Experiment No 3

Name:- Shrikrushna C Gundre

PRN:- 2122010191

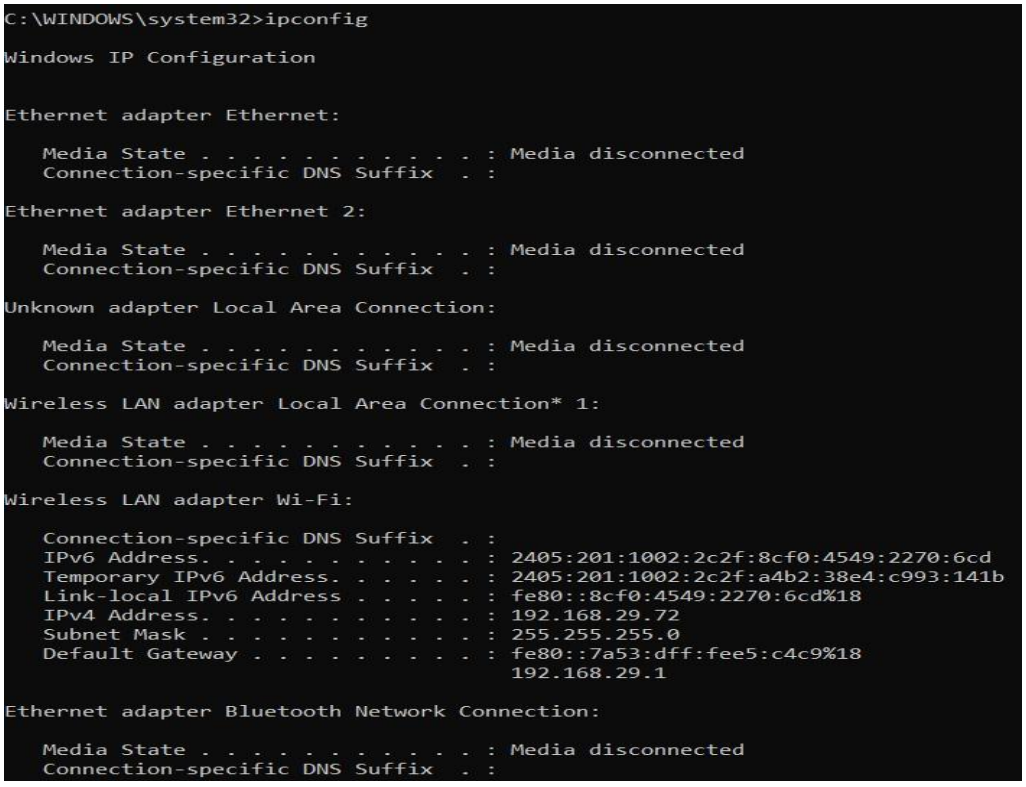
Roll no:- DCSE 12

Study of connectivity test tools with all its options

a) ipconfig

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

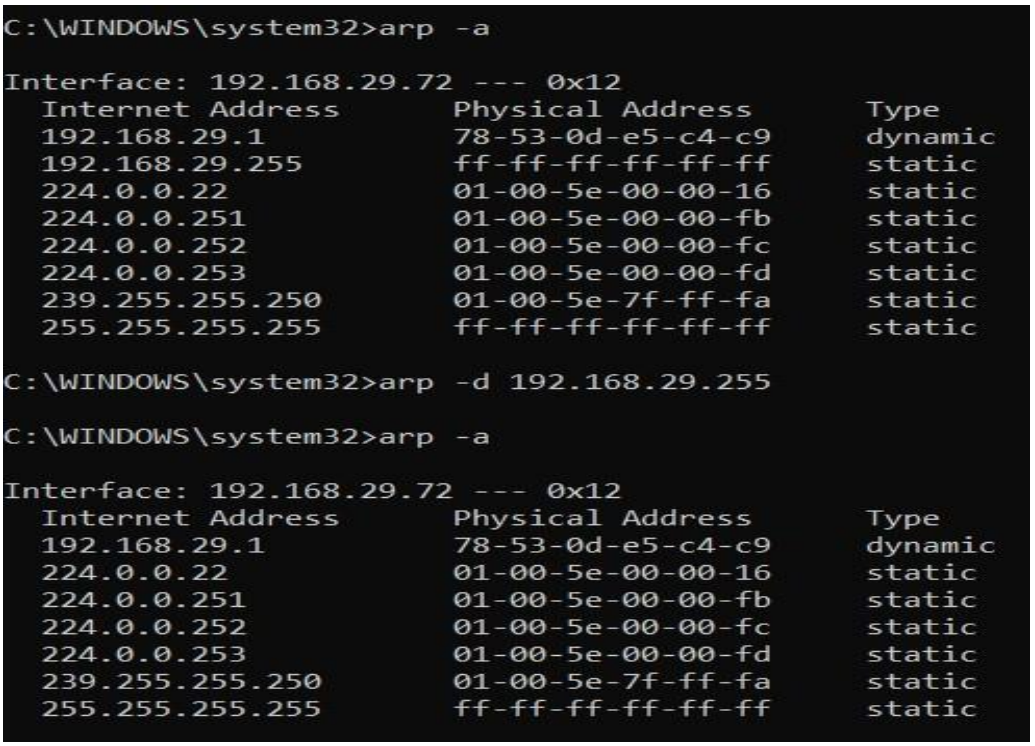


```
> ipconfig                         ... Show information
> ipconfig /all                    ... Show detailed information
> ipconfig /renew                  ... renew all adapters
> ipconfig /renew EL*              ... renew any connection that has its
                                       name starting with EL
> ipconfig /release *Con*          ... release all matching connections,
                                       eg. "Wired Ethernet Connection 1" or
                                           "Wired Ethernet Connection 2"
> ipconfig /allcompartments        ... Show information about all
                                       compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                                       compartments
```

