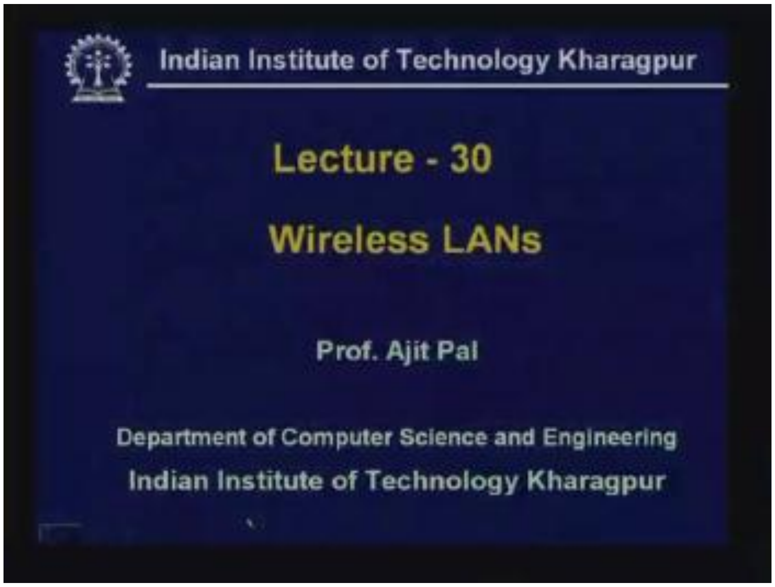
Data Communication
Prof. A. Pal
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture # 30
Wireless LANs

Hello viewers, welcome to today’s lecture on wireless local area networks.

(Refer Slide Time: 01:01)



Indian Institute of Technology Kharagpur

Lecture - 30

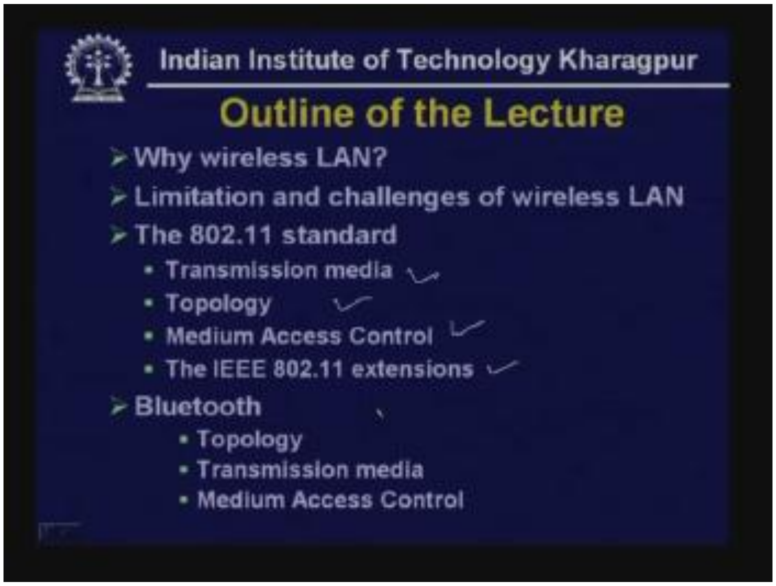
Wireless LANs

Prof. Ajit Pal

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

In the last two lectures we discussed about two different types of LANs. In the first lecture on LAN we discussed about the legacy LAN based on IEEE 802.3, 4 and 5 and in the last lecture we have discussed about the high speed LANs using token ring that is FDDI and also by using CSMA/CD particularly the Fast Ethernet and Gigabit Ethernet. Today we shall discuss about the wireless LANs. Here is the outline of the lecture.

(Refer Slide Time: 02:30)



Indian Institute of Technology Kharagpur

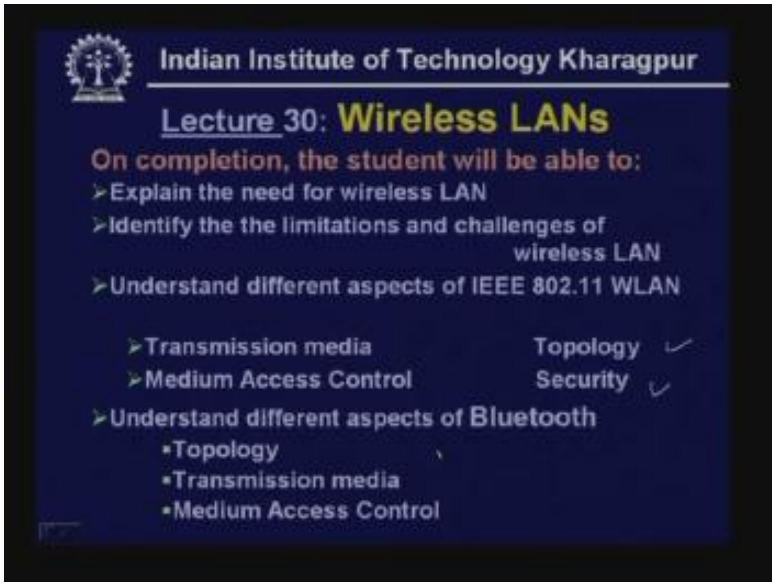
Outline of the Lecture

- Why wireless LAN?
- Limitation and challenges of wireless LAN
- The 802.11 standard
  - Transmission media ✓
  - Topology ✓
  - Medium Access Control ✓
  - The IEEE 802.11 extensions ✓
- Bluetooth
  - Topology
  - Transmission media
  - Medium Access Control

First we shall discuss why wireless LAN and then consider some of the points we will be discussing dealing with limitation and challenges of wireless LAN then we shall consider two important standards; one is IEEE 802.11 standard and various aspects of this standard like transmission media, topology, medium access control and also various extensions that have taken place. Then another very important technology is Bluetooth. Although it is not LAN it is essentially used for private area network PAN. We shall consider topology transmission medium and also medium access control technique used in Bluetooth.

And on completion the student will be able to explain the need for wireless LAN and they will be able to identify the limitations and challenges of wireless LAN, they will be able to understand different aspects of IEEE 802.11 wireless LAN particularly the transmission media, topology, medium access control and security techniques used in this particular standard.

(Refer Slide Time: 03:20)



Indian Institute of Technology Kharagpur

Lecture 30: Wireless LANs

On completion, the student will be able to:

- Explain the need for wireless LAN
- Identify the the limitations and challenges of wireless LAN
- Understand different aspects of IEEE 802.11 WLAN
  - Transmission media   Topology ✓
  - Medium Access Control   Security ✓
- Understand different aspects of Bluetooth
  - Topology
  - Transmission media
  - Medium Access Control

They will be able to understand different aspects of Bluetooth particularly the topology, transmission media and medium access control. First let us focus on why wireless LAN.

