Kalinga University

Department of Computer Science &Information Technology

Course:BCAAIML **Semester: IV**

Subject: Computer Network

Subject Code: BCAAIML403

UNIT – III

RandomAccess:

ALOHA

In the 1970s, a significant breakthrough was made by Norman Abramson and his colleagues at the University of Hawaii. They devised a new and elegant method, known as the ALOHA system, to solve the channel allocation problem. This work has since been extended by numerous researchers, marking a crucial milestone in the field of computer networks (Abramson,1985).

AlthoughAbramson'swork,calledtheALOHAsystem,usedground-basedradiobroadcasting,the basic idea applies to any system in which uncoordinated users compete for a single shared channel. There are two versions of ALOHA: pure and slotted. They differ concerning whether time is divided into discrete slots that all frames must fit. Pure ALOHA does not require global time synchronisation; slotted ALOHA does.

Pure ALOHA:

The basic idea of an ALOHA system is simple: let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. However, due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way other users do. With a LAN, the feedback is immediate;withasatellite,thereisadelayof270msecbeforethesenderknowsifthetransmission was successful. If listening while transmitting is not possible for some reason, acknowledgements are needed. If the frame is destroyed, the sender waitsarandom amount of time and sends it again. The waiting time must be random or the same frames will collide repeatedly, in lockstep. Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contentionsystems.

For a clearer understanding, let's take a look at a visual representation of frame generation in an ALOHA system (see Fig.1). In this illustration, we've made the frames all the same length. This is because the throughput of ALOHA systems is maximized by having a consistent frame length.

Uniform frame size rather than allowing variable length frames.

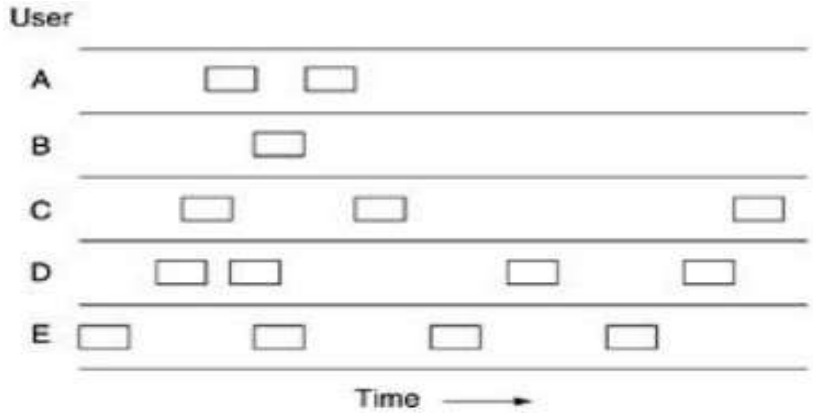


Fig.1 In pure ALOHA, frames are transmitted at completely arbitrary times.

Whenever two frames try to occupy the channel at the same time, they will collide, and both will be garbled. If the first bit of a new frame overlaps with just the last bit of an almost-finished frame, both frames will be destroyed, and both will have to be retransmitted later. The checksum cannot (and should not) distinguish between a total loss and a nearmiss.

Let the "frame time" denote the time needed to transmit the standard, fixed-length frame (i.e., the frame length divided by the bit rate). At this point, we assume that the infinite population of users generates new frames according to a Poisson distribution with mean N frames per frame time. (The infinite-population assumption is needed to ensure that N does not decrease as users become blocked.) If $N > 1$, the user community is generating frames at a higher rate than the channel can handle, and nearly every frame will suffer a collision. For reasonable throughput, we would expect $0 < N < 1$. In addition to the new frames, the stations generate retransmissions of frames that previously suffered collisions. Let us assume that the probability of k transmission attempts per frame time, old and new combined, is also Poisson, with mean G per frame time. $G \geq N$. At low load (i.e., N 0), there will be few collisions, hence few retransmissions, so G N. At high load, there will be many collisions, so $G > N$. Under all loads, the throughput, S, is just the offered load, G, times the probability, P0, of atransmissionsucceeding—thatis,$S=GP0$,where$P0$istheprobabilitythataframedoesnotsuffer acollision.

As shown in Fig. 2, a frame will not suffer a collision if no other frames are sent within one frame time of its start.

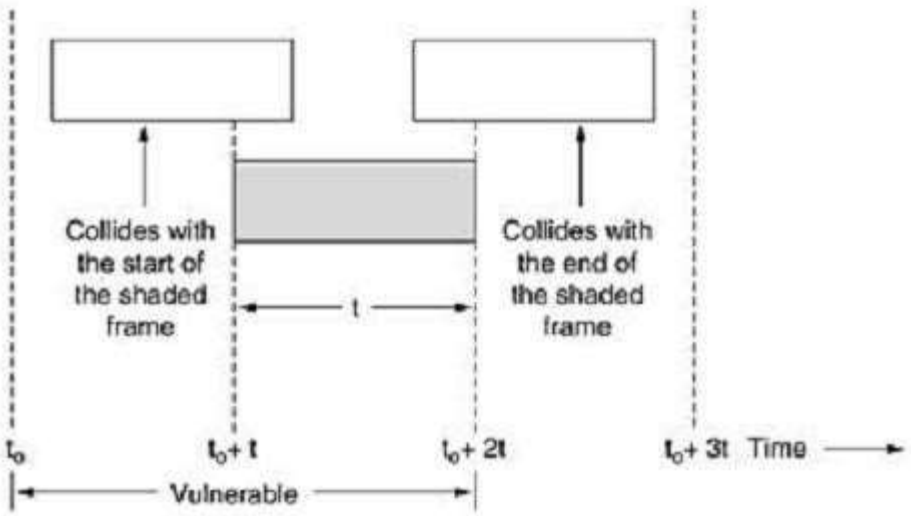


Fig.2. Vulnerable period for the shaded frame

Under what conditions will the shaded frame arrive undamaged? Let t be the time required to send a frame. If any other user has generated a frame between time t0 and t0+tr, the end of that framewillcollidewiththebeginningoftheshadedone.Theshadedframe'sfatewasalready sealed even before the first bit was sent, but since a station does not listen to the channel before transmitting in pure ALOHA, it cannot know that another frame was already underway. Similarly,anyotherframestartedbetweent0+t andt0+2twillbumpintotheendofthe shadedframe.

The probability that k frames are generated during a given frame time is given by the Poisson distribution:

Equation

$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

So, the probability of zero frames is just e-G. The mean number of frames generated is 2G in an interval two frame times long. The probability of no other traffic being initiated during the entire vulnerable period is thus given by P0 = e -2G. Using S = GP0, weget

$$S = Ge^{-2G}$$

The relation between the offered traffic and the throughput is shown in Fig. 4-3. The maximum

Throughput occurs at G = 0.5, with S = 1/2e, which is about 0.184. In other words, the best we can hope for is a channel utilisation of 18 per cent. This result could have been more encouraging, but we could hardly have expected a 100% success rate with everyone transmitting at will.

Slotted ALOHA:

In 1972, Roberts published a method for doubling the capacity of an ALOHA system (Robert, 1972). He proposed to divide time into discrete intervals, each corresponding to one frame. This approach requires the users to agree on slot boundaries. One way to achieve synchronisation would be to have one particular station emit a pip at the start of each interval, like a clock.

In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA, a computer is not permitted to send whenever a carriage return is typed. Instead, waiting for the beginning of the next slot is required. Thus, the continuous pure ALOHA is turned

into a discrete one. Since the vulnerable period is now halved, the probability of no other traffic during the same slot as our test frame is e-G, which leads to

\Equation

$$S = Ge^{-G}$$

As shown in Fig.3, slotted ALOHA peaks at G = 1, with a throughput of S=1/e or about 0.368, twice that of pure ALOHA. If the system operates at G = 1, theprobability of an empty slot is 0.368. The best we can hope for using slotted ALOHA is 37 per cent of the slots empty, 37 per cent successes, and 26 per centcollisions.OperatingathighervaluesofGreducesthe number of empties but increases the number of collisionsexponentially.

