UNIT 4 WIRELESS LAN AND DATALINK LAYER SWITCHING

Structure **Page Nos.**

4.0 INTRODUCTION

The Previous discussion, we had in this block was related to wired LANs but recently, wireless LANs are taking a dominant position due to coverage of location difficult to wire, to satisfy the requirement of mobility and adhoc networking. In a few years from now, we will notice a broader range of wireless devices accessing the Internet, such as digital cameras, automobiles, security systems, kitchen appliances. **KUROSE** and **ROSS** [reference] writes that some day wireless devices that communicate with the Internet may be present everywhere: on walls, in our cars, in our bedrooms, in our pockets and in our bodies.

In this unit, we cover two broad topics: Wireless LAN, its protocols, its standard and Data Link Layer Switching. In organisation we need an interconnection mechanism so that all nodes can talk to each other. Bridges and switches are used for this purpose. The spanning tree algorithms are used to build plugs and act as bridges.

4.1 OBJECTIVES

After going through this unit, you should be able to:

- understand what is a wireless LAN;
- describe the various LAN Protocols;
- understand the IEEE 802.11 Standard, and
- describe the operation of bridges (transparent, spanning tree and remote bridges).

4.2 INTRODUCTION TO WIRELESS LAN

As the number of mobile computing and communication devices grows, so does the demand to connect them to the outside world. A system of notebook computers that communicate by radio can be regarded as a wireless LAN. These LANs have different properties than conventional LANs and require special MAC sublayer protocols. The 802.11b standard defines the physical layer and media access sublayer for wireless local area network.

To understand the concept, we will take a simplistic view that, all radio transmitters have some fixed range. When a receiver is within a range of two active transmitters, the resulting signal will generally be garbled and of no use. It is important to realise that in some wireless LANs, not all stations are within the range of one another, which leads to a variety of complications, which we will discuss in the next sections.

Wireless LANs are commonly being used in academic institutions, companies, hospitals and homes to access the internet and information from the LAN server while on roaming.

4.3 WIRELESS LAN ARCHITECTURE (IEEE 802.11)

The wireless LAN is based on a cellular architecture where the system is subdivided into cells as shown in *Figure1*. Each cell (called basic service set or BSS, in the 802.11) is controlled by a base station (called access point or AP). Wireless LAN may be formed by a single cell, with a single access point (it can also work within an AP), most stations will be formed by several cells, where the APs are connected through some kind of backbone (called distribution system or DS). This backbone may be the Ethernet and in some cases, it can be the wireless system. The DS appears to upper-level protocols (for example, IP) as a single 802 network, in much the same way as a bridge in wire 802.3. The Ethernet network appears as a single 802 network to upper-layer protocols.

