Computer Networks

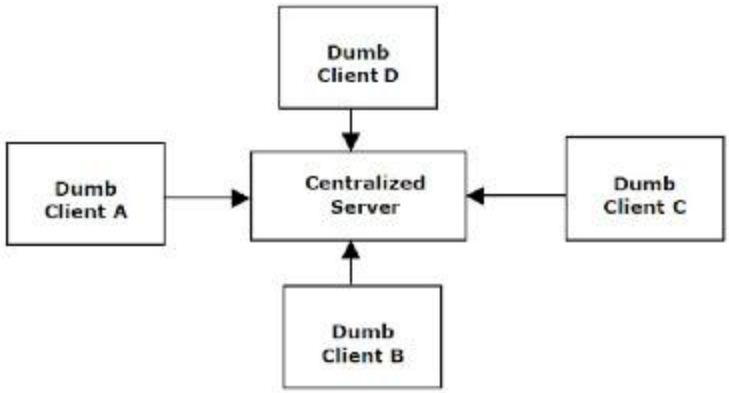
A computer network consists of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there. The most basic computer network (which consists of just two connected computers) can expand and become more usable when additional computers join and add their resources to those being shared. The first computer, yours, is commonly referred to as your local computer. It is more likely to be used as a location where you do work, a workstation, than as a storage or controlling location, a server. As more and more computers are connected to a network and share their resources, the network becomes a more powerful tool, because employees using a network with more information and more capability are able to accomplish more through those added computers or additional resources. The real power of networking computers becomes apparent if you envision your own network growing and then connecting it with other distinct networks, enabling communication and resource sharing across both networks. That is, one network can be connected to another network and become a more powerful tool because of the greater resources.

Models of network Computing

The three **models** for **network computing** are as follows: Centralized **computing**. Distributed **computing**. Collaborative or cooperative **computing**.

Centralized Network Computing Model

In the centralized network computing model, the clients use the resources of high-capacity servers to process information. In this model, the clients are also referred to as dumb terminals with very low or no processing capability. The clients only connect to the server and not to each other. The following figure shows the centralized network computing model:



Centralized Network Computing Model

Advantages

Some of the advantages of the centralized network computing model are:

- Centralized data management: In a centralized network computing model, data is stored on the server. This increases the reliability of data because all data modifications are stored at a central location.

- High level of security: The centralized network computing model is a highly secure network model. This is because network security can be implemented and monitored centrally from the server.
- Cost effectiveness: High-end investment is required for establishing a high-capacity and secure server. On the other hand, clients require very low investment. This reduces the overall cost of setting up a centralized network.

Limitations

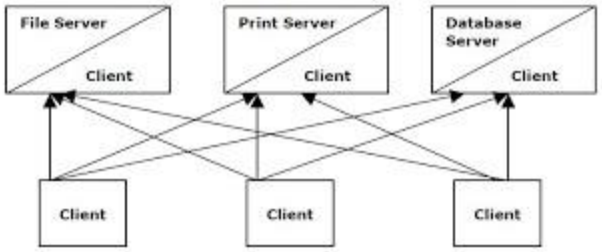
The centralized network computing model is a conventional model that is used only by a few network setups due to the following limitations:

- Low performance and network speed: The centralized network computing model consists of a server that manages numerous requests, simultaneously. This increases network traffic, consequently reducing the speed and performance of the network.
- Central point of failure: The server is the central place for storing data and processing all client requests. If the server fails, the functioning of the entire network is disrupted.

Distributed Network Computing Model

The distributed network computing model allows all network computers to take part in processing but at their respective ends, separately. This model allows sharing data and services but does not help the other network computers in processing.

In this network model, a processing-intensive task is broken into a subset of tasks and distributed among multiple nodes. The nodes work on their individual subsets of tasks. The following figure shows the distributed network computing model:



Distributed Network Computing Model

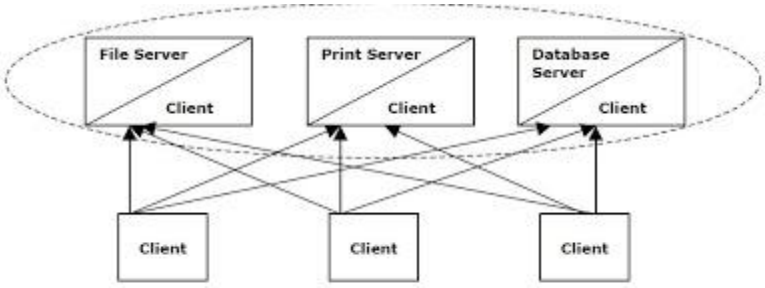
Advantages

Some of the advantages of the distributed network computing model are:

- Faster data access: The distributed network model allows a node to store the information locally. As a result, data can be accessed faster than in the centralized network model.
- High reliability: In the distributed network model, no single point of failure exists because the network does not entirely depend on a single node. This ensures lower network downtime.
- Customized network setup: The distributed network model offers the flexibility of treating different computers as clients and servers. It allows the optimized use of resources because the roles of the server and the client are interchangeable.

Collaborative Network Computing Model

The collaborative network computing model is an advanced distributed computing model. In this model, nodes also share processing capabilities apart from sharing data, resources, and other services. In other words, processes can run on two or more computers. The following figure shows the collaborative network computing model:



Collaborative Network Computing Model

Advantages

The advantage of the collaborative network computing model is: Increased processing speed: The nodes on the collaborative network share the task of processing the request. This reduces the processing time and increases the overall network performance.

Peer To Peer Network

Peer-to-peer (**P2P**) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

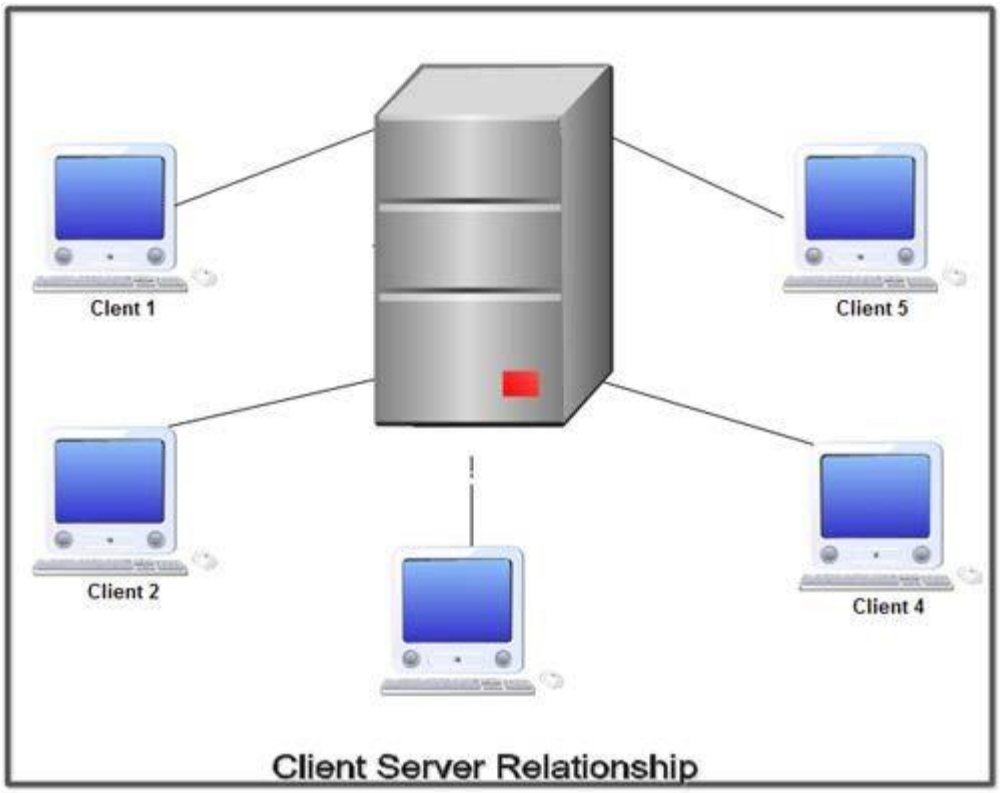
Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.[1] Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

Client Server Networking

A Computer networking model where one or more powerful computers (servers) provide the different computer network services and all other user'of computer network (clients) access those services to perform user's tasks is known as client/server computer networking model.
• In such networks, there exists a central controller called server. A server is a specialized computer that controls the network resources and provides services to other computers in the network.

• All other computers in the network are called clients. A client computer receives the requested services from a server.
• A server performs all the major operations like security and network management.
• All the clients communicate with each other via centralized server
• If client 1 wants to send data to client 2, it first sends request to server to seek permission for it. The server then sends a signal to client 1 allowing it to initiate the communication.
• A server is also responsible for managing all the network resources such as files, directories, applications & shared devices like printer etc.
• If any of the clients wants to access these services, it first seeks permission from the server by sending a request.
• Most Local Area Networks are based on client server relationship.

Client-server networking became popular in the late 1980s and early 1990s as many applications were migrated from centralized minicomputers and mainframes to computer networks of persona computers.



The design of applications for a distributed computing environment required that they effetely be divided into two parts: client (front end) and server (back end). The network model on which they were implemented mirrored this client-server model with a user's PC (the client) typically acting as the requesting machine and a more powerful server machine to which it was connected via either a LAN or a WAN acting as the supplying machine. It requires special networking operating system. It provides user level security and it is more expensive.

Advantages of Client Server Networks

1. Centralized back up is possible.

2. Use of dedicated server improves the performance of whole system.

3. Security is better in these networks as all the shared resources are centrally administered.

4. Use of dedicated servers also increases the speed of sharing resources.

Disadvantages of Client Server Networks

1. It requires specialized servers with large memory and secondary storage. This leads to increase in the cost.

2. The cost of network operating system that manages the various clients is also high.

3. It requires dedicated network administrator.

Switching

A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection in between pair of devices. But this increases the number of connection. The other solution could be to have a central device and connect every device to each other via the central device which is generally known as Star Topology. Both these methods are wasteful and impractical for very large network. The other topology also can not be used at this stage. Hence a better solution for this situation is SWITCHING. A switched network is made up of a series of interconnected nodes called switches.

Types of Switching Techniques

There are basically three types of switching methods are made available. Out of three methods, circuit switching and packet switching are commonly used but the message switching has been opposed out in the general communication procedure but is still used in the networking application.

1) CircuitSwitching
2) Packet Switching
3) Message Switching

Circuit Switching is generally used in the public networks. It come into existence for handling voice traffic in addition to digital data. How ever digital data handling by the use of circuit switching methods are proved to be inefficient. The network for Circuit Switching is shown in figure.

Circuit Switching Network

- Here the network connection allows the electrical current and the associated voice with it to flow in between the two respective users. The end to end communication was established during the duration of call.
- In circuit switching the routing decision is made when the path is set up across the given network. After the link has been sets in between the sender and the receiver then the information is forwarded continuously over the provided link.
- In Circuit Switching a dedicated link/path is established across the sender and the receiver which is maintained for the entire duration of conversation.

Packet Switching

In Packet Switching, messages are broken up into packets and each of which includes a header with source, destination and intermediate node address information. Individual Packets in packet switching technique take different routes to reach their respective destination. Independent routing of packets is done in this case for following reasons:

1. Bandwidth is reduces by the splitting of data onto different routes for a busy circuit.
2. For a certain link in the network, the link goes down during transmission the the remaining packet can be sent through the another route.

Packet Switching Network

- The major advantage of Packet switching is that they they are used for performing data rate conversion.
- When traversing the network switches, routers or the other network nodes then the packets are buffered in the queue, resulting in variable delay and throughput depending on the network's capacity and the traffic load on network.
- Packet switching contrasts with another principal networking paradigm, circuit switching, a method which sets up a limited number of dedicated connections of constant bit rate and constant delay between nodes for exclusive use during the communication session.
- In cases where traffic fees are charged, for example in cellular communication, packet switching is characterized by a fee per unit of information transmitted.

Message Switching

In case of Message Switching it is not necessary to established a dedicated path in between any two communication devices. Here each message is treated as an independent unit and includes its own destination source address by its own. Each complete message is then transmitted from one device to another through internetwork.

Message Switching Data Network

- Each intermediate device receive the message and store it until the nest device is ready to receive it and then this message is forwarded to the next device. For this reason a message switching network is sometimes called as Store and Forward Switching.
- Message switches can be programmed with the information about the most efficient route as well as information regarding to the near switches that can be used for forwarding the present message to their required destination.
- The storing and Forwarding introduces the concept of delay. For this reasons this switching is not recommended for real time applications like voice and video.

The 7 Layers of the OSI Model

The Open System Interconnection (OSI) model defines a networking framework to implement protocols in seven layers. Use this handy guide to compare the different layers of the OSI model and understand how they interact with each other.

The Open System Interconnection (OSI) model defines a networking framework to implement protocols in seven layers. There is really nothing to the OSI model. In fact, it's not even tangible. The OSI model doesn't perform any functions in the networking process. It is a conceptual framework so we can better understand complex interactions that are happening.

Who Developed the OSI Model?

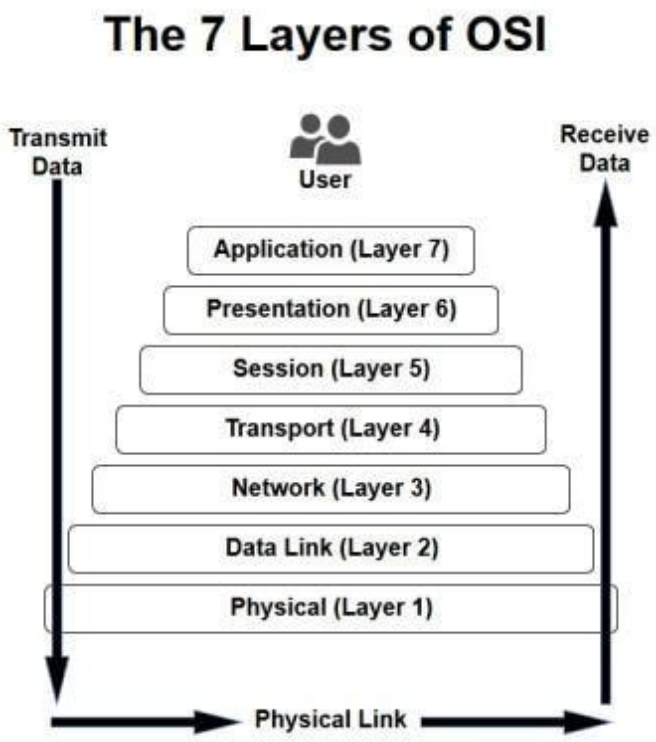
The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model. It divides network communication into seven layers. Layers 1-4 are considered the lower layers, and mostly concern themselves with moving data around. Layers 5-7, the upper layers, contain application-level data. Networks operate on one basic principle: "pass it on." Each layer takes care of a very specific job, and then passes the data onto the next layer.