To see how this rapid growth of collisions with G comes about, consider the transmission of a test frame. The probability that it will avoid a collision is e-G, the likelihood that all the other users are silent in that slot. The possibility of a crash is then just 1 – e-G. The possibility of a transmission requiring exactly k attempts (i.e., k – 1 collisions followed by one success)is

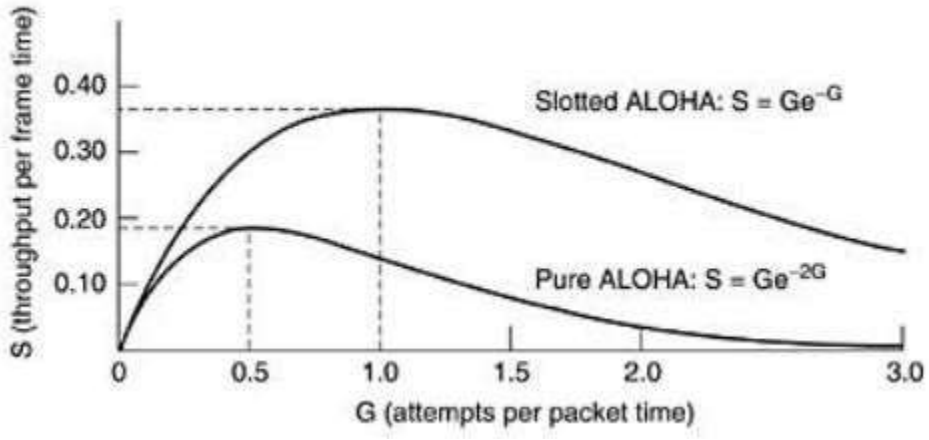


Fig.3 Throughput versus offered traffic for ALOHA systems.

$$P_k = e^{-G}(1 - e^{-G})^{k-1}$$

The expected number of transmissions, E, per carriage return typed, is then.

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1 - e^{-G})^{k-1} = e^{G}$$

As a result of the exponential dependence of E upon G, small increases in the channel load can drastically reduce its performance.

CSMA

Carrier Sense Multiple Access Protocols:

With slotted ALOHA, the best channel utilisationis 1/e. This is hardly surprising since stations transmit at will without paying attention to what the other stations are doing, and there are bound to be many collisions. In local area networks, however, stations can detect what other stations are doing and adapt their behaviour accordingly. These networks can achieve a much better utilisation than 1/e. In thissection, we will discuss some protocols for improving performance. Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols. A number of them have been proposed. Kleinrock and Tobagi (1975) have analysed several such protocols in detail. Below, we will mention several versions of the carrier sense protocols.

1.1-persistent CSMA:

Thefirstcarriersenseprotocolwe will study here is **1-persistentCSMA**(CarrierSense Multiple Access). When a station has data to send, it first listens to the channel to see if anyone else is transmitting. If the channel is busy, the station waits until it becomes idle. Whenthestationdetectsanidlechannel,itsendsaframe.Ifacollisionoccurs,thestationwaits a random amount of time and starts again. The protocol is called 1- persistent because the station transmits with a probability of 1 when it finds the channelidle.

Thepropagationdelayhasanessentialeffectontheperformanceoftheprotocol. After a station begins sending, another station will become ready to send and sense the channel. If the first station's signal has not yet reached the second one, the latter will sense an idle channel and begin sending, resulting in a collision. The longer the propagation delay, the more critical this effect becomes, and the worse the protocol performance. Even if the propagation delay is zero, there will still be collisions. Suppose two stations become ready in the middle of a third station's transmission. In that case, both will wait politely until the transmission ends and begin transmitting exactly simultaneously, resulting in a collision. If they were not so impatient, there would be fewer collisions. Even so, this protocol is farbetterthanpureALOHAbecausebothstationshavethedecencytoprevent interferencewith the third station's frame. Intuitively, this approach will lead to a higher performance than pure ALOHA. Precisely, the same holds for slottedALOHA.

2. Non-persistentCSMA:

A second carrier sense protocol is **nonpersistent CSMA**. This protocol makes a conscious attempt to be less greedy than in the previous one. Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it to seize it immediately upon detecting the end of the previous transmission. Instead, it waits a random period and then repeats the algorithm. Consequently, this algorithm leads to better channel utilisation but longer delays than 1-persistentCSMA.

3. P-persistentCSMA:

Thelastprotocolis**p-persistentCSMA**. Itappliestoslottedchannelsandworksasfollows.When astationbecomesreadytosend,itsensesthechannel.Ifidle,ittransmitswithaprobability

p.Withaprobabilityq=1-p,itdefersuntilthenextslot.Ifthatslotis idle, Ittransmits or defers again, with probabilities p and q. This process is repeated until either the frame hasbeen transmitted or another station has begun transmitting. In the latter case, the unlucky station acts as if there had been a collision (i.e., it waits a random time and starts again). If the station initiallysensesthechannelis busy,itwaitsuntilthenextslotandappliestheabovealgorithm.Figure 4showsthecomputedthroughputversusofferedtrafficforallthreeprotocols and pure and slotted ALOHA.

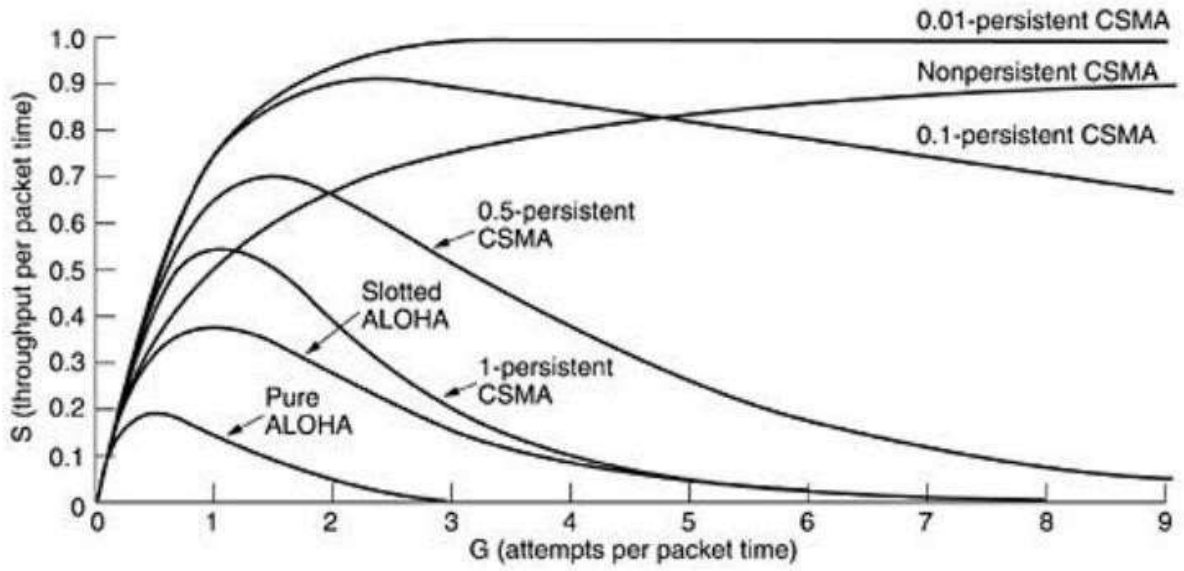


Fig.4 Comparison of the channel utilisation versus load for various random access protocols

CSMA with Collision Detection:

Persistent and nonpersistent CSMA protocols are an improvement over ALOHA because they ensure that no station begins to transmit when it senses the channel is busy. Another improvement is for stations to abort their transmissions when they detect a collision. Inother words, if two stations sense the channel as idle and begin transmitting simultaneously, they will detect the collision almost immediately. Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the crash is detected. Quickly terminating damaged frames saves time andbandwidth.

