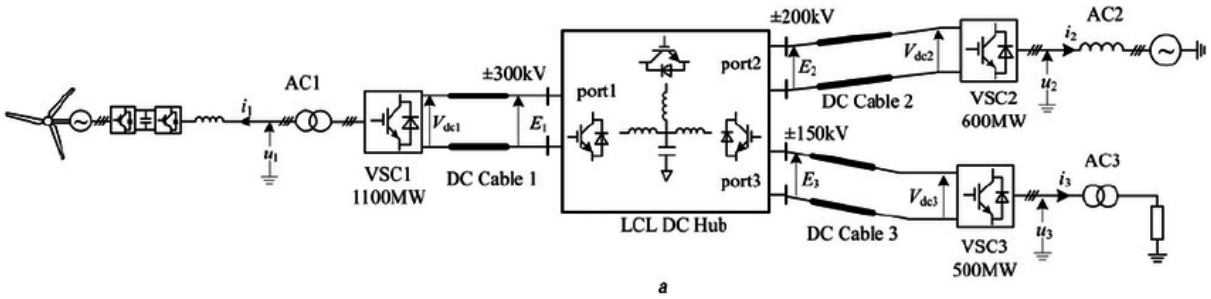
Network Components

1. Hub

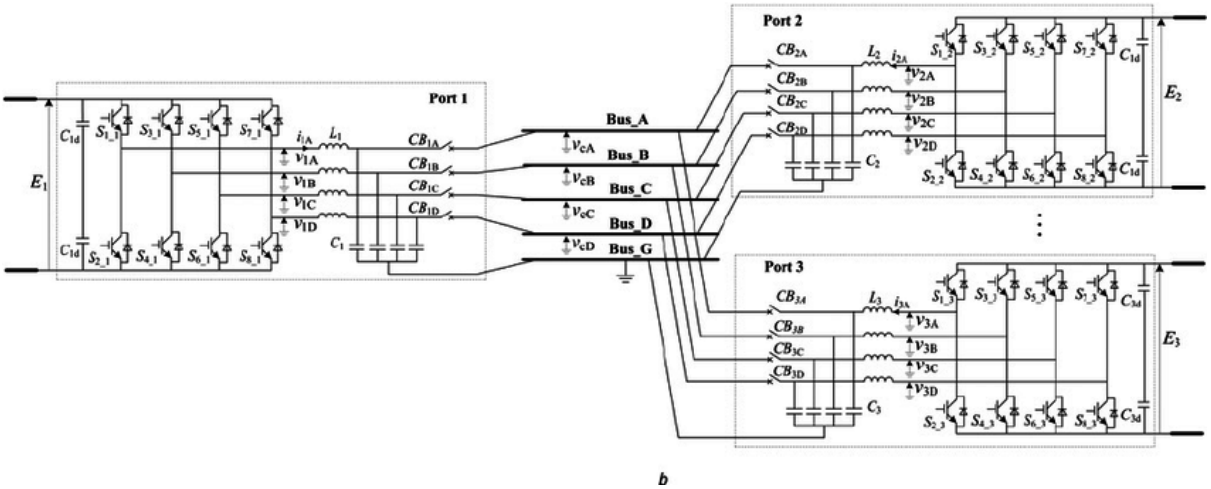
Description – A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

Working Principle – A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

Diagram –



a



b

Advantages –

- It can extend total distance of the network.
- It does not affect performance of the network seriously.
- It can connect different media types.

Disadvantages –

- It does not have mechanisms such as collision detection and retransmission of packets.
- It does not operate in full duplex mode.
- It cannot connect different network architectures such as token ring and ethernet etc.
- It cannot filter information i.e. it passes packets to all the connected segments.
- It does not have mechanism to reduce the network traffic.

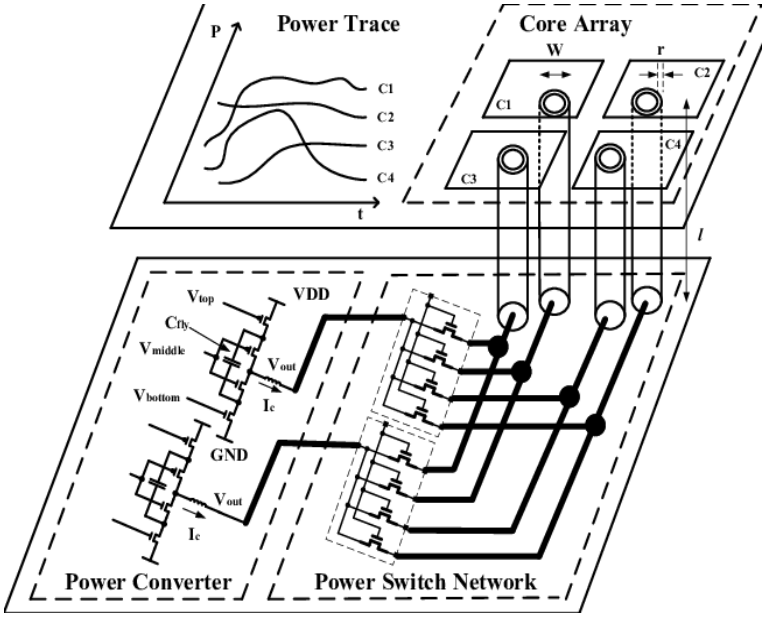
Layer –Physical layer of the OSI model

2. Switch

Description – A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

Working Principle – Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.