The 7 Layers of the OSI

In the OSI model, control is passed from one layer to the next, starting at the application layer (Layer 7) in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model takes the task of inter-networking and divides that up into what is referred to as a vertical stack that consists of the following 7 layers.

Note: Click each hyperlink in the list below to read detailed information and examples of each layer or continue scrolling to read the full article:

- Layer 7 - Application
- Layer 6 - Presentation
- Layer 5 - Session
- Layer 4 - Transport
- Layer 3 - Network
- Layer 2 - Data Link
- Layer 1 - Physical



Application (Layer 7)

OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

Presentation (Layer 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

Session (Layer 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Layer 5 Session examples include NFS, NetBios names, RPC, SQL.

Transport (Layer 4)

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Layer 4 Transport examples include SPX, TCP, UDP.

Network (Layer 3)

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Layer 3 Network examples include AppleTalk DDP, IP, IPX.

Data Link (Layer 2)

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocolknowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control(LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Layer 2 Data Link examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

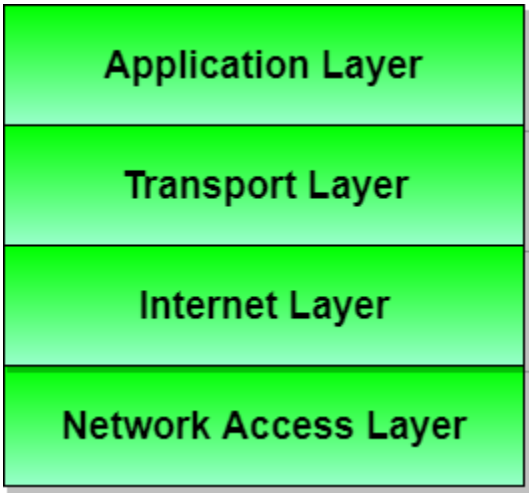
Physical (Layer 1)

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

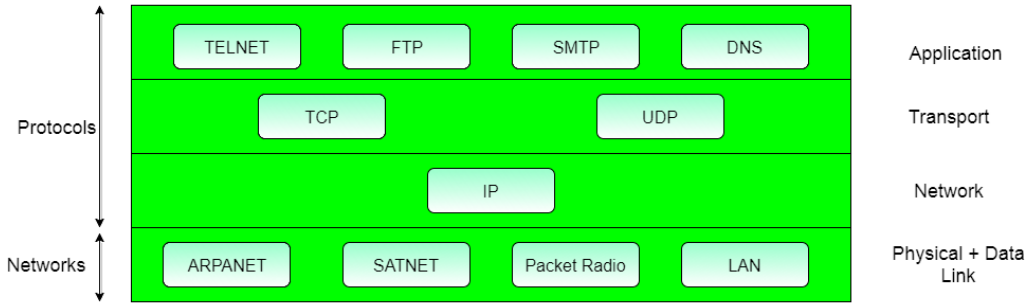
Layer 1 Physical examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.

2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
    - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.

- **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address.

Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon. 2 Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses. A source address is always a unicast address—the frame comes from only one station. The destination address,

however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of Logical Addresses

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address

Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks .So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may. The computer with logical address 3 A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F. Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2. Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

IP address

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995, and standardized in December 1998. In July 2017, a final definition of the protocol was published. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as *172.16.254.1* in IPv4, and *2001:db8:0:1234:0:567:8:1* in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., *192.168.1.15/24*, which is equivalent to the historically used subnet mask *255.255.255.0*.

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a *static* (fixed or permanent) or *dynamic* basis, depending on its software and practices.

Function

An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there." The header of each IP packet contains the IP address of the sending host, and that of the destination host.

IP versions

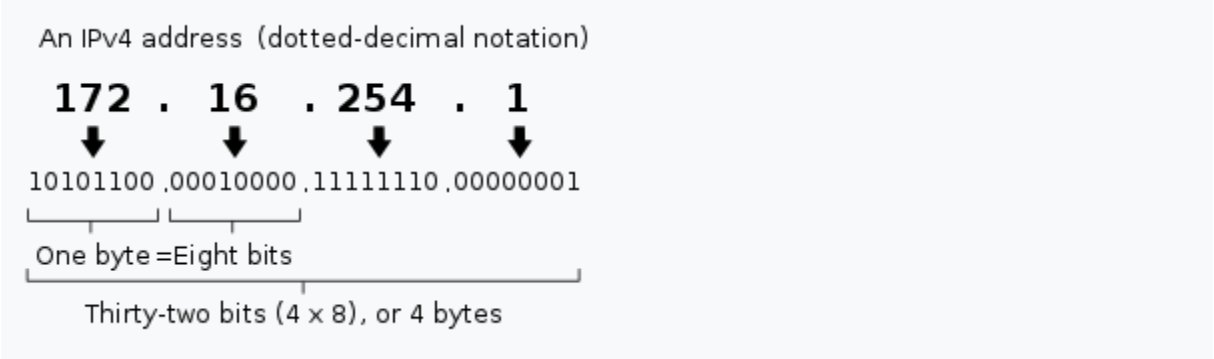
Two versions of the Internet Protocol are in common use in the Internet today. The original version of the Internet Protocol for use in the Internet is Internet Protocol version 4 (IPv4), first deployed in 1983.

The rapid exhaustion of IPv4 address space available for assignment to Internet service providers and end user organizations by the early 1990s, prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the addressing capability in the Internet. The result was a redesign of the Internet Protocol which became eventually known as Internet Protocol Version 6 (IPv6) in 1995. IPv6 technology was in various testing stages until the mid-2000s, when commercial production deployment commenced.

Today, these two versions of the Internet Protocol are in simultaneous use. Among other technical changes, each version defines the format of addresses differently. Because of the historical prevalence of IPv4, the generic term *IP address* typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4 and IPv6 resulted from the assignment of version 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

IPv4 addresses

Main article: IPv4 § Addressing



Decomposition of an IPv4 address from dot-decimal notation to its binary value.

An IPv4 address has a size of 32 bits, which limits the address space to 4294967296 (2^{32}) addresses. Of this number, some addresses are reserved for special purposes such as private networks (~18 million addresses) and multicast addressing (~270 million addresses).

IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., *172.16.254.1*. Each part represents a group of 8 bits (an octet) of the address. In some cases of technical writing,[IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

Subnetting

In the early stages of development of the Internet Protocol, network administrators interpreted an IP address in two parts: network number portion and host number portion. The highest order octet (most significant eight bits) in an address was designated as the *network number* and the remaining bits were called the *rest field* or *host identifier*, and were used for host numbering within a network.

This early method soon proved inadequate as additional networks developed that were independent of the existing networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.[1]

Classful network design allowed for a larger number of individual network assignments and fine-grained subnetwork design. The first three bits of the most significant octet of an IP address were defined as the *class* of the address. Three classes (*A*, *B*, and *C*) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (*B* and *C*). The following table gives an overview of this now obsolete system.

Historical classful network architecture

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	*0.0.0.0*	*127.255.255.255*
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	*128.0.0.0*	*191.255.255.255*
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	*192.0.0.0*	*223.255.255.255*

Classful network design served its purpose in the startup stage of the Internet, but it lacked scalability in the face of the rapid expansion of the network in the 1990s. The class system of the address space was replaced with Classless Inter-Domain Routing (CIDR) in 1993. CIDR is based on variable-length subnet masking (VLSM) to allow allocation and routing based on arbitrary-length prefixes.

Today, remnants of classful network concepts function only in a limited scope as the default configuration parameters of some network software and hardware components (e.g. netmask), and in the technical jargon used in network administrators' discussions.

Private addresses

Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be uniquely assigned to a particular computer or device. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the Internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Three non-overlapping ranges of IPv4 addresses for private networks are reserved.[6] These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry.

Today, when needed, such private networks typically connect to the Internet through network address translation (NAT).

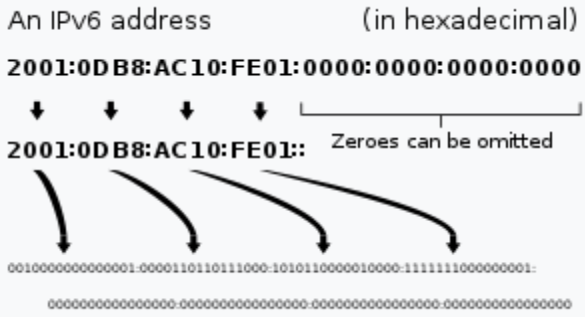
Reserved private IPv4 network ranges[6]

Start	End	Number of addresses
10.0.0.0	*10.255.255.255*	16777216
172.16.0.0	*172.31.255.255*	1048576
192.168.0.0	*192.168.255.255*	65536

Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of *192.168.0.0* through *192.168.0.255* (*192.168.0.0/24*).

IPv6 addresses

Main article: IPv6 address



Decomposition of an IPv6 address from hexadecimal representation to its binary value.

In IPv6, the address size was increased from 32 bits in IPv4 to 128 bits or 16 octets, thus providing up to 2^{128} (approximately 3.403×10^{38}) addresses. This is deemed sufficient for the foreseeable future.

The intent of the new design was not to provide just a sufficient quantity of addresses, but also redesign routing in the Internet by more efficient aggregation of subnetwork routing prefixes. This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 2^{64} hosts, which is the square of the size of the entire IPv4 Internet. At these levels, actual address utilization ratios will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a

network segment, i.e. the local administration of the segment's available space, from the addressing prefix used to route traffic to and from external networks. IPv6 has facilities that automatically change the routing prefix of entire networks, should the global connectivity or the routing policy change, without requiring internal redesign or manual renumbering.

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is no need to have complex address conservation methods as used in CIDR.

All modern desktop and enterprise server operating systems include native support for the IPv6 protocol, but it is not yet widely deployed in other devices, such as residential networking routers, voice over IP (VoIP) and multimedia equipment, and network peripherals.

Private addresses

Just as IPv4 reserves addresses for private networks, blocks of addresses are set aside in IPv6. In IPv6, these are referred to as unique local addresses (ULA). The routing prefix *fc00::/7* is reserved for this block,[7] which is divided into two */8* blocks with different implied policies. The addresses include a 40-bit pseudorandom number that minimizes the risk of address collisions if sites merge or packets are misrouted.

Early practices used a different block for this purpose (*fec0::*), dubbed site-local addresses.[8] However, the definition of what constituted *sites* remained unclear and the poorly defined addressing policy created ambiguities for routing. This address type was abandoned and must not be used in new systems.[9]

Addresses starting with fe80:, called link-local addresses, are assigned to interfaces for communication on the attached link. The addresses are automatically generated by the operating system for each network interface. This provides instant and automatic communication between all IPv6 host on a link. This feature is required in the lower layers of IPv6 network administration, such as for the Neighbor Discovery Protocol.

Private address prefixes may not be routed on the public Internet.

IP subnetworks

IP networks may be divided into subnetworks in both IPv4 and IPv6. For this purpose, an IP address is logically recognized as consisting of two parts: the *network prefix* and the *host identifier*, or *interface identifier* (IPv6). The subnet mask or the CIDR prefix determines how the IP address is divided into network and host parts.

The term *subnet mask* is only used within IPv4. Both IP versions however use the CIDR concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the *routing prefix*. For example, an IPv4 address and its subnet mask may be *192.0.2.1* and *255.255.255.0*, respectively. The CIDR notation for the same IP address and subnet is *192.0.2.1/24*, because the first 24 bits of the IP address indicate the network and subnet.

IP address assignment

IP addresses are assigned to a host either dynamically at the time of booting, or permanently by fixed configuration of the host hardware or software. Persistent configuration is also known as using a *static IP address*. In contrast, when a computer's IP address is assigned newly each time it restarts, this is known as using a *dynamic IP address*.

The configuration of a static IP address depends in detail on the software or hardware installed in the computer. Computers used for the network infrastructure, such as routers and mail servers, are typically configured with static addressing, Static addresses are also sometimes convenient for locating servers inside an enterprise.[*citation needed*]

Dynamic IP addresses are assigned using methods such as Zeroconf for self-configuration, or by the Dynamic Host Configuration Protocol (DHCP) from a network server. The address assigned with DHCP usually has an expiration period, after which the address may be assigned to another device, or to the originally associated host if it is still powered up. A network administrator may implement a DHCP method so that the same host always receives a specific address.

DHCP is the most frequently used technology for assigning addresses. It avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows devices to share the limited address space on a network if only some of them are online at a particular time. Typically, dynamic IP configuration is enabled by default in modern desktop operating systems. DHCP is not the only technology used

to assign IP addresses dynamically. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

In the absence or failure of static or stateful (DHCP) address configurations, an operating system may assign an IP address to a network interface using stateless auto-configuration methods, such as Zeroconf.

Sticky dynamic IP address

A *sticky dynamic IP address* is an informal term used by cable and DSL Internet access subscribers to describe a dynamically assigned IP address which seldom changes. The addresses are usually assigned with DHCP. Since the modems are usually powered on for extended periods of time, the address leases are usually set to long periods and simply renewed. If a modem is turned off and powered up again before the next expiration of the address lease, it often receives the same IP address.

Address autoconfiguration

Address block *169.254.0.0/16* is defined for the special use in link-local addressing for IPv4 networks. In IPv6, every interface, whether using static or dynamic address assignments, also receives a local-link address automatically in the block *fe80::/10*.

