2.3 BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other.Bluetooth technology has several applications.Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.

Bluetooth was started by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway.

Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

Piconets

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary.

Note that a piconet can have only one primary station. Figure 2.3.1 shows a piconet.

A piconet can have a maximum of seven secondaries, and additional secondaries can be in the parked state.A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state.

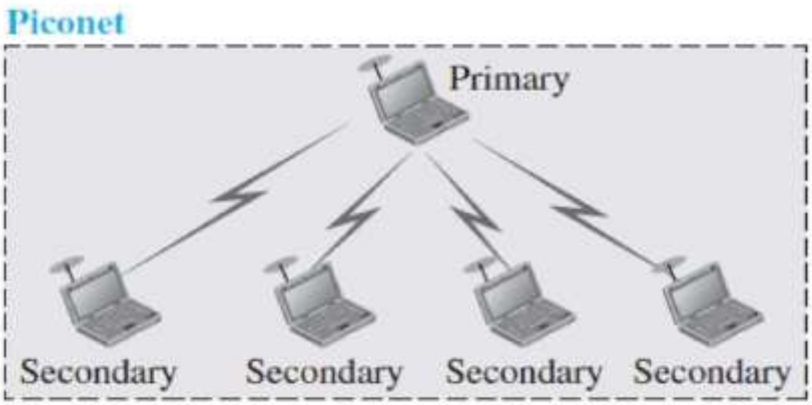


Fig2.3.1: Piconet architecture.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-452]

Scatternet

Piconets can be combined to form what is called a scatternet as in figure 2.3.2. A secondary station in one piconet can be the primary in another piconet.

This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

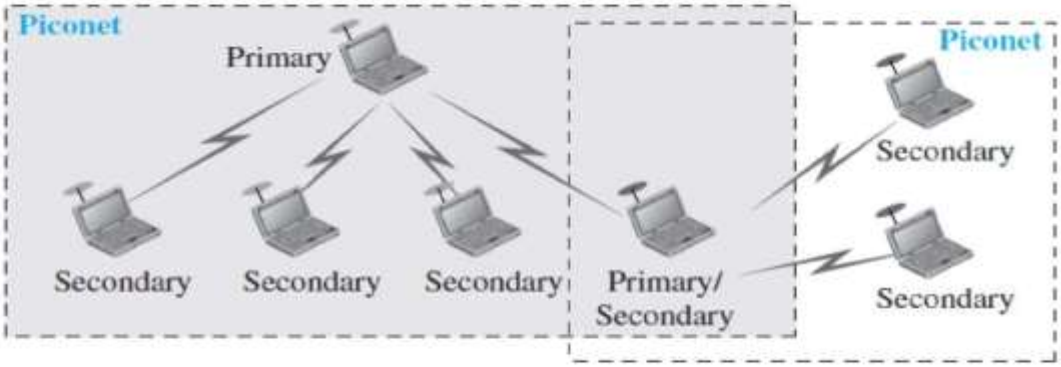


Fig2.3.2: Scatternet architecture.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-452]

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is1 Mbps with a 2.4-GHz bandwidth.

Bluetooth Layers : Bluetooth has several layers .

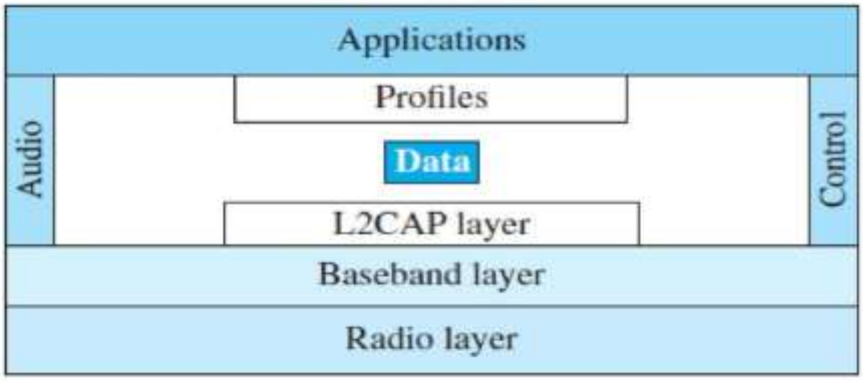


Fig2.3.3: Bluetooth layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-453]

L2CAP

The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL),.

It is used for data exchange on an ACL link; SCO channels do not use L2CAP. Figure 2.3.4 shows the format of the data packet at this level.The 16-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level .

The L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management.

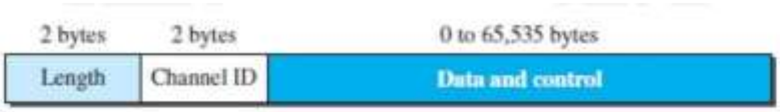


Fig2.3.4: L2CAP packet format.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-452]

Multiplexing

The L2CAP can do multiplexing. At the sender site, it accepts data from one of theupper-layer protocols, frames them, and delivers them to the baseband layer.At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

Segmentation and Reassembly

The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes.

This includes 4 bytes to define the packet and packet length. Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes.The L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. The L2CAP segments the packets at the source and reassembles them at the destination.

QoS

Bluetooth allows the stations to define a quality-of-service level.

Baseband Layer: The baseband layer is equivalent to the MAC sublayer in LANs.

The access method is TDMA.The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 µs.

This means that during the time that one frequency is used, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.

Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA).

Single-Secondary Communication

If the piconet has only one secondary, the TDMA operation is very simple.The time is divided into slots of 625 μs. The primary uses even-numbered slots (0, 2, 4,…); the secondary uses odd-numbered slots (1, 3, 5,…). TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.

In slot 0, the primary sends and the secondary receives;in slot 1, the secondary sends and the primary receives. The cycle is repeated.Figure 2.3.5 shows the concept.

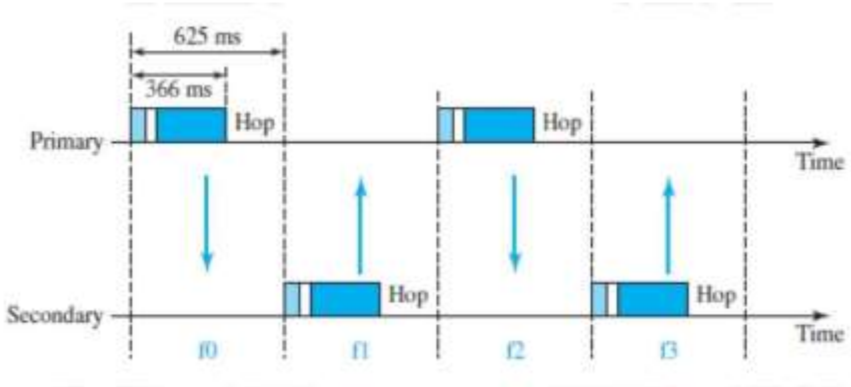


Fig2.3.5: Single secondary communication.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-454]

Multiple-Secondary Communication

The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it. All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

The figure 2.3.6. illustrates the concept. In slot 0, the primary sends a frame to secondary 1. In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent.

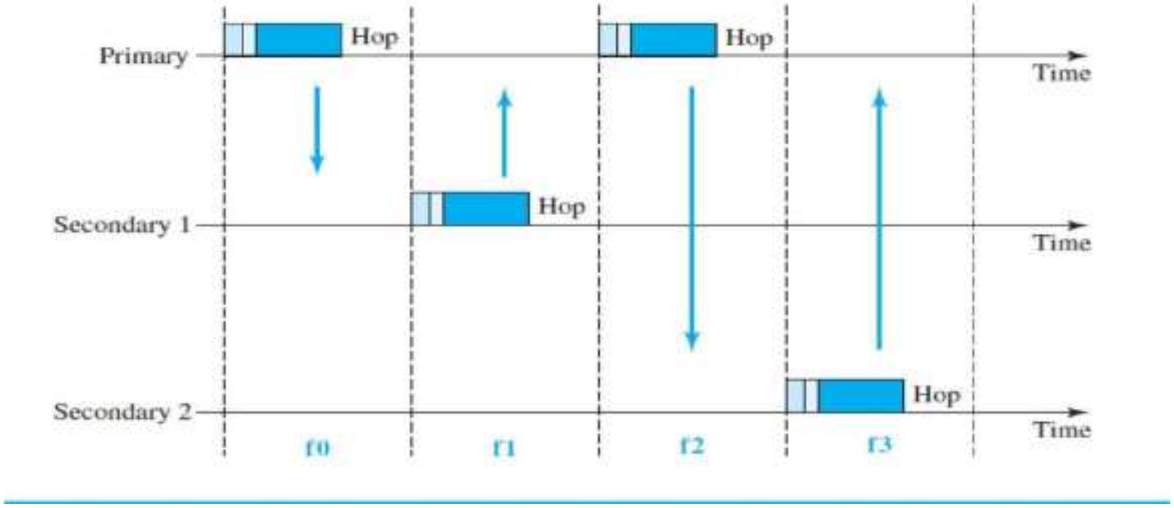


Fig2.3.6: Multiple secondary communication.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-455]

In slot 2, the primary sends a frame to secondary 2.In slot 3, only secondary 2 sends a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent. The cycle continues.

Links

Two types of links can be created between a primary and a secondary: SCO links and ACL links.

SCO A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals.

ACL An asynchronous connectionless link (ACL) is used when data integrity is more important than latency. In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted.

Frame Format

A frame in the baseband layer can be one of three types: one-slot, three-slot, or five slot.

In a one-slot frame exchange, 259 µs s needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 µs.With a 1-MHz bandwidth and 1 bit/Hz, the size of a one slot frame is 366 bits. A three-slot frame occupies three slots. Since 259 µs is used for hopping, the length of the frame is 3 × 625 − 259 = 1616 µs or 1616 bits.

A device that uses a three-slot frame remains at the same hop (at the same carrier frequency) for three slots.

