

NAME-ARPAN TOMAR

Branch-MAC

2022UCM2341

MAC 5th Sem

Instructor-Dr. Vipin Pal

COMPUTER NETWORKS

INDEX

|  |  |
| --- | --- |
| S.No. | Practical |
| 1 | Computer Network Commands |
| 2 | Create a LAN in Cisco packet tracer |
| 3 | Understand how to configure a router with basic settings to enable inter-network communication. |
| 4 | Learn how to set up a DHCP server in Packet Tracer to automatically assign IP addresses to network devices. |
| 5 | Learn how to manually configure static routes on routers to control network traffic paths. |
| 6 | Understand how NAT works to enable private IP addresses to communicate with external networks. |
| 7 | Familiarity with wireshark |

**Computer Network commands**

**traceroute**

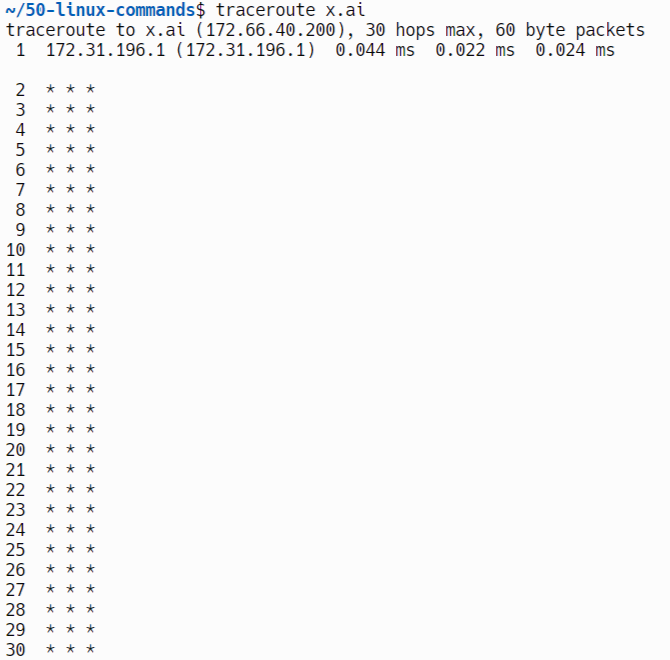
 **Purpose**: Traces the path packets take to a network host.

 **Syntax**: traceroute [options] destination

 **Options**:

* -m max\_ttl: Set the max number of hops.
* -p port: Set the destination port number.

Ouput:



+**ifconfig**

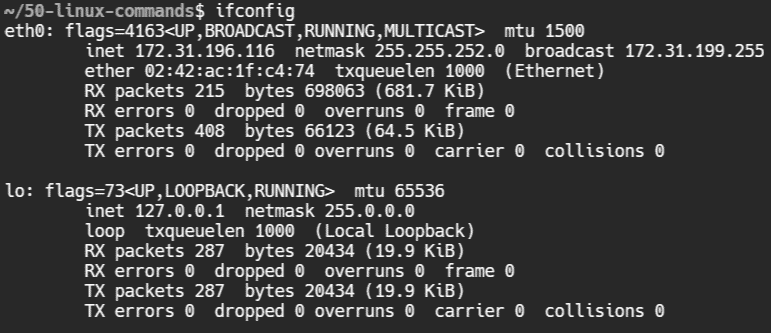
 **Purpose**: Configures and displays network interface parameters.

 **Syntax**: ifconfig [interface] [options]

 **Options**:

* up/down: Activate/deactivate an interface.
* netmask address: Set the network mask.

Output:



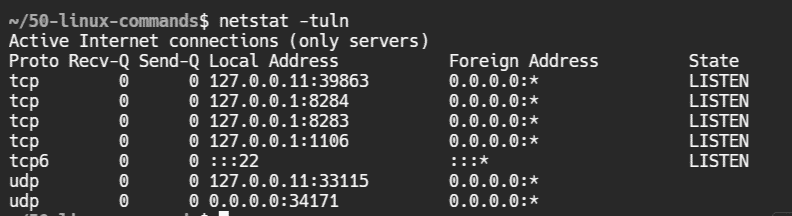
**netstat**

 **Purpose**: Displays network connections, routing tables, and interface statistics.

 **Syntax**: netstat [options]

 **Options**:

* -a: Show all connections.
* -r: Display the routing table.



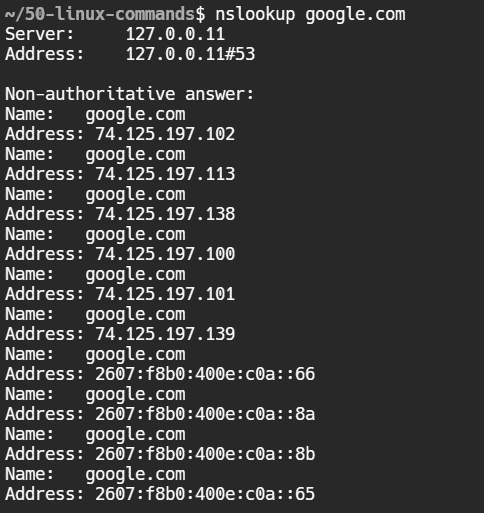
**nslookup**

 **Purpose**: Queries DNS to obtain domain name or IP address mapping.

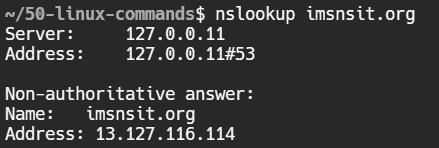
 **Syntax**: nslookup [options] [hostname]

 **Options**:

* server: Use a specific DNS server.
* -type=record\_type: Specify the query type (e.g., A, MX).



**nslookup**



**curl**

 **Purpose**: Transfers data from or to a server using various protocols.

 **Syntax**: curl [options] [url]

 **Options**:

* -o file: Save the output to a file.
* -I: Fetch only the HTTP headers



**hostname**

 **Purpose**: Displays or sets the system's hostname.

 **Syntax**: hostname [new\_name]

 **Options**:

* -i: Display IP address.



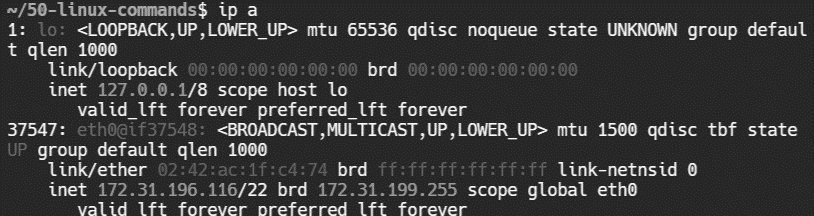
**ip**

 **Purpose**: Manages IP addresses, routes, and network interfaces.

 **Syntax**: ip [options] object command

 **Options**:

* addr: Manage IP addresses.
* link: Manage network interfaces.



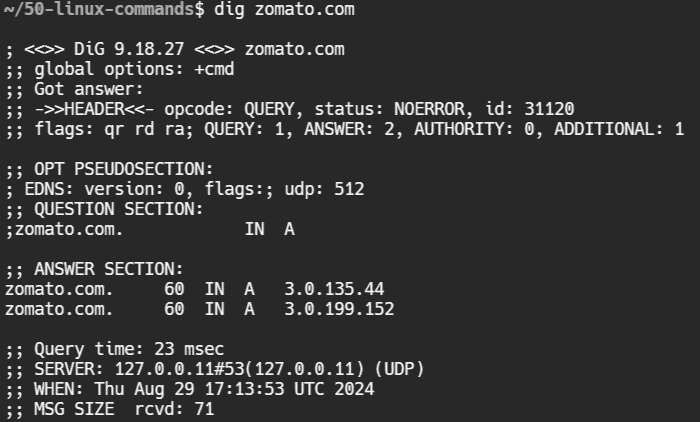
**dig**

 **Purpose**: Queries DNS servers for information.

 **Syntax**: dig [options] [hostname]

 **Options**:

* +short: Display a brief answer.
* -t type: Specify the DNS record type.



