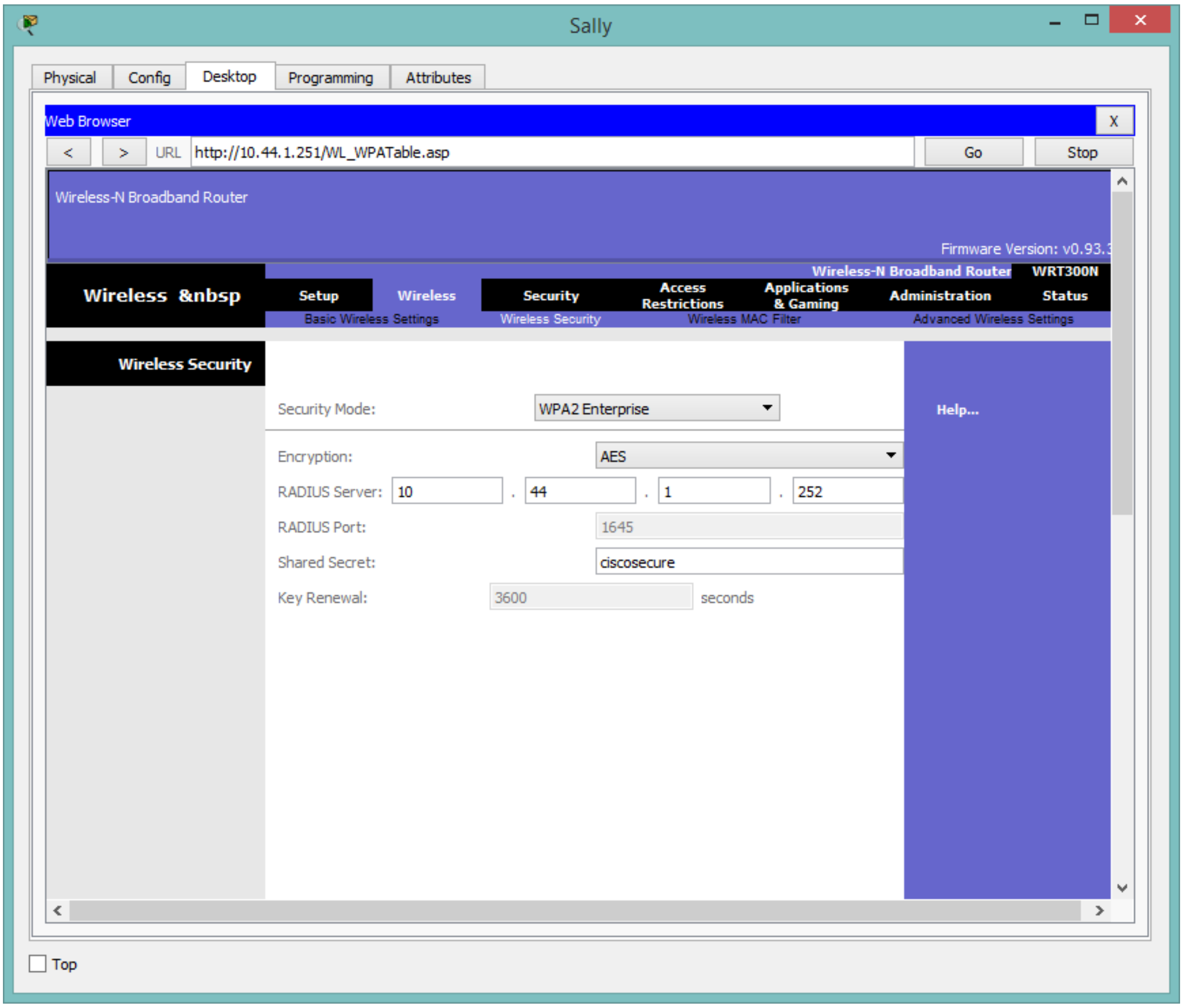
b. Click the drop down menu and set the Security Mode to **WPA2-Enterprise**.

c. Keep the encryption option set to **AES** and enter the following RADIUS server credentials:

RADIUS SERVER IP: **10.44.1.252**

Shared Secret: **ciscosecure**

d. Click **Save Settings**. Click **Continue**.



URL http://10.44.1.251/WL_WPATable.asp

Security Mode: WPA2 Enterprise

Encryption: AES

RADIUS Server: 10 . 44 . 1 . 252

RADIUS Port: 1645

Shared Secret: ciscosecure

Key Renewal: 3600 seconds

Step 3: Configure the RADIUS server.

a. Within the **Metropolis Bank HQ** site, click the **NTP/AAA** server.

b. Click the **Services** tab and click on **AAA**.

c. Enter the following information in **Network Configuration**:

Client Name:.... **HQ**

Client IP:.......... **10.44.1.251**

Secret:............. **ciscosecure**

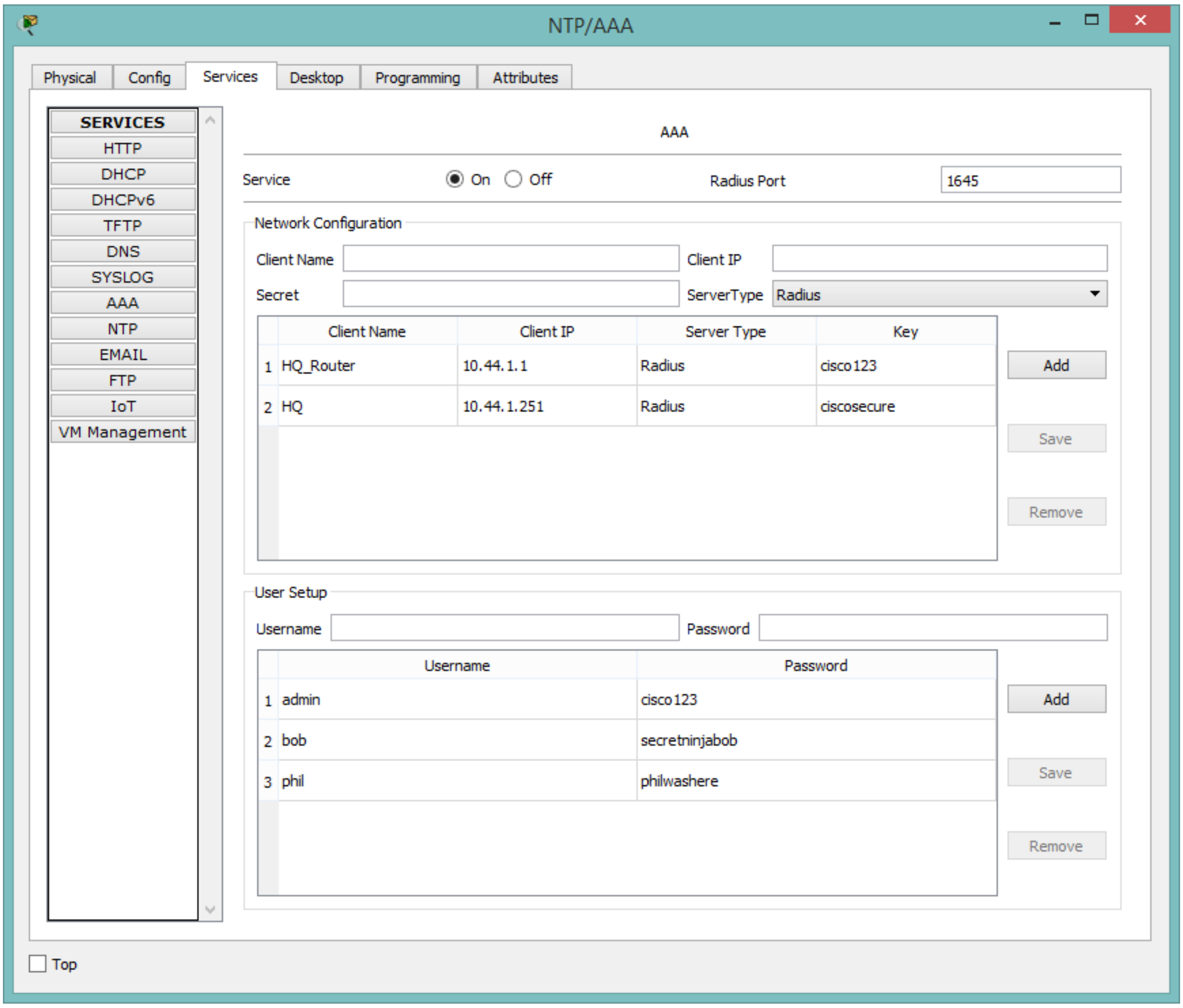
ServerType:..... **Radius**

d. Click **Add**.

e. Enter the following information in **User Setup** and click **Add** to add the new username:

Username: **bob** Password: **secretninjabob**

Username: **phil** Password: **philwashere**



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	HQ_Router	10.44.1.1	Radius	cisco123
2	HQ	10.44.1.251	Radius	ciscosecure

User Setup

Username Password

	Username	Password
1	admin	cisco123
2	bob	secretninjabob
3	phil	philwashere

Step 4: Connect the Clients.

a. Within the **Metropolis Bank HQ** site, click **Bob's** computer.

b. Click the **Desktop** tab and click on **PC Wireless**.

c. Click the **Profiles** tab and click **New**.

d. Name the Profile **RADIUS** and click **OK**.

e. Click **Advanced Setup**.

f. Enter the Wireless Network Name **HQ** and click **Next**.

g. Do not modify the Network Settings and click **Next**.