Diagram –



Advantages –

- They increase the available bandwidth of the network.
- They help in reducing workload on individual host PCs.
- They increase the performance of the network.
- Networks which use switches will have less frame collisions. This is due to the fact that switches create collision domains for each connection.
- Switches can be connected directly to workstations.

Disadvantages –

- They are more expensive compare to network bridges.
- Network connectivity issues are difficult to be traced through the network switch.
- Broadcast traffic may be troublesome.
- Proper design and configuration is needed in order to handle multicast packets.
- While limiting broadcasts, they are not as good as routers.

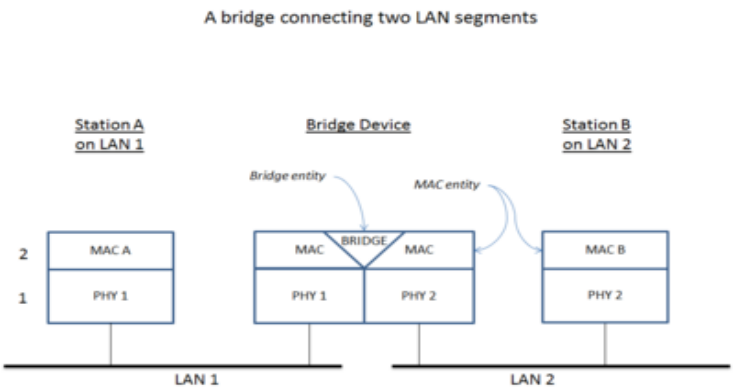
Layer – Data link layer of OSI model

3. Bridge

Description – A network bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called network bridging.

Working Principle – Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.

Diagram –



Advantages –

- It helps in extension of physical network.
- It reduces network traffic with minor segmentation.
- It creates separate collision domains. Hence it increases available bandwidth to individual nodes as fewer nodes share a collision domain.
- It reduces collisions.
- Some bridges connect networks having different architectures and media types

Disadvantages –

- It is slower compare to repeaters due to filtering.
- It does not filter broadcasts.
- It is more expensive compare to repeaters.

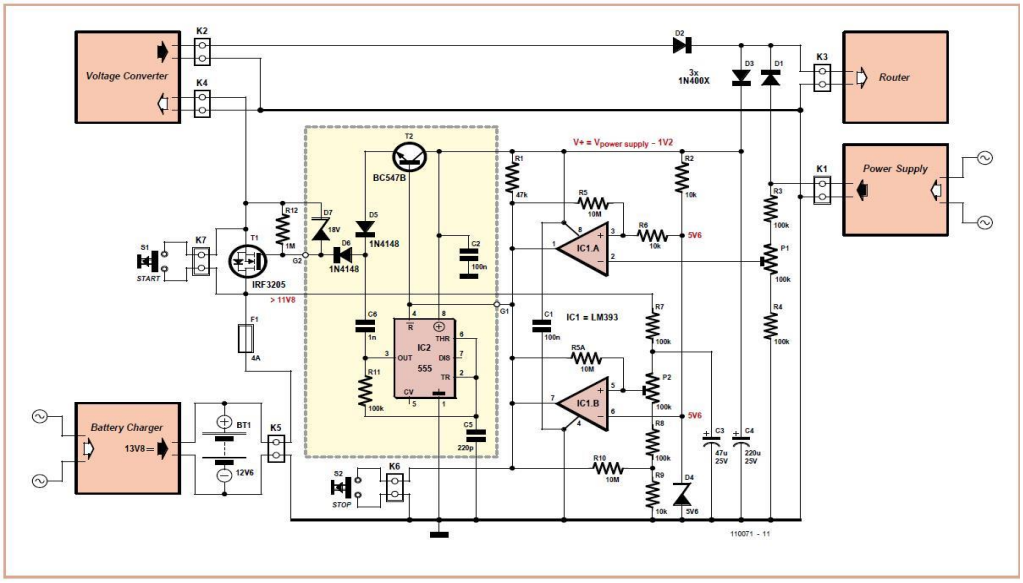
Layer – Data link layer of OSI model

4. Router

Description – This networking device provides interconnection between two dissimilar networks.

Working Principle – It uses IP addressing for routing the packets. The IP address of each hosts contain two parts viz. network address and host address. The router checks destination host address, source host address and network address in order to route IP packet Access Points appropriately.

Diagram –



Advantages –

- It provides connection between different network architectures such as ethernet & token ring etc.
- It can choose best path across the internetwork using dynamic routing algorithms.
- It can reduce network traffic by creating collision domains and also by creating broadcast domains.
- It provides sophisticated routing, flow control and traffic isolation.
- They are configurable which allows network manager to make policy based on routing decisions.

Disadvantages –

- They operate based on routable network protocols.
- They are expensive compare to other network devices.
- Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
- They are slower as they need to analyze data from layer-1 through layer-3.
- They require considerable number of initial configurations.
- They are protocol dependent devices which must understand the protocol they are forwarding.

