Packet Tracer Lab 4: Configuring VPN Transport Mode

Securing FTP Traffic with VPN Encryption

Student Name

November 17, 2025

Contents

Chapter 1

Introduction

1.1 Objective

This laboratory activity demonstrates the critical importance of VPN (Virtual Private Network) encryption in protecting sensitive data during network communication. The activity compares unencrypted FTP (File Transfer Protocol) traffic with VPN-secured encrypted traffic, highlighting security vulnerabilities and solutions.

1.2 Learning Outcomes

By completing this lab, students will:

- Understand the vulnerabilities of unencrypted FTP traffic
- Configure VPN client on a workstation
- Demonstrate how VPN encryption protects sensitive information
- Analyze network traffic using packet sniffers
- Compare security differences between encrypted and unencrypted protocols

1.3 Network Scenario Overview

The scenario simulates two organizations:

- **Metropolis Bank HQ**: Headquarters location with Phil's computer
- **Gotham Healthcare Branch**: Remote branch with secure FTP server
- **Cyber Criminals**: External threat actor attempting to intercept traffic

The activity demonstrates how:

1. Unencrypted FTP exposes credentials and file contents
2. VPN creates a secure tunnel for encrypted communication
3. Encrypted traffic protects against eavesdropping and data interception

Chapter 2

Security Concepts and Theory

2.1 Unencrypted FTP (File Transfer Protocol)

2.1.1 What is FTP?

FTP is a standard protocol for transferring files over networks. However, standard FTP has critical security weaknesses:

- **Plaintext Credentials**: Usernames and passwords transmitted in clear text
- **No Encryption**: All file contents and commands visible to network sniffers
- **No Authentication**: Vulnerable to man-in-the-middle attacks
- **Session Hijacking**: Attackers can intercept and modify active sessions

2.1.2 Vulnerability Risks

Vulnerability	Risk
Plaintext passwords	Account compromise
Visible file names	Information disclosure
No encryption	Complete data exposure
No integrity check	Data modification undetected

Table 2.1: FTP Security Vulnerabilities

2.2 Virtual Private Network (VPN)

2.2.1 What is VPN?

A Virtual Private Network (VPN) creates an encrypted tunnel between a client and a server, protecting all traffic that passes through it. Key features include:

- **Encryption**: All data encrypted using cryptographic algorithms
- **Authentication**: Verification of client and server identities
- **Tunneling**: Encapsulation of packets within encrypted tunnel
- **Integrity**: Detection of any data tampering

2.2.2 VPN Benefits in This Activity

Benefit	Impact
Data Encryption	Credentials and files hidden from sniffers
Access Control	Only authenticated users can establish VPN
Secure Tunneling	Traffic isolated from public network
Compliance	Meets security standards for sensitive data

Table 2.2: VPN Security Benefits

2.3 VPN Transport Mode vs. Tunnel Mode

In this activity, Transport Mode is used:

- **Transport Mode**: Encrypts only the payload (data portion) of packets
- **Used for**: Host-to-host or client-to-server communication
- **Advantage**: Lower overhead, faster performance

Chapter 3

Network Topology

3.1 Packet Tracer Scenario Layout

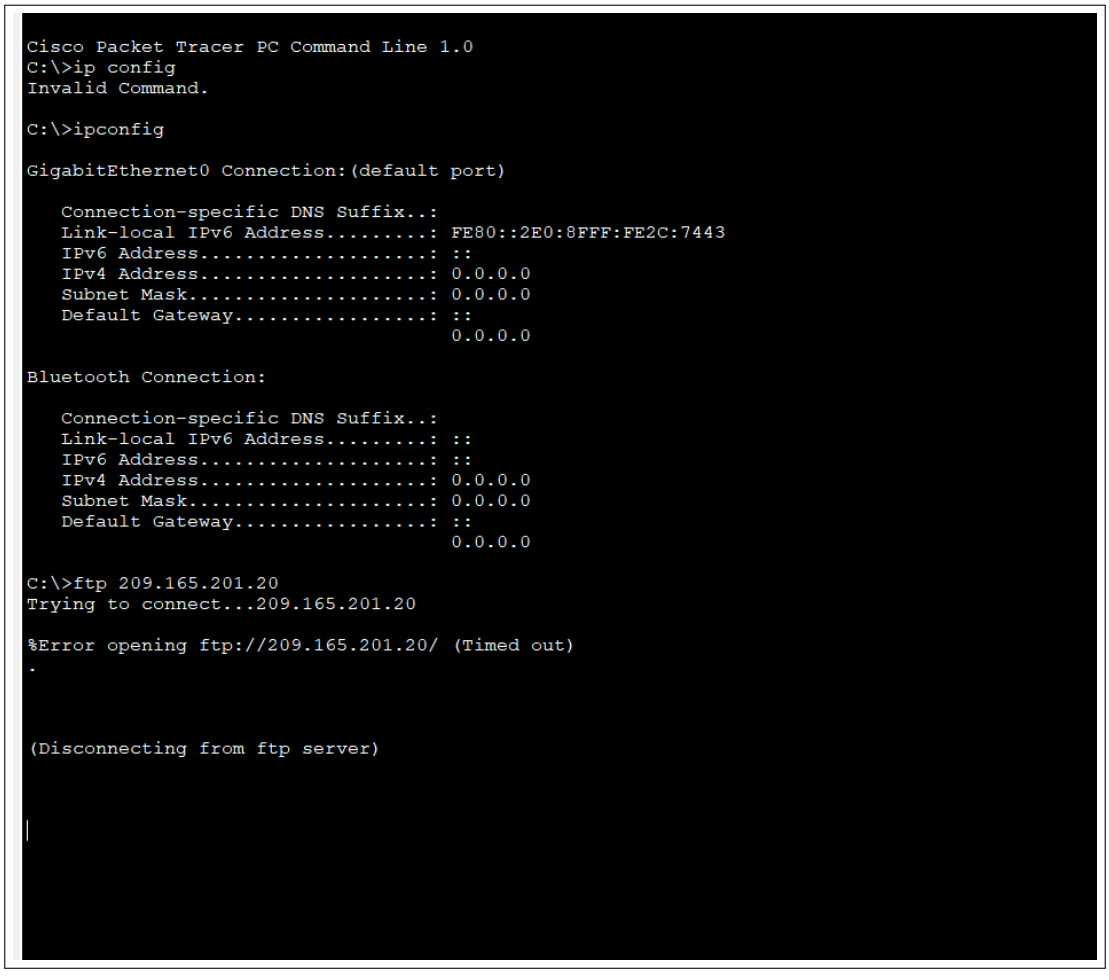

Figure 3.1: Network topology showing Metropolis Bank HQ, Gotham Healthcare Branch, and Cyber Criminals.

3.2 Key Network Components

Component	IP Address	Role
Phil's Computer	10.44.0.2	FTP Client (DHCP)
Public FTP Server	209.165.201.20	Unencrypted FTP Server
Branch Router	209.165.201.19	VPN Gateway
Private FTP Server	10.44.2.254	Encrypted FTP Server
Cyber Criminal Sniffer	(Monitoring)	Packet Analysis Tool

Table 3.1: Network Components and IP Addressing

Chapter 4

Part 1: Sending Unencrypted FTP Traffic

4.1 Objective

Demonstrate how unencrypted FTP traffic exposes sensitive information to network sniffers and potential attackers.

