Computer Networks

- Download Computer Network PDF.
- Computer Networks.
- Uses of Computer Networks.
- Computer Networks Related CMD Commands.
- Types of Networks.
- Types of Network Topology.
- Repeaters in Networking
- Hubs in Networking
- Bridges in Networking
- Switches in Networking
- Routers in Networking
- Modems in Networking
- Firewalls in Networking
A computer network is a connection between two or more computers with the help of medium such as coaxial cables, Wi-Fi, optical fibers, LAN cables etc.

Data transmission medium or connecting media is divided into two parts wired and wireless.

- **Wired**: Coaxial cable, optical fiber, twisted pair cabling these are examples of wired media.
- **Wireless**: Wi-Fi, Bluetooth, Communication Satellites which uses microwave radio waves, cellular system, radio spectrum etc. are examples of wireless media.

The Internet is the greatest example of a computer network. Now, everything including your mobile phone, your smart television, your smart home, CCTV camera all of these are connected with the help of the Internet.

I am going to centralize this article on Internet related computer network only. With the help of this article, you can know about different terminologies related to a computer network.

**Why Computer Network is important?**

If you are using your laptop or your mobile and you are asked to use them without the internet, then what you’ll do?

I think you can’t do that. Why?
The answer is simple Internet provide us seamless opportunity to share our views, emotions, money, news, information and many other things. Internet helps us in accomplishing most of our task so easily. You want to watch video open YouTube and watch, you want to purchase anything go to amazon website and you can purchase anything.

All these things are possible only because of computer networks. When one computer is connected to another computer it means now you can communicate with another person with the help of your computer. This is why the computer network is the most important part of our life.
Uses of Computer Networks

There is numerous use of computer networks. Some of them are listed below:

**Sharing Information:** You want to share information with others then computer networks have made this task much easier for you. Sharing information with others was the main goal of starting computer networks.

The most perfect example is the Facebook. If you use Facebook then you can easily share your information like your likes, photos, videos, your places you visit etc. Computer networks make all these tasks so easy.

**Sharing Resources:** If you want to share a physical or digital resource like your printer, bike, car, house, video etc. then you can do with the help of computer networks. On the internet there many websites like Uber, 99acres, OLX which makes sharing possible in a much easier way only with the help of computer networks.
9 Computer Networks Related CMD Commands

These are some useful CMD commands related to computer networks.

If you are the user of the Windows Operating System, then with the help of this command you can perform and know about different computer networks related tasks.

1. Netstat
2. Ipconfig
3. Ping
4. ARP
5. Hostname
6. Tracert
7. Pathping
8. Netsh
9. NSlookup

1. **Netstat Command**: If you want to know about all active connections of your computer then you can use Netstat command. It provides you detailed information about computer network and how it is communicating with other networks. Netstat also helps in detecting malware and spyware.
2. **Ipconfig Command**: This command will help you in knowing all about IP (Internet Protocol). You can know your computer IP address.

State of different computer network devices such as Ethernet Adapter, Wireless LAN (Local Area Network), Tunnel Adapter etc. You can check whether all these network devices are active or not.

```
C:\Users\Praveen>ipconfig

Windows IP Configuration

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

Wireless LAN adapter Local Area Connection* 2:
    Media State ................ : Media disconnected
    Connection-specific DNS Suffix : 

Wireless LAN adapter Local Area Connection* 15:
    Media State ................ : Media disconnected
    Connection-specific DNS Suffix : 

Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix : 
    Link-local IPv6 Address ........ : fe80::2051:12d5:c13b:2f42%20
    IPv4 Address ................ : 192.168.43.30
    Subnet Mask ................ : 255.255.255.0
    Default Gateway .............. : 192.168.43.1

Tunnel adapter Local Area Connection* 14:
    Connection-specific DNS Suffix : 
    Link-local IPv6 Address ........ : fe80::2829:1282:df0f:1fc7%12
    Default Gateway .............. : 

C:\Users\Praveen>
```
3. **Ping Command:** If you are using the Internet and want to test the reachability of any website then you can use Ping command. Ping command also provides us with many useful data such as round trip time i.e. time taken to send and receive data packets.

```
C:\Users\Praveen>ping google.com

Ping statistics for 216.58.196.206:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 45ms, Maximum = 62ms, Average = 53ms
```

```
4. **ARP Command**: ARP command stands for Address Resolution Protocol Command. This command will show you matching MAC addresses of IP addresses.

You can clearly observe in the given below example that when I typed ‘ARP –a’ in the command prompt it shows me a list of IP address along with its matching Physical Address which is also known as MAC address.