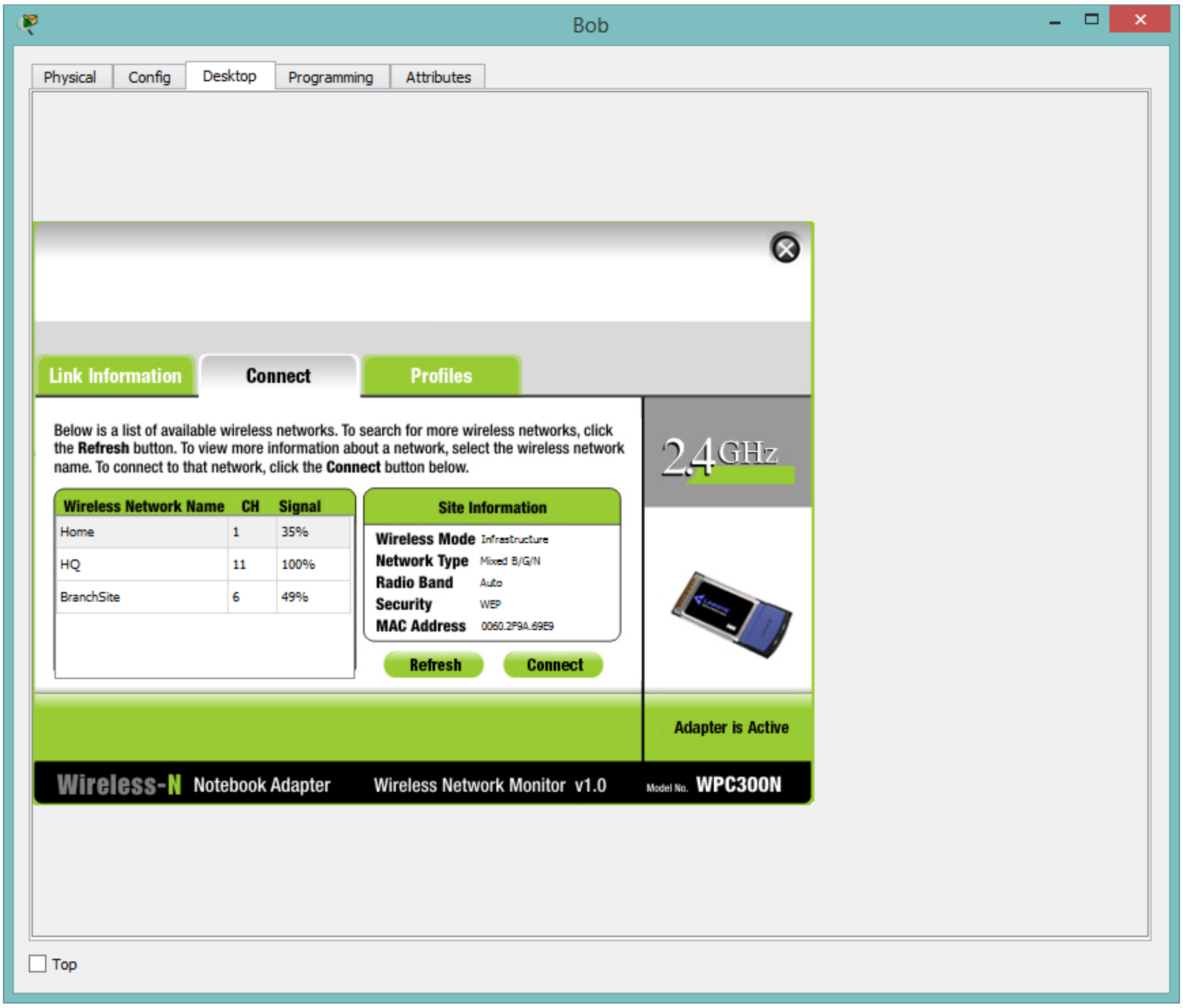
h. Change the Wireless Security drop down menu to **WPA2-Enterprise** and click **Next**.

i. Enter the login name of **bob** and the password of **secretninjabob** and click **Next**.

j. Click **Save** and then **Connect to Network**.

k. **Bob's** computer will connect automatically.

l. Repeat steps **a-j** for **Phil's** laptop using the authentication information from Step 3e.



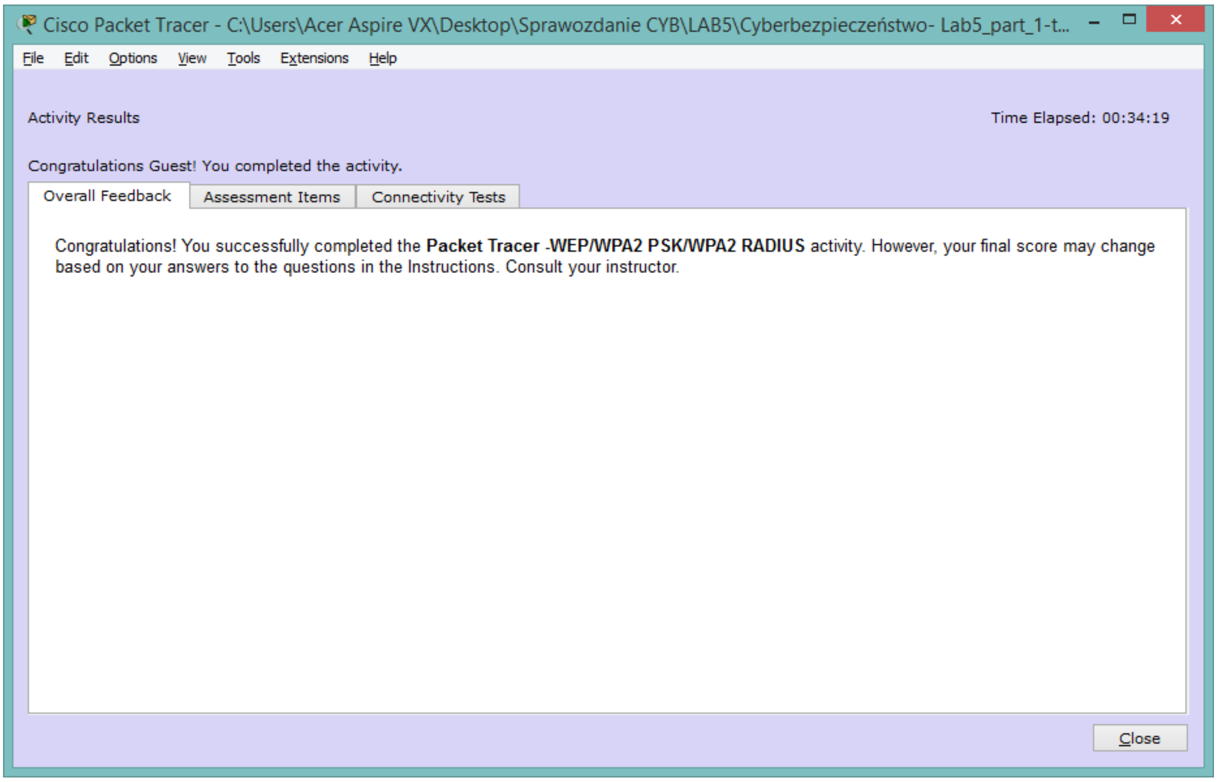
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Home	1	35%
HQ	11	100%
BranchSite	6	49%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WEP
MAC Address	0060.2F9A.69E9

Jest to najbezpieczniejszy sposób zabezpieczeń.


Cisco Packet Tracer - C:\Users\Acer Aspire VX\Desktop\Sprawozdanie CYB\LAB5\Cyberbezpieczeństwo- Lab5_part_1-t...
File Edit Options View Tools Extensions Help
Overall Feedback
Assessment Items
Connectivity Tests
Close

Activity Results

Time Elapsed: 00:34:19

Congratulations Guest! You completed the activity.

Congratulations! You successfully completed the **Packet Tracer -WEP/WPA2 PSK/WPA2 RADIUS** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Wszystkie zadania zostały wykonane poprawnie.

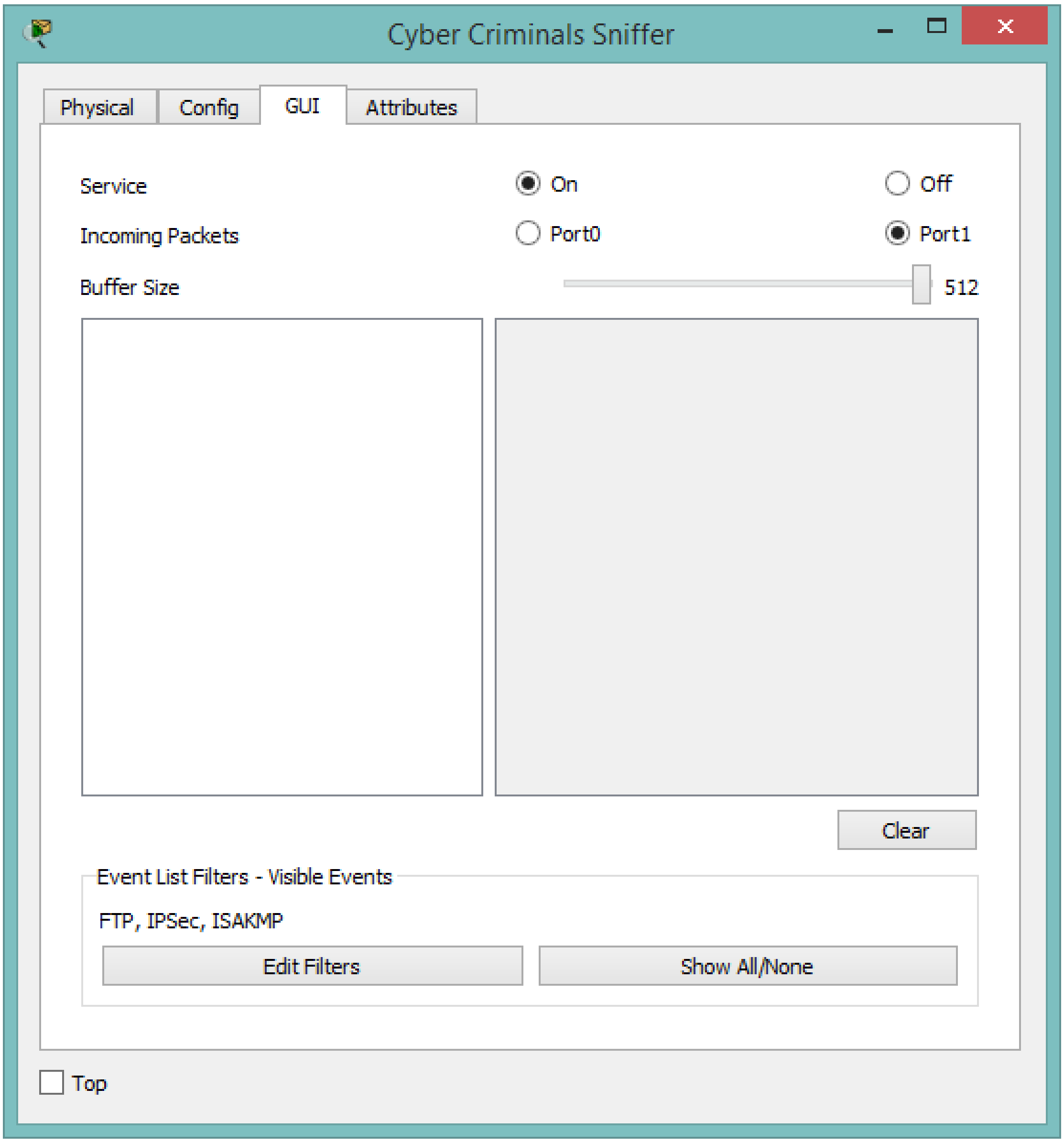
Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