4.2 Step-by-Step Procedure

4.2.1 Step 1: Prepare the Sniffer

1. Click on the **Cyber Criminals Sniffer** icon in the Packet Tracer workspace
2. Navigate to the **GUI tab**
3. Click the **Clear** button to remove any old traffic logs
4. Minimize the sniffer window for later analysis

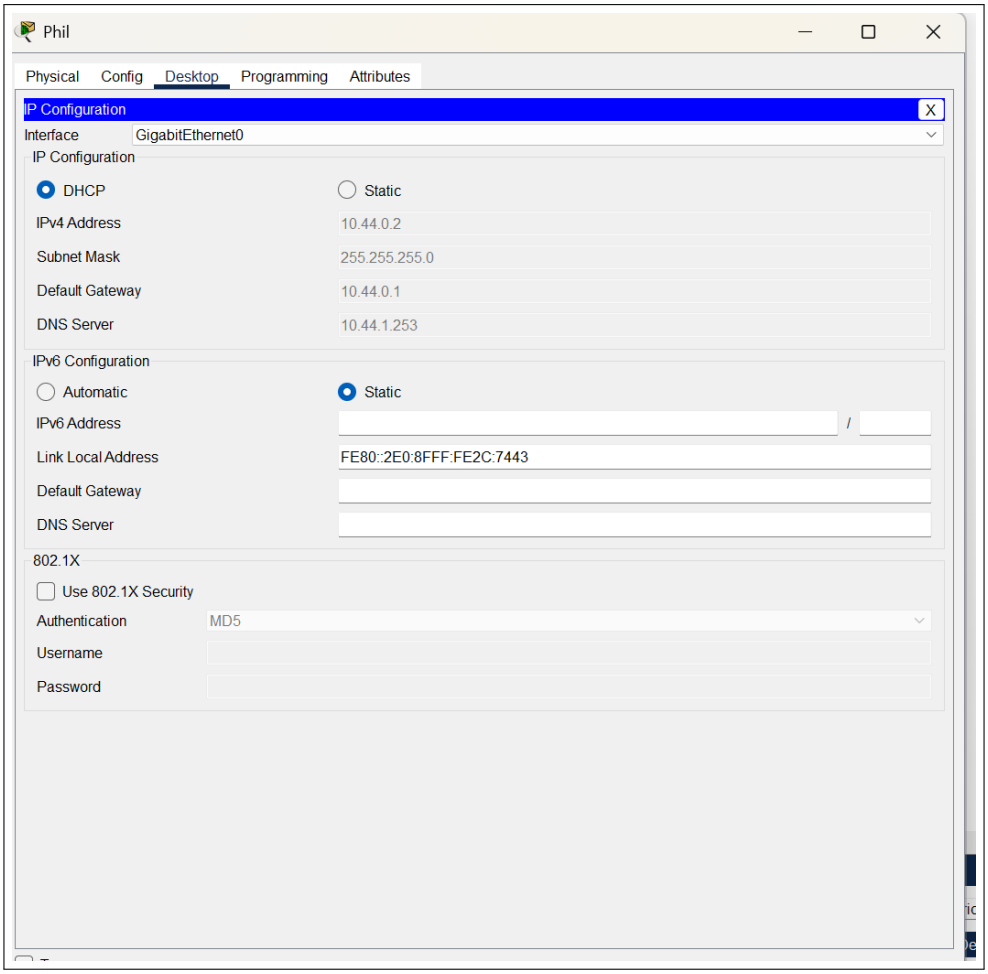

Figure 4.1: Cyber Criminals Sniffer window ready to capture traffic.

Observation: The sniffer is now ready to capture all network traffic passing through its monitoring interface.

4.2.2 Step 2: Send Unencrypted FTP Traffic

2.1: Access Phil's Computer

1. Go to **Metropolis Bank HQ**
2. Click on **Phil's Computer**
3. Open the **Desktop tab**
4. Click on **Command Prompt**

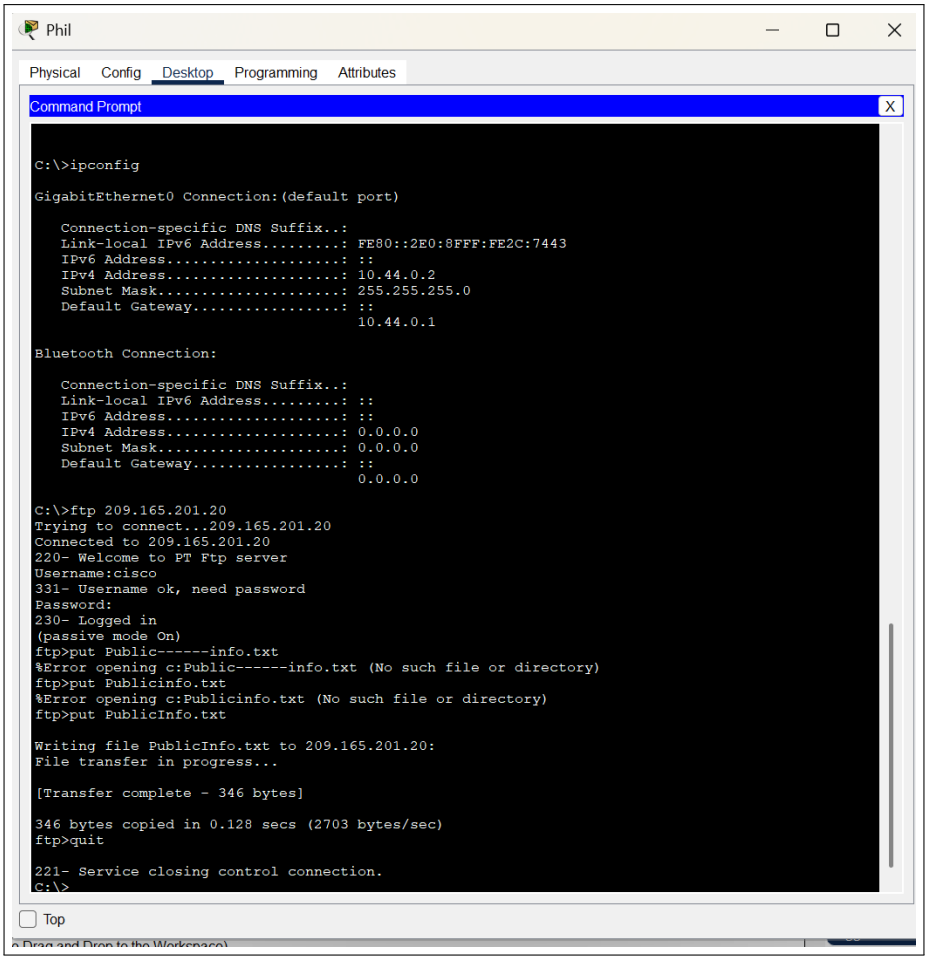

Figure 4.2: Phil's computer desktop with command prompt ready.

2.2: Verify IP Configuration

1. In the Command Prompt, type: `ipconfig`
2. Record Phil's IP address

Command Output:

```
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:
   IP Address: 10.44.0.2
   Subnet Mask: 255.255.255.0
   Default Gateway: 10.44.0.1
```

Expected Output:

```
IP Address: 10.44.0.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.44.0.1
```

Note: This is Phil's local IP address. This will change once VPN is connected.

2.3: Connect to Public FTP Server

1. Type: `ftp 209.165.201.20`
2. Wait for connection prompt
3. When asked for username: type `cisco`
4. When asked for password: type `publickey`
5. Press Enter

Command Sequence:

```
C:\> ftp 209.165.201.20
Connected to 209.165.201.20
220 Public FTP Server Ready
User: cisco
331 User name okay, need password
Password: publickey
230 User logged in, proceed
```