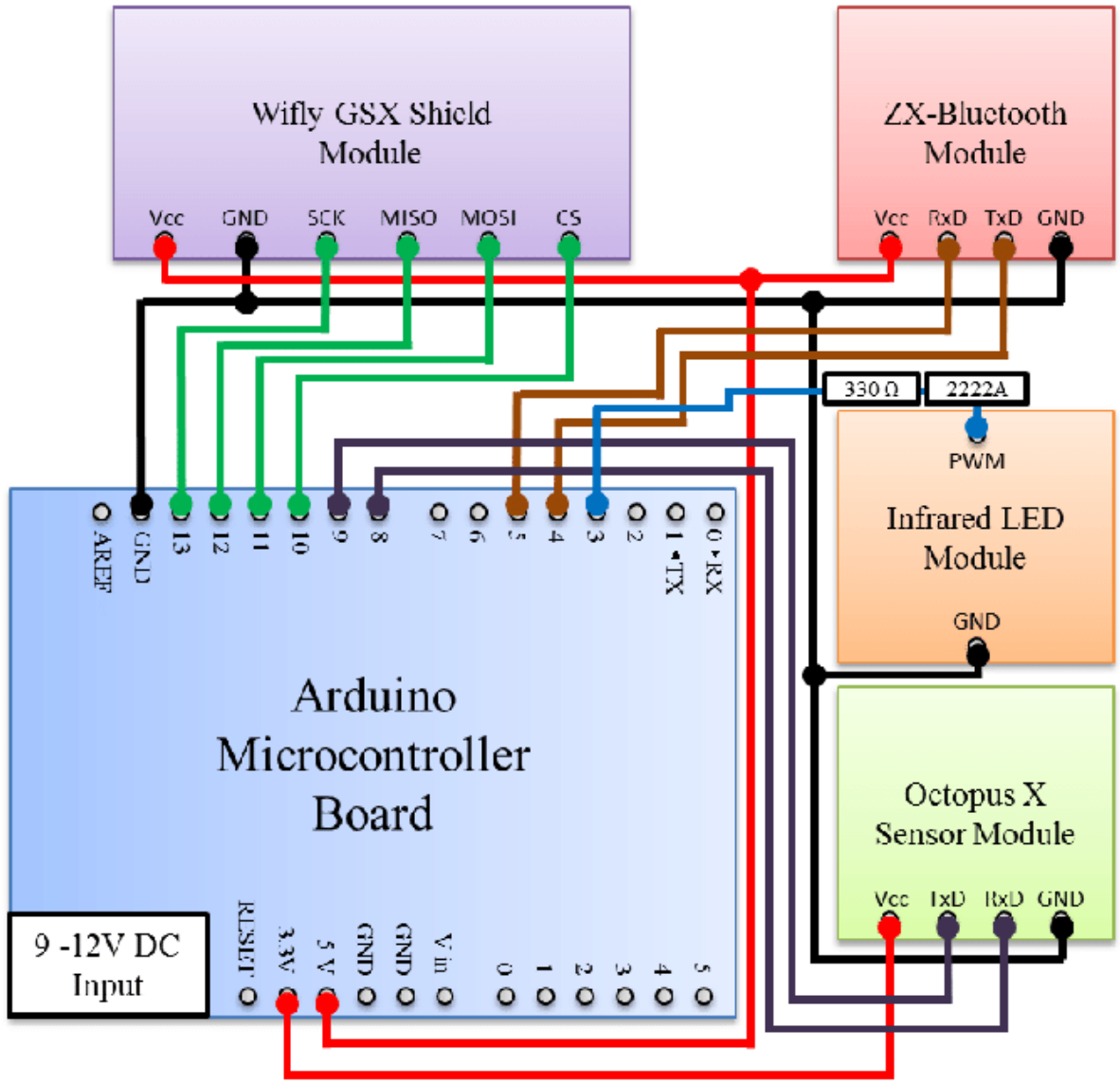
Layer – Network layer of OSI model

5. Gateway

Description – Gateway is a network connecting device that can be used to connect two devices in two different networks implementing different networking protocols and overall network architecture.

Working Principle – When a data packet arrives at the gateway, it first checks the header information. After checking the destination IP address and any kind of errors in the data packets. It performs data translation and protocol conversion of the data packet as per the destination network needs. Finally, it forwards the data packet to the destination IP address by setting up a specific transmission path for the packet.

Diagram –



Advantages –

- It can connect the devices of two different networks having dissimilar structures.
- It is an intelligent device with filtering Access Points abilities.
- It has control over both collisions as well as a broadcast domain.
- It uses a full-duplex mode of communication.
- It has the fastest data transmission speed amongst all network connecting devices.
- It can perform data translation and protocol conversion of the data packet as per the destination network's need.
- It has improved security than any other network connecting device.

Disadvantages –

- It is complex to design and implement.
- The implementation cost is very high.
- It requires a special system administration configuration.