c. Minimize the **Cyber Criminals Sniffer**.



Cyber Criminals Sniffer

Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

Event List Filters - Visible Events

FTP, IPSec, ISAKMP

□ Top

Step 2: Connect to the Public_FTP server using an insecure FTP connection.

a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

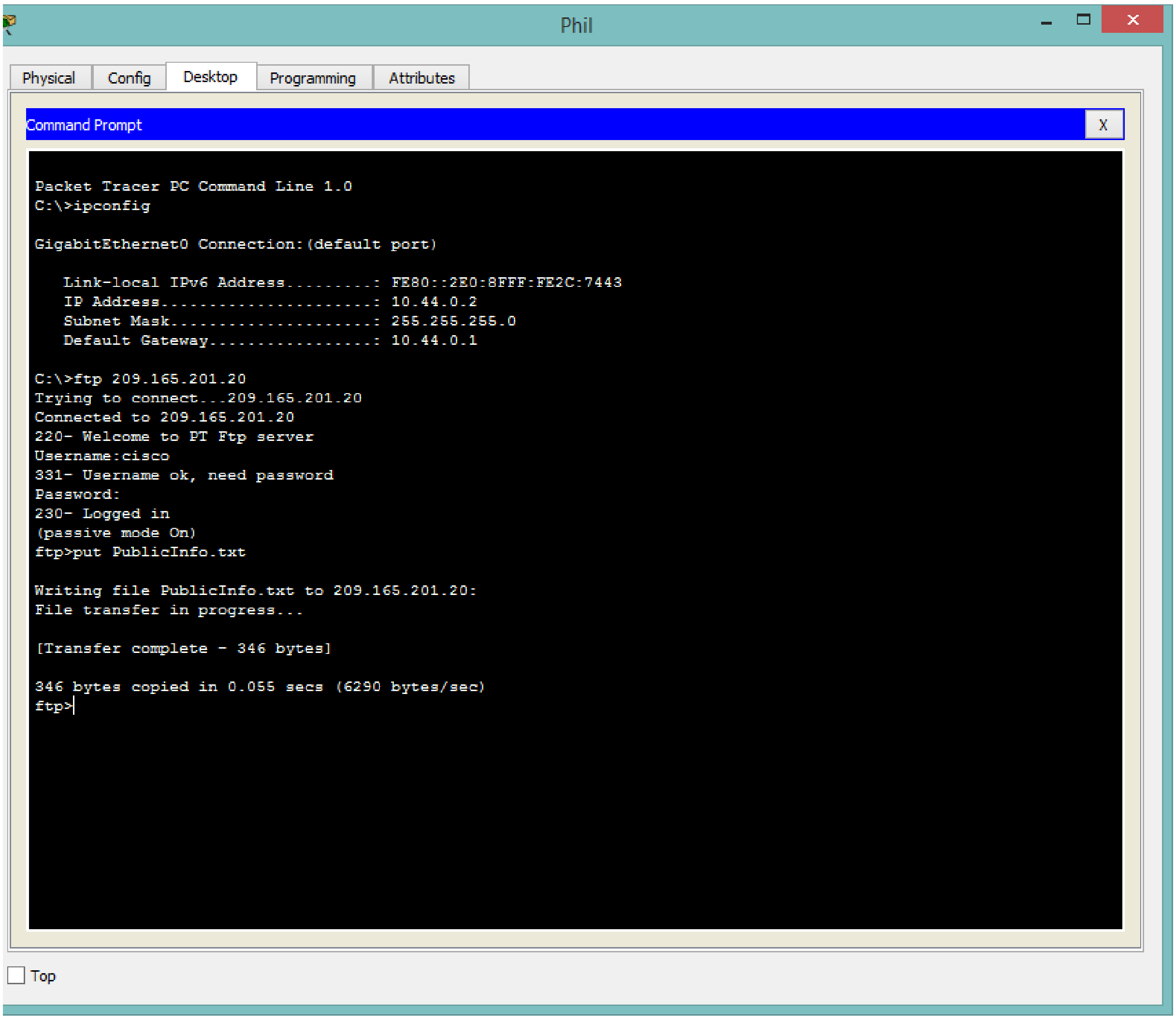
b. Click the **Desktop** tab and click on **Command Prompt**.

c. Use the **ipconfig** command to view the current IP address of **Phil's** computer.

d. Connect to the **Public_FTP** server at **Gotham Healthcare Branch** by entering **ftp 209.165.201.20** in the command prompt.

e. Enter the username of **cisco** and password of **publickey** to login to the **Public_FTP** server.

f. Use the **put** command to upload the file **PublicInfo.txt** file to the **Public_FTP** server.



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

GigabitEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE2C:7443
   IP Address......................: 10.44.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.0.1

C:\>ftp 209.165.201.20
Trying to connect...209.165.201.20
Connected to 209.165.201.20
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put PublicInfo.txt

Writing file PublicInfo.txt to 209.165.201.20:
File transfer in progress...

[Transfer complete - 346 bytes]