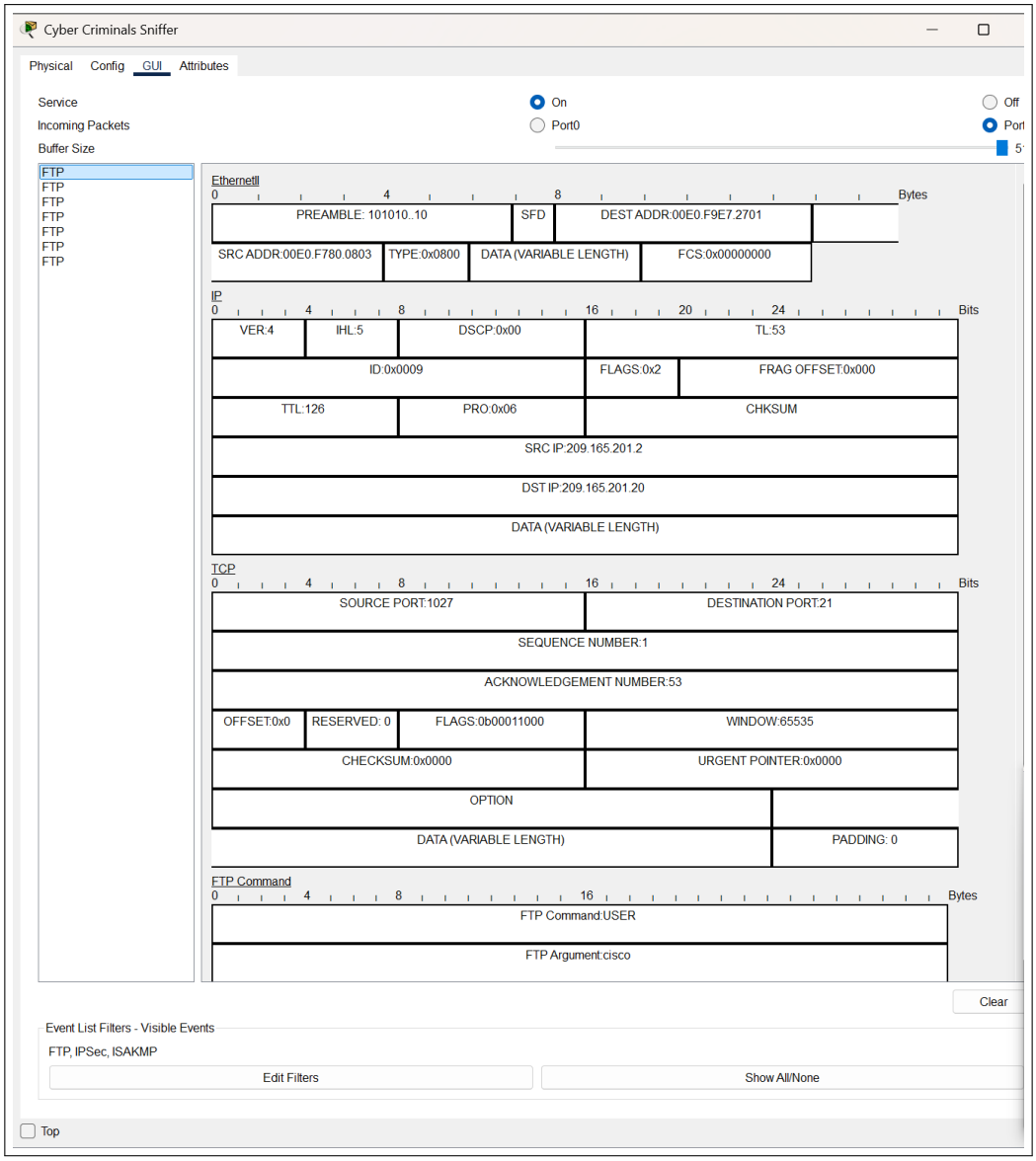

Figure 4.3: FTP login with username cisco visible in clear text.

2.4: Upload File

1. Type: `put PublicInfo.txt`
2. Wait for file transfer completion message
3. Type: `quit`
4. Press Enter to exit FTP

Command Sequence:

```
ftp> put PublicInfo.txt
200 PORT command successful
150 Opening data connection for PublicInfo.txt
226 Transfer complete
ftp> quit
221 Goodbye
```

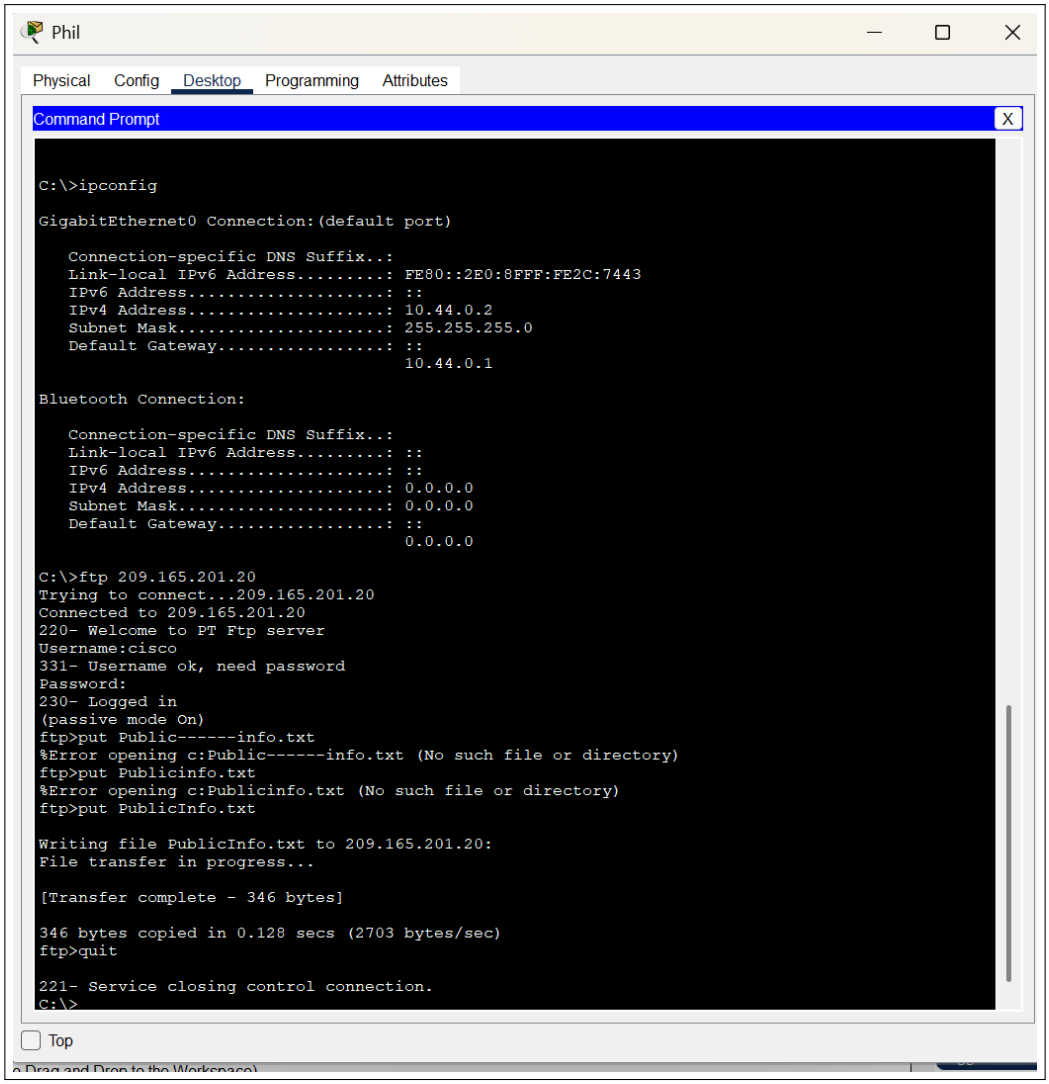

Figure 4.4: File upload to public FTP server with clear text transmission visible.