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

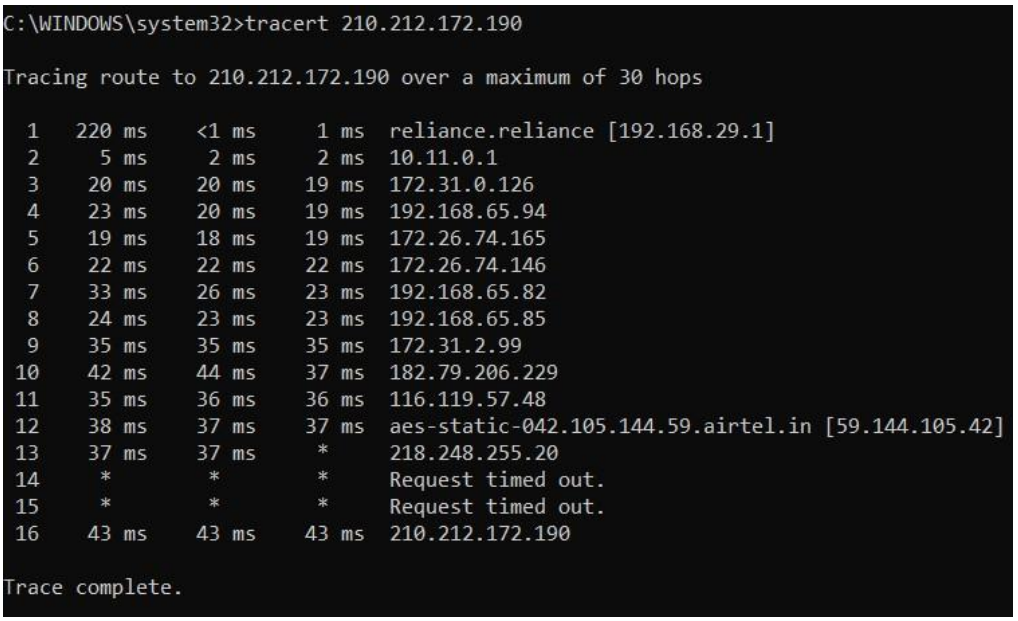
```
C:\WINDOWS\system32>route PRINT
===========================================================================
Interface List
 15...50 81 40 9c e5 13 ......Realtek Gaming GbE Family Controller
  6...00 ff 3a 21 76 20 ......ExpressVPN TAP Adapter
 17...........................ExpressVPN Wintun Driver
 12...ca 94 02 46 fd 21 ......Microsoft Wi-Fi Direct Virtual Adapter
 20...ea 94 02 46 fd 21 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...c8 94 02 46 fd 21 ......Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
  5...c8 94 02 46 fd 22 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
 10...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.29.1    192.168.29.72     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.29.0    255.255.255.0         On-link     192.168.29.72    306
    192.168.29.72  255.255.255.255         On-link     192.168.29.72    306
   192.168.29.255  255.255.255.255         On-link     192.168.29.72    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.29.72    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.29.72    306
===========================================================================
Persistent Routes:
  None
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 18     66 ::/0                     fe80::7a53:dff:fee5:c4c9
  1    331 ::1/128                  On-link
 10    331 2001::/32                On-link
 10    331 2001:0:2851:fcb0:18e0:15eb:cedb:d2af/128
                                    On-link
 18     66 2405:201:1002:2c2f::/64  On-link
 18    306 2405:201:1002:2c2f:8cf0:4549:2270:6cd/128
                                    On-link
 18    306 2405:201:1002:2c2f:a4b2:38e4:c993:141b/128
                                    On-link
 18    306 fe80::/64                On-link
 10    331 fe80::/64                On-link
 10    331 fe80::18e0:15eb:cedb:d2af/128
                                    On-link
 18    306 fe80::8cf0:4549:2270:6cd/128
                                    On-link
  1    331 ff00::/8                 On-link
 18    306 ff00::/8                 On-link
 10    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

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

```
C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49669        LAPTOP-3G2PNS3L:49670  ESTABLISHED
  TCP    127.0.0.1:49670        LAPTOP-3G2PNS3L:49669  ESTABLISHED
  TCP    127.0.0.1:49705        LAPTOP-3G2PNS3L:65001  ESTABLISHED
  TCP    127.0.0.1:49712        LAPTOP-3G2PNS3L:49747  ESTABLISHED
  TCP    127.0.0.1:49747        LAPTOP-3G2PNS3L:49712  ESTABLISHED
  TCP    127.0.0.1:50685        LAPTOP-3G2PNS3L:4843   SYN_SENT
  TCP    127.0.0.1:65001        LAPTOP-3G2PNS3L:49705  ESTABLISHED
  TCP    192.168.29.72:49717    20.197.71.89:https     ESTABLISHED
  TCP    192.168.29.72:49779    20.197.71.89:https     ESTABLISHED
  TCP    192.168.29.72:49969    s3-us-west-2-r-w:https  CLOSE_WAIT
  TCP    192.168.29.72:50151    117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.29.72:50346    219:https              ESTABLISHED
```

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.

```
C:\Users\SHRI>finger

Displays information about a user on a specified system running the
Finger service. Output varies based on the remote system.

FINGER [-l] [user]@host [...]

  -l        Displays information in long list format.
  user      Specifies the user you want information about. Omit the user
            parameter to display information about all users on the
            specifed host.
  @host     Specifies the server on the remote system whose users you
            want information about.
```