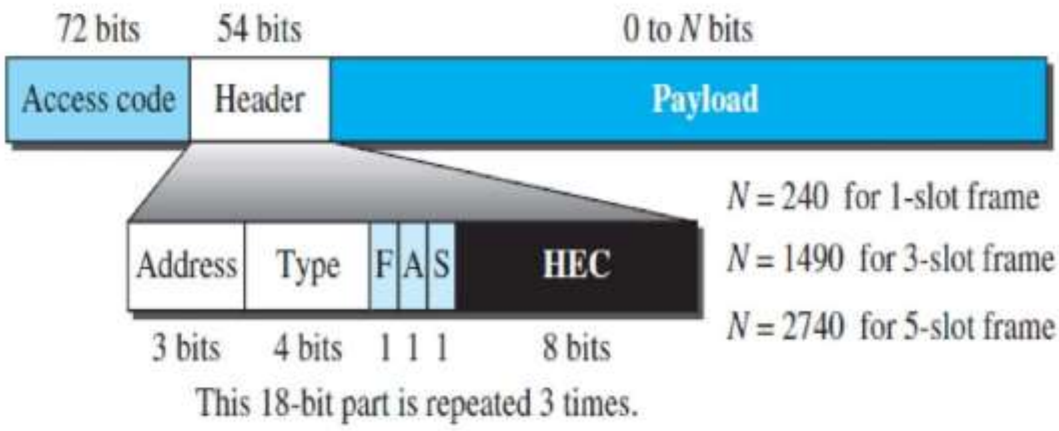


Fig2.3.7: Bluetooth frame format.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-456]

Description of each field:

Access code.This 72-bit field as in figure 2.3.7, normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.

Header.This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:

Address. The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.

Type. The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.

F. This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).

A. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.

S. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.

HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

The header has three identical 18-bit sections.The receiver compares these three sections, bit by bit. If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules. This is a form of forward error correction (for the header only). This double error control is needed because the nature of the communication, via air, is very noisy. No retransmission in this sublayer.

Payload: This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Radio Layer: The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band: Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.

Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency1600 times per second.

……………………………………………………………………………

2.2 ETHERNET (IEEE 802.3)

The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.

It has four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps).

Characteristics: Connectionless and unreliable service

Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame. Ethernet has no connection establishment or connection termination phases.

Frame Format

The Ethernet frame contains seven fields as in figure 2.2.1.

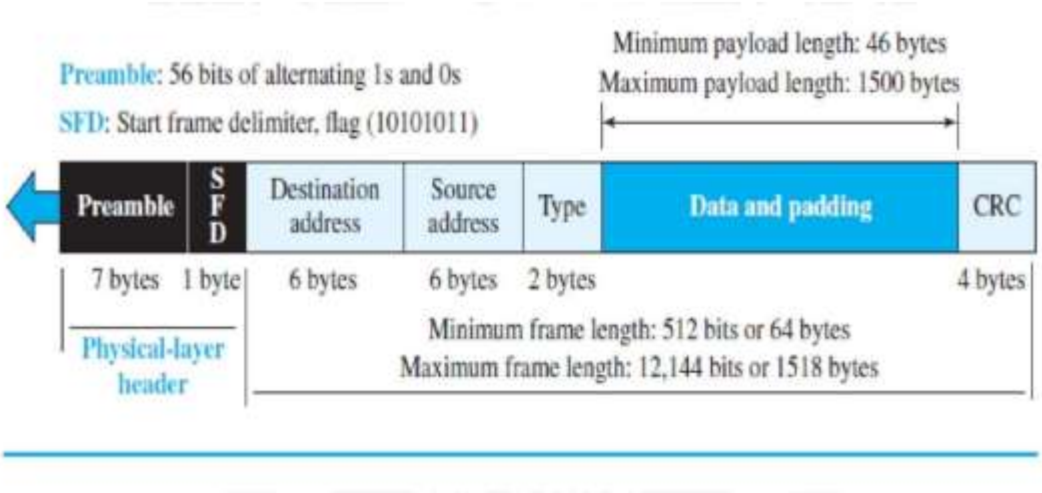

Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
Type
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Fig2.2.1: The Ethernet frame.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-364]

Preamble: This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock.The pattern provides only an alert and a timing pulse.The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer .

Start frame delimiter (SFD): This field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits are (11)2 and alert the receiver that the next field is the destination address. This field is actually a flag that defines the beginning of the frame.

Destination address (DA): This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.

Source address (SA): This field is six bytes and contains the link-layer address of the sender of the packet.

Type: This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on. It is used for multiplexing and demultiplexing.

Data: This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.

CRC: The last field contains error detection information. The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

Frame Length

An Ethernet frame needs to have a minimum length of 512 bits or64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is 64 -18= 46 bytes.

If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. Minimum frame length: 64 bytes ,Maximum frame length: 1518 bytes, Minimum data length: 46 bytes , Maximum data length: 1500 bytes

Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address.The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

For example,

Ethernet MAC address: 4A:30:10:21:10:1A

Standard Ethernet uses a coaxial cable (bus topology) or a set of twisted-pair cables with a hub (star topology) as shown in Figure .

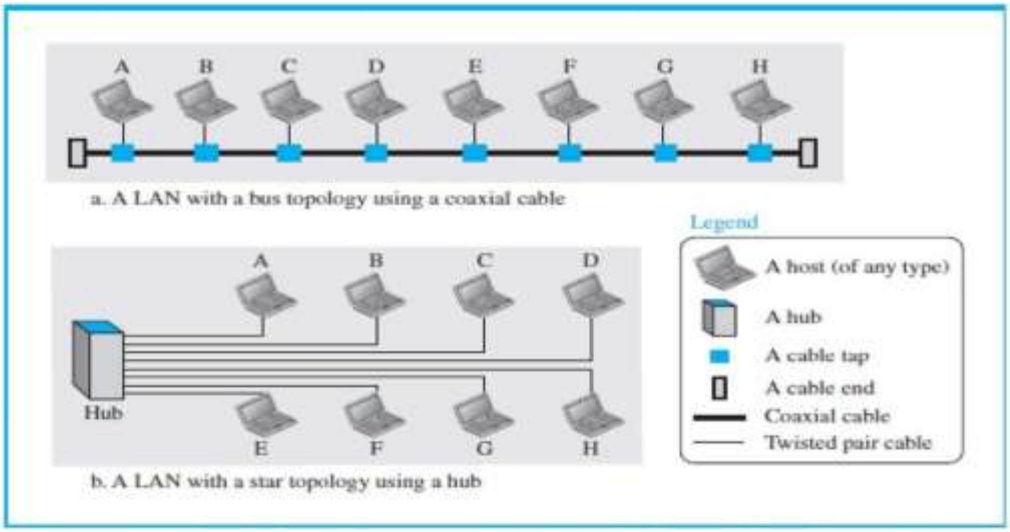


Fig2.2.2: The Implementation of Ethernet.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-368]

In the bus topology, when station A sends a frame to station B, all stations will receive it.

In the star topology, when station A sends a frame to station B, the hub will receive it. Since the hub is a passive element, it does not check the destination address of the frame; it regenerates the bits (if they have been weakened) and sends them to all stations except station A.

In a unicast transmission, all stations will receive the frame, the intended recipient keeps and handles the frame; the rest discard it.In a multicast transmission, all stations will receive the frame, the stations that are members of the group keep and handle it; the rest discard it.

In a broadcast transmission, all stations (except the sender) will receive the frame and all stations (except the sender) keep and handle it.

Access Method

The standard Ethernet has CSMA/CD as the access method.

Assume station A in Figure 2.2.2 has a frame to send to station D. Station A first should check whether any other station is sending (carrier sense). Station A measures the level of energy on the medium (for a short period of time, normally less than 100 μs.

If there is no signal energy on the medium, it means that no station is sending (or the signal has not reached station A). Station A interprets this situation as idle medium. It starts sending its frame. If the signal energy level is not zero, it means that the medium is being used by another station. Station A continuously monitors the medium until it becomes idle for 100 μs. It then starts sending the frame.

Efficiency of Standard Ethernet

The efficiency of the Ethernet is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station. The practical efficiency of standard Ethernet has been measured to be

Efficiency= 1/(1+6.4xa) ,the parameter "*a*" is the number of frames that can fit on the medium.

Implementation

Encoding and Decoding

All standard implementations use digital signalling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data as in figure 2.2.3.

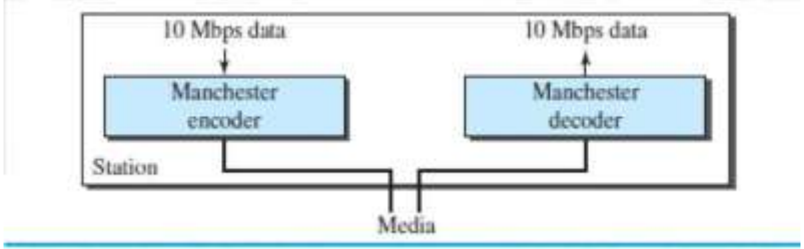


Fig2.2.3: The encoding scheme for Standard Ethernet.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-371]

10Base5: Thick Ethernet

The first implementation is called 10Base5, thick Ethernet, or Thicknet as shown in figure 2.2.4.

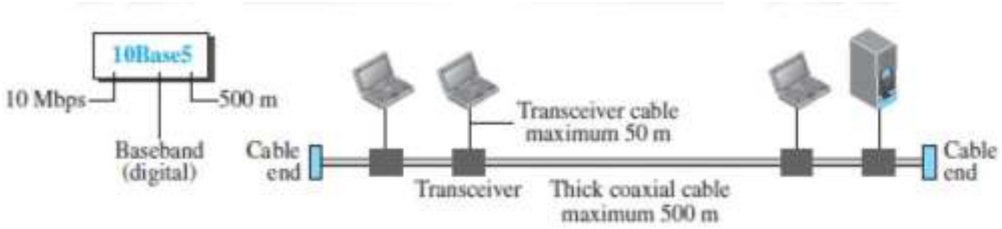


Fig2.2.4: Thick Ethernet

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-371]

The transceiver is responsible for transmitting, receiving, and detecting collisions.

The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

The maximum length of the coaxial cable must not exceed 500 m, otherwise, there is excessive degradation of the signal.

10Base2: Thin Ethernet

The second implementation is called 10Base2, thin Ethernet, or Cheapernet as shown in figure 2.2.5. 10Base2 uses a bus topology and the cable is much thinner and more flexible. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

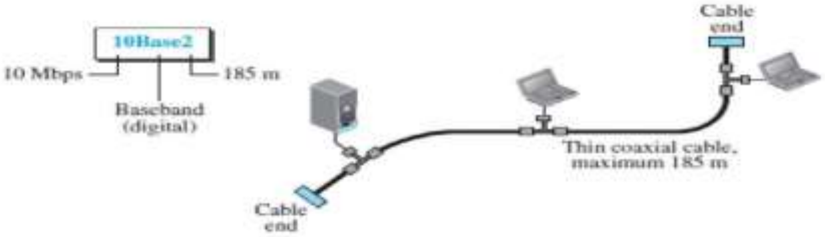


Fig2.2.5: Thin Ethernet.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-372]

Full-Duplex Ethernet

The limitations of 10Base5 and 10Base2 is that communication is half-duplex,a station can either send or receive, but may not do both at the same time.The next step is to move from switched Ethernet to full-duplex switched Ethernet.