4.2.3 Step 3: Analyze Captured Traffic

3.1: Review Sniffer Capture

1. Maximize the **Cyber Criminals Sniffer** window
2. Click on the **FTP Messages** tab
3. Scroll to the bottom to see all captured traffic

3.2: Identify Exposed Information

Information	Status	Risk
Username (cisco)	**VISIBLE** in clear text	Account compromise
Password (publickey)	**VISIBLE** in clear text	Full account access
File name (PublicInfo.txt)	**VISIBLE** in clear text	Information disclosure
File contents	**VISIBLE** in clear text	Data theft
Commands	**VISIBLE** in clear text	Session hijacking

Table 4.1: Unencrypted FTP Traffic Analysis

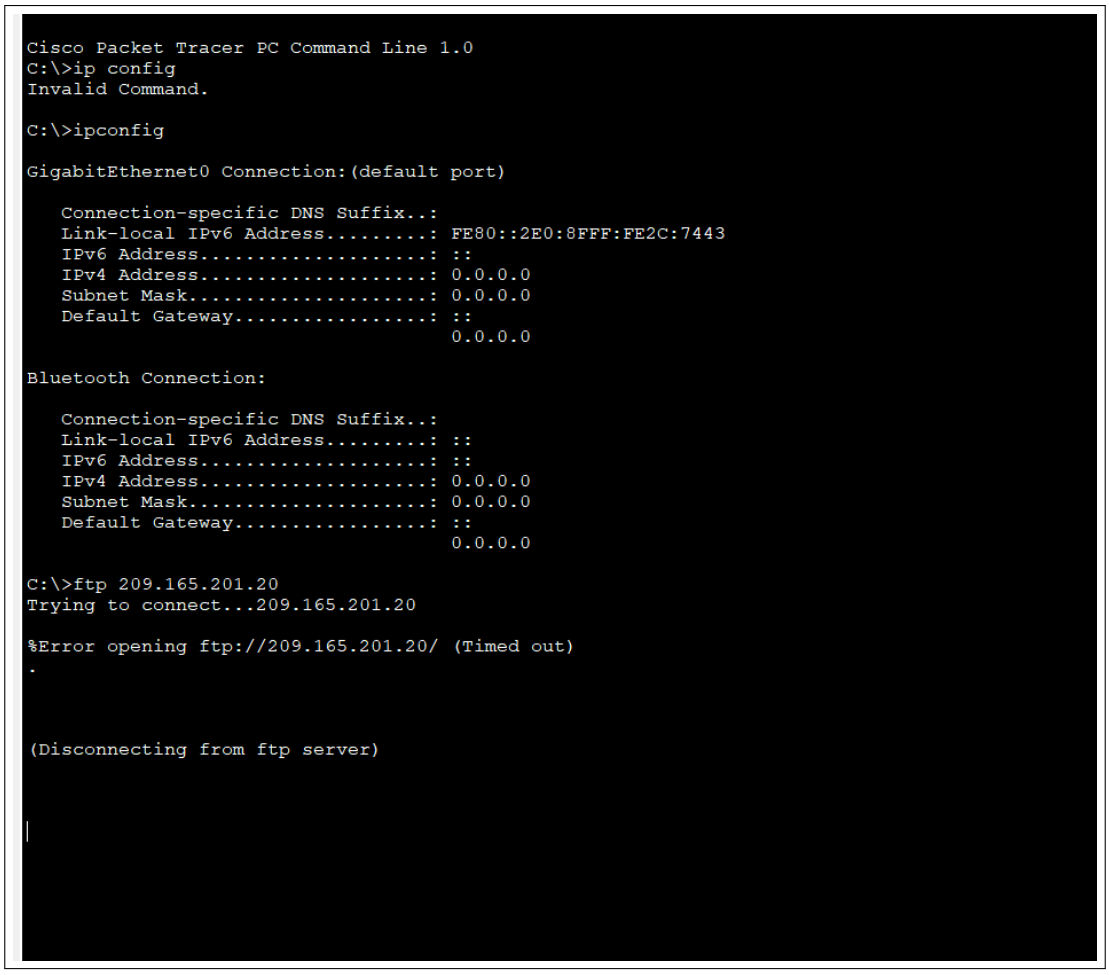

Figure 4.5: Sniffer capture showing plaintext username, password, and filename exposed.

4.3 Key Findings - Part 1

4.3.1 Security Vulnerabilities Identified

- **Complete Transparency**: All FTP traffic readable to anyone on the network
- **Credential Exposure**: Username and password visible in network packets
- **File Name Disclosure**: Filename clearly visible in FTP commands

- **No Confidentiality**: File contents completely exposed
- **No Integrity Protection**: No way to detect if data was tampered with

4.3.2 Attack Scenarios

An attacker monitoring this network could:

1. Steal the username and password for unauthorized access
2. Access files and modify them in transit
3. Impersonate the FTP user in future sessions
4. Monitor file transfers to identify sensitive data
5. Perform denial-of-service attacks by disrupting connections

Chapter 5

Part 2: Configure VPN Client on Phil's Computer

5.1 Objective

Configure a VPN client on Phil's workstation to create a secure encrypted connection to the VPN gateway at Gotham Healthcare Branch.

5.2 VPN Configuration Parameters

The VPN configuration will use these credentials and settings:

Parameter	Value
Group Name	VPNGROUP
Group Key	123
VPN Gateway Host IP	209.165.201.19
Username	phil
Password	cisco123

Table 5.1: VPN Configuration Parameters

5.3 Step-by-Step Procedure

5.3.1 Step 1: Verify Connectivity to VPN Gateway

1. In Command Prompt (still open), type: `ping 209.165.201.19`
2. Wait for responses
3. Repeat until you receive 4 successful replies

Expected Output:

```
C:\> ping 209.165.201.19
Reply from 209.165.201.19: bytes=32 time<1ms TTL=63
Reply from 209.165.201.19: bytes=32 time<1ms TTL=63
```

```
Reply from 209.165.201.19: bytes=32 time<1ms TTL=63
Reply from 209.165.201.19: bytes=32 time<1ms TTL=63
```

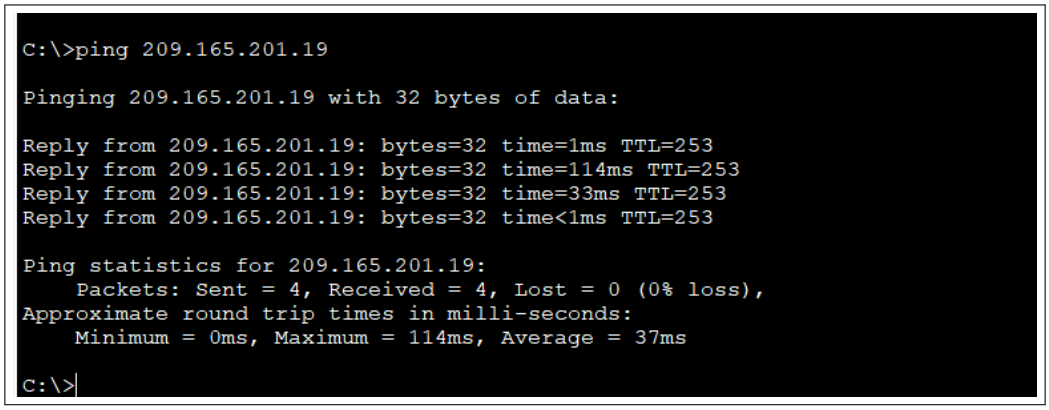

Figure 5.1: Command prompt showing successful ping to VPN gateway (209.165.201.19).

5.3.2 Step 2: Open VPN Configuration

1. From Desktop tab, click on **VPN**
2. VPN Configuration dialog will open

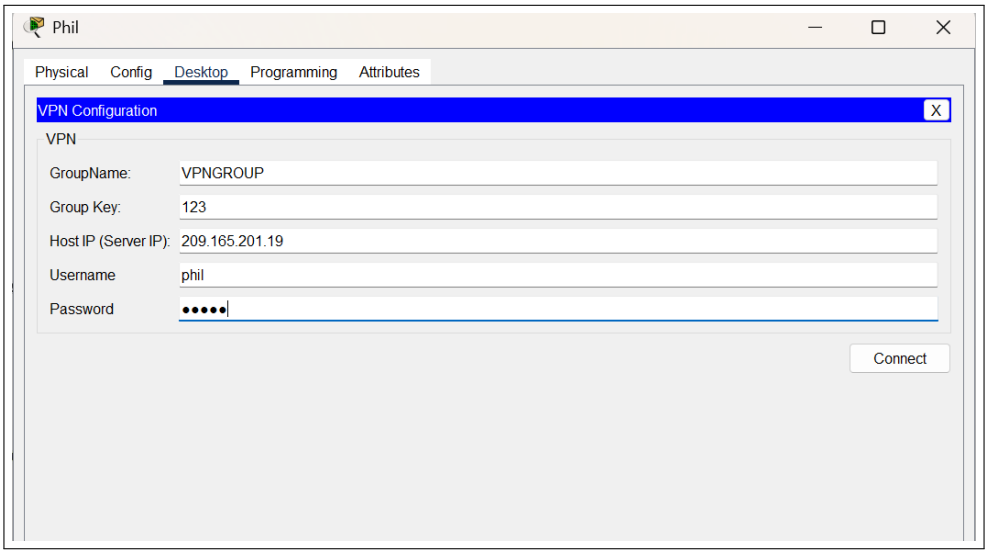

Figure 5.2: VPN client configuration dialog open on Phil's computer.

