**Experiment No 3**

**Name:-** Shrikrushna C Gundre

**PRN:-** 2122010191

**Roll no:-** DCSE 12

**a) ipconfig**

**Study of connectivity test tools with all its options**

Ipconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed. If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

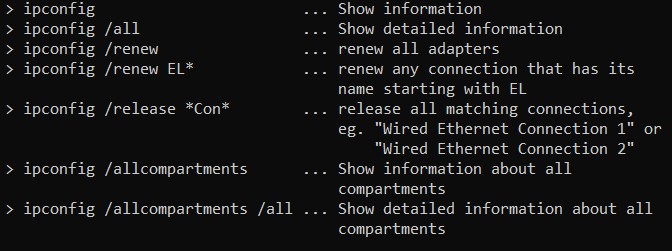
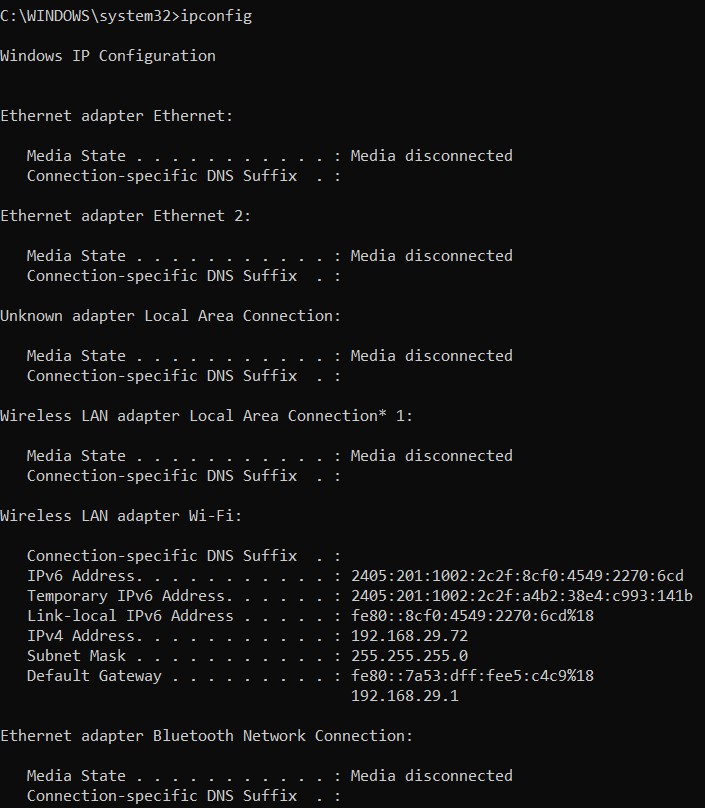
• **ipconfig eth0**- display the current status of interface mentioned in command

• **ipconfig -a** - display status of all the available interfaces on the computer

• **ipconfig eth0 down**- shutdown the interface mentioned in command (super user privileges are required)

• **ipconfig eth0 up**- up the interface mentioned in command (super user privileges are required)

• **ipconfig 172.25.3.5** - set the given ip address to the interface



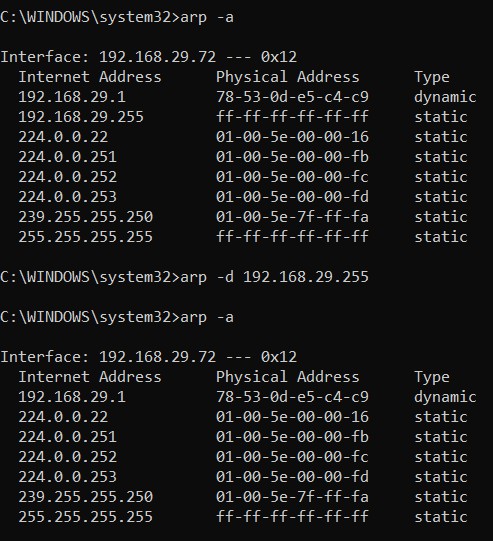
**b) arp**

Arp manipulates the kernel’s ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting up one. For debugging purposes, the arp program also allows a complete dump of the ARP cache.