The full-duplex mode increases the capacity of each domain from 10 to 20 Mbps.

No Need for CSMA/CD .In full-duplex switched Ethernet, there is no need for the CSMA/CD method. In a full duplex switched Ethernet, each station is connected to the switch via two separate links.

2.6 IPV4 ADDRESS

An IPv4 address is a 32-bit address that defines the connection of a host or a router to the Internet. The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet.

If a device has two connections to the Internet, via two networks it has two IPv4 addresses.

Address Space

An address space is the total number of addresses used by the protocol. If a protocol uses *b* bits to define an address, the address space is 2*b* because each bit can have two different values (0 or 1).

IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296(more than four billion).If there were no restrictions, more than 4 billion devices could be connected to the Internet.

There are three common notations to show an IPv4 address:

Binary notation (base 2),dotted-decimal notation (base 256), and hexadecimal notation (base 16) as shown in figure 2.6.1.

In binary notation, an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces are usually inserted between each octet (8 bits). Each octet is often referred to as a byte.To make the IPv4 address more compact and easier to read, it is written in decimal form with a decimal point (dot) separating the bytes. This format is referred to as dotted-decimal notation.

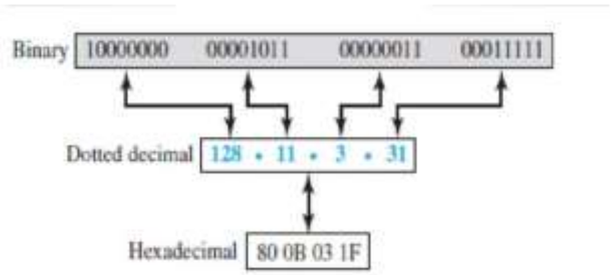


Fig2.6.1: The IPv4 address format.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-529]

Classfull Addressing

An IPv4 address was designed with a fixed-length prefix.

Three fixed-length prefixes were designed for this . That is (*n* = 8, *n* = 16, and *n* = 24).

The whole address space was divided into five classes (class A, B, C, D, and E), as shown in Figure 2.6.2 . This scheme is called as classful addressing.

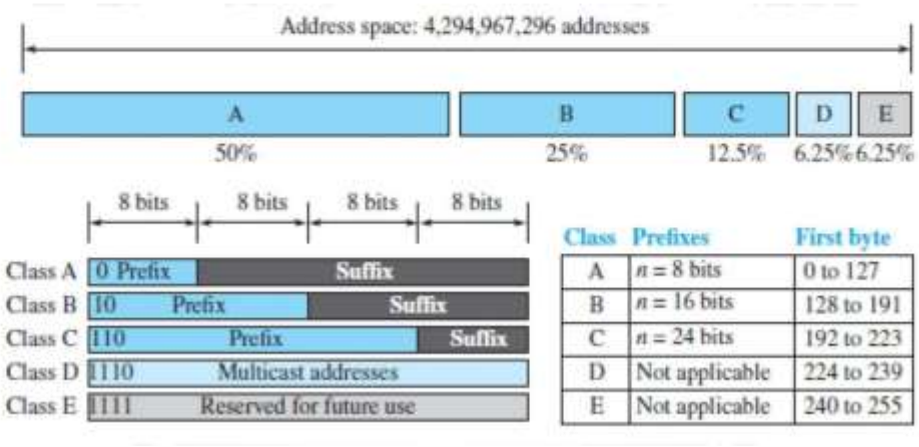
In class A, the network length is 8 bits, First bit is 0, which defines the class, and seven bits as the network identifier. This means there are only 2^7 =128 networks in the world that can have a class A address.

In class B, the network length is 16 bits, but since the first two bits, which are

$(10)_2$, define the class, we can have only 14 bits as the network identifier. This means there are only 2^{14} =16,384 networks in the world that can have a class B address.

In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier.All addresses that start with (110)2 belong to class C. This means there are 2^{21} = 2097,152 networks in the world that can have a class C address.

Class D is not divided into prefix and suffix. It is used for multicast addresses. All addresses that start with 1111 in binary belong to class E.



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Fig2.6.2: Address space in classful addressing.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-531]

Address Depletion

Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet.

To understand the problem,let us think about class A. This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network). Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).

Advantage of Classful Addressing

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately.

With the growth of the Internet, it was clear that a larger address space was needed. The larger address space, requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed. The available address should be distributed to all organizations. This is called classless addressing. In other words, the class privilege was removed from the distribution to compensate for the address depletion.

In classless addressing, the whole address space is divided into variable length blocks as shown in Figure 2.6.3.The prefix in an address defines the block (network); the suffix defines the node(device).

Theoretically, we can have a block of 2^0, 2^1, 2^2, ..2^{32} addresses.

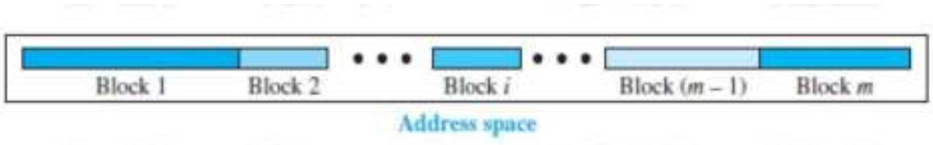


Fig2.6.3: Variable length blocks in classless addressing.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-532]

A small prefix means a larger network; a large prefix means a smaller network.

Prefix Length: Slash Notation

The first question that we need to answer in classless addressing is how to find the prefix length if an address is given. Since the prefix length is not inherent in the address,we need to separately give the length of the prefix. In this case, the prefix length, *n*, is added to the address, separated by a slash.

The notation is informally referred to as slash notation and formally as classless inter domain routing or CIDR (pronounced cider) strategy. An address in classless addressing can then be represented as shown in Figure 2.6.4.

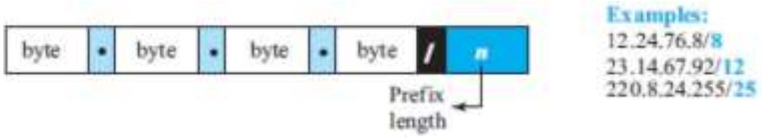


Fig2.6.4: Slash notation.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-533]

Extracting Information from an Address

Given any address in the block, we normally like to know three pieces of information about the block to which the address belongs: the number of addresses, the first address in the block, and the last address. Since the value of prefix length, *n*, is given, we can easily find these three pieces of information, as shown in Figure 2.6.5.

The number of addresses in the block is found as N =$2^{32-n.}$

To find the first address, we keep the n leftmost bits and set the (32 -n) right most bits all to 0s. To find the last address, we keep the n leftmost bits and set the (32 - n) right most bits all to 1s.

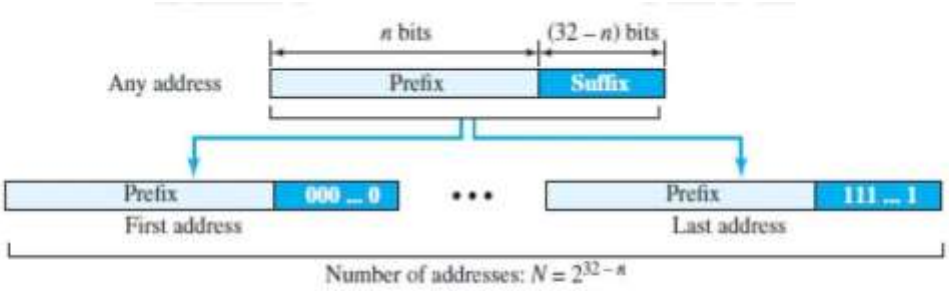


Fig2.6.5:Information extraction.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-534]

2.7 .7 NETWORK-LAYER PROTOCOLS

INTERNET PROTOCOL (IP)

The protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer. IP layer position is shown in figure 2.7.1.

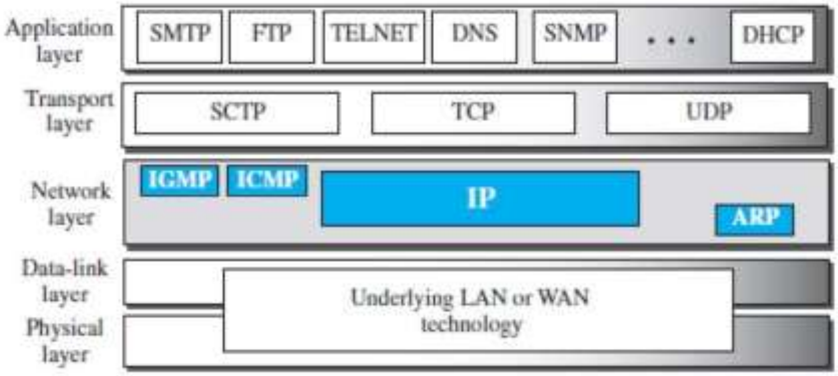


Fig2.7.1: Position of IP and other layers .

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-562]

IPv4 is also a connectionless protocol that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order.

Datagram Format

Packets used by the IP are called datagrams.