346 bytes copied in 0.055 secs (6290 bytes/sec)
ftp>
```

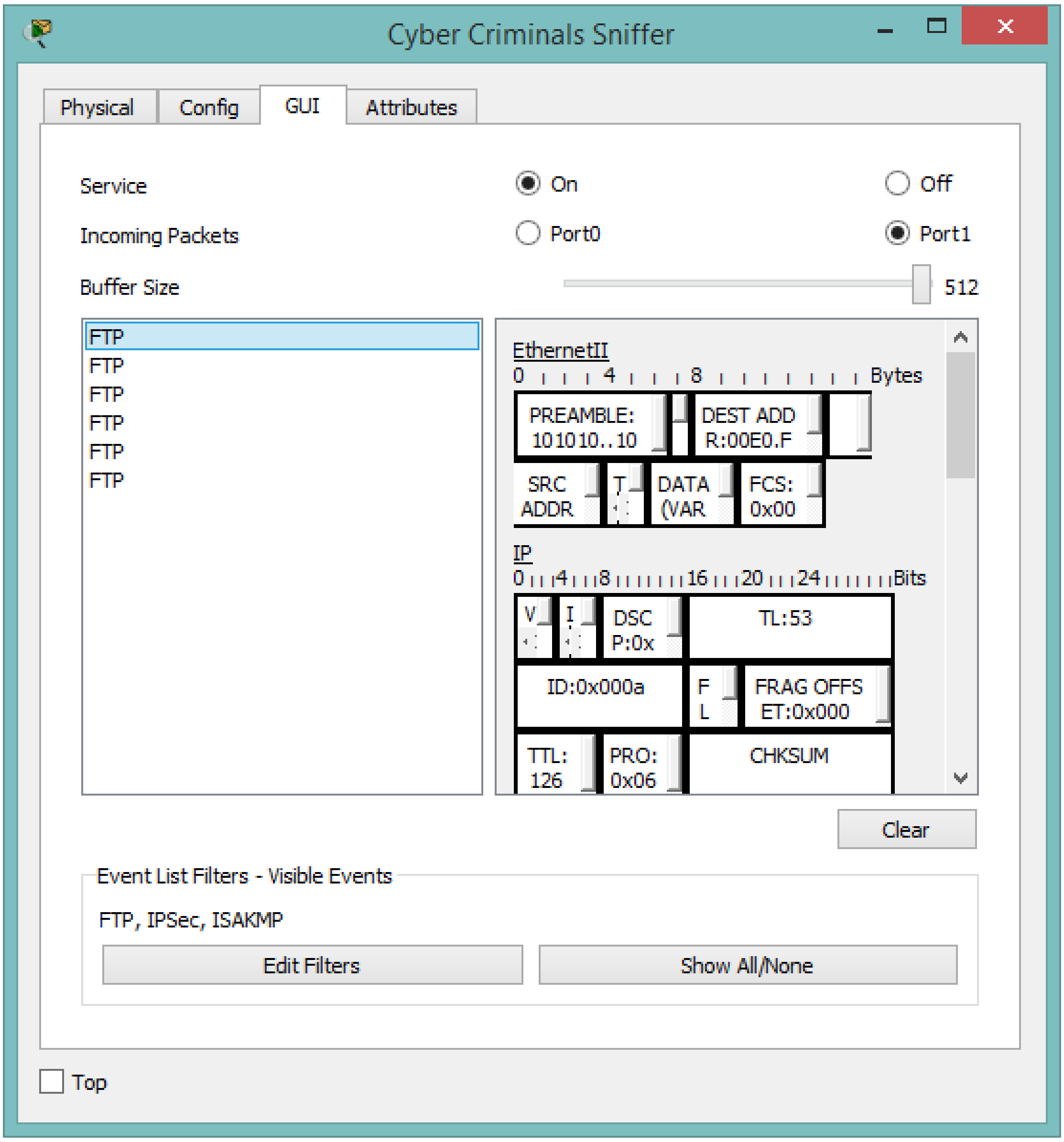
Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

c. Type **quit** to exit **Public_FTP** server.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

FTP
FTP
FTP
FTP
FTP
FTP

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10 | DEST ADDR:00E0.F | SRC ADDR | T | DATA (VAR | FCS: 0x00

IP

0 4 8 16 20 24 Bits

V | I | DSCP:0x | TL:53 | ID:0x000a | FL | FRAG OFFSET:0x000 | TTL: 126 | PRO: 0x06 | CHKSUM

Event List Filters - Visible Events

FTP, IPSec, ISAKMP

□ Top

Part 2: Configuring the VPN Client on Phil's Computer

a. From **Phil's** computer, use the **ping** command and target the IP address of the **Branch_Router**. The first few pings may timeout. Enter the **ping** to get four successful pings.

b. On the **Desktop** tab, click on **VPN**

c. Within the **VPN Configuration** window, enter the following settings:

GroupName:............ **VPNGROUP**

Group Key:.............. **123**

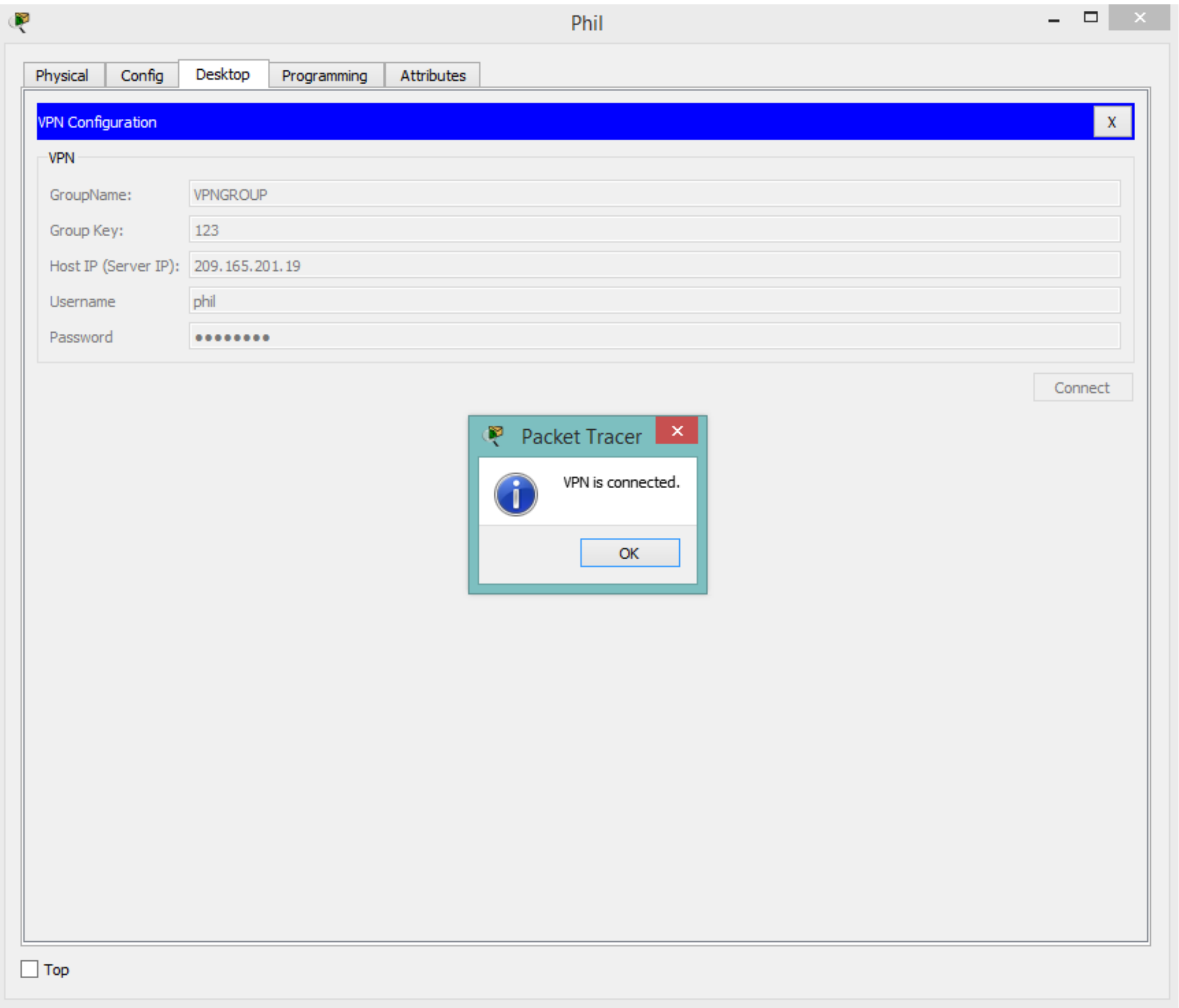
Host IP (Server IP):.. **209.165.201.19**

Username:............... **phil**

Password:............... **cisco123**

d. Click **Connect** and Click **OK** on the next window.

What is the Client IP for the client-to-site VPN connection?



GroupName: VPNGROUP

Group Key: 123

Host IP (Server IP): 209.165.201.19

Username phil

Password ••••••••

VPN is connected.

Part 3: Sending Encrypted FTP Traffic

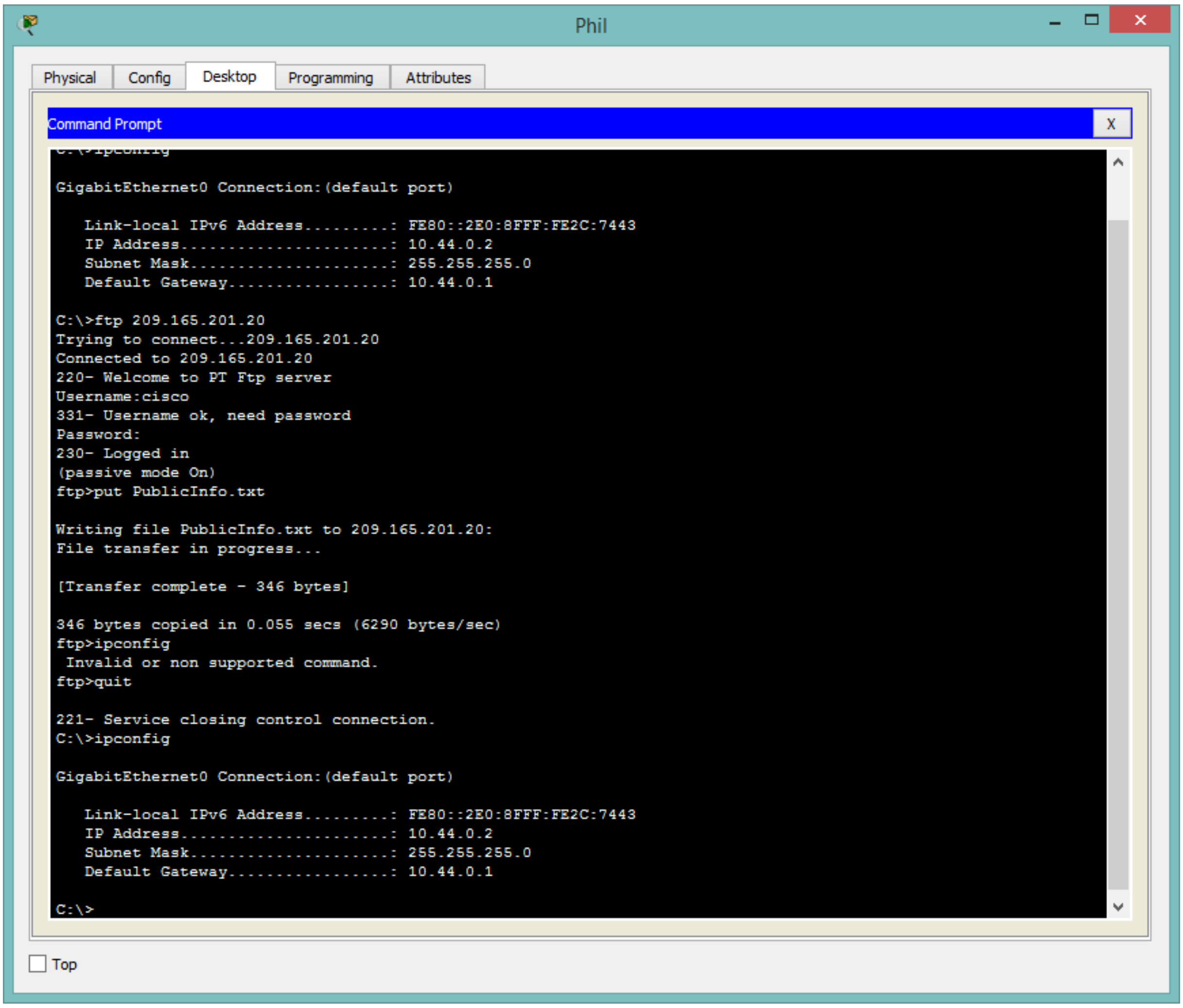
Step 1: View the current IP addressing on Phil’s computer.

a. Within the **Metropolis Bank HQ** site, click **Phil’s** computer.

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

c. Use the **ipconfig** command to view the current IP address of **Phil’s** PC.

What extra IP address is now shown that was not shown before in Part 1 Step 2c?



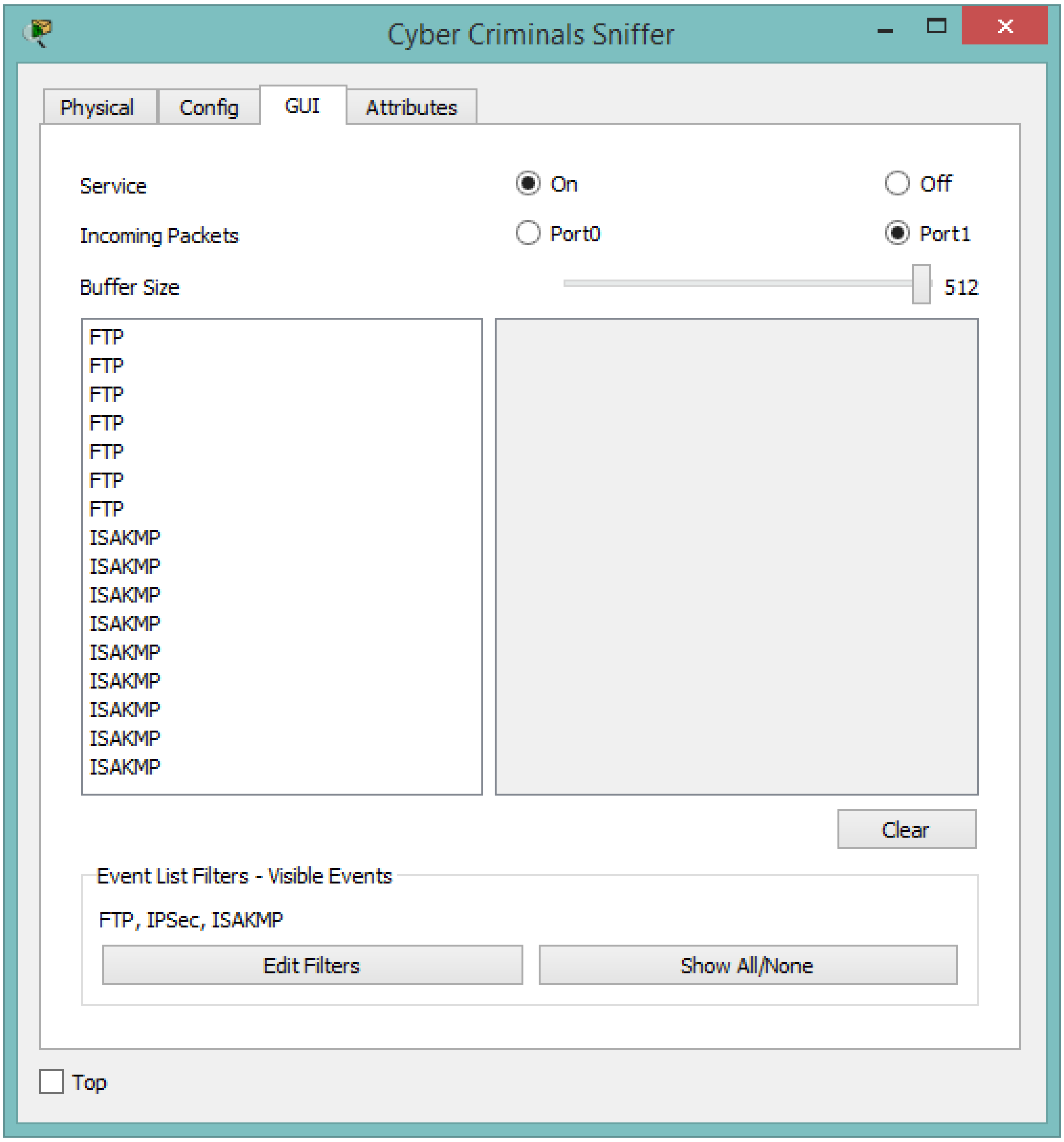
```
C:\>ipconfig

GigabitEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE2C:7443
   IP Address......................: 10.44.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.0.1

C:\>ftp 209.165.201.20
Trying to connect...209.165.201.20
Connected to 209.165.201.20
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put PublicInfo.txt

Writing file PublicInfo.txt to 209.165.201.20:
File transfer in progress...

[Transfer complete - 346 bytes]

346 bytes copied in 0.055 secs (6290 bytes/sec)
ftp>ipconfig
 Invalid or non supported command.
ftp>quit

221- Service closing control connection.
C:\>ipconfig

GigabitEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE2C:7443
   IP Address......................: 10.44.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.0.1

C:\>
```

Step 2: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages displaying the password of internal or the file upload of PrivateInfo.txt? Explain.



Service ● On ○ Off

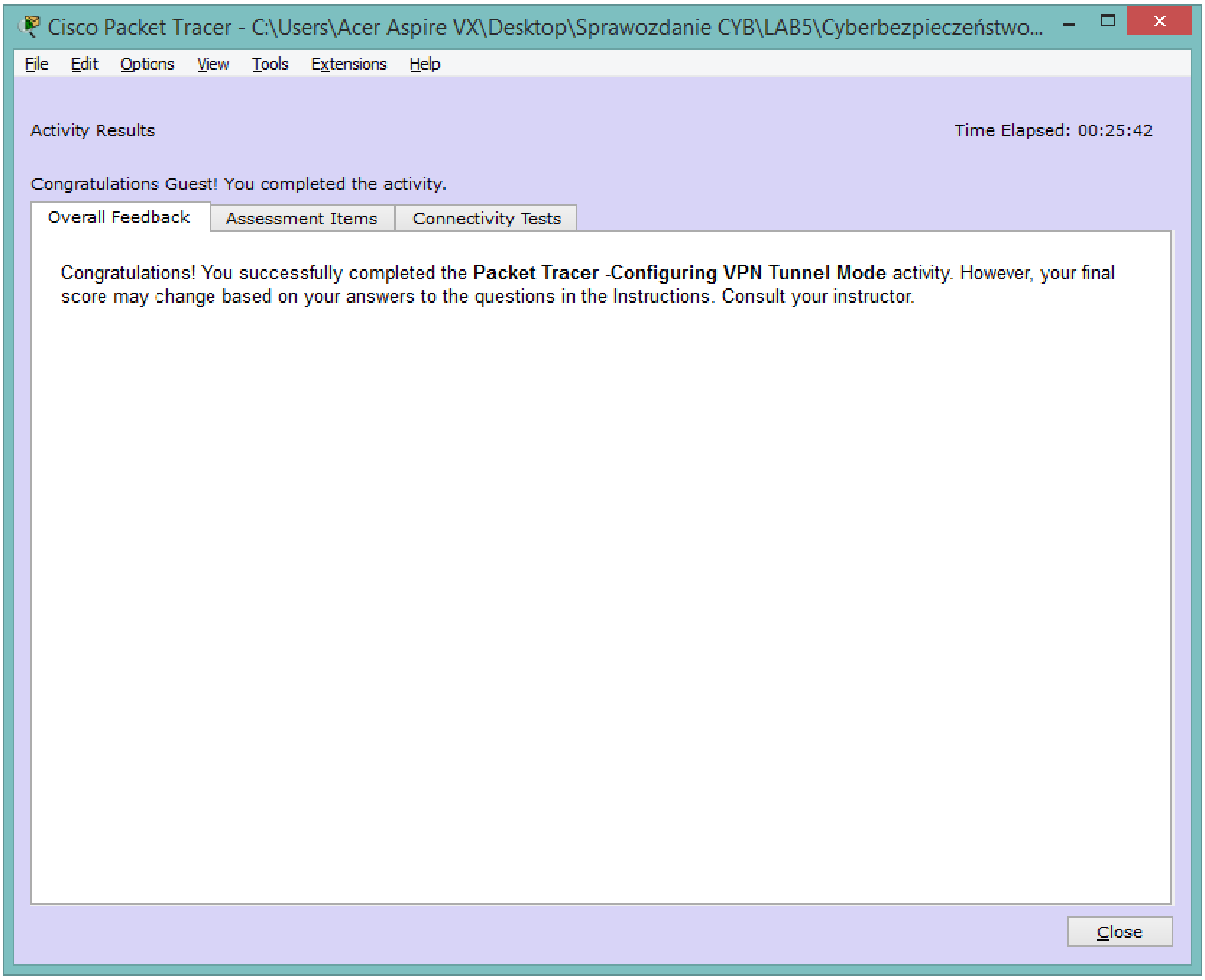
Incoming Packets ○ Port0 ● Port1

Buffer Size 512