```
\Users\Praveen>arp
Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g Same as -a.
-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.
inet_addr Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.
```

**Example:**
```
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a
.... Displays the arp table.
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>192.168.43.30</th>
<th>0x14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Address</td>
<td>Physical Address</td>
<td>Type</td>
</tr>
<tr>
<td>192.168.43.1</td>
<td>7e-4b-85-06-b4-e1</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.43.255</td>
<td>ff-ff-ff-ff-ff-ff</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.20</td>
<td>01-00-5e-00-00-16</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.25</td>
<td>01-00-5e-00-00-00</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.252</td>
<td>01-00-5e-00-00-0c</td>
<td>static</td>
</tr>
</tbody>
</table>
5. **Hostname Command**: If you want to see your computer name or you want to set your computer name then you can use hostname command.

![Command Prompt]

```
C:\Users\Praveen>hostname
DESKTOP-H2P2LOE
C:\Users\Praveen>
```

6. **Tracert Command**: If you want to trace network packet being sent and received then you can use Tracert command. You can find an example in the given below snap in which when I typed `tracert google.com` then it detected number packets sent and received through my IP address to Google IP address.

```
C:\Users\Praveen>Tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]

Options:
   -d Do not resolve addresses to hostnames.
   -h maximum_hops Maximum number of hops to search for target.
   -j host-list  Loose source route along host-list (IPv4-only).
   -R          Trace round-trip path (IPv6-only).
   -s srcaddr  Source address to use (IPv6-only).

C:\Users\Praveen>tracert google.com
Tracing route to google.com [172.217.166.238] over a maximum of 30 hops:
1    1 ms 1 ms 1 ms 152.108.43.1
2    * Request timed out.
3    30 ms 41 ms 53 ms 16.72.48.50
4    41 ms 38 ms 38 ms 172.25.44.169
5 General failure.
Trace complete.
```

Here it is written ‘over a maximum of 30 hops’. Hops mean a number of routers through which data packet must pass through the source and the destination.
7. **Pathping Command:** if you want to combine ‘ping’ command with ‘tracert’ then you can use ‘pathping’ command. Suppose that I want to trace the route of google.com along with its sent and received packets then I can use ‘pathping’ command.

```
C:\Users\Praveen>pathping google.com
```

```
Tracing route to google.com [216.58.196.206]
over a maximum of 30 hops:
   0 DESKTOP-H2P2LOE [192.168.43.30]
   * * *
Computing statistics for 0 seconds...
   Source to Here    This Node/Link            Address
   Hop   RTT    Lost/Sent = Pct  Lost/Sent = Pct
   0  
Trace complete.
C:\Users\Praveen>
```
8. **Netsh Command:** You can know detail information about the network configuration of your computer with the help of ‘netsh’ command.

Know about your connected Wi-Fi password with the help of command ‘netsh wlan show profile Wi-Fi-name key=clear’ by opening CMD in administrator mode. Also, you can view the whole set of network configuration data in details.
9. **NSLookup Command:** Know about DNS (Domain Name System) of any domain with the help of DNS command. You can know about the IP address and domain name as this information is stored in DNS records.