Figure 2.7.2 shows the IPv4 datagram format. A datagram is a variable length packet consisting of two parts: header and payload (data). The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

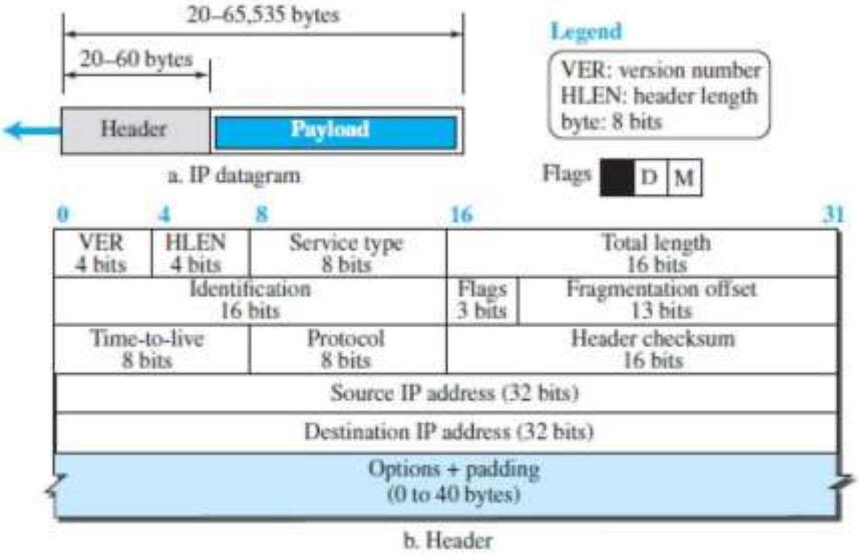


Fig2.7.2: IP datagram.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-563]

Version Number.The 4-bit version number (VER) field defines the version of theIPv4 protocol, which, has the value of 4.

Header Length.The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.

Service Type. This field is called as type of service (TOS), which defined how the datagram should be handled.

Total Length.This 16-bit field defines the total length (header plus data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1s).

Identification, Flags, and Fragmentation Offset. These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

Time-to-live.Due to some malfunctioning of routing protocols a datagram may be circulating in the Internet, visiting some networks over and over without reaching the destination.

This may create extra traffic in the Internet.

The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram.

Protocol.In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol.

A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP. A datagram can also carry a packet from other protocols that directly use the service of the IP.

Header check sum.IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP. The datagram header, is added by IP, and its error-checking is the responsibility of IP.

Errors in the IP header can be a disaster. For example, if the destination IP address is corrupted, the packet can be delivered to the wrong host.

If the protocol field is corrupted, the payload may be delivered to the wrong protocol. If the fields related to the fragmentation are corrupted, the datagram cannot be reassembled correctly at the destination.

Source and Destination Addresses.

The 32-bit source and destination address fields define the IP address of the source and destination respectively.The source host should know its IP address. The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS.

Options.A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging.

Payload. Payload, or data, is the main reason for creating a datagram.

Payload is the packet coming from other protocols that use the service of IP.Comparing a datagram to a postal package, payload is the content of the package. In order to make the IP protocol independent of the physical network, the designers decided to make the maximum length of the IP datagram equal to 65,535 bytes. For physical networks, we must divide the datagram to make it possible for it to pass through these networks. This is called fragmentation.

When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some have been changed.A datagram can be fragmented by the source host or any router in the path. The Reassembly of the datagram, however, is done only by the destination host, because each fragment becomes an independent datagram.

The fragmented datagram can travel through different routes, and we can never control or guarantee which route a fragmented datagram may take, all of the fragments belonging to the same datagram should finally arrive at the destination host.

Three fields in an IP datagram are related to fragmentation: identification, flags, and fragmentation offset.

The 16-bit identification field identifies a datagram originating from the source host. The combination of the identification and source IP address must uniquely define a datagram as it leaves the source host.To guarantee uniqueness, the IP protocol uses a counter to label the datagrams. The counter is initialized to a positive number.

When the IP protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one. As long as the counter is kept in the main memory, uniqueness is guaranteed.

When a datagram is fragmented,the value in the identification field is copied into all fragments. In other words, all fragments have the same identification number, which is also the same as the original datagram. The identification number helps the destination in reassembling the datagram.

Note: All fragments having the same identification value should be assembled into one datagram.

The 3-bit flags field defines three flags.

The leftmost bit is reserved (not used). The second bit (D bit) is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram.If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host .If its value is 0, the datagram can be fragmented if necessary. The third bit (M bit) is called the more fragment bit.If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment.

MOBILE IP

Mobile IP is the extension of IP protocol that allows mobile computers to be connected to the internet at any location where the connection is possible.

Stationary Hosts

The original IP addressing was based on the assumption that a host is stationary, attached to one specific network. A router uses an IP address to route an IP datagram. For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8. This implies that a host in the Internet does not have an address that it can carry with itself from one place to another.

The address is valid only when the host is attached to the network. If the network changes, the address is no longer valid. Routers use this association to route a packet; they use the prefix to deliver the packet to the network to which the host is attached. This scheme works perfectly with stationary hosts.

Mobile Hosts

When a host moves from one network to another, the IP addressing structure needs to be modified.

Changing the Address

One simple solution is to let the mobile host change its address as it goes to the new network. The host can use DHCP to obtain a new address to associate it with the new network. This approach has several drawbacks. First, the configuration files would need to be changed. Second, each time the computer moves from one network to another, it must be rebooted. Third, the DNS tables need to be revised so that every other host in the Internet is aware of the change. Fourth, if the host roams from one network to another during a transmission, the data exchange will be interrupted. This is because the ports and IP addresses of the client and the server must remain constant for the duration of the connection.

Two Addresses

The approach that is more feasible is the use of two addresses. The host has its original address, called the **home address,** and a temporary address, called the **care-of address.** The home address is permanent; it associates the host with its home network, the network that is the permanent home of the host. The care-of address is temporary. When a host moves from one network to another, the care-of address changes; it is associated with the foreign network, the network to which the host moves. Figure 2.7.3 shows the concept.

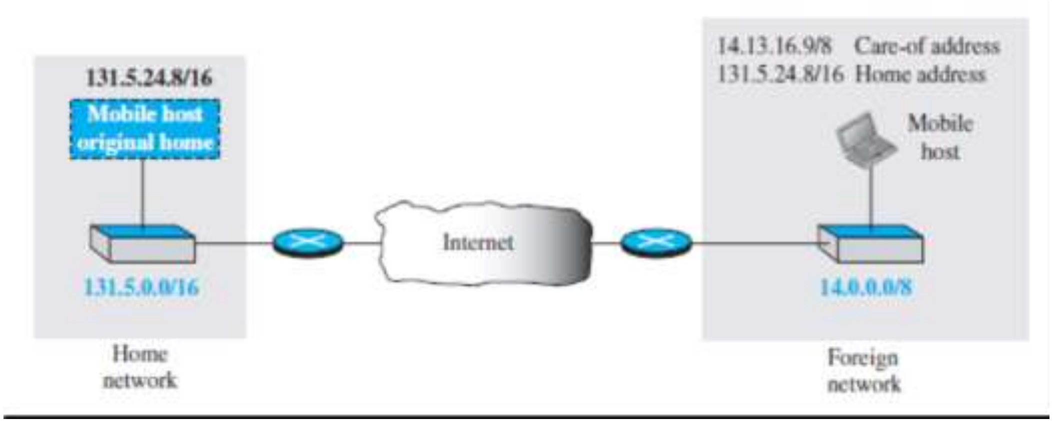


Fig2.7.3: Home address and care-of address

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-582]

ICMP

The Internet Control Message Protocol version 4 (ICMPv4) is a network-layer protocol.

When an IP datagram encapsulates an ICMP message, the value of the protocol field in the IP datagram is set to 1 to indicate that the IP payroll is an ICMP message.

ICMP messages are divided into two categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host(destination) may encounter when it processes an IP packet.

The query messages, help a host or a network manager get specific information from a router or another host.

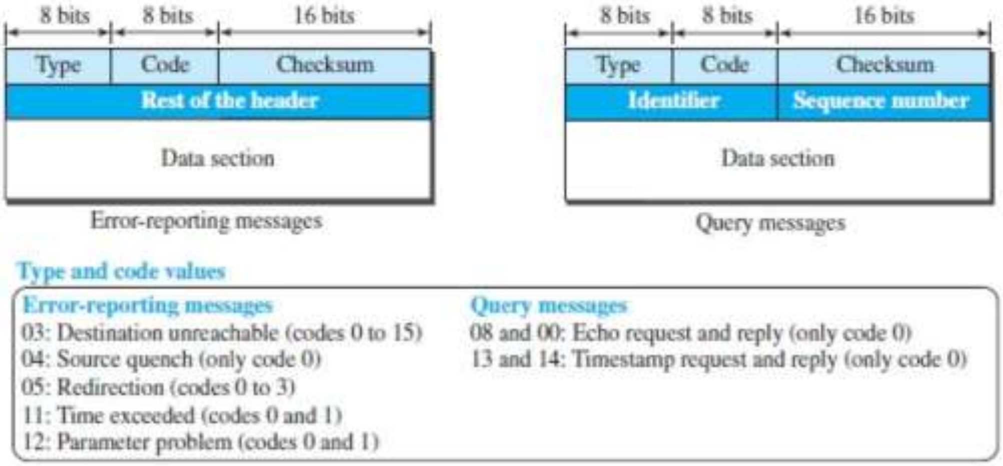
For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages. An ICMP message has an 8-byte header and a variable-size data section. The first 4 bytes are common to all. The first field, ICMP type, defines the type of the message.The code field specifies the reason for the particular message type. The last common field is the checksum field.

Error Reporting Messages

One of the main responsibilities of ICMP is to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them. Error correction is done by the higher-level protocols.The format is shown in figure 2.7.4.

Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses. ICMP uses the source IP address to send the error message to the source (originator) of the datagram. To make the error-reporting process simple, ICMP follows some rules in reporting messages.

First, no error message will be generated for a datagram having a multicast address or special address (such as this host or loopback).Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.



Type and code values

Error-reporting messages
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages
08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Fig2.7.4: The format of ICMP messages.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-575]

Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram.

The original datagram header is added to give the original source, which receives the error message,information about the datagram itself.

The 8 bytes of data are included because the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCPor UDP) about the error. Data field is shown in figure 2.7.5.

Destination Unreachable

The most widely used error message is the destination unreachable (type 3). This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.

For example, code 0 tells the source that a host is unreachable.

This may happen, for example, when we use the HTTP protocol to access a web page, but the server is down. The message "destination host is not reachable" is created and sent back to the source.

Source Quench

Source quench (type 4) message informs the sender, that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.

Redirection Message

The redirection message (type 5) is used when the source uses a wrong router to send out its message.

