Classless IP addressing / CIDR(Classless inter-domain routing)

Class C supports 254 hosts by default and class B 254*254 hosts but if we need 300 hosts in the network .neither class B or class C supports it. Because class C does not support required IPs and if we use class B , it will lead to great deal of IP addresses wastage.

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28.

Example : Given IP Address – 172.16.0.0/25, find the number of subnets and the number of hosts per subnet.
Solution : This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.
No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$

Rules For Creating CIDR Block-

A CIDR block is created based on the following 3 rules-

Rule-01:

- All the IP Addresses in the CIDR block must be contiguous.

Rule-02:

- The size of the block must be presentable as power of 2.
- Size of the block is the total number of IP Addresses contained in the block.
- Size of any CIDR block will always be in the form 2^1, 2^2, 2^3, 2^4, 2^5 and so on.

CIDR Notation-

CIDR IP Addresses look like-

a.b.c.d / n

- They end with a slash followed by a number called as IP network prefix.
- IP network prefix tells the number of bits used for the identification of network.
- Remaining bits are used for the identification of hosts in the network.

Example-

An example of CIDR IP Address is-

182.0.1.2 / 28

It suggests-

- 28 bits are used for the identification of network.
- Remaining 4 bits are used for the identification of hosts in the network.

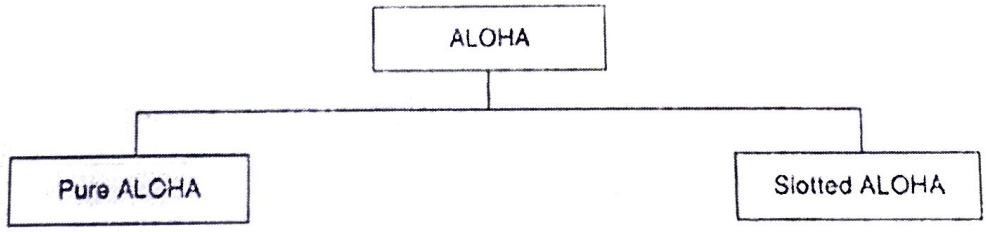
ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versior.s/types of ALOHA:

(i) Pure ALOHA
(ii) Slottecl ALOHA



Types of ALOHA

(i) Pure ALOHA

• **In** pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

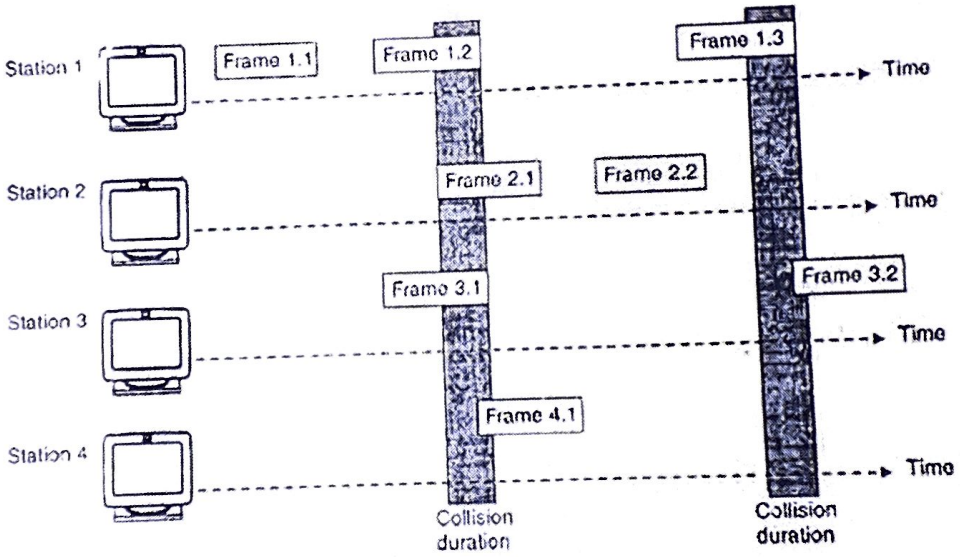
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



Frames in Pure ALOHA

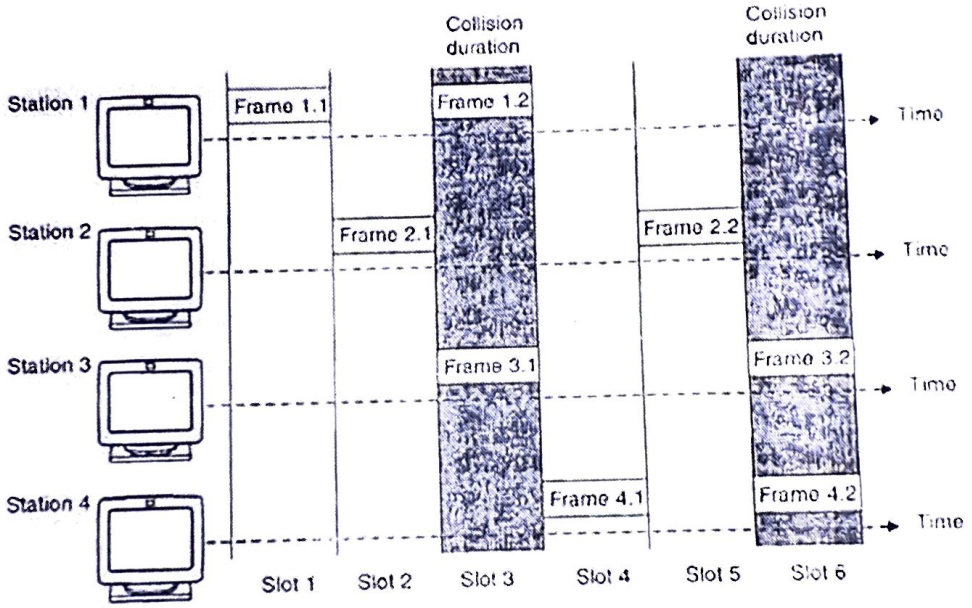
• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last

bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

(ii) Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.

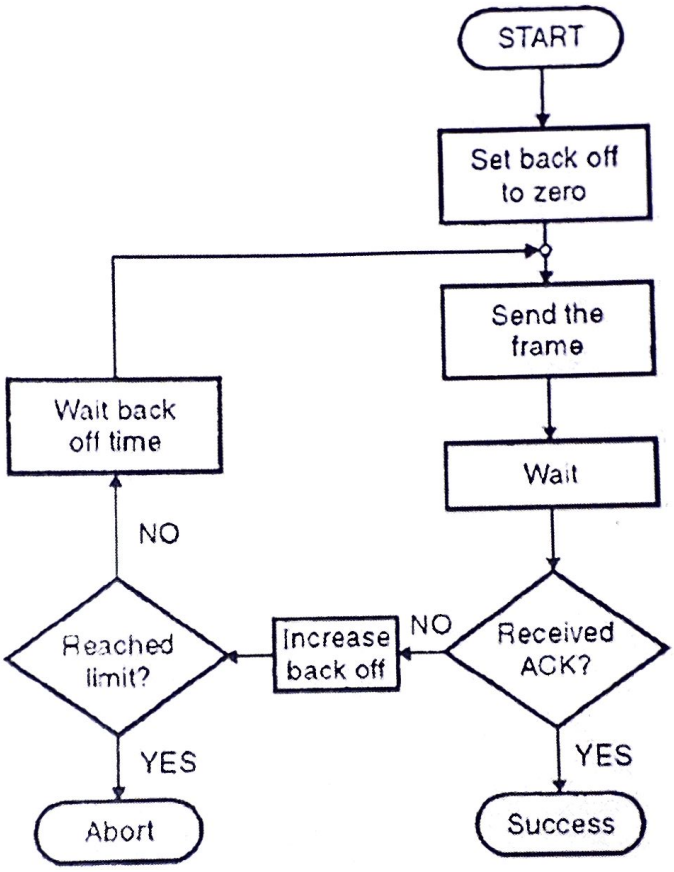


Frames in Slotted ALOHA

- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

Protocol Flow Chart for ALOHA:

Fig. shows the protocol flow chart for ALOHA.



