**NETWORKING**

1. **TCP / IP**

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet. TCP/IP is also used as a communications protocol in a private computer network

It chooses how the information will be traded over the web through end-to-end communications that incorporate how the information ought to be organized into bundles (bundles of data), addressed, sent, and received at the goal.

This communication protocol can also be utilized to interconnect and organize devices in a private network such as an intranet or an extranet.

HISTORY

The Defense Advanced Research Projects Office (DARPA), the investigation department of the U.S. Department of Defense, made the TCP/IP shown in the 1970s for utilization in ARPANET, a wide zone organize that gone before the web.

TCP/IP was initially planned for the Unix working framework, and it has been built into all of the working frameworks that came after it.

### **Characteristics of TCP/IP:**

* Share Data Transfer: The TCP allows applications to create channels of communication across a network. It also permits a message to be separated into smaller packets before they are transmitted over the web and after that collected in the right order at the destination address. So, it guarantees the solid transmission of data across the channel.
* Internet Protocol: The IP address tells the packets the address and route so that they reach the proper destination. It includes a strategy that empowers portal computers on the internet-connected to arrange forward the message after checking the IP address.
* Reliability: The most vital feature of TCP is solid data delivery. In arrange to supply unwavering quality, TCP must recover information that’s harmed, misplaced, copied, or conveyed out of arrange by the Arrange Layer.
* Multiplexing: Multiplexing can be achieved through the number of ports.
* Connections: Before application forms can send information by utilizing TCP, the devices must set up a connection. The associations are made between the harbor numbers of the sender and the collector devices.

### **TCP/IP Layers**

* Application Layer An application layer is the topmost layer within the TCP/IP model. When one application layer protocol needs to communicate with another application layer, it forwards its information to the transport layer.
* Transport Layer It is responsible for the reliability, flow control, and correction of data that is being sent over the network. There are two protocols used in this layer User Datagram Protocol and Transmission control protocol.
* Internet/Network Layer It is the third layer of the TCP/IP Model and is also known as the Network layer. The main responsibility of this layer is to send the packets from any network, and they arrive at the goal irrespective of the route they take.
* Network Access Layer It is the lowest layer of the TCP/IP Model. It is the combination of the Physical Layer and the Data link layer present in the OSI Model. Its main responsibility is to the transmission of information over the same network between two devices.

### **How does TCP/ IP works?**

* TCP/IP employs the client-server demonstration of communication in which a client or machine (a client) is given a benefit (like sending a webpage) by another computer (a server) within the network.
* Collectively, the TCP/IP suite of conventions is classified as stateless, which suggests each client request is considered new since it is irrelevant to past requests. Being stateless liberates up network paths so they can be utilized continuously.
* The transport layer itself, is stateful. It transmits a single message, and its connection remains open until all the packets in a message have been received and reassembled at the destination.
* The TCP/IP model differs from the seven-layer Open System Interconnection (OSI) model designed after it.

### **Application/Uses of TCP/IP**

Some Real-Time Applications are:

* Simple Mail Transfer Protocol(SMTP): It helps to send email to another email address.
* File Transfer Protocol(FTP): It is used for sending large files.
* Dynamic Host Configure Protocol(DHCP): It assigns the IP address.
* Telnet: Bi-directional text communication via a terminal application.
* HyperText Transfer Protocol(HTTP): Used to transfer web pages.
* Domain Name System(DNS): It translates the website name to IP addresses.
* Simple Network Time Protocol(SNTP): It provides the time of a day to the network devices.

**PORT NUMBER**

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain [protocols](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) — for example, all [Hypertext Transfer Protocol (HTTP)](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) messages go to port 80. While [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) enable messages to go to and from specific devices, port numbers allow the targeting of specific services or applications within those devices.

Port number is a 16-bit numerical value that ranges from 0 to 65535. Well-known port (0-1023), registered port (1024-49151), and dynamic port is three types of port number space. (49152-65535). When interacting over the Internet, TCP and UDP protocols make connections, recompile data packages after the transfer, and then deliver them to applications on the recipient’s device.