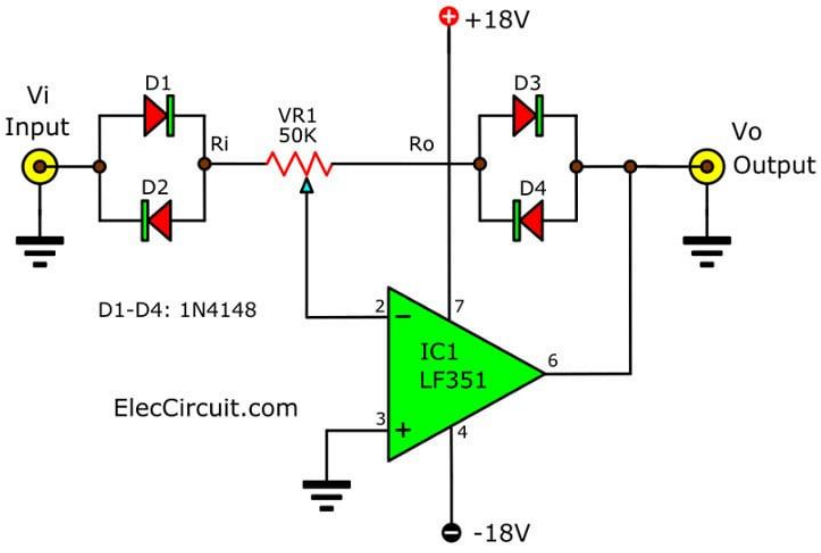
Layer – All layers of OSI model

6. Repeater

Description – Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.

Working Principle – When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Diagram –



Advantages –

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages –

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

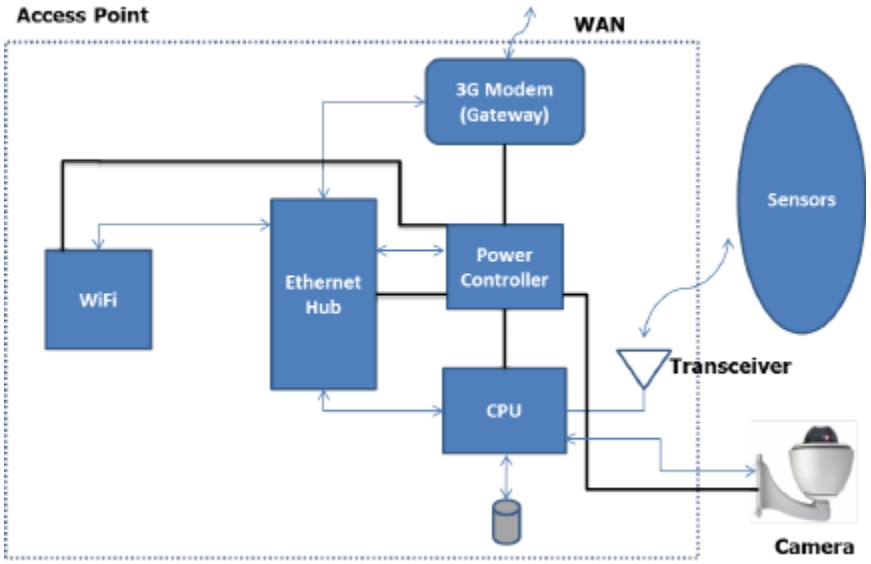
Layer – Physical layer of the OSI model

7. Access Points

Description – An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

Working Principle – Access Points work by connecting direct to your broadband router or network switch with a Ethernet or data cable. This provides the ACCESS POINTS with the internet connection and bandwidth required.

Diagram –



Advantages –

- More users access
- Broader range of transmission
- Flexible networking
- Multi-Access points interconnection