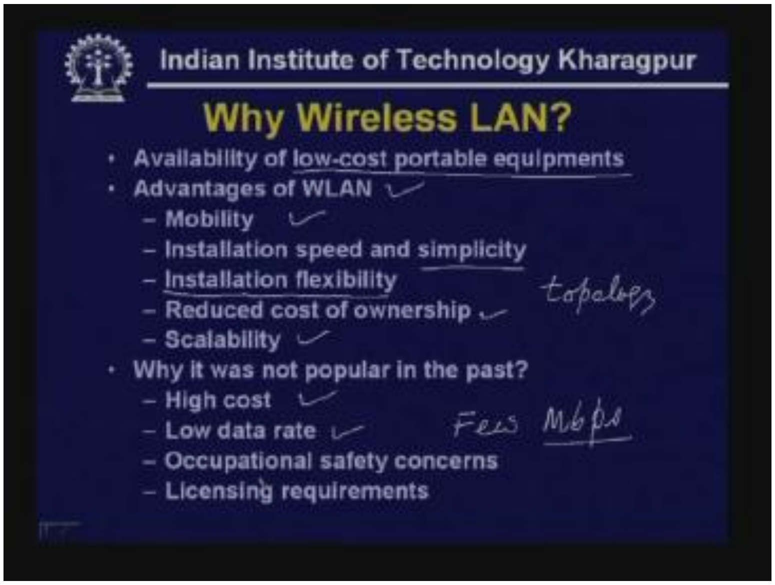
In the last couple of years the number of portable equipments have increased exponentially because of the advancement of VLSI technology and miniaturization possible. Now small sized battery operated computer laptops, palmtops, cell phones, PDAs all these are available. So these low-cost portable equipments are essentially the driving force behind wireless LAN. Moreover, it offers many advantages. First of all it is mobility. when a person is traveling, when a person is possibly taking food in a restaurant, when a person is attending conference or a meeting even then he can communicate with the other computers so the mobility is the main feature of this wireless LAN. It allows mobility.

People are on the move nowadays and while moving, while going from one place to another they can communicate with others. And also it has got other benefits. For example, it is installation speed and simplicity. Wireless LAN can be installed in a matter of hours. On the other hand, wired LAN will take very long time to install. You have to do the wiring, cabling and also install equipments and various other things. It is quite simple to install and deploy.

It offers installation flexibility. By installation flexibility I mean very easily it can be configured in various ways. It can have different types of topology, you can configure it and reconfigure it many ways so it gives you a very flexible way of deploying local area network. Then it has got reduced cost of ownership. Initial cost of deploying wireless LAN may be little high but in the long run whenever particularly you are in a dynamic situation you are moving from one office to another, you are expanding the business so in such situation it offers you reduced cost of ownership.

Scalability is another important advantage. It can be very easily scaled. Initially business can start with few computers and as the business grows or whenever the need for more and more computers and other equipment increase they can be very easily connected to the LAN by using the wireless LAN technique. And you may be asking if it has got so many advantages why it was not so popular in the past. There are several reason for that. First of all earlier the cost was very high, thanks to the advancement of VLSI technology, cost is gradually decreasing based on Moore's Law, you may have heard of it, the cost is decreasing at a fast rate and as a result this is one of the factors which is pushing wireless LAN technology.

(Refer Slide Time: 07:44)



Indian Institute of Technology Kharagpur

Why Wireless LAN?

- Availability of low-cost portable equipments
- Advantages of WLAN
  - Mobility
  - Installation speed and simplicity
  - Installation flexibility topology
  - Reduced cost of ownership
  - Scalability
- Why it was not popular in the past?
  - High cost
  - Low data rate Few Mbps
  - Occupational safety concerns
  - Licensing requirements

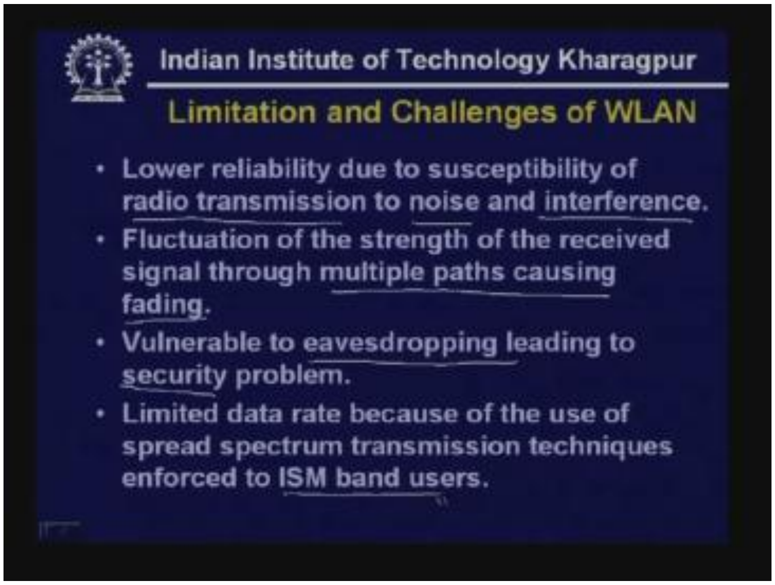
Of course it has got another limitation. It has got low data rate compared to the high speed of wired LAN. We have seen that now, ten gigabits per second is available, LANs are available. On the other hand you will see the data rate for wireless LAN is limited to few Mbps so it is only few Mbps. but this few Mbps may serve the purpose in many situations. Another important concern is occupation safety concerns.

People were not very sure whether wireless LAN is affecting their health or not, even that controversy is going on. For example, whether these cell phones should be used or cell phone has some effect on the health, this is not known so there were some occupational safety concerns regarding the use of wireless LAN so there is a question mark but people have started using it so far no ill effects have been reported.

Another important limitation is licensing requirements. Whenever the transmission is done in a particular frequency certain frequencies cannot be used so you have to take permission, you have to take license so there are disputes and restrictions or a restriction on the use of different frequency bands and as a result there is a constraint from the view point of licensing requirements. So these were the limitations. In spite of that wireless LAN is gradually becoming popular.

Although it has got some advantages and disadvantages it offers a number of limitations and also a number of challenges. First one is low reliability due to susceptibility of radio transmission to noise and interference. In case of wired LAN this problem is much less because you are sending data through some kind of guided media. On the other hand, in case of wireless transmission it is susceptible to radio transmission to noise and interference. Other devices may be working in the same frequency band so that will interfere with the signal. As a result there is some reliability concern regarding the susceptibility of radio transmission to noise and interference.

(Refer Slide Time: 9:44)



Indian Institute of Technology Kharagpur

Limitation and Challenges of WLAN

- Lower reliability due to susceptibility of radio transmission to noise and interference.
- Fluctuation of the strength of the received signal through multiple paths causing fading.
- Vulnerable to eavesdropping leading to security problem.
- Limited data rate because of the use of spread spectrum transmission techniques enforced to ISM band users.

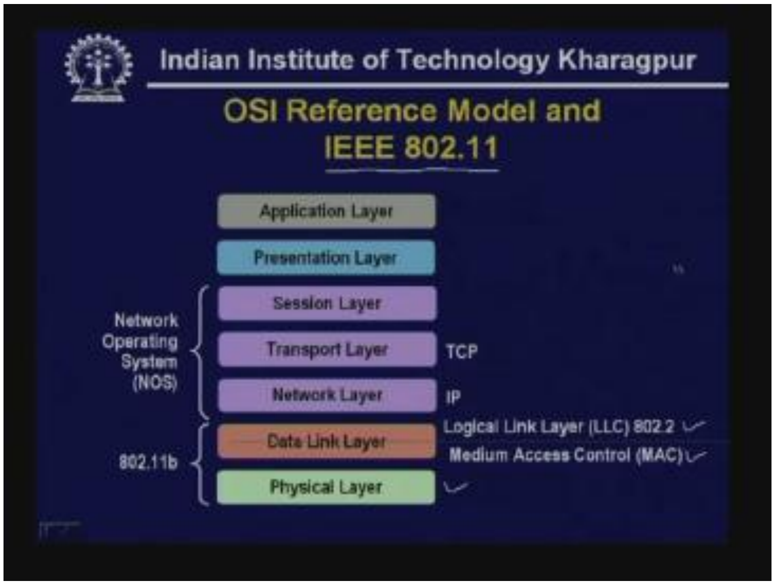
Fluctuation of strength of the received signal through multiple paths causing fading, so these signals can come through multiple paths and that leads to fading. It is a common phenomenon. In TV you must have seen ((ghost)) images and other things because of multiple paths. That problem arises in wireless LAN.

