

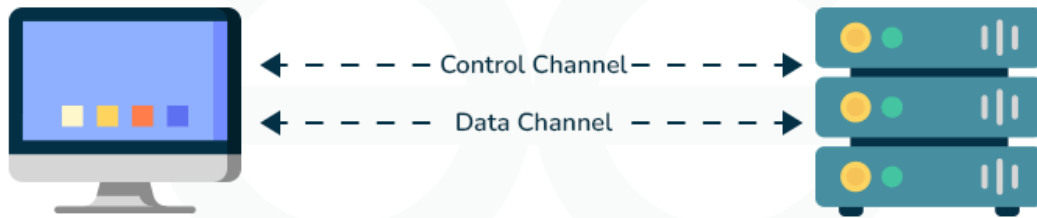
# **ASSIGNMENT NUMBER 01**

**NAME: WAJID IQBAL**

**ASSIGNMENT: FTP, TELNET,  
RDESKTOP, DORA WIRESHARK**

**SUBMITTED BY: SIR MOIZUDDIN  
RAFFAY**

# FTP



Use Case :- Upload / Download Files



What is FTP?

FTP, or **File Transfer Protocol**, is a standard network protocol used for transferring files between a client and a server over a computer network. It operates on the client-server model, where the client initiates a connection to the server to upload or download files.

## Key Features of FTP:

1. **File Transfer:** FTP allows users to transfer files from one host to another, enabling both uploads and downloads.
2. **Authentication:** FTP typically requires a username and password for authentication, although anonymous access is also possible.
3. **Modes of Transfer:**
  - **Active Mode:** The client opens a port and listens while the server actively connects to it.
  - **Passive Mode:** The server opens a port and waits, allowing the client to connect to it.
4. **Data Representation:** FTP supports different data types (ASCII and binary) to accommodate different types of files.
5. **Command and Data Channels:** FTP uses two separate channels:
  - **Command Channel:** Used for sending commands and receiving responses.
  - **Data Channel:** Used for transferring file data.
6. **Security:** By default, FTP is not encrypted, making it vulnerable to interception. Secure versions like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) are used to encrypt the data transfer.

## Basic FTP Commands:

- **USER:** Sends the username to the server.
- **PASS:** Sends the password to the server.
- **LIST:** Lists the files and directories on the server.
- **RETR:** Retrieves (downloads) a file from the server.
- **STOR:** Stores (uploads) a file to the server.
- **DELE:** Deletes a file from the server.
- **MKD:** Creates a directory on the server.
- **RMD:** Removes a directory on the server.

### **Applications of FTP:**

- **Website Management:** Web developers use FTP to upload and manage files on web servers.
- **Backup and Recovery:** Transferring backup files between systems.
- **File Sharing:** Sharing large files that are too big to send via email.

### **Advantages:**

- **Ease of Use:** Widely supported and easy to set up.
- **Batch Transfers:** Can handle multiple files and directories efficiently.

### **Disadvantages:**

- **Lack of Encryption:** Default FTP is not secure, making it susceptible to data interception.
- **Firewall Issues:** Active mode can cause issues with firewalls and NAT (Network Address Translation).

For secure file transfers, it is recommended to use **SFTP** (SSH File Transfer Protocol) or **FTPS** (FTP Secure), which provide encryption and enhanced security features.

## FIRST WE CHECK GATEWAY:

```
File Actions Edit View Help
(wajid@Windows8)-[~]
$ route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.0.1     0.0.0.0         UG      100    0      0 eth0
192.168.0.0      0.0.0.0         255.255.255.0   U       100    0      0 eth0
```

## THEN WE CHECK IP:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\wajid787>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4f6:af7e:47ae:263d%11
    IPv4 Address. . . . . : 192.168.0.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{09E8E403-A2EC-42D7-870D-743E4DD07554}:

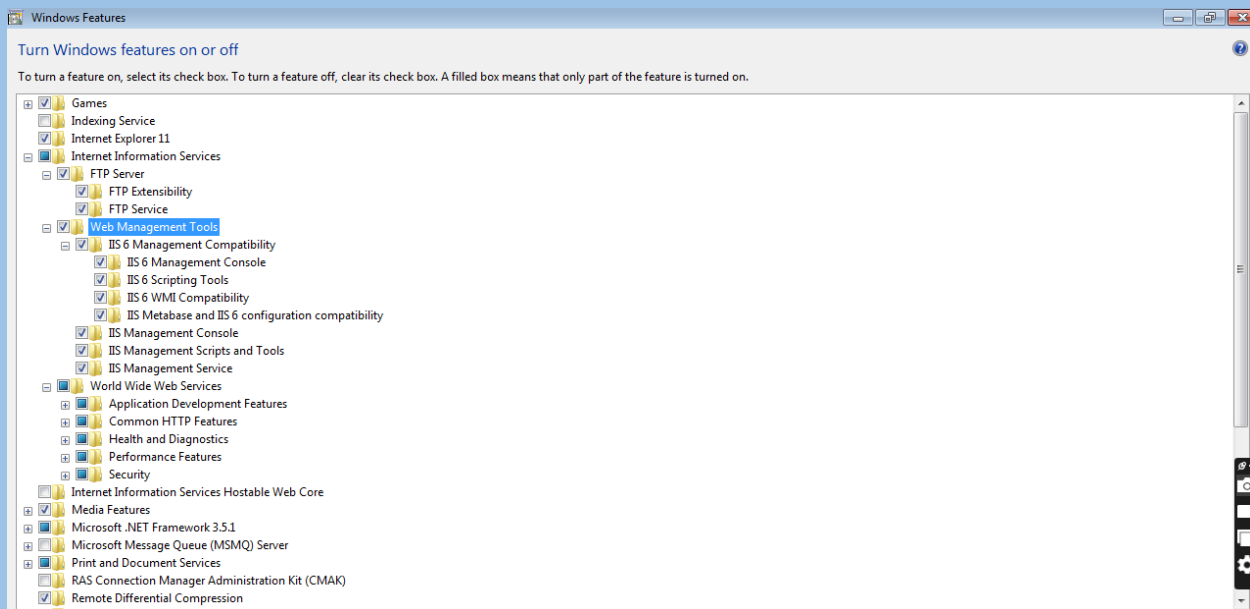
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\wajid787>
```

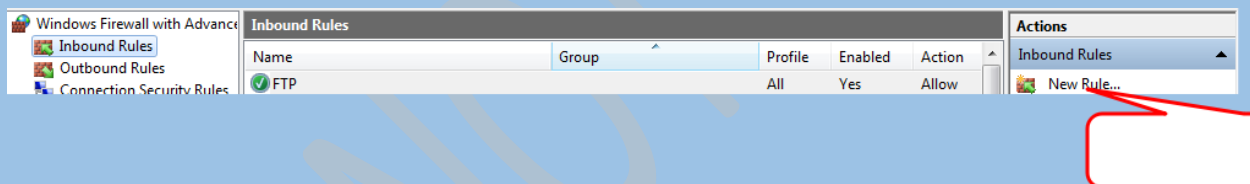
THEN WE CHECK PORT THOUGH TO LINUX:

```
(wajid@Windows8)-[~]  
$ sudo nmap -p21 192.168.0.113  
[sudo] password for wajid:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 00:03 PDT  
Nmap scan report for 192.168.0.113  
Host is up (0.00034s latency).  
  
PORT      STATE      SERVICE  
21/tcp    filtered  ftp  
MAC Address: 08:00:27:8D:C1:CC (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 8.99 seconds
```

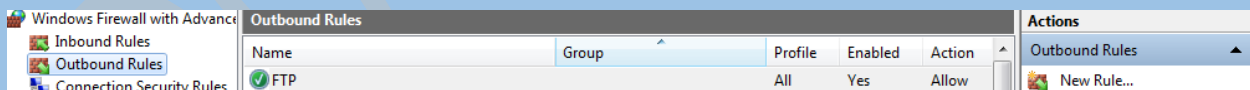
THEN WE WILL ON FTP SERVER WINDOWS FEATURES:



THEN WE WILL CREATE INBOUND RULE FOR FTP:



AFTER WE WILL CREATE OUTBOUND RULE FOR FTP:



THEN WE WILL CHECK THROUGH TO NMAP, FTP PORT IS OPEN OR NOT:

```

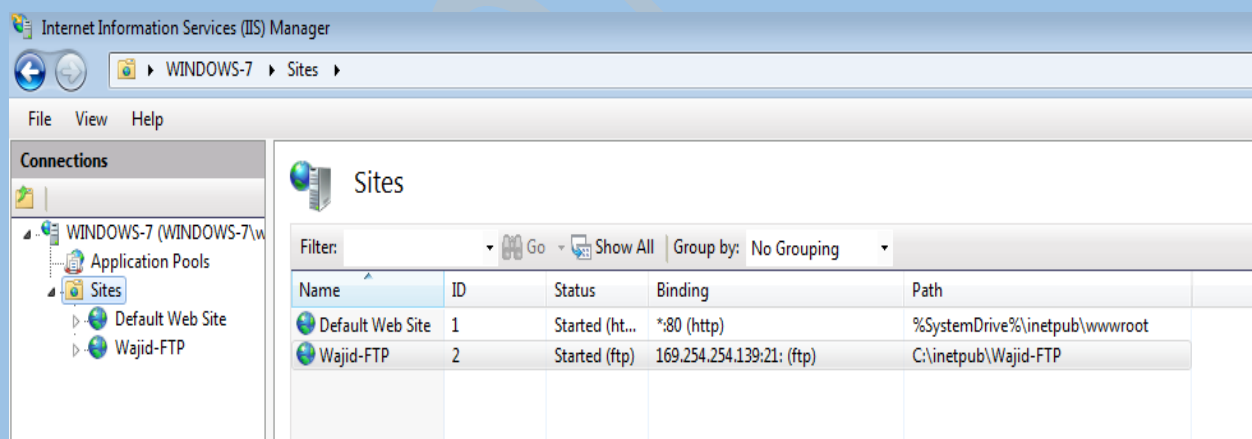
(wajid@Windows8)-[~]
$ sudo nmap -p21 192.168.0.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 00:11 PDT
Nmap scan report for 192.168.0.113
Host is up (0.00042s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:8D:C1:CC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

```

THEN WE WILL CREATE FTP SERVER IN INTERNET INFORMATION SERVICES MANAGER (IIS):



THEN WE WILL CREATE USER ACCOUNT IN COMPUTER MANAGEMENT:



ftpuser

ftpuser



THEN WE WILL CONNECT FTP THROUGH TO LINUX:

```
(wajid@Windows8)-[~]
$ ftp 192.168.0.113
Connected to 192.168.0.113.
220 Microsoft FTP Service
Name (192.168.0.113:wajid): Wajid-FTP
331 Password required for Wajid-FTP.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

NOW IT'S COMPLETE.



# What is Telnet?



## What is Telnet?

Telnet is a network protocol that provides a command-line interface for communication with a remote device or server. It is one of the earliest protocols used on the internet and is designed for bidirectional text-based communication. Telnet allows users to remotely access and manage devices, typically over TCP/IP networks.

### Key Features of Telnet:

1. **Remote Access:** Telnet allows users to connect to and control remote computers or devices, such as servers, routers, or network switches.
2. **Command-Line Interface:** Users interact with the remote system through a text-based command-line interface, similar to a local terminal.
3. **Unencrypted Communication:** Telnet transmits data in plaintext, which includes usernames, passwords, and commands, making it insecure for sensitive data.
4. **Simple Protocol:** Telnet uses a straightforward protocol that establishes a connection and transmits data using TCP on port 23 by default.

## Basic Telnet Commands:

- **open:** Establishes a connection to a specified host (e.g., `open hostname port`).
  - **close:** Closes the current Telnet session.
  - **quit:** Exits the Telnet program.
  - **send:** Sends special Telnet protocol commands.
- **status:** Displays the current status of the Telnet connection.