This protocol, CSMA/CD (CSMA with Collision Detection), is widely used on LANsin the MAC sublayer. In particular, it is the basis of the popular Ethernet LAN, so it is worth devoting some time to looking at it in detail. CSMA/CD and many other LAN protocols use the conceptual

model of Fig.5. At the point marked t0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

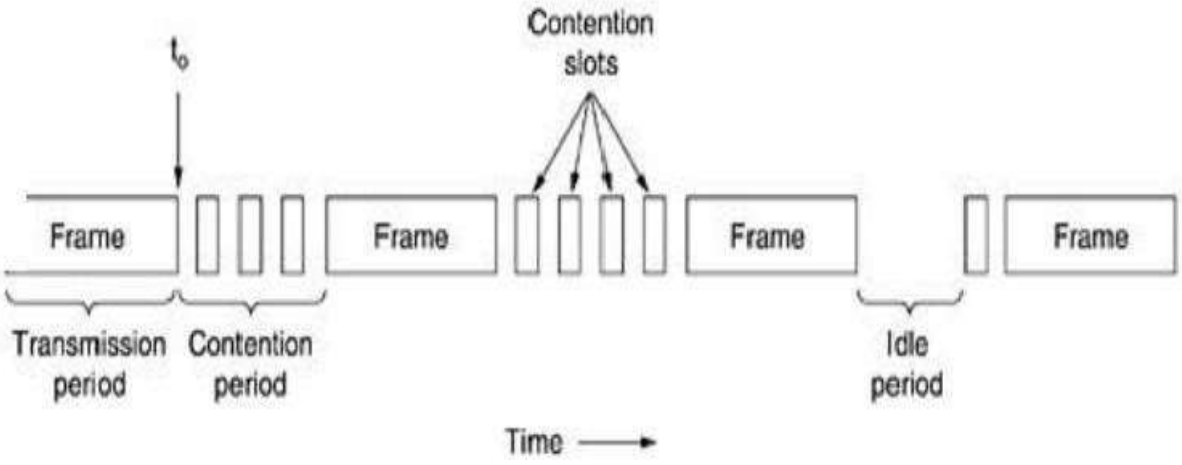


Fig.5. CSMA/CD can be in one of three states: contention, transmission, or idle. After a station detects a collision, it aborts its transmission, waits a random period, and then tries again, assuming that no other station has started transmitting.Therefore, ourmodelforCSMA/CDwillconsistofalternatingcontentionand transmissionperiods,withidle periods occurring when all stations are quiet (e.g., for lack of work).

Let's delve into the contention algorithm, a crucial component of the CSMA/CD protocol. Imagine two stations start transmitting at the same time, t0. How long will it take for them to detect a collision? This question is pivotal in determining the length of the contention period and, consequently, the delay and throughput. The minimum time to detect a collision is the time it takes for the signal to propagate from one station to the other, a key factor in the CSMA/CD protocol.

Based on this reasoning, you might think that a station not hearing a collision for a time equal to the entire cable propagation time after starting its transmission could be sure it had seized thecable. By "seized," we mean that all other stations knew it was transmitting and would not interfere. This conclusion is wrong. Consider the following worst-case scenario. Let the time for a signal propagating between the two farthest stations be. At t0, one station begins transmitting. An instant before the signal arrives at the most distant station, that station also begins transmitting. Of course, it detects the collision almost instantly and stops, but the little noiseburst

caused by the crashonly gets back to the original station atthe time. In other words, in the worst case, a station can only be sure it has seized the channel once it has transmitted without hearing a collision. For this reason, we will model the contention interval as a slotted ALOHA system with slot width. On a 1-km-long coaxial cable, For simplicity, we will assume that each slot contains just 1 bit. Once the channel has been seized, a station can transmit at any rate it wants to, of course, not just at 1 bit persec.

IEEESTANDARDS

In 1985, the Computer Society of the IEEE started a project called Project 802 to set standards to enable intercommunication among equipment from various manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it specifies functions of the physical layer and the data link layer of major LAN protocols.

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802. Figure 1 shows the relationship of the 802 Standard to the traditional OSI model.

The IEEE has subdivided the data link layer into two sublayers:

logical link control (LLC) and media access control (MAC).

IEEE has also created several physical layer standards for different LAN protocols.

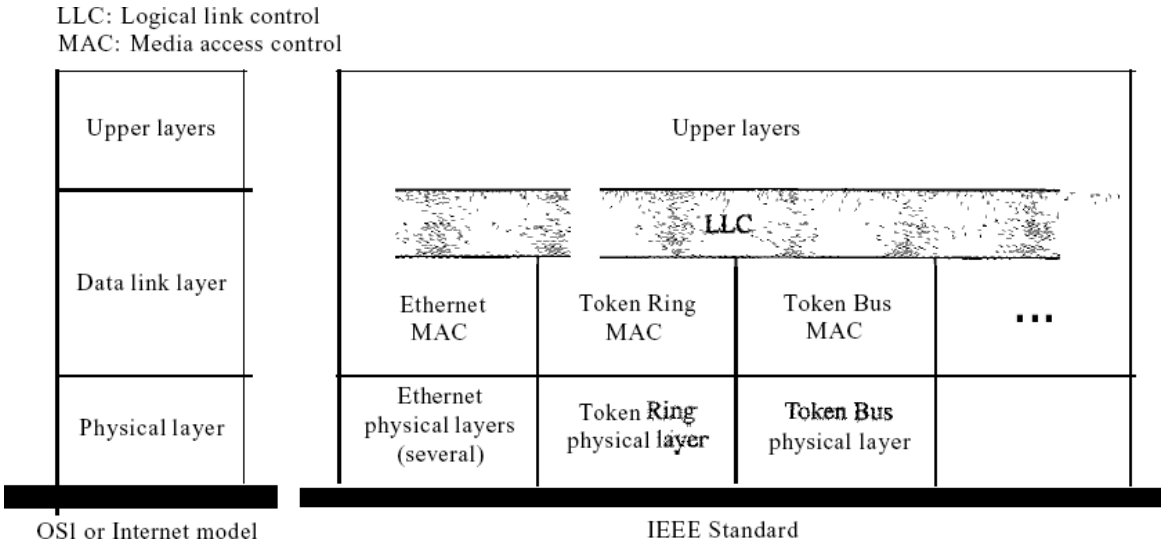


Figure 1 *IEEE standardfor LANs*

As mentioned before, the data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

Logical Link Control (LLC)

We said data link control handles framing, flow, and error control. In IEEE Project 802,flowcontrol,errorcontrol,andpartoftheframingdutiesarecollectedintoonelogical link control sublayer. Framing is handled in both the LLC sublayer and the MACsublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC differs from the media access control sublayer, which offers different protocols for different LANs. A single LLC protocol can interconnect different LANs because it makes the MAC sublayer transparent. Figure 1 shows one single LLC protocol serving several MAC protocols. Framing LLC defines a protocol data unit (PDU) as similar to HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol, such as HDLC, are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer, as shown in Figure2.

Need for LLC The purpose of LLC is to provide flow and error control for the upper-layer protocols that demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application-layer protocols. However, most upper-layer protocols, such as IP, do not use LLC services.