**arp**

 **Purpose**: Manipulates or displays the kernel's ARP cache.

 **Syntax**: arp [options] [hostname]

 **Options**:

* -a: Display all entries.
* -d hostname: Delete an entry



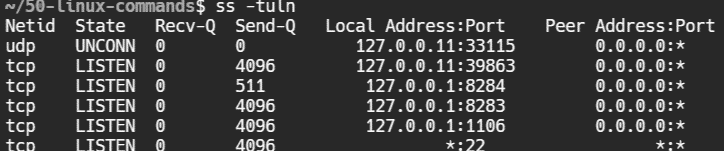
**ss**

 **Purpose**: Displays socket statistics.

 **Syntax**: ss [options]

 **Options**:

* -t: Display TCP sockets.
* -u: Display UDP sockets.



**Curl -I**

 **Purpose**: Transfers data from or to a server using various protocols.

 **Syntax**: curl [options] [url]

 **Options**:

* -o file: Save the output to a file.
* -I: Fetch only the HTTP headers.



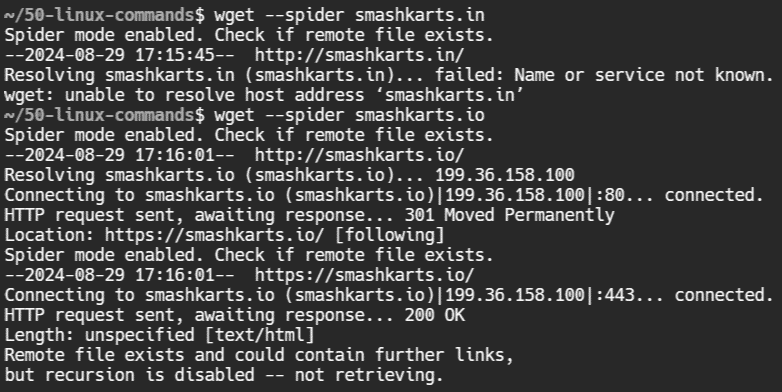
**wget**

 **Purpose**: Downloads files from the web.

 **Syntax**: wget [options] url

 **Options**:

* -c: Resume broken downloads.
* -r: Download recursively.



**ip route**

 **Purpose**: Displays or modifies the IP routing table.

 **Syntax**: ip route [options]

 **Options**:

* show: Display the routing table.
* add route: Add a new route.



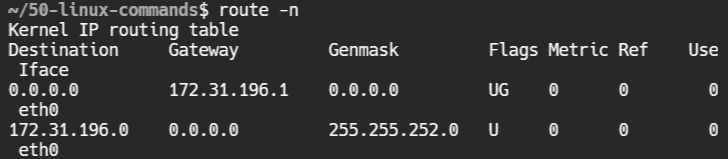
**route**

 **Purpose**: Displays/manages the IP routing table.

 **Syntax**: route [options]

 **Options**:

* add: Add a new route.
* del: Delete a route.



**ip link**

 **Purpose**: Displays or modifies network interfaces.

 **Syntax**: ip link [options]

 **Options**:

* show: Display interfaces.
* set interface: Modify interface properties.



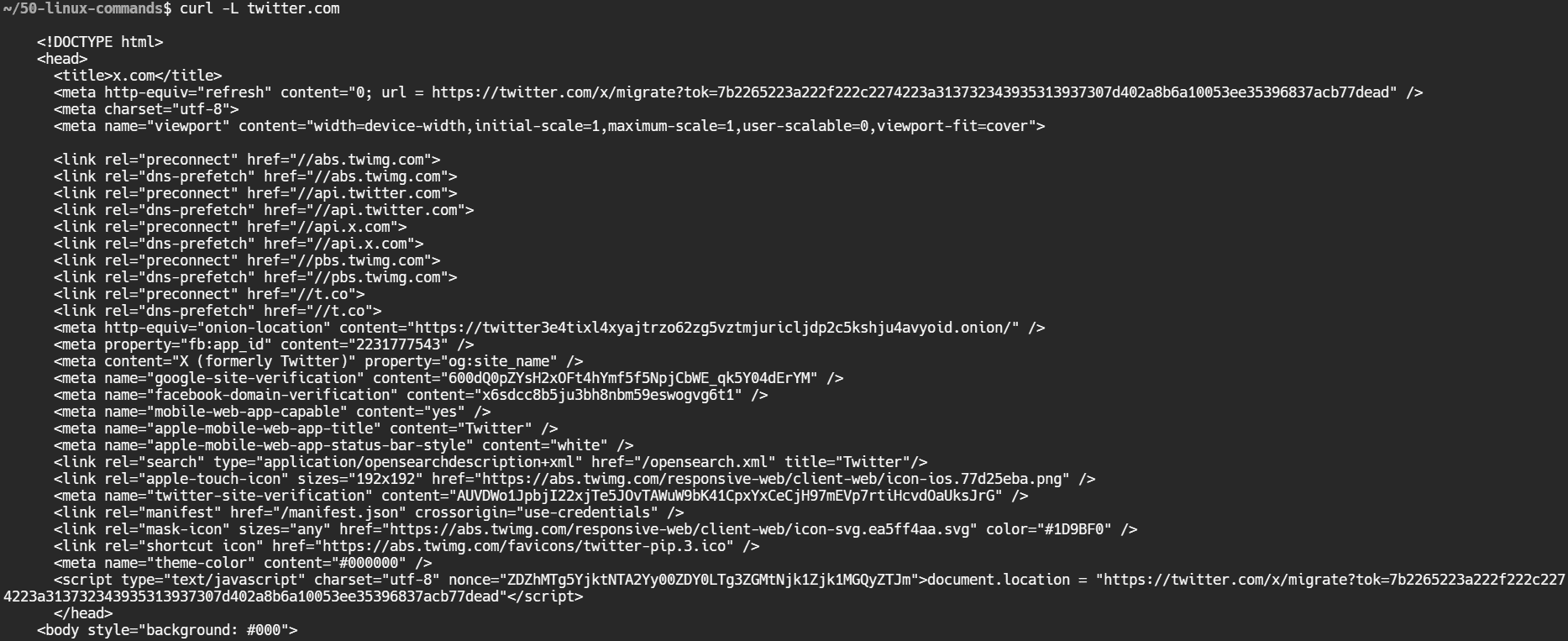
**Curl -L**

 **Purpose**: Transfers data from or to a server using various protocols.

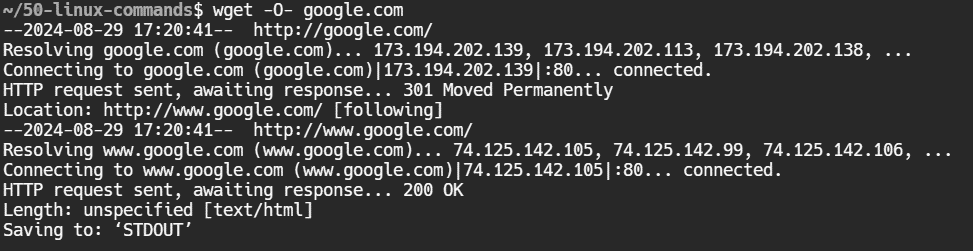
 **Syntax**: curl [options] [url]

 **Options**:

* -o file: Save the output to a file.
* -I: Fetch only the HTTP headers.