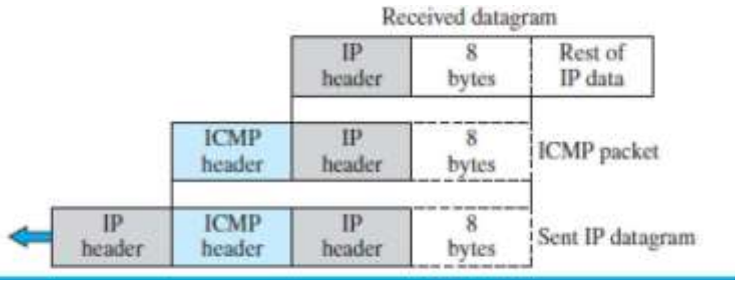


Fig2.7.5: The Contents of data field.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-577]

The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.

Parameter Problem

A parameter problem message (type 12) can be sent when either there is a problem inthe header of a datagram (code 0) or some options are missing or cannot be interpreted(code 1).

Query Messages

Query messages in ICMP can be used independently without relation to an IP datagram. A query message needs to be encapsulated in a datagram, as a carrier.

Query messages are used to test the liveliness of hosts or routers inthe Internet, find the one-way or the round-trip time for an IP datagram between two devices, or even find out whether the clocks in two devices are synchronized.

Query messages pairs: request and reply.

The echo request (type 8) and the echo reply (type 0) pair of messages are used bya host or a router to test the liveliness of another host or router.

A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.

The timestamp request (type 13) and the timestamp reply (type 14) pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.The timestamp request message sends a 32-bitnumber, which defines the time the message is sent. The timestamp reply resends that number, and includes two new 32-bit numbers representing the time the request was received and the time the response was sent.

Deprecated Messages

Three pairs of messages are declared obsolete by IETF:

Information request and replay messages are not used today because their duties are done by the Address Resolution Protocol (ARP).

Address mask request and reply messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

Router solicitation and advertisement messages are not used today because their duties are done by the Dynamic Host Configuration Protocol (DHCP).

2.5 NETWORK LAYER SERVICES

The main duty of the network layer is packetizing. Packetizing means encapsulating the payload(data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network layer packet at the destination.Encapsulation means adding the payload in the network layer.

In other words, one duty of the network layer is to carry a payload from the source to the destination without changing it or using it.

The network layer is doing the service of a carrier such as the postal office, which is responsible for delivery of packages from a sender to a receiver without changing or using the contents.

The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and some other information that is required by the network-layer protocol and delivers the packet to the data-link layer. The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented.

The destination host receives the network-layer packet from its data-link layer, decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.

If the packet is fragmented at the source or at routers along the path, the network layer is responsible for waiting until all fragments arrive, reassembling them, and delivering them to the upper-layer protocol.The routers in the path are not allowed to de capsulate the packets they received unless the packets need to be fragmented. The routers are not allowed to change source and destination addresses either. They just inspect the addresses for the purpose of forwarding the packet to the next network on the path.

Routing and Forwarding

The network layer is responsible for routing the packet from its source to the destination.

A physical network is a combination of networks (LANs and WANs) and routers that connect them. This means that there is more than one route from the source to the destination. The network layer is responsible for finding the best one among these possible routes. The network layer needs to have some specific strategies for defining the best route.

Forwarding

If routing is applying strategies and running some routing protocols to create the decision-making tables for each router, then forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.

The decision-making table used by the router for applying this action is called the forwarding table and sometimes the routing table.When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (in unicast routing) or to some attached networks (in multicast routing).

Figure2.5.1 shows the forwarding process in a router.

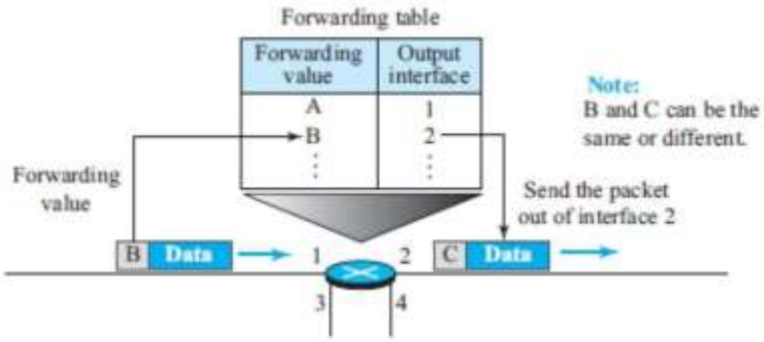


Fig2.5.1: The forwarding process in a router.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-514]

Congestion Control

Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet.

Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers. In this situation, some routers may drop some of the datagrams.

Quality of Service

Internet has lot of new applications such as multimedia communication (in particular real-time communication of audio and video), the quality of service (QoS) of the communication has become more and more important.The Internet has taken more effort to provide better quality of service to support these applications.

Security

Today, security is a big concern. To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service.

PACKET SWITCHING

Packet switching is a network transmission process in which data is broken into suitably-sized pieces or blocks for fast and efficient transfer via different network devices.

When a computer attempts to send a file to another computer, the file is broken into packets so that it can be sent across the network in the most efficient way. These packets are then routed by network devices to the destination.

There are two major modes of packet switching:

1. Connectionless Packet Switching: Each packet contains complete addressing or routing information and is routed individually.This can result in out-of-order delivery and different paths of transmission, depending on the variable loads on different network nodes (adapters, switches and routers) at any given time. This is called as datagram switching.

In connectionless packet switching, each packet has the following information written in its header section:

The destination address

The source address

Total number of pieces

The sequence number needed to enable reassembly

After reaching the destination through different routes, the packets are rearranged to form the original message.

2. Connection-Oriented Packet Switching: Data packets are sent sequentially over a predefined route. Packets are assembled, given a sequence number and then transported over the network to a destination in order. In this mode, address information is not required. This is called virtual circuit switching.

Datagram Approach: Connectionless Service

The network layer was designed to provide a connectionless service in which the network-layer protocol treats each packet independently, with each packet having no relationship to any other packet. Figure 2.5.2 shows the conceptual idea.

When the network layer provides a connectionless service, each packet traveling in the Internet is an independent entity; there is no relationship between packets belonging to the same message. The switches in this type of network are called routers.

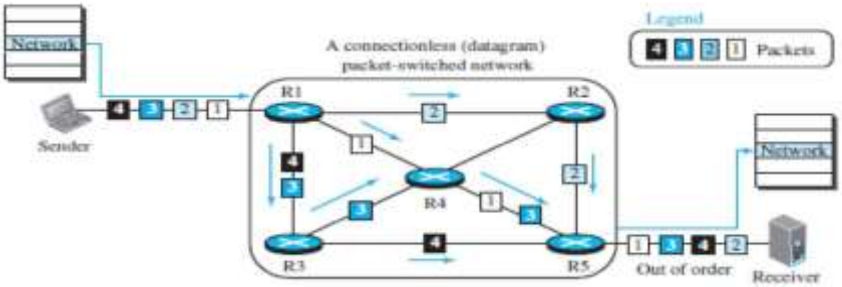


Fig2.5.2:Connectionless packet switched network.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-517]

Each packet is routed based on the information contained in its header: source and destination addresses.The router in this case routes the packet based only on the destination address. The source address may be used to send an error message to the source if the packet is discarded.

Virtual-Circuit Approach: Connection-Oriented Service

In a connection-oriented service (also called virtual-circuit approach), there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can all follow the same path.

In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow. Figure 2.5.3 shows the concept of connection-oriented service.

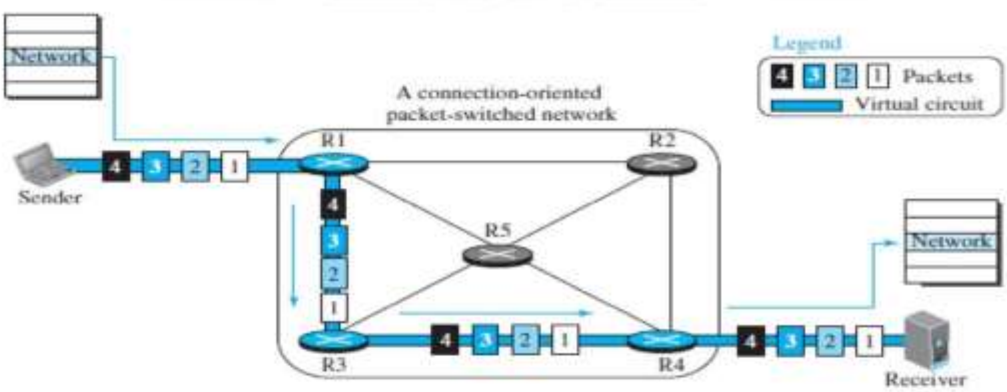


Fig2.5.3: Connection oriented packet switched network.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-518]

To create a connection-oriented service ,a three-phase process is used:

1.setup 2.data transfer 3.teardown.

In the setup phase, the source and destination addresses of the sender and receiver are used to make table entries for the connection-oriented service.

In the teardown phase, Source A, after sending all packets to B, sends a special packet called a teardown packet. Destination B responds with a confirmation packet. All routers delete the corresponding entries from their tables.

Data-Transfer Phase

The second phase is called the data-transfer phase. After all routers have created their forwarding table for a specific virtual circuit, then the network-layer packets belonging to one message can be sent one after another.

Advantages of Packet switching

Set up time and teardown time is less

Improved bandwidth

More flexible

Disdvantages

Complex algorithms are used

Complex protocols are required

Packet loss may occur

UNIT 2 MEDIA ACCESS AND INTERNETWORKING

2.1 OVERVIEW OF DATA LINK CONTROL

The data link control (DLC) deals with procedures for communication between two adjacent nodes.ie: node-to-node communication.No matter whether the link is dedicated or broadcast.

The functions of Data link control are as follows:

Framing, flow and error control.

Framing

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination.The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing.

The main function of Framing:

Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address.The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Frames can be of two types: Fixed or variable size.

In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM WAN, which uses frames of fixed size called cells.

In variable-size framing, we need a way to define the end of one frame and the beginning of the next.

Character-Oriented Framing

In character-oriented (or byte-oriented) framing as shown in figure 2.1.1, data to be carried are 8-bit characters from a coding system such as ASCII. Here 8 bit data is used.The header, normally carries the source and destination addresses and other control information, and the trailer, which carries error detection redundant bits, and multiples of 8 bits. To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

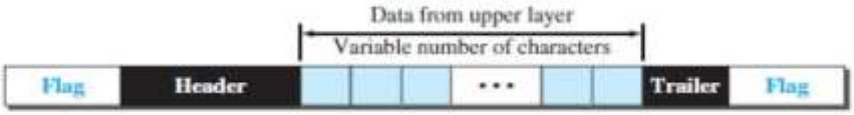


Fig2.1.1: Frame in character oriented protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-295]

We can also send other types of information such as graphs, audio, and video; any character used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame.