Disadvantages –

- High cost
- Inability to be used alone

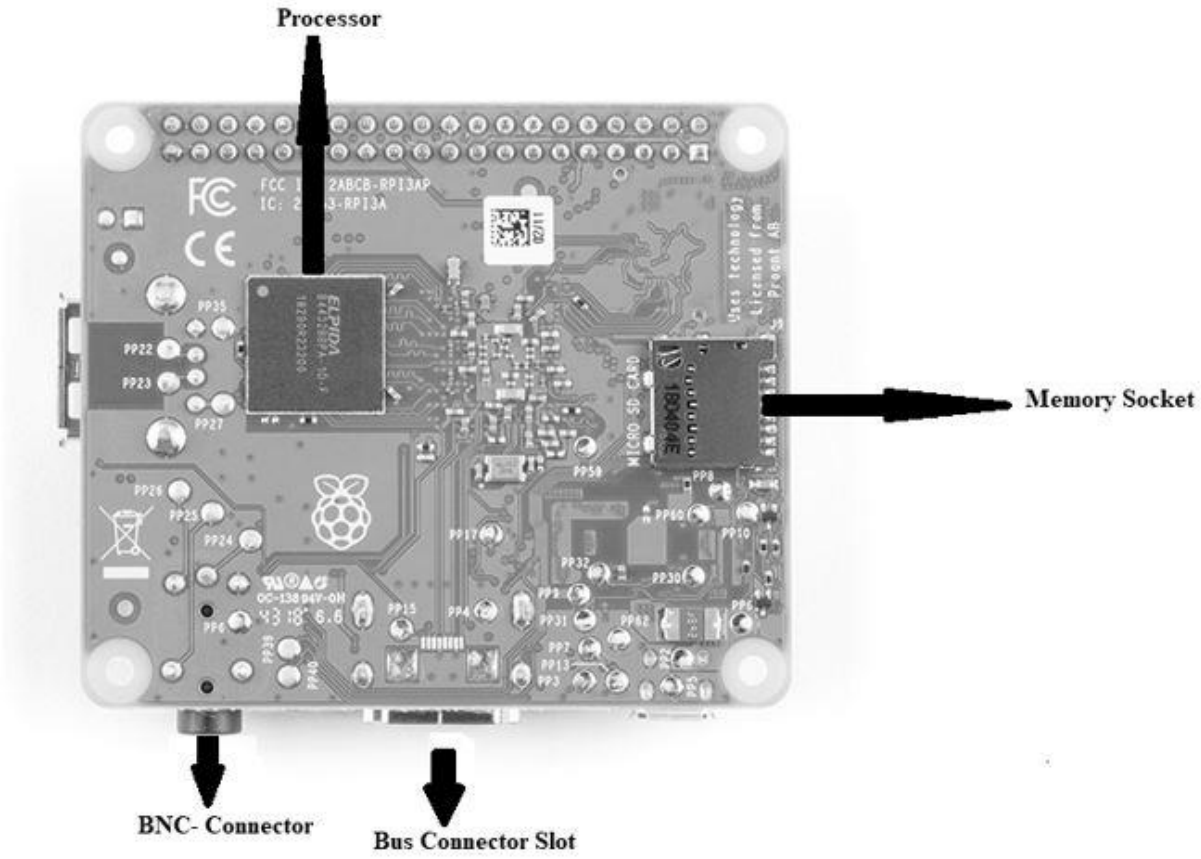
Layer – Data link layer of OSI model

8. Network Interface Card (NIC)

Description – A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter

Working Principle – A NIC provides a computer with a dedicated, full-time connection to a network by implementing the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network. The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer. The network card operates as a middleman between a computer and a data network.

Diagram –



Advantages –

- The communication speed using the Internet is high usually in Gigabytes
- Highly reliable connection
- Many peripheral devices can be connected using many ports of NIC cards.
- Bulk data can be shared among many users.

Disadvantages –

- Inconvenient in case of wired cable NIC, as it is not portable like a wireless router
- The configuration should be proper for better communication.
- Data is unsecured.

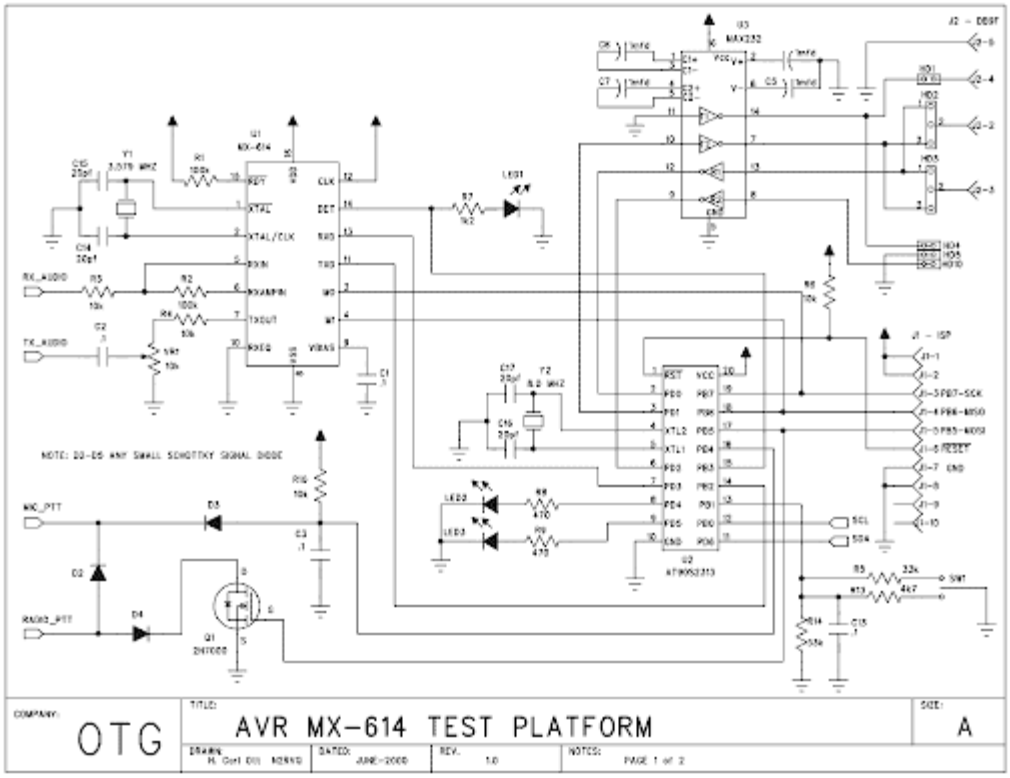
Layer – Data link layer of OSI model

9. Modem

Description – Modem is short for "Modulator-Demodulator." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet.

Working Principle – It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Similarly, it converts digital data from a computer or other device into an analog signal that can be sent over standard telephone lines.