**wget**



**netcat**

 **Purpose**: Networking tool to read/write data over TCP/UDP.

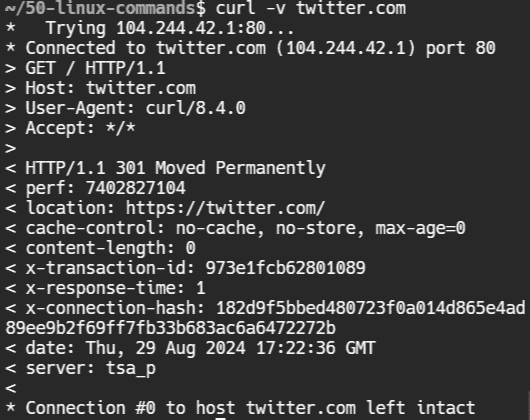
 **Syntax**: netcat [options] hostname port

 **Options**:

* -l: Listen mode.
* -z: Port scanning mode.



**curl -v**



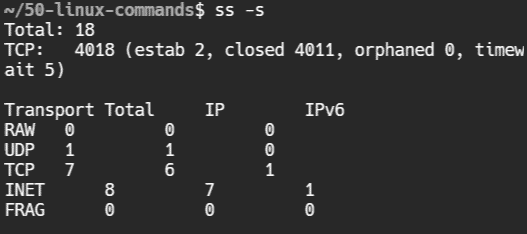
**ss**

 **Purpose**: Displays socket statistics.

 **Syntax**: ss [options]

 **Options**:

* -t: Display TCP sockets.
* -u: Display UDP sockets.



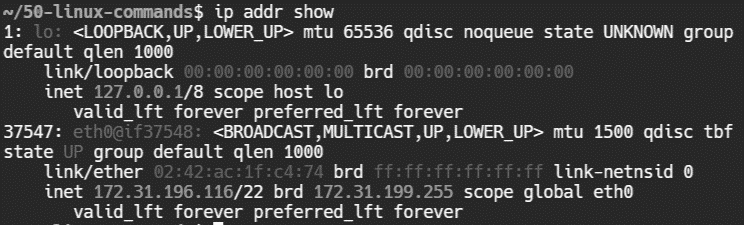
**ip addr**

 **Purpose**: Displays IP addresses and properties.

 **Syntax**: ip addr [options]

 **Options**:

* show: Display IP addresses.



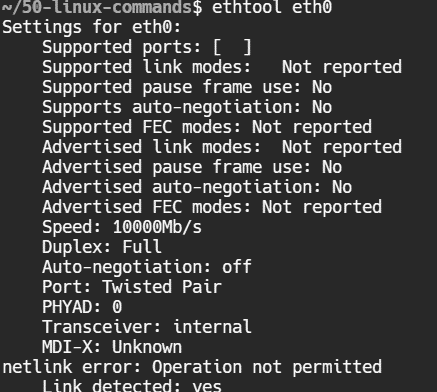
**ethtool**

 **Purpose**: Displays or modifies Ethernet device settings.

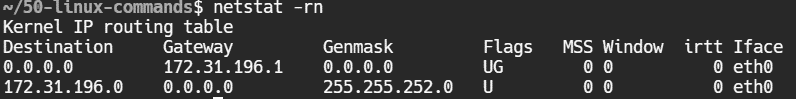
 **Syntax**: ethtool [options] device

 **Options**:

* -s: Change settings.
* -i: Display driver information.



**netstat**



**Ip maddr**



**dig**

 **Purpose**: Queries DNS servers for information.

 **Syntax**: dig [options] [hostname]

 **Options**:

* +short: Display a brief answer.
* -t type: Specify the DNS record type.



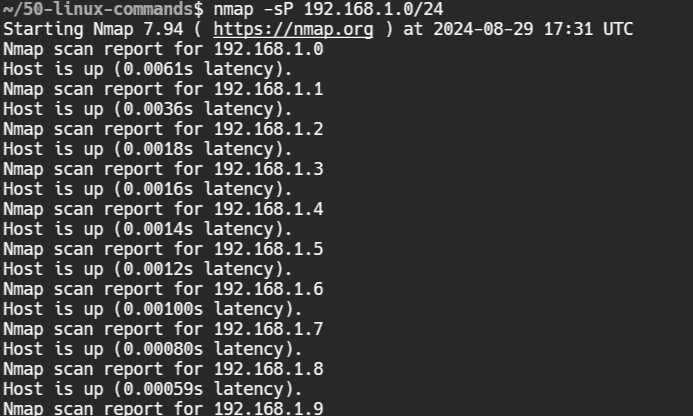
**nmap**

 **Purpose**: Scans networks for open ports and services.

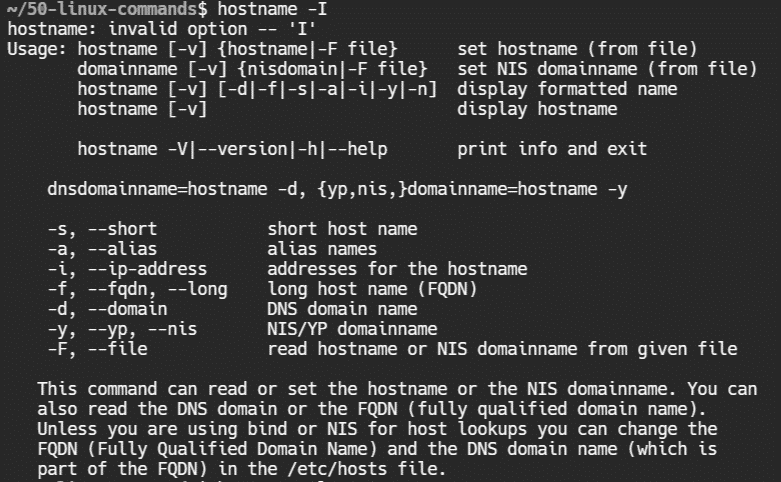
 **Syntax**: nmap [options] target

 **Options**:

* -p ports: Specify port range.
* -sP: Perform a ping scan.



**hostname**



**ss -antp**

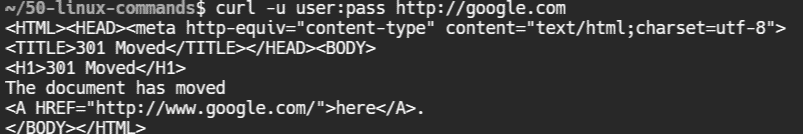
**Purpose**: The ss command is used to display socket statistics. It's a powerful tool for monitoring network connections, providing detailed information about network sockets. The -antp options modify the output to show specific details.



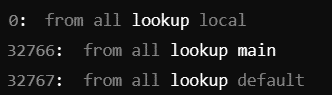
**curl -u user**

**Purpose**: The curl command transfers data from or to a server using various protocols, including HTTP, HTTPS, FTP, and others. The -u option is used to provide a username and password for server authentication.

-u user: Specifies the username for server authentication. If you don't specify the password, curl will prompt you to enter it. The user can be followed by a colon and a password (e.g., -u user:password), but it's generally more secure to avoid including the password in the command line to prevent it from being exposed.



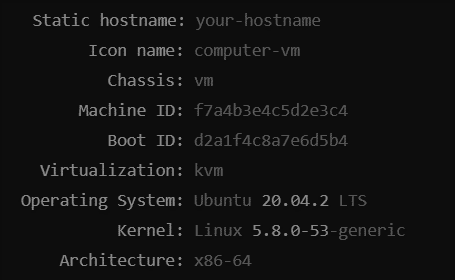
**Ip rule**

****

**Ip mroute**

****

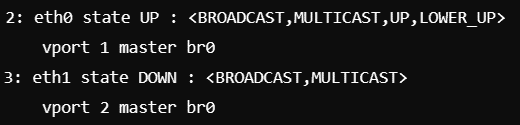
**Hostnamect**

****

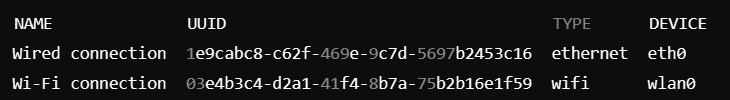
**Iw**

****

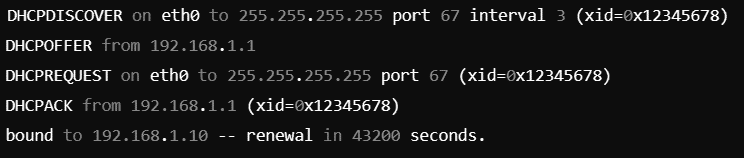
**bridge**

****

**Nmcli connnection show**

****

**dhclient**

****

**Vnstat**

Purpose: Monitors network traffic and bandwidth usage.