To overcome this problem, a byte-stuffing strategy was added to character oriented framing.

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.

The data section is stuffed with an extra byte as in figure 2.1.2 . This byte is called the escape character (ESC) and has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.

.

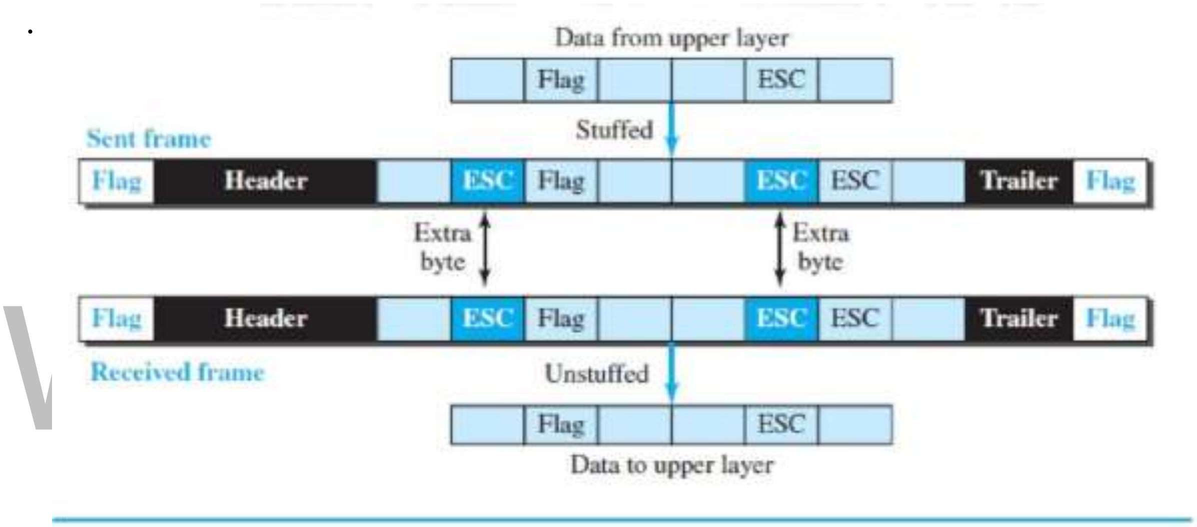


Fig2.1.2: Byte stuffing and unstuffing .

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-295]

Bit-Oriented Framing

In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.In addition to headers ,we need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame, as shown in Figure .

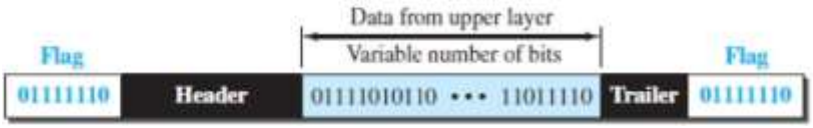


Fig2.1.3: Bit oriented framing.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-296]

If the flag pattern appears in the data, we need to inform the receiver that this is not the end of the frame.By stuffing 1 single bit(instead of 1 byte) we can prevent the pattern from looking like a flag. This strategy is called bit stuffing.

In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra0 is added as shown in figure 2.1.3. This extra stuffed bit is eventually removed from the data by the receiver.Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

Flow and Error Control

Flow Control

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates. If the items are produced faster than they can be consumed, the consumer can be overwhelmed and may need to discard some items.

Flow control is implemented to prevent traffic.

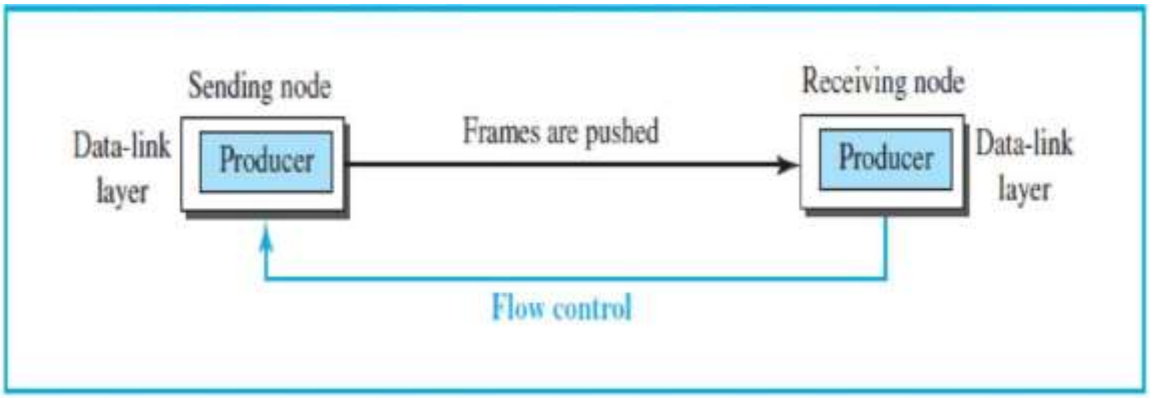


Fig2.1.4: Flow control at the data-link layer .
[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-297]

In the figure2.1.4, the data-link layer at the sending node tries to push frames towards the data-link layer at the receiving node. If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes over whelmed (traffic) with frames.

Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

Buffers

Although flow control can be implemented in several ways, one of the solutions is normally to use two buffers; one at the sending data-link layer and the other at the receiving data-link layer.

A buffer is a set of memory locations that can hold packets at the sender and receiver.

Error Control

Error control at the data-link layer is very simple and implemented using one of the following two methods. In both methods, a CRC is added to the frame header by the sender and checked by the receiver.

In the first method, if the frame is corrupted, it is silently discarded; if it is not corrupted,the packet is delivered to the network layer. This method is used mostly in wired LANs such as Ethernet.

In the second method, if the frame is corrupted, it is silently discarded; if it is not corrupted, an acknowledgment is sent (for the purpose of both flow and error control)to the sender.

DATA-LINK LAYER PROTOCOLS

The behavior of a data-link-layer protocol is shown as a finite state machine (FSM). An FSM is a machine with a finite number of states. The machine is always in one of the states until an event occurs.

Each event has two reactions: defining the list (possibly empty) of actions to be performed and determining the next state (which can be the same as the current state). One of the states must be defined as the initial state, the state in which the machine starts when it turns on.

Here rounded-corner rectangles are used to show states, colored text to show events, and regular black text to show actions.A horizontal line is used to separate the event from the actions. The arrow shows the movement to the next state.There are only three possible events and three possible actions. The machine starts in state I. If event 1 occurs, the machine performs actions 1 and 2 and moves to state II. When the machine is in state II, two events may occur.

If event 1 occurs, the machine performs action 3 and remains in the same state, state II. If event 3 occurs, the machine performs no action, but move to state I.

Simple Protocol

This is a simple protocol with neither flow nor error control. Assume that the receiver can immediately handle any frame it receives. In other words, the receiver can be free of congestion with incoming frames. Figure2.1.5 shows the layout for this protocol.

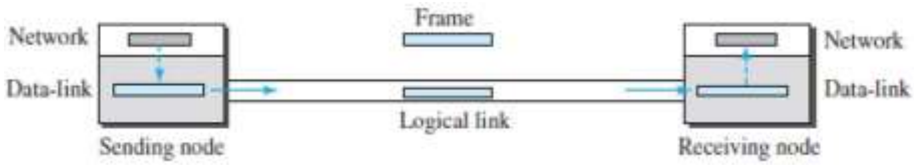


Fig2.1.5: Layout of simple protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-300]

The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame. The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.

FSMs (Description of Simple protocol function)

The sender should not send a frame until its network layer has a message to send.The receiver site cannot deliver a message to its network layer until a frame arrives. Requirements are based on two FSMs. Each FSM has only one state, the ready state as shown in figure 2.1.6.

The sending machine remains in the ready state until a request comes from the process in the network layer. When this event occurs, the sending machine encapsulates the message in a frame and sends it to the receiving machine.

The receiving machine remains in the ready state until a frame arrives from the sending machine. When this event occurs, the receiving machine decapsulates the message out of the frame and delivers it to the process at the network layer.

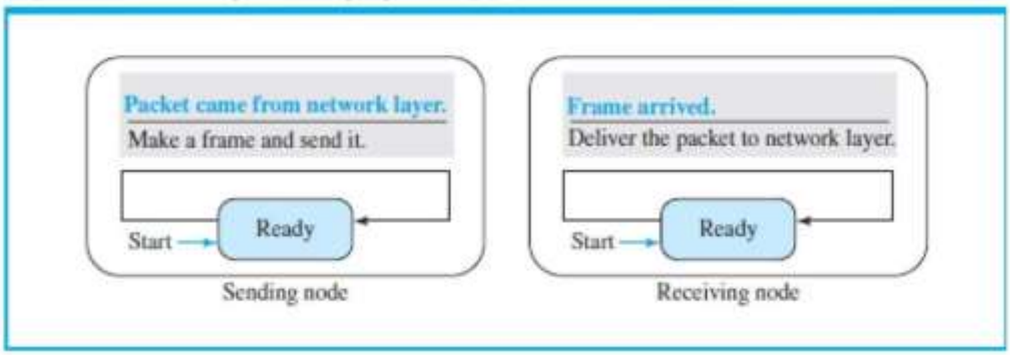

Packet came from network layer.
Make a frame and send it.
Start
Ready
Sending node
Frame arrived.
Deliver the packet to network layer.
Start
Ready
Receiving node

Fig2.1.6: FSM for simple protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-301]

Stop-and-Wait Protocol

Stop-and-Wait protocol, uses both flow and error control.In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, we need to add a CRC to each data frame shown in figure 2.1.7.

When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost.

Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keepa copy of the frame until its acknowledgment arrives.

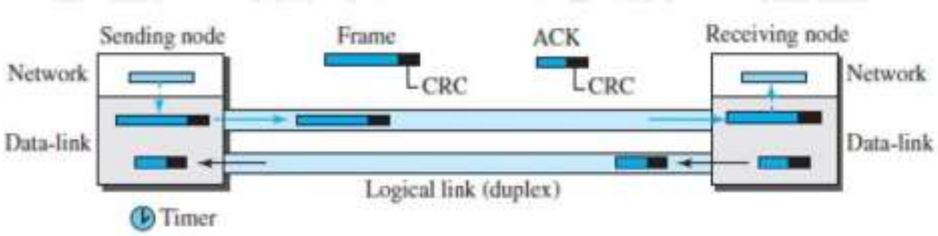


Fig2.1.7: Stop and wait protocol .