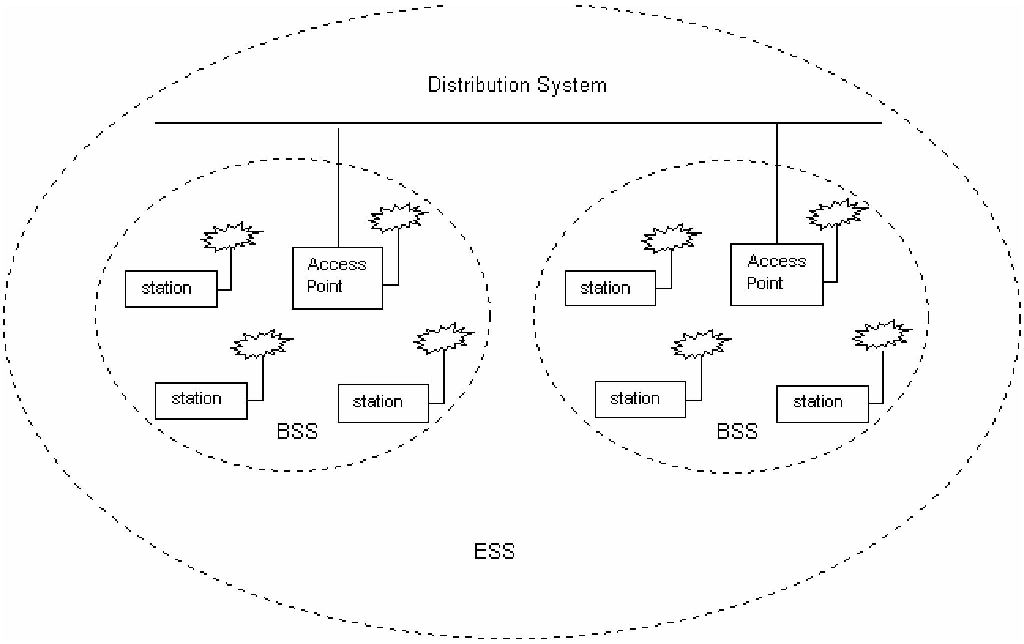


Figure 1: Wireless LAN architecture

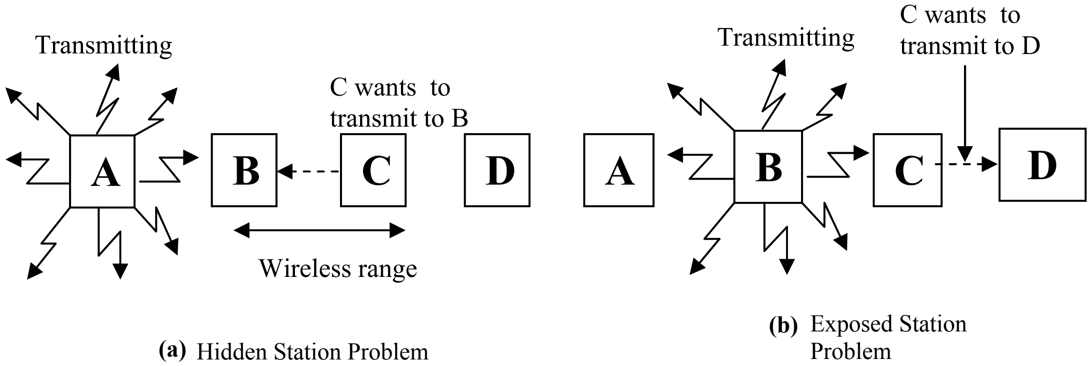
Stations can also group themselves together to form an *ad hoc* network: a network with no central control and with no connections to the "outside world." Here, the network is formed "on the fly," simply because, there happens to be mobile devices that have found themselves in proximity to each other, that have a need to communicate, and that find no preexisting network infrastructure. An *ad hoc* network might be formed when people with laptops meet together (for example, in a conference room, a train, or a car) and want to exchange data in the absence of a centralised AP. There has been tremendous interest in *ad hoc* networking, as communications between devices continue to proliferate.

4.4 HIDDEN STATION AND EXPOSED STATION PROBLEMS

There are two fundamental problems associated with a wireless network. Assume that there are four nodes A, B, C and D. B and C are in the radio range of each other. Similarly A and B are in the radio range of each other. But C is not in the radio range of A.

Now, suppose that there is a transmission going on between A and B (*Figure 2 (a)*). If C also wants to transmit to B, first, it will sense the medium but will not listen to A's transmission to B because, A is outside its range. Thus, C will create garbage for the frame coming from A if, it transmits to B. This is called the **hidden station problem.** The problem of a station not being able to detect another node because that node is too far away is called hidden station problem.

Now, let us consider the reverse situation called the **exposed station problem.** (*Figure 2 (b).*)



(a) Hidden Station Problem

(b) Exposed Station Problem

Figure 2: Hidden and exposed station problem

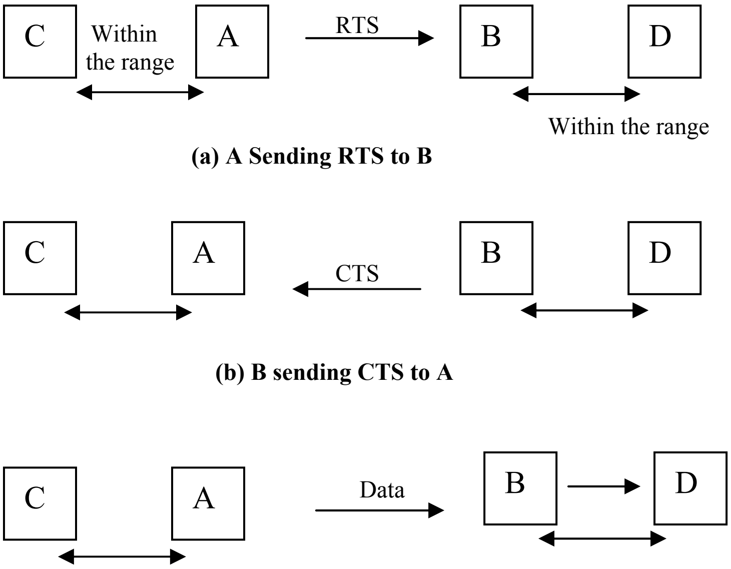
In this case, B is transmitting to A. Both are within radio range of each other. Now C wants to transmit to D. As usual, it senses the channel and hears an ongoing transmission and falsely concludes that it cannot transmit to D. But the fact is transmission between C and D would not have caused any problems because, the intended receivers C and D are in a different range. This is called exposed station problem.

4.5 WIRELESS LAN PROTOCOLS: MACA AND MACAW

In this section, we, will describe two wireless LAN protocols: MACA and MACAW. MACA is the oldest protocol of the two. MACA was proposed as an alternative to CSMA Protocol which has certain drawbacks:

First, it senses the channel to see if the channel is free, it transmits a packet, otherwise it waits for a random amount of time.

- Hidden Station Problems leading to frequent collision.
- Exposed terminal problems leading to worse bandwidth utilisation. MACA eliminates the hidden and exposed station problems using RTS (Repeat to Send) and CTS (Clear to Send) handshake mechanism, which is explained below through a *Figure 3*. RTS and CTS packets carry the expected duration of the data transmission, which will have some implications. All nodes near the sender/receiver after hearing RTS/CTS will defer the transmission. Therefore, it avoids some cases of hidden and exposed station problems. However, it does not always avoid these problems. If, the neighbour hears the RTS only, it is free to transmit once the waiting interval is over.



(a) A Sending RTS to B

(b) B sending CTS to A

(c) Data Transmission between A and B

Figure 3: MACA Protocol

Just assume that, there are four nodes A, B, C, and D in a wireless LAN (*Figure 3*). A is a sender and B is a receiver. The station C is within range of A but not within range of B. Therefore, it can hear transmission from A (i.e., RTS) but not transmission from B (i.e., CTS) (*Figure 3(a) and 3(b)*). Therefore, it must remain silent long enough for the CTS to be transmitted back to A without conflict. The station D is within the range of B but not A so it hears CTS but not RTS. Therefore, it must remain silent during the upcoming data transmission, whose length it can tell by examining the CTS frame. This is illustrated through a diagram (*Figure 3(a) and 3(c)*) A sends RTS to B. Then B sends CTS to A. Then, follows data between A and B.