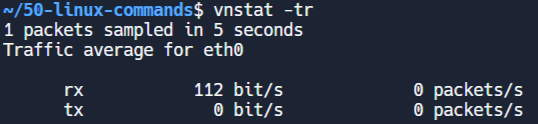
Syntax: vnstat [options]

Example: vnstat -i eth0

## Options:

* -i: Specify network interface.
* -d: Display daily traffic summary.

-m: Display monthly traffic summary

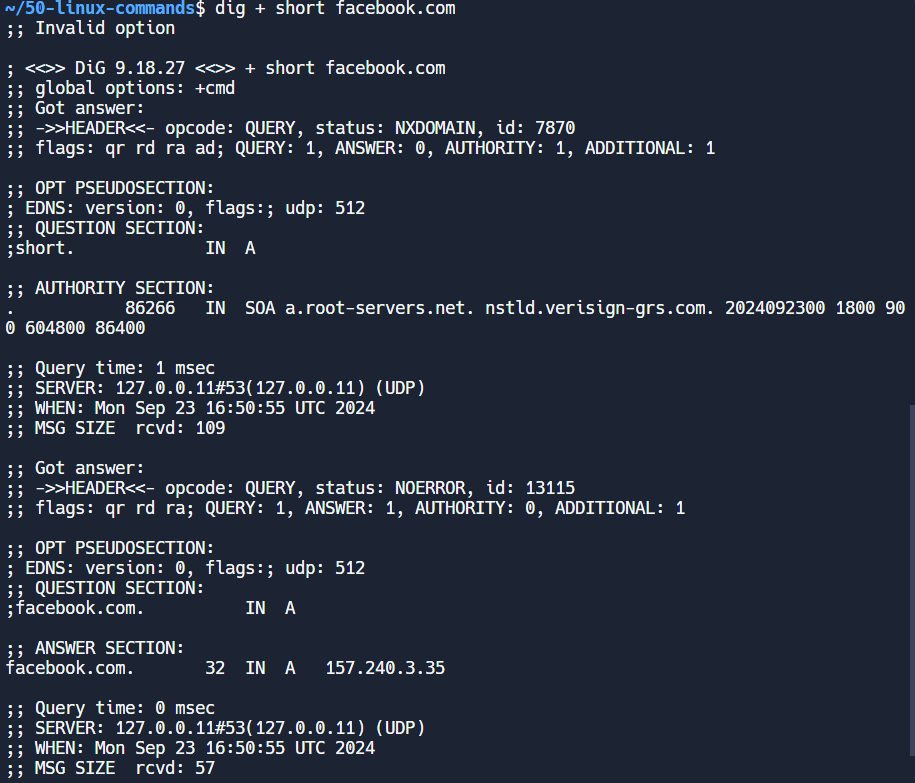
****

**Dig + short**

Purpose: Queries DNS servers and shows minimal output.

Syntax: dig +short [domain]

Example: dig +short google.com

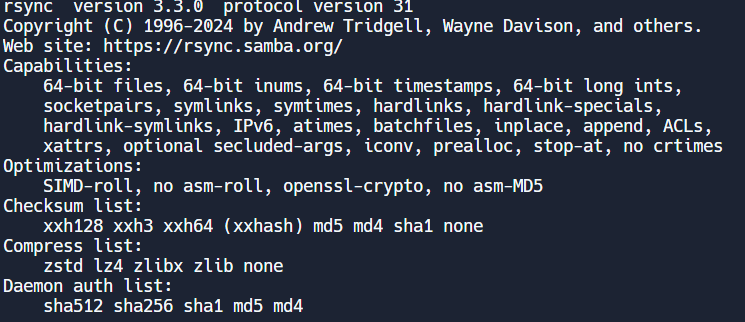
****

**Rsync**

Purpose: Synchronizes files and directories between two locations over a network.

Syntax: rsync [options] source destination

Example: rsync -avz /local/dir user@remote:/remote/dir

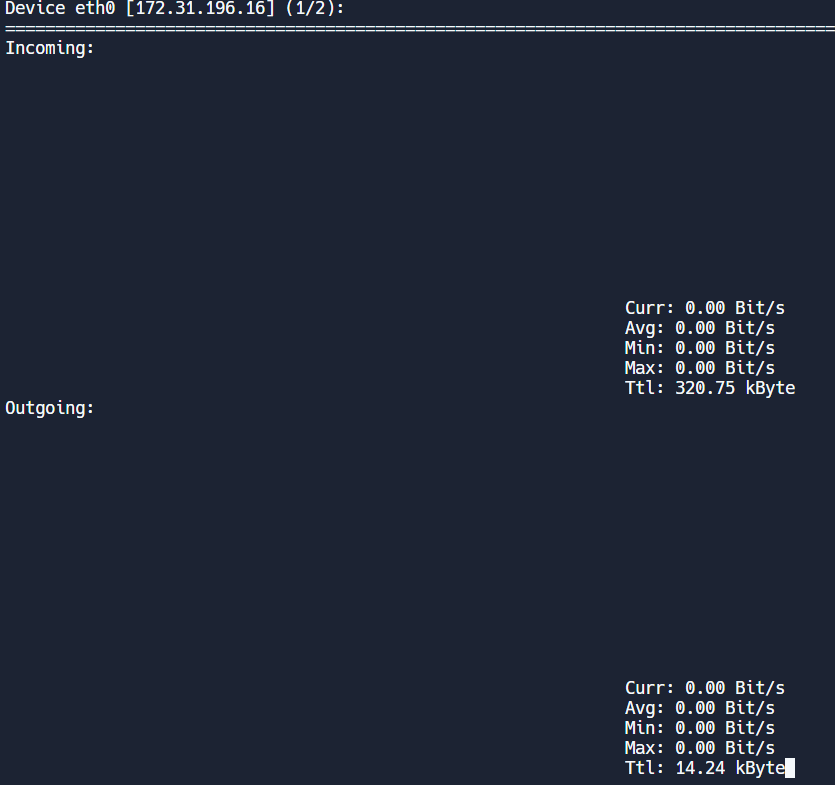
****

**Nload**

Purpose: Monitors incoming and outgoing traffic separately on a network interface.

Syntax: nload [options] [device]

Example: nload eth0

****

**Firewall**

Purpose: Manages firewall rules dynamically without restarting the firewall.

Syntax: firewalld [options]

Example: firewall-cmd --list-all

****

**Smbclient**

Purpose: Provides access to SMB/CIFS shares on Windows or Samba servers.

Syntax: smbclient [options] [share]

Example: smbclient //server/share

****

# **tftp**

Purpose: Transfers files between machines using the Trivial File Transfer Protocol.

Syntax: tftp [options] [host]

Example: tftp 192.168.1.1

**Iftop**

Purpose: Displays bandwidth usage on an interface by host.

Syntax: iftop [options]

Example: iftop -i eth0

# **mtr**

Purpose: Combines the functionality of ping and traceroute for network diagnostics.

Syntax: mtr [options] [host]

Example: mtr google.com

**PACKET TRACER**

**LAN using PCs and a switch**

**1-Select the Devices**

1:In the device list on the left, find the **End Devices** section.

