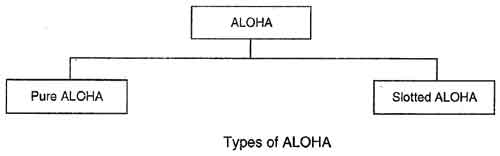
**ALOHA:**ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented 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](http://ecomputernotes.com/computernetworkingnotes/computer-network/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

[](http://ecomputernotes.com/images/Type-of-ALOHA.jpg)

**(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.

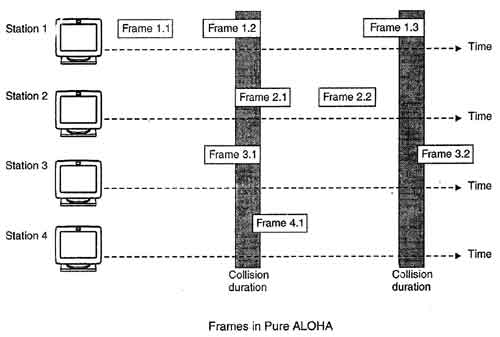
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• 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.

[](http://ecomputernotes.com/images/Frames-in-Pure-ALOHA.jpg)

• 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.

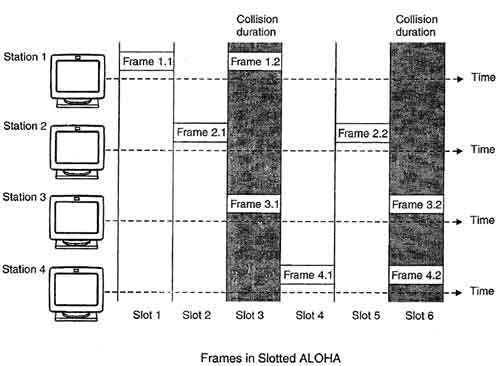
• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

**(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.

[](http://ecomputernotes.com/images/Frames-in-Slotted-ALOHA.jpg)

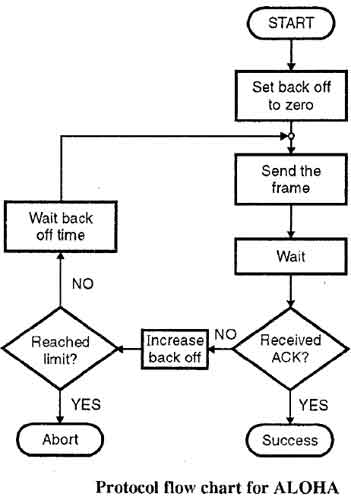
• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.*it misses the time slot then the station has to wait until the beginning of the next time slot.

• 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.

[](http://ecomputernotes.com/images/Protocol-flow-chart-for-ALOHA.jpg)

**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**

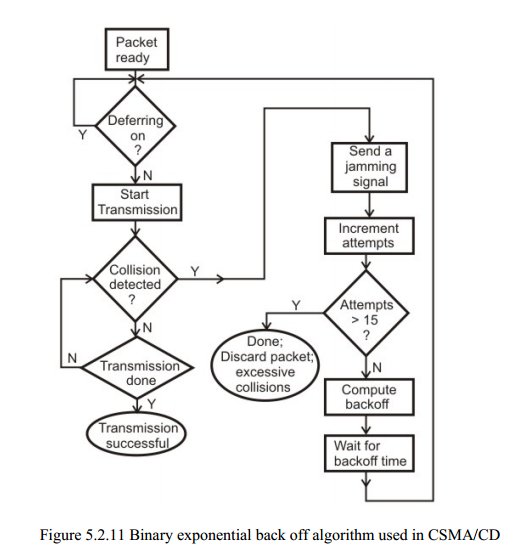
(i) 1-persistent CSMA: In this case, a node having data to send, start sending, if the channel is sensed free. If the medium is busy, the node continues to monitor until the channel is idle. Then it starts sending data.

(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.



**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.

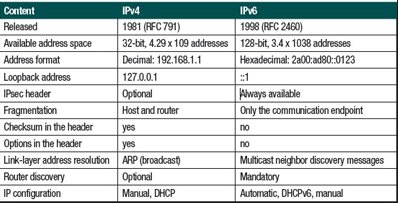
While IPv4 uses 32 bits to address the IP (provides approximately 232 = 4,294,967,296 unique addresses – but in fact about 3.7 billion addresses are assignable because the IPv4 addressing system separates the addresses into classes and reserves addresses for multicasting, testing, and other specific uses), IPv6 uses up to 128 bits which provides 2128 addresses or approximately 3.4 \* 1038 addresses. Well, maybe we should say it is extremely extremely extremely huge.