Another problem is due to security. So it is vulnerable to eavesdropping leading to security concern. So whenever somebody is transmitting some signal in wireless media obviously it is some kind of broadcasting, anybody can intercept that and make improper use of it. Thus, eavesdropping is a concern.

Finally limited data rate because of the use of spread spectrum transmission techniques enforced to the ISM band users. As we shall see one important technique that is spread spectrum is used in case of wireless LAN and this leads to smaller data rate compared to wired LAN data rates. These are the limitations and challenges ahead of wireless LAN. Let us see how some of these limitations and challenges are overcome.

First we shall focus on important standard that is IEEE 802.11. The most popular standard is IEEE the 802.11b which is commonly used nowadays and like any other LAN technology it uses two layers physical layer and data link layer and data link layer again has got two sublayers one is medium access control layer and logical link control layer which is common to any other LAN. So essentially these two medium access control layer and physical layer will be different and other part will be the same like the upper layers can be TCP, IP and other things.

(Refer Slide Time: 11:45)



Indian Institute of Technology Kharagpur

OSI Reference Model and IEEE 802.11

Application Layer

Presentation Layer

Network Operating System (NOS)

Session Layer

Transport Layer TCP

Network Layer IP

802.11b

Data Link Layer

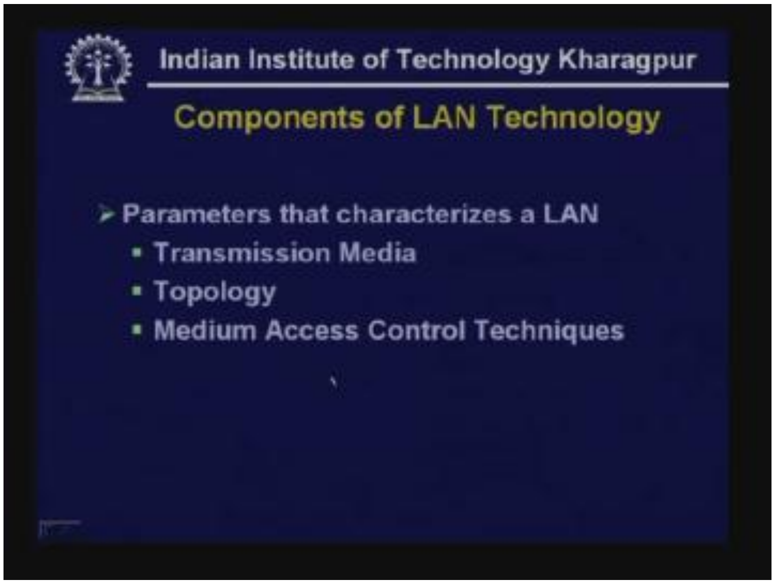
Logical Link Layer (LLC) 802.2

Medium Access Control (MAC)

Physical Layer

As we have already mentioned there are three important parameters that characterize a LAN; the transmission media, topology and medium access control techniques. So we shall focus on these three aspects of the two wireless LANS that we shall discuss in this lecture.

(Refer Slide Time: 12:05)



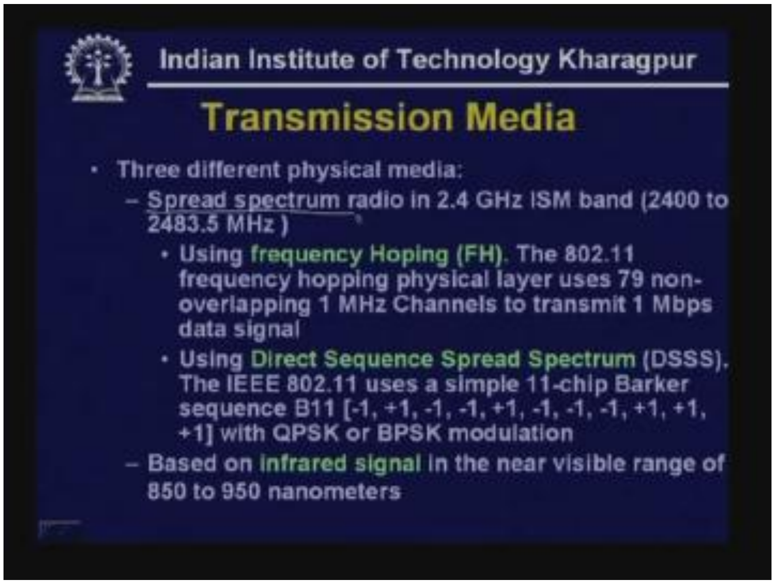
Indian Institute of Technology Kharagpur

Components of LAN Technology

- Parameters that characterizes a LAN
  - Transmission Media
  - Topology
  - Medium Access Control Techniques

First is the transmission media.

(Refer Slide Time: 12:27)



Indian Institute of Technology Kharagpur

Transmission Media

- Three different physical media:
  - Spread spectrum radio in 2.4 GHz ISM band (2400 to 2483.5 MHz)
    - Using frequency Hoping (FH). The 802.11 frequency hopping physical layer uses 79 non-overlapping 1 MHz Channels to transmit 1 Mbps data signal
    - Using Direct Sequence Spread Spectrum (DSSS). The IEEE 802.11 uses a simple 11-chip Barker sequence B11 [-1, +1, -1, -1, +1, -1, -1, -1, +1, +1, +1] with QPSK or BPSK modulation
  - Based on infrared signal in the near visible range of 850 to 950 nanometers

As I mentioned the 802.11 in fact any wireless LAN technique uses spread spectrum technique so spread spectrum radio in 2.4 GHz ISM band that is 2400 to 2483.5 MHz, this is the ISM band (Refer Slide Time: 12:50). The ISM band is very popular which is used by most of the household equipments.

What is the typical characteristic of spread spectrum?

In spread spectrum there are two popular approaches. Frequency Hoping, this is Frequency Hoping spread spectrum and another is Direct Sequence Spread Spectrum. In both the cases what is being done is the frequency spectrum is spread over a wider range. For example, if the initial frequency spectrum is like this and after spread spectrum technique it is spread over a much higher frequency band. It has got several advantages.

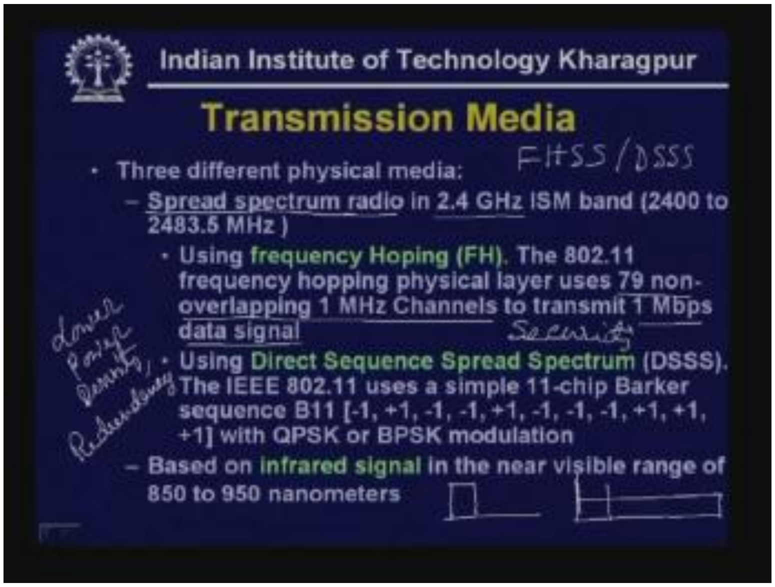
Power Density: It gets spread over a much wider frequency band. This has got many advantages. Whenever it is concentrated on a small frequency band it adversely affects other wireless equipments, so this is being overcome and also this allows some kind of redundancy. Thus, there are two aspects; one is lower power density. For example, in this frequency band power density is lower compared to this one and redundancy. These are the two important benefits of this spread spectrum technique.