Diagram –



Advantages –

- Signal Conversion
- More Speed
- Less Cost
- Automatic Dialing
- Fax Compatibility

Disadvantages –

- Prone to Malware Attack
- Less Mobility
- Less Availability
- Need for traffic Maintenance
- May interfere with Telephone Services

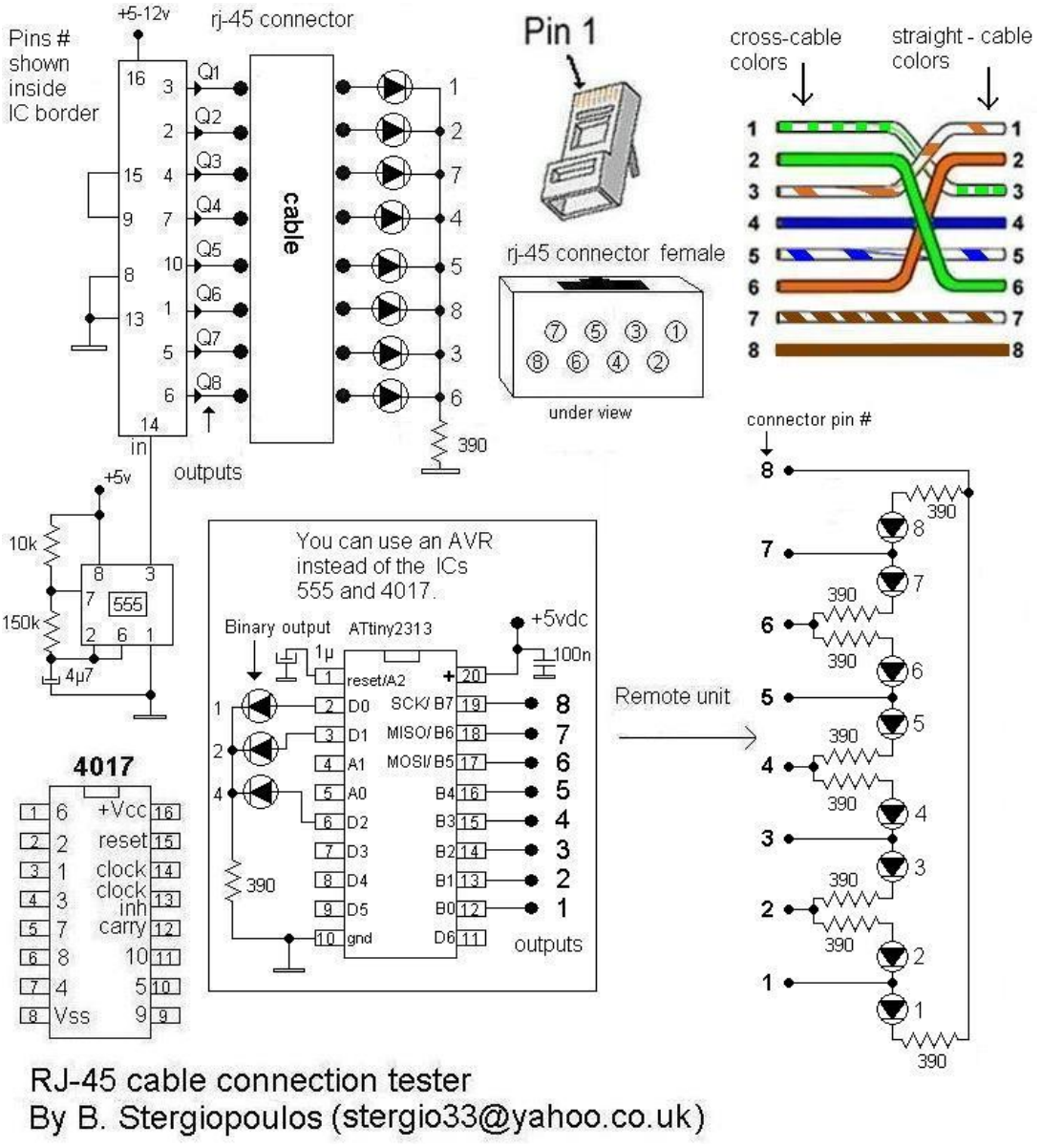
Layer – Data link layer of OSI model

10. LAN

Description – A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

Working Principle – Early LAN networks were formed using coaxial cable, coax is an electric cable and it is used to carry radio signals. LAN (Local Area Network) setup is developed by connecting two or more than two computers with each other using a physical connection in order to share files and data overtime.

Diagram –



Advantages –

- Sharing of resources:
- Client and server relationship
- Sharing of the internet
- Software program sharing
- Securing of data
- Communication is easy, fast, and time-saving
- Computer identification

Disadvantages –

- Data security problem:
- Limitation of distance:
- Setting up a LAN is expensive:

Layer – Physical layer of the OSI model

11. Brouters

Description – A brouter is a device that functions as both a bridge and a router. It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).

Working Principle – The main purpose of a bridge is to connect two separate networks. It simply forwards the incoming packets from one network to the next. A router, on the other hand, is more advanced since it can route packets to specific systems connected to the router. A brouter combines these two functions by routing some incoming data to the correct systems, while forwarding other data to another network. In other words, a brouter functions as a filter that lets some data into the local network, while redirecting unrecognized data to another network.

Advantages –

- It supports packet filtering and packet switching.
- It can be used with both LAN and WAN.
- It offers NAT to be configured and hence hides real IP address of internal network which makes network more secure.
- It can connect with different mediums.

Disadvantages –

- It is expensive compare to hub and router.
- It is complex to manage and requires considerable amount of initial configuration.