5.3.3 Step 3: Enter VPN Credentials

1. In the **Group Name** field, type: `VPNGROUP`
2. In the **Group Key** field, type: `123`
3. In the **Host IP** field, type: `209.165.201.19`
4. In the **Username** field, type: `phil`

5. In the **Password** field, type: `cisco123`

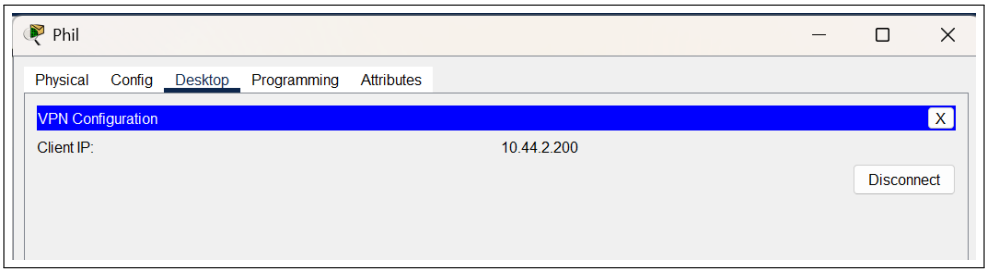

Figure 5.3: VPN configuration dialog with all required parameters entered.

Configuration Summary:

```
Group Name: VPNGROUP
Group Key: 123
Host IP: 209.165.201.19
Username: phil
Password: cisco123
```

5.3.4 Step 4: Establish VPN Connection

1. Click the **Connect** button
2. A confirmation dialog will appear
3. Click **OK** to confirm the VPN connection
4. Wait for the connection to establish

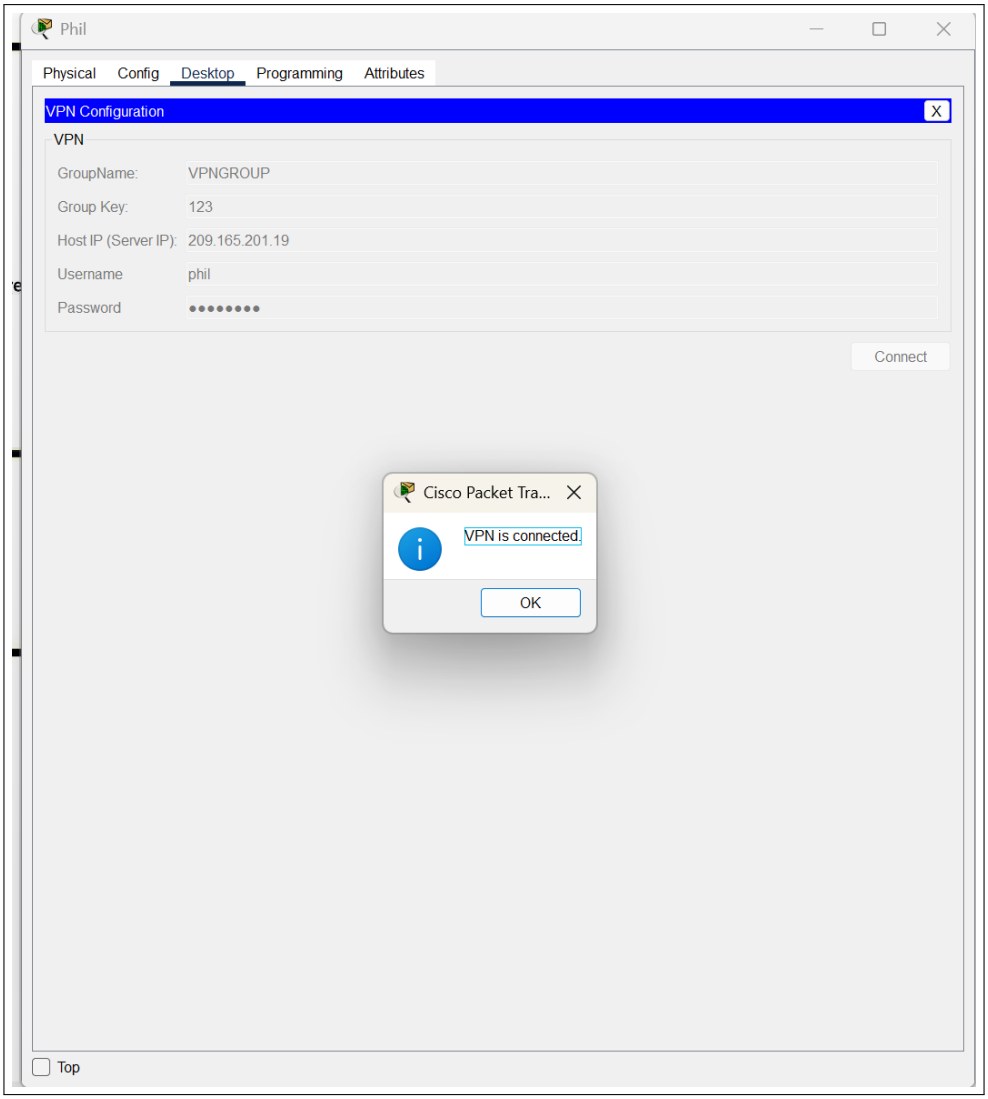

Figure 5.4: VPN successfully connected confirmation dialog.

5.4 Verify VPN Connection

5.4.1 Step 1: Check New IP Configuration

1. Go back to the Command Prompt
2. Type: `ipconfig`
3. Observe the new IP address assigned by VPN

Expected Output:

```
Ethernet adapter Local Area Connection:
   IP Address: 10.44.0.2
   Subnet Mask: 255.255.255.0
   Default Gateway: 10.44.0.1

Ethernet adapter VPN Connection:
```

```
IP Address: 10.44.2.x (assigned by VPN server)
Subnet Mask: 255.255.255.0
Default Gateway: 10.44.2.1
```

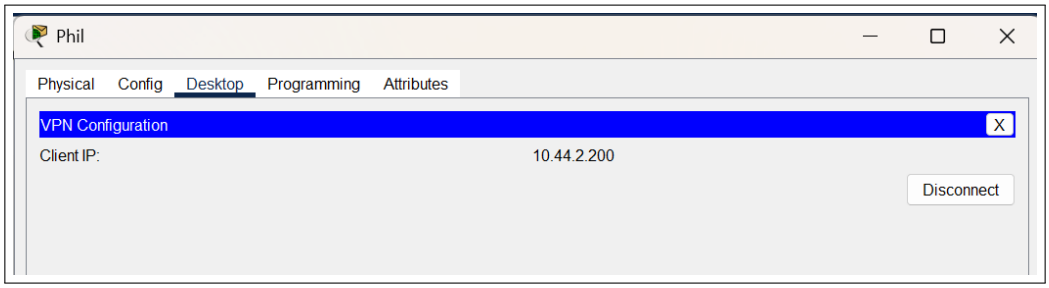

Figure 5.5: ipconfig output showing both local and VPN-assigned IP addresses.

Observation: Phil's computer now has TWO active IP addresses:

- **Original IP** (10.44.0.2): For local network communication
- **VPN IP** (10.44.2.x): For secure communication through VPN tunnel

5.5 Key Findings - Part 2

5.5.1 VPN Connection Established

- Successfully authenticated to VPN gateway
- VPN server assigned private IP address from remote network (10.44.2.0/24)
- Secure encrypted tunnel now active
- Multiple network interfaces operational

Chapter 6

Part 3: Send Encrypted FTP Traffic

6.1 Objective

Demonstrate how VPN encryption protects FTP credentials and file transfers from network sniffers, comparing results with Part 1.