2:Drag and drop at least two **PCs** onto the workspace.

3:Name them for clarity, such as **PC1** and **PC2**.

4:In the Network Devices section, locate the Switches category.

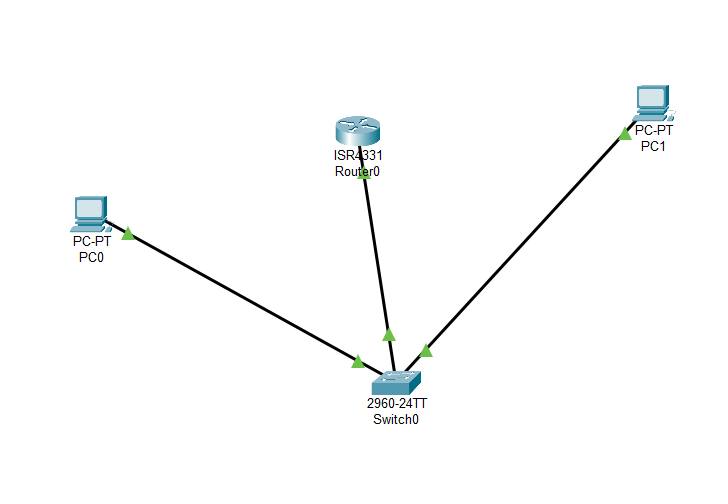
5:Drag and drop a switch .

**2-Connect The devices**

1:Select the **Connections** tool from the toolbar and choose a straight copper wire.

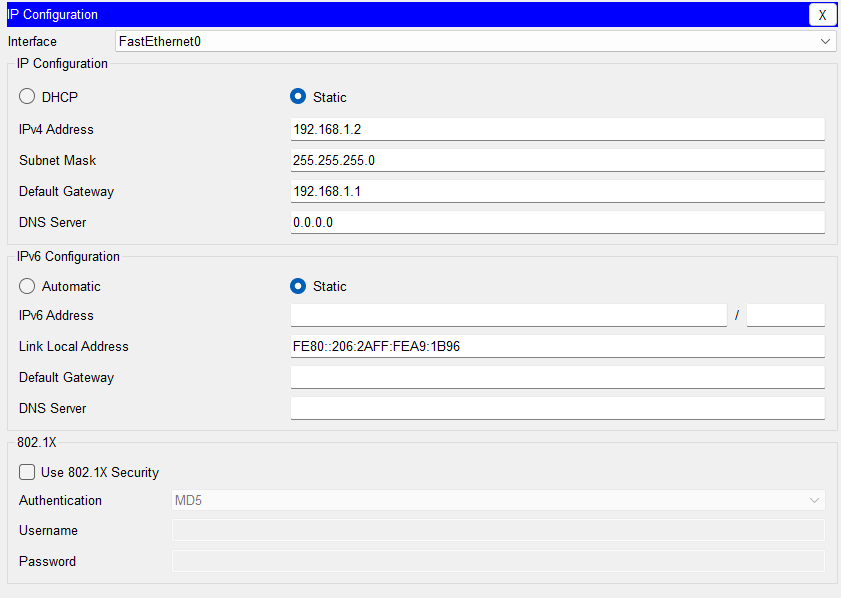
2:Connect a pc and switch through this wire

3:Connect router and switch thorugh the same wire.

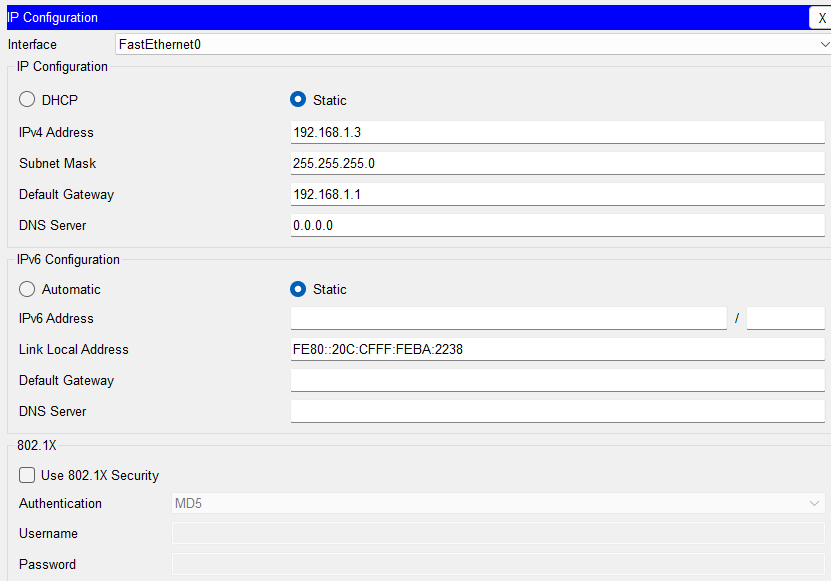
****

**IP-Configurations:**

**PC-1:**

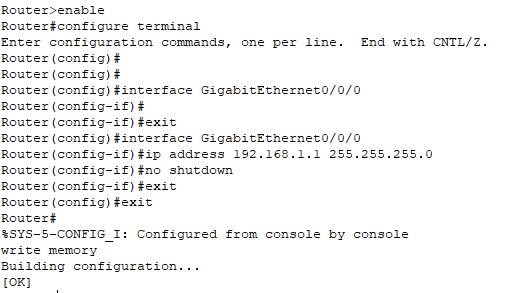
****

**PC-2:**

****

**Router Configuration**

**Task:**Select the router and navigate to the CLI and run following commands

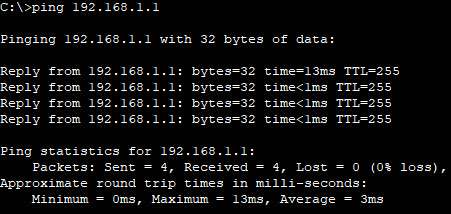
****

**TESTING:**

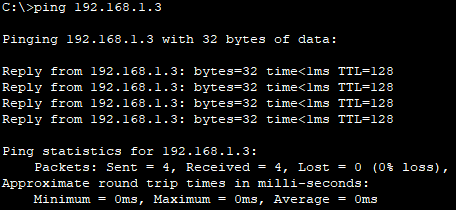
**Task:**

Select one of the PCs and navigate to the command prompt under desktop tab .

1:Ping the router’s IP address.

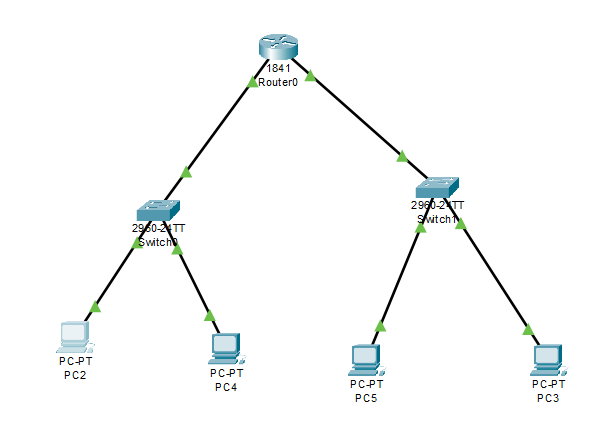
****

2:Ping another PC’s IP address

****

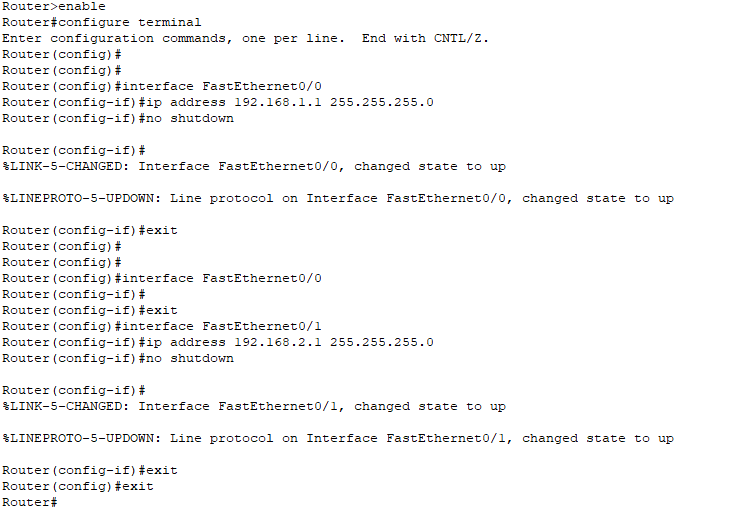
**2:** **Understand how to configure a router with basic settings to enable inter-network communication**