## Common Uses of Telnet:

- **Network Administration:** Telnet is often used by network administrators to configure and manage network devices such as switches, routers, and firewalls.
- **Remote System Management:** It allows administrators to log into remote servers to perform administrative tasks, such as file management, software installation, and troubleshooting.
- **Testing and Debugging:** Telnet can be used to test and debug network services by connecting to specific ports on remote servers to check their status and response.

## Advantages:

- **Simplicity:** Telnet is simple to use and widely supported.
- **Real-Time Interaction:** Provides immediate interaction with the remote system, making it useful for real-time troubleshooting.

## Disadvantages:

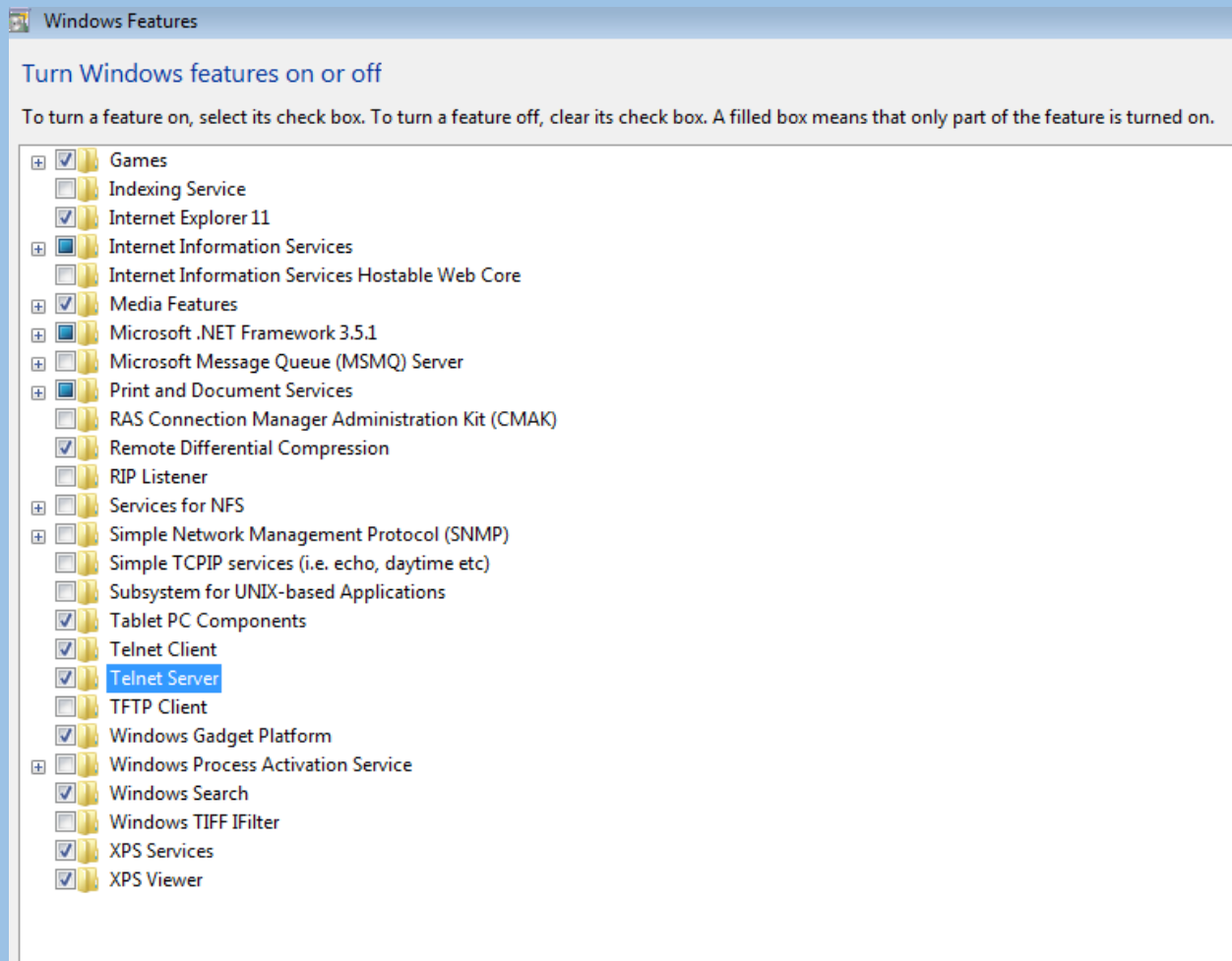
- **Lack of Security:** Telnet's major drawback is its lack of encryption. Data sent over Telnet, including login credentials, can be intercepted and read by attackers.
- **Obsolescence:** Due to its security issues, Telnet has largely been replaced by more secure protocols like SSH (Secure Shell).

## Secure Alternatives:

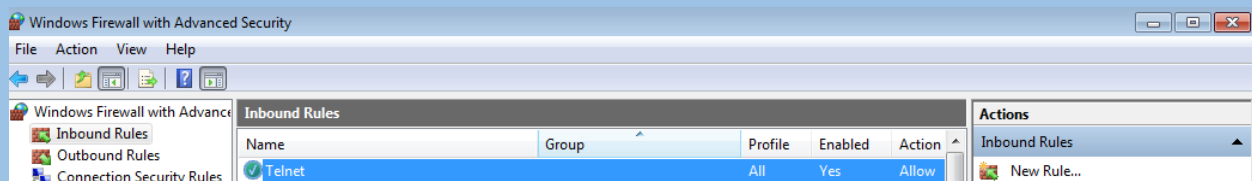
- **SSH (Secure Shell):** SSH is the preferred alternative to Telnet. It provides encrypted communication, ensuring that data transferred between the client and the remote server is secure. SSH uses port 22 by default.
- **SSL/TLS Telnet:** Some implementations of Telnet use SSL/TLS to encrypt the communication, but this is less common than SSH.