C hears the RTS from A but not the CTS from B. As long as it does not interfere with the CTS, it is free to transmit while the data frame is being sent. In contrast, the station D is within range of B but not A. It does not hear the RTS but does hear the CTS. Hearing the CTS tips it off that, it is close to a station that is about to receive a frame, so it defers sending anything until that frame is expected to be finished.

Despite these precautions, collisions can still occur. For example, B and C could both send RTS frames to A at the same time. These frames will collide and will be lost. In the event of a collision, an unsuccessful transmitter (i.e. one that does not hear a CTS within the expected time interval) waits a random amount of time and tries again later. MACAW (MACA for wireless) extends MACA to improve its performance which will have the following handshaking mechanism. RTS-CTS-DS-Data → ACK. It is also illustrated through the following diagram (Figure 4).

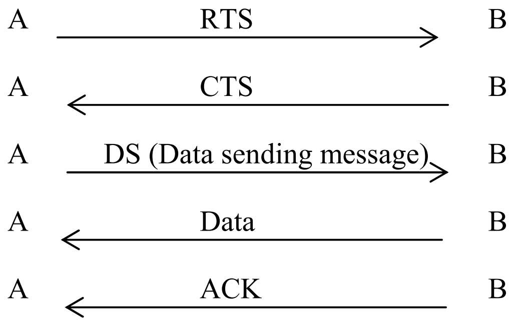


Figure 4: The MACAW protocol

MACAW extends MACA with the following features:

- **Data link layer acknowledgement:** It was noticed that without data link layer acknowledgements, lost frames were not retransmitted until the transport layer noticed their absences, much later. They solved this problem by introducing an ACK frame after each successful data frame.

- **Addition of carrier sensing:** They also observed that CSMA has some use, namely, to keep a station from transmitting a RTS while at the same time another nearby station is also doing so to the same destination, so carrier sensing was added.

- **An improved backoff mechanism:** It runs the backoff algorithm separately for each data stream (source-destination pair), rather than for each station. This change improves the fairness of the protocol.

- **DS (Data sending) message:** Say a neighbour of the sender overhears an RTS but not a CTS from a receiver. In this case it can tell if RTS-CTS was successful or not. When it overhears DS, it realises that the RTS-CTS was successful and it defers its own transmission.

Finally, they added a mechanism for stations to exchange information about congestion and a way to make the back off algorithm react less violently to temporary problems, to improve system performance.

☞ Check Your Progress 1

1) What is Hidden Station Problem?

…………………………………………………………………………………

…………………………………………………………………………………

…………….……………………………………………………………………...

2) Why CSMA/CD cannot be used in wireless LAN environment? Discuss.

…………………………………………………………………………………

…………………………………………………………………………………

………..…………………………..………..……………………………..……

3) How is MACAW different from MACA?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4.6 IEEE 802.11 PROTOCOL STACK

IEEE 802.11 standard for wireless LAN is similar in most respects to the IEEE 802.3 Ethernet standard addresses. As shown in the *Figure 5* the physical layer of 802.11 corresponds to the OSI physical layer fairly well but, the data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAC (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next. Above it is the LLC (Logical Link Control) sublayer, whose job is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

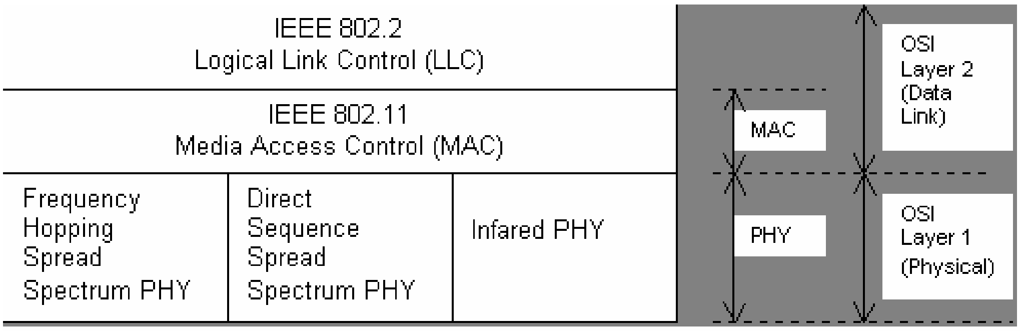

IEEE 802.2
Logical Link Control (LLC)
IEEE 802.11
Media Access Control (MAC)
Frequency Hopping Spread Spectrum PHY
Direct Sequence Spread Spectrum PHY
Infared PHY
MAC
PHY
OSI Layer 2 (Data Link)
OSI Layer 1 (Physical)

Figure 5: Part of the 802.11 protocol stack

4.6.1 The 802.11 Physical Layer

The 802.11 physical layer (PHY) standard specifies three transmission techniques allowed in the physical layer. The infrared method used much the same technology as television remote controls do. The other two use short-range radio frequency (RF) using techniques known as FHSS (Frequency Hopped Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). Both these techniques, use a part of the spectrum that does not require licensing (the 2.4 –GHz ISM band). Radio-controlled garage door openers also use the same piece of the spectrum, so your notebook computer may find itself in competition with your garage door. Cordless telephones and microwave ovens also use this band. All of these techniques operate at 1 or 2 Mbps and at low enough power that they do not conflict too much. RF is capable of being used for ‘not line of sight’ and longer distances.