Protocol flow chart for ALOHA

Explanation:

- A station which has a frame ready will send it.
- Then it waits for some time.
- If it receives the acknowledgement then the transmission is successful.

• Otherwise the station uses a backoff strategy, and sends the packet again.

• After many times if there is no acknowledgement then the station aborts the idea of transmission.

CSMA/CD used in ALOHA

(i) 1-persistent CSMA: In this case, a node having data to send, start sending, if the channel is sensed free. If the medium is busy, the node continues to monitor until the channel is idle. Then it starts sending data.

(ii) Non-persistent CSMA: If the channel is sensed free, the node starts sending the packet. Otherwise, the node waits for a random amount of time and then monitors the channel.

(iii) p-persistent CSMA: If the channel is free, a node starts sending the packet. Otherwise the node continues to monitor until the channel is free and then it sends with probability p.

Binary Back off Algorithm

Binary exponential backoff refers to a collision resolution mechanism used in random access MAC protocols. This algorithm is used in Ethernet (IEEE 802.3) wired LANs. In Ethernet networks, this algorithm is commonly used to schedule retransmissions after collisions.

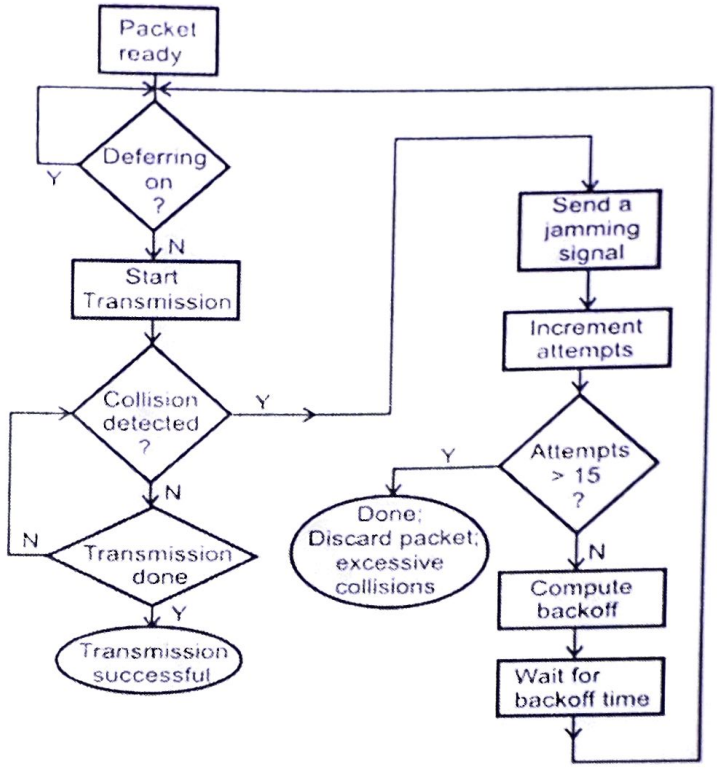


Figure 5.2.11 Binary exponential back off algorithm used in CSMA/CD

IPV6

Internet has been growing extremely fast so the IPv4 addresses are quickly approaching complete depletion. Moreover, many other devices than PC & laptop are requiring an IP address to go to the Internet. To solve these problems in long-term, a new version of the IP protocol – version 6 (IPv6) was created and developed.

IPv6 was created by the Internet Engineering Task Force (IETF), a standards body, as a replacement to IPv4 in 1998. So what happened with IPv5? IP Version 5 was defined for experimental reasons and never was deployed.

While IPv4 uses 32 bits to address the IP (provides approximately 2^{32} = 4,294,967,296 unique addresses – but in fact about 3.7 billion addresses are assignable because the IPv4 addressing system separates the addresses into classes and reserves addresses for multicasting, testing, and other specific uses), IPv6 uses up to 128 bits which provides 2^{128} addresses or approximately $3.4 * 10^{38}$ addresses. Well, maybe we should say it is extremely extremely extremely huge.

IPv6 address format

Format:

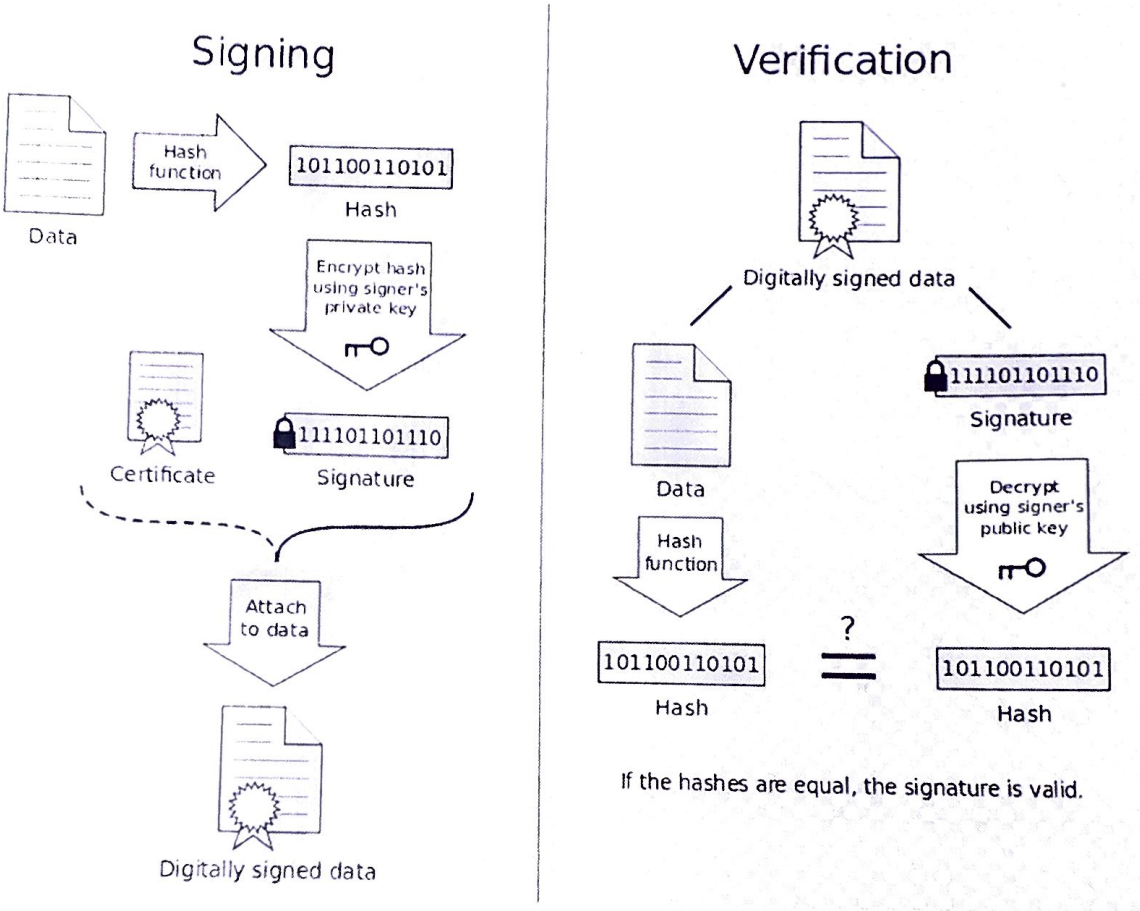
x:x:x:x:x:x:x:x – where **x** is a 16 bits hexadecimal field and **x** represents four hexadecimal digits.
An example of IPv6:
2001:0000:5723:0000:0000:D14E:DBCA:0764