These two approaches Frequency Hoping and Direct Sequence Spread Spectrum use two radically different approaches. For example in case of frequency hoping spread spectrum technique the frequency uses 79 non-overlapping one megahertz channels to transmit 1 Mbps data signal. So this frequency hoping technique is somewhat like this.

Suppose you have to transmit some FM radio signal what can be done is a small part of the music can be sent using one carrier frequency, next part can be sent by using another carrier frequency, next part by using another carrier frequency and so on. So the receiver also has to keep on changing the carrier frequency if it wants to listen otherwise it will not be able to listen so it has got two benefits.

Number one is power density becomes smaller over a small spectrum frequency band. Another advantage is that it provides you higher security. If it is used to a particular frequency it will simply hear some noise so they will not be able to receive the music. This is the first approach.

(Refer Slide Time: 16:02)



Indian Institute of Technology Kharagpur

Transmission Media

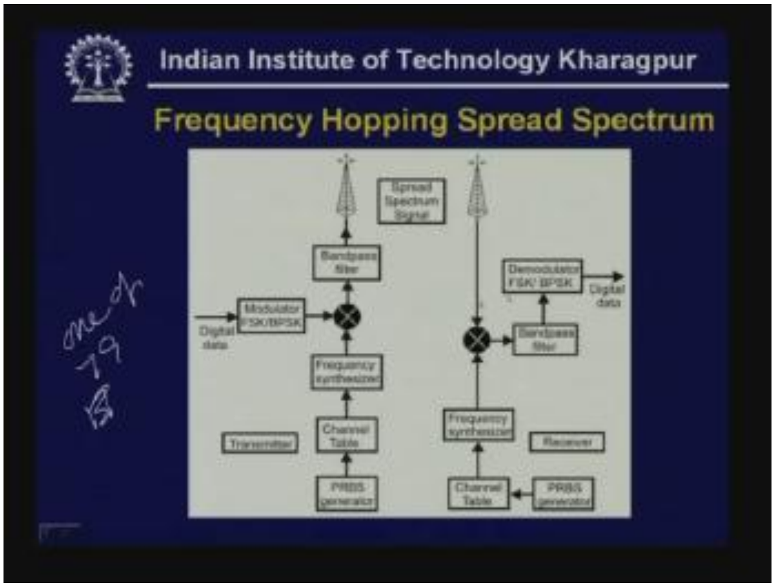
- Three different physical media: FHSS / DSSS
  - Spread spectrum radio in 2.4 GHz ISM band (2400 to 2483.5 MHz)
    - Using frequency Hoping (FH). The 802.11 frequency hopping physical layer uses 79 non-overlapping 1 MHz Channels to transmit 1 Mbps data signal Security
    - Using Direct Sequence Spread Spectrum (DSSS). The IEEE 802.11 uses a simple 11-chip Barker sequence B11 [-1, +1, -1, -1, +1, -1, -1, -1, +1, +1, +1] with QPSK or BPSK modulation
  - Based on infrared signal in the near visible range of 850 to 950 nanometers

Lower Power Density, Redundancy

The carrier frequency keeps on changing and it sends 79 such frequency channels for sending the signal. Then using Direct Sequence Spread Spectrum particularly in case of 802.11 it uses a simple eleven chip barker sequence, this is the barker sequence with QPSK or BPSK modulation. That means first some kind of modulo 2 addition is performed.

For example, using the sequence this plus 1 corresponds to plus 1, minus 1 some kind of modulo 2 addition is performed with 0 or 1 and then QPSK or BPSK modulation is performed before transmission. And third approach is based on infra red signal in the near visible range of 850 to 950 nanometer; this is also used but not that popular. We shall mainly focus on the spread spectrum techniques which are commonly used. This is the basic schematic diagram of the transmitter and receiver used in frequency hoping spread spectrum technique.

(Refer Slide Time: 17:50)

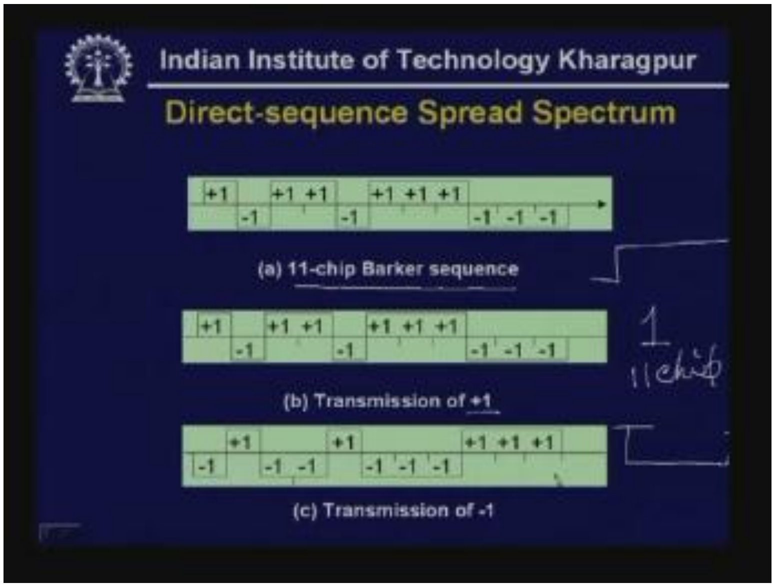


Indian Institute of Technology Kharagpur

Frequency Hopping Spread Spectrum

As you can see there is a pseudo random sequence generator which can select one of the 79 frequency channels. So you have got 79 frequency channels so this pseudo random code will select one of the channel and with the help of the frequency synthesizer that carrier frequency generated is being multiplied the modulator FSK BPSK data comes and that is multiplied and it is passed through a band pass filter and it is transmitted so here you get the spread spectrum signal. but at the other end the signal is received and by using the same pseudo random binary sequence generator it generates the sequence in the same order as it is done in the transmitter then the carrier frequency is generated with the help of the sequence synthesizer and channel table and it is being multiplied with the received signal and then it passes through the band pass filter and finally it is demodulated whether it is FSK or BPSK and by performing demodulation here we get the digital data. This is how the frequency hoping spread spectrum operates.

(Refer Slide Time: 18:50)


Indian Institute of Technology Kharagpur

Direct-sequence Spread Spectrum

(a) 11-chip Barker sequence

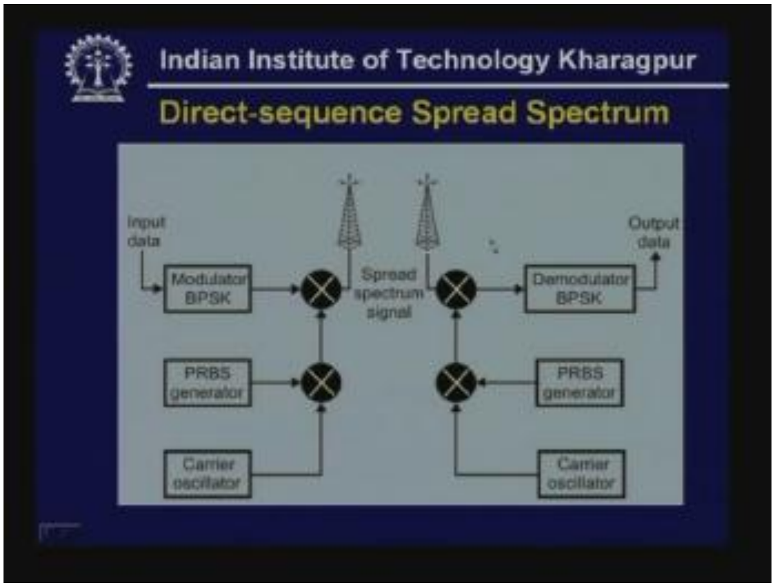
(b) Transmission of +1

(c) Transmission of -1

On the other hand, in case of Direct Sequence Spread Spectrum it uses eleven chip barker sequence and as you can see this is the barker sequence (Refer Slide Time: 19:10) and when a plus 1 is sent simply a 1 is converted into a sequence of eleven chips so it is eleven chips. So this is the signal which is being sent and similarly for a 0 a eleven chip sequence which is just opposite that is being transmitted bit by bit. So this is the transmission of minus 1 and this is the transmission of plus 1. So plus 1 is essentially 1 and minus 1 is 0, this is used for pedagogical purposes.