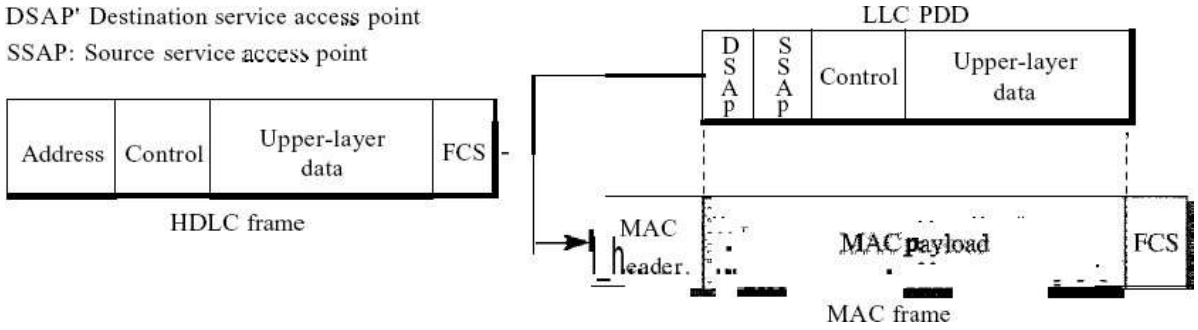


Figure 13.2 *HDLCframe compared with LLC and MAC frames*

Media Access Control (MAC)

IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines *CSMA/CD* as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs. As discussed in the previous section, the MAC layer also handles part of the framing function. In contrast to the LLC sublayer, the MAC sublayer contains several distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

PhysicalLayer

The physical layer depends on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet, there are different physical layer specifications for each Ethernet implementation.

StandardEthernet

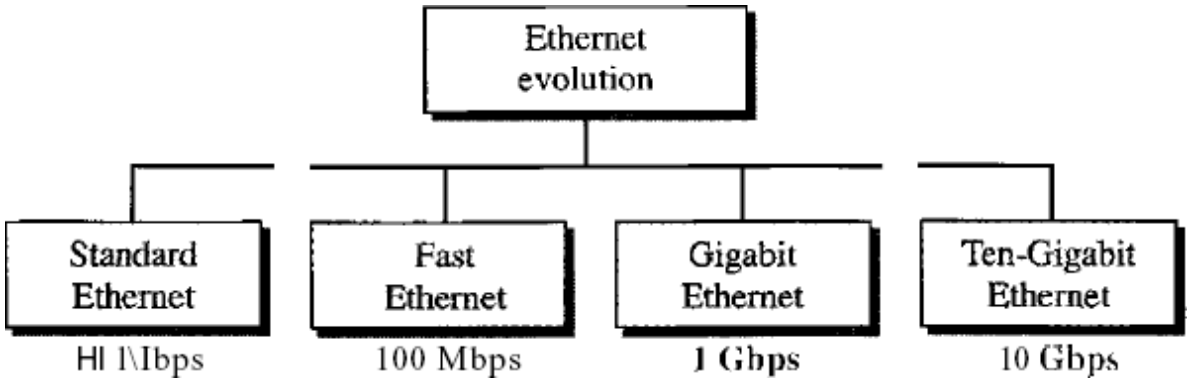


Figure 3 *Ethernet evolution through four generations*

MACSublayer

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRe. Ethernet does not provide any mechanism for acknowledging received frames, making it an unreliablemedium.

Acknowledgements must be implemented at the higher layers. The format of the MAC frame is shown in Figure 4.

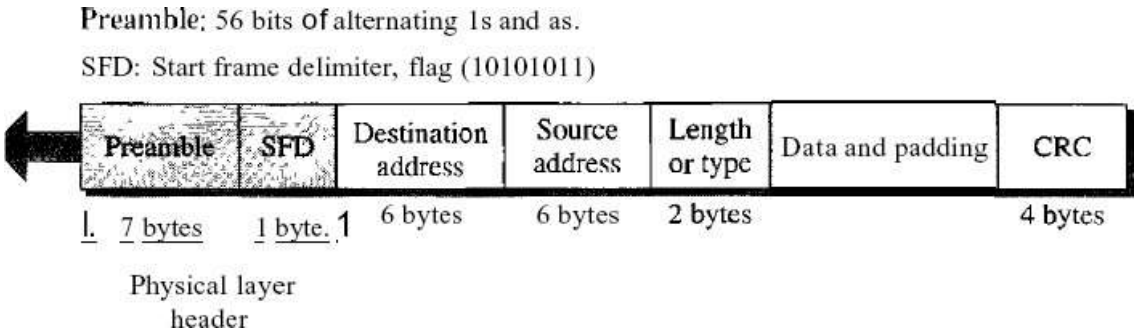


Figure 4 *802.3 MACframe*

- D Preamble. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and Is that alerts the receiving system to the coming frame and enables it to synchronise its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allowsthestationstomisssomebitsatthebeginningoftheframe.Thepreambleisadded at the physical layer and is not (formally) part of theframe.
- D Start frame delimiter (SFD). The second field (l 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 two bits are 11, alerting the receiver that the next field is the destination address.
- Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive thepacket.
- Source address (SA). The SA field is also 6 bytes and contains the physical address of the packet's sender. We will discuss addressing this shortly.
- Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. TheIEEEstandarduseditasthelengthfieldtodeterminethenumberofbytesinthedatafield. Both uses are commontoday.
- 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, such as a CRC-32.

Frame Length

Ethernet has imposed restrictions on a frame's minimum and maximum lengths, as shown in Figure 5.

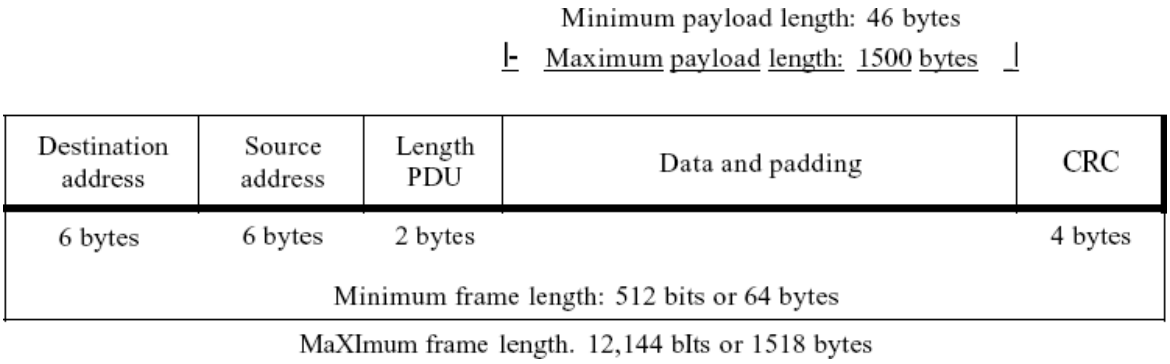


Figure 5 *Minimum and maximum lengths*

The minimum length restriction is required for the correct operation of *CSMAlCD*. An Ethernet framemusthaveaminimumlengthof512bitsor64bytes.Partofthislengthistheheaderand 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 size 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 thedifference.

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. There are two historical reasons for the restriction on maximum length. First, memory was costly when Ethernet was designed: a maximum length restriction helped reduce the buffer's size. Second, the maximum length restriction prevents one station from monopolising the shared medium, blocking other stations with data tosend.

Frame length:

Minimum: 64 bytes (512 bits) Maximum: 1518 bytes (12,144 bits)

Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its network interface card (NIC). The NIC fits inside the station and provides the stationwith a 6-byte

physical address. As shown in Figure 6, the Ethernet address is 6 bytes (48 bits), nonnally written in hexadecimal notation, with a colon between thebytes.

06:01 :02:01:2C:4B

6 bytes =12 hex digits =48 bits

Figure 6 *Example ofan Ethernet address in hexadecimal notation*

Unicast, Multicast, and Broadcast Addresses A source address is always a unicast address-the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. Figure 7 shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

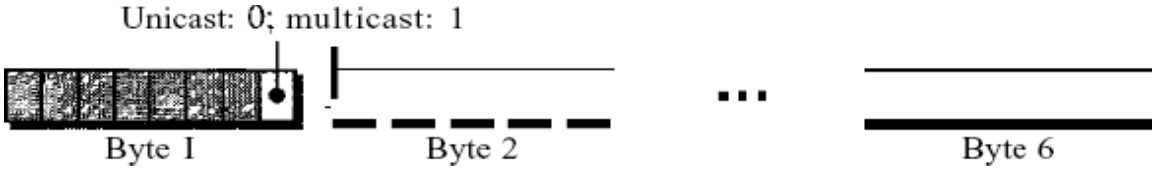


Figure 7 *Unicast and multicast addresses*

A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationshipbetweenthesenderandthereceiversisone-to-many.Thebroadcastaddressisaspecial caseofthemulticastaddress;therecipientsareallthestationsontheLAN.Abroadcastdestination address isforty-eight.