The other two short range radio frequency techniques are known as spread spectrum. It was initially developed for military and intelligence requirement. The essential idea is to spread information signal over a wider bandwidth to make jamming and interception more difficult. The spread spectrum is ideal for data communication because, it is less susceptible to radio noise and creates little interference. It is used to comply with the regulations for use with ISM Band.

There are two types of spread spectrum:

(i) Frequency Hopping (FH), and
(ii) Direct Sequence (DS)

Both these techniques are used in wireless data network products as well as other communication application such as, a cordless telephone please refer to [5] for further studies.

Under this scheme, the signal is broadcast over a seemingly random data sequence RF hopping from frequency to frequency at split second intervals. A receiver hopping between frequencies in synchronisation with the transmitter, picks up the message. Using FHSS (Frequency Hopped Spread Spectrum) the 2.4 GHz is divided into 75 MHz Channel. In this scheme, a pseudorandom number generator is used to produce the sequence of the frequencies hopped to. As long as all stations use the same seed to the pseudorandom number generator and stay synchronised in time, they will hop to the same frequencies simultaneously. FHSS' randomisation provides a fair way to allocate spectrum in the unregulated ISM band. It also provides some sort of security. Because an intruder does not know the hopping sequence it cannot eavesdrop on transmissions. Over longer distance, multipath fading can be an issue, and FHSS offers good resistance to it. It is also relatively insensitive to radio interference, which makes it popular for building-to-building links. Its main disadvantage is its low bandwidth. FHSS allows for a less complex radio design than DSSS but FHSS is limited to 2 Mbps data transfer rate due to FCC regulations that restrict subchannel bandwidth to 1 MHz causing many hops which means a high amount of hopping overhead. The DSSS is a better choice for WLAN application. It is also restricted to 1 or 2 Mbps.

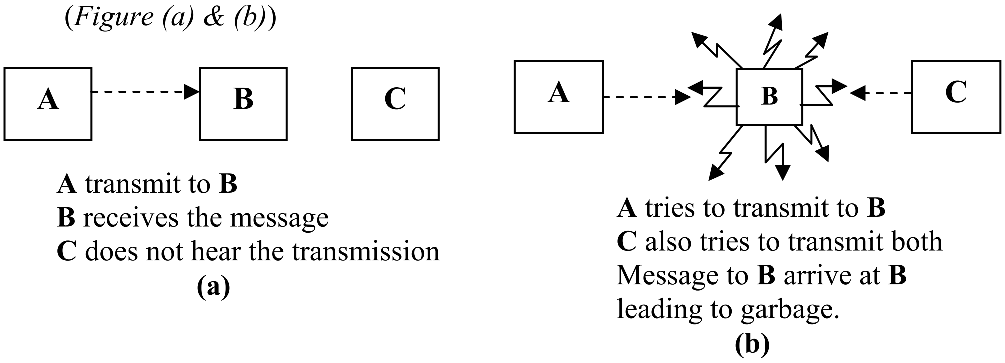
DSSS divides 2.4 GHz band into 14 channels. Channels using at the same location should be separated 25 MHz from each other to avoid interference. FHSS and DHSS are fundamentally different signaling techniques and are not capable of interoperating with each other. Under this scheme, each but in the original signal is represented by multiple bits in the transmitted signal, which is known as chipping code. The chipping code spreads the signal across a wider frequency band in direct proportion to the number of bits used. Therefore, a 10 bit chopping code spreads signal across a frequency band that is 10 times greater than 1 bit chipping code (Ref. 3).

4.6.2 The 802.11 MAC Sub-layer Protocol

After the discussion on the physical layer it is time to switch over to the IEEE 802.11 MAC sublayer protocols which are quite different from that of the Ethernet due, to the inherent complexity of the wireless environment compared to that of a wired system. With Ethernet (IEEE 802.3) a node transmits, in case, it has sensed that the channel is free. If, it does not receive a noise burst back within the first 64 bytes, the frame has almost assuredly been delivered correctly. With wireless technology, this situation does not hold.

As mentioned earlier 802.11 does not use CSMA/CD due to the following problems:

(i) The Hidden Station Problem: CSMA does not avoid the hidden station problem (*Figure (a) & (b)*)

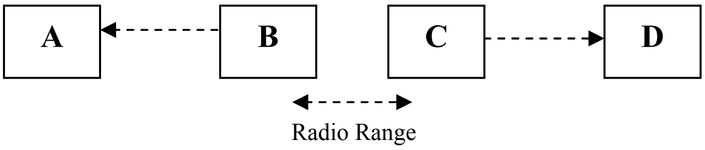


A transmit to **B**
B receives the message
C does not hear the transmission
(a)

A tries to transmit to **B**
C also tries to transmit both
Message to **B** arrive at **B**
leading to garbage.
(b)

Figure 6: (a) The hidden station problem

(ii) The exposed Station Problem CSMA may cause nodes to unnecessarily refrain from accessing the channel as shown in the *Figure below:*



B Transmits to **A** which is heard by **C**
C unnecessarily avoids sending a message to **D** even though there would be no collision.

Figure 6: (b) The exposed station problem

(iii) In addition, most radios are half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency as Ethernet does.

To deal with this problem, 802.11 supports two modes of operation.