**SETUP:**

****

**CONFIGURATIONS:**

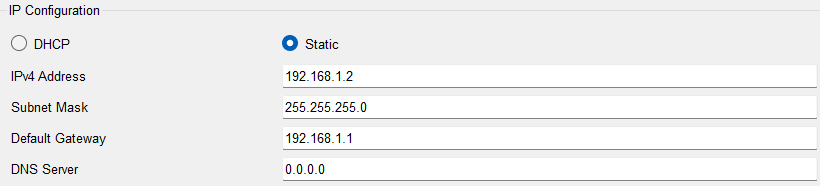
**ROUTER:**

****

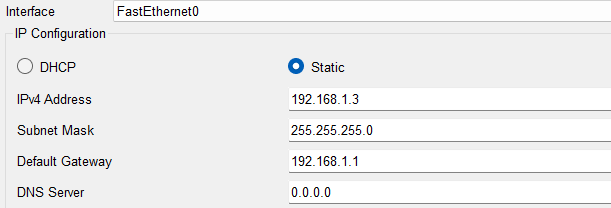
**PCs:**

**Network 1:**

**PC2:**

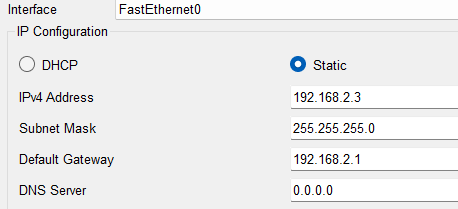
****

**PC4:**

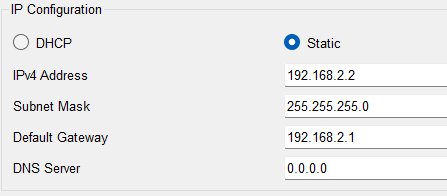
****

**Network 2:**

**PC5:**

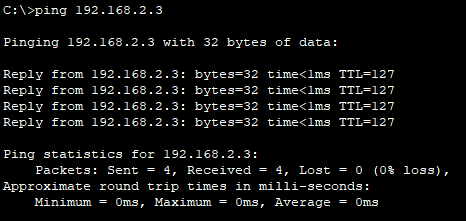
****

**PC3:**

****

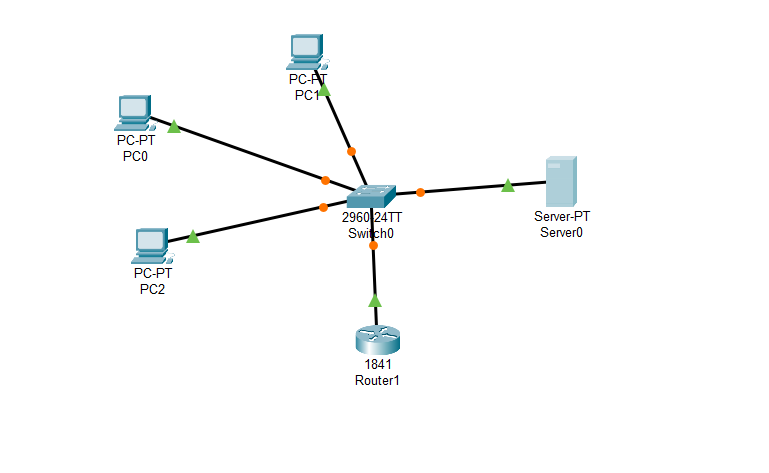
**TESTING:**

**Ping a PC (PC5) of 2nd network from 1st network(internetworking) i.e PC4**

****

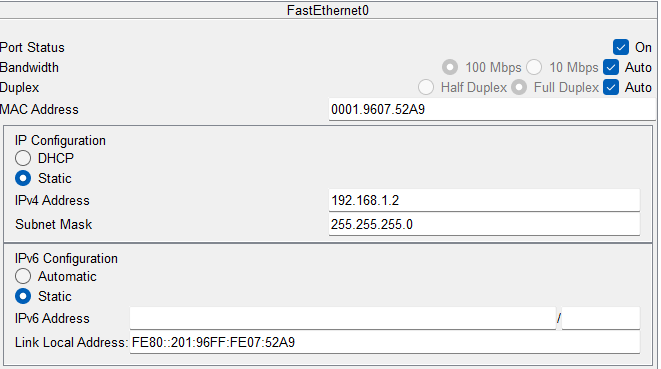
**3: Learn how to set up a DHCP server in Packet Tracer to automatically assign IP addresses to network devices.**