In summary, while Telnet played a crucial role in early network communication, its lack of security features has led to its decline in favor of more secure alternatives like SSH.

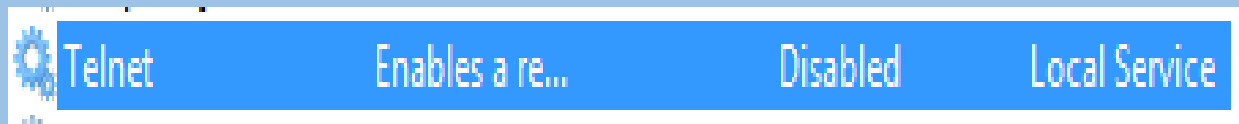
## FIRST WE WILL ON TELNET SERVER WINDOWS FEATURES:



## THEN WE WILL CREATE INBOUND RULE FOR TELNET:



**THEN WE WILL CHECK TELNET SERVICE START OR DISABLE:**



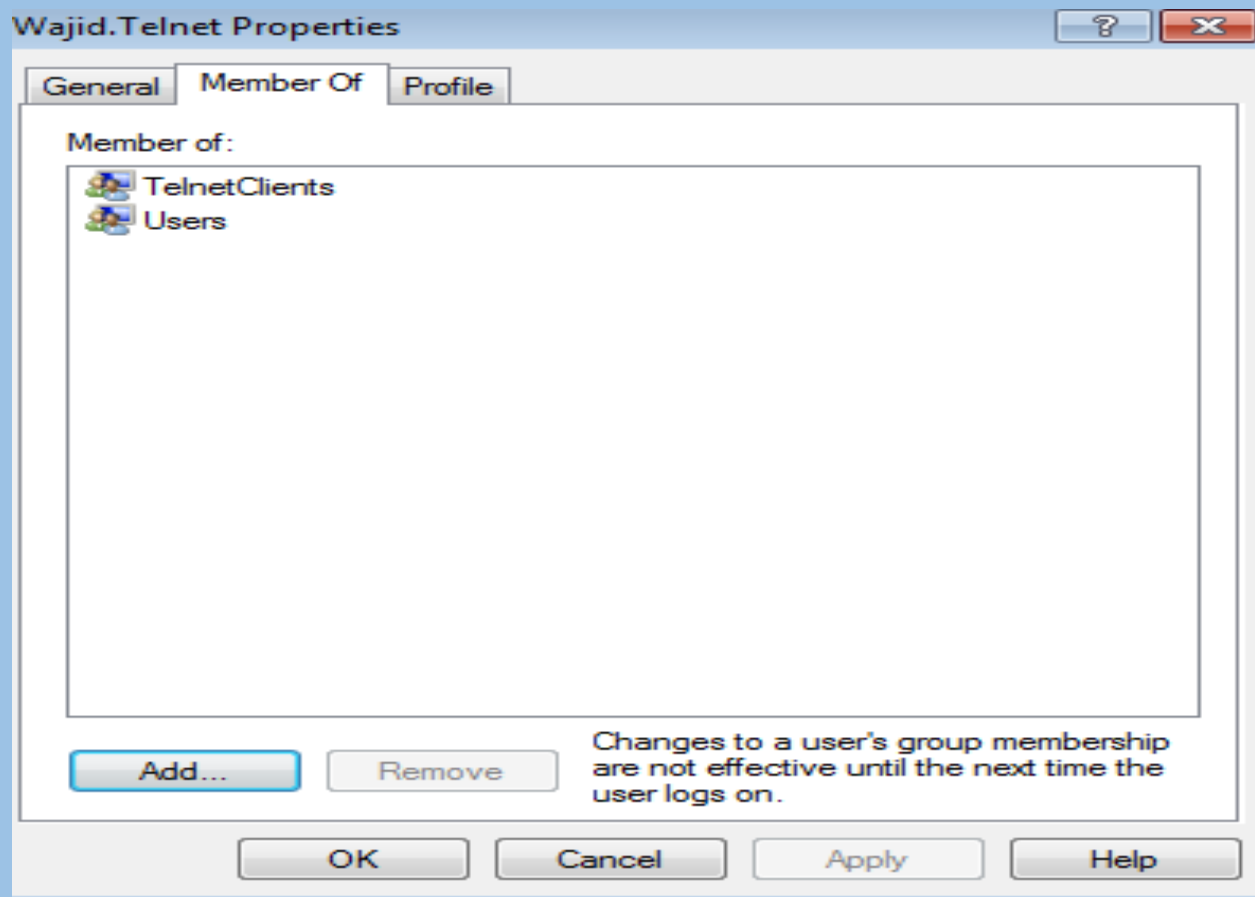
**THEN WE WILL START TELNET SERVICE:**



**THEN WE WILL CREATE USER ACCOUNT IN COMPUTER  
MANAGEMENT:**



THEN WE WILL PERMISSION TELNET:



THEN WE WILL CHECK THROUGH TO NMAP, TELNET PORT IS  
OPEN OR NOT:

```
(wajid@Windows8)-[~]
$ sudo nmap -p23 192.168.0.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 05:54 PDT
Nmap scan report for 192.168.0.109
Host is up (0.00057s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.20 seconds
```

THEN WE WILL CONNECT TELNET THROUGH TO LINUX:

```
(wajid@Windows8)-[~]
$ telnet 192.168.0.109
Trying 192.168.0.109 ...
Connected to 192.168.0.109.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: Wajid.Telnet
password:

*=====
Microsoft Telnet Server.
*=====
C:\Users\Wajid.Telnet>
```

```
*=====
Microsoft Telnet Server.
*=====
C:\Users\Wajid.Telnet>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b0c6:ce9e:b47f:fd6a%14
    IPv4 Address. . . . . : 192.168.0.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{B58C1819-0B72-4307-86D7-30626AEF0BF4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Wajid.Telnet>█
```

NOW IT'S COMPLETE.