- DCF (Distributed Coordination Function)
- PCF (Point Coordinated Function) (optional)

Now, we, will examine IEEE 802.11 DCF separately. It does not use any central control. In this respect it is similar to Ethernet.

When DCF is employed, 802.11 uses a protocol called CSMA/CA (CSMA with Collision Avoidance). In this protocol, both **physical channel sensing** and **virtual channel sensing** are used. Two methods of operation are supported by CSMA/CA. In the first method (Physical sensing), before the transmission, it senses the channel. If the channel is sensed idle, it just wants and then transmitting. But it does not sense the channel while transmitting but, emits its entire frame, which may well be destroyed at the receiver's end due to interference there. If, the channel is busy, the sender defers transmission until it goes idle and then starts transmitting. If, a collision occurs, the colliding stations wait for a random time, using the Ethernet binary exponential backoff algorithm and then try again later.

The second mode of CSMA/CA operation is based on MACAW and uses virtual **channel sensing**, as illustrated in *Figure 6*. In this example, there are four stations A, B, C, and D. A is a transmitter and B is a receiver, C is within the radio range of A (and possibly within the range of B) where as D is within the range of B but not within range of A.

When A has to send data to B, it begins by sending an RTS frame to B to request permission to send it a frame. When B receives this request, it may decide to grant permission, in which case it sends the CTS frame back. Upon receipt of the CTS, A now sends its frame and starts an ACK timer. Upon correct receipt of the data frame, B responds with an ACK frame leading to the closure of data transfer operation between A & B. In case A's ACK timer expires before the ACK gets back to it, the whole protocol is run again.

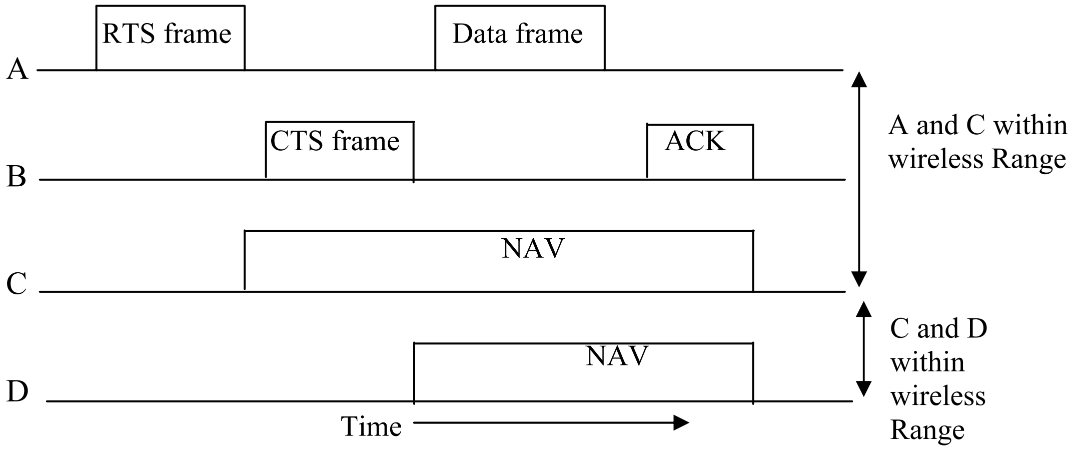


Figure 7: The use of virtual channel sensing using CSMA/CA

Now, how will C and D nodes react to it? Node C is within range of A, so it may receive the RTS frame. C may receive the RTS frame because it is in the rage of A. From the information in the RTS frame it estimates how long the transfer will take, including the final ACK and asserting a kind of virtual channel busy for itself, indicated by NAV (Network Allocation Vector) as shown in *Figure 7.* Similarly, D also asserts the NAV signal for itself because it hears the CTS. The NAV signals are not for transmission. They are just internal reminders to keep quite for a certain period of time.

In contrast to wired networks, wireless networks are noisy and unreliable.
To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces, each with its own checksum because, if a frame is too long, it has very little chance of getting through undamaged and will, probably have to be retransmitted. The fragments are individually numbered and acknowledged using a stop and wait protocol at LLC (i.e., the sender may not transmit fragment k+1 until it has received the acknowledgement for fragment k). Once the channel has been acquired using RTS and CTS, multiple fragments can be sent in a row, as shown in Fig. 8. A sequence of fragments is called a **fragment burst.**