These addresses are only valid on the link, such as a local network segment or point-to-point connection, that a host is connected to. These addresses are not routable and like private addresses cannot be the source or destination of packets traversing the Internet.

When the link-local IPv4 address block was reserved, no standards existed for mechanisms of address autoconfiguration. Filling the void, Microsoft created an implementation that is called Automatic Private IP Addressing (APIPA). APIPA has been deployed on millions of machines and has, thus, become a de facto standard in the industry. Many years later, in May 2005, the IETF defined a formal standard for it.

Addressing conflicts

An IP address conflict occurs when two devices on the same local physical or wireless network claim to have the same IP address. A second assignment of an address generally stops the IP functionality of one or both of the devices. Many modern operating systems notify the administrator of IP address conflicts. If one of the devices is the gateway, the network will be crippled. When IP addresses are assigned by multiple people and systems with differing methods, any of them may be at fault.

Routing

IP addresses are classified into several classes of operational characteristics: unicast, multicast, anycast and broadcast addressing.

Unicast addressing

The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but a device or host may have more than one unicast address. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.

Broadcast addressing

In IPv4 it is possible to send data to all possible destinations ("all-hosts broadcast"), which permits the sender to send the data only once, and all receivers receive a copy of it. In the IPv4 protocol, the address *255.255.255.255* is used for local broadcast. In addition, a directed (limited) broadcast can be made by combining the network prefix with a host suffix composed entirely of binary 1s. For example, the destination address used for a directed broadcast to devices on the *192.0.2.0/2* network is *192.0.2.255*. IPv6 does not implement broadcast addressing and replaces it with multicast to the specially-defined all-nodes multicast address.

Multicast addressing

A multicast address is associated with a group of interested receivers. In IPv4, addresses *224.0.0.0* through *239.255.255.255* (the former Class D addresses) are designated as multicast addresses. IPv6 uses the address block with the prefix *ff00::/8* for multicast applications. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary

routers take care of making copies and sending them to all receivers that have joined the corresponding multicast group.

Anycast addressing

Like broadcast and multicast, anycast is a one-to-many routing topology. However, the data stream is not transmitted to all receivers, just the one which the router decides is logically closest in the network. Anycast address is an inherent feature of only IPv6. In IPv4, anycast addressing implementations typically operate using the shortest-path metric of BGP routing and do not take into account congestion or other attributes of the path. Anycast methods are useful for global load balancing and are commonly used in distributed DNSsystems.

What is an IP classless and classful network?

An IP is not classfull or classless but this term is applicable to networks and routing protocols.

Classful addressing: In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.Each of the IP address belongs to a particular class that's why they are classful addresses.Earlier this addressing system did not have any name,but when classless addressing system came into existence then it is named as Classful addressing system.The main disadvantage of classful addressing is that it limited the flexibility and number of addresses that can be assigned to any device.One of the major disadvantage of classful addressing is that it does not send subnet information but it will send the complete network address. The router will supply its own subnet mask based on its locally configured subnets. As long as you have the same subnet mask and the network is contiguous, you can use subnets of a classful network address.

Classless Addressing: Classless addressing system is also known as CIDR(Classless Inter-Domain Routing).Classless addressing is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes.What happened in classful addressing is that if any company needs more than 254 host machines but far fewer than the 65,533 host addresses then the only option for the company is to take the class B address.Now suppose company needs only 1000 IP addresses for its host computers then in this (65533-1000=64533) IP addresses get wasted.For this reason, the Internet was, until the arrival of CIDR, running out of address space much more quickly than necessary. CIDR effectively solved the problem by providing a new and more flexible way to specify network addresses in routers.A CIDR network address looks like this:

192.30.250.00/15

NAT (Network Address Translation)

Primarily NAT was introduced to the world of IT and networking due to the lack of IP addresses, or looking at it from another view, due to the vast amount of growing IT technology relying on IP addresses. To add to this, NAT adds a layer of security, by hiding computers, servers and other IT equipment from the outside world.

How NAT works

When computers and servers within a network communicate, they need to be identified to each other by a unique address, in which resulted in the creation of a 32 bit number, and the combinations of these 32 bits would accommodate for over 4 billion unique addresses, known as IP address. This was named IPv4, and although over 4 billion addresses sounds a lot, it really is not considering how fast the world of computers and the internet has grown.

To circumvent this problem, a temporary solution was produced known as NAT. NAT resulted in two types of IP addresses, public and private. A range of private addresses were introduced, which anyone could use, as long as these were kept private within the network and not routed on the internet. The range of private addresses known as RFC 1918 are;

Class A 10.0.0.0 - 10.255.255.255

Class B 172.16.0.0 - 172.31.255.255

Class C 192.168.0.0 - 192.168.255.255

NAT allows you to use these private IP address on the internal network. So within your private network you would assign a unique IP address to all your computers, servers and other IP driven resources, usually done via DHCP. Another company can use the same private IP addresses as well, as long as they are kept internal to their network. So two companies maybe using the same range of IP addresses but because they are private to their network, they are not conflicting with each other.

However when internal hosts do need to communicate to the public network (Internet) then this is where a public address comes into the equation. This address usually purchased from an ISP is a routable public address everyone can see, which would represent your network gateway. This public address would be unique, no one else would use this address.

Now getting to the point; When a host on the internal network with an internal IP address does need to communicate outside it's private network, it would use the public IP address on the network's gateway to identify itself to the rest of the world, and this translation of converting a private IP address to public is done by NAT. For example a computer on an internal address of 192.168.1.10 wanted to communicate with a web server somewhere on the internet, NAT would translate the address 192.168.1.10 to the company's public address, lets call this 1.1.1.1 for example. so that the internal address is identified as the public address when communicating with the outside world. This has to be done because when the web server somewhere on the internet was to reply to this internal computer, it needs to send this to a unique and routable address on the internet, the public address. It can not use the original address of 192.168.1.10, as this is private, none routable and hidden from the outside world. This address, of 1.1.1.1 would be the address of the public address for that company and can be seen by everyone. Now the web server would reply to that public address, 1.1.1.1. NAT would then use its records to translate the packets received from the web server that was destined to 1.1.1.1 back to the internal network address of 192.168.1.10, and though the computer who requested the original info, will receive the requested packets.

Now you can obviously see the two benefits of NAT. Firstly it would save on the IP addresses we use, as every single computer does not need a public address, and also it would hide these private computers from the outside world. Everyone can only see the public address, the rest is hidden behind this public address. So from the internet only the public address on the external interface of the firewall or router can be seen, and nothing beyond it.

Types of NAT

Three main types of NAT rules are used today depending on what needs to be accomplished;

Static NAT

A pool of public IP addresses are assigned to the NAT device. A private IP address can then be statically mapped to anyone of these public addresses. This type of NATTING scheme is usually used for servers requiring the same IP address always, hence the name "static", so server 1 will always have the same IP address assigned to it, server 2 will have a different public IP address assigned to it and so on.

Dynamic NAT

Again the NAT device will consist of a pool of IP addresses. This time though the pool of IP addresses will be used when needed and then given back to the pool. So if computer A needed a public address, it would take one from the pool, then hand it back when done. The next time the same computer wanted an IP address it may be assigned a different public address from the pool, because the one used previously may be in use by another computer, hence the name "dynamic". So users who want to communicate on the internet at any one time will be limited by how many public IP addresses are available in the NAT pool. A company would purchase a number of public IP's depending on their need.

Port Address Translation (PAT)

In this type of setup, a company would only have one public IP address assigned to their network, and so everyone would share this one public address when using the internet, browsing the web for example. Yes, you may be asking how can everyone share one address, well the clue lies within the name, Port address translation. When a computer wants to use the internet, the NAT device, using the PAT method will remember the IP address and source port of the internal host. For example 192.168.1.10 with a source port of 55331 wanted to browse Amazon.com. The NAT device will keep a note of this, and when Amazon replies to the public address and the port number of 55331, the NAT device will use the PAT method and look up the port information which maps to the internal computer requesting it. So it would be saying, this information Amazon has sent back to the public address and port number 55331, maps to the IP address 192.168.1.10 who originally requested it, though the information is for that computer. So the connections are uniquely identified by a source port, all using the same public IP but with unique source ports to identify who requested what information.

A company would save a reasonable amount of money and IP addresses using this method because it is only using one IP address. This has been a major factor to why IPv6 has been mentioned for some years now but still not required in most countries.

NAT is also implemented in home based routers and hardware firewalls such as the Netgear's and the Linksys of this world as well as the high end hardware firewalls such as the likes of Cisco and Juniper.

This has proved a valuable feature on hardware firewalls for saving public IP addresses and also a countermeasure for some types of attacks such as a reconnaissance attack.

Disadvantages of NAT

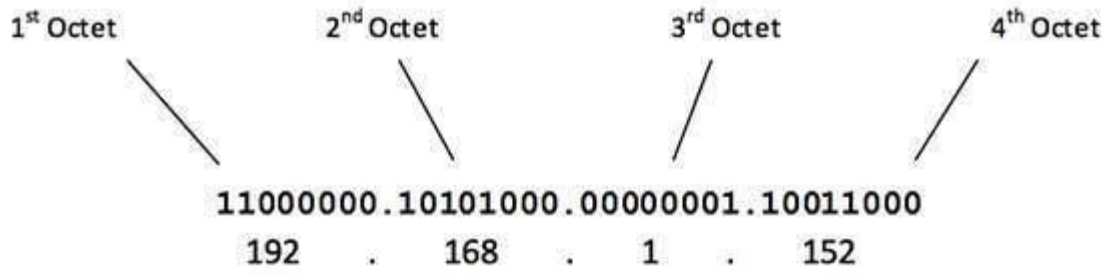
As with everything, NAT does have it's drawbacks. Some applications and services such as VPN and video conferencing struggle to process via NAT (Not entirely true as you can most of the time get them configured to work with NAT, but can get a little messy when setting rules up in applications,, routers and firewalls).

IPv4 - Address Classes

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

Number of networks = 2^network_bits

Number of Hosts/Network = 2^host_bits – 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

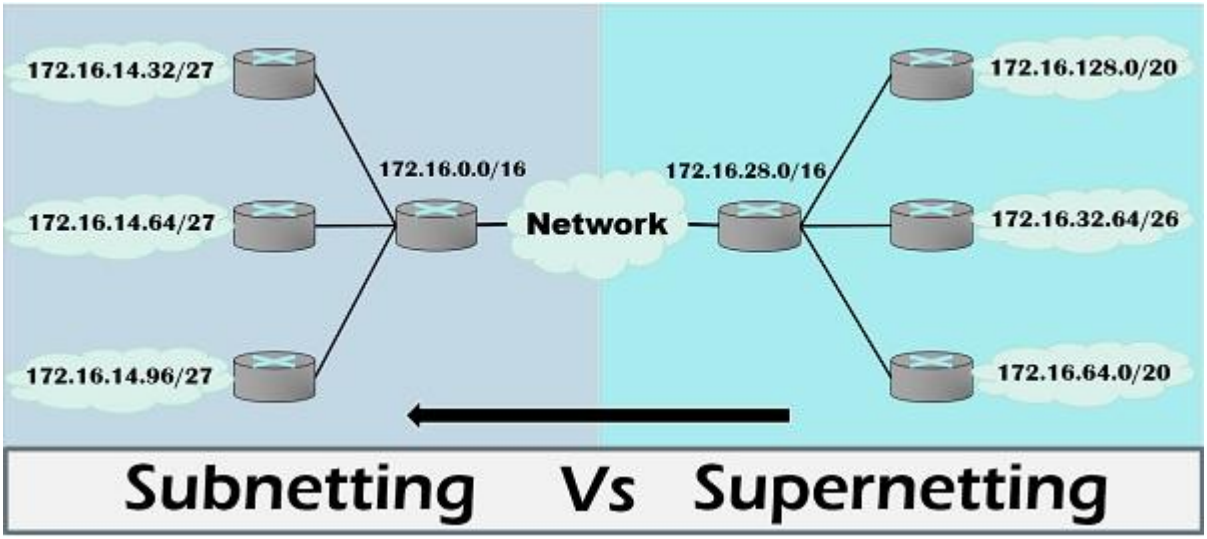
11100000 – 11101111
224 – 239

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Difference between Subnetting and Supernetting



Subnetting is the technique of partitioning a large network into smaller networks. On the other hand, the supernetting is the method used for combining the smaller ranges of addresses into larger space. Supernetting was devised to make the routing process more convenient. Additionally, it reduces the size of routing table information so that it could consume less space in the router's memory. The well-defined method for the subnetting is FLSM and VLSM while for supernetting CIDR is used.

Subnetting and supernetting are the techniques invented for resolving the problem of address depletion. Although, the techniques were not able to eliminate the problem, but certainly decreased the rate of address depletion. Supernetting is inverse process of subnetting.

Content: Subnetting Vs Supernetting

Comparison Chart

BASIS FOR COMPARISON	SUBNETTING	SUPERNETTING
Basic	A process of dividing a network into subnetworks.	A process of combining small networks into a larger network.
Procedure	The number of bits of network addresses is increased.	The number of bits of host addresses is increased.
Mask bits are moved towards	Right of the default mask.	Left of the default mask.
Implementation	VLSM (Variable-length subnet masking).	CIDR (Classless interdomain routing).
Purpose	Used to reduce the address depletion.	To simplify and fasten the routing process.