## What is rdesktop?

rdesktop is an open-source client for Microsoft's Remote Desktop Protocol (RDP), which allows users to connect to and control remote Windows desktops. It is primarily used on Unix-based systems, including Linux and BSD, to access and manage Windows servers and workstations.

### Key Features of rdesktop:

1. **Remote Desktop Access:** Enables users to access and control a remote Windows desktop from a Unix-based machine.
2. **RDP Support:** Implements the Remote Desktop Protocol (RDP), allowing compatibility with various versions of Windows.
3. **Graphical User Interface (GUI):** Provides a GUI for interacting with the remote Windows desktop, similar to sitting in front of the actual machine.
4. **Multiple Protocol Versions:** Supports multiple versions of the RDP protocol, ensuring compatibility with different Windows operating systems.
5. **Performance Optimization:** Offers options to optimize performance, such as adjusting the screen resolution, color depth, and network bandwidth usage.

### Basic Usage:

To use rdesktop, you typically run it from the command line with various options to specify the remote server and connection settings. Here are some common command-line options:

- `rdesktop [options] server`: Connects to the specified remote Windows server.
  - `-u username`: Specifies the username for login.
- `-p password`: Specifies the password for login (use with caution as it may expose the password in the command history).
  - `-g geometry`: Sets the screen resolution (e.g., `-g 1024x768`).
    - `-f`: Enables full-screen mode.
  - `-a color_depth`: Sets the color depth (e.g., `-a 16` for 16-bit color).
  - `-d domain`: Specifies the domain for login if needed.

### Example Command:

```
rdesktop -u myusername -p mypassword -g 1280x1024 -f myremoteserver
```

### Advantages:

- **Cross-Platform:** Allows Unix-based users to connect to Windows desktops and servers, facilitating cross-platform administration and use.



- **Open Source:** Free to use and modify, with a community contributing to its development and improvement.
- **Customizable:** Offers various options to customize the connection settings according to user preferences and network conditions.

### **Disadvantages:**

- **Security:** Transmitting passwords via command line can be insecure. It is better to use other methods like Kerberos or NTLM for authentication where possible.
- **Protocol Limitations:** While rdesktop supports many features of the RDP protocol, it may not support all advanced features available in newer versions of RDP or proprietary Microsoft RDP clients.
- **Performance:** Performance can vary based on network conditions and the configuration of both the client and server.

### **Alternatives:**

- **Remmina:** A modern, feature-rich remote desktop client that supports RDP, VNC, SPICE, and other protocols.
- **FreeRDP:** Another open-source RDP client that aims to be more compatible with newer versions of the RDP protocol and offers more features than rdesktop.

In summary, rdesktop is a useful tool for Unix-based users who need to access and manage Windows desktops and servers. Despite its limitations, it remains a popular choice due to its simplicity and effectiveness. For more advanced features and better security, alternatives like Remmina and FreeRDP might be preferred.

FIRST WE WILL CHECK THROUGH TO NMAP, RDESKTOP PORT IS OPEN OR NOT:

```
(wajid@Windows8)-[~]  
$ sudo nmap -p3389 192.168.0.109  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-12 06:21 PDT  
Nmap scan report for 192.168.0.109  
Host is up (0.00039s latency).  
  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
MAC Address: 08:00:27:C7:A2:DD (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
```

THEN WE WILL CONNECT RDESKTOP THROUGH TO LINUX:

```
(wajid@Windows8)-[~]  
$ rdesktop 192.168.0.109  
Autoselecting keyboard map 'en-us' from locale  
  
ATTENTION! The server uses and invalid security certificate which can not be trusted for  
the following identified reasons(s);  
  
1. Certificate issuer is not trusted by this system.  
  
Issuer: CN=Windows-7  
  
Review the following certificate info before you trust it to be added as an exception.  
If you do not trust the certificate the connection attempt will be aborted:  
  
Subject: CN=Windows-7  
Issuer: CN=Windows-7  
Valid From: Sat May 11 06:14:17 2024  
To: Sun Nov 10 05:14:17 2024  
  
Certificate fingerprints:  
  
sha1: 37a6c15261fee595303604261ea5b200a908b591  
sha256: f0556b6ce99a259b4b746c2192341a52466ef77427675dd01c710d7167e3b100
```