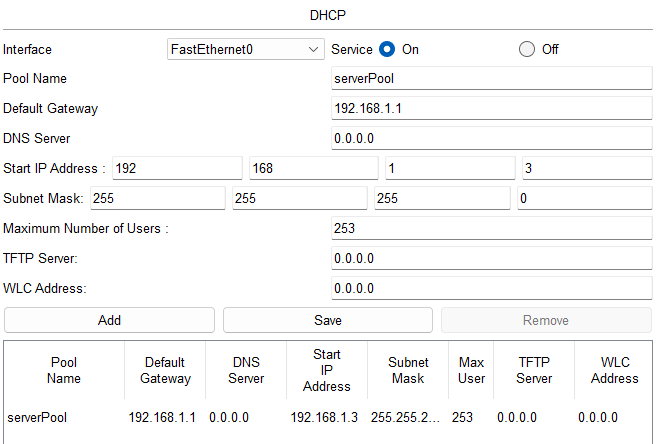
**SETUP:**

****

**CONFIGURATIONS:**

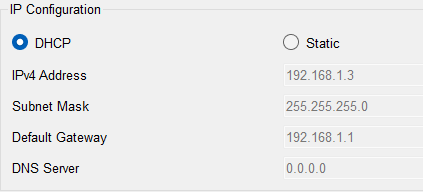
**SERVER:**

****

****

**PCs:**

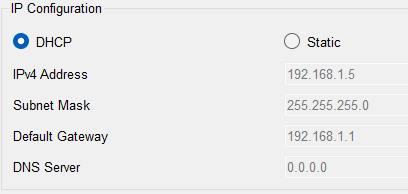
**PC0:**

****

**PC1:**

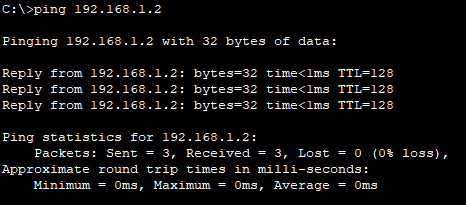
****

**PC2:**

****

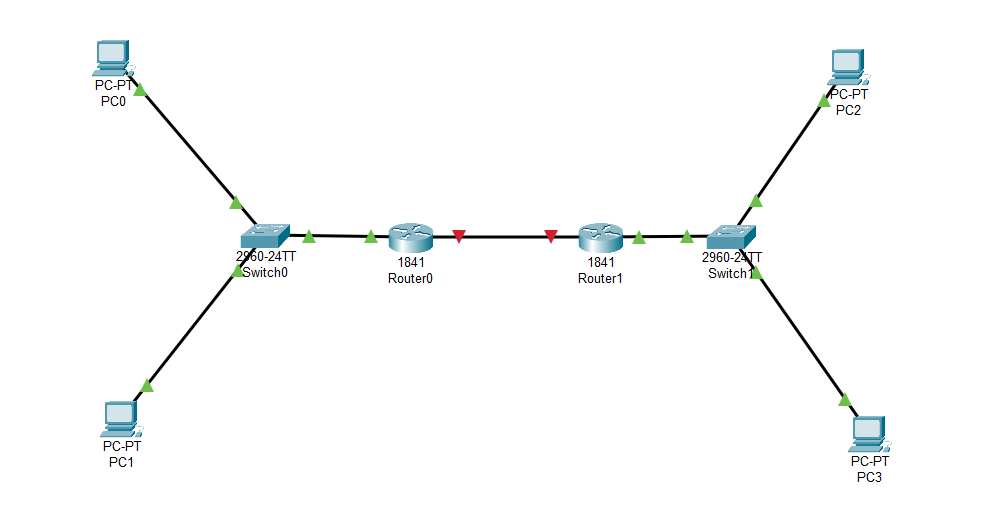
**TESTING:**

**Ping server from one of the PCs (PC2 here).**

****

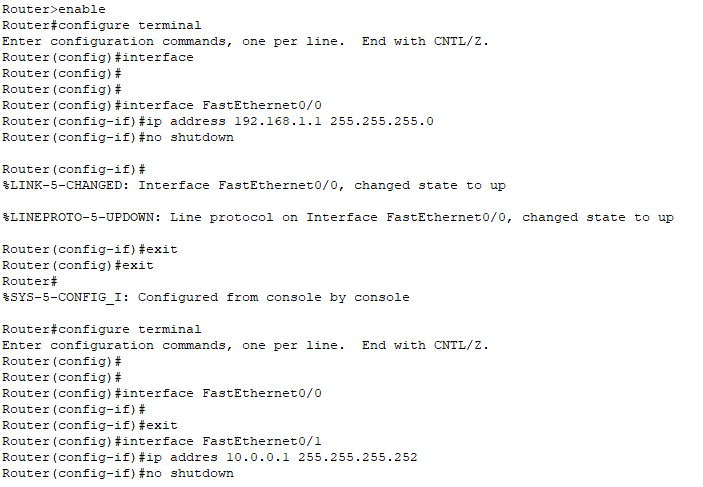
**4:** **Learn how to manually configure static routes on routers to control network traffic paths.**

**SETUP:**

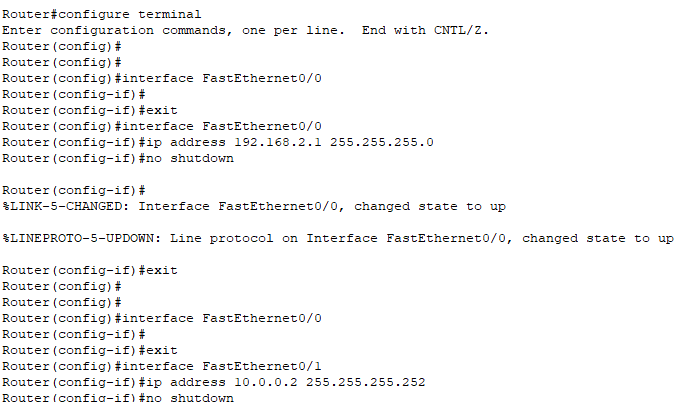
****

**Confirgurations :**

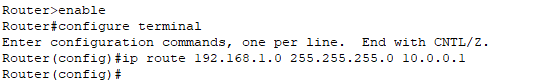
**Router0:**

****

**Router1:**

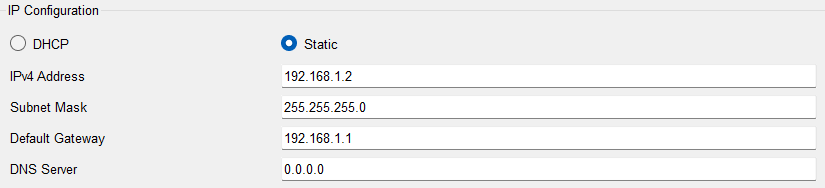
****

**Connecting networks through routers:**

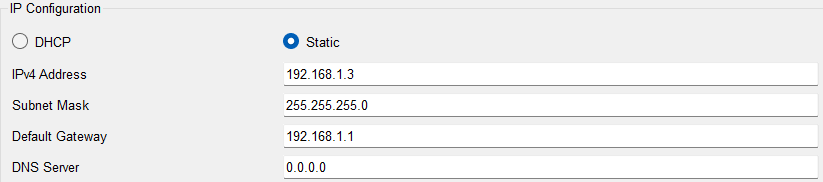
****

**PC configurations :**

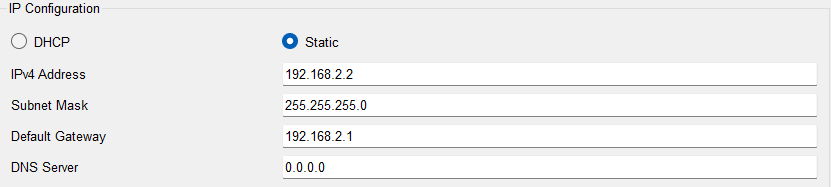
**PC0:**

****

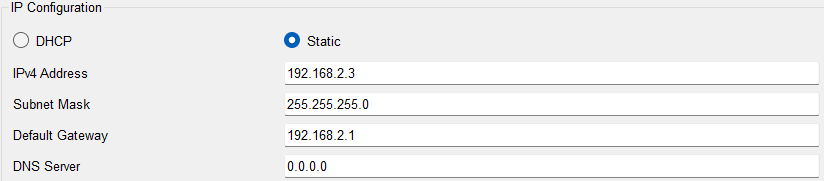
**PC1:**

****

**PC2:**

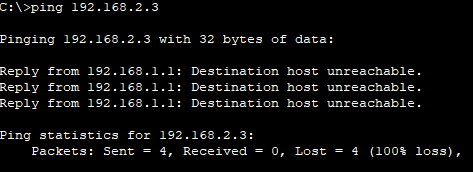
****

**PC3:**

****

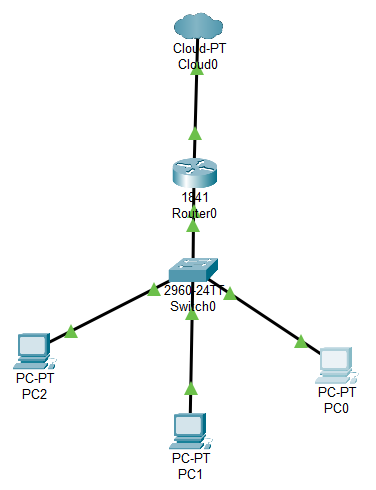
**TESTING:**

**Ping PC3 from PC0 i.e internetwork communication:**

****

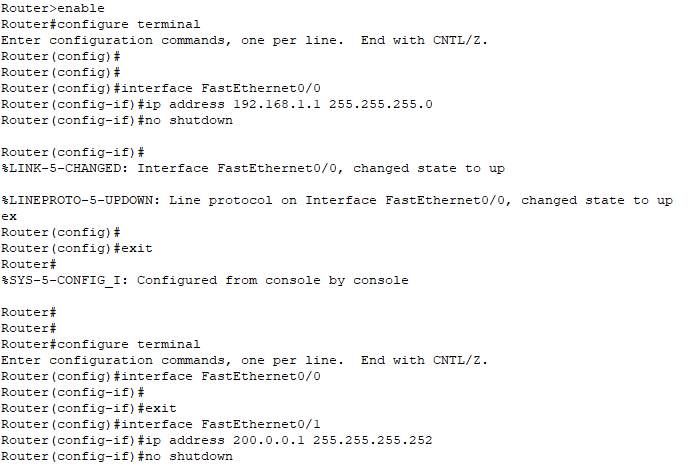
**5:** **Understand how NAT works to enable private IP addresses to communicate with external networks.**