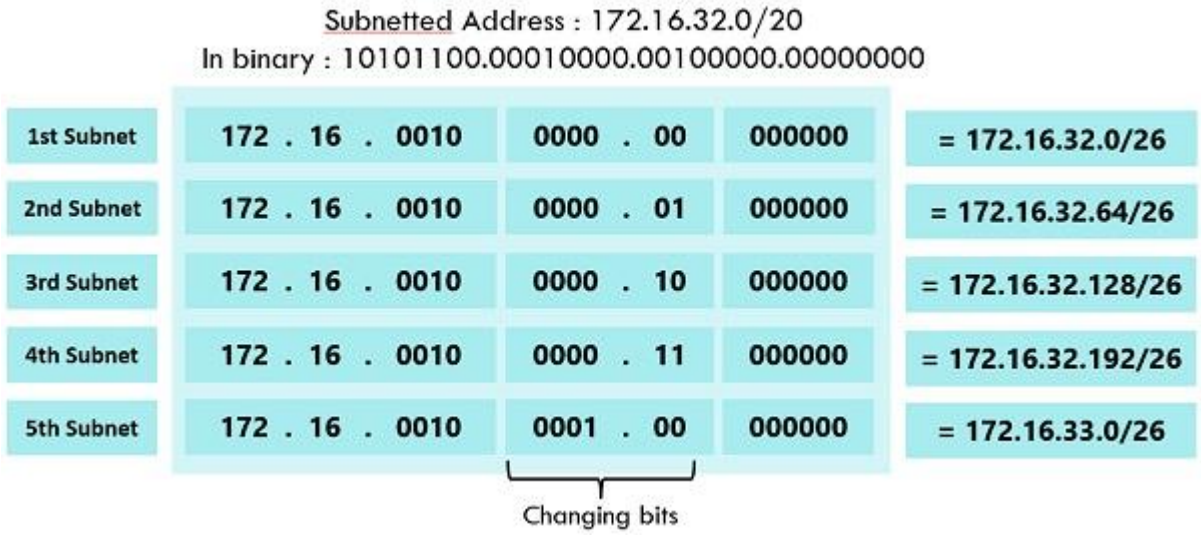
Definition of Subnetting

Subnetting is a technique of partitioning an individual physical network into several small-sized logical sub-networks. These subnetworks are known as **subnets**. An IP address is made up of the combination of the network segment and a host segment. A subnet is constructed by accepting the bits from the IP address host portion which are then used to assign a number of small-sized sub-networks in the original network.

The Subnetting basically convert the host bits into the network bits. As mentioned above the subnetting strategy was initially devised for slowing down the depletion of the IP addresses.

The subnetting permits the administrator to partition a single class A, class B, class C network into smaller parts. **VLSM (Variable Length Subnet Mask)** is a technique which partitions IP address space into subnets of different sizes and prevent memory wastage. Furthermore, when the number of hosts is same in subnets, that is

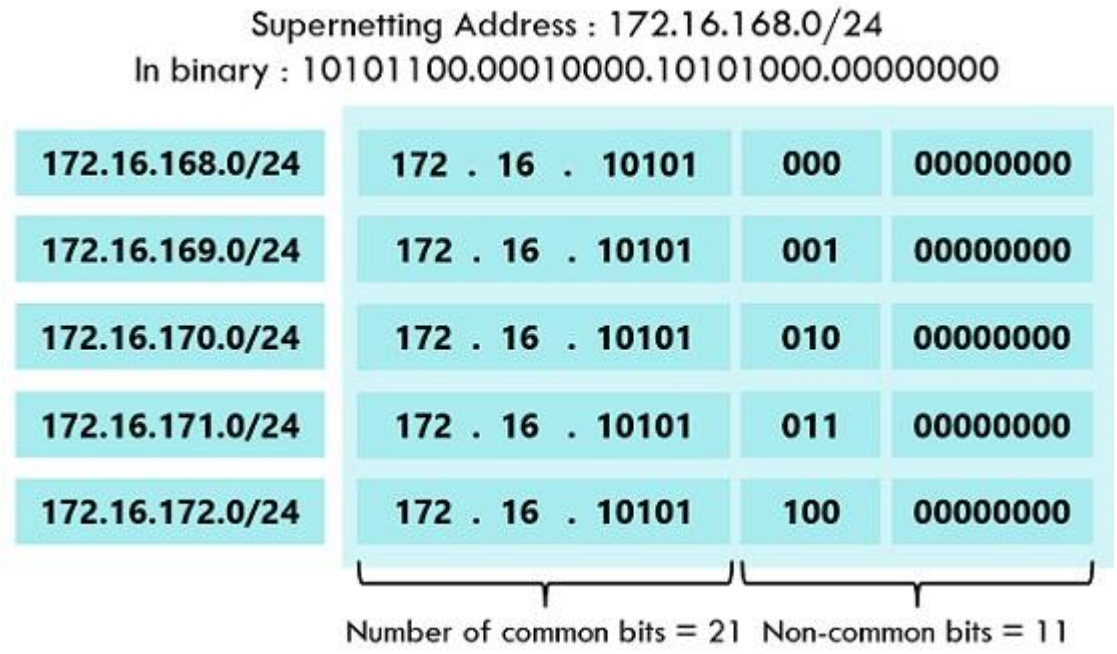
known as **FLSM (Fixed Length Subnet Mask)**.



Definition of Supernetting

Supernetting is inverse process of subnetting, in which several networks are merged into a single network. While performing supernetting, the mask bits are moved toward the left of the default mask. The supernetting is also known as **router summarization** and **aggregation**. It results in the creation of more host addresses at the expense of network addresses, where basically the network bits are converted into host bits.

The supernetting is performed by internet service provider rather than the normal users, to achieve the most efficient IP address allocation. **CIDR (Classless Inter-Domain Routing)** is scheme used to route the network traffic across the internet. CIDR is a supernetting technique where the several subnets are combined together for the network routing. In simpler words, CIDR allows the IP addresses to be organized in the subnetworks independent of the value of the addresses.



Key Differences Between Subnetting and Supernetting

1. The strategy used to divide a huge network into smaller subnetworks is known as subnetting. On the contrary, supernetting is the technique of merging multiple networks into a single one.

2. The subnetting process involves the increment of network part bits from the IP address. Conversely, in supernetting, the host part bits of the address are increased.
3. In order to perform subnetting the mask bits are repositioned towards the right of the default mask. As against, in supernetting, the mask bits are moved left of the default mask.
4. VLSM is a method of subnetting whereas CIDR is a supernetting technique.

Advantages of Subnetting

- Minimizes the network traffic through decreasing the volume of broadcasts.
- Increases addressing flexibility.
- Increases the number of allowed hosts in local area network.
- The network security can be readily employed between subnets rather than employing it in the whole network.
- Subnets are easy to maintain and manage.

Advantages of Supernetting

- The size of the router memory table is minimized by summarizing several routing information entries into a single entry.
- It also increases the speed of routing table lookup.
- Provision for the router to isolate the topology changes from the other routers.
- It also reduces the network traffic.

Disadvantages of Subnetting

- However, it is quite expensive.
- It requires trained administrator to perform subnetting.

Disadvantages of Supernetting

- The combination of blocks should be made in power 2; alternatively, if the three blocks are required, then there must be assigned four blocks.
- The whole network should exist in the same class.
- When merged, it lacks covering different areas.

Conclusion

Subnetting and supernetting both the terms have inverse meaning where subnetting is used to separate the smaller subnetworks form each other by dividing a larger network. Conversely, supernetting is used to combine the smaller range of addresses into a larger one to make routing process more easy and fast. Ultimately, both techniques are used to increase the availability of the IP addresses and reduce the depletion of IP addresses.

Loopback

loop-back, refers to the routing of electronic signals, digital data streams, or flows of items back to their source without intentional processing or modification. This is primarily a means of testing the transmission or transportation infrastructure.

Many example applications exist. It may be a communication channel with only one communication endpoint. Any message transmitted by such a channel is immediately and only received by that same channel. In telecommunications, loopback devices perform transmission tests of access lines from the serving switching center, which usually does not require the assistance of personnel at the served terminal. Loop around is a method of testing between stations that are not necessarily adjacent, wherein two lines are used, with the test being done at one station and the two lines are interconnected at the distant station. A patch cable may also function as loopback, when applied manually or automatically, remotely or locally, facilitating a loop-back test.

Where a system (such as a modem) involves round-trip analog-to-digital processing, a distinction is made between **analog loopback**, where the analog signal is looped back directly, and **digital loopback**, where the

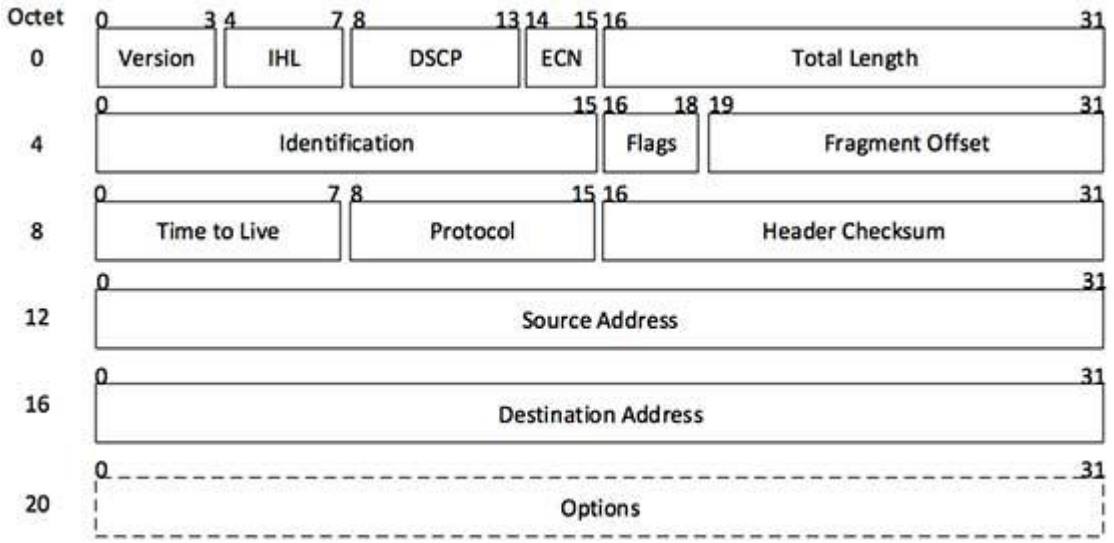
signal is processed in the digital domain before being re-converted to an analog signal and returned to the source.

IPv4 - Packet Structure

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

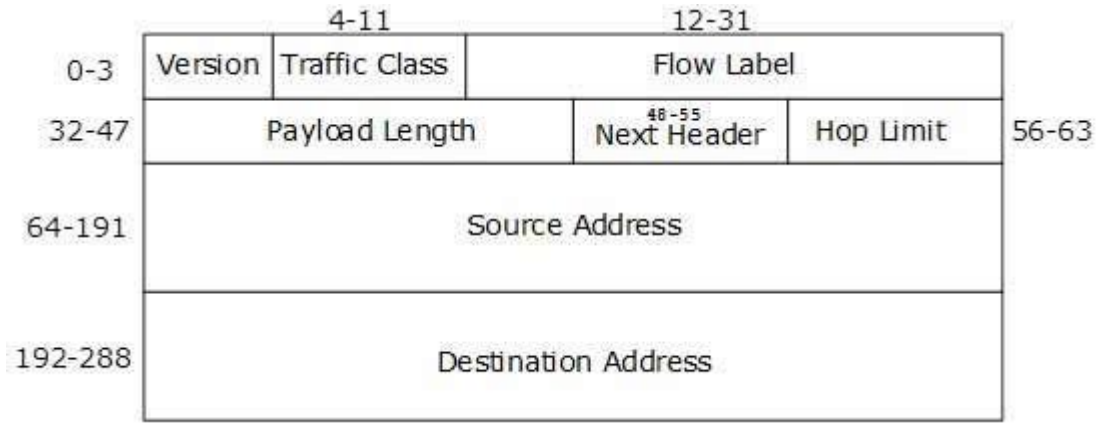
- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv6 - Headers

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

Fixed Header



[*Image: IPv6 Fixed Header*]

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.

2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Extension Headers

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.

If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.

The following Extension Headers must be supported as per RFC 2460:

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

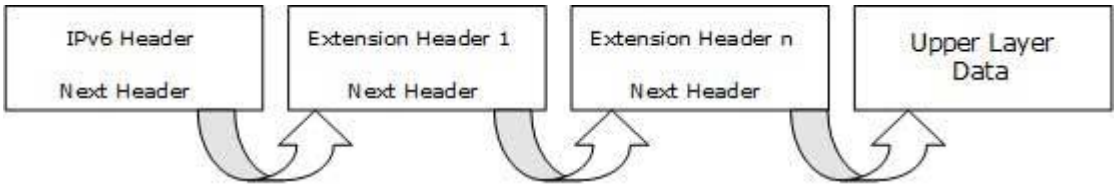
The sequence of Extension Headers should be:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

These headers:

- 1. should be processed by First and subsequent destinations.
- 2. should be processed by Final Destination.

Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:



Introduction to Ethernet

1. Introduction

Ethernet was originally developed by Digital, Intel and Xerox (DIX) in the early 1970's and has been designed as a 'broadcast' system, i.e. stations on the network can send messages whenever and wherever it wants. All

stations may receive the messages, however only the specific station to which the message is directed will respond.

The original format for Ethernet was developed in Xerox Palo Alto Research Centre (PARC), California in 1972. Using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) it had a transmission rate of 2.94Mb/s and could support 256 devices over cable stretching for 1km. The two inventors were Robert Metcalf and David Boggs.

Ethernet versions 1.0 and 2.0 followed until the IEEE 802.3 committee re-jigged the Ethernet II packet to form the Ethernet 802.3 packet. (IEEE's Project 802 was named after the time it was set up, February 1980. It includes 12 committees 802.1 to 802.12, 802.2 is the LLC, 802.4 Token Bus, 802.11 Wireless, 802.12 100VG-AnyLAN etc.) Nowadays you will see either Ethernet II (DIX) (invented by **D**igital, **I**ntel and **X**erox) format or Ethernet 802.3 format being used.

The 'Ether' part of Ethernet denotes that the system is not meant to be restricted for use on only one medium type, copper cables, fibre cables and even radio waves can be used.

802.3 Ethernet uses **Manchester Phase Encoding (MPE)** for coding the data bits on the outgoing signal. The next few sections describe how Ethernet works and how Ethernet is structured.