```
FTP
FTP
FTP
FTP
FTP
FTP
FTP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
ISAKMP
```

Event List Filters - Visible Events

FTP, IPSec, ISAKMP



Cisco Packet Tracer - C:\Users\Acer Aspire VX\Desktop\Sprawozdanie CYB\LAB5\Cyberbezpieczeństwo...
File Edit Options View Tools Extensions Help
Overall Feedback
Assessment Items
Connectivity Tests
Close

Activity Results

Time Elapsed: 00:25:42

Congratulations Guest! You completed the activity.

Congratulations! You successfully completed the **Packet Tracer -Configuring VPN Tunnel Mode** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Wszystkie zadania zostały wykonane poprawnie.

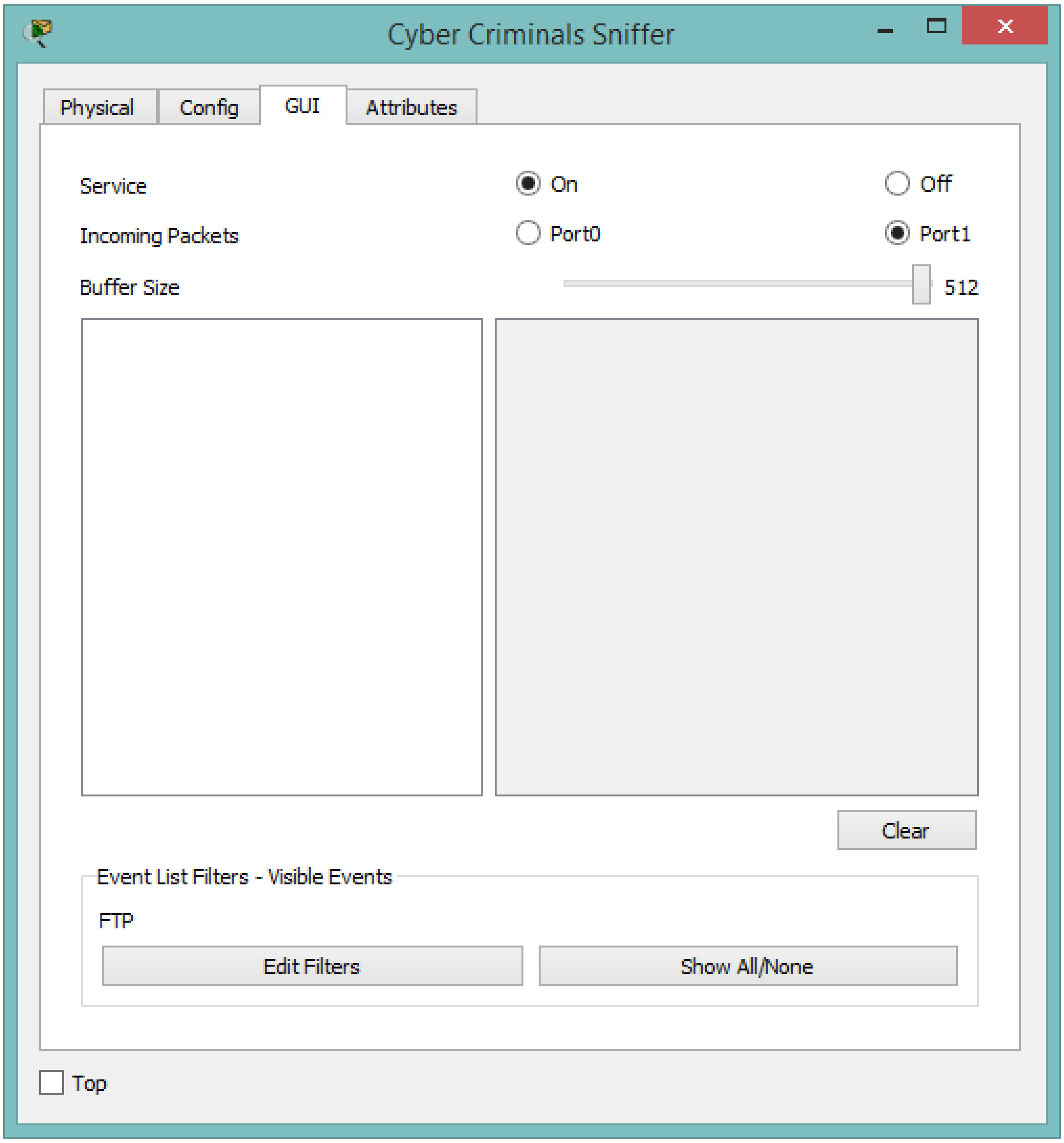
Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

c. Minimize the **Cyber Criminals Sniffer**.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

FTP

□ Top

Step 2: Connect to the FTP Backup server using an insecure FTP connection.

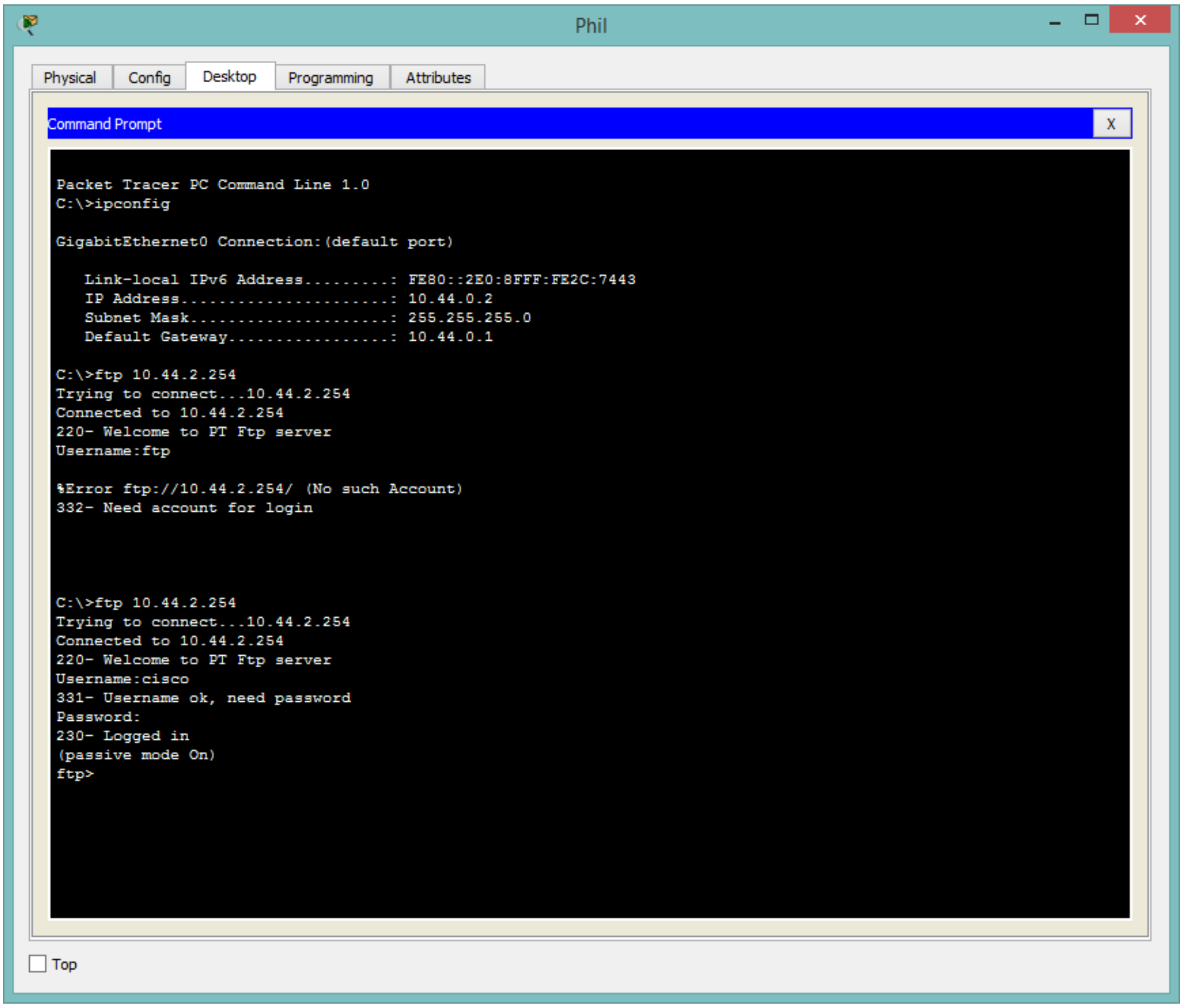
a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

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

c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

a. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server.

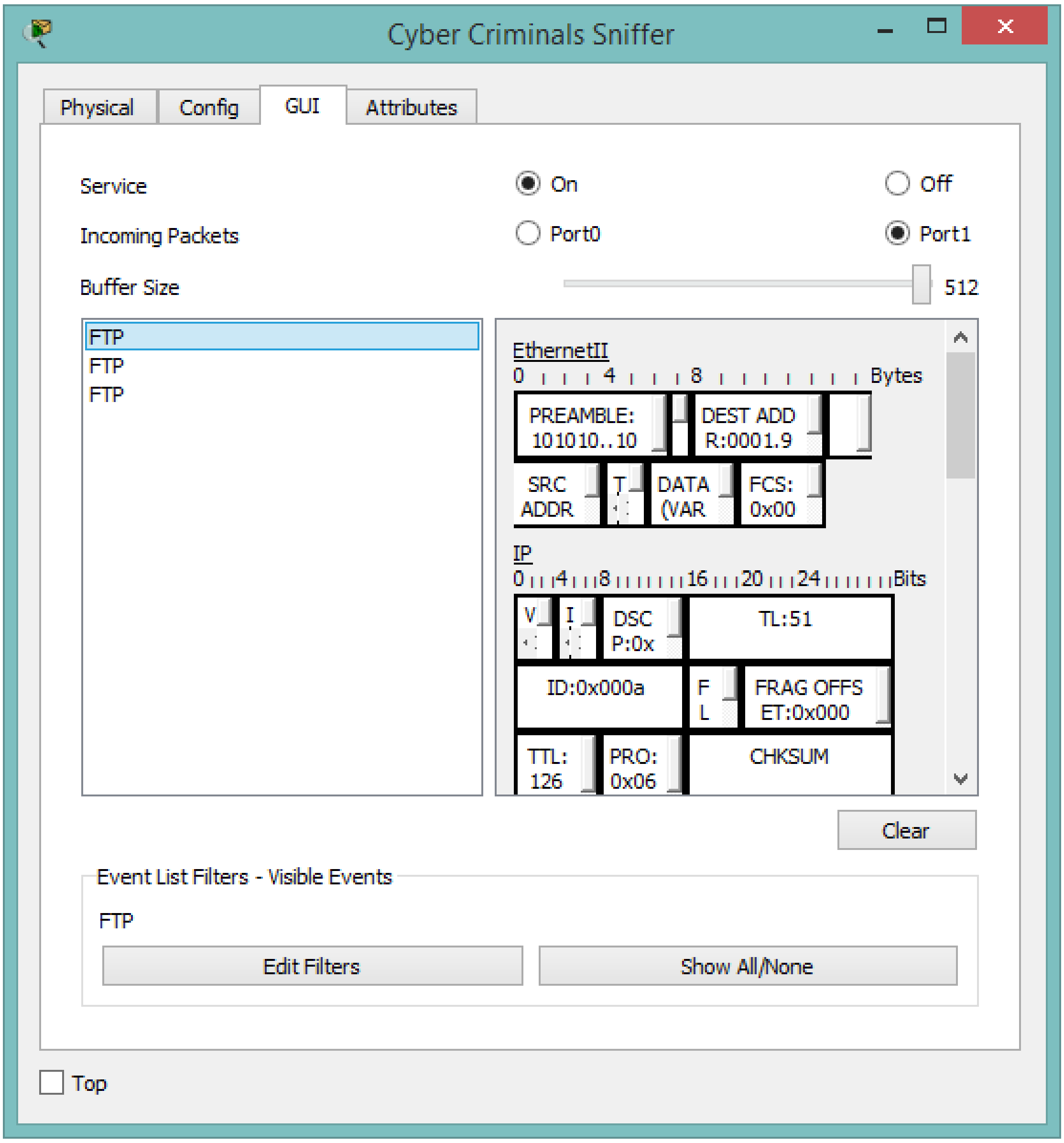