Therefore, using this eleven chip sequence the transmitter and receiver schematic is shown here. this is the carrier oscillator (Refer Slide Time: 19:58) that pseudo random sequence generator which essentially generates that barker sequence which is multiplied then the data comes and it is modulated by BPSK then this is demodulated and sent.

(Refer Slide Time: 20:12)

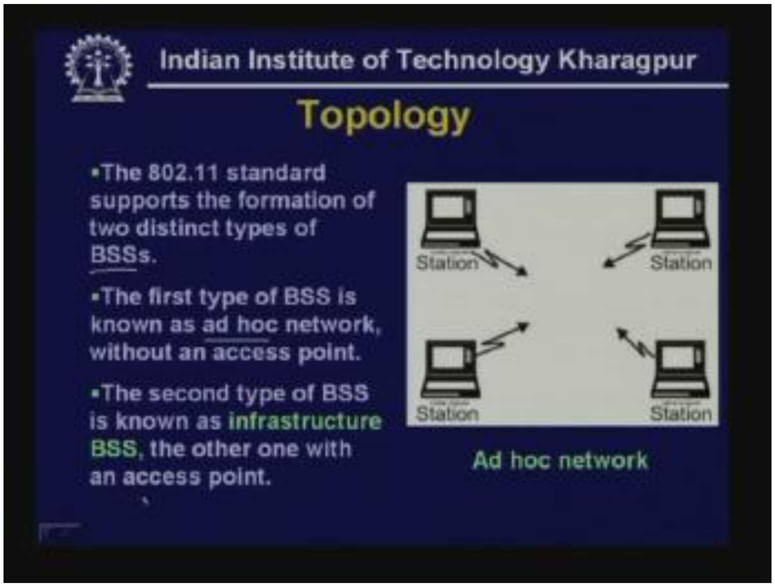


Indian Institute of Technology Kharagpur

Direct-sequence Spread Spectrum

The spread spectrum signal is transmitted and at the other end it is received and using the same sequence the multiplication is done then after demodulation you get back the output data. This is how the Direct Sequence Spread Spectrum occurs. This is the transmission media.

(Refer Slide Time: 21:00)



Indian Institute of Technology Kharagpur

Topology

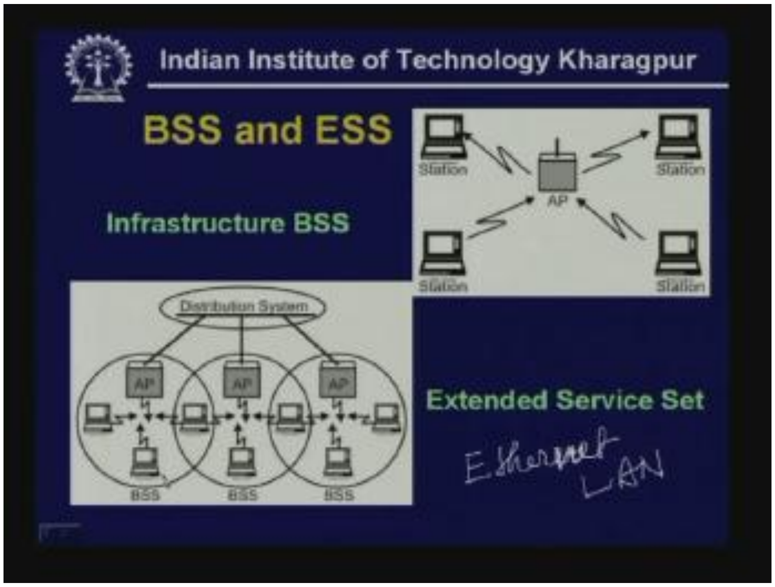
- The 802.11 standard supports the formation of two distinct types of BSSs.
- The first type of BSS is known as ad hoc network, without an access point.
- The second type of BSS is known as infrastructure BSS, the other one with an access point.

Let us look at the topology, 802.11 standard supports formation of two distinct types of BSS Basic Service Set, BSS stands for Basic Service Set. The first type of Basic Service Set is the ADHOC network in which as you can see you have got four mobile stations, they can directly communicate with each other and form some kind of network.

Second type of Basic Service Set is known as infrastructure Basic Service Set and this one is having a special type of device known as access point. Here you can see there is an access point (Refer Slide Time: 21:17) where all the communication is done through the access point. This access point can be connected to a distribution system. this distribution system can be say Ethernet LAN, there is no restriction, so this can be a Ethernet LAN so on this Ethernet LAN these access points are connected.

As you can see here this is a Basic Service Set, this is another Basic Service Set, this is another Basic Service Set so the mobile stations can move from one Basic Service Set to another Basic Service Set and also the access points can communicate with each other through this distribution system and in this the advantage is the mobile stations can also communicate with stationary stations.

(Refer Slide Time: 22:07)



Indian Institute of Technology Kharagpur

BSS and ESS

Infrastructure BSS

Extended Service Set

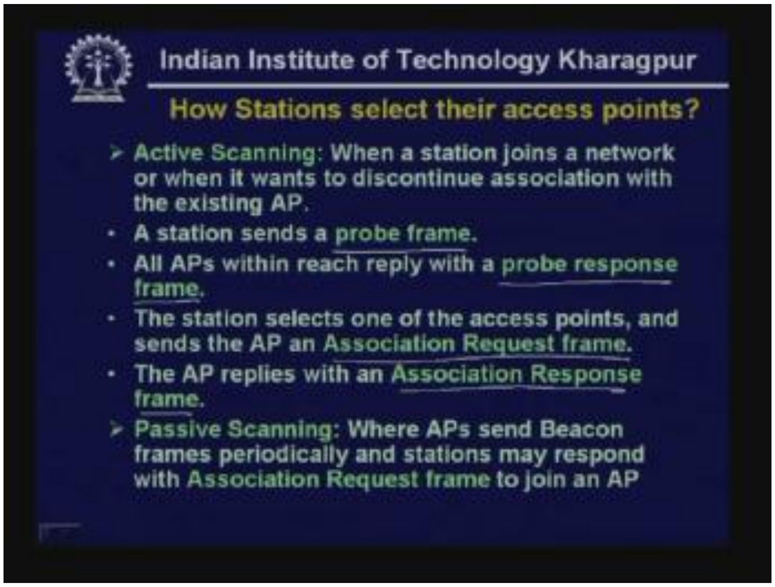
Ethernet LAN

For example, the systems which are connected to the Ethernet LAN connected to the distribution system can communicate with any one of these Basic Service Sets. However, here the communication is little difficult. apart from the address of the destination access point source access point are to be incorporated so some kind of four addresses will be involved as we shall see. This is known as extended services set which requires more than one access points. This is the basic topology used in 802.11.