There are:
+ 8 groups of 4 hexadecimal digits.
+ Each group represents 16 bits (4 hexa digits * 4 bit)
+ Separator is ":"
+ Hex digits are not case sensitive, so "**DBCA**" is same as "dbca" or "DBca"...

Content	IPv4	IPv6
Released	1981 (RFC 791)	1998 (RFC 2460)
Available address space	32-bit, 4.29 x 109 addresses	128-bit, 3.4 x 1038 addresses
Address format	Decimal: 192.168.1.1	Hexadecimal, 2a00:ad80::0123
Loopback address	127.0.0.1	::1
IPsec header	Optional	Always available
Fragmentation	Host and router	Only the communication endpoint
Checksum in the header	yes	no
Options in the header	yes	no
Link-layer address resolution	ARP (broadcast)	Multicast neighbor discovery messages
Router discovery	Optional	Mandatory
IP configuration	Manual, DHCP	Automatic, DHCPv6, manual

Digital Signatures

A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

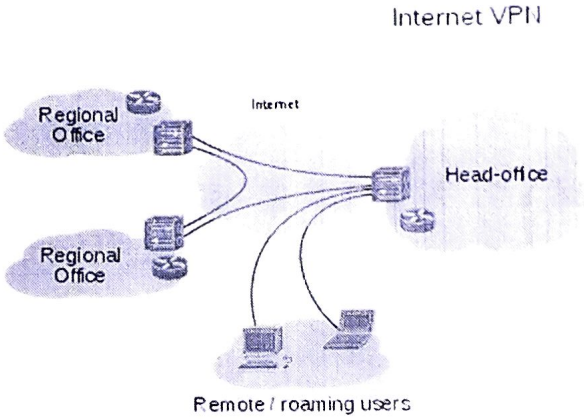


VPN

A **virtual private Network (VPN)** extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.[1] This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A virtual private network connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPNs allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPNs securely and cost-effectively connect geographically disparate offices of an organization, creating one cohesive virtual network.



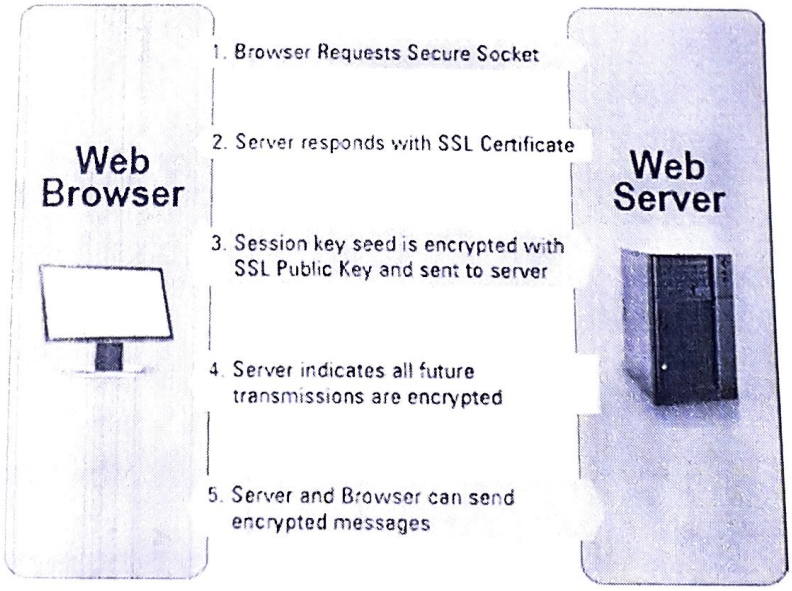
Differences between HTTP and HTTPs

HTTP	HTTPS
URL begins with "http://"	URL begins with "https://"
It uses port 80 for communication	It uses port 443 for communication
Unsecured	Secured
Operates at Application Layer	Operates at Transport Layer
No encryption	Encryption is present
No certificates required	Certificates required

SSL

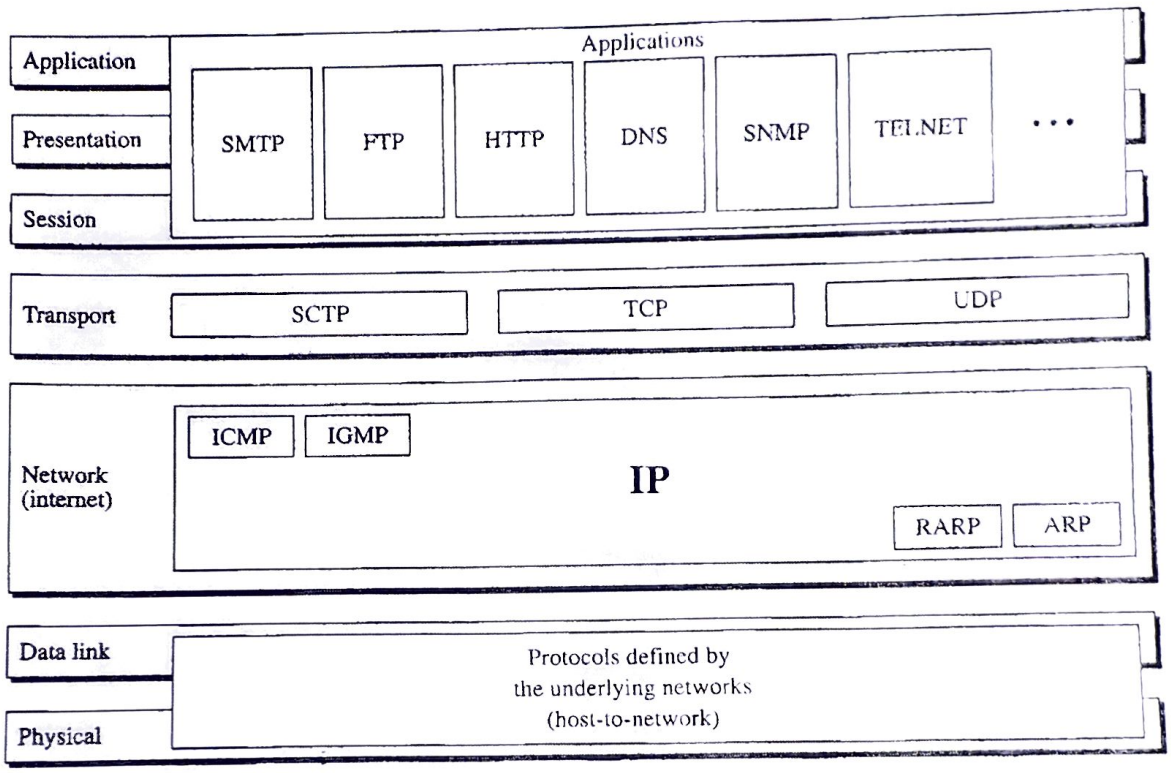
SSL is short for *Secure SocketsLayer*, a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http:*.