PhysicalLayer

The Standard Ethernet defines several physical layer implementations; four of the most common, are shown in Figure 8.

Encoding and Decoding

All standard implementations use digital signaling (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. Manchester encoding is self-synchronous, providing a transition at each bit interval. Figure 9 shows the encoding scheme for Standard Ethernet.

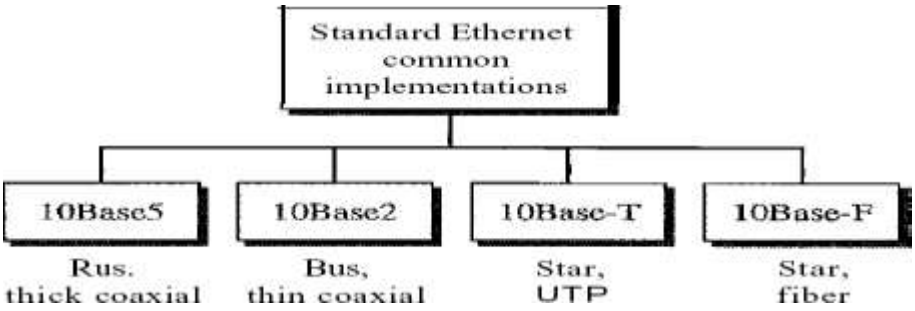


Figure 8 *Categories ofStandard Ethernet*

FastEthernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

The goals of Fast Ethernet can besummarized as follows:

1. Upgrade the data rate to 100Mbps.
2. Make it compatible with StandardEthernet.
3. Keep the same 48-bitaddress.
4. Keep the same frameformat.
5. Keep the same minimum and maximum framelengths.

- **MAC Sublayer**
- **Physical Layer**

6.4 IEEE 802.11

6.4.1 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 block 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). Figure 9 shows two sets in this standard.

The BSS without anAP is a stand-alone network and cannot send data to other BSSs. It is called

an *ad hoc architecture.* In this architecture, stations can form a network without the need of an

AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an *infrastructure* network.

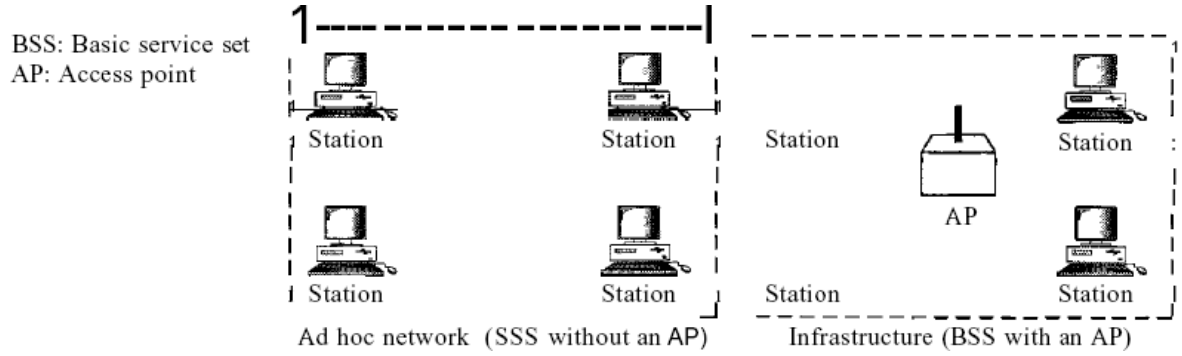


Figure. 9 *Basic service sets (BSSs)*

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs areconnectedthrough*adistributionsystem*,whichisusuallyawiredLAN.Thedistributionsystem connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobileandstationary.Themobilestationsarenormalstationsinsidea BSS.Thestationarystations are AP stations that are part of a wired LAN. Figure 10 shows anESS.

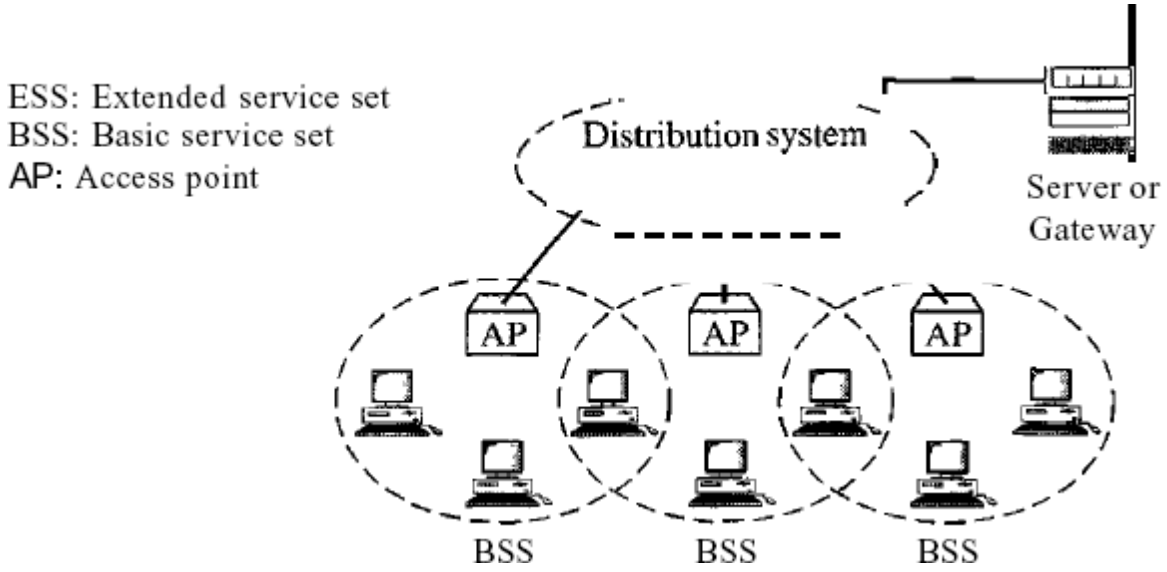


Figure 10 *Extended service sets (ESSs)*

Bluetooth:

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgetshasthiscapability.ABluetoothLAN,bynature,cannotbelarge.Iftherearemanygadgets that try to connect, there ischaos.

Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at aconference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand*translates to *Bluetooth* in English.

Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.Thestandarddefinesawirelesspersonal-areanetwork(PAN)operableinanareathesize of a room or ahall.

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;t the rest are called secondaries. All the secondary stations synchronizetheirclocksandhoppingsequencewiththeprimary.Notethatapiconetcanhaveonly one primary station. The communication between the primary and the secondary can be one- to-one or one-to-many. Figure 1 shows apiconet.

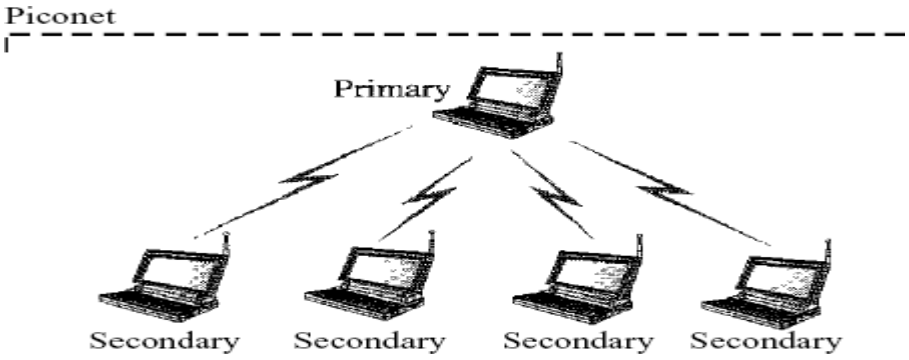


Figure 1 *Piconet*

Although a piconet can have a maximum of seven secondaries, an additional eight 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. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scat/ernet

Piconets can be combined to form what is called a scatternet. 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.