![NSLookup Command Example]

```
C:\Users\Praveen>nslookup google.com
Server: Unknown
Address: 192.168.43.1

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4002:809::200e
172.217.166.238
```

C:\Users\Praveen>
Types of Networks

Computer networks have been classified into different types according to size and use. Below you can find some major types of networks.

1. PAN (Personal Area Network)
2. LAN (Local Area Network)
3. WLAN (Wireless Local Area Network)
4. CAN (Campus Area Network)
5. MAN (Metropolitan Area Network)
6. WAN (Wide Area Network)
7. SAN (Storage Area Network)
8. VPN (Virtual Private Network)

1. **PAN (Personal Area Network):** When you use a computer network for your personal use such as you are transferring your pictures from mobile to laptop or printing a document from your mobile then you are in Personal Area Network (PAN). PAN can have mobiles, tablets, laptops connected with other at your home.
2. LAN (Local Area Network):

When you connect a group of computers inside a building or two or three buildings then this type of networks is called LAN. You have observed that at your school or office whole computer are connected with each other to share file or documents. This comes under Local Area Network (LAN).
3. **WLAN (Wireless Local Area Network):** WLAN is similar to LAN. The only difference between LAN and WLAN is the wireless connectivity of WLAN. Mostly WLAN is connected with Wi-Fi whereas LAN is connected with cables.

4. **CAN (Campus Area Network):** CAN is used for campus computer network connectivity. When computers inside a college campus having two or more branches or university or group of government or private campus is connected with each other then it comes under the CAN. CAN is larger in comparison to LAN but smaller in comparison of MAN. The best example of the CAN is Wi-Fi connectivity at big airports and railway stations.
5. **MAN (Metropolitan Area Network):** You have observed that in many big cities an entire geographical area is connected to a network such as free Wi-Fi. Such type of computer network which is larger than CAN but smaller that WAN is known as Metropolitan Area Network (MAN).

![MAN Network Use](image)

6. **WAN (Wide Area Network):** The best example of WAN is the internet. It is more complex and bigger in comparison to the Metropolitan Area Network (MAN). WAN connects larger numbers of the computer together.

7. **SAN (Storage Area Network):** Storage Area Network is totally different from LAN or other simple computer network types. When you want to enhance your storage device such as servers then you can use SAN. SAN is faster to provide data storage and retrieval facility.
8. **VPN (Virtual Private Network):** VPN is used when a private company or government want to share their data with each other in a secure way.

Suppose that you are working on a large project and you want to remain connected with other people on that same project but all those project members are in different parts of the world. Then you can use Virtual Private Network to share your data in a secure way as when you use VPN your data travels in an encrypted way.
Types of Network Topology

The network topology is the arrangement of computers in a network. The word ‘topology’ is a Greek word which is related to geometry and set theory.

Computer networks have been classified into different topology according to the arrangement of computers and Nodes in a computer network.

Here Nodes means the inter-connecting point of a network. You can clearly understand nodes meaning if you know about these things:

- Hubs
- Repeaters
- Bridges
- Switches
• Routers
• Modems
• Firewalls

Now, these are types of network topology:

• Bus
• Star
• Ring
• Mesh
• Hybrid

**Bus Topology:**

In computer networking, bus topology is the simplest one. Mainly used in local area networks each computer in bus topology is connected to a single cable.

The main cable is called bus and all other network nodes are connected to this cable only.

**Advantages of Bus Topology**

- Effective to use in smaller networks like LAN.
- Less costly as cable requirement is less.
Disadvantages of Bus Topology

- If the main cable fails, then the whole system will stop working.
- Data transmit only in one direction.
- Slower in comparison to other network topology.

Star Topology:

Start topology is more complex in comparison to bus topology. Here each computer is connected to a master computer which is also known as a central hub with a point-to-point connection.

In the start topology, each computer is indirectly connected. Here every traffic has to be passed from a central hub which acts as a signal repeater.
Advantages of Star Topology

- Easy to set up.
- Can be upgraded easily as it is easy to add a new node.
- Problems can be easily detected.