Another protocol for transmitting data securely over the World Wide Web is *Secure HTTP (S-HTTP)*. Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.



TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.



Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol--a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer.

function of common networking protocols.

- **TCP**

  The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. It is a reliable stream delivery service that guarantees delivery of a data stream sent from one host to another without duplication or losing data.

- **FTP**

  File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and server. Authentication is accomplished through the use of a clear-text sign-in protocol and is not considered to be secure.

- **UDP**

  The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice.

- **DHCP**

  The Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol that enables a server on an IP network to automatically assign an IP address to a computer from a predetermined range of numbers. The most essential information needed is an IP address, and a default route and routing prefix. DHCP controls the assignment of unique dynamic IP addresses and routing information, eliminating the manual task by a network administrator.

- **TFTP**

  Trivial File Transfer Protocol (TFTP) is a simple insecure protocol used to transfer files. It is typically implemented on top of the User Datagram Protocol (UDP) using port number 69. Packets are limited to a 512 byte limit and can be easily lost. When a

packet smaller than 512 bytes is received, the server assumes the end of the file has been reached and closes the connection. Transmission is not guaranteed to be complete and has no provision for user authentication. TFTP is designed to be small and easy to implement, therefore, lacks most of the features of FTP. TFTP only reads and writes files (or mail) to or from a remote server, it cannot list directories. TFTP can be used for remote booting of devices without hard drives. Used in conjunction with a bootp server, the device receives its addressing information and the address of the TFTP server from which it should boot.

- **DNS**

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. Internet and TCP utilities such as telnet, FTP, and SMTP use DNS to translate computer host and domain names to their corresponding IP addresses. DNS allows you to type recognizable names into your Web browser and your computer will automatically find that address on the Internet. Address information is stored in several locations in a hierarchical structure.

- **HTTPS**

Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems. HTTPS uses port 443 by default.

- **HTTP**

Hypertext Transfer Protocol (HTTP) is an application-level protocol used to request and deliver web pages between a server and browser. HTTP is the foundation of data communication for the World Wide Web.

- **ARP**

Address Resolution Protocol (ARP) is a low-level network protocol used for the resolution of network layer IP addresses into corresponding link layer MAC (Media Access Control) addresses. ARP is the standard of identifying a host's hardware address when only its network IP address is known.

- **SSH**

Secure Shell (SSH) is a cryptographic remote login protocol for secure data communication over an unsecured network. Designed as a replacement for telnet and rlogin, which send information in plaintext, SSH client and server programs provide strong host-to-host and user authentication as well as a number of securely encrypted methods of communication to provide confidentiality and integrity of data. SSH supports data stream compression between the client and the server.

- **POP3**

  Post Office Protocol (POP3) is a simple, standardized application-layer protocol used for retrieving incoming email from a remote mail server over a TCP/IP connection and saving to a local device. A POP3 server listens on well-known port TCP/110.

- **IMAP4**

  Internet message access protocol (IMAP) is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the Post Office Protocol (POP). Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server. IMAP is a client/server protocol in which e-mail is received and held by your Internet server and downloaded from the server by request. Imap permits the manipulation of remote mailboxes as though they were local, and works well with slower modem connections.

- **Telnet**

  Short for Telecommunications network, TELNET is a text based interface protocol that provides an insecure remote access to other computers. Telnet uses a command line interface and can be accessed in Windows from the Start menu by clicking <Start>, <Run>, then by typing: telnet (somesite) 23. Port number 23 is the default port used by telnet, but is usually optional and often not required.

- **SMTP**

  Simple Mail Transfer Protocol (SMTP) is a reliable and efficient mail transport and delivery protocol that is capable of transporting outgoing email across multiple networks. SMTP requires a reliable data stream channel for transmission.

- **SNMP**

  Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

- **ICMP**

  The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

- **IGMP**

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

- **TLS**

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

Protocol	Common Port
FTP (File Transfer Protocol)	20, 21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name Service)	53
TFTP (Trivial File Transfer Protocol)	69
HTTP (Hypertext Transfer Protocol)	80
POP3 (Post Office Protocol version 3)	110
NNTP (Network News Transport Protocol)	119
NTP (Network Time Protocol)	123
IMAP4 (Internet Message Access Protocol version 4)	143
HTTPS (Hypertext Transfer Protocol Secure)	443

Network Security

Network security: Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side-effects.

Reasons for securing our network

Or

Why do we protect our networks ?

- Damage or destruction of computer systems.
- Damage or destruction of internal data.
- Loss of sensitive information to hostile parties.
- Use of sensitive information to steal items of monitary value.
- Use of sensitive information against the organization's customers which may result in legal action by customers against the organization and loss of customers.
- Damage to the reputation of an organization.
- Monitary damage due to loss of sensitive information, destruction of data, hostile use of sensitie data, or damage to the organization's reputation.

What to do

- **Confidentiality** - Information is available only to people with rightful access.
- **Integrity** - Information can only be changed by authorized personnel. Integrity - The receiver of the message should be able to tell the message was not modified. Requires key exchange.
- **Availability** - Information is available to only those who need it.
- **Verification - nonrepudiation** - There is proof that the sender sent the message
- **Authentification** - The receiver of the message should be able to be sure of the origin of the message. Requires a digital signature

Threats : Threats are the various risks or dangers a network has to face during its Operation.

Threats are of 2 types

1).Internal threats

2).External threats

Internal Threats

When people think of an information security threat or a "security breach", hackers come to mind. Companies usually make sizeable investments to prevent intrusions to their systems, put protections in place and know the seriousness of external threats

But guess who knows more about these loopholes and ports of penetration than anyone? A company's own employees.

This means Internal threats are risks offered by internal persons who knows the network and its loopholes better. Internal threats might be someone who knows the weaknesses of the software being used or has the ability to introduce viruses into a system

Various Internal Threats

1). An internal person knowing weakness of network can introduce viruses onto network. Viruses can come from within simply by opening e-mail attachments

2). Some employees find it easy to gain access to restricted areas; this may include the possession of unauthorized passwords. If something is password-protected, chances are there is confidential information involved

3). With all the home office workers, laptops are in frequent use. Many times the security prevention in a laptop is turned off when remotely connecting. This is another major internal vulnerability or internal threat

Preventions of Internal Threats

1. Perform a security audit, or have one performed.
2. Unless the knowledge, experience and manpower exist in-house, consult an outside expert on audits, policies, and the subsequent security monitoring and prevention service.
3. Ensure adequate background checks on employees.
4. Establish a security policy, and enforce it. This includes implementing things like swipe cards, changing passwords often and restricting sensitive areas. This creates the right attitude toward information security in your company and clarifies the consequences of any found internal breach. A professional consulting firm specializing in policy development can save time and money and ensure an up-to-date policy.
5. Use firewalls. Firewalls protect against unauthorized logins usually from the outside world, preventing hackers from logging on to your network.
6. Use virus scanning software. Attachments to e-mails received and passed around are the biggest reason for the spread of viruses.
7. Implement ongoing managed services

External Threats : External Threats are threats are risks offered to a network and its resources

Compiled By: Vinod sharma

by some external agents or intruders for the purpose of stealing data or capturing the network clients and resources

Various External Threats

1). **Eavesdropping**. Anonymous users can intercept the radio signals of your wireless network and be able to read the data you are transmitting. Eavesdroppers can get the following information on the network they are trying to "attack": who uses the wireless network, which files or computers in the network are accessible, and its coverage area, among others.