**IPv6 address format**

Format:

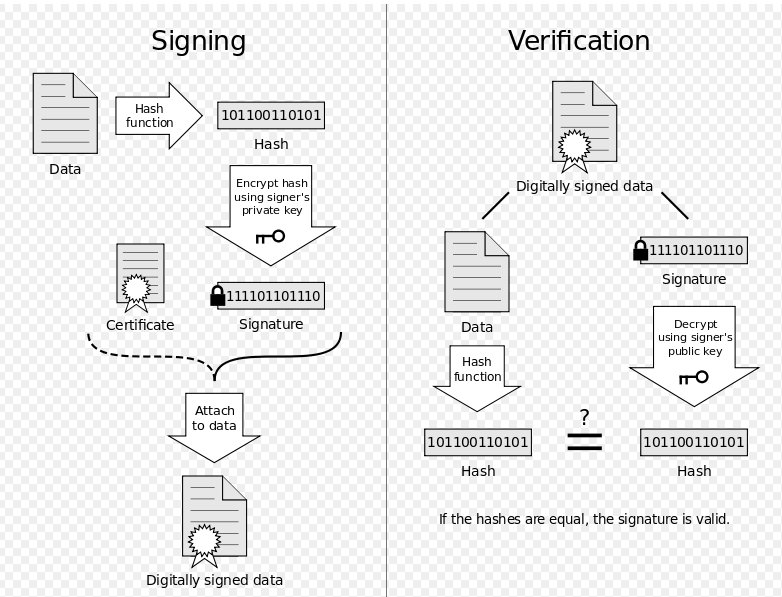
**x:x:x:x:x:x:x:x** – where **x** is a 16 bits hexadecimal field and **x** represents four hexadecimal digits.  
An example of IPv6:  **2001:0000:5723:0000:0000:D14E:DBCA:0764**

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”…



**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](http://en.wikipedia.org/wiki/Authentication) and [non-repudiation](http://en.wikipedia.org/wiki/Non-repudiation)) and that the message was not altered in transit ([integrity](http://en.wikipedia.org/wiki/Data_integrity)). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

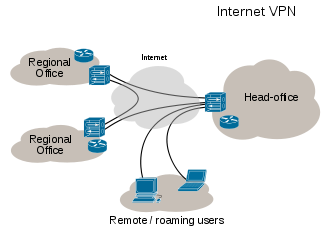


**VPN**

A **virtual private Network** (**VPN**) extends a [private network](http://en.wikipedia.org/wiki/Private_network) across a[public](http://en.wikipedia.org/wiki/Public) network, such as the [Internet](http://en.wikipedia.org/wiki/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]](http://en.wikipedia.org/wiki/Virtual_private_network#cite_note-1) This is done by establishing a virtual [point-to-point](http://en.wikipedia.org/wiki/Point-to-point_(network_topology)) 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](http://en.wikipedia.org/wiki/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 ***S***ecure***S***ockets***L***ayer, a [protocol](http://www.webopedia.com/TERM/P/protocol.html) developed by [Netscape](http://www.webopedia.com/TERM/N/Netscape.html) for transmitting private documents via the [Internet](http://www.webopedia.com/TERM/I/Internet.html). SSL uses a [cryptographic](http://www.webopedia.com/TERM/C/cryptography.html) system that uses two [keys](http://www.webopedia.com/TERM/K/key.html) to [encrypt](http://www.webopedia.com/TERM/E/encryption.html) data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both [Netscape Navigator](http://www.webopedia.com/TERM/N/Navigator.htm) and I[nternet Explorer](http://www.webopedia.com/TERM/I/Internet_Explorer.htm) support SSL, and many [Web sites](http://www.webopedia.com/TERM/W/web_site.htm) use the protocol to obtain confidential user information, such as credit card numbers. By convention,[URLs](http://www.webopedia.com/TERM/U/URL.htm) that require an SSL connection start with https: instead ofhttp:.

Another protocol for transmitting data securely over the [World Wide Web](http://www.webopedia.com/TERM/W/World_Wide_Web.htm) is [Secure HTTP (S-HTTP)](http://www.webopedia.com/TERM/S/S_HTTP.htm). Whereas SSL creates a secure connection between a client and a [server](http://www.webopedia.com/TERM/S/server.htm), 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)](http://www.webopedia.com/TERM/I/IETF.htm) as a [standard](http://www.webopedia.com/TERM/S/standard.htm).