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-302]

FSM (Finite State Machine)

Figure 2.1.8 shows the FSMs for the Stop-and-Wait protocol. Sender and receiver states are described as follows.

Sender States

The sender is initially in the ready state, but it can move between the ready and blocking state.

Ready State.When the sender is in this state, it is only waiting for a packet from the network layer. If a packet comes from the network layer, the sender creates a frame, saves a copy of the frame, starts the only timer and sends the frame. The sender then moves to the blocking state.

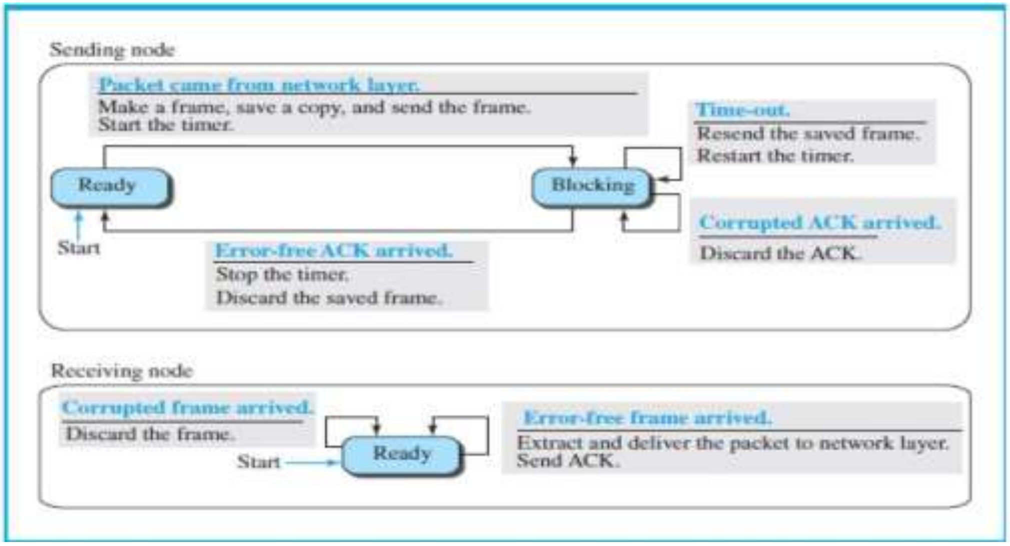


Fig2.1.8: FSM for the stop and wait protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-302]

Blocking State .1.When the sender is in this state, three events can occur:

If a time-out occurs, the sender resends the saved copy of the frame and restarts the timer.

2.If a corrupted ACK arrives, it is discarded.

3.If an error-free ACK arrives, the sender stops the timer and discards the saved copy of the frame. It then moves to the ready state.

Receiver

The receiver is always in the *ready* state. Two events may occur:

1.If an error-free frame arrives, the message in the frame is delivered to the network layer and an ACK is sent. If a corrupted frame arrives, the frame is discarded.

2.4 WIRELESS LAN

Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

Architecture of wired and wireless LAN

In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).

In a wireless LAN, a host is notphysically connected to the network; it can move freely and can use the services provided by the network.

IEEE 802.11 PROJECT

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11.

Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN.

A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture.

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network.

The distribution system connects the APs in the BSSs. IEEE802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. The extended service set uses two types of stations: mobile and stationary.The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 2.4.1 shows an ESS.

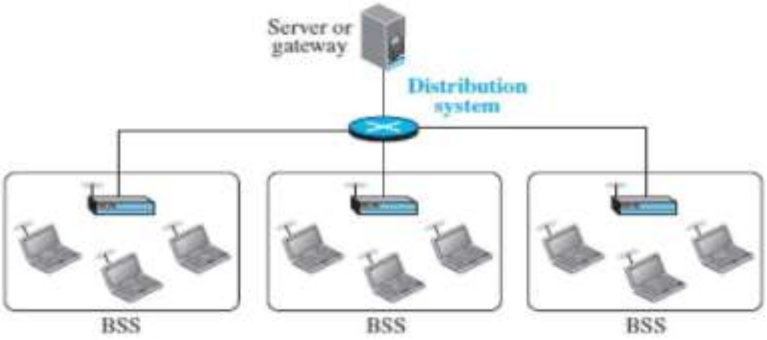


Fig 2.4.1 :Extended service set.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-441]

Station Types – Three stations

A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS. A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS. A station with ESS-transition mobility can move from one ESS to another.

MAC Sublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF).Figure 2.4.2 shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.

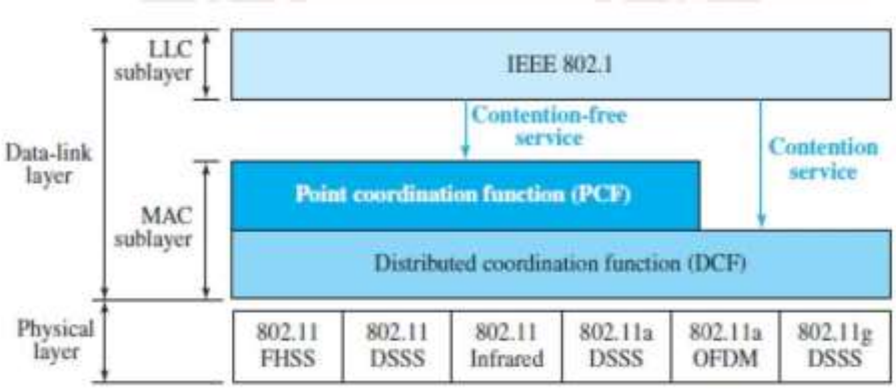


Fig 2.4.2:MAC layers.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-442]

Distributed Coordination Function

One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method.

Figure 2.4.3 shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.The channel uses a persistence strategy with back off until the channel is idle.After the station is found to be idle, the station waits for a period of time called the distributed inter frame space (DIFS); then the station sends a control frame called the request to send (RTS).

2.After receiving the RTS and waiting a period of time called the short inter frame space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station.

This control frame indicates that the destination station is ready to receive data.The source station sends data after waiting an amount of time equal to SIFS.The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

Hidden-Station Problem

The solution to the hidden station problem is the use of the handshake frames (RTS andCTS). Figure 2.4.3 shows that the RTS message from B reaches A, but not C. However,because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A, reaches C. Station C knows that some hidden station is using the channel and wait for some time from transmitting until that duration is over.

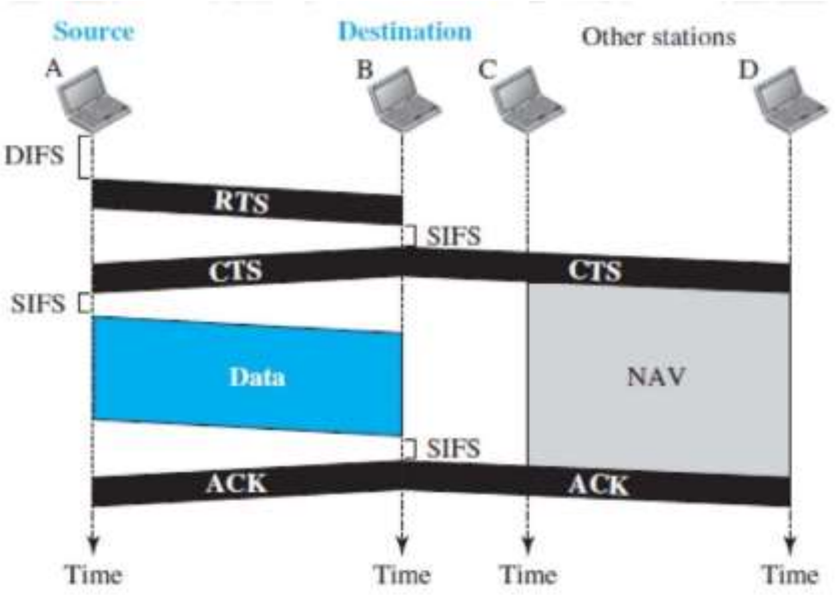


Fig 2.4.3:Hidden station problem.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-442]

Frame Format

The MAC layer frame consists of nine fields as in figure 2.4.4.

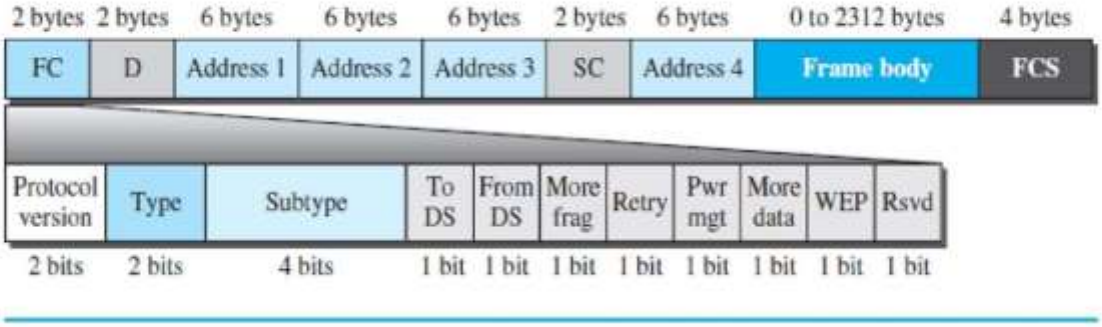


Fig2.4.4: MAC layer frame.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-444]

Frame control (FC). The FC field is 2 bytes long and defines the type of frame and some control information.

D. This field defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

Addresses.There are four address fields, each 6 bytes long. The meaning of eac h address field depends on the value of the To DS and From DS subfields and will be discussed later.

Sequence control.This field, often called the SC field, defines a 16-bit value.

The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

Frame body. This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

FCS.The FCS field is 4 bytes long and contains a CRC-32 error-detection sequence.

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames: Management frames, control frames, and data frames.

Management Frames: Management frames are used for the initial communication between stations and access points.

Control Frames: Control frames are used for accessing the channel and acknowledging frames. Figure2.4.5 shows the format.

Data Frames:Data frames are used for carrying data and control information.