2. CSMA/CD

As mentioned earlier, Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD). When an Ethernet station is ready to transmit, it checks for the presence of a signal on the cable i.e. a voltage indicating that another station is transmitting. If no signal is present then the station begins transmission, however if a signal is already present then the station delays transmission until the cable is not in use. If two stations detect an idle cable and at the same time transmit data, then a collision occurs. On a star-wired UTP network, if the transceiver of the sending station detects activity on both its receive and transmit pairs before it has completed transmitting, then it decides that a collision has occurred. On a coaxial system, a collision is detected when the DC signal level on the cable is the same or greater than the combined signal level of the two transmitters, i.e.. significantly greater than +/- 0.85v. Line voltage drops dramatically if two stations transmit at the same and the first station to notice this sends a high voltage jamming signal around the network as a signal. The two stations involved with the collision lay off transmitting again for a time interval which is randomly selected. This is determined using **Binary Exponential Backoff**. If the collision occurs again then the time interval is doubled, if it happens more than 16 times then an error is reported.

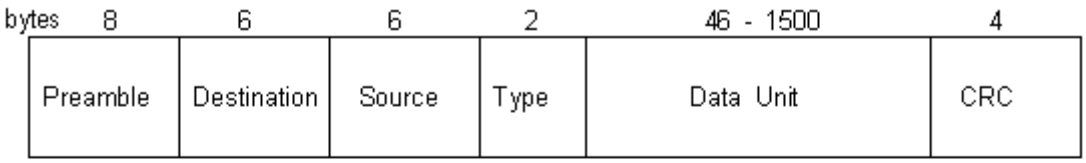
A **Collision Domain** is that part of the network where each station can 'see' other stations' traffic both unicast and broadcasts. The Collision Domain is made up of one segment of Ethernet coax (with or without repeaters) or a number of UTP shared hubs. A network is segmented with bridges (or microsegmented when using switches) that create two segments, or two Collision Domains where a station on one segment can not see traffic between stations on the other segment unless the packets are destined for itself. It can however still see all broadcasts as a segmented network, no matter the number of segments, is still one **Broadcast Domain**. Separate

Broadcast Domains are created by VLANs on switches so that one physical network can behave as a number of entirely separate LANs such that the only way to allow stations on different VLANs to communicate is at a layer 3 level using a router, just as if the networks were entirely physically separate.

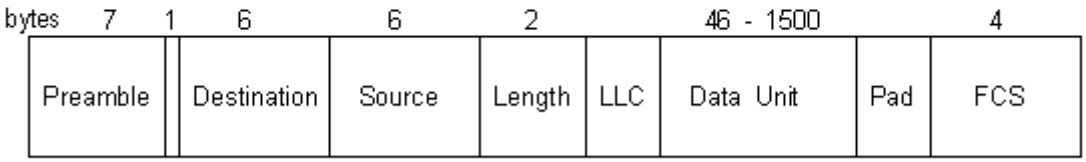
3. Ethernet Frame

3.1 Frame Formats

The diagrams below describe the structure of the older DIX (Ethernet II) and the now standard 802.3 Ethernet frames. The numbers above each field represent the number of bytes.



DIX Ethernet Packet



IEEE 802.3 Frame

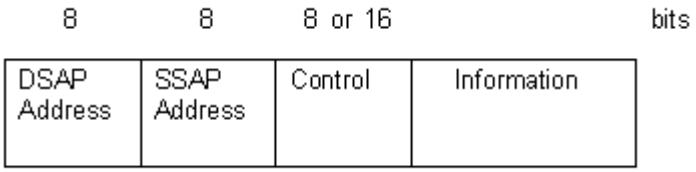
- **Preamble field:** Establishes bit synchronisation and transceiver conditions so that the PLS circuitry synchs in with the received frame timing. The DIX frame has 8 bytes for the preamble rather than 7, as it does not have a Start Frame Delimiter (or Start of Frame).
- **Start Frame Delimiter:** Sequence 10101011 in a separate field, only in the 802.3 frame.
- **Destination address:** Hardware address (MAC address) of the destination station (usually 48 bits i.e. 6 bytes).
- **Source address:** Hardware address of the source station (must be of the same length as the destination address, the 802.3 standard allows for 2 or 6 byte addresses, although 2 byte addresses are never used, N.B. Ethernet II can only uses 6 byte addresses).
- **Type:** Specifies the protocol sending the packet such as IP or IPX (only applies to DIX frame).
- **Length:** Specifies the length of the data segment, actually the number of LLC data bytes, (only applies to 802.3 frame and replaces the Type field).
- **Pad:** Zeros added to the data field to 'Pad out' a short data field to 46 bytes (only applies to 802.3 frame).
- **Data:** Actual data which is allowed anywhere between 46 to 1500 bytes within one frame.
- **CRC:** Cyclic Redundancy Check to detect errors that occur during transmission (DIX version of FCS).

- **FCS:** Frame Check Sequence to detect errors that occur during transmission (802.3 version of CRC). This 32 bit code has an algorithm applied to it which will give the same result as the other end of the link, provided that the frame was transmitted successfully.

From the above we can deduce that the maximum 802.3 frame size is 1518 bytes and the minimum size is 64 bytes. Packets that have correct CRC's (or FCS's) but are smaller than 64 bytes, are known as 'Runts'.

The hardware address, or MAC address is transmitted and stored in Ethernet network devices in **Canonical** format i.e. Least significant Bit (LSB) first. You may hear the expression **Little-Endian** to describe the LSB format in which Ethernet is transmitted. Token Ring and FDDI, on the other hand, transmit the MAC address with the Most Significant Bit (MSB) first, or **Big-Endian**, This is known as **Non-Canonical** format. Note that this applies on a byte by byte basis i.e. the bytes are transmitted in the same order it is just the bits in each of those bytes that are reversed! The storage of the MAC addresses in Token Ring and FDDI devices however, may sometimes still be in Canonical format so this can sometimes cause confusion. The reference to, the distribution of MAC addresses and the OUI desinations are always carried out in Canonical format.

Some discussion is warranted on the LLC field. The 802.2 committee developed the **Logical Link Control (LLC)** to operate with 802.3 Ethernet as seen in the above diagram. LLC is based on the **HDLC** format and more detail can be found by following the link. Whereas Ethernet II (2.0) combines the MAC and the Data link layers restricting itself to connectionless service in the process, IEEE 802.3 separates out the MAC and Data Link layers. 802.2 (LLC) is also required by Token Ring and FDDI but cannot be used with the Novell 'Raw' format. There are three types of LLC, Type 1 which is connectionless, Type 2 which is connection-oriented and Type 3 for Acknowledged Connections.



The **Service Access Point (SAP)** is used to distinguish between different data exchanges on the same end station and basically replaces the Type field for the older Ethernet II frame. The **Source Service Access Point (SSAP)** indicates the service from which the LLC data unit is sent, and the **Destination Service Access Point (DSAP)** indicates the service to which the LLC data unit is being sent. As examples, NetBIOS uses the SAP address of **F0** whilst IP uses the SAP address of **06**. The following lists common SAPs:

- **00** - Null LSAP
- **02** - Individual LLC Sublayer Management Function
- **03** - Group LLC Sublayer Management Function
- **04** - IBM SNA Path Control (individual)

- **05** - IBM SNA Path Control (group)
- **06** - ARPANET Internet Protocol (IP)
- **08** - SNA
- **0C** - SNA
- **0E** - PROWAY (IEC955) Network Management & Initialization
- **14** - ICL OSLAN SSAP (TP4 over 802.3)
- **18** - Texas Instruments
- **42** - IEEE 802.1 Bridge Spanning Tree Protocol
- **4E** - EIA RS-511 Manufacturing Message Service
- **54** - ICL OSLAN DSAP (TP4 over 802.3)
- **7E** - ISO 8208 (X.25 over IEEE 802.2 Type 2 LLC)
- **80** - Xerox Network Systems (XNS)
- **86** - Nestar
- **8E** - PROWAY (IEC 955) Active Station List Maintenance
- **98** - ARPANET Address Resolution Protocol (ARP)
- **BC** - Banyan VINES
- **AA** - SubNetwork Access Protocol (SNAP)
- **E0** - Novell NetWare
- **F0** - IBM NetBIOS
- **F4** - IBM LAN Management (individual)
- **F5** - IBM LAN Management (group)
- **F8** - IBM Remote Program Load (RPL)
- **FA** - Ungermann-Bass
- **FE** - ISO Network Layer Protocol
- **FF** - Global LSAP

The Control Field identifies the type of LLC, of which there are three:

- **Type 1** - uses **Unsequenced Information (UI)** (Indicated by a Control Field value of **03**) frames to set up unacknowledged connectionless sessions.
- **Type 2** - uses **Information (I)** frames and maintains the sequence numbers during an acknowledged connection-oriented transmission.
- **Type 3** - uses **Acknowledged Connection (AC)** frames in an acknowledged connectionless service.

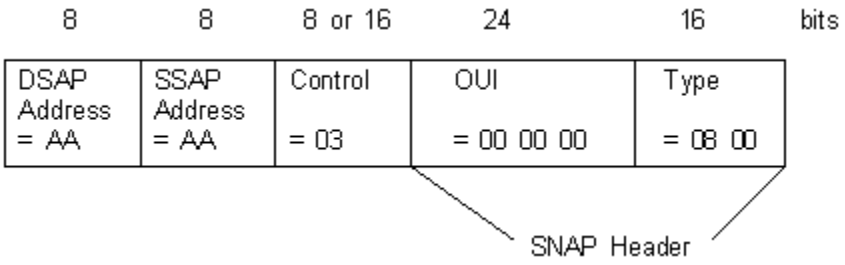
3.2 I/G and U/L within the MAC address

With an Ethernet MAC address, the first octet uses the lowest significant bit as the I/G bit (Individual/Group address) only and does not have such a thing as the U/L bit (Universally/Locally administered). The U/L bit is used in Token Ring A destination Ethernet MAC address starting with the octet '05' is a group or multicast address since the first bit (LSB) to be transmitted is on the right hand side of the octet and is a binary '1'. Conversely, '04' as the first octet indicates that the destination address is an individual address. Of course, in Ethernet, all source address will have a binary '0' since they are always individual.

The first 3 octets of the MAC address form the Organisational Unique Identifier (OUI) assigned to organisations that requires their own group of MAC addresses. A list of OUIs can be found at **OUI Index**.

3.3 Subnetwork Access Protocol (SNAP)

The SNAP protocol was introduced to allow an easy transition to the new LLC frame format for vendors. SNAP allows older frames and protocols to be encapsulated in a Type 1 LLC header so making any protocol 'pseudo-IEEE compliant'. SNAP is described in **RFC 1042**. The following diagram shows how it looks:



As you can see, it is an LLC data unit (sometimes called a **Logical Protocol Data Unit (LPDU)**) of Type 1 (indicated by 03). The DSAP and SSAP are set to **AA** to indicate that this is a SNAP header coming up. The SNAP header then indicates the vender via the **Organisational Unique Identifier (OUI)** and the protocol type via the Ethertype field. In the example above we have the OUI as 00-00-00 which means that there is an Ethernet frame, and the Ethertype of 08-00 which indicates IP as the protocol. The official list of types can be found at **Ethertypes**. More and more vendors are moving to LLC1 on the LAN but SNAP still remains and crops up time and time again.

Have a look at the document **IPX** for further discussion of 802.3 and 802.5 headers (SNAP etc.) in an IPX environment.

4. Media

4.1 10Base5

Traditionally, Ethernet is used over 'thick' coaxial cable (Normally yellow in colour) called 10Base5 (the '10' denotes 10Mbps, base means that the signal is baseband i.e. takes the whole bandwidth of the cable (so that only one device can transmit at one time on the same cable), and the '5' denotes 500m maximum length). The minimum length between stations is 2.5m.

The cable is run in one long length forming a 'Bus Topology'. Stations attach to it by way of inline N-type connections or a transceiver which is literally screwed into the cable (by way of a 'Vampire Tap') providing a 15-pin AUI (Attachment Unit Interface) connection (also known as a DIX connector or a DB-15 connector) for a drop lead connection (maximum of 50m length) to the station. The segments are terminated with 50 ohm resistors and the shield should be grounded at one end only.

5-4-3 Rule

The segment could be appended with up to a maximum of 4 repeaters, therefore 5 segments (total length of 2,460m) can be connected together. Of the 5 segments only 3 can have devices attached (100 per segment). A total of 300 devices can be attached on a Thicknet broadcast domain.

4.2 10Base2

It was common to see the Thick coax used in Risers to connect Repeaters which in turn provide 'Thin Ethernet' coaxial connections for runs around the floors to up to 30 workstations. Thin ethernet (Thinnet) uses RG-58 cable and is called 10Base2 (The '2' now denoting 200m maximum length, strictly speaking this is 185m). The minimum length between stations is 0.5m. Following is a table detailing various types of coaxial cable:

- RG-58 /U - solid copper core (0.66mm or 0.695mm), 53.5 ohms.
- RG-58 A/U - stranded copper core (0.66mm or 0.78mm), 50 ohms.
- RG-58 C/U - military version of RG58 A/U (0.66mm), 50 ohms.
- RG-59 - broadband transmissions e.g. cable TV.
- RG-6 - higher frequency broadband transmissions. A larger diameter than RG-59.
- RG-62 - ArcNet.
- RG-8 - Thicknet, 50 ohms.

Each station connects to the thinnet by way of a Network Interface Card (NIC) which provides a BNC (British Naval Connector). At each station the thinnet terminates at a T-piece and at each end of the thinnet run (or 'Segment') a 50-ohm terminator is required to absorb stray signals, thereby preventing signal bounce. The shield should be grounded at one end only.

A segment can be appended with other segments using up to 4 repeaters, i.e. 5 segments in total. 2 of these segments however, cannot be tapped, they can only be used for extending the length of the broadcast domain (to 925m). What this means is that 3 segments with a maximum of 30 stations on each can give you 90 devices on a Thinnet broadast domain.

(There is also a little used 10Broad36 standard where 10 Mbps Ethernet runs over broadband up to 3.6km. With broadband, a number of devices can transmit at the same time using multiple basebands e.g. multiple TV stations each with its own baseband signal frequency on one wire).