2). **Communications jamming**. This type of threat happens when there is interference (either intentional or unintentional) that overwhelms either the sender or receiver in the link.

3). **Denial of Service Attack**. When an "attacker" manages to jam the entire network he can cause a Denial of Service (DOS) attack. There are two types of DOS attacks that you should be wary of:

- Client jamming – By jamming the client station, an attacker can take over or impersonate the jammed client.
- resource jamming – With this type of jamming, the attacker can assume the role of the resource by capturing that resource.

4). **Data modification and injection**. This happens when an attacker manages to add or change data in an existing connection as a means of hijacking the connection or sending malicious data or commands.

5). **Man in the Middle attack**. These are quite similar to injection attacks. The attacker may pretend to be the legitimate network resource. When a PC in a network establishes connection the attacker can now capture the connection. He then would initiate the completion of the connection to the original resource, proxying the communications to that resource. The attacker now has the ability to do all sorts of malicious commands to your computer.

6).**Rogue clients**. Attackers can clone a client's identification and then try to enter a network and use its services.

7).**Rogue network access points**. An attacker can make a rogue access point and then use it to pretend he's a legitimate network resource.

8). **Client to Client attacks**. Once an attacker is able to successfully access a network client, he can use that connection to leverage further attacks on other PCs in the network.

9). **Data theft**. Attackers can steal delicate or sensitive information or data from your network

10). **Back door and remote administration programs**

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer.

11). Email borne viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address

12). Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems

13). Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus. More information about Trojan horses can be found in the following document.

14). IP Spoofing.

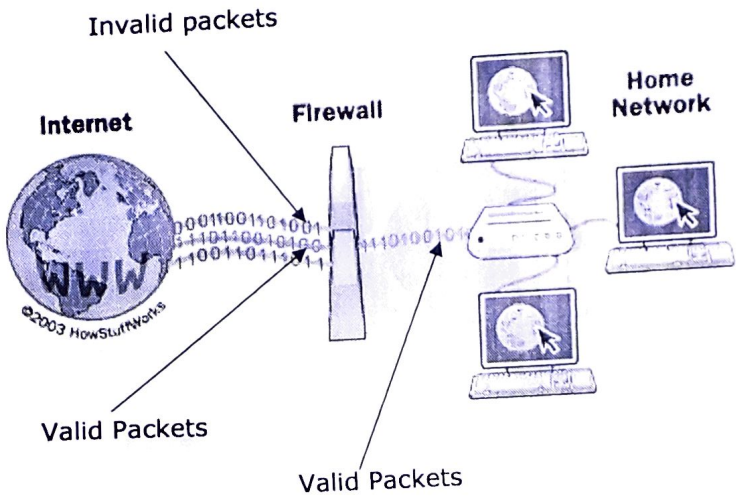
This is where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker: he can send packets to a host, perhaps causing it to take some sort of action.

Preventions or Recommendations

1. Consult your system support personnel if you work from home
2. Use virus protection software
3. Use a firewall
4. Don't open unknown email attachments
5. Don't run programs of unknown origin
6. Disable hidden filename extensions
7. Keep all applications (including your operating system) patched
8. Turn off your computer or disconnect from the network when not in use
9. Disable Java, JavaScript, and ActiveX if possible
10. Disable scripting features in email programs
11. Make regular backups of critical data

Compiled By: Vinod sharma

12. Make a boot disk in case your computer is damaged or compromised



Error Correction and the Hamming Code

The use of simple parity allows detection of single bit errors in a received message. Correction of such errors requires more information, since the position of the bad bit must be identified if it is to be corrected. (If a bad bit can be found, then it can be corrected by simply complementing its value.) Correction is not possible with one parity bit since any bit error in any position produces exactly the same information - "bad parity".

If more bits are included with a message, and if those bits can be arranged such that different errored bits produce different error results, then bad bits could be identified. In a 7-bit message, there are seven possible single bit errors, so three error control bits could potentially specify not only that an error occured but also which bit caused the error.

Similarly, if a family of codewords is chosen such that the minimum distance between valid codewords is at least 3, then single bit error correction is possible. This distance approach is "geometric", while the above error-bit argument is 'algebraic'.

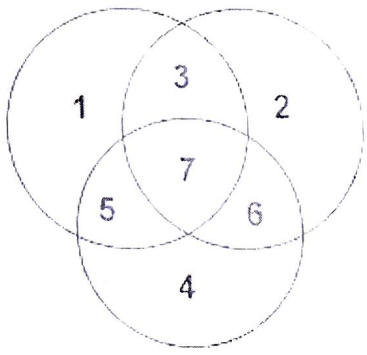
Either of the above arguments serves to introduce the Hamming Code, an error control method allowing correction of single bit errors.

The Hamming Code

Consider a message having four data bits (D) which is to be transmitted as a 7-bit codeword by adding three error control bits. This would be called a (7,4) code. The three bits to be added are three EVEN Parity bits (P), where the parity of each is computed on different subsets of the message bits as shown below.

7	6	5	4	3	2	1	
D	D	D	P	D	P	P	7-BIT CODEWORD
D	-	D	-	D	-	P	(EVEN PARITY)
D	D	-	-	D	P	-	(EVEN PARITY)
D	D	D	P	-	-	-	(EVEN PARITY)

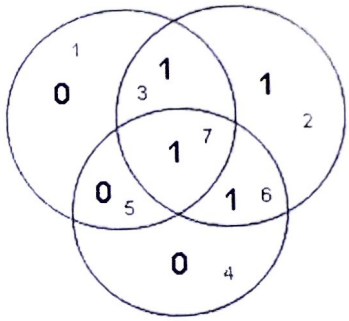
Why Those Bits? - The three parity bits (1,2,4) are related to the data bits (3,5,6,7) as shown at right. In this diagram, each overlapping circle corresponds to one parity bit and defines the four bits contributing to that parity computation. For example, data bit 3 contributes to parity bits 1 and 2. Each circle (parity bit) encompasses a total of four bits, and each circle must have EVEN parity. Given four data bits, the three parity bits can easily be chosen to ensure this condition.



It can be observed that changing any one bit numbered 1..7 uniquely affects the three parity bits. Changing bit 7 affects all three parity bits, while an error in bit 6 affects only parity bits 2 and 4, and an error in a parity bit affects only that bit. The location of any single bit error is determined directly upon checking the three parity circles.

For example, the message 1101 would be sent as 1100110, since:

7	6	5	4	3	2	1	
1	1	0	0	1	1	0	7-BIT CODEWORD
1	-	0	-	1	-	0	(EVEN PARITY)
1	1	-	-	1	1	-	(EVEN PARITY)
1	1	0	0	-	-	-	(EVEN PARITY)



When these seven bits are entered into the parity circles, it can be confirmed that the choice of these three parity bits ensures that the parity within each circle is EVEN, as shown here.

It may now be observed that if an error occurs in any of the seven bits, that error will affect different combinations of the three parity bits depending on the bit position.