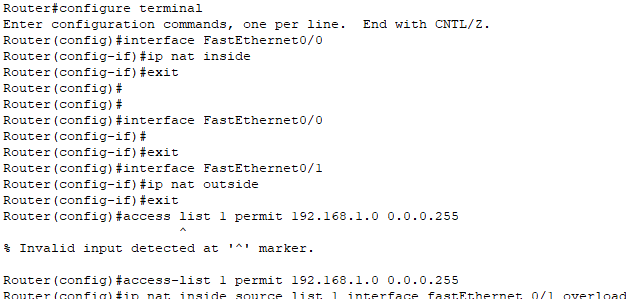
**SETUP:**

****

**CONFIGURATIONS**

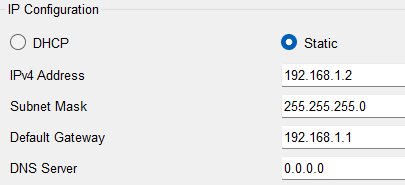
**Router:**

****

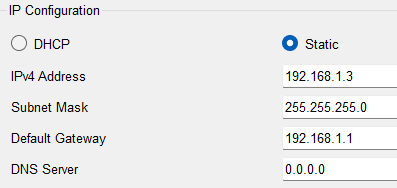
****

**PCs:**

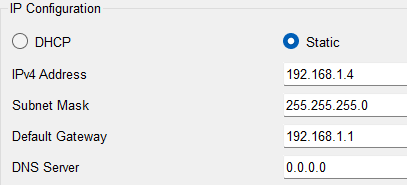
**PC0:**

****

**PC1:**

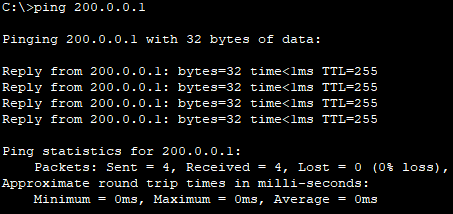
****

**PC2:**

****

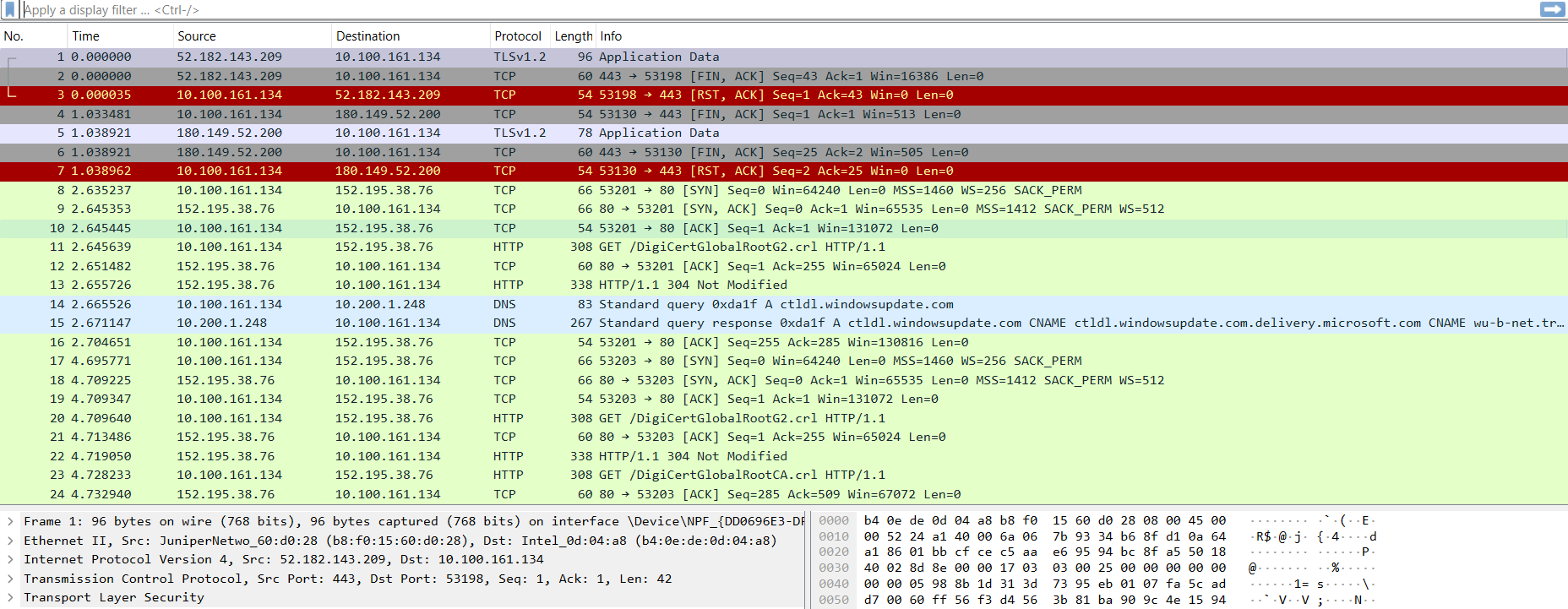
**TESTING:**

Ping the public network from our private network from a PC through a router .

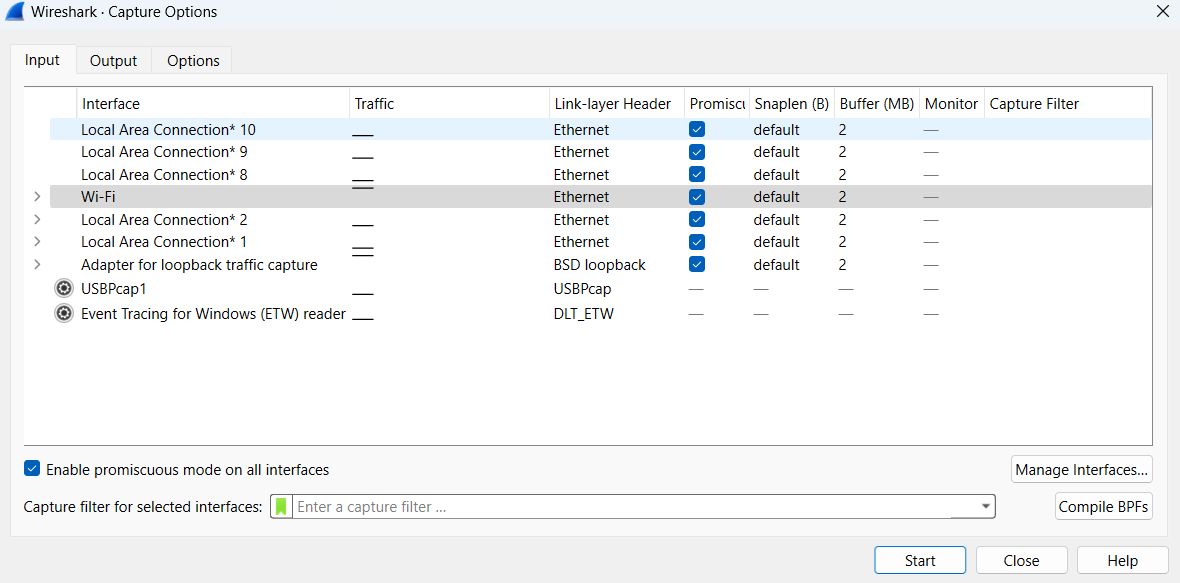
****

**FAMILIARITY WITH WIRESHARK**

1:Go to wifi and capture network.

****

**2:Capture Options**

****