4.3 10BaseT

Nowadays, it is becoming increasingly important to use Ethernet across Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP), this being called 10BaseT (the 'T' denoting twisted pair). For instance, Category 5 UTP is installed in a 'Star-wired' format, with runs recommended at no greater than 100m (including patch

leads, cable run and flyleads) and Ethernet Hubs with UTP ports (RJ45) centrally located. It has been found though that runs of up to 150m are feasible, the limitations being signal strength. Also, there should be no more than a 11.5dB signal loss and the minimum distance between devices is 2.5m. The maximum delay for the signal in a 10Mbps network is 51.2 microseconds. This comes from the fact that the bit time (time to transmit one bit) is 0.1 microseconds and that the slot time for a frame is 512 bit times.

The wires used in the RJ45 are 1 and 2 for transmit, 3 and 6 for receive.

In order to connect to ethernet in this 'Star Topology', each station again has a NIC which, this time, contains an RJ45 socket which is used by a 4-pair RJ45 plug-ended droplead to connect to a nearby RJ45 floor or wall socket.

Each port on the hub sends a 'Link Beat Signal' which checks the integrity of the cable and devices attached, a flickering LED on the front of the port of the hub tells you that the link is running fine. The maximum number of hubs (or, more strictly speaking, repeater counts) that you can have in one segment is 4 and the maximum number of stations on one broadcast domain is 1024.

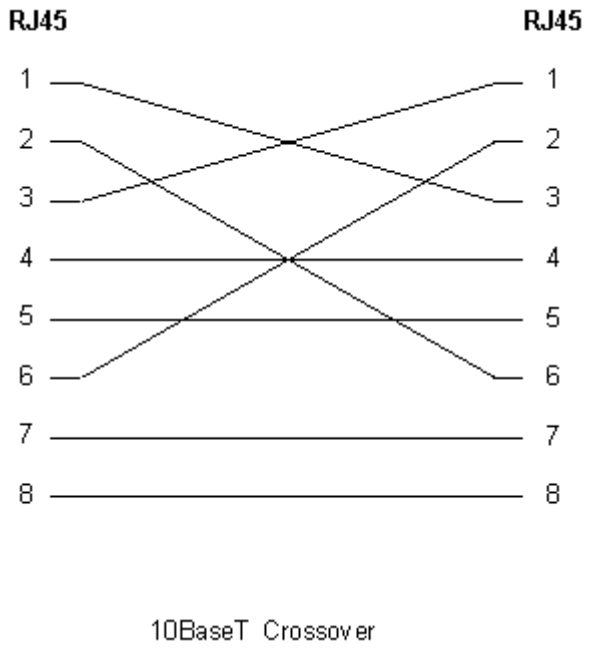
The advantages of the UTP/STP technology are gained from the flexibility of the system, with respect to moves, changes, fault finding, reliablity and security.

The following table shows the RJ45 pinouts for 10BaseT:

RJ45 Pin	**Function**	**Colour**
1	Transmit	White/Orange
2	Transmit	Orange/White
3	Receive	White/Green
4		Blue/White
5		White/Blue
6	Receive	Green/White
7		White/Brown

8		Brown/White

If you wish to connect hub to hub, or a NIC directly to another NIC, then the following 10BaseT cross-over cable should be used:



10BaseT Crossover

The 4 repeater limit manifests itself in 10/100BaseT environments where the active hub/switch port is in fact a repeater, hence the name multi-port repeater. Generally, the hub would only have one station per port but you can cascade hubs from one another up to the 4 repeater limit. The danger here of course, is that you will have all the traffic from a particular hub being fed into one port so care would need to be taken on noting the applications being used by the stations involved, and the likely bandwidth that the applications will use.

There is a semi-standard called Lattisnet (developed by Synoptics) which runs 10MHz Ethernet over twisted pair but instead of bit synchronisation occurring at the sending (as in 10BaseT) the synchronisation occurs at the receiving end.

4.4 10BaseF

The 10BaseF standard developed by the IEEE 802.3 committee defines the use of fibre for ethernet. 10BaseFB allows up to 2km per segment (on multi-mode fibre) and is designed for backbone applications such as cascading repeaters. 10BaseFL describes the standards for the fibre optic links between stations and repeaters, again allowing up to 2km per segment on multi-mode fibre. In addition, there is the 10BaseFP (Passive

components) standard and the FOIRL (Fibre Optic Inter-Repeater Link) which provides the specification for a fibre optic MAU (Media Attachment Unit) and other interconnecting components.

The 10BaseF standard allows for 1024 devices per network.

4.5 Fast Ethernet (802.3u) 100BaseTx

Fast Ethernet uses the same frame formats and CSMA/CD technology as normal 10Mbps Ethernet. The difference is that the maximum delay for the signal across the segment is now 5.12 microseconds instead of 51.2 microseconds. This comes from the fact that the bit time (time to transmit one bit) is 0.01 microseconds and that the slot time for a frame is 512 bit times. The Inter-Packet Gap (IPG) for 802.3u is 0.96 microseconds as opposed to 9.6 microseconds for 10Mbps Ethernet.

Fast Ethernet is the most popular of the newer standards and is an extension to 10BaseT, using CSMA/CD. The '100' denotes 100Mbps data speed and it uses the same two pairs as 10BaseT (1 and 2 for transmit, 3 and 6 for receive) and must only be used on Category 5 UTP cable installations with provision for it to be used on Type 1 STP. The Copper physical layer being based on the **Twisted Pair-Physical Medium Dependent (TP-PMD)** developed by ANSI X3T9.5 committee. The actual data throughput increases by between 3 to 4 times that of 10BaseT.

Whereas 10BaseT uses **Normal Link Pulses (NLP)** for testing the integrity of the connection, 100BaseT uses **Fast Link Pulses (FLP)** which are backwardly compatible with NLPs but contain more information. FLPs are used to detect the speed of the network (e.g. in 10/100 switchable cards and ports).

The ten-fold increase in speed is achieved by reducing the time it takes to transmit a bit to a tenth that of 10BaseT. The **slot-time** is the time it takes to transmit 512 bits on 10Mbps Ethernet (i.e. 5.12 microseconds) and listen for a collision (see earlier). This remains the same for 100BaseT, but the network distance between nodes, or span, is reduced. The encoding used is **4B/5B** with **MLT-3** wave shaping plus **FSR**. This wave-shaping takes the clock frequency of 125MHz and reduces it to 31.25MHz which is the frequency of the carrier on the wire.

The round trip signal timing is the critical factor when it comes to the distance that the signal can run on copper UTP. The cable has to be Category 5 and the distance must not exceed 100m.

The IEEE use the term **100BaseX** to refer to both 100BaseTx and 100BaseFx and the **Media-Independent Interface (MII)** allows a generic connector for transceivers to connect to 100BaseTx, 100BaseFx and 100BaseT4 LANs.

There is no such thing as the 5-4-3 rule in Fast Ethernet. All 10Base-T repeaters are considered to be functionally identical. Fast Ethernet repeaters are divided into two classes of repeater, **Class I** and **Class II**. A

Class I repeater has a repeater propagation delay value of 140 bit times, whilst a Class II repeater is 92 bit times. The Class I repeater (or **Translational Repeater**) can support different signalling types such as 100BaseTx and 100BaseT4. A Class I repeater transmits or repeats the incoming line signals on one port to the other ports by first translating them to digital signals and then retranslating them to line signals. The translations are necessary when connecting different physical media (media conforming to more than one physical layer specification) to the same collision domain. Any repeater with an MII port would be a Class I device. Only one Class I repeater can exist within a single collision domain, so this type of repeater cannot be cascaded. There is only allowed one Class I repeater hop in any one segment.

A Class II repeater immediately transmits or repeats the incoming line signals on one port to the other ports: it does not perform any translations. This repeater type connects identical media to the same collision domain (for example, TX to TX). At most, two Class II repeaters can exist within a single collision domain. The cable used to cascade the two devices is called and unpopulated segment or IRL (Inter-Repeater Link). The Class II repeater (or **Transparent Repeater**) can only support one type of physical signalling, however you can have two Class II repeater hops in any one segment (Collision Domain).

4.6 100BaseT4

100BaseT4 uses all four pairs and is designed to be used on Category 3 cable installations. Transmit is on pairs 1 and 2, receive is on pairs 3 and 6, whilst data is bidirectional on 4 and 5 and on 7 and 8. The signaling is on three pairs at 25MHz each using **8B/6T** encoding. The fourth pair is used for collision detection. Half-Duplex is supported on 100BaseT4.

4.7 100BaseFx

100BaseFx uses two cores of fibre (multi-mode 50/125um, 60/125um or single-mode) and 1300nm wavelength optics. The connectors are SC, Straight Tip (ST) or Media Independent Connector (MIC). The 100BaseT MAC mates with the ANSI X3T9.5 FDDI Physical Medium Dependent (PMD) specification. At half-duplex you can have distances up to 412m, whereas Full-duplex will give 2km.

There is also a proposed **100BaseSx** which uses 850nm wavelength optics giving 300m on multi-mode fibre.

The encoding used is **4B/5B** with **NRZ-I** wave shaping with a clock frequency of 125MHz.

4.8 100BaseT2

This little known version of Fast Ethernet is for use over two pairs of Category 3 cable and uses PAM-5 for encoding. There is simultaneous transmission and reception of data in both pairs and the electronics uses DSP technology to handle alien signals in adjacent pairs.

100BaseT2 can run up to 100m on Category 3 UTP.

4.9 100VG-AnyLAN

Based on 802.12 (Hewlett Packard), 100VG-AnyLAN uses an access method called **Demand Priority**. The 'VG' stands for 'Voice Grade' as it is designed to be used with Category 3 cable. This is where the repeaters (hubs) carry out continuous searches round all of the nodes for those that wish to send data. If two devices cause a 'contention' by wanting to send at the same time, the highest priority request is dealt with first, unless the priorities are the same, in which case both requests are dealt with at the same time (by alternating frames). The hub only knows about connected devices and other repeaters so communication is only directed at them rather than broadcast to every device in the broadcast domain (which could mean 100's of devices!). This is a more efficient use of the bandwidth. This is the reason why a new standard was developed called 802.12 as it is not strictly Ethernet. In fact 802.12 is designed to better support both Ethernet and Token Ring.

The encoding techniques used are **5B/6B** and **NRZ**.

All four pairs of UTP are used. On Cat3 the longest cable run is 100m but this increases to 200m on Cat5.

The clock rate on each wire is 30MHz, therefore 30Mbits per second are transmitted on each pair giving a total data rate of 120Mbits/sec. Since each 6-bits of data on the line represents 5 bits of real data due to the 5B/6B encoding, the rate of real data being transmitted is 25Mbits/sec on each pair, giving a total rate of real data of 100Mbits/sec. For 2-pair STP and fiber, the data rate is 120Mbits/sec on the transmitting pair, for a real data transmission rate of 100Mbits/sec.

4.10 Gigabit Ethernet

Although the functional principles of Gigabit Ethernet are the same as Ethernet and Fast Ethernet i.e. CSMA/CD and the Framing format, the physical outworking is very different. One difference is the slot time. The standard Ethernet slot time required in CSMA/CD half-duplex mode is not long enough for running over 100m of copper, so **Carrier Extension** is used to guarantee a 512-bit slot time.

1000BaseX (802.3z)

802.3z is the committee responsible for formalising the standard for **Gigabit Ethernet**. The 1000 refers to 1Gb/s data speed. The existing Fibre Channel interface standard (ANSI X3T11) is used and allows up to 4.268Gbps speeds. The Fibre Channel encoding scheme is **8B/10B**.

Gigabit Ethernet can operate in half or full duplex modes and there is also a standard 802.3x which manages XON/XOFF flow control in full duplex mode. With 802.3x, a receiving station can send a packet to a sending station to stop it sending data until a specified time interval has passed.

There are three media types for 1000BaseX. 1000BaseLX, 1000BaseSX and 1000BaseCX.

With 1000BaseSX, 'S' is for Short Haul, and this uses short-wavelength laser (850nm) over multi-mode fibre. 1000BaseSX can run up to 300m on 62.5/125um multimode fibre and up to 550m on 50/125um multimode fibre.

Using 1300nm wavelength, Gigabit Ethernet (1000BaseLX where the 'L' is for Long wavelength laser, or Long Haul) can run up to 550m on 62.5/125um multi-mode fibre or 50/125um multi-mode fibre. In addition, 1000BaseLX can run up to 5km (originally 3km) on single-mode fibre using 1310nm wavelength laser.

1000BaseCX is a standard for STP copper cable and allows Gigabit Ethernet to run up to 25m over STP cable.

There is currently an issue as many multimode fibre installations using 62.5/125um fibre and so 220m is often the limit for the backbone when it should be 500m to satisfy ISO 11801 and EIA/TIA 568A.

1000BaseT (802.3ab)

Many cable manufacturers are enhancing their cable systems to 'enhanced Category 5' standards in order to allow Gigabit Ethernet to run at up to 100m on copper. The Category 6 standard has yet to be ratified, and is not likely to be due for a while.

In order to obtain the 1000Mbps data bit rate across the UTP cable without breaking the FCC rules for emission, all 4 pairs of the cable are used. Hybrid circuits at each end of each pair are used to allow simultaneous transmission and reception of data (full-duplex) by separating the transmission signal from the receiving signal. Because some transmission signal still manages to couple itself to the receiving side there is an additional echo canceller built in, this is called a NEXT canceller. This system minimises the symbol rate.

Leased Line

A **leased line** is a private bidirectional or symmetric telecommunications circuit between two or more locations provided in exchange for a monthly rent. Sometimes known as a **private circuit** or **data line** in the UK.

Unlike traditional PSTN lines they do not have telephone numbers, each side of the line being permanently connected and dedicated to the other. Leased lines can be used for telephone, Internet, or other data services. Some are ringdown services, and some connect to a private branch exchange or router.

Typically, leased lines are used by businesses to connect geographically distant offices. Unlike dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection does not carry anybody else's communications, the carrier can assure a given level of quality.

