Types of Network Topology

The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are :

a) Mesh Topology :

In mesh topology, every device is connected to another device via particular channel.

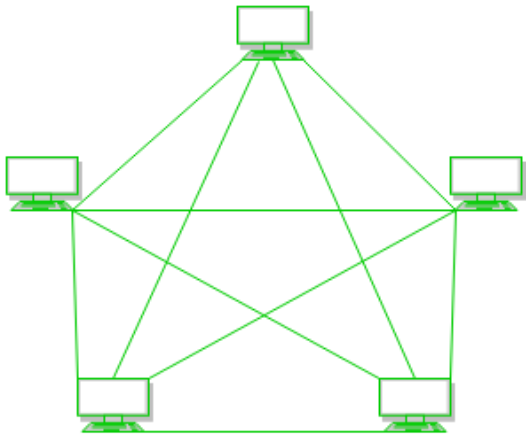


Figure 1 : Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.
- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

Advantages of this topology :

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

- Provides security and privacy.

Problems with this topology :

- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

b) Star Topology :

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hubs. Active hubs have repeaters in them.

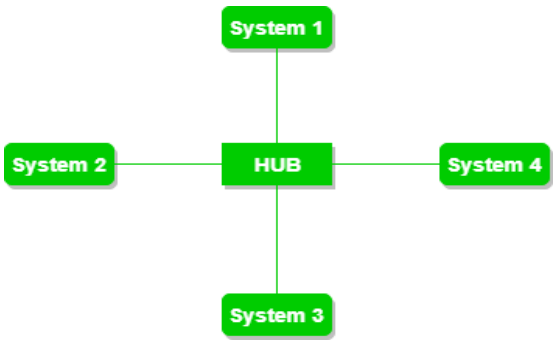


Figure 2 : A star topology having four systems connected to single point of connection i.e. hub.

Advantages of this topology :

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device require only 1 port i.e. to connect to the hub.

Problems with this topology :

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.

- Performance is based on the single concentrator i.e. hub.

c) Bus Topology :

Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

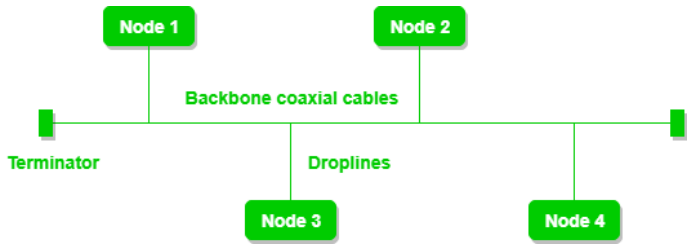


Figure 3 : A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology :

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Problems with this topology :

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology :

In this topology, it forms a ring connecting a devices with its exactly two neighbouring devices.

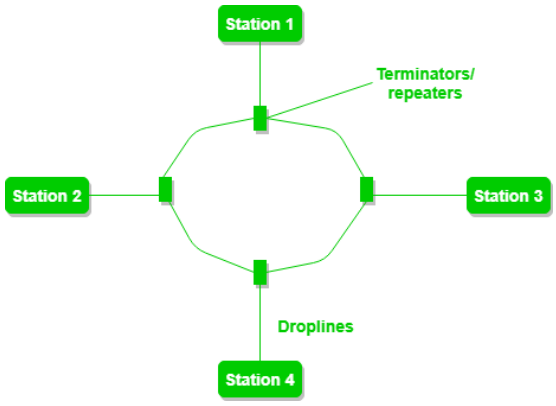


Figure 4 : A ring topology comprises of 4 stations connected with each forming a ring..

The following operations takes place in ring topology are :

- One station is known as monitor station which takes all the responsibility to perform the operations.
- To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques : Early token release releases the token just after the transmitting the data and Delay token release releases the token after the acknowledgement is received from the receiver.

Advantages of this topology :

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with this topology :

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

e) Hybrid Topology :

This topology is a collection of two or more topologies which are described above. This is a scalable topology which can be expanded easily. It is reliable one but at the same it is a costly topology.