rdesktop - 192.168.0.109

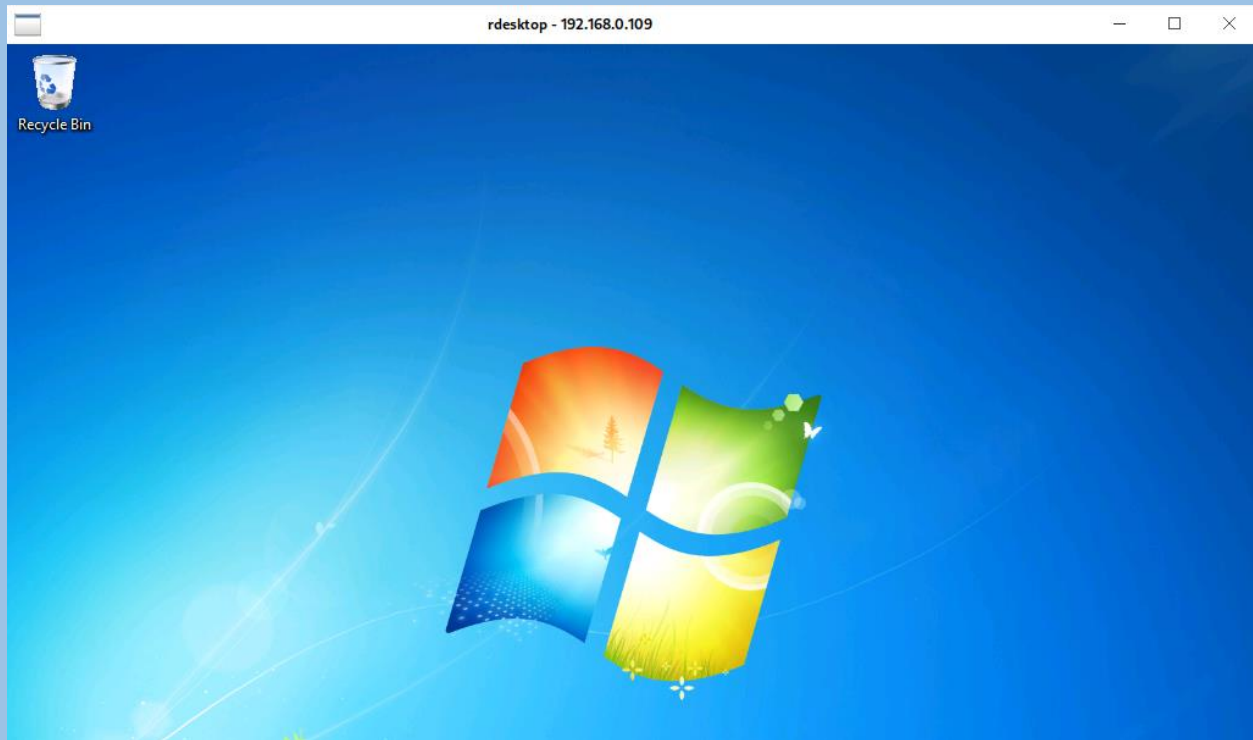


wajid

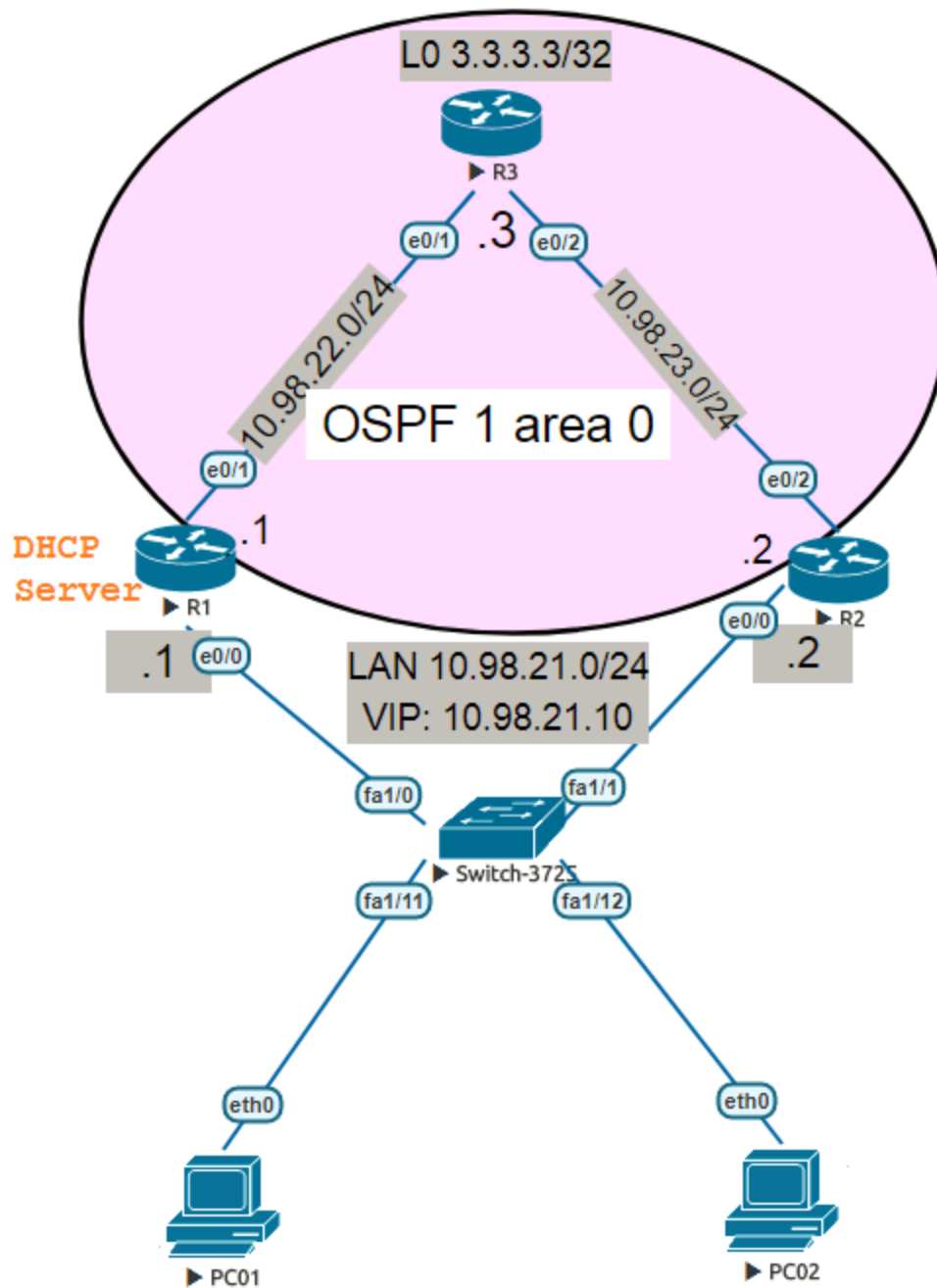


Other User

Cancel



**NOW IT'S COMPLETE.**



What is Dora Process in Wireshark?

In the context of networking and the use of Wireshark, **DORA** refers to the DHCP (Dynamic Host Configuration Protocol) process used to obtain an IP address and other network configuration details from a DHCP server. DORA stands for **Discover, Offer, Request, Acknowledge**. Wireshark is a network protocol analyzer that can capture and display these DHCP messages, allowing for detailed analysis of the DHCP process.

### **DORA Process Steps:**

#### **1. Discover:**

- **Description:** The client (e.g., a computer or device) broadcasts a DHCP Discover message to locate available DHCP servers.
- **Wireshark Capture:** This message can be identified in Wireshark with the message type "DHCP Discover."