For example, suppose the above message 1100110 is sent and a single bit error occurs such that the codeword 1110110 is received:

```
      transmitted message                          received message
      1 1 0 0 1 1 0          ------------>          1 1 1 0 1 1 0
BIT:  7 6 5 4 3 2 1                          BIT:  7 6 5 4 3 2 1
```

The above error (in bit 5) can be corrected by examining which of the three parity bits was affected by the bad bit:

7	6	5	4	3	2	1		
1	1	1	0	1	1	0	7-BIT CODEWORD	
1	-	1	-	1	-	0	(EVEN PARITY)	NOT! 1
1	1	-	-	1	1	-	(EVEN PARITY)	OK! 0
1	1	1	0	-	-	-	(EVEN PARITY)	NOT! 1

- **Slot type (ST) :** This 1 bit field defines two types of slots, one for packet transmission and other for isochronous transmission.
- **Reserved (R) :** It is reserved for future.
- **Previous slot read (PSR) :** This two bit field is set to 0 by the addressed station once it has read the contents of the slot.
- **Request (RQ) :** It consists of three bits set by the station to make reservations for slot. These three bits represents 8 levels of priority in network.

2. **Address field :** The address field holds a 20 bit virtual channel identifier (VCI) to be used for MAN and WAN transmission.
3. **Type field :** This 2 byte field identifies the payload as user data, management data and so on.
4. **Priority field :** The priority field identifies the priority of slot in a network that uses priority.
5. **CRC field :** This field contains 8 bit CRC.

9.4.5 IEEE 802.11 : WIRELESS LAN

Wireless communication is one of the fastest growing technologies these days. Wireless LANs are commonly found in office buildings, college campuses, and in many public areas.

IEEE 802.11 standard provides wireless communication with the use of infrared or radiowaves.

802.11 Architecture

The 802.11 architecture defines two types of services and three different types of stations

802.11 Services

The two types of services are

1. Basic services set (BSS)
2. Extended Service Set (ESS)

1. Basic Services Set (BSS)

- The basic services set contains stationary or mobile wireless stations and a central base station called access point (AP).
- The use of access point is optional.

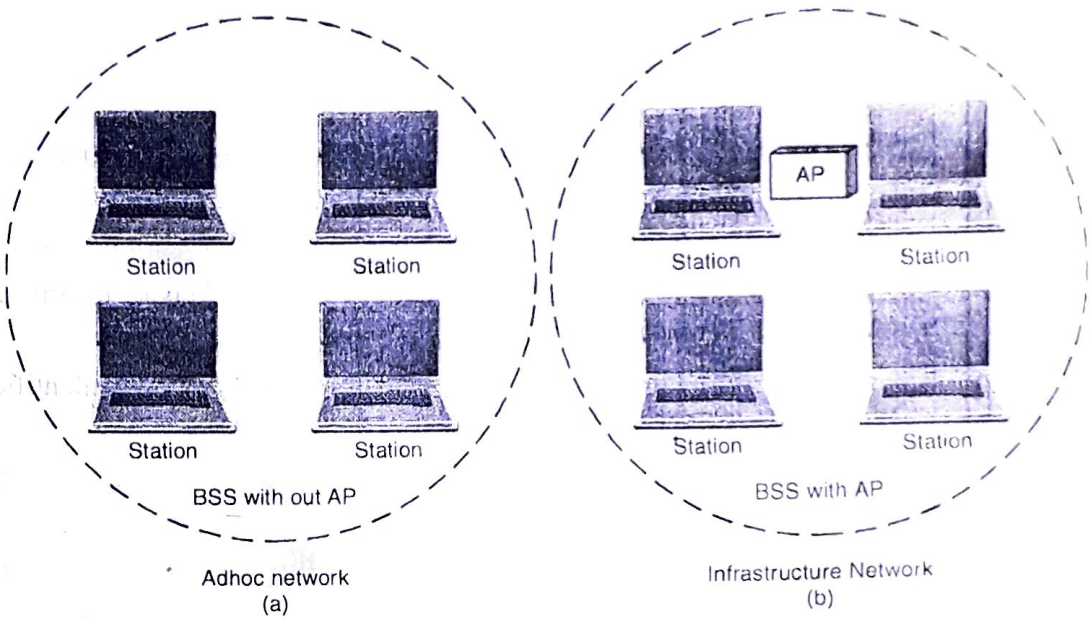


Fig. 9.56. Basic Service Sets

- If the access point is not present, it is known as stand-alone network. Such a BSS cannot send data to other BSSs. This type of architecture is known as **adhoc architecture** (see fig. 9.56 (a)).
- The BSS in which an access point is present is known as an **infrastructure** network (See fig. 9.56 (b)).

2. Extend Service Set (ESS)

- An extended service set is created by joining two or more basic service sets (BSS) having access points (APs) as shown in fig. 9.57.
- These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.
- The distribution system can be any IEET LAN.
- There are two types of stations in ESS :

  (i) Mobile stations : These are normal stations inside a BSS.

  (ii) Stationary stations : These are AP stations that are part of a wired LAN.
- Communication between two stations in two different BSS usually occurs via two APs.
- A mobile station can belong to more than one BSS at the same time.

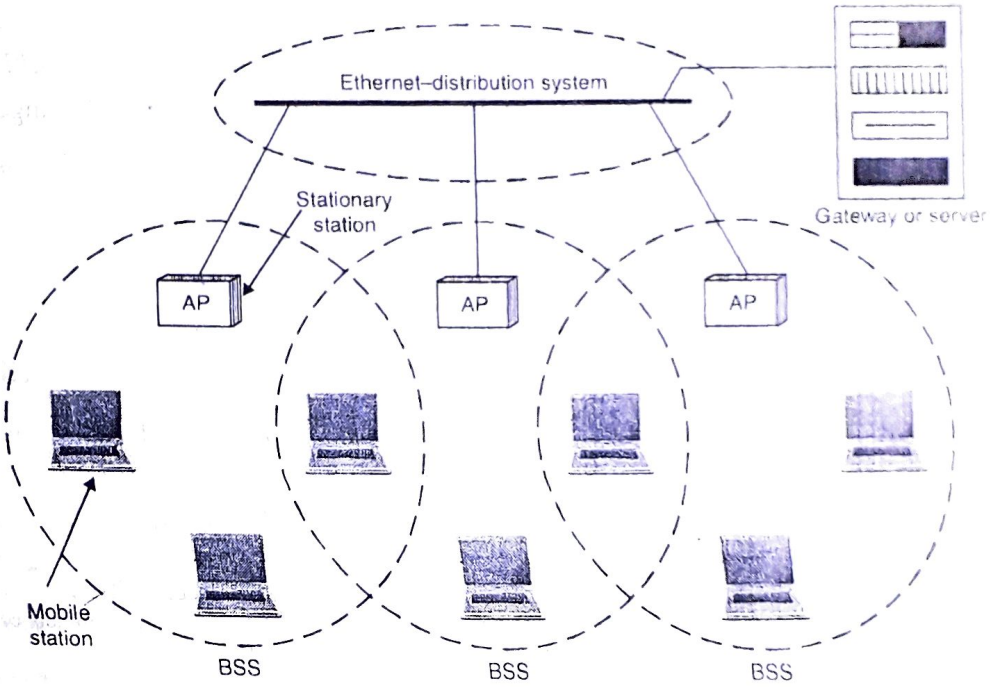


Fig. 9.57 Extended Service Set

802.11 Station Types

IEEE 802.11 defines three types of stations on the basis of their mobility in wireless LAN. These are :

1. No-transition Mobility
2. BSS-transition Mobility
3. ESS-transition Mobility

1. **No-transition Mobility :** These types of stations are either stationary *i.e.* immovable or move only inside a BSS.
2. **BSS-transition mobility :** These type of stations can move from one BSS to another but the movement is limited inside an ESS.
3. **ESS-transition mobility :** These type of stations can move from one ESS to another. The communication may or may not be continuous when a station moves from one ESS to another ESS.