Vastly different types of data flow to and from a computer over the same network connection. The use of ports helps computers understand what to do with the data they receive.

| Port Number | Service name | Transport protocol | Description |
| --- | --- | --- | --- |
| 7 | Echo | TCP, UDP | Echo service |
| 20 | FTP-data | TCP, SCTP | File Transfer Protocol data transfer |
| 21 | FTP | TCP, UDP, SCTP | File Transfer Protocol (FTP) control connection |
| 22 | SSH-SCP | TCP, UDP, SCTP | Secure Shell, secure logins, file transfers (scp, sftp), and port forwarding |
| 23 | Telnet | TCP | Telnet protocol—unencrypted text communications |
| 25 | SMTP | TCP | Simple Mail Transfer Protocol, used for email routing between mail servers |
| 53 | DNS | TCP, UDP | Domain Name System name resolver |
| 69 | TFTP | UDP | Trivial File Transfer Protocol |
| 80 | HTTP | TCP, UDP, SCTP | Hypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2.  HTTP/3 uses QUIC, a transport protocol on top of UDP |
| 88 | Kerberos | TCP, UDP | Network authentication system |

**TOPOLOGY**

| point | bus | star | ring | mesh | tree |
| --- | --- | --- | --- | --- | --- |
| Architecture | is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable. The cable to which the nodes connect is called a "backbone". If the backbone is broken, the entire segment fails. | is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch. A star takes more cable | A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points in a circle. Together, devices in a ring topology are referred to as a ring network. | a network setup, all the computers are connected to each other in a network. It is very difficult to establish the connections of the mesh topology. In a Mesh topology, every computer has a point-to-point connection to the other computer. In order to connect n nodes, mesh topology requires n(n-1)/2 communication links. | in Tree Topology, all the computer is connected to the central hub, in the computer networking, tree topology is known as a combination of a star network topology and a bus topology. In tree topology, all the computers are connected like the branches of a tree. |
| Complexity | Easy to connect or remove nodes in a network without affecting any other node | average complexity each device connects to a central device with only one link only | Complexity because of simple to data to devices | Installation is complex in a mesh topology, as each node is connected to more than one node. | More complex because the tree is a combination of a star network topology and a bus topology |
| Security | Any computer that is connected to a bus topology network will be able to see all the data transmissions on all the other computers | Security depends on central device security | data travels from one device to the next until they reach their destination | The data pass over more than one node | The data pass over more than one node |
| Advantages | It works well when you have a small network.  • It's the easiest network topology for connecting computers or peripherals in a linear fashion.  • It requires less cable length than a star topology. | Centralized management of the network, through the use of the central computer, hub, or switch. Easy to add another computer to the network. If one computer on the network fails, the rest of the network continues to function normally. | • All data flows in one direction, reducing the chance of packet collisions.  • A network server is not needed to control network connectivity between each workstation.  • Data can transfer between workstations at high speeds.  • Additional workstations can be added without impacting the performance of the network. | The failure of a single node in the network can cause the entire network to fail.  • The transmission speed drops with an increase in the number of nodes.  • Fault tolerance.  • Guaranteed communication channel capacity.  • Easy to troubleshoot. | It is a combination of bus and star topology  • It provides high scalability, as leaf nodes can add more nodes in the hierarchical chain.  • Other nodes in a network are not affected, if one of their nodes gets damaged  • It provides easy maintenance and fault identification.  • Supported by several hardware and software vendors.  • Point-to-point wiring for individual segments. |
| Disadvantages | It can be difficult to identify the problems if the whole network goes down.  • It can be hard to troubleshoot individual device issues.  • Bus topology is not great for large networks.    • Terminators are required for both ends of the main cable.  • Additional devices slow the network down.  • If a main cable is damaged, the network fails or splits into two. | • May have a higher cost to implement, especially when using a switch or router as the central network device.  • The central the network device determines the performance and number of nodes, the network can handle.  • If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network. | • All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.  • The entire the the network will be impacted if one workstation shuts down.    • The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches. | • A lot of cabling is required. Thus, the costs are high.    • Owing to its complexity, the administration of a mesh network is difficult.  • Difficulty of installation and reconfiguration.  • Cost of maintaining the redundant link. | • Large cabling is required as compared to star and bus topology.    • On the failure of a hub, the entire network fails.  • Tree network is very difficult to build Architecture than other network topologies. |