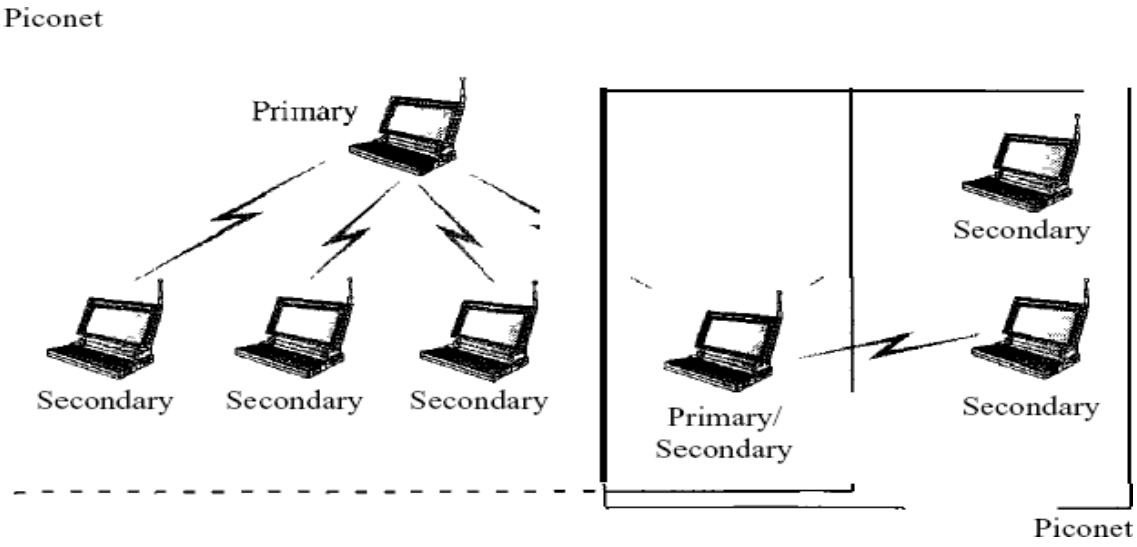


Figure 2 illustrates a scatternet.

Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and BluetoothLANs.

BluetoothLayers

Bluetoothusesseverallayersthatdonotexactlymatchthoseoftheinternetmodelwehavedefined in this book. Figure 3 shows theselayers.

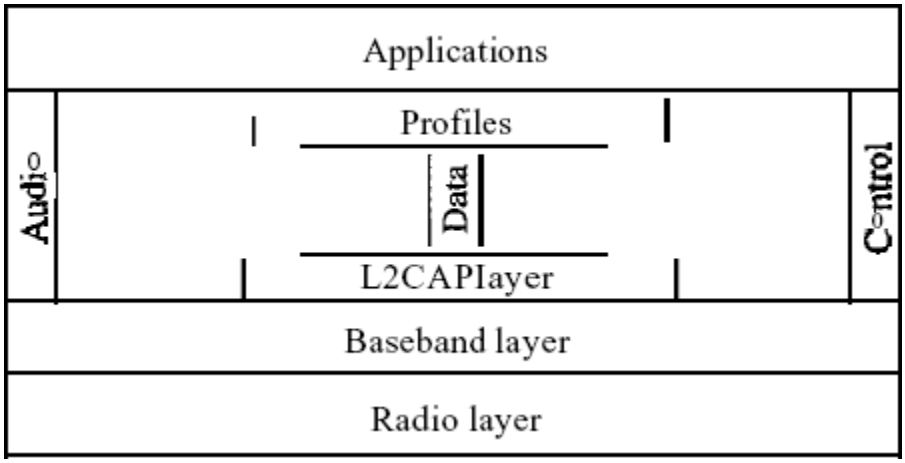


Figure 3 *Bluetooth layers*

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 frequency 1600 times per second. A device uses a frequency for only 625 Ils (1/1600 s) before it hops to another frequency; the dwell time is 625 *Ils.*

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering; a discussion of this topic is beyond the scope of this book). GFSK has a can'ier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit ais represented by a frequency deviation below the carrier. The frequencies, in megahertz, are defined according to the following formula for each channel:

$fc=2402+n$ n =0, 1,2,3, ..., 78

For example, the first channel uses carrier frequency 2402 MHz (2.402 GHz), and the second channel uses carrier frequency 2403 MHz (2.403 GHz).

Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA (see Chapter 12). The primary and secondary communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 Ils. This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary. Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

TDMA

Bluetooth uses a form of TDMA (see Chapter 12) that is called TDD-TDMA (timedivision duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time (halfduplex); however, the communication for each direction uses different hops. This is similar to walkie-talkies using different carrierfrequencies.

Single-Secondary Communication If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 Ils. The primary uses evennumbered 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 4 shows the concept.

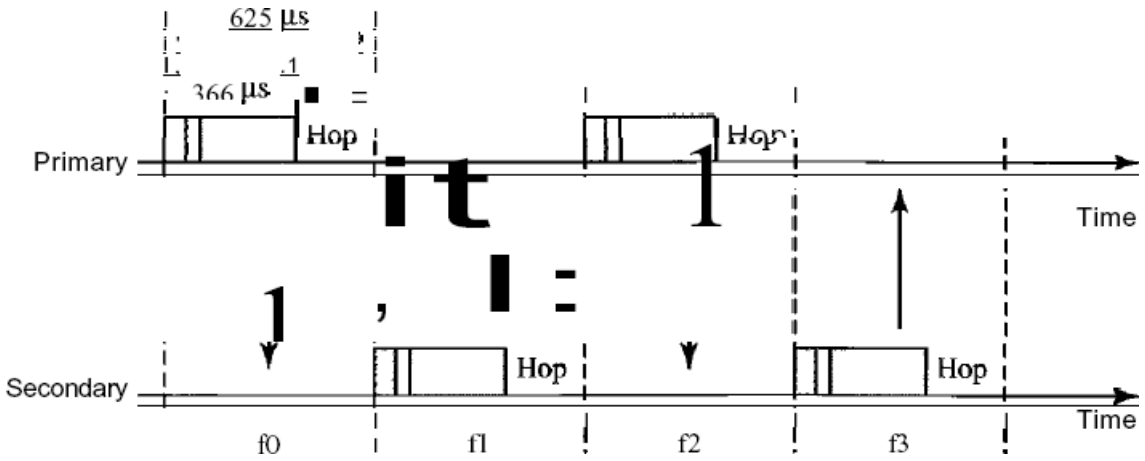


Figure 4 *Single-secondary communication*

8. Data Link LayerSwitching

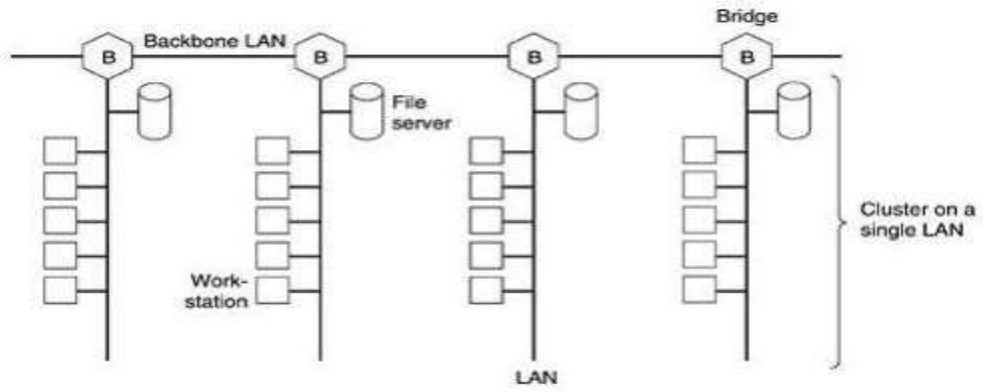
Bridges:

Many organizations have multiple LANs and wish to connect them. LANs can be connected by devices called bridges, which operate in the data link layer. Bridges examine the data layer link addresses to do routing. Some common situations in which bridges are used.