Now you may be asking how stations select their access points. you have seen in the previous case, say under this Basic Service Set you have got several mobile stations, under this also there are several stations (Refer Slide Time: 23:05), these access points are somewhat similar to base stations used in cellular network. Nowadays cellular telephone is very popular and people are familiar with base stations. These access points are somewhat similar to base stations for these mobile hosts or stations.

Now as you can see this particular mobile host can move gradually from this Basic Service Set to other Basic Service Set. So what is explained here is how they get attached to a particular access point. This can be done in two ways. One is known as active scanning. When a station joins a network or when it wants to discontinue association with the existing access points what it does is, it sends a probe frame and all access points within the reach reply with a probe response frame and the station selects one of the access points and sends the AP an association request frame and the AP replies with association response frame. Thus, these are the frame exchanges that take place and by doing that a particular mobile host gets associated with a particular access point.

(Refer Slide Time: 24:30)



Indian Institute of Technology Kharagpur

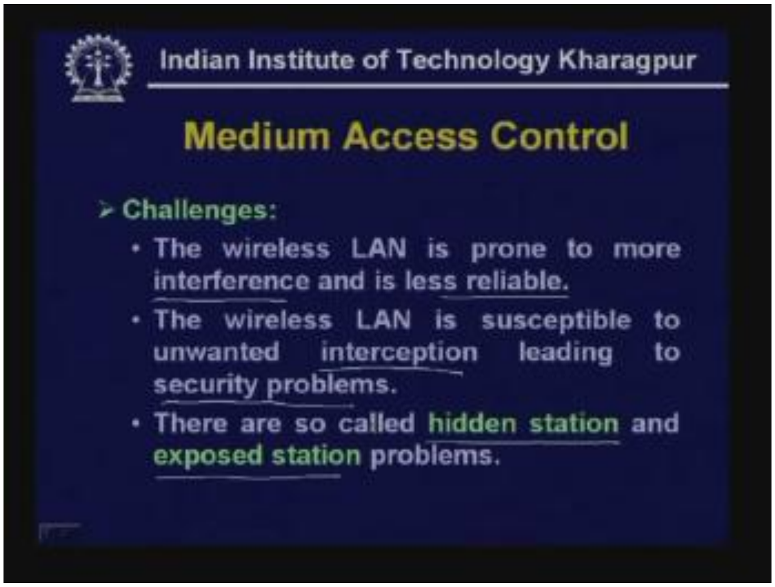
How Stations select their access points?

- Active Scanning: When a station joins a network or when it wants to discontinue association with the existing AP.
  - A station sends a probe frame.
  - All APs within reach reply with a probe response frame.
  - The station selects one of the access points, and sends the AP an Association Request frame.
  - The AP replies with an Association Response frame.
- Passive Scanning: Where APs send Beacon frames periodically and stations may respond with Association Request frame to join an AP

Second approach is passive scanning where access points beacon frames periodically and stations may respond with association request frame to join an access point. So, in this particular case a particular access point can advertise and ask, is anybody there to join me. So in that way it sends the beacon frames and then association request frames are generated by the mobile host to join a particular access point. This is how it takes place. And once the station joins an access point communication is done through that access point.

Now as I mentioned the medium access control in wireless LAN has got several challenges, particularly it is prone to more interference and it is less reliable compared to wired LAN and the wireless LAN is susceptible to unwanted interception leading to security problems. We shall discuss how they can be overcome, moreover there are so called hidden station and exposed station problems which I have discussed in detail while discussing the CDMA protocol.

(Refer Slide Time: 25:40)



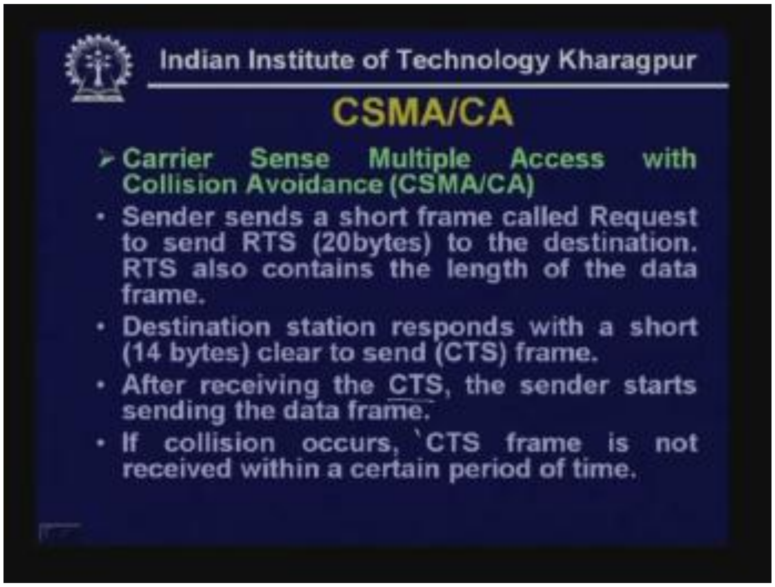
Indian Institute of Technology Kharagpur

Medium Access Control

- Challenges:
  - The wireless LAN is prone to more interference and is less reliable.
  - The wireless LAN is susceptible to unwanted interception leading to security problems.
  - There are so called hidden station and exposed station problems.

In fact this 802.1 uses little extended form of Carrier Sense Multiple Access Collision Avoidance Protocol CSMA/CA protocol and here the sender sends a short frame called request to send which is 20 bytes to the destination so request to send also contains the length of the data frame.

(Refer Slide Time: 26:20)



Indian Institute of Technology Kharagpur

CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Sender sends a short frame called Request to send RTS (20bytes) to the destination. RTS also contains the length of the data frame.
- Destination station responds with a short (14 bytes) clear to send (CTS) frame.
- After receiving the CTS, the sender starts sending the data frame.
- If collision occurs, CTS frame is not received within a certain period of time.

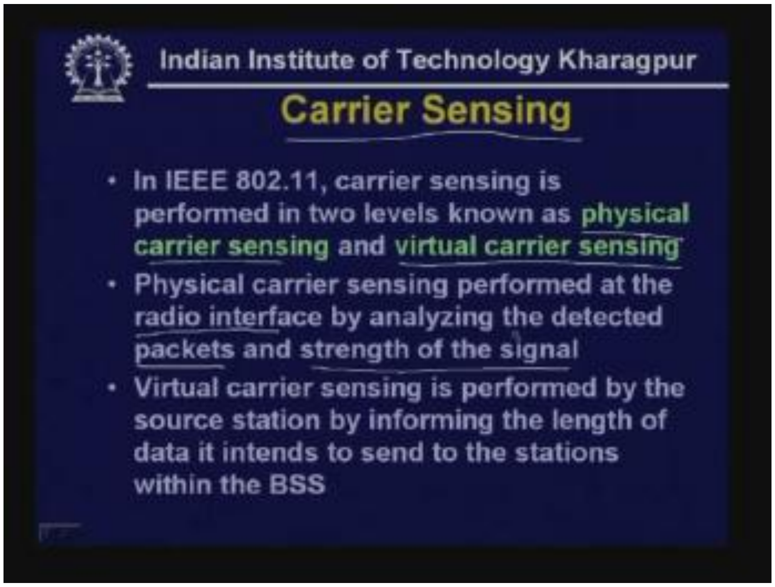
So, destination station responds with a short clear to send frame and after receiving that clear to send frame the sender starts sending the data frame.

Of course in this case collision can still occur as I have explained in detail and in such a case clear to send frame is not received with a certain period of time and that it has to come out from collision by using that binary exponential backoff algorithm used in the case of wired LAN Ethernet, that's why this approach is also known as wireless Ethernet LAN. There are many similarities with Ethernet.

Now, apart from similarities there are some dissimilarities. One is carrier sensing.