```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

GigabitEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE2C:7443
   IP Address......................: 10.44.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.0.1

C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:ftp

%Error ftp://10.44.2.254/  (No such Account)
332- Need account for login



C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

FTP
FTP
FTP

Event List Filters - Visible Events

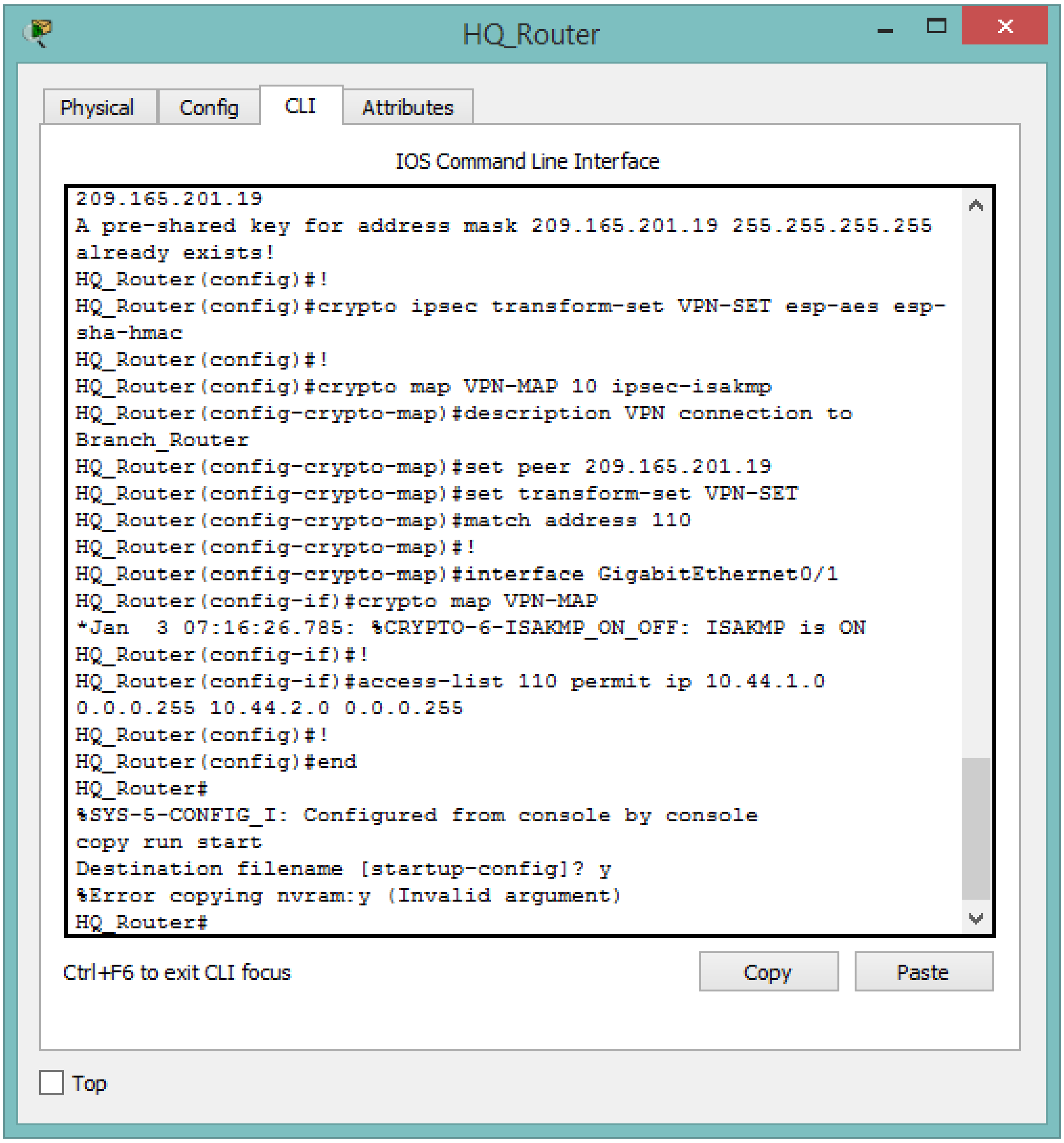
FTP

□ Top

Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.

b. Copy the IPSec VPN site-to site configuration below and paste it into **HQ_Router**.



```
209.165.201.19
A pre-shared key for address mask 209.165.201.19 255.255.255.255
already exists!
HQ_Router(config)#!
HQ_Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-
sha-hmac
HQ_Router(config)#!
HQ_Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
HQ_Router(config-crypto-map)#description VPN connection to
Branch_Router
HQ_Router(config-crypto-map)#set peer 209.165.201.19
HQ_Router(config-crypto-map)#set transform-set VPN-SET
HQ_Router(config-crypto-map)#match address 110
HQ_Router(config-crypto-map)#!
HQ_Router(config-crypto-map)#interface GigabitEthernet0/1
HQ_Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HQ_Router(config-if)#!
HQ_Router(config-if)#access-list 110 permit ip 10.44.1.0
0.0.0.255 10.44.2.0 0.0.0.255
HQ_Router(config)#!
HQ_Router(config)#end
HQ_Router#
%SYS-5-CONFIG_I: Configured from console by console
copy run start
Destination filename [startup-config]? y
%Error copying nvram:y (Invalid argument)
HQ_Router#
```

Part 3: Sending Encrypted FTP Traffic

Step 1: Send FTP traffic from Sally’s PC to the File Backup server.

a. Within the **Metropolis Bank HQ** site, click **Sally’s** computer.

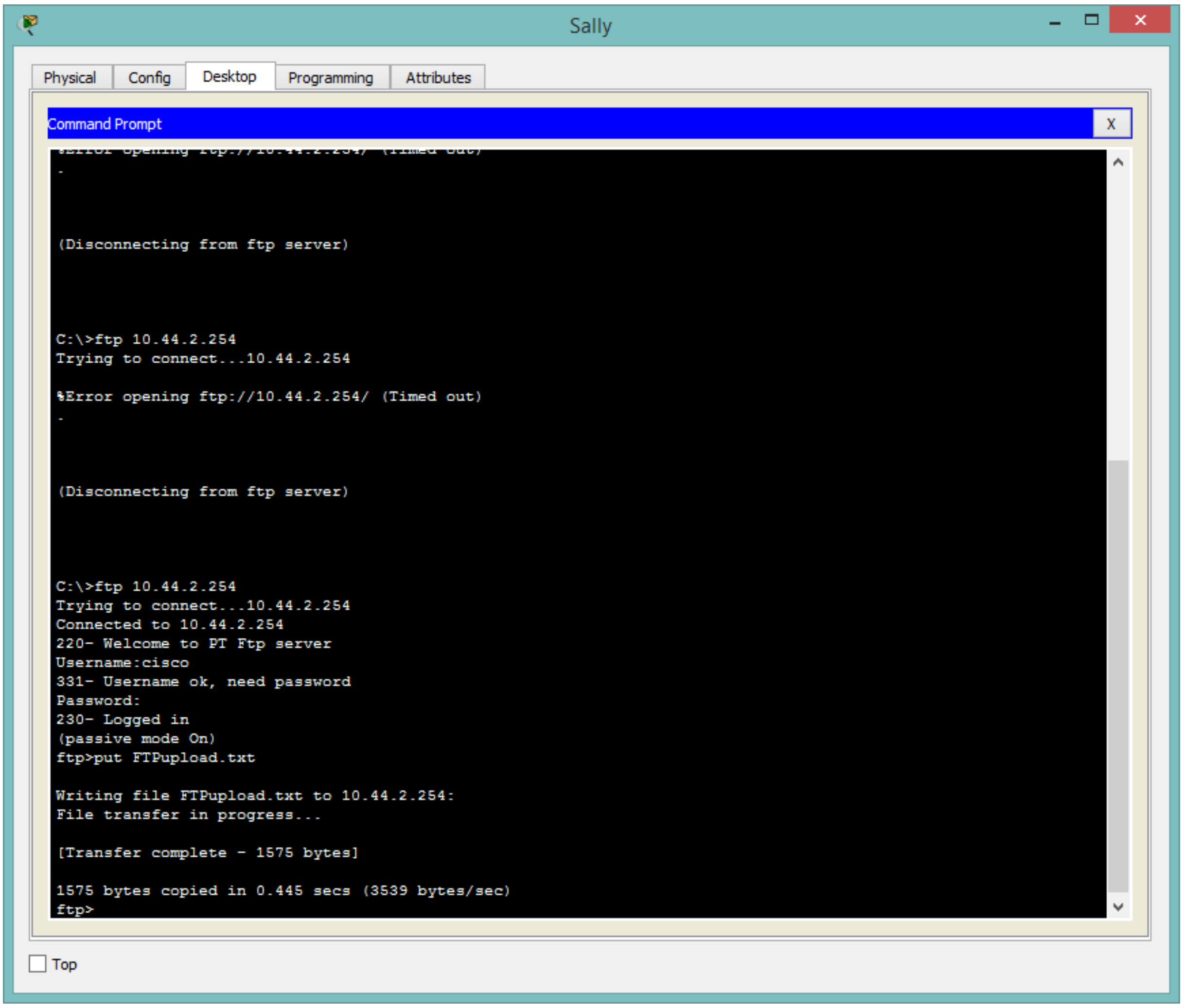
b. Click the **Desktop** tab and then click **Command Prompt**.

c. Use the **ipconfig** command to view the current IP address of **Sally’s** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt. (It may take 2-5 attempts)

e. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server

f. Use the **put** command to upload the file **FTPupload.txt** to the **File Backup** server.