An Internet leased line is a premium Internet connectivity product, normally delivered over fiber, which provides uncontended, symmetrical speeds with full duplex. It is also known as an ethernet leased line, dedicated line, data circuit or private line.

For example, a T1 can be leased and provides a maximum transmission speed of 1.544 Mbit/s. The user can channelize the T1 to separate the 24 DS0 circuits for voice communication, partial the T1 for data and voice communications, or multiplex the channels into a single data circuit. Leased lines, as opposed to DSL, are being used by companies and individuals for Internet access because they afford faster data transfer rates and are cost-effective for heavy users of the Internet.

ISDN

Integrated Services Digital Network (**ISDN**) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book.[1] Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. In some countries, ISDN found major market application for Internet access, in which ISDN typically provides a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In common use, ISDN is often limited to usage to Q.931 and related protocols, which are a set of signaling protocols establishing and breaking circuit-switched connections, and for advanced calling features for the user. They were introduced in 1986.[2]

In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

PSTN, ISDN, ADSL – What does it all mean?!

So you've just been told that the business is expanding and you need to look after the communication services at the new office. You immediately go into a panic as you don't know where to start, there are too many acronyms and the technical jargon is all too confusing!
Well, today you're in luck! I'm about to simplify some services to make your life a lot easier. Let's talk about the most common services in communications; PSTN, ISDN and ADSL.

PSTN or *Public Switched Telephone Network* is simply or most commonly known as a 'telephone line'. This is the most commonly used method by all users that only have the need to use one line for one conversation at a time using only one phone number. PSTN uses an old technology whereby circuit-switched copper phone lines are used to transmit analogue voice data. It is the basic service that you have at home and in a small business. As a dedicated service, a PSTN line cannot be used for any other purpose while a call is being made. A PSTN phone number is equivalent to one phone line.

ISDN or *Integrated Services Digital Network* provides digital transmission of voice and data services. Although now it is primarily used for Voice as it give you the options of having more than one Channel (line). They come in many 'flavours'… 2, 10, 20 and 30 and you can also increase the number of Channels as your business

expands by multiple ISDNs to meet your requirements. Medium to large businesses prefer this product as it gives them the option of integrating it with their phone systems (PABX) and takes advantage of multiple features. Like using a 100 number range, groups, queues, on hold music and RVAs, etc. When ISDN was launched it was able to simultaneously support early video conferencing systems and analogue phone lines. A few years ago ISDN was the fastest Internet speed available (128 kbps) but its popularity is rapidly declining due to the introduction of cloud communications.

ADSL or *Asymmetric Digital Subscriber line* or in other words 'the Internet'. Ok, not quite the Internet, but it is the means to connect to the Internet. This type of service is most commonly used by small businesses because it provides enough bandwidth for a small group of users to access the Internet. It works only over an existing PSTN, so you need to have an active PSTN to be able to have ADSL.

ISDN and PSTN days are numbered: what you should do

Does your business still use PSTN or ISDN for its phone system? With the progressive rollout of the NBN network, over the next 2 years or so PSTN and ISDN will be phased out. This means that PSTN and ISDN users will need to switch their phone systems to a VoIP (also known as voice over IP) based service.

If your business uses a traditional PBX the hardware will need to be replaced so its compatible with a cloud based phone solution or IP based voice services. But just replacing your PBX hardware may not be enough to keep your business efficient and competitive.

With communications technology rapidly changing everyday, it's crucial for business success that you understand the risks and costs of keeping your old PBX system. These include:

- Possible system outages and/or unplanned downtime that damages your business profitability and reputation
- A loss of ground to competitors who have future proof, seamless communication capabilities
- Expensive outlays to keep PBX server environments up to date

Still feel attached to your PBX system? Here are some scenarios that may make you think again!

When your business grows it can be challenging to easily scale your communications. From moving offices to launching new locations and hiring remote employees. If your current PBX business communications don't keep pace with your business growth, your business may be out of pocket with expensive, labour intensive 'solutions' of countless routers, wires and switches.

A state of the art cloud based communications system can give your business the flexibility and agility to respond to your communication requirements. From adding phone lines and locations, to disconnecting them when they're no longer needed. Our cloud system only needs an Internet connection.

And if your business needs hot desking, call monitoring, mobile collaboration and CRM integration an Arrow and 8×8 Business Phone system delivers. From a single application and workflow, your employees can easily locate, check, click to chat or call and/or click to collaborate. With minimal IT assistance required, a cloud communications system can easily deploy new features remotely and centrally via the Internet.

One of the main considerations for your choice of business communication needs to be the future growth of the business. It's also important to choose a solution that can easily adapt to a growing and perhaps increasingly remote workforce.

5 signs you need to update your business communication systems

If your current communication system isn't efficient or effective, you're not alone. A recent survey of IT decision makers found that

"only 1 in 4 organizations are highly satisfied with their current communications and collaboration solutions."

The survey also revealed that 71% of IT professionals face challenges with unified communications complexities. While they can step in to solve many of the problems, this can end up being costly and complicated. A unified communication solution *(the preference for 72% of IT professionals)* can provide your business with a single, unified platform for collaboration, voice and conferencing.

A more connected and productive workforce not only boosts morale and productivity for your business. Your customer service and ability to engage in real time can make your business stand apart from the competition. The common drivers for business to introduce unified communications include:

- Reduced costs
- Fast, easy to use communication platforms, systems and devices
- Increased productivity
- Improved internal and external collaboration
- Seamless support of mobile and remote employees

When your medium to large business is looking for cloud communications options, it's important that they provide unified communications, contact center capabilities, analytics and team collaboration in a single, open, real-time platform. The 8×8 Communications Cloudreduces communication costs, improves productivity and enhances customer experience. And with the ease of migration to 8×8, your IT professionals can get back to working on your core business.

Not sure if your business needs unified cloud communication? The following 5 signs indicate that your unified communication needs to be updated.

1. Your legacy PBX has disjointed, inefficient multi-vendor communications

Many medium to large businesses legacy communication systems have separate solutions from multiple vendors. Over time these disjointed capabilities can become costly and reduce the productivity of your organisation. When you switch to cloud communications these silos are eliminated and your communication capabilities integrate seamlessly.

2. Your business is expanding but your legacy PBX can't accommodate this growth

As your medium to large business grows, it's important that your communication system can adapt easily. Increasing the scale of services on your legacy PBX can be expensive and labor intensive. Cloud communications systems easily adapts to your business growth including opening up new offices locally or internationally to providing future proof communication solutions for remote and mobile employees.

3. Your legacy PBX is unable to support the communication features you need

If most of your employees are using a mobile device for work, your PBX may not be able to accommodate the ever-increasing needs of a mobile, wireless world. Switching to cloud communications will give your business the agility and mobility now and in the future with features including hot desking, call monitoring, CRM integrations and mobile collaboration.

4. You're unable to get the reporting and analysis your business needs

Does your PBX system give you the timely, relevant information your business needs to succeed? Using open technologies, cloud based communications can give your business the insights, reporting capabilities and analytics from all your communications.

5. If your business faced a disaster your communication system would fail

Does your PBX system give you the timely, relevant information your business needs to succeed? Using open technologies, cloud based communications can give your business the insights, reporting capabilities and analytics from all your communications.

In the event of a natural disaster, onsite PBX systems don't have the capability to provide continuous connectivity for your business. Unlike PBX, cloud communication systems have no single point of failure, ensuring your business stays connected no matter what happens.

How your business can benefit by using cloud communications

There is an alternative to trying to wrestle functionality out of your out-dated PBX. Cloud communications (also known as hosted voice over IP – VoIP) is a smarter business phone system with the features, mobility and reliability your business needs to stay competitive and be ready for anything.

The cloud based VoIP Arrow and 8×8 Business Phone system has capabilities that provide your business with a lot more than your traditional PBX system, at only a fraction of the cost. All your business needs for this future proof, easy to use communication system is a high speed Internet connection with a phone of your choice.

Benefits of the 8×8 communications solution include:

- Single interface for all communications: phone calls, chat, meetings, faxes and customer interactions
- Improved team collaboration
- Real time platform
- Contact centre capabilities
- Efficient collaboration

Combine these benefits with 8×8 disaster recovery capabilities and service reliability and it's easy to see why more medium to large businesses are converted from PSTN and ISDN to cloud communications. Need some help with your unified communications solution? Call Arrow Voice and Data today!

Very Small Aperture Terminal (VSAT)

Communication systems increasingly offer the possibility to communicate to somebody anywhere and anytime. In telephony, this becomes evident by the development of cellular telephone networks. Proposals, such as Iridium exist for a global network in which handheld telephones directly have access to low-Earth-orbit (LEO) satellites.

Satellite data communication systems show a similar development as telephone systems. The tendency here is towards smaller and transportable groundstations. This is shown by the popularity of the very small aperture terminals (VSATs) in the United States of America. VSATs are small satellite groundstations, normally linked within a VSAT network. The size of a VSAT is limited to a maximum antenna diameter of approximately 240 cm. VSATs are suitable for low rate data traffic (approximately 64 kbit/s).

VSAT Applications

Due to the small bit rate on the return link, the system is especially suitable for data collection applications. Suppose the system is divided into smaller subsystems, each with its own hub station. These subsystems could for example be used for national weather data collection. The complete system could also be used for international data collection. In principle, with three geostationary satellites, a global coverage is possible. In this way it is possible to collect (weather) data for, for example, global climate (change) research.

VSAT Network

VSAT networks consist of a number of terminals and a satellite through which the terminals communicate. Usually a bigger groundstation, often called a "hub station", is added for network control. If it is not possible to transfer messages directly from one VSAT to another, the hub can also be used as an intermediate station. VSAT networks have a number of advantages over traditional terrestrial networks. Among these advantages are that VSAT networks can easily cover a wide geographical area and that it is relatively easy to change the network configuration.

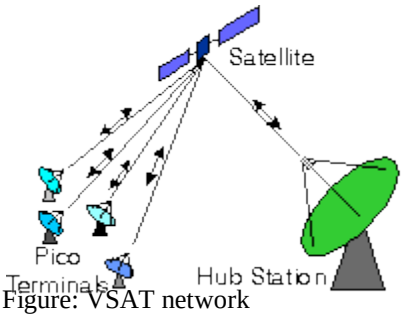


Figure: VSAT network

Through the development of powerful satellites operating in the 30/20 GHz frequency bands it is possible to further reduce the size of VSATs. Ultra-small fully portable satellite groundstations (picoterminals) with an antenna diameter of approximately 10-20 cm are possible in principle. However these terminals will have a very low data rate of a few kbit/s or even lower. So their primary purpose lies in telex-like message transfer, although technically it is possible to use them for coded speech transfer (for example 4.8 kbit/s).

Multiple Access

One satellite can simultaneously support thousands of picoterminal accesses. This means that the number of users in a picoterminal network can be a multiple of this, resulting in a communication network with an enormous size. To control such a number of terminals, the multiple access scheme for picoterminals may be a combination of frequency division multiple access (FDMA) and code division multiple access (CDMA). The CDMA spread-spectrum technique normally used for satellite communications is direct sequence spread spectrum.

The use of spread spectrum techniques in picoterminal networks has several advantages.

- It is advantageous as multiple access scheme, because (asynchronous) SSMA does not need network control and synchronisation.
- A second advantage is the inherent interference protection of the system. This is important for picoterminals which will be more or less sensitive to interference from unwanted directions due to their small antennas.
- A third advantage is that picoterminals can transmit with low power densities giving less interference problems.
- Finally SSMA gives some kind of message privacy through the encryption with a code word.

Picoterminal satellite communications network

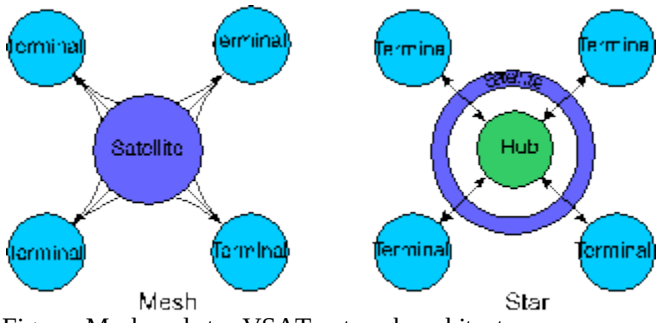


Figure: Mesh and star VSAT network architectures

Two basic architectures for a picoterminal satellite communications network exist. These are the full mesh architecture and the star architecture. In a full mesh architecture a terminal can directly communicate with another terminal via the satellite. In a star network communication between two picoterminals is via a larger hub station.

IPLC (international private leased circuit)

An IPLC (international private leased circuit) is a point-to-point private line used by an organization to communicate between offices that are geographically dispersed throughout the world. An IPLC can be used for Internet access, business data exchange, video conferencing, and any other form of telecommunication.

To simplify IPLC ordering and billing, a concept called One Stop Shopping (OSS) was developed. OSS allows an organization to place a single order with a single carrier for two private leased circuits for two offices in two different countries. In the past, an organization had to contact each carrier in each country to order the two circuits, which included two separate invoices. OSS consolidates the billing for both circuits into a single invoice, handles all currency issues, and allows the organization to report all problems from either circuit to one carrier.

NIC

NIC is short for *network interface card*. It's network adapter hardware in the form of an add-in card that fits in an expansion slot on a computer's motherboard. Most computers have them built-in (in which case they're just a part of the circuit board) but you can also add your own NIC to expand the functionality of the system.

The NIC is what provides the hardware interface between a computer and a network. This is true whether the network is wired or wireless since the NIC can be used for Ethernet networks as well as Wi-Fi ones, as well as whether it's a desktop or laptop.

"Network cards" that connect over USB are not actually cards but instead regular USB devices that enable network connections through the USB port. These are called network adapters.

Note: NIC also stands for Network Information Center. For example, the organization InterNIC is a NIC that provides information to the general public on internet domain names.

What Does a NIC Do?

Put simply, a network interface card enables a device to network with other devices. This is true whether the devices are connected to a central network (like in infrastructure mode) or even if they're paired together, directly from one device to the other (i.e. ad-hoc mode).