In case of wired LAN or Ethernet the carrier sensing is very, very easy; all stations are attached to the medium so from that the carrier sensing can be done. In this particular case carrier sensing is done in two ways. One is known as physical carrier sensing, another is virtual carrier sensing. So, in case of physical carrier sensing physical carrier sensing is performed at the radio interface by analyzing the detected packets and strength of the signal. That means all the mobile stations will be receiving signals generated by other stations within that Basic Service Set and the signals will be analyzed at the radio interface and after performing it will analyze the detected packets comparing the strength of the signals. Obviously whenever there is collision strength of the signal will be ((less)). This is one way of detecting collision.

(Refer Slide Time: 28:00)



Indian Institute of Technology Kharagpur

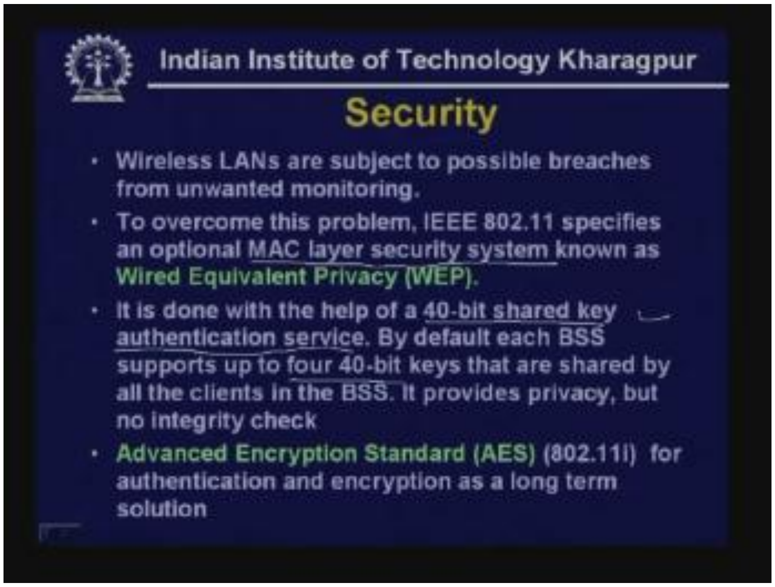
Carrier Sensing

- In IEEE 802.11, carrier sensing is performed in two levels known as physical carrier sensing and virtual carrier sensing
- Physical carrier sensing performed at the radio interface by analyzing the detected packets and strength of the signal
- Virtual carrier sensing is performed by the source station by informing the length of data it intends to send to the stations within the BSS

Another alternative is virtual carrier sensing which is performed by the source station. By informing the length of the data it intends to send to the stations within the Basic Service Set. This is actually related to this protocol. Here as you have seen (Refer Slide Time: 28:38) whenever this request to send frame is sent as a part of that the length of data is also mentioned. That means whenever this clear to send signal is generated all the stations will withdraw except the destination station and all other stations know the length of the data. Obviously for that duration all the stations will not generate any data. These are the two approaches used for carrier sensing. This is virtual so without actually sensing the carrier, carrier sensing is performed because a particular station will send for a specific period of time based on the data rate and length of frame.

Coming to the security, wireless LANs are subject to possible breaches from unwanted monitoring because in case of wireless LAN all the other stations within the range will be able to hear so how to overcome this problem.

(Refer Slide Time: 30:35)



Indian Institute of Technology Kharagpur

Security

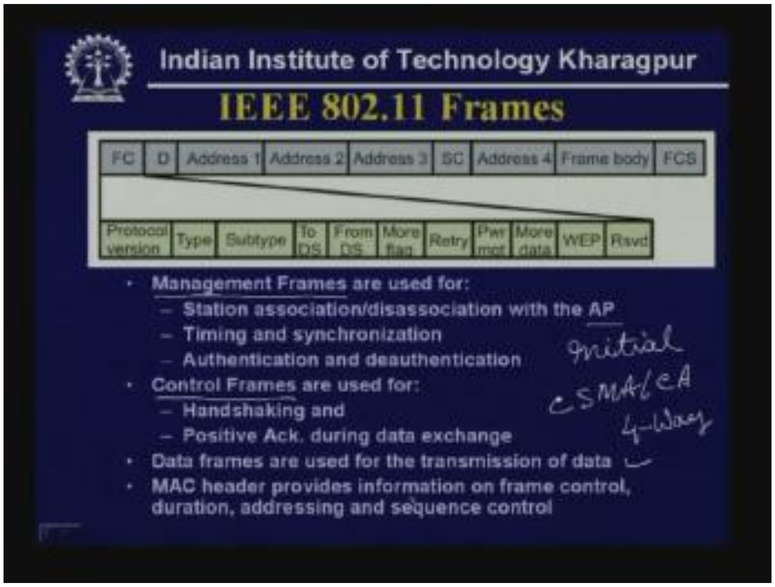
- Wireless LANs are subject to possible breaches from unwanted monitoring.
- To overcome this problem, IEEE 802.11 specifies an optional MAC layer security system known as Wired Equivalent Privacy (WEP).
- It is done with the help of a 40-bit shared key authentication service. By default each BSS supports up to four 40-bit keys that are shared by all the clients in the BSS. It provides privacy, but no integrity check
- Advanced Encryption Standard (AES) (802.11i) for authentication and encryption as a long term solution

To overcome this problem IEEE 802.11 specifies an optional MAC layer security system known as wired equivalent privacy. The basic idea is that it should have the privacy level or security level same as the wired LAN. to do that what is being done is, with the help of a 40-bit shared key authentication service, and by default each Basic Service Set supports up to four 40-bit keys that has shared by all the clients in the Basic Service Set it provides privacy but no integrity check. Later on we shall discuss about this 40-bit shared key authentication service in more detail.

There is some extended version of the standard, Advanced Encrypted Standard AES that is being proposed in this standard 802.11i. This is the revision for authentication and encryption as a long term solution. So by using AES authentication and encryption can be used as a long term solution. Obviously in this particular case there will be an overhead for encryption and decryption but it will give you security as well as authentication.

Now here are the IEEE 802.11 frames. As we know there are three basic operations to be performed by these frames. First of all we have the management frames.

(Refer Slide Time: 32:45)



Indian Institute of Technology Kharagpur

IEEE 802.11 Frames

FC	D	Address 1	Address 2	Address 3	SC	Address 4	Frame body	FCS

Protocol version	Type	Subtype	To DS	From DS	More frag	Retry	Pwr mgt	More data	WEP	Rsvd

- Management Frames are used for:
  - Station association/disassociation with the AP
  - Timing and synchronization
  - Authentication and deauthentication
- Control Frames are used for:
  - Handshaking and
  - Positive Ack. during data exchange
- Data frames are used for the transmission of data
- MAC header provides information on frame control, duration, addressing and sequence control

initial

CSMA/CA

4-Way

Management frames are used for:

- Station association, disassociation with the access points
- Timing and synchronization
- Authentication and deauthentication

I have already explained the protocols in brief and obviously with the help of the management frames these functions are performed. This is required in the initial phase when a particular station gets associated with an access point.