#### **2. Offer:**

- **Description:** One or more DHCP servers respond to the Discover message with a DHCP Offer message, which includes an IP address and other network configuration options.
- **Wireshark Capture:** This message is identified as "DHCP Offer."

#### **3. Request:**

- **Description:** The client selects an offer from the received DHCP Offers and broadcasts a DHCP Request message, indicating the chosen DHCP server and requested IP address.
- **Wireshark Capture:** This message is identified as "DHCP Request."

#### **4. Acknowledge:**

- **Description:** The selected DHCP server responds with a DHCP Acknowledge (ACK) message, confirming that the client can use the offered IP address and providing any additional network configuration information.
- **Wireshark Capture:** This message is identified as "DHCP ACK."

### **Analyzing the DORA Process with Wireshark:**

Wireshark can be used to capture and analyze DHCP traffic, allowing you to observe the DORA process in detail. Here's how you can use Wireshark to analyze the DHCP DORA process:

#### **1. Start a Wireshark Capture:**

- Open Wireshark and start capturing packets on the network interface connected to the DHCP client.

#### **2. Filter DHCP Traffic:**

- Use the display filter `bootp` or `dhcp` to filter DHCP traffic, as DHCP messages are part of the BOOTP protocol.
  - Example filter: `dhcp` or `bootp`.

#### **3. Identify DORA Messages:**

- Look for the four key DHCP message types: Discover, Offer, Request, and Acknowledge.
- Each message type will be listed with details in the packet list pane.

#### **4. Examine Message Details:**

- Click on each DHCP message to view detailed information in the packet details pane.
- For example, examine the DHCP Discover message to see the client's MAC address and requested parameters, and the DHCP Offer message to see the IP address being offered by the server.

#### 5. **Analyze Timing and Sequence:**

- Ensure the messages follow the correct sequence: Discover → Offer → Request → Acknowledge.
- Check the timestamps to analyze the timing between each step and identify any delays or issues.

### **Example Wireshark Analysis Steps:**

#### 1. **Capture Start:**

- Start capturing packets before initiating a network connection or DHCP renewal on the client.

#### 2. **Discover Message:**

- Look for a DHCP Discover message from the client. This will be a broadcast message (destination IP 255.255.255.255).

#### 3. **Offer Message:**

- Find the DHCP Offer messages from one or more DHCP servers. These will be directed to the client's MAC address.

#### 4. **Request Message:**

- Locate the DHCP Request message from the client, which selects an IP offer.

#### 5. **Acknowledge Message:**

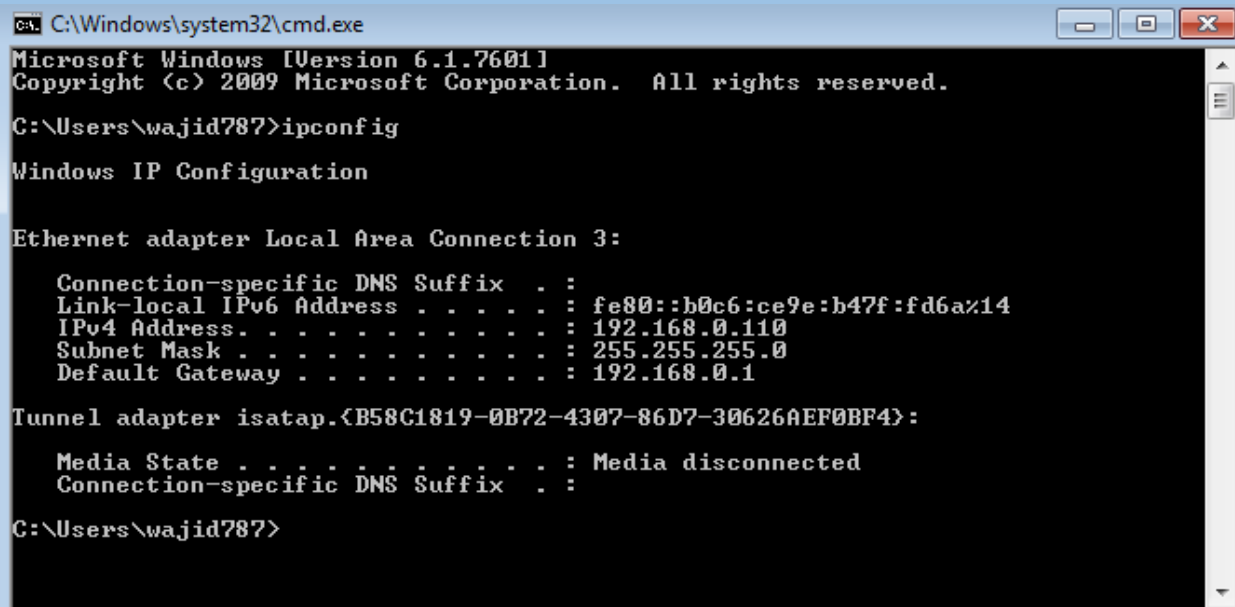
- Finally, find the DHCP ACK message from the selected DHCP server confirming the lease.

### **Troubleshooting with Wireshark:**

- **Missing Messages:** If any of the DORA messages are missing, it indicates where the DHCP process is failing.
- **Network Issues:** Look for signs of network issues such as delays or retransmissions.
- **Configuration Problems:** Verify that the offered IP addresses and configuration details are correct.

In summary, the DORA process in DHCP involves four key steps: Discover, Offer, Request, and Acknowledge. Wireshark is a powerful tool for capturing and analyzing these DHCP messages to ensure proper network configuration and troubleshoot issues.