First, many university and corporate departments have their own LANs, primarily to connect theirownpersonalcomputers,workstations,andservers.Sincethegoalsofthevariousdepartments differ, different departments choose different LANs, without regard to what other departmentsare doing. Sooner or later, there is a need for interaction, so bridges are needed. In this example, multiple LANs came into existence due to the autonomy of theirowners.

Second, the organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges and laser links than to run a single cable over the entire site.

Third, it may be necessary to split what is logically a single LAN into separate LANs to



accommodate the load. At many universities, for example, thousands of workstations are available for student and faculty computing. Files are normally kept on file server machines and are downloaded to users' machines upon request. The enormous scale of this system precludes putting all the workstations on a single LAN—the total bandwidth needed is far too high. Instead, multiple LANs connected by bridges are used, as shown in Fig.17.1. Each LAN contains a cluster of workstations with its own file server so that most traffic is restricted to a single LAN and does not addloadtothebackbone.

It is worth noting that although we usually draw LANs as multi drop cables as in Fig.(the classic look), they are more often implemented with hubs or especially switches nowadays. However, a long multi drop cable with multiple machines plugged into it and a hub with the machines connected inside the hub are functionally identical. In both cases, all the machines belong to the same collision domain, and all use the CSMA/CD protocol to sendframes.

Fourth, in some situations, a single LAN would be adequate in terms of the load, but the physical distancebetweenthemostdistantmachinesistoogreat(e.g.,morethan2.5kmforEthernet).Even if laying the cable is easy to do, the network would not work due to the excessively long round- trip delay. The only solution is to partition the LAN and install bridges between the segments. Using bridges, the total physical distance covered can beincreased.

Fifth, there is the matter of reliability. On a single LAN, a defective node that keeps outputting a continuous stream of garbage can cripple the LAN. Bridges can be inserted at critical places, like fire doors in a building, to prevent a single node that has gone berserk from bringing down the entire system. Unlike a repeater, which just copies whatever it sees, a bridge can be programmed to exercise some discretion about what it forwards and what it does not forward.

Sixth, and last, bridges can contribute to the organization's security. Most LAN interfaces have a promiscuous mode, in which all frames are given to the computer, not just those addressed to it. Spies and busybodies love this feature. By inserting bridges at various places and being careful not to forward sensitive traffic, a system administrator can isolate parts of the network so that its traffic cannot escape and fall into the wrong hands.

Operation of Two PortBridge:

Fig.2 illustrates the operation of a simple two-port bridge. Host A on a wireless (802.11) LAN has a packet to send to a fixed host, B, on an (802.3) Ethernet to which the wireless LAN is connected. The packet descends into the LLC sublayer and acquires an LLC header (shown in black in the figure). Then it passes into the MAC sublayer and an 802.11 header is prepended to

it (also a trailer, not shown in the figure). This unit goes out over the air and is picked up by the base station, which sees that it needs to go to the fixedEthernet.

Whenithitsthebridgeconnectingthe802.11networktothe802.3network,itstartsinthephysical layer and works its way upward. In the MAC sublayer in the bridge, the 802.11 header is stripped off. The bare packet (with LLC header) is then handed off to the LLC sublayer in the bridge. In thisexample,thepacketisdestinedforan802.3LAN,soitworksitswaydownthe802.3 side

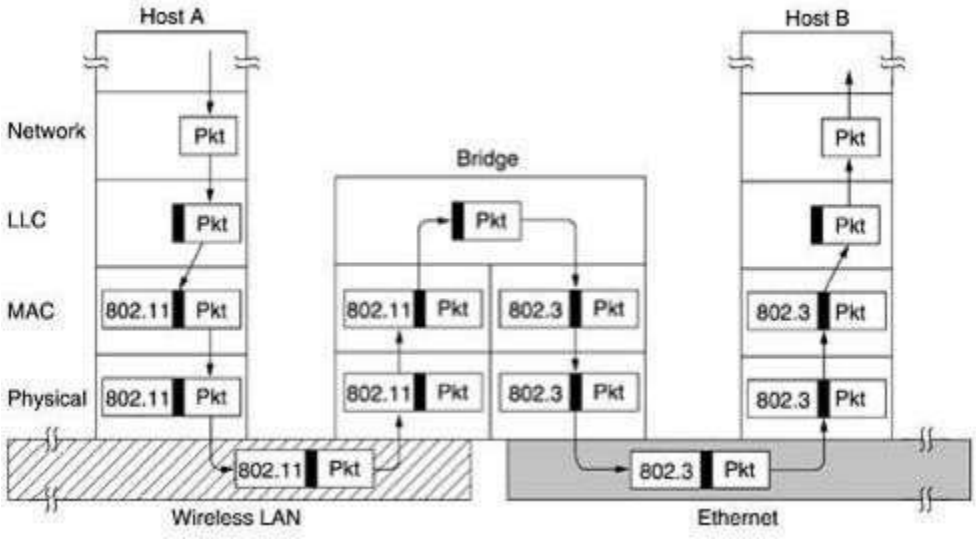


Fig.2 Operation of a LAN bridge from 802.11 to 802.3 Spanning Tree Bridges:

of the bridge and off it goes on the Ethernet. Note that a bridge connecting k different LANs will have k different MAC sublayers and k different physical layers, one for each type.

To increase reliability, some sites use two or more bridges in parallel between pairs of LANs, is shown in Fig.3. This arrangement, however, also introduces some additional problems because it creates loops in the topology. A simple example of these problems can be seen by observing how a frame, F, with unknown destination is handled in Fig.17.3. Each bridge, following the normal rules for handling unknown destinations, uses flooding, which in this example just means copying it to LAN 2. Shortly thereafter, bridge 1 sees F2, a frame with an unknown destination,

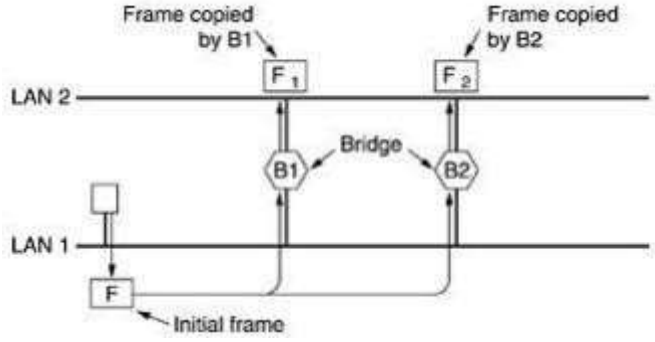


Fig.3. Two parallel transparent bridges.

which it copies to LAN 1, generating F3 (not shown). Similarly, bridge 2 copies F1 to LAN 1 generatingF4(alsonotshown).Bridge1nowforwardsF4andbridge2copiesF3.Thiscyclegoes onforever.

The solution to this difficulty is for the bridges to communicate with each other and overlay the actualtopologywithaspanningtreethatreacheseveryLAN. Ineffect,somepotentialconnections between LANs are ignored in the interest of constructing a fictitious loop-free topology. For example, in Fig.4 (a) we see nine LANs interconnected by ten bridges. This configuration can be abstracted into a graph with the LANs as the nodes. An arc connects any two LANs that are connectedbyabridge.Thegraphcan bereducedtoaspanningtreebydroppingthearcsshownas dotted lines in Fig.4 (b). Using this spanning tree, there is exactly one path from every LAN to everyotherLAN.Oncethebridgeshaveagreedonthespanningtree,allforwardingbetweenLANs follows the spanning tree. Since there is a unique path from eachsource to each destination, loops are impossible.