Layer – Network layer and Data link layer of the OSI model

Network Commands

1. Ping

Description –

```
C:\Users\Grihit>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Output –

```
C:\Users\Grihit>ping vit.ac.in

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=67ms TTL=52
Reply from 136.233.9.13: bytes=32 time=67ms TTL=52
Reply from 136.233.9.13: bytes=32 time=67ms TTL=52
Reply from 136.233.9.13: bytes=32 time=67ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 67ms, Average = 67ms

C:\Users\Grihit>
```

-t

```
C:\Users\Grihit>ping vit.ac.in -t

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=86ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 9, Received = 9, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 86ms, Average = 83ms
Control-C
^C
C:\Users\Grihit>
```

-a

```
C:\Users\Grihit>ping vit.ac.in -a

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 84ms, Average = 83ms

C:\Users\Grihit>
```

-n count

```
C:\Users\Grihit>ping vit.ac.in -n 3

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 84ms, Average = 83ms
```

-l size

```
C:\Users\Grihit>ping vit.ac.in -l 3

Pinging vit.ac.in [136.233.9.13] with 3 bytes of data:
Reply from 136.233.9.13: bytes=3 time=83ms TTL=52
Reply from 136.233.9.13: bytes=3 time=83ms TTL=52
Reply from 136.233.9.13: bytes=3 time=83ms TTL=52
Reply from 136.233.9.13: bytes=3 time=84ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 84ms, Average = 83ms

C:\Users\Grihit>
```

-f

```
C:\Users\Grihit>ping vit.ac.in -f

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=86ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 86ms, Average = 84ms

C:\Users\Grihit>
```

-i TTL

```
C:\Users\Grihit>ping vit.ac.in -i 2

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 117.97.128.1: TTL expired in transit.
Reply from 117.97.128.1: TTL expired in transit.
Reply from 117.97.128.1: TTL expired in transit.
Reply from 117.97.128.1: TTL expired in transit.

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Grihit>
```

-v TOS

```
C:\Users\Grihit>ping vit.ac.in -v TOS

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52
Reply from 136.233.9.13: bytes=32 time=83ms TTL=52
Reply from 136.233.9.13: bytes=32 time=84ms TTL=52

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 84ms, Average = 83ms

C:\Users\Grihit>
```

-r count

```
C:\Users\Grihit>ping vit.ac.in -r 3

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=21ms TTL=254
Reply from 136.233.9.13: bytes=32 time=3ms TTL=254
Reply from 136.233.9.13: bytes=32 time=3ms TTL=254
Reply from 136.233.9.13: bytes=32 time=3ms TTL=254