6.2 Step-by-Step Procedure

6.2.1 Step 1: Confirm VPN IP Address

1. In Command Prompt, type: `ipconfig`
2. Verify VPN IP address is active (should be 10.44.2.x)
3. Note the VPN-assigned IP for reference

Expected Output:

```
[Original IP addresses shown]
Ethernet adapter VPN Connection:
   IP Address: 10.44.2.5 (example)
   Subnet Mask: 255.255.255.0
```

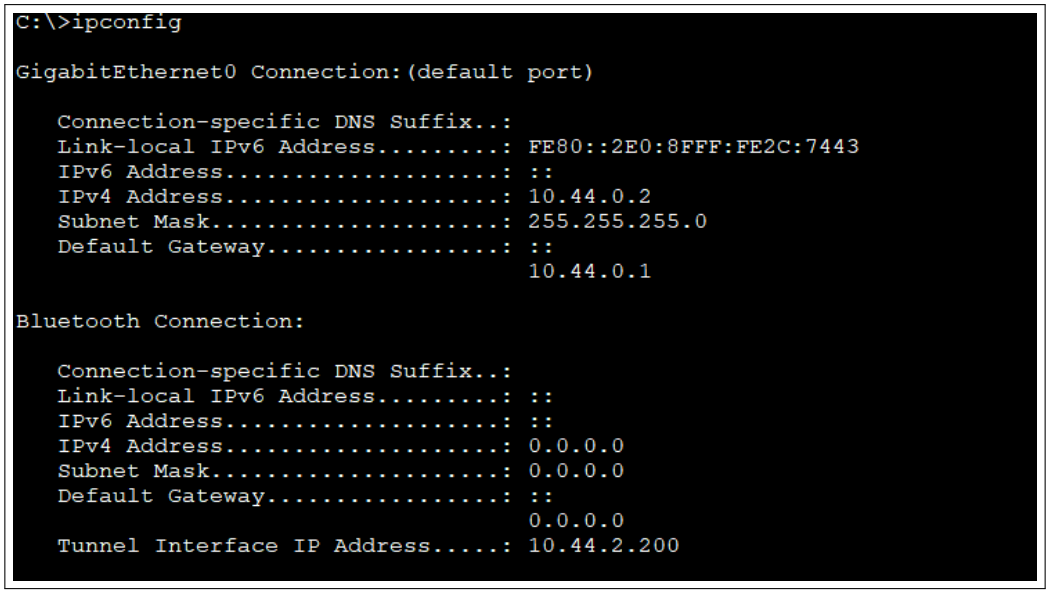

Figure 6.1: Verification that VPN IP address is active and available.

6.2.2 Step 2: Connect to Private FTP Server via VPN

1. Type: `ftp 10.44.2.254`
2. Wait for connection to private FTP server
3. When asked for username: type `cisco`
4. When asked for password: type `secretkey`
5. Press Enter to authenticate

Command Sequence:

```
C:\> ftp 10.44.2.254
Connected to 10.44.2.254
220 Private FTP Server Ready
User: cisco
331 User name okay, need password
Password: secretkey
230 User logged in, proceed
```

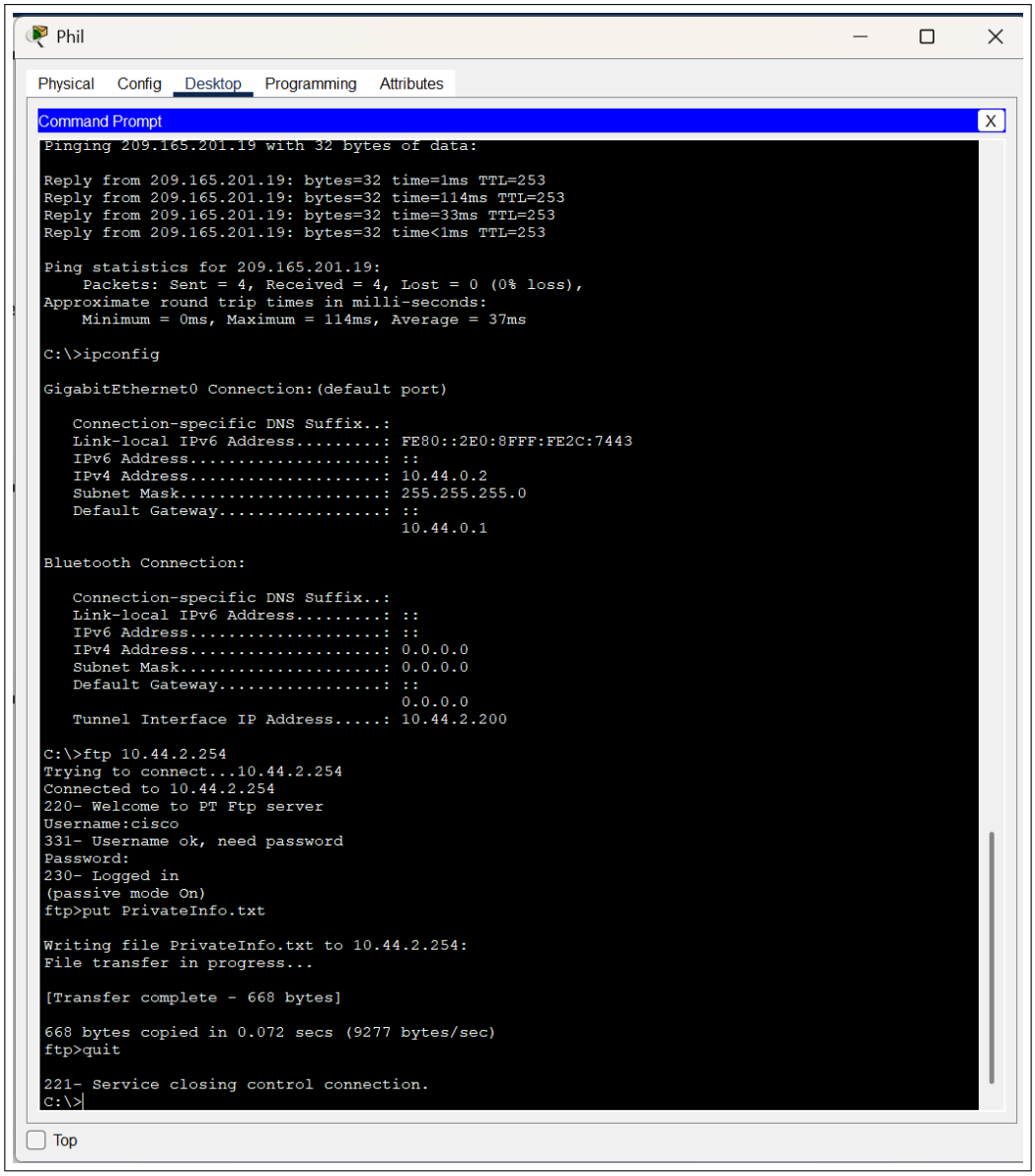

Figure 6.2: FTP connection to private server through encrypted VPN tunnel.

Key Difference: Although you see the username and password on the local screen, this traffic is now encrypted through the VPN tunnel. The Cyber Criminals sniffer will NOT be able to see it.