Physical layer functions

- As we know that physical layer is responsible for converting data stream into signals, the bits of 802.11 network can be converted to radio waves or infrared waves.

- These are six different specifications of IEEE 802.11. These implementations, except the first one, operates in *industrial, scientific and medical (ISM)* band. These three banks are unlicensed and their ranges are (See fig. 9.58)

  1. 902–928 MHz
  2. 2.400–4.835 GHz
  3. 5.725–5.850 GHz

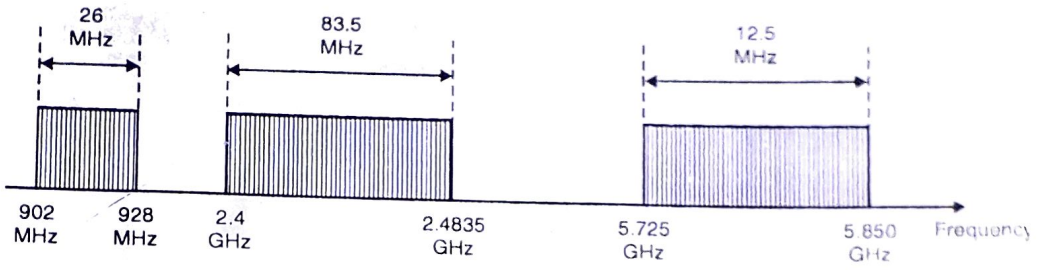


Fig. 9.58 Industrial, scientific and medical (ISM) band

- The different implementations of IEE802.11 are given below:-

1. IEEE 802.11 infrared

- It uses diffused (not line of sight) infrared light in the range of 800 to 950 nm.
- It allows two different speeds : 1 Mbps and 2Mbps.
- For a 1-Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen Os and a single 1.
- For a 2-Mbps data rate, a 2 bit code is encoded into 4 bit code. This 4 bit code contains three Os and a single 1.
- The modulation technique used is pulse position modulation (PPM) *i.e.* for converting digital signal to analog.

2. IEEE 802.11 FHSS

- IEEE 802.11 uses Frequency Hoping Spread Spectrum (FHSS) method for signal generation.
- This method uses 2.4 GHz ISM band. This band is divided into 79 subbands of 1MHz with some guard bands.

- In this method, at one moment data is sent by using one carrier frequency and then by some other carrier frequency at next moment. After this, an idle time is there in communication. This cycle is repeated after regular intervals.
- A pseudo random number generator selects the hopping sequence.
- The allowed data rates are 1 or 2 Mbps.
- This method uses frequency shift keying (two level or four level) for modulation *i.e.* for converting digital signal to analogy.

IEEE 802.11 DSSS

- This method uses Direct Sequence Spread Spectrum (DSSS) method for signal generation. Each bit is transmitted as 11 chips using a Barker sequence.
- DSSS uses the 2.4–GHz ISM band.
- It also allows the data rates of 1 or 2 Mbps.
- It uses phase shift keying (PSK) technique at 1 M baud for converting digital signal to analog signal.

IEEE 802.11a OFDM

- This method uses Orthorgonal Frequency Division Multiplexing (OFDM) for signal generation.
- This method is capable of delivering data upto 18 or 54 Mbps.
- In OFDM all the subbands are used by one source at a given time.
- It uses 5 GHz ISM band.
- This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control information.
- If phase shift keying (PSK) is used for modulation then data rate is 18 Mbps. If quadrature amplitude modulation (QAM) is used, the data rate can be 54 Mbps.

IEEE 802.11b HR-DSSS

- It uses High Rate Direct Sequence Spread Spectrum method for signal generation.
- HR-DSSS is similar to DSSS except for encoding method.
- Here, 4 or 8 bits are encoded into a special symbol called complementary code key (CCK).

- It uses 2.4 GHz ISM band.
- It supports four data rates : 1, 2, 5.5 and 11 Mbps.
- 1 Mbps and 2 Mbps data rates uses phase shift modulation.
- The 5.5. Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.
- The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

6. IEEE 802.11g OFDM

- It uses OFDM modulation technique.
- It uses 2.4 GHz ISM band.
- It supports the data rates of 22 or 54 Mbps.
- It is backward compatible with 802.11b.

MAC sublayer Functions

802.11 supports two different modes of operations. These are :

1. Distributed Coordination Function (DCF)
2. Point Coordination Function (PCF)

1. Distributed Coordination Function

- The DCF is used in BSS having no access point.
- DCF uses CSMA/CA protocol for transmission.
- The following steps are followed in this method (see figure 9.59) :
  1. When a station wants to transmit, it senses the channel to see whether it is free or not.
  2. If the channel is not free the station waits for back off time.
  3. If the station finds a channel to be idle, the station waits for a period of time called **distributed interframe space (DIFS).**
  4. The station then sends control frame called **request to send (RTS)** as shown in figure.
  5. The destination station receives the frame and waits for a short period of time called **short interframe space (SIFS).**
  6. The destination station then sends a control frame called **clear to send (CTS)** to the source station. This frame indicates that the destination station is ready to receive data.

Comparison of Wi-Fi standards

As the Wi-Fi specification has evolved, its performance in terms of both range and throughput has improved. as the table below

Standard	802.11b	802.11a	802.11g	802.11n	802.11ac
Theoretical Speed – Up to	11 Mbps	54 Mbps	54 Mbps	300 Mbps	1 Gbps
Frequency	2.4 GHz	5 GHz	2.4 Ghz	2.4 and/or 5 Ghz	5 Ghz
Range ft	100 – 150	25-75	100 - 150	~ 230	Not known

Five Stages in the WiFi Network

WIFI client is going through the five stages:

1. Scanning
2. Joining
3. Authentication
4. Association
5. Reassociaton

Scanning

The scanning is the process of finding the WiFi network. Classical wired networks use cables for the interconnection. In the wireless network, the first thing you need to do is to to identify the appropriate network. WiFi **clients use the scanning to find existing networks in the area**. After scanning, the client can choose to join one of the available wireless networks.

Joining

Joining does not guarantee the network access. It is only the first step for the client to be connected to the WLAN network. After joining, the client also needs to pass the authentication and associate stage.

The client can connect to the BSS in two ways:

- Manually
- Automatically

In the manual joining the client chooses the BSS manually. In the automatic joining wireless client picks the best access point according to a power level and signal strength.
In the both cases, parameters configured on wireless client and access point, need to match.

Authentication

In wireless networks, you don't need the physical access to the network. You only need to be within the range. **Wireless authentication is the security method in the wireless networks**. More about the wireless authentication and authentication types read on wireless authentication.

Association

Association is the process that **enables the client the actual access to the WLAN networ**k. It is the same like plugging the cable into the wired network. It is not possible to be associated in more than one access point.