FIRST WE WILL CHECK IP:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\wajid787>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b0c6:ce9e:b47f:fd6a%14
    IPv4 Address. . . . . : 192.168.0.110
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{B58C1819-0B72-4307-86D7-30626AEF0BF4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\wajid787>
```

THEN WE WILL GIVE STATIC IP:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

|                  |                     |
|------------------|---------------------|
| IP address:      | 192 . 168 . 0 . 115 |
| Subnet mask:     | 255 . 255 . 255 . 0 |
| Default gateway: | 192 . 168 . 0 . 1   |

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

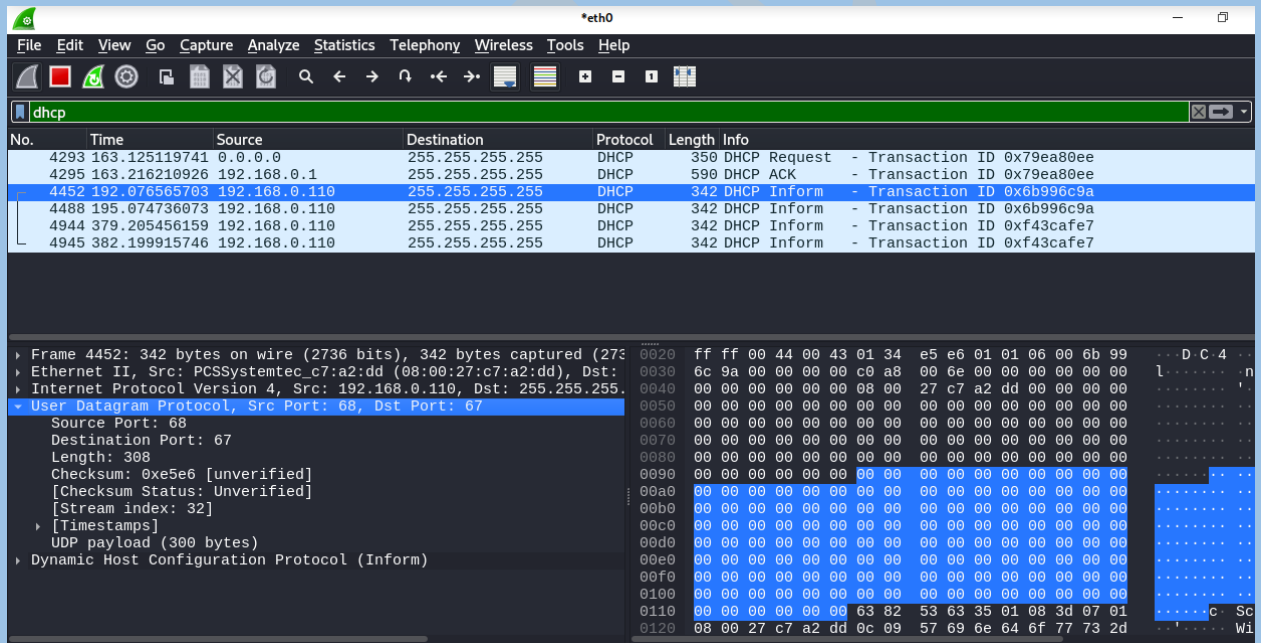
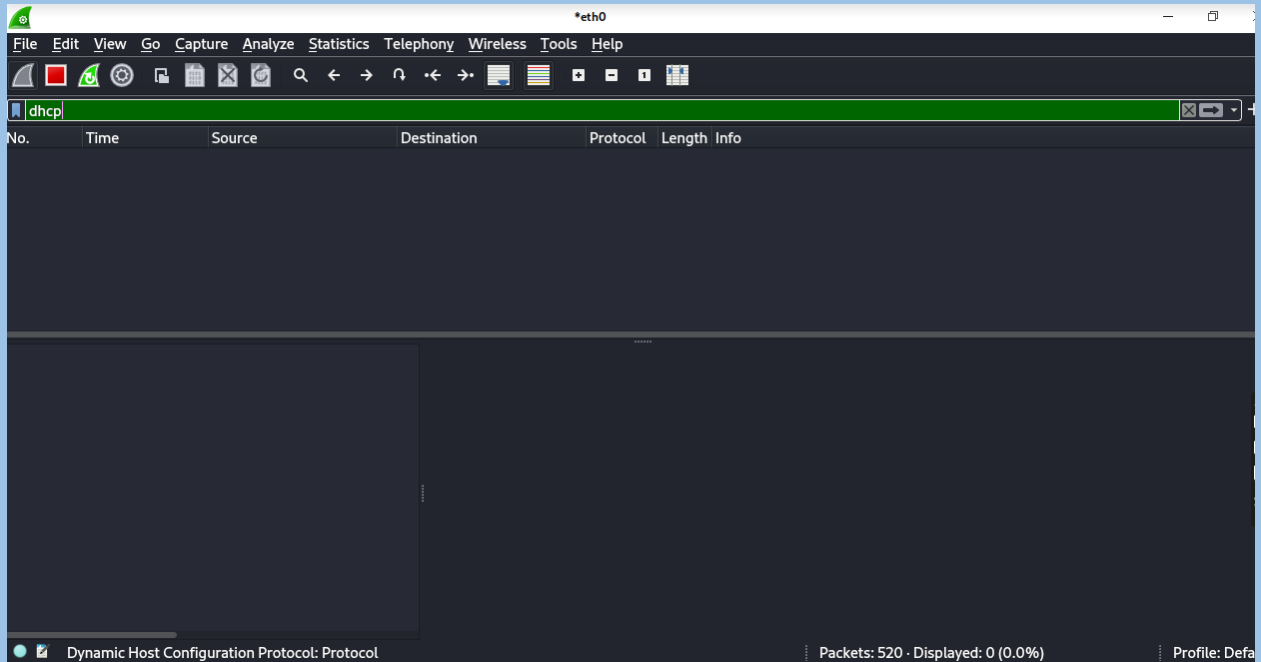
|                       |                   |
|-----------------------|-------------------|
| Preferred DNS server: | 192 . 168 . 0 . 1 |
| Alternate DNS server: | . . .             |

☐ Validate settings upon exit

Advanced...

OK Cancel

THEN WE WILL START PROCESS:



NOW IT'S COMPLETE