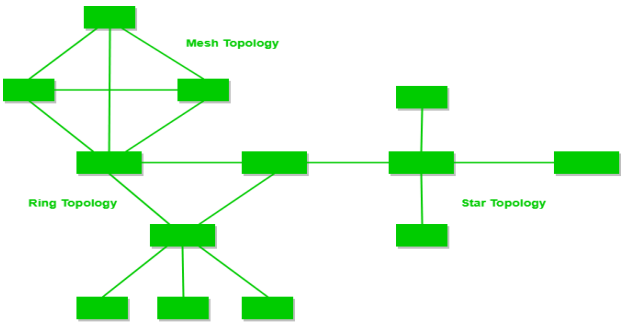
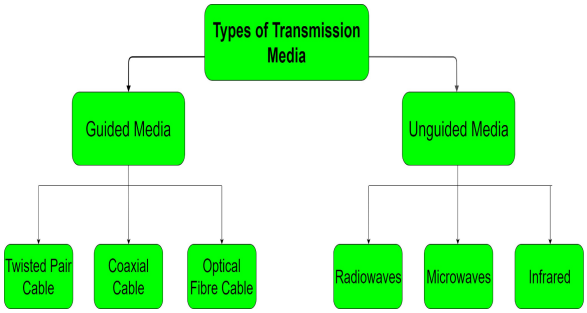


Figure - A Hybrid Topology

Figure 5 : A hybrid topology which is a combination of ring and star topology.

Types of Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High speed capacity

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparitively faster

Disadvantages:

- Comparitively difficult to install and manufacture
- More expensive
- Bulky

(ii) Coaxial Cable –

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

High Bandwidth

Better noise Immunity

Easy to install and expand

Inexpensive

Disadvantages:

Single cable failure can disrupt the entire network

(iii) Optical Fibre Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volumes of data.

Advantages:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile
- unidirectional, ie, will need another fibre, if we need bidirectional communication

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

Features:

- Signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 major types of Unguided Media:

(i) Radiowaves –

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Medium access control

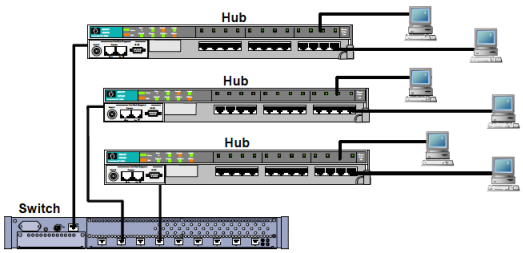
In IEEE 802 LAN/MAN standards, the medium access control (MAC, also called media access control[1]) sublayer is the layer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. The MAC sublayer and the logical link control (LLC) sublayer together make up the data link layer. Within the data link layer, the LLC provides flow control and multiplexing for the logical link (i.e. EtherType, 802.1Q VLAN tag etc), while the MAC provides flow control and multiplexing for the transmission medium.

These two sublayers together correspond to layer 2 of the OSI model. For compatibility reasons, LLC is optional for implementations of IEEE 802.3 (the frames are then "raw"), but compulsory for implementations of other IEEE 802 physical layer standards. Within the hierarchy of the OSI model and IEEE 802 standards, the MAC sublayer provides a control abstraction of the physical layer such that the complexities of physical link control are invisible to the LLC and upper layers of the network stack. Thus any LLC sublayer (and higher layers) may be used with any MAC. In turn, the medium access control block is formally connected to the PHY via a media-independent interface. Although the MAC block is today typically integrated with the PHY within the same device package, historically any MAC could be used with any PHY, independent of the transmission medium.

When sending data to another device on the network, the MAC sublayer encapsulates higher-level frames into frames appropriate for the transmission medium (i.e. the MAC adds a syncword preamble and also padding if necessary), adds a frame check sequence to identify transmission errors, and then forwards the data to the physical layer as soon as the appropriate channel access method permits it. For topologies with a collision domain (bus, ring, mesh, point-to-multipoint topologies), controlling when data is sent and when to wait is necessary to avoid collisions. Additionally, the MAC is also responsible for compensating for collisions by initiating retransmission if a jam signal is detected. When receiving data from the physical layer, the MAC block ensures data integrity by verifying the sender's frame check sequences, and strips off the sender's preamble and padding before passing the data up to the higher layers.

What’s the Difference Between Hubs, Switches & Bridges?

The key difference between hubs, switches and bridges is that hubs operate at Layer 1 of the OSI model, while bridges and switches work with MAC addresses at Layer 2. Hubs broadcast incoming traffic on all ports, whereas bridges and switches only route traffic towards their addressed destinations



What is a Hub?