Control frames are used for:

- Handshaking and
- Positive acknowledgement during data exchange

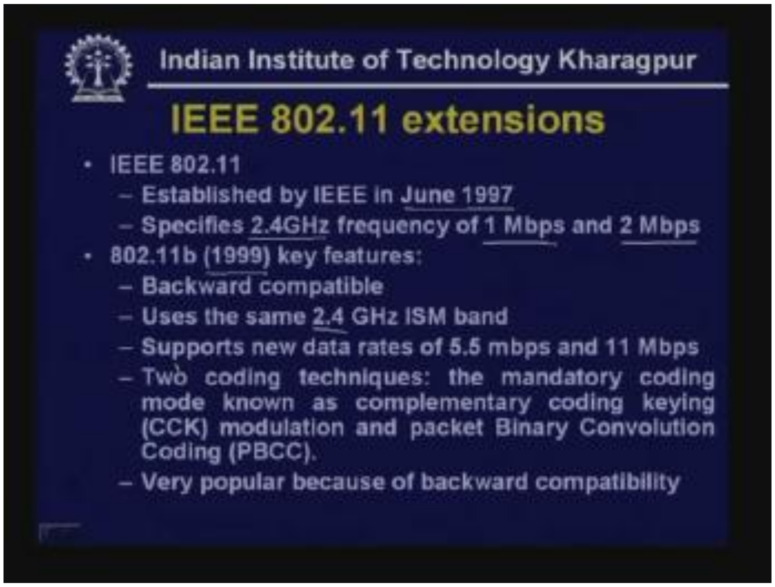
You have seen that CSMA Carrier Sense Multiple Access CA protocol uses a four way handshaking approach so this handshaking and positive acknowledgment during data exchange is going to be performed with the help of these control frames. Finally data frames are used for transmission of data so there are three different types of frames possible in IEEE 802.11 and this frame control bits decides the various types of control frames.

Then MAC header provides information on the control frame duration addressing and sequence control. This is in brief of what is being performed by the various data packets various frames used in IEEE 802.11.

Now, as I mentioned the 802.11 has been extended in various directions. First it was established in June 1997 which specifies 2.4 GHz ISM band and frequency of 1 Mbps or 2 Mbps data rate and it was extended to IEEE 802.11b in 1999 having the following key features:

It is backward compatible with 802.11, it uses the same 2.4 ISM band then it supports new data rates of 5.5 Mbps and 11 Mbps by using special coding and particularly two coding techniques are used. The mandatory coding mode is known as Complementary Coding Key CCK modulation and Packet Binary Convolution Coding.

(Refer Slide Time: 33:50)



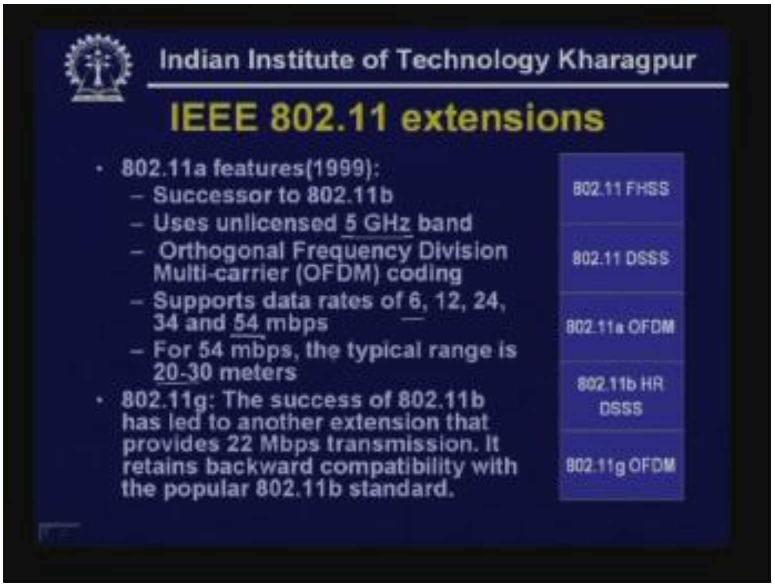
Indian Institute of Technology Kharagpur

IEEE 802.11 extensions

- IEEE 802.11
  - Established by IEEE in June 1997
  - Specifies 2.4GHz frequency of 1 Mbps and 2 Mbps
- 802.11b (1999) key features:
  - Backward compatible
  - Uses the same 2.4 GHz ISM band
  - Supports new data rates of 5.5 mbps and 11 Mbps
  - Two coding techniques: the mandatory coding mode known as complementary coding keying (CCK) modulation and packet Binary Convolution Coding (PBCC).
  - Very popular because of backward compatibility

With the help of coding high data rates are possible 5.5 Mbps and 11 Mbps using the same ISM band. It is very popular because of backward compatibility with the original standard IEEE 802.11. Subsequently IEEE 802.11a has been proposed which is the successor of 802.11 b. It uses unlicensed 5 GHz band and it uses a special type of coding known as orthogonal frequency division multi-carrier coding. It is very similar to frequency division multiplexing but there are some differences and it supports a variety of data rates starting from 6 Mbps to 54 Mbps that is 6, 12, 24, 34 and 54 Mbps and for 54 Mbps the typical range is small 20 to 30 m and for lower rates the range is 100 m.

(Refer Slide Time: 35:28)



Indian Institute of Technology Kharagpur

IEEE 802.11 extensions

- 802.11a features(1999):
  - Successor to 802.11b
  - Uses unlicensed 5 GHz band
  - Orthogonal Frequency Division Multi-carrier (OFDM) coding
  - Supports data rates of 6, 12, 24, 34 and 54 mbps
  - For 54 mbps, the typical range is 20-30 meters
- 802.11g: The success of 802.11b has led to another extension that provides 22 Mbps transmission. It retains backward compatibility with the popular 802.11b standard.

802.11 FHSS

802.11 DSSS

802.11a OFDM

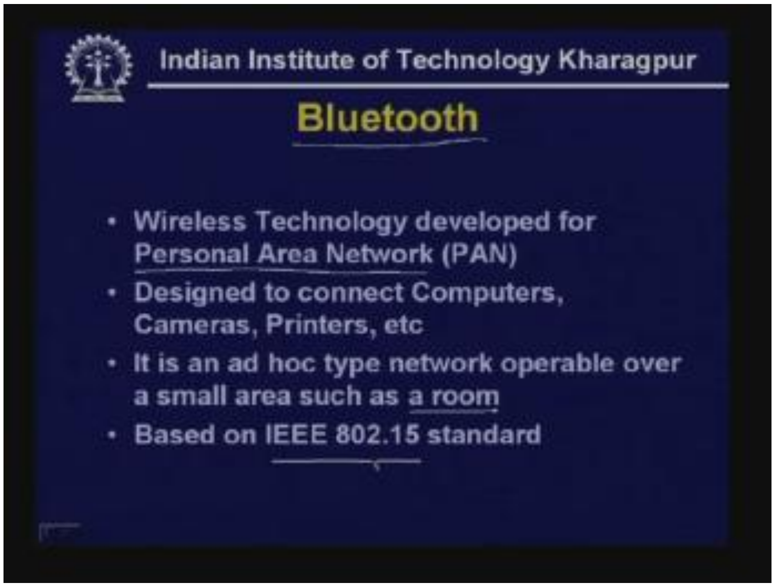
802.11b HR DSSS

802.11g OFDM

Another standard IEEE 802.11g is actually compatible with IEEE 802.11b but 802.11a is not compatible with IEEE 802.11b. The success of IEEE 802.11b has led to another extension that provides 22 Mbps transmission. It retains the backward compatibility with the popular 802.11b standard. Here are the various extensions shown here; 802.11 which is a frequency hoping spread spectrum and Direct Sequence Spread Spectrum, 802.11a which is a OFDM, then IEEE 802.11b which is a Direct Sequence Spread Spectrum and 802.11g which again uses a OFDM.

Now we move on to another important standard which is Bluetooth. This Bluetooth has been developed for personal area networking particularly used for design to connect computers, cameras, printers and various household equipments which are used in houses so this is essentially used as a private area network typically to be used in your house. Nowadays the number of intelligent equipments is increasing in your house which can be networked with personal area network and it is an ADHOC type network operational over a small area such as a room and it is based on IEEE 802.15 standard so you can see that Bluetooth actually conforms to IEEE 802.11 standard.

(Refer Slide Time: 37:20)