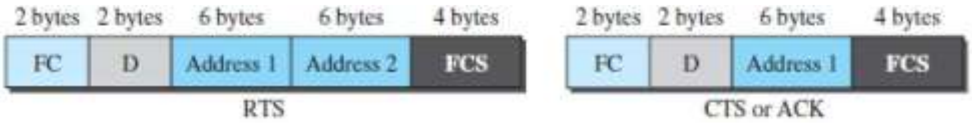


Fig2.4.5:Control frames.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-446]

Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS.

Each flag can be either 0 or 1, resulting in four different situations.

Address 1 is always the address of the next device that the frame will visit.

Address 2 is always the address of the previous device that the frame has left. Address 3is the address of the final destination station if it is not defined by address 1 or the original source station if it is not defined by address 2.

Address 4 is the original source when the distribution system is also wireless.

DS- Distributed system

Case 1: 00 In this case, To DS =0 and From DS =0. This means that the frame is not going to a distribution system (To DS =0) and is not coming from a distribution system (From DS =0).

The frame is going from one station in a BSS toanother without passing through the distribution system.

Case 2: 01 In this case, To DS =0 and From DS =1. This means that the frame is coming from a distribution system (From DS =1). The frame is coming from an AP and going to a station.

Note that address 3 contains the original sender of the frame (in another BSS).

Case 3: 10 In this case, To DS =1 and From DS =0. This means that the frame is going to a distribution system (To DS=1). The frame is going from a station to an AP. The ACK is sent to the original station.

Note that address 3 contains the final destination of the frame in the distribution system.

Case 4: 11 In this case, To DS =1 and From DS =1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system. Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

Exposed Station Problem

In this problem a station refrains from using a channel when it is, available.

In Figure 2.4.6 , station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.

Here, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

The handshaking messages RTS and CTS cannot help in this case.

Station C hears the RTS from A and refrains from sending, eventhough the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.

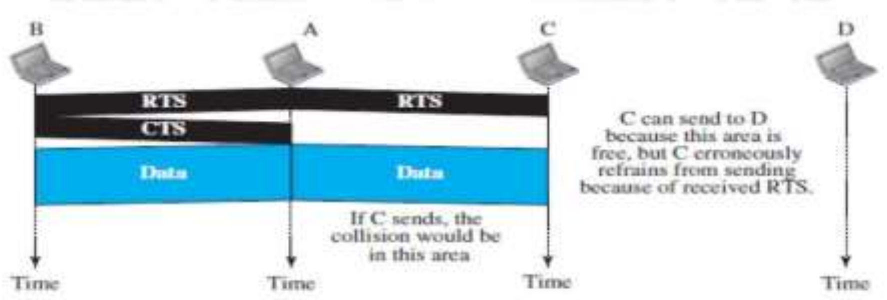

B
A
C
D
RTS
RTS
CTS
Data
Data
C can send to D because this area is free, but C erroneously refrains from sending because of received RTS.
If C sends, the collision would be in this area
Time
Time
Time
Time

Fig 2.4.6: Exposed Station Problem.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-448]

2.8 ZIGBEE

Zigbee is a personal area network standardized by the IEEE is the 802.14.5 standard.

Zigbee is operated at low powered,lower-data-rate, lower-duty-cycle applications.

For example, home temperature and light sensors, security devices, and wall mounted switches are all very simple, low-power, low-duty-cycle, low-cost devices.

Zigbee defines channel rates of 20, 40,100, and 250 Kbps, depending on the channel frequency.

Nodes in a Zigbee network come in two flavors.

Reduced-function devices" operate as slave devices under the control of a single "fullfunction device," much as Bluetooth slave devices.

A full-function device can operate as a master device as in Bluetooth by controlling multiple slave devices, and multiple full-function devices can additionally be configured into a mesh network in which full-function devices route frames amongst themselves. Zigbee shares many protocol mechanisms such as beacon frames and link-layer acknowledgments (similar to 802.11),carrier-sense random access protocols with binary exponential backoff (similar to 802.11 and Ethernet), and fixed, guaranteed allocation of time slots .

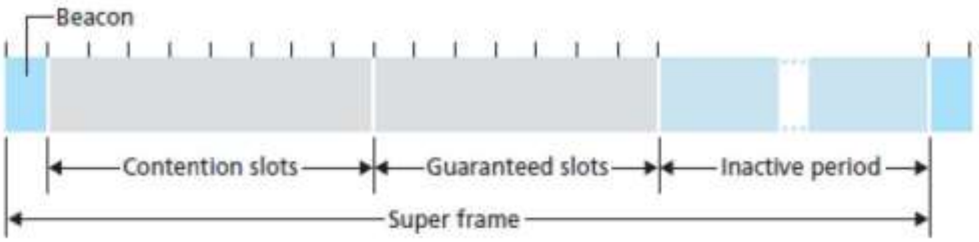


Fig2.8.1: Zigbee super frame structure.
[Source : Computer Networking, top down approach byKuroze ross,Page-546]

Zigbee Configuration

Zigbee networks can be configured in many different ways.

Consider a single full-function device controlling multiple reduced-function devices in a time-slotted manner using beacon frames. Figure 2.8.1 shows the case where the Zigbee network divides time into recurring super frames, each of which begins with a beacon frame.

Each beacon frame divides the super frame into an active period (during which devices may transmit) and an inactive period (during which all devices, including the controller, can sleep and thus conserve power).

The active period consists of 16 time slots, some of which are used by devices in a CSMA/CA random access manner, and some of which are allocated by the controller to specific devices, thus providing guaranteed channel access for those devices.

WiFi Technology

Wireless fidelity (WiFi) a term trademarked by the WiFi Alliance technology is a set of standards for wireless local area networks (WLANs).

WiFi allows mobile devices, such as laptop computers, digital cameras, and personal digital assistants (PDAs), to connect to local area networks. WiFi is also intended for Internet access and wireless voice over IP (VoIP) phones.

WiFi networks can be connected to the Internet through wireless routers with gateway/bridge.

A wireless router with gateway/bridge is a router that can provide radio communications to certain wireless access points, as well as routing to wired Internet devices.

Such router/gateways can also communicate with one another.

For example, if we consider two routers A and B are communicating directly to establish connection for WiFi users 1 and 2; these two users could also be connected through the Internet.

However, because an Ethernet uses contention access in WiFi, all users wanting to pass data through an access point contend for its attention on a random basis.

The connection is made by radio link signals. A hotspot is defined as an access point in a geographical region covered by WiFi.

The range of an access point built into a typical WiFi home router is 50 meters indoors and 90 meters outdoors.

WiFi is based on the IEEE 802.11 standard.

The most widespread version of WiFi is based on IEEE 802.11b/g operating over 11 channels (5 MHz each), centered on Channel 1 at 2,412 MHz all the way to Channel 11 at 2,462 MHz.

Several routing protocols are used to set up WiFi devices. One of these protocols is the Optimized Link State Routing (OLSR) protocol developed for mobile networks.

OLSR operates as a table-driven and proactive protocol. Thus, it regularly exchanges topology information with other nodes of the network. Nodes are selected as multipoint relays by some neighboring nodes. They exchange this information periodically in their control messages.

With WiFi, most networks rely heavily on open source software or even publish their setup under an open source license. WiFi allows LANs to be deployed without cabling, thereby lowering the cost of network deployment and expansion. WiFi may be used in places where cables cannot be laid. The use of the 2.4 GHz WiFi band does not require a license in most of the world, provided that one stays below the local regulatory limits and accepts interference from other sources, including interference that causes devices to no longer function.

6 LoWPAN

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), is a low power wireless mesh network where every node has its own IPv6 address. This allows the node to connect directly with the Internet using open standards.

6LoWPAN came to exist from the idea that the Internet Protocol could and should be applied even to the smallest devices, and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.

- It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets.
- It offers end-to-end IP addressable nodes. There’s no need for a gateway, only a router which can connect the 6LoWPAN network to IP.
- It supports self-healing, robust and scalable mesh routing.
- Offers one-to-many & many-to-one routing.
- The 6LoWPAN mesh routers can route data to others nodes in the network.
- In a 6LowPAN network, leaf nodes can sleep for a long duration of time.
- It also offers thorough support for the PHY layer which gives freedom of frequency band & physical layer, which can be used across multiple communication platforms like Ethernet, WI-Fi, 802.15.4 or Sub-1GHz ISM with interoperability at the IP level.
- It is a standard: RFC6282

6LoWPAN protocol stack is shown in figure 2.8.2

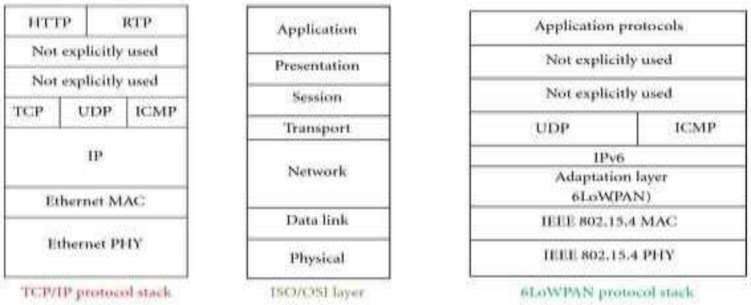


Fig2.8.2: 6LoWPAN protocol stack.

[Source : https://radiocrafts.com/technologies/6lowpan]

6LoWPAN Application Areas

With many low power wireless sensor networks and other forms of wireless networks designed to tackle specific problems, it is essential that any new wireless system has a defined area which it addresses. While there are many forms of wireless networks including wireless sensor networks, 6LoWPAN addresses an area that is currently not addressed by any other system, for example, that of using IP, and in particular IPv6 to carry the data.

The overall system is aimed at providing wireless internet connectivity at low data rates and with a low duty cycle. However, there are many applications where 6LoWPAN is being used:

- **Automation:**There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- **Industrial monitoring:** Industrial plants and automated factories provide a great opportunity for 6LoWPAN. Major savings can be made by using automation in every day practices. Additionally, 6LoWPAN can connect to the cloud which opens up many different areas for data monitoring and analysis.
- **Smart Grid:** Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator’s monitoring and billing system using the IPv6.
- **Smart Home:**By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

6LoWPAN Security

6LoWPAN can use AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.Further security is provided by the transport layer security mechanisms. This is defined in RFC 5246 and runs over TCP.

For systems where UDP is used, the transport layer protocol defined under RFC 6347 can be used.