However, a NIC isn't always the only component needed to interface with other devices. For example, if the device is part of a larger network and you want it to have access to the internet, like at home or in a business, a router is required too. The device, then, uses the network interface card to connect to the router, which is connected to the internet.

NIC Physical Description

Network cards come in many different forms but the two main ones are wired and wireless.

Wireless NICs need to use wireless technologies to access the network, so they have one or more antennas sticking out of the card. You can see an example of this with the TP-Link PCI Express Adapter.

Wired NICs just use an RJ45 port since they have an Ethernet cable attached to the end. This makes them much flatter than wireless network cards. The TP-Link Gigabit Ethernet PCI Express Network Adapter is one example.

No matter which is used, the NIC protrudes from the back of the computer next to the other plugs, like for the monitor. If the NIC is plugged into a laptop, it's most likely attached to the side.

How Fast Are Network Cards?

All NICs feature a speed rating, such as 11 Mbps, 54 Mbps or 100 Mbps, that suggest the general performance of the unit. You can find this information in Windows by right-clicking the network connection from the **Network and Sharing Center > Change adapter settings** section of Control Panel.

It's important to keep in mind that the speed of the NIC does not necessarily determine the speed of the internet connection. This is due to reasons like available bandwidth and the speed you're paying for.

For example, if you're only paying for 20 Mbps download speeds, using a 100 Mbps NIC will not increase your speeds to 100 Mbps, or even to anything over 20 Mbps. However, if you're paying for 20 Mbps but your NIC only supports 11 Mbps, you will suffer from slower download speeds since the installed hardware can only work as fast as it's rated to work.

In other words, the speed of the network, when just these two factors are considered, is determined by the slower of the two.

Another major player in network speeds is bandwidth. If you're supposed to be getting 100 Mbps and your card supports it, but you have three computers on the network that are downloading simultaneously, that 100 Mbps will be split in three, which will really only serve each client around 33 Mbps.

Where to Buy Network Cards

There are many places where you can buy NICs, both in stores and online.

Some online retailers include Amazon and Newegg, but physical stores like Walmartsell network cards too.

How to Get Drivers for Network Cards

All hardware devices need device drivers in order to work with the software on the computer. If your network card isn't working, it's likely that the driver is missing, corrupted or outdated.

Updating network card drivers can be tricky since you usually need the internet in order to download the driver, but the driver issue is precisely what's preventing you from accessing the internet! In these cases, you should download the network driver on a computer that works and then transfer it to the problem system with a flash drive or CD.

The easiest way to do this is to use a driver updater tool that can scan for updates even when the computer is offline. Run the program on the PC that needs the driver and then save the information to a file. Open the file in the same driver updater program on a working computer, download the drivers and then transfer them to the non-working computer to update the drivers there.

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
  Passive Hub :- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges :-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges :-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

6. **Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

Network troubleshooting tools

Network troubleshooting tools are a necessity for every network administrator. When getting started in the networking field, it is important to amass a number of tools that can be used to troubleshoot a variety of different network conditions.

While it is true that the the use of specific tools can be subjective and at the discretion of the engineer, the selection of tools in this article has been made based on their generality and common use. This article reviews the top 10 basic tools that can help you troubleshoot most networking issues.

10. Ping

The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an Internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the Internet provider. Figure 1 below shows an example of the ping utility being used to obtain the reachability status of the locally connected

router.

9. Tracert/traceroute

Typically, once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts. Figure 2 below shows an example of the tracert utility being used to find the path from a host inside an office to www.google.com. The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux/*nix based machines.

8. Ipconfig/ifconfig

One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities that can be used to find out this IP configuration information include the ipconfig utility on Windows machines and the ifconfig utility on Linux/*nix based machines. Figure 3 below shows an example of the ifconfig utility showing the IP configuration information of a queries host.

7. Nslookup

Some of the most common networking issues revolve around issues with Dynamic Name System (DNS) address resolution issues. DNS is used by everyone using the Internet to resolve commonly known domain names (i.e. google.com) to commonly unknown IP addresses (i.e. 74.125.115.147). When this system does not work, most of the functionality that people are used to goes away, as there is no way to resolve this information. The nslookup utility can be used to lookup the specific IP address(es) associated with a domain name. If this utility is unable to resolve this information, there is a DNS issue. Along with simple lookup, the nslookup utility is able to query specific DNS servers to determine an issue with the default DNS servers configured on a host. Figure 4 below shows an example of how the nslookup utility can be used to query the associated IP address information.

6. Netstat

Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. Figure 5 below shows an example of the netstat utility being used to display the currently active ports on a Linux machine.

5. PuTTY/Tera Term

When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the puTTY and Tera Term programs are able to provide these functionalities. The selection of

one over the other is strictly a personal preference. Figures 6 and 7 below show both puTTY and Tera Term being used to connect to a host via SSH.

4. Subnet and IP Calculator

One of the most important tools in the belt of a junior network engineer is an IP network calculator. These can be used to unsure a correct IP address selection and with this a correct IP address configuration. While this type of tool is used by senior level network engineers, much of the information obtained from the tool becomes simpler to calculate the longer and more experience you have in the field. Two of the more commonly used free IP calculators include Wildpackets (Bitcricket) Network Calculator and Solarwinds Advanced Subnet Calculator which can be found at the links below.

3. Speedtest.net/pingtest.net

A very easy test that can be used to both determine the Internet bandwidth available to a specific host and to determine the quality of an Internet connection is the use of the tools available at the speedtest.net and pingtest.net websites. The speedtest.net site provides the ability to determine the amount of bandwidth that is available to a specific host at a specific point in time; this is often a good tool to use when measuring how long it is going to take to upload or download information from a local to remote host. This measurement can also be used to determine whether the connection is offering the amount of bandwidth that was purchased from the Internet provider; keep in mind however that some amount of bandwidth difference is expected between the quoted bandwidth purchased and the measured bandwidth. The pingtest.net website is used to determine the quality of the connection by measuring the ping response times and jitter amounts over a short period of time. This information can be used to determine a likelihood of how well the measured connection will deal with certain types of high demand traffic like Voice over IP (VoIP) or gaming. Figure 9 and 10 below show example output from both of these sites.

2. Pathping/mtr

In an effort to take advantage of the benefits of both the ping and tracert/traceroute commands, the pathping and mtr utilities were developed. Both of these tools take the functionality and information that can be obtained from these types of tools and provide a more detailed single picture of the path characteristics from a specific host to a specific destination. Figure 11 and 12 below show examples of these two tools and what information they provide.

1. Route

The last of the tools covered in this article is the route utility. This utility is used to display the current status of the routing table on a host. While the use of the route utility is limited in common situations where the host only has a single IP address with a single gateway, it is vital in other situations where multiple IP address and multiple gateways are available. Figure 13 below shows an example of the route utility being used on a Windows machine.

IEEE 802.11 Architecture

Each computer, mobile, portable or fixed, is referred to as a station in 802.11 [**Wireless Local Area Networks**].

The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement.

When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer. There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

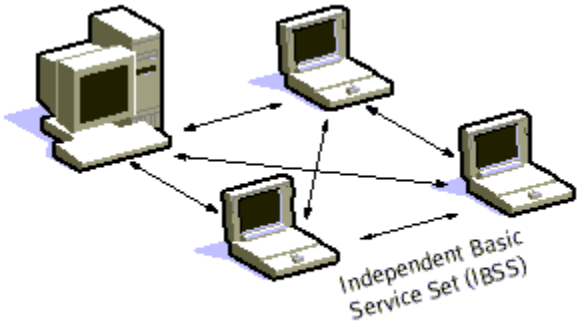


Fig 1: "Adhoc Mode"

When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS′s transparently to the LLC.

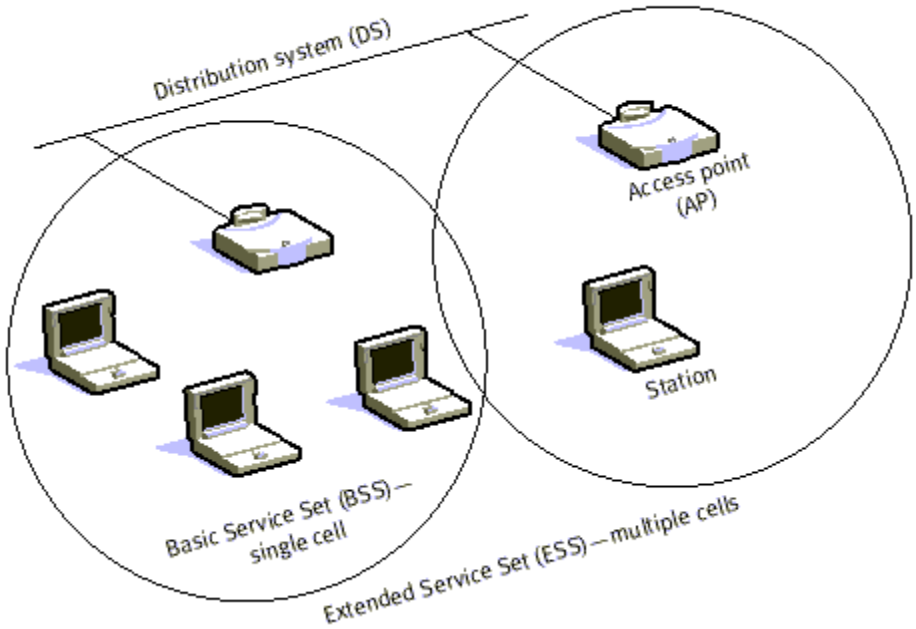


Fig 2: Infrastructure Mode

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.

The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.

While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections

1. Station Services (SS)
2. Distribution System Services (DSS).

There are five services provided by the DSS

1. Association
2. Reassociation
3. Disassociation
4. Distribution
5. Integration

The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition. A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by Associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP. This ensures that the DS always knows where the station is.

Association supports no-transition mobility but is not enough to support BSS-transition. Enter Reassociation. This service allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. ESS-transition are not supported. A station can move to a new ESS but will have to reinitiate connections.

Distribution and Integration are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

Station services are:

1. Authentication
2. Deauthentication
3. Privacy
4. MAC Service Data Unit (MSDU) Delivery.

With a wireless system, the medium is not exactly bounded as with a wired system. In order to control access to the network, stations must first establish their identity. This is much like trying to enter a radio net in the military.

Before you are acknowledged and allowed to converse, you must first pass a series of tests to ensure that you are who you say you are. That is really all authentication is. Once a station has been authenticated, it may then associate itself. The authentication relationship may be between two stations inside an IBSS or to the AP of the BSS. Authentication outside of the BSS does not take place.

There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second type is Shared

Key Authentication. In order to become authenticated the users must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all stations ahead of time in some secure method (such as someone walking around and loading the secret onto each station).

Deauthentication is when either the station or AP wishes to terminate a stations authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions, which are encrypted, are called ciphertext. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

The bottom line is this, authentication is basically a network wide password. Privacy is whether or not encryption is used. Wired Equivalent Privacy is used to protect authorized stations from eavesdroppers. WEP is reasonably strong. The algorithm can be broken in time. The relationship between breaking the algorithm is directly related to the length of time that a key is in use. So, WEP allows for changing of the key to prevent brute force attack of the algorithm. WEP can be implemented in hardware or in software. One reason that WEP is optional is because encryption may not be exported from the United States. This allows 802.11 to be a standard outside the U.S. albeit without the encryption.

Wireless Communication - Bluetooth

Bluetooth wireless technology is a short range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on **Ad-hoc technology** also known as **Ad-hoc Pico nets**, which is a local area network with a very limited coverage.

History of Bluetooth

WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs)**.

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.
- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.
- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.

Symbol of Bluetooth

An example of a Bluetooth device

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.
- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Piconets and Scatternets

Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as **Piconets**. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for **master** and **slave** to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a **PICONET**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the **master**.

The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme which is shown below.

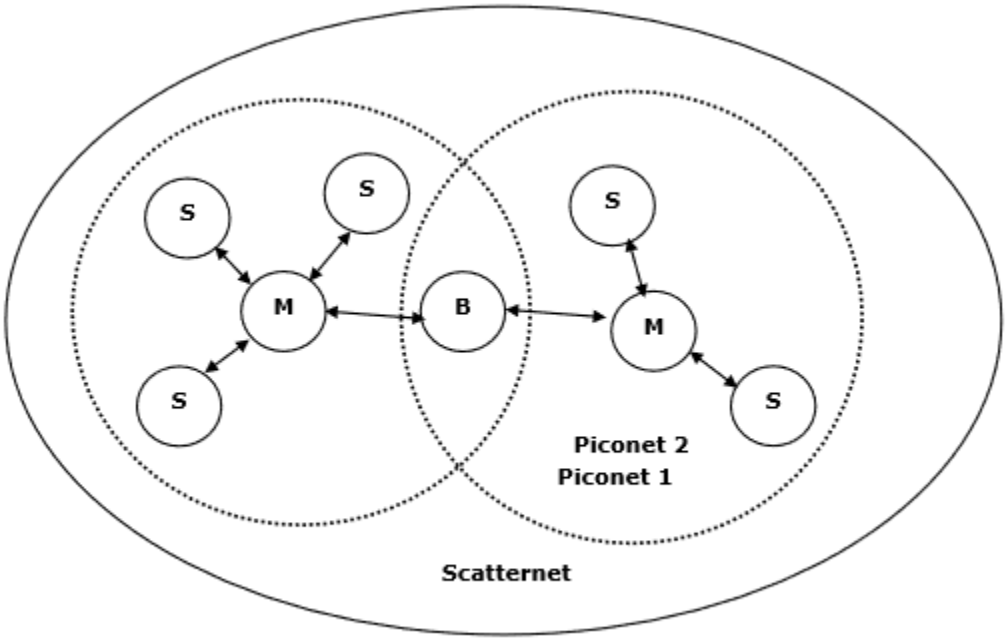


Figure: Piconets and Scatternets

The features of Piconets are as follows −

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique **48-bit address** of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.
- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as **Scatternet**.

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available and unlicensed in most countries.

Range

Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Data rate

Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.