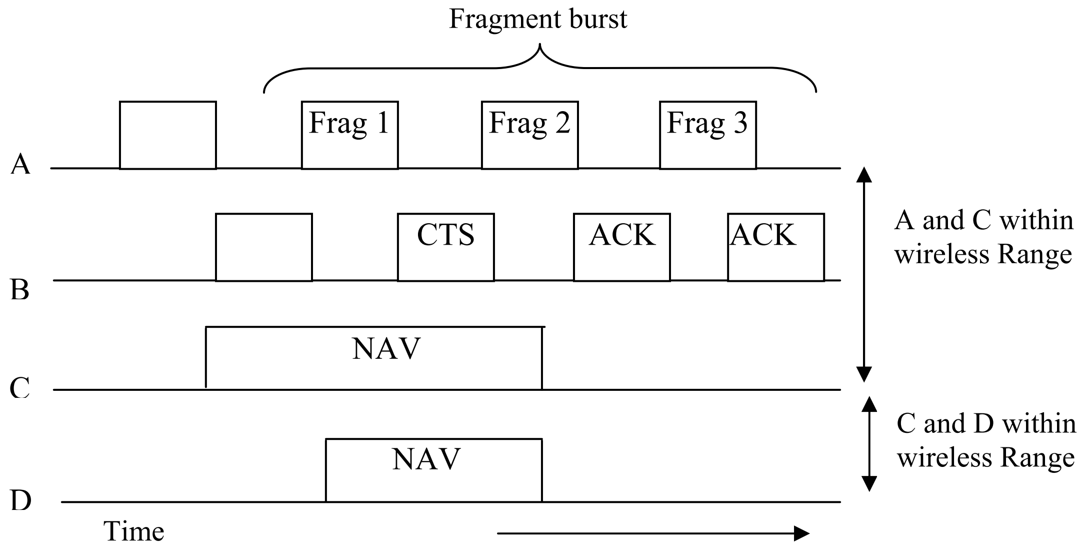


Figure 8: A fragment burst

The second advantage of fragmentation is that it increases the channel throughput by not allowing retransmission to the bad fragments rather than the entire frame. The size of C fragment can be adjusted by a base station in a cell. A base station in a cell can adjust the size of C fragment. The NAV mechanism keeps other stations quiet, only until the next acknowledgement, but another mechanism (described below) is used to allow a whole fragment burst to be sent without interference.

So, far we have discussed DCF in which, the base station polls the other stations, asking them if they have any frames to send. Since, transmission order is completely controlled by the base station in PCF mode, no collisions ever occurs. The standard prescribes the mechanism for polling, but not the polling frequency, polling order, or even whether all stations need to get equal service.

The basic mechanism is for the base station to broadcast a beacon frame periodically (10 to 100 times per second). The beacon frame contains system parameters, such as hopping sequences and dwell times (for FHSS), clock synchronisation, etc. It also invites new stations to sign up for polling services. Once a station has signed up for polling service at a certain rate, it is effectively guaranteed a certain fraction of the bandwidth, thus making it possible to give guarantee of quality services.

Battery life is always an issue with mobile wireless devices, so 802.11 pays attention to the issue of power management. In particular, the base station can direct a mobile station to go into sleep state until explicitly awakened by the base station or the user. Having told a station to go to sleep, however, means that the base station has the responsibility for buffering any frames directed at it while the mobile station is asleep. These can be collected later.

PCF and DCF can coexist within one cell. At first it might seem impossible to have central control and distributed control operating at the same time, but 802.11 provides a way to achieve this goal. It works by carefully defining the interframe time interval. After a frame has been sent, a certain amount of dead time is required before any station can send a frame.

4.7 SWITCHING AT DATA LINK LAYER

Before discussing data link layer switching devices, let us talk about repeaters which are layer 1 devices. Repeaters provide both physical and electrical connections. Their functions are to regenerating and propagate a signal in a channel. Repeaters are used to extend the length of the LAN which depends upon the type of medium. For example 10 mbps 802.3 LAN that uses UTP cable (10 BASE-T) has a maximum restriction of 100 meters. Many organisations have multiple LANs and wish to connect them. LANs can be connected by devices called **bridges,** which operate as the data link layer. Unlike repeaters, bridges connect networks that have different physical layers. It can also connect networks using either the same or different types of architecture at the MAC. (Token ring, FDDI, Ethernet etc).

Bridges have some other characteristics:

(i) Store and forward device.
(ii) Highly susceptible to broadcast storms.

Bridges are store and forward devices to provide error detection. They capture an entire frame before deciding whether to filter or forward the frame, which provides a high level of error detection because a frame's CRC checksum can be calculated by the bridge. Bridge are highly succeptable to broadcast storms. A broadcast storm occurs when several broadcasts are transmitted at the same time. It can take up huge bandwidth.

Before looking at the technology of bridges, it is worthwhile taking a look at some common situations in which bridges are used. **Tanenbaun** [Ref.1] has six reasons why a single organisation may end up with multiple LANs.

1) **Multiple LANs in organisation:** Many university and corporate departments have their own LANs, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ, different departments choose different LANs. But there is a need for interaction, so bridges are needed.

2) **Geographical difference:** The organisation 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 later link them to run a single cable over the entire site.

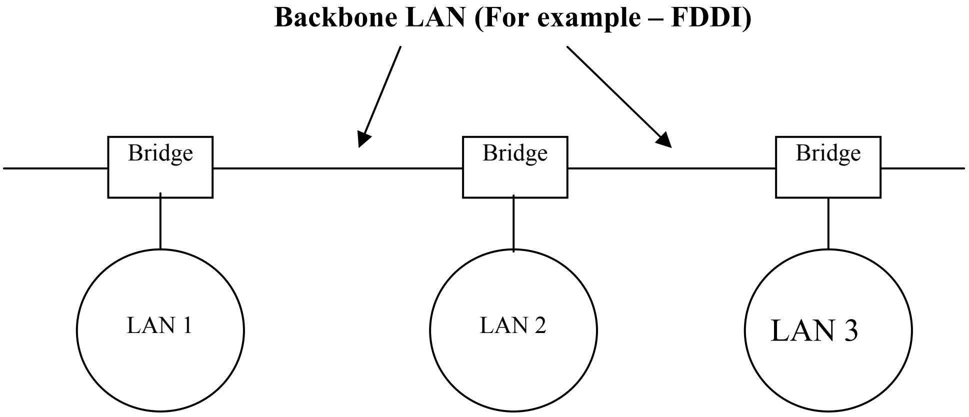


Figure 9: Multiple LANs connected by a backbone to handle a total load higher than the capacity of single LAN

3) **Load distribution**: It may be necessary to split what is logically a single LAN into separate LANs to accommodate the load.