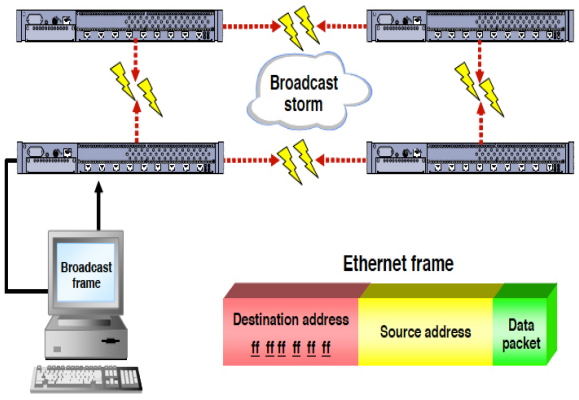
Hubs provide a dedicated physical connection for every device, which helps reduce the possibility that a failure of one computer will cause all computers to lose connectivity. However, because a hub is still a shared bandwidth device, connectivity is limited to half-duplex. Collisions remain an issue as well, so hubs do not help improve the performance of the network.

Hubs are essentially multiport repeaters. They ignore the content of an Ethernet frame and simply resend every frame they receive out of every interface on the hub. The challenge is that the Ethernet frames will show up at every device attached to a hub, instead of just the intended destination (a security gap), and inbound frames often collide with outbound frames (a performance issue).

What is a Bridge?

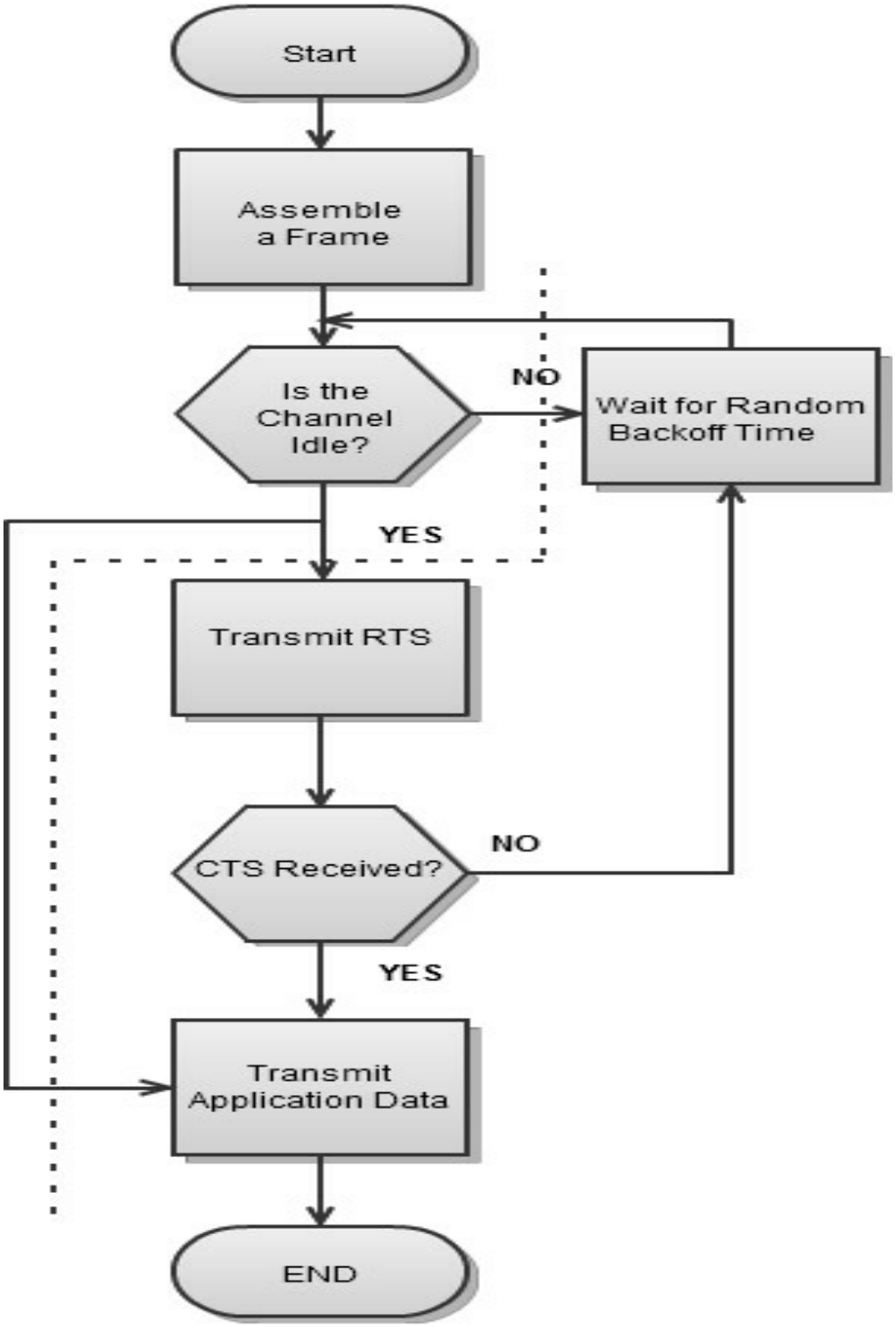
In the physical world, a bridge connects roads on separate sides of a river or railroad tracks. In the technical world, bridges connect two physical network segments. Each network bridge keeps track of the MAC addresses on the network attached to each of its interfaces. When network traffic arrives at the bridge and its target address is local to that side of the bridge, the bridge filters that Ethernet frame, so it stays on the local side of the bridge only.