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 21ms, Average = 7ms

C:\Users\Grihit>
```

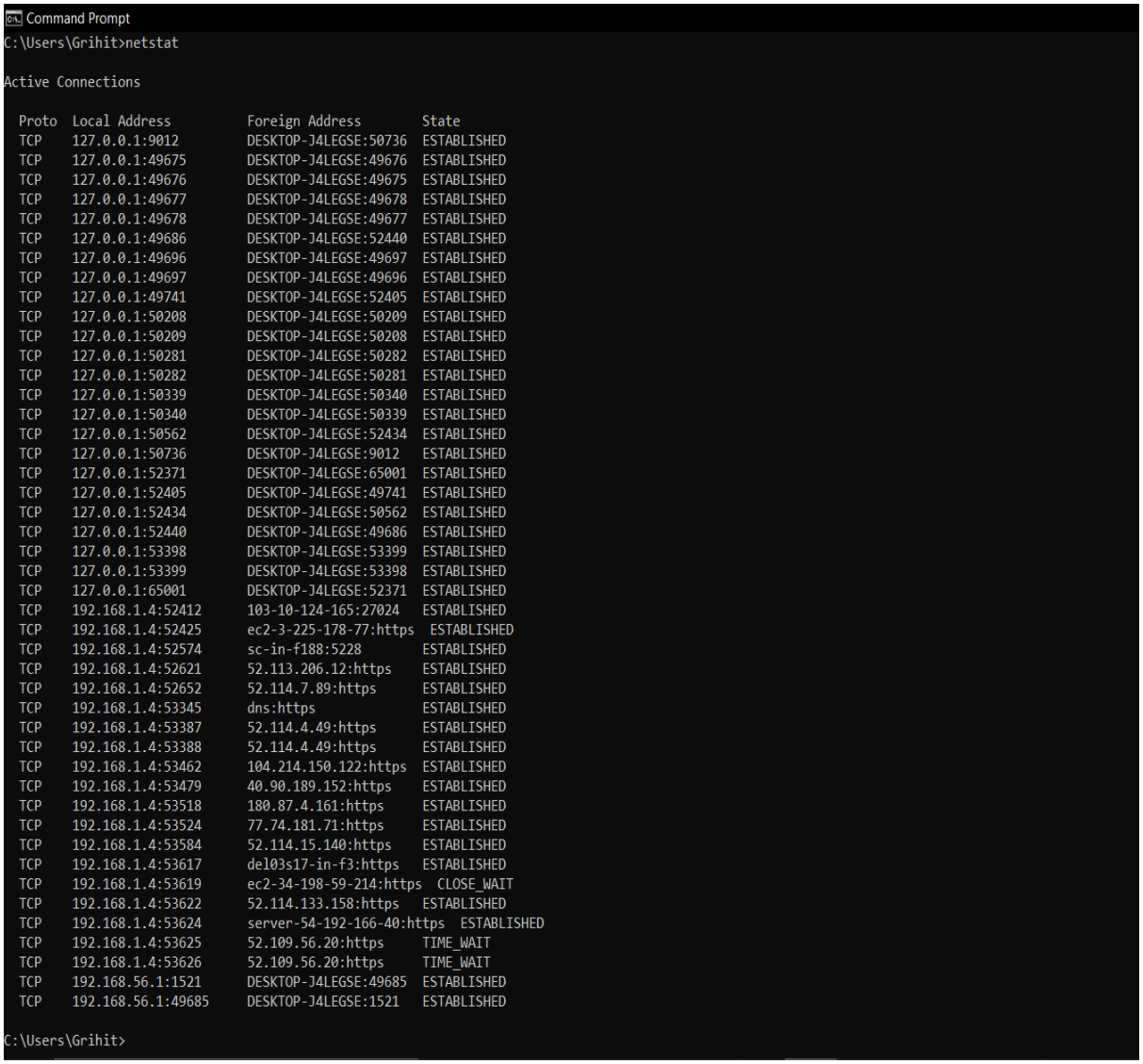
-s count

```
C:\Users\Grihit>ping vit.ac.in -s 3

Pinging vit.ac.in [136.233.9.13] with 32 bytes of data:
Reply from 136.233.9.13: bytes=32 time=3ms TTL=254
Reply from 136.233.9.13: bytes=32 time=3ms TTL=254
Reply from 136.233.9.13: bytes=32 time=15ms TTL=254
Reply from 136.233.9.13: bytes=32 time=22ms TTL=254

Ping statistics for 136.233.9.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 22ms, Average = 10ms

C:\Users\Grihit>
```

2. Netstat

Description – Displays protocol statistics and current TCP/IP network connections.

Output –



3.Hostname

Description – To display full computer name of the computer.

Output –

```
C:\Users\Grihit>hostname
DESKTOP-J4LEGSE

C:\Users\Grihit>
```

4.nslookup

Description – nslookup is a network administration command-line tool available for many computer operating systems. It is used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping information. The main use of nslookup is for troubleshooting DNS related problems.

Output –

```
C:\Users\Grihit>nslookup google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:80b::200e
          216.58.200.206


C:\Users\Grihit>
```

5.traceroute

Description – Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

Output –

```
C:\Users\Grihit>tracert google.com

Tracing route to google.com [216.58.200.206]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  192.168.1.1
  2     4 ms     3 ms     3 ms  abts-north-dynamic-1.128.97.117.airtelbroadband.in [117.97.128.1]
  3     3 ms     9 ms     3 ms  125.16.34.237
  4     4 ms     4 ms     4 ms  182.79.152.79
  5     6 ms     6 ms     6 ms  142.250.161.56
  6     8 ms     7 ms     7 ms  172.253.68.93
  7     7 ms     7 ms     6 ms  172.253.51.5
  8     6 ms     6 ms     6 ms  nrt12s12-in-f206.1e100.net [216.58.200.206]

Trace complete.
```

6.nmap

Description – Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Output –

```
C:\Users\Grihit>nmap google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:11 India Standard Time
Nmap scan report for google.com (172.217.160.238)
Host is up (0.019s latency).
rDNS record for 172.217.160.238: del03s09-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds

C:\Users\Grihit>
```

7. ip route show

Description – In computing, route is a command used to view and manipulate the IP routing table in Unix-like and Microsoft Windows operating systems and also in IBM OS/2 and ReactOS. Manual manipulation of the routing table is characteristic of static routing.

Output –

```
C:\Users\Grihit>route print
===========================================================================
Interface List
 21...54 bf 64 4d 1a f2 ......Killer E2400 Gigabit Ethernet Controller #2
 23...00 ff c9 0f d9 88 ......TAP-ProtonVPN Windows Adapter V9
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter
 22...3c 6a a7 83 ba 45 ......Microsoft Wi-Fi Direct Virtual Adapter
 24...3e 6a a7 83 ba 44 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  3...00 ff 17 0d e9 8c ......Kaspersky Security Data Escort Adapter
 15...02 18 2d ad 0d 6c ......Intel(R) Wireless-AC 9560 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.4     55
        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
      192.168.1.0    255.255.255.0         On-link       192.168.1.4    311
      192.168.1.4  255.255.255.255         On-link       192.168.1.4    311
    192.168.1.255  255.255.255.255         On-link       192.168.1.4    311
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        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      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link       192.168.1.4    311
  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      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link       192.168.1.4    311
===========================================================================
Persistent Routes:
  None
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 12    281 fe80::/64                On-link
 15    311 fe80::/64                On-link
 15    311 fe80::cbf:5703:e84d:b703/128
                                    On-link
 12    281 fe80::396a:302e:a984:df49/128
                                    On-link
  1    331 ff00::/8                 On-link
 12    281 ff00::/8                 On-link
 15    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\Grihit>
```

8.ipconfig

Description – The ipconfig command is a fast way of determining your computer's IP address and other information, such as the address of its default gateway—useful if you want to know the IP address of your router's web interface.

Output –