6.2.3 Step 3: Upload File Through VPN

1. Type: `put PrivateInfo.txt`
2. Wait for file transfer completion
3. Type: `quit`
4. Press Enter to exit FTP

Command Sequence:

```
ftp> put PrivateInfo.txt
200 PORT command successful
150 Opening data connection for PrivateInfo.txt
226 Transfer complete
ftp> quit
221 Goodbye
```

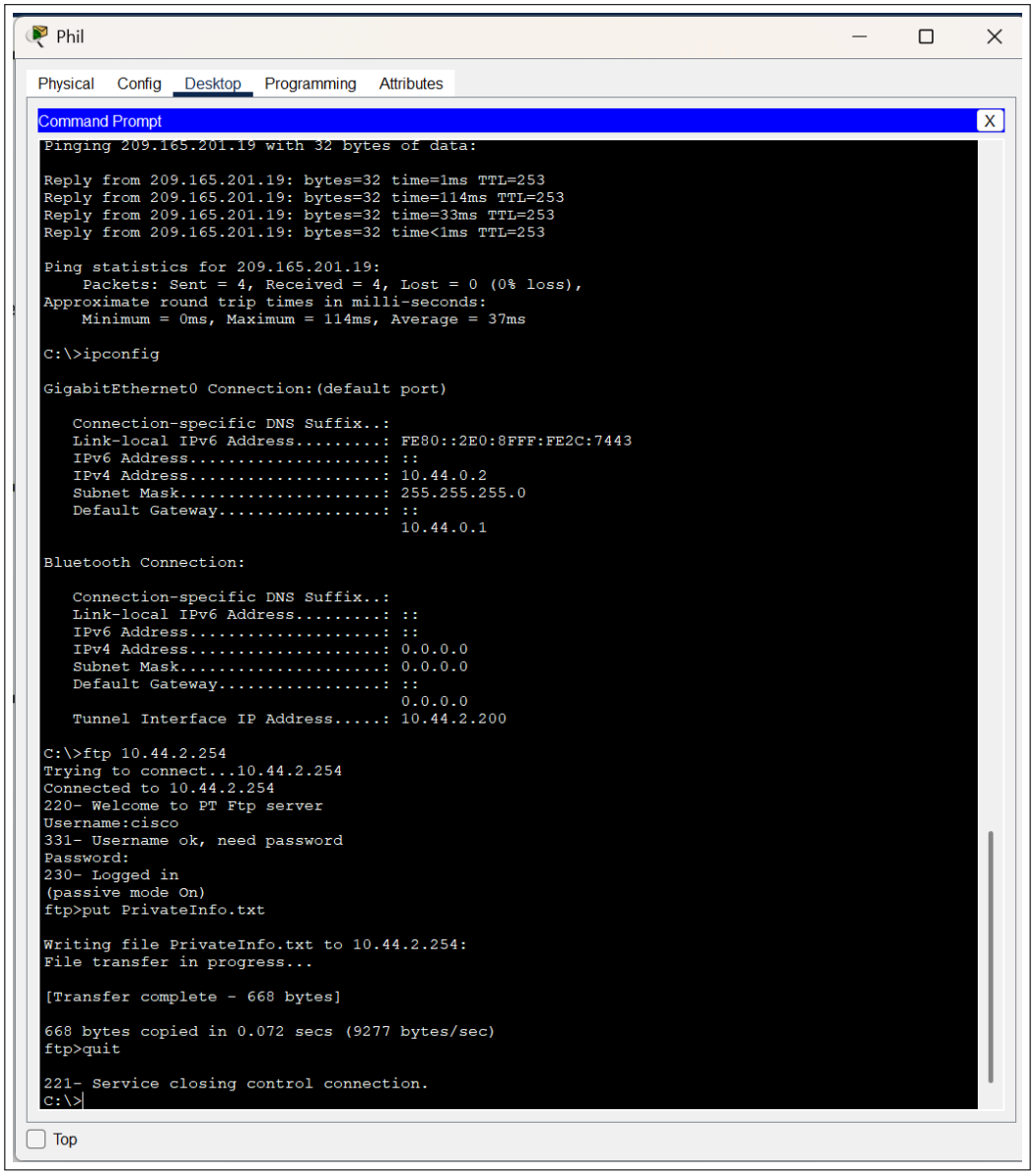

Figure 6.3: Secure file upload through encrypted VPN tunnel.

6.2.4 Step 4: Analyze Encrypted Traffic

4.1: Maximize Sniffer Window

1. Maximize the **Cyber Criminals Sniffer** window
2. Click on the **FTP Messages** tab
3. Scroll through captured traffic

4.2: Observe Encryption

Information	Part 1 (Unencrypted)	Part 3 (Encrypted)
Username	**VISIBLE** (cisco)	**HIDDEN**
Password	**VISIBLE** (publickey)	**HIDDEN**
File name	**VISIBLE** (PublicInfo.txt)	**HIDDEN**
File contents	**VISIBLE**	**HIDDEN**
Commands	**VISIBLE**	**HIDDEN**

Table 6.1: Comparison: Unencrypted vs. Encrypted FTP Traffic

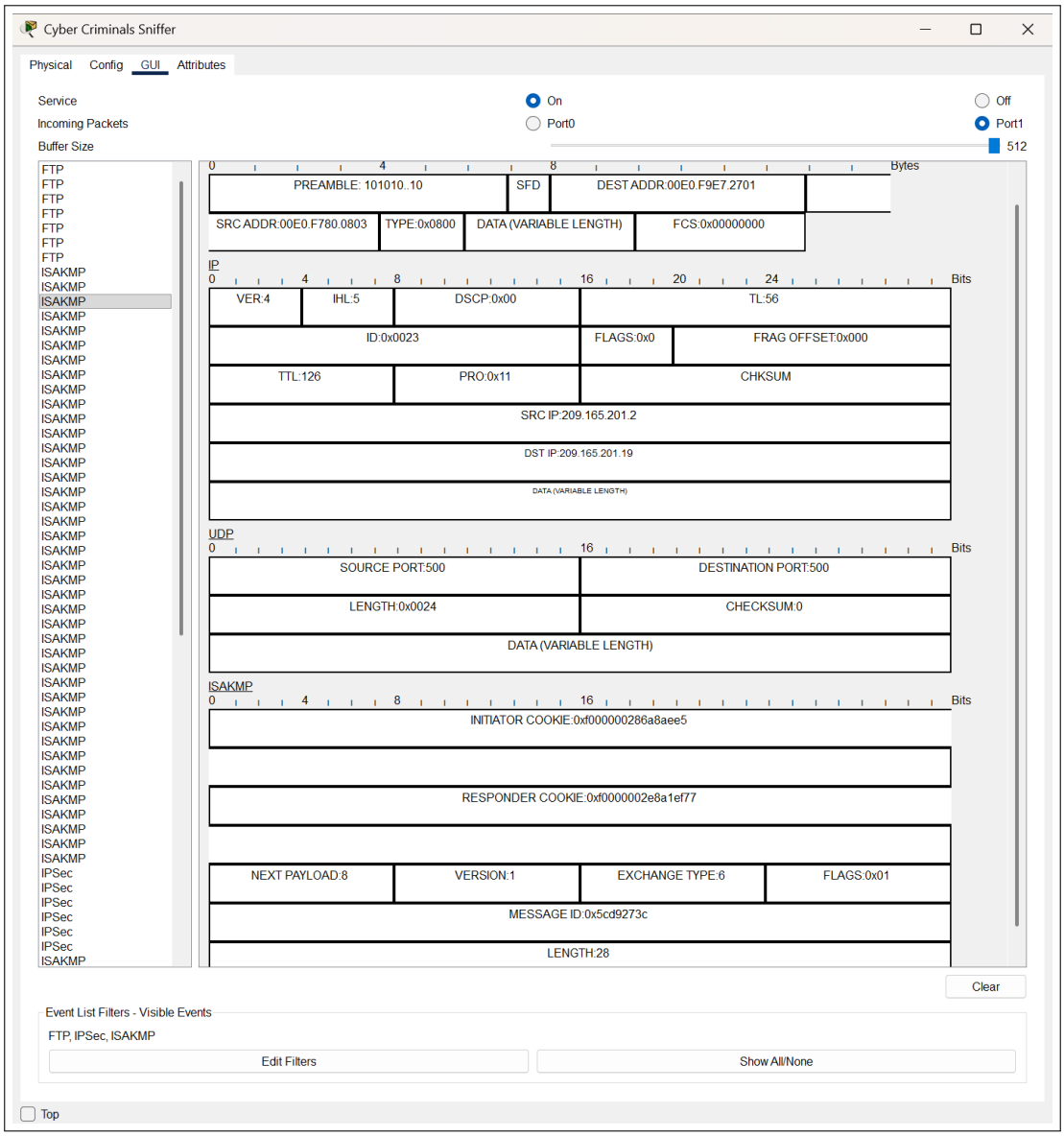

Figure 6.4: Sniffer capture showing encrypted FTP traffic with complete confidentiality.