• **arp -a** -show the entries of specified host

• **arp -s** ip addr mac address- used to add corresponding entry in cache

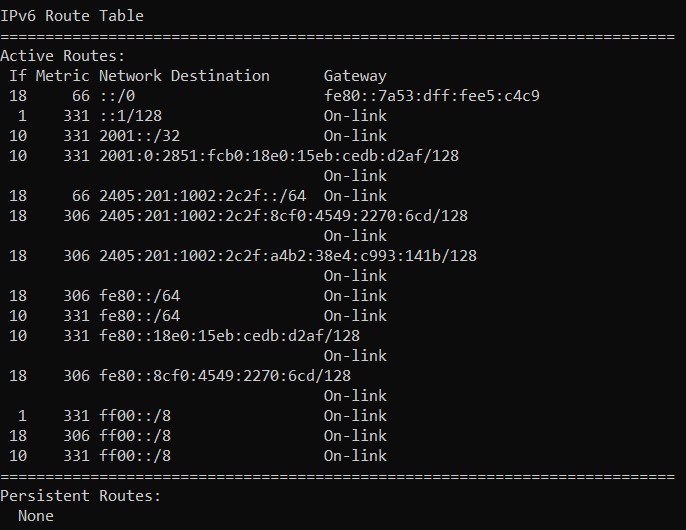
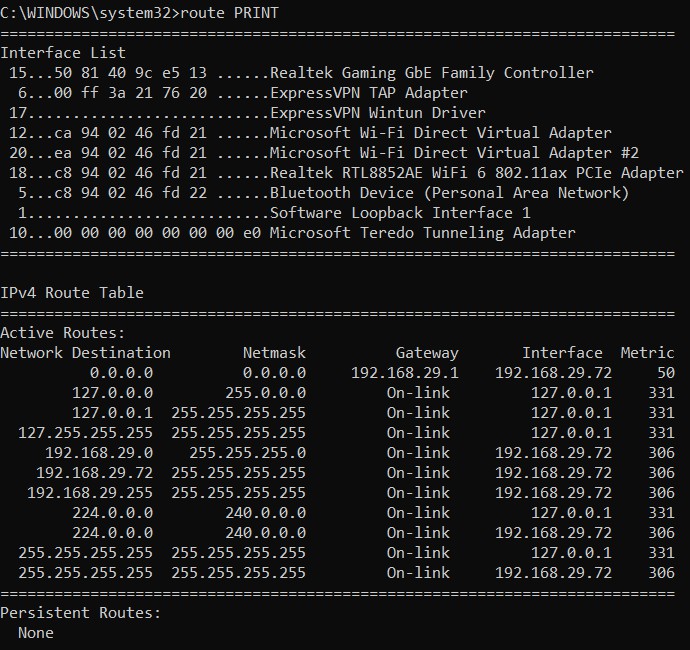
• **arp -d** ip addr - used to delete specific entry from the cache



**c) route**

route manipulates the kernel’s IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig(8) program. When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

**route** - display kernel’s IP routing tables

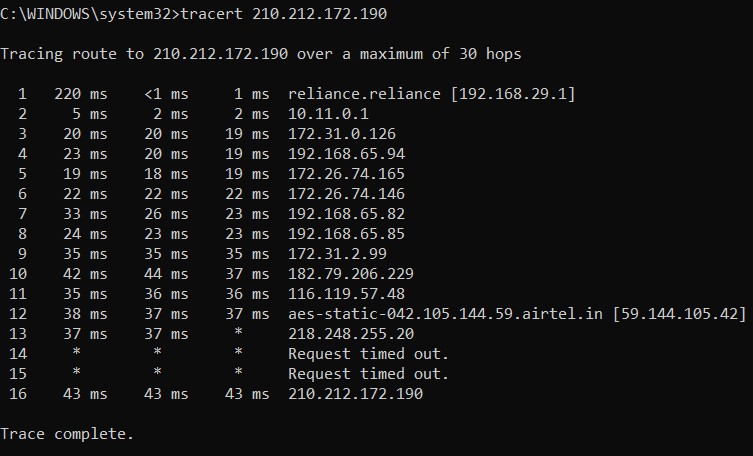


**d)traceroute**/

**tracert**

traceroute tracks the route packets taken from an IP network on their way to a given host. It utilizes the IP protocol’s time to live (TTL) field and attempts to elicit an ICMP TIME\_EXCEEDED response from each gateway along the path to the host.

**Traceroute/tracert 210.212.172.190** - displays the response from each gateway.



**e) nmap**

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

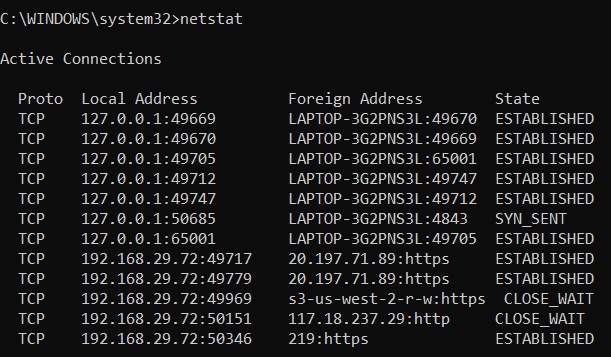
**nmap 172.25.3.100** - scanning the given system

**nmap 172.25.3.100 172.27.100.2** - scanning two systems

**f) netstat**

Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Netstat prints information about the Linux networking subsystem.

**netstat**- display network subsystem information



**g) finger**

The finger displays information about the system users

**finger -s** - Finger displays the user’s login name, real name, terminal name and write status idle time, login time, office location and office phone number.