If the bridge is unable to find the target address on the side that received the traffic, it forwards the frame across the bridge, hoping the destination will be on the other network segment. At times, there are multiple bridges to cross to get to the destination system.



The big challenge is that broadcast and multicast traffic must be forwarded across each bridge, so every device has an opportunity to read those messages. If the network manager builds redundant circuits, it often results in a flood of broadcast or multicast traffic, preventing unicast traffic flow.

CSMA/CD


Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
YES
Transmit RTS
CTS Received?
NO
YES
Transmit Application Data
END

Short for carrier sense multiple access/collision detection, CSMA/CD is a MAC (media access control) protocol. It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.

There are several CSMA access modes: 1-persistent, P-persistent, and O-persistent. 1-persistent is used in CSMA/CD systems, like Ethernet. This mode waits for the medium to be idle, then transmits data. P-persistent is used in CSMA/CA (collision avoidance) systems, like Wi-Fi. This mode waits for the medium to be idle, then transmits data with a probability p. If the data node does not transmit the data (probability 1-p), the sender waits for the medium to be idle again. Then, it and transmits the data with the same probability p. O-persistent is used by CobraNet, LonWorks, and the controller area network. This mode assigns a transmission order to each data node. When the medium becomes idle, the data node next in line can transmit data. The data node next in line waits for the medium to be idle again and then transmits its data. After each data node transmits data, the transmission order is updated to reflect what data nodes have already transmitted, moving each data node through the queue.

What Is Fibre Channel?

Fibre Channel technology is used with server storage networks. Fibre Channel is a high-speed network technology used to connect servers to data storage area networks. Fibre Channel technology handles high-performance disk storage for applications on many corporate networks, and it supports data backups, clustering, and replication.

Fibre Channel technology supports both fiber and copper cabling, but copper limits Fibre Channel to a maximum recommended reach of 100 feet, whereas more expensive fiber optic cables reach up to 6 miles. The technology was specifically named Fibre Channel rather than Fiber Channel to distinguish it as supporting both fiber and copper cabling.

Fibre Channel Speed and Performance

The original version of Fibre Channel operated at a maximum data rate of 1 Gbps. Newer versions of the standard increased this rate up to 128 Gbps, with 8, 16, and 32 Gbps versions also in use.

Fibre Channel does not follow the typical OSI model layering. It is split into five layers:

FC-4 – Protocol-mapping layer

FC-3 – Common services layer

FC-2 – Signalling Protocol

FC-1 – Transmission Protocol

FC-0 – PHY connections and cabling

Fibre Channel networks have a historical reputation for being expensive to build, difficult to manage, and inflexible to upgrade due to incompatibilities between vendor products. However, many storage area network solutions use Fibre Channel technology. Gigabit Ethernet has emerged, however, as a lower cost alternative for storage networks. Gigabit Ethernet can better take advantage of internet standards for network management like SNMP.

TCP/IP model

The TCP/IP model was developed prior to the OSI model.

The TCP/IP model is not exactly similar to the OSI model.

The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Network Access Layer

A network layer is the lowest layer of the TCP/IP model.

A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

It defines how the data should be sent physically through the network.

This layer is mainly responsible for the transmission of the data between two devices on the same network.

The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

An internet layer is the second layer of the TCP/IP model.

An internet layer is also known as the network layer.

The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Internet Protocol

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since c. 2006.