Reassociation

The association can occur only in the ESS wireless network. The client, in this case, associates to the other access point in the same ESS. It is triggered when the client detects that the other access point have a stronger wireless signal.

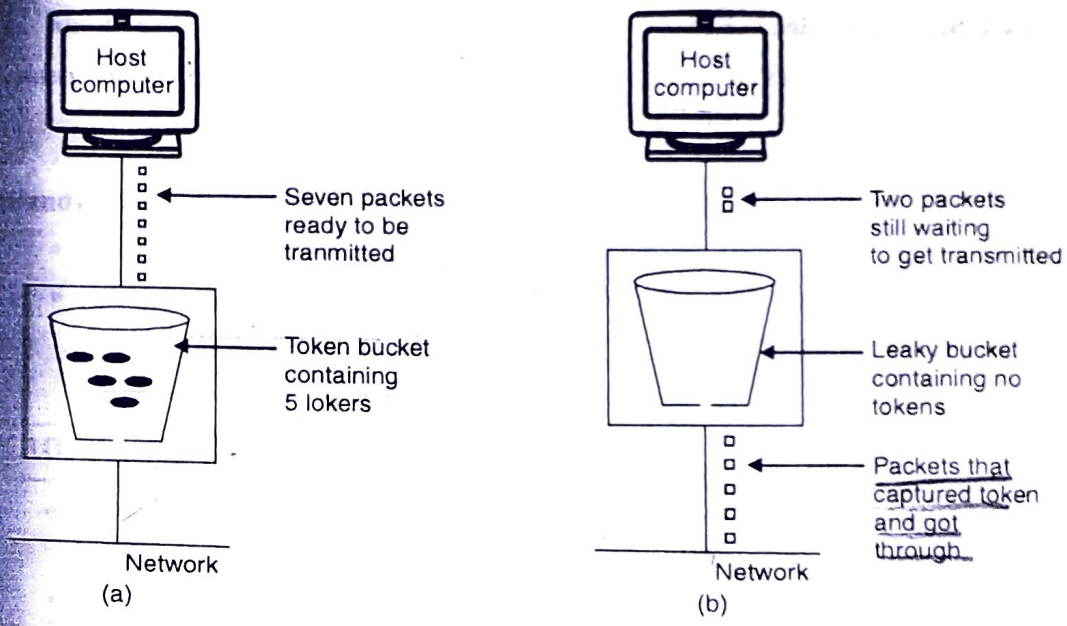


Fig. 10.29. Implementation of token bucket

Comparison between leaky bucket and token bucket algorithm

S.No.	Leaky Bucket	Token Bucket
1.	Leaky bucket is rigid algorithm as it outputs the data at an average rate and does not support bursty data.	Token bucket algorithm is flexible as it enables the bursty data to be sent immediately.
2.	It does not credit the idle time of the host *i.e.* it does not generate tokens.	It credits the idle time of the host and accumulates it in form of the tokens.
3.	The leaky bucket algorithm discards the incoming packets if the bucket (FIFO queue) is full.	The token bucket algorithm throws away tokens if bucket is full. It never discards packets when bucket is full.

10.7 QUALITY OF SERVICE

Quality of service (QOS) is an internetworking issue. We can informally define quality of service as something flow seeks to attain.

Now, if the host wants to send bursty data, it can consume all 10,000 to at once for sending 10,000 cells or bytes.

Thus a host can send bursty data as long as bucket is not empty.

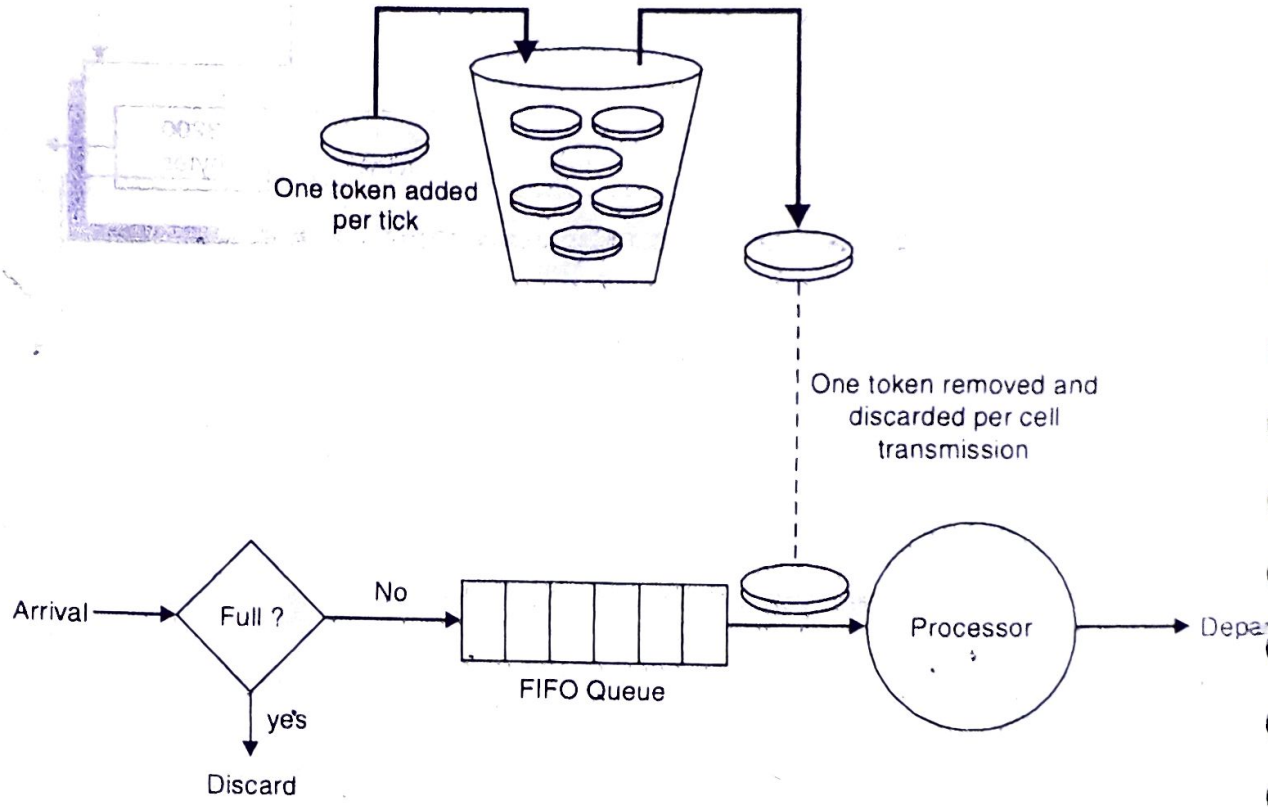


Fig. 10.28. Token bucket algorithm

Implementation of token bucket algorithm

1. This algorithm make use of a variable or counter that counts the token. counter is initialized to zero.
2. The counter is incremented by 1, each time a token is generated.
3. Whenever a packet is sent, the counter is decremented by one.
4. When the counter becomes zero, no packets can be sent.

For example, as shown in fig. 10.29 (a), token bucket contains 5 tokens and 7 pa are waiting to be transmitted.

In order to get transmitted, each packet captures and destroy one token.

Fig. 10.29 (b) shows that 5 out of 7 packet have gotten through, but the other tw struck waiting for two more tokens to be generated.