Disadvantages of Star Topology

- Costly in comparison to bus topology.
- Hub is the central part. So, if the hub fails the whole system will stop working.

Ring Topology:

In a ring topology, each computer is connected to another to form a ring. It is similar to bus topology except that ring topology is in a closed loop.

Advantages of Ring Topology

- Able to handle high traffic as each node in a ring topology is act as a repeater.
- Here no server or hub is required to control connectivity.
Disadvantages of Ring Topology

- As the whole network is interlinked with each other if one computer fails then it affects the whole network.
- Removing and adding a new computer to a network is difficult.

Mesh Topology:

Mesh topology is really a mesh. Here each computer may be connected to every other computer in the network. It is a point-to-point connection between computers.

Advantages of Mesh Topology

- It is fully connected, robust and independent from each other.
Disadvantages of Mesh Topology

- Costlier as more cables are required.
- Difficult to install and configure.

Hybrid Topology:

A hybrid topology is a combination of two or more topologies. Suppose that you want to combine a ring topology with bus topology and then with mesh topology then it comes under hybrid topology.

Advantages of Hybrid Topology

- Effective, scalable and reliable.
Disadvantages of Hybrid Topology

- Costly and complex.

Hubs in Networking

In computer networks hub is a device through which you can connect multiple computers at a time. It has many Ethernet ports that help in connecting many computers at a time.

For e.g., you want to connect two or more computers to a network or the internet then you can use a hub and with the help of Ethernet, you can connect all of them together.
Repeaters in Networking

If you want to repeat a received signal with more power. You can use repeaters. You have seen telecommunication towers that are used to extend signals. That towers are repeaters.

Repeaters perform several tasks such as receiving a signal, re-transmitting a signal with more power, removing noise.
Bridges in Networking

What does a bridge do in real life?

It connects two distant places. Bridges in networking connect two or more networks that use the same protocol.

How Bridge is different from repeaters?
Bridge join two networks having same protocol means bridge perform traffic filtering where are repeaters do not perform traffic filtering it join all the traffic they receive.

**Switches in Networking**

Switches connect two or more networks same as bridges. Here you might have a question that if switches and bridges perform the same task then why there are two different devices i.e. switches and bridges?

The answer is bridged are slow it matches MAC address having same protocol then connects the networks whereas switches are faster.
Switches split each port. So, there is no more collision. It also provides a full duplex mode of transmission.

Routers in Networking

Routers in networking are a device that receives incoming data packets from computer networks and then analyzes incoming traffic to redirect those traffic within the network or to another network.

Routers are more efficient in comparison to other networking devices such as hub, bridges, and switch.
Modems in Networking

Modems in networking are a device which converts digital signal to analog and analog signal to digital signal. The full form of Modems is Modulator and Demodulator.

In simple words when we use a landline connection for computer networking or internet connection then the modem is required.
Basically, digital signal can’t be transmitted through landline cables. The signal which is transmitted by phone cables is analog.

And a computer only understands the digital signal. So, a modem converts that analog signal to digital at the time of receiving and digital to an analog signal at the time of sending.

**Firewalls in Networking**

In a computer, networking firewall is a system designed for network security. The firewall may be a software or may be a hardware or may be a combination of both.

The main task of the firewall is to prevent unauthorized access in a private network by analyzing network traffic.
Suppose that your computer is connected to a LAN network and that LAN network is connected to WAN network. If an unknown or untrusted application or computer from WAN wants to enter into your LAN network, then the firewall will prevent that unwanted access to secure your network. This is the simple use of firewall in computer networks.

**Conclusion**

*With the help of this article, I tried to clear all basic concepts of computer networks, types of networks use of computer networks, computer networks topology, some networking devices such as modems, routers, switch, hub etc.*
Please share this article and leave a comment below if you have any questions.