4) **Long Round Trip delay:** In some situations, a single LAN would be adequate in terms of the load, but the physical distance between the most distant machines is can be great (e.g. more than 2.5 km for Ethernet). 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 be increased.

5) **Reliability:** By inserting bridges at critical points reliability can be enforced in the network by isolating a defective node. Unlike a repeater, which just copies whatever it sees, a bridge can be programmed to exercise some discretion regarding what forwards and what it does not forward.

6) **Security** is a very important feature in bridges today, and can control the movement of sensitive traffic by isolating the different parts of the network.

In an ideal sense, a bridge should have the following characters:

(i) **Fully transparent:** It means that it should allow the movement of a machine from one cable segment to another cable segment without change of hardware and software or configuration tools.

(ii) **Interpretability:** It should allow a machine on one LAN segment to talk to another machine on another LAN segment.

4.7.1 Operation of Bridges in Different LAN Environment

Having studied the features of bridges and why we require multiple LANs, let's learn how they work. Assume that, there are two machines A and B. Both of them are attached to a different LANs. Machine A is on a wireless LAN (Ethernet IEEE 802.3). While B is on both LANs are connected to each other through a bridge. Now, A has a packet to be sent to B. The flow of information at Host A is shown below:

1) The packet at machine A arrives at the LLC sublayer from the application layer through the transport layer and network layer.

2) LLC Sublayer header get attached to the packet.

3) Then it moves to the MAC Sublayer. The packet gets MAC sublayer header for attachment.

4) Since the node is part of a wireless LAN, the packet goes to the air using GRF.

5) The packet is then picked up by the base station. It examines its destination address and figures that it should be forwarded to the fixed LAN (it is Ethernet in our case).

6) When the packet arrives at the bridge which connects the wireless LAN and Ethernet LAN, it starts at the physical layer of the bridge and moves to its LLC layer. At the MAC sublayer its 802.11 header is removed.

7) The packet arrives at the LLC of a bridge without any 802.11 header.

8) Since the packet has to go to 802.3 LAN, the bridge prepares packets accordingly.

Note that a bridge connecting *k* different LANs will have *K* different MAC sublayers and *k* different physical layers. One for each type.

So far we have presented a very simplistic scenario in forwarding a packet from one LAN to another through a bridge. In this section, we will point out some of the difficulties that one encounters when trying to build a bridge between the various 802 LANs due to focus on the following reasons:

1) **Different frame Format :**To start with, each of the LANs uses a different frame format. Unlike the differences between Ethernet, token bus, and token ring, which were due to history and big corporate egos, here the differences are to some extent legitimate. For example, the *Duration* field in 802.11 is there, due to the MACAW protocol and that makes no sense in Ethernet. As a result, any copying between different LANs requires reformatting, which takes CPU time, requires a new checksum calculation, and introduces the possibility of undetected errors due to bad bits in the bridge's memory.

2) **Different data rates**: When forwarding a frame from a fast LAN to a slower one, the bridge will not be able to get rid of the frames as fast as they come in. Therefore, it has to be buffered. For example, if a gigabit Ethernet is pouring bits into an 11-Mbps 802.11 LAN at top speed, the bridge will have to buffer them, hoping not to run out of memory.

3) **Different frame lengths:** An obvious problem arises when a long frame must be forwarded onto a LAN that cannot accept it. This is the most serious problem. The problem comes when a long frames arrives. An obvious solution is that the frame must be split but, such a facility is not available at the data link layer. Therefore the solution is that such frames must be discarded. Basically, there is no solution to this problem.

4) **Security:** Both 802.11 and 802.16 support encryption in the data link layer, but the Ethernet does not do so. This means that the various encryption services available to the wireless networks are lost when traffic passes over the Ethernet.

5) **Quality of service:** The Ethernet has no concept of quality of service, so traffic from other LANs will lose its quality of service when passing over an Ethernet.

4.7.2 Transparent Bridges

In, the previous section, we dealt with the problems encountered in connecting two different IEEE 802 LANs via a single bridge. However, in large organisations with many LANs, just interconnecting them all raises a variety of issues, even if they are all just Ethernet. In this section, we introduce a type of bridge called Transparent Bridge, which is a plug and play unit which you connect to your network and switch it on. There is no requirement of hardware and software changes, no setting of address switches , no downloading of routing tables, just plug and play. Furthermore, the operation of existing LANs would not be affected by the bridges at all. In other words, the bridges would be completely transparent (invisible to all the hardware and software). Operating in a promiscuous mode, a transparent bridge captures every frame that is transmitted in all the networks to which the bridge is connected. The bridge examines every frame it receives and extracts each frame’s source address, which it adds to the backward address table.

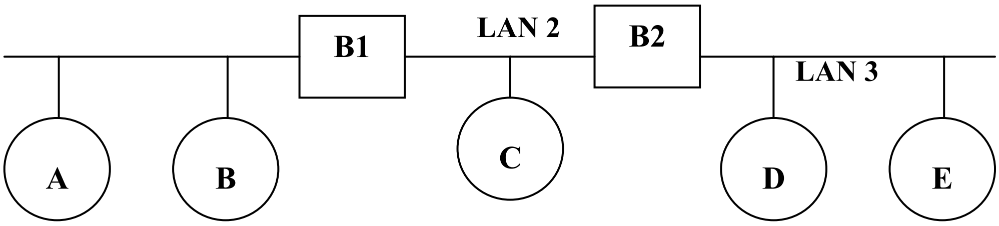


Figure 10: A configuration with four LANs and two bridges.