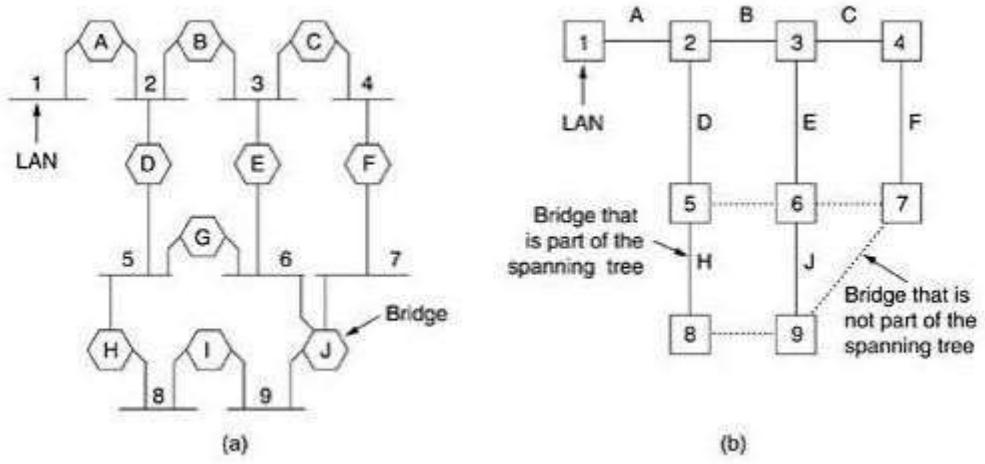


Fig.4 (a) Interconnected LANs. (b) A spanning tree covering the LANs. The dotted lines are not part of the spanning tree.

To build the spanning tree, first the bridges have to choose one bridge to be the root of the tree. They make this choice by having each one broadcast its serial number, installed by the manufacturer and guaranteed to be unique worldwide. The bridge with the lowest serial number becomes the root. Next, a tree of shortest paths from the root to every bridge and LAN is constructed. This tree is the spanning tree. If a bridge or LAN fails, a new one is computed.

The result of this algorithm is that a unique path is established from every LAN to the root and

thus to every other LAN. Although the tree spans all the LANs, not all the bridges are necessarilypresentinthetree(topreventloops).Evenafterthespanningtreehasbeenestablished, the algorithm continues to run during normal operation in order to automatically detect topology changes and update thetree.

RemoteBridges:

A common use of bridges is to connect two (or more) distant LANs. For example, a company might have plants in several cities, each with its own LAN. Ideally, all the LANs should be interconnected, so the complete system acts like one large LAN. This goal can be achieved by putting a bridge on each LAN and connecting the bridges pairwise with point-to-point lines (e.g., lines leased from a telephone company). A simple system, with three LANs, is illustrated in Fig.5. The usual routing algorithms apply here. The simplest way to see this is to regard the three point-to-point lines as hostlessLANs. Then we have a normal system of six LANS interconnected by fourbridges.

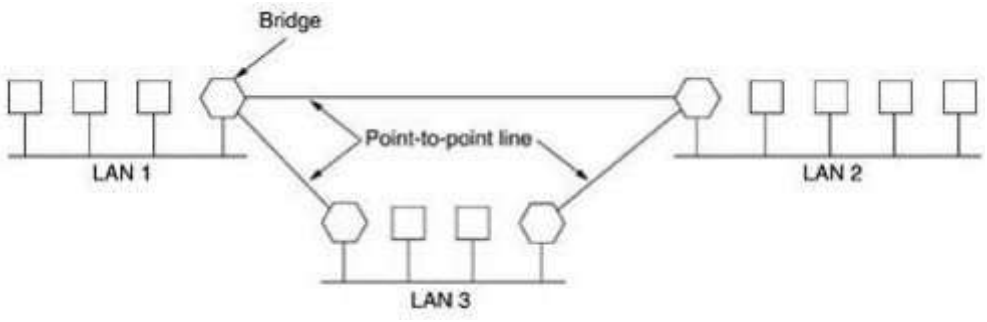


Fig.5. Remote bridges can be used to interconnect distant LANs.

Various protocols can be used on the point-to-point lines. One possibility is to choose some standard point-to-point data link protocol such as PPP, putting complete MAC frames in the payloadfield.ThisstrategyworksbestifalltheLANsareidentical,andtheonlyproblemisgetting frames to the correct LAN. Another option is to strip off the MAC header and trailer at the source bridge and put what is left in the payload field of the point-to-point protocol. A new MAC header and trailer can then be generated at the destination bridge. A disadvantage of this approach isthatthechecksumthatarrivesatthedestinationhostisnottheonecomputed bythesourcehost, so errors caused by bad bits in a bridge's memory may not bedetected.

VirtualLANs

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of

membership is geographic. What happens if we need a virtual connection between two stations belonging to two different physical LANs? We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

Let us use an example to elaborate on this definition. Figure 6 shows a switched LAN in an engineering firm in which 10 stations are grouped into three LANs that are connected by a switch. The first four engineers work together as the first group, the next three engineers work together as the second group, and the last three engineers work together as the third group. The LAN is configured to allow thisarrangement.

But what would happen if the administrators needed to move two engineers from the first group to the third group, to speed up the project being done by the thirdgroup?

The LAN configuration would need to be changed. The network technician must rewire. The problem is repeated if, in another week, the two engineers move back to their previous group. Ina switched LAN, changes in the work group mean physical changes in the network configuration.

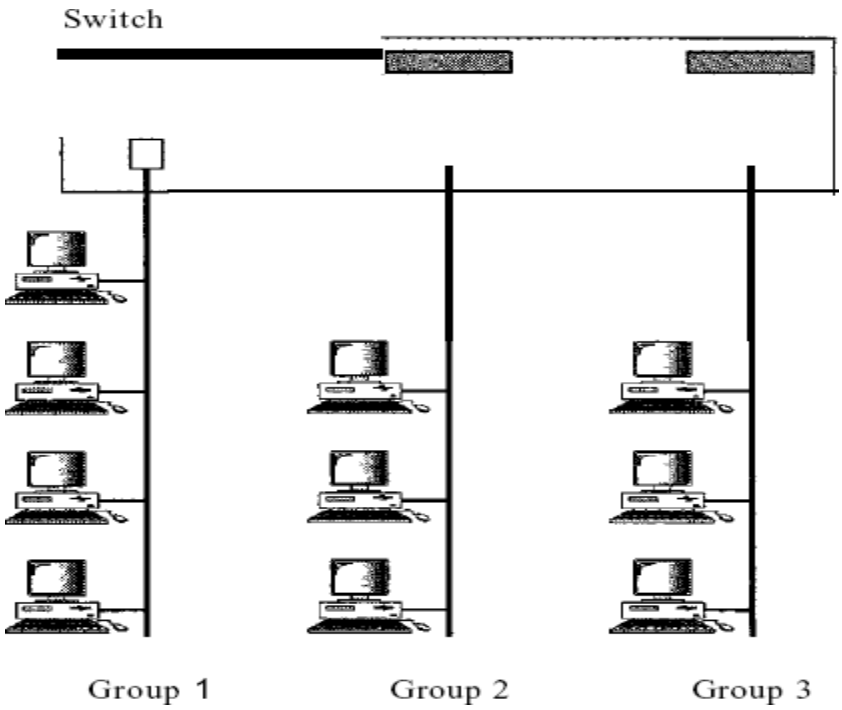


Figure 6 *A switch connecting three LANs*