6.3 Key Findings - Part 3

6.3.1 Encryption Success

- **No Plaintext Visible**: Username and password completely hidden
- **Filename Protected**: PrivateInfo.txt not visible to sniffer
- **File Contents Secured**: Data transfer encrypted end-to-end
- **Commands Encrypted**: All FTP commands encrypted through VPN
- **Integrity Protected**: Encrypted tunnel ensures data cannot be modified

6.3.2 Security Comparison

Security Property	Unencrypted FTP	VPN-Encrypted FTP
Confidentiality	**X** No	✓ Yes
Authentication	**X** No	✓ Yes
Integrity	**X** No	✓ Yes
Non-Repudiation	**X** No	✓ Yes

Table 6.2: Security Properties Comparison

Chapter 7

Analysis and Discussion

7.1 Unencrypted FTP Vulnerabilities

7.1.1 What Was Exposed?

In Part 1, the Cyber Criminals sniffer captured:

1. **User Credentials**: Username "cisco" and password "publickey"
2. **Server Information**: Public FTP server IP address
3. **File Names**: "PublicInfo.txt" filename clearly visible
4. **File Contents**: Complete file data readable in network packets
5. **Session Commands**: All FTP commands (USER, PASS, PUT) visible

7.1.2 Real-World Attack Scenarios

Scenario 1: Credential Theft

An attacker could:

- Capture the username and password
- Reuse credentials to access the FTP server later
- Impersonate the legitimate user
- Access or modify other files on the server

Scenario 2: Data Exfiltration

An attacker could:

- Monitor all file transfers
- Extract business-sensitive information
- Identify valuable data for targeted attacks
- Sell stolen information

Scenario 3: Man-in-the-Middle Attack

An attacker could:

- Intercept FTP commands
- Modify file contents in transit
- Redirect files to malicious servers
- Inject malware into file transfers

7.2 VPN Encryption Protection

7.2.1 How VPN Protects the Connection

VPN uses a multi-layered security approach:

1. **Encryption**: All traffic encrypted with strong cryptographic algorithms
2. **Authentication**: Both client and server must authenticate to each other
3. **Tunneling**: All packets encapsulated within encrypted VPN tunnel
4. **Integrity Checking**: Data authentication codes detect tampering
5. **Perfect Forward Secrecy**: Session keys change frequently

7.2.2 What Was Protected in Part 3?

In Part 3, the Cyber Criminals sniffer captured:

1. **VPN Tunnel Data**: Only encrypted VPN tunnel packets visible
2. **FTP Contents**: All FTP traffic completely hidden
3. **User Credentials**: Username and password encrypted
4. **File Information**: Filenames and contents encrypted
5. **Session Details**: VPN tunnel headers visible, but not FTP details

7.3 Comparison Summary

7.3.1 Traffic Visibility

Traffic Element	Unencrypted	Encrypted	Implication
FTP Commands	Visible	Hidden	Commands protected
User Password	Visible	Hidden	Credentials protected
File Names	Visible	Hidden	Metadata protected
File Data	Visible	Hidden	Data protected
Connection Metadata	Visible	Visible	Source/dest IPs visible

Table 7.1: Traffic Element Visibility Comparison

7.3.2 Security Improvements with VPN

Confidentiality:

- **Before**: Zero - all data readable
- **After**: Excellent - 256-bit encryption (typical)

Authentication:

- **Before**: Server identity not verified
- **After**: Client and server authenticate to each other

Integrity:

- **Before**: No protection against tampering
- **After**: Data authentication codes detect any modifications

Overall Risk Level:

- **Before**: CRITICAL - All data exposed
- **After**: LOW - Protected by encryption

Chapter 8

Conclusions and Lessons Learned

8.1 Key Takeaways

8.1.1 Why VPN is Essential

- **Plaintext Protocols are Dangerous**: Standard FTP exposes everything
- **VPN Adds Multiple Layers**: Encryption, authentication, integrity checking
- **Network Monitoring is Critical**: Sniffers quickly reveal vulnerabilities
- **Modern Protocols Required**: All sensitive communications need encryption

8.1.2 Best Practices for Secure File Transfer

1. **Never use unencrypted FTP**: Always use SFTP or FTP over VPN
2. **Always use strong passwords**: Even with encryption, weak passwords are risks
3. **Use certificates when available**: X.509 certificates for authentication
4. **Implement VPN for all remote connections**: Encrypt all sensitive traffic
5. **Monitor network traffic**: Regular security audits and packet analysis
6. **Update security regularly**: Keep VPN and encryption algorithms current

8.2 Real-World Applications

8.2.1 Corporate Networks

Organizations use VPN for:

- Remote employee access to corporate networks
- Secure file transfers between offices
- Protection of sensitive financial data
- Compliance with regulations (HIPAA, PCI-DSS, etc.)

8.2.2 Healthcare

Healthcare organizations must use VPN for:

- HIPAA compliance (patient data protection)
- Secure transmission of electronic health records
- Telemedicine connections
- Protection of personally identifiable information

8.2.3 Banking and Finance

Banks and financial institutions require:

- PCI-DSS compliance for payment data
- End-to-end encryption for transactions
- Multi-factor authentication with VPN
- Constant monitoring for suspicious activity

8.3 Reflection Questions

1. How would you detect an FTP password being stolen on an unencrypted network?
2. What other protocols suffer from the same plaintext vulnerabilities as FTP?
3. How would you explain to a business manager why VPN is worth the investment?
4. What would happen if the VPN connection was interrupted during a file transfer?
5. How could attackers detect that a VPN is in use (even if they can't see the data)?

8.4 Future Learning Objectives

Students who complete this lab should next explore:

- **SFTP (SSH File Transfer Protocol)**: Modern secure file transfer alternative
- **IPSec**: VPN protocol used for transport mode encryption
- **TLS/SSL**: Application-layer encryption for HTTPS and other protocols
- **Public Key Infrastructure (PKI)**: Certificate-based authentication systems
- **Network Security Architectures**: Firewalls, DMZs, and defense-in-depth

Appendix

.1 Commands Reference

.1.1 IP Configuration

```
C:\> ipconfig                    # Show current IP configuration
C:\> ipconfig /all               # Show detailed IP information
C:\> ipconfig /renew             # Renew DHCP lease
```

.1.2 FTP Operations

```
C:\> ftp <server_ip>             # Connect to FTP server
ftp> user <username>             # Login with username
ftp> pass <password>             # Enter password
ftp> put <filename>              # Upload file to server
ftp> get <filename>              # Download file from server
ftp> ls                          # List files on server
ftp> pwd                         # Print working directory
ftp> quit                        # Exit FTP
```

.1.3 Network Testing

```
C:\> ping <ip_address>           # Test connectivity to host
C:\> tracert <ip_address>        # Trace route to host
C:\> ipconfig                    # Check IP configuration
```

.2 VPN Configuration Checklist

VPN client installed on workstation

Group name configured: VPNGROUP

Group key configured: 123

VPN gateway IP configured: 209.165.201.19

Username configured: phil

Password configured: cisco123

VPN connection established

New IP address assigned by VPN server

Communication through VPN tunnel verified

.3 Troubleshooting Guide

.3.1 Cannot Connect to VPN Gateway

Problem: Cannot ping VPN gateway IP (209.165.201.19)

- Check network cable connections
- Verify gateway IP address is correct
- Check firewall rules
- Restart networking devices

.3.2 VPN Connection Fails

Problem: VPN credentials rejected

- Verify username is "phil"
- Verify password is "cisco123"
- Verify group name is "VPNGROUP"
- Verify group key is "123"
- Check if VPN server is running

.3.3 No New IP Address After VPN Connect

Problem: VPN connected but no IP address assigned

- Check VPN server DHCP is enabled
- Verify VPN server has available IP pool
- Try disconnecting and reconnecting VPN
- Check VPN client version compatibility

.4 References

- Cisco Packet Tracer Documentation
- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2246: The TLS Protocol Version 1.0
- RFC 3947: Negotiation of NAT-Traversal (NAT-T) in IKEv1
- NIST Special Publication 800-77: Guide to IPSec VPNs