As an example take the following Confirmation (Figure10). There are 3 LANs: LAN1, LAN2 and LAN3 and two Bridges B1 and B2. B1 is connected to LAN1 and LAN2 and bridges B2 is connected to LAN2 and LAN3. The routing procedure for an incoming frame depends on the LAN it arrives on (the source LAN) and the LAN its destination is on (the destination LAN), as follows:

1) If destination and source LANs are the same, discard the frame. (For example packet from A is going to B. Both are on the same LAN i.e. LAN1).

2) If the destination and source LANs are different, forward the frame. (For example, a packet from A on LAN1 has to go to D on LAN 3)

3) If the destination LAN is unknown, use flooding.

When the bridges are first plugged in, all its hash tables are empty. None of the bridges know where these destination nodes are exactly. Therefore, they use a flooding algorithm: every incoming frame for an unknown destination is output on all the LANs to which the bridge is connected, except to the one it arrived on. Gradually, the bridges learn where destinations are. Once the destination is known there is no more flooding and the packet is forwarded on the proper LAN.

The algorithm used by the transparent bridges is called **backward learning.** As mentioned above, the bridges operate in promiscuous mode, so they see every frame sent on any of their LANs. By looking at the source address, they can tell which machine is accessible on which LAN. For example, if bridge B2 in Figure 10 sees a frame on LAN 3 coming from D*,* it knows that D must be reachable via LAN 3, so it makes an entry in its hash table noting that frames going to D should use LAN 3.

4.7.3 Spanning Tree Bridges

For reliability, some networks contain more than one bridge, which increases the likelihood of *networking loops.* A networking loop occurs when frames are passed from bridge to bridge in a circular manner, never reaching its destination. To prevent networking loops when multiple bridges are used, the bridges communicate with each other and establish a map of the network to derive what is called a spanning tree for all the networks. A spanning tree consists of a single path between source and destination nodes that does not include any loops. Thus, a spanning tree can be considered to be a loop-free subset of a network's topology. The spanning tree algorithm, specified in IEEE 802.1d, describes how bridges (and switches) can communicate to avoid network loops.

4.7.4 Source Routing Bridges

IBM introduced source routing bridges for use in token ring networks. With source routing, the sending machine is responsible for determining whether, a frame is destined for a node on the same network or on a different network. If, the frame is destined for a different network, then, the source machine designates this by setting the high-order bit of the group address bit of the source address to 1. It also includes in the frame's header the path the frame is to follow from source to destination. Source routing bridges are based on the assumption that a sending machine will provide routing information for messages destined for different networks. By making the sending machine responsible for this task, a source routing bridge can ignore frames that have not been "marked" and forward only those frames with their high-order destination bit set to 1.

☞ Check Your Progress 2

1) What are the features of a transparent bridge?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

2) What are the difficulties in building a bridge between the various 802 LANs ?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4.8 SUMMARY

In this unit we discussed two major topics wireless LANs and switching mechanism at the data link layer with IEEE at the data link layer. With IEEE 802.11 standardisation, wireless LANs are becoming common in most of the organisations but, they have their own problems and solutions CSMA/CD does not work due to hidden station problem. To make CSMA work better two new protocols, MACA and MACAW were discussed. The physical layer of wireless LAN standard i.e. IEEE 802.11 allows five different transmission modes, including infrared, various spread spectrum schemes etc. As a part of inter LANs connecting mechanism we discussed different types of bridges. Bluetooth was not taken up in this unit, although, it is a very important topic today. It is a also a wireless network used for connecting handsets and other peripherals to computers without wires.

4.9 SOLUTIONS/ANSWERS

Check Your Progress 1

1) The problem of a station not being able to detect another node for the medium because the competitor is outside its wireless range is called hidden station problem.

2) The crux of the issue is that the CSMA can be applied to wireless environment. Because it simply informs whether there is a transmission activity around the sender node that senses the carrier. Whereas, in a wireless environment, before sending a transmission, a station needs whether there is activity around the receiver or not. With a wire, all signals inform all stations, so, only one transmission can take place at a time, anywhere in the system.

3) It is different in the following ways:

   - Addition of a data link layer acknowledgement
   - Addition of carrier sensing
   - An improved backoff mechanism
   - Addition of DS message

Check Your Progress 2

1) It is a plug and play device. There are no additional requirement of Hardware and Software changes, no setting of address switches, no downloading of routing table, in case, it is used to connect LANs. It does not affect the operation of LANs.

2) The following are the difficulties in building a bridge between the various 802 LAN:
   i) Different frame formats
   ii) Different data rates
   iii) Different frame length
   iv) Security.

4.10 FURTHER READINGS

1) *Computer Networks*, A. S. *Tanenbaum* 4th Edition, Practice Hall of India, New Delhi. 2003.

2) *Computer Networking*, J.F. Kurose & K.W. Ross, A Top Down Approach Featuring the Internet, Pearson Edition, 2003.

3) *Introduction to Data Communication & Networking,* Behrouz Forouzan, Tata McGraw Hill, 1999.

4) *Communications Networks*, Leon Garcia, and Widjaja, Tata McGraw Hill, 2000.

5) *Data and Computer Communications,* Willian Stallings, 6th Edition, Pearson Education, New Delhi.