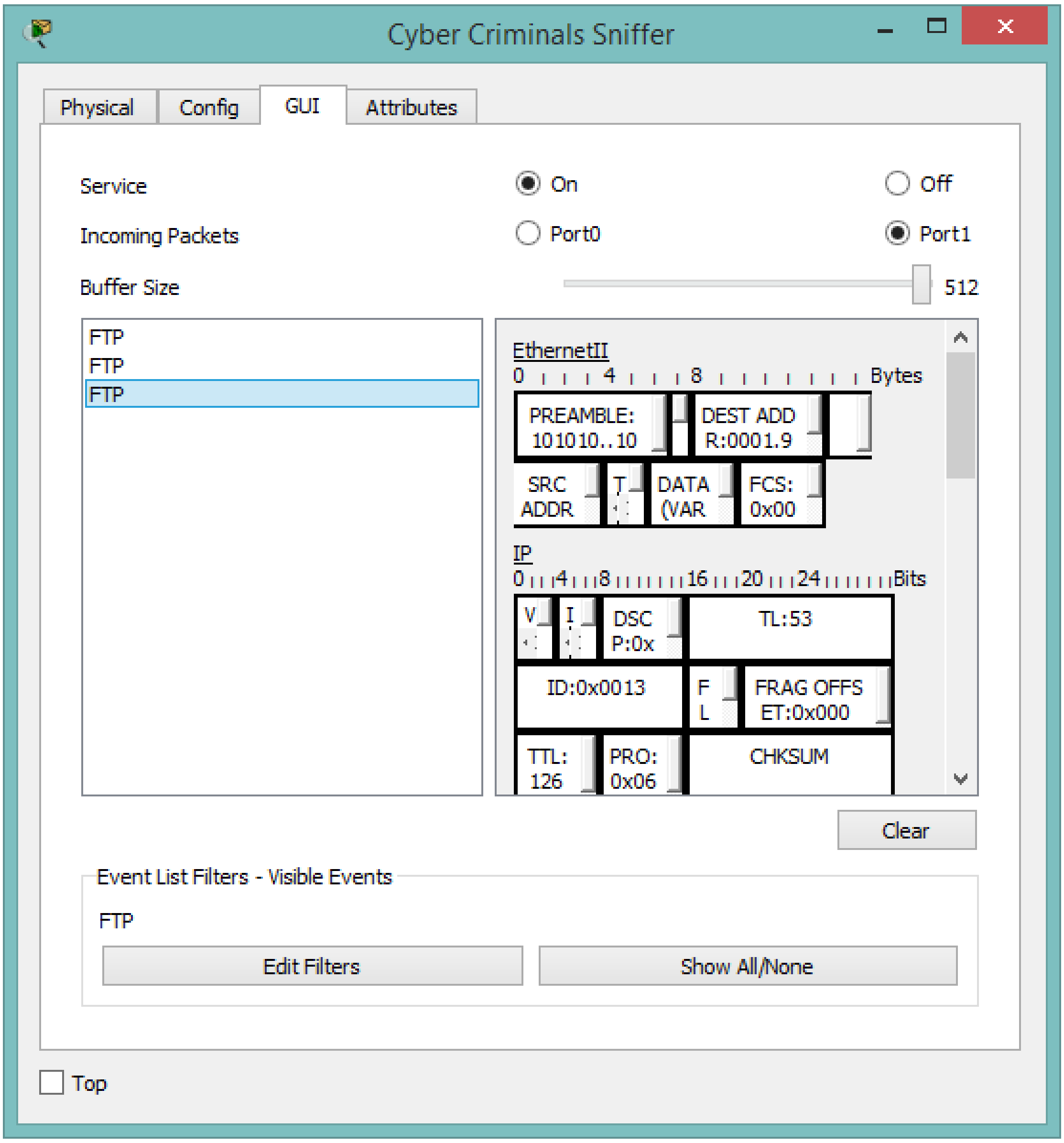
```
%Error opening ftp://10.44.2.254/ (Timed out)
.



(Disconnecting from ftp server)




C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254

%Error opening ftp://10.44.2.254/ (Timed out)
.



(Disconnecting from ftp server)




C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put FTPupload.txt

Writing file FTPupload.txt to 10.44.2.254:
File transfer in progress...

[Transfer complete - 1575 bytes]

1575 bytes copied in 0.445 secs (3539 bytes/sec)
ftp>
```

Step 2: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages sourced from the IP of **Sally's** computer? Explain.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

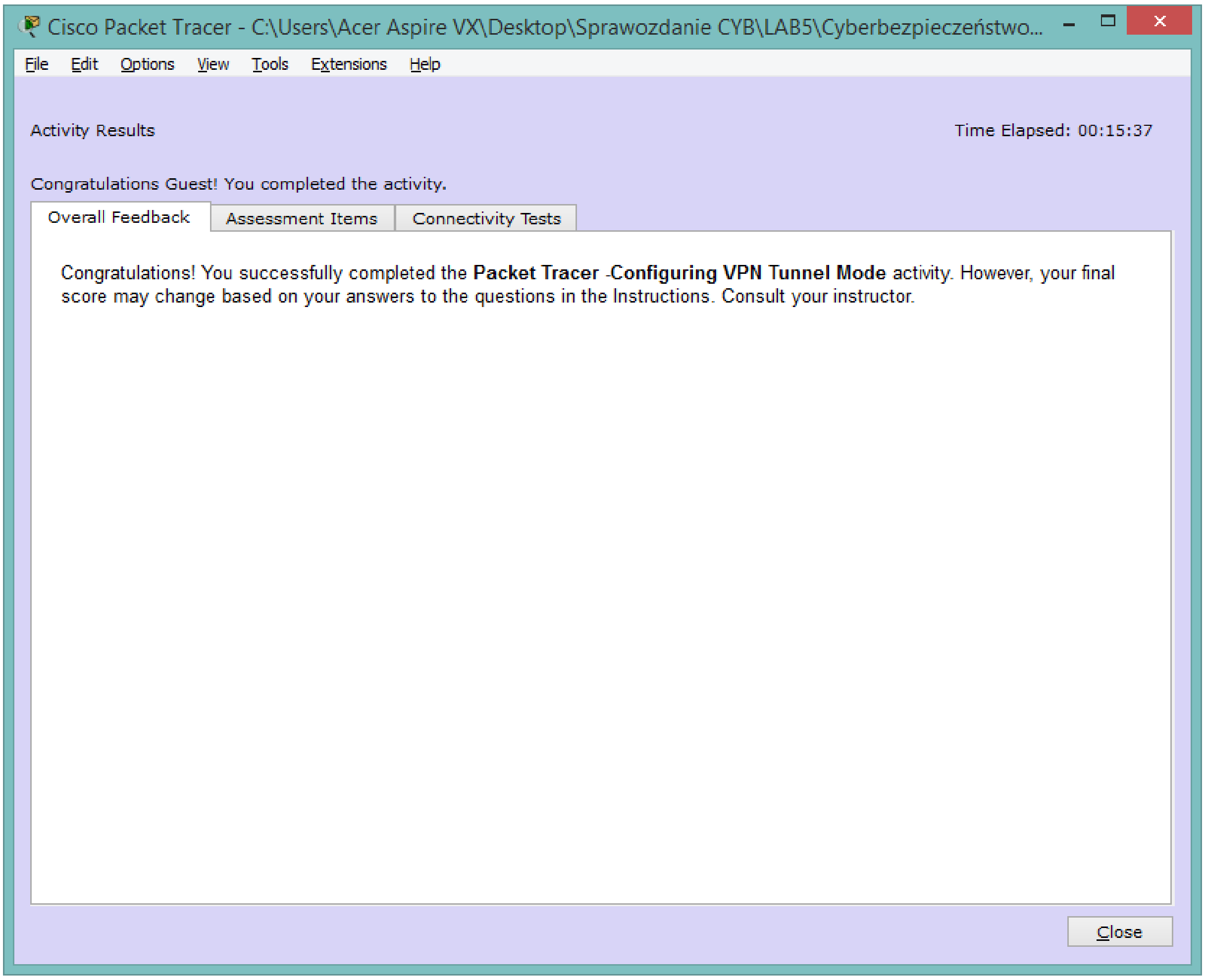
Buffer Size 512

FTP
FTP
FTP

Event List Filters - Visible Events

FTP

□ Top


Cisco Packet Tracer - C:\Users\Acer Aspire VX\Desktop\Sprawozdanie CYB\LAB5\Cyberbezpieczeństwo...
File Edit Options View Tools Extensions Help
Overall Feedback
Assessment Items
Connectivity Tests
Close

Activity Results

Time Elapsed: 00:15:37

Congratulations Guest! You completed the activity.

Congratulations! You successfully completed the **Packet Tracer -Configuring VPN Tunnel Mode** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Wszystkie zadania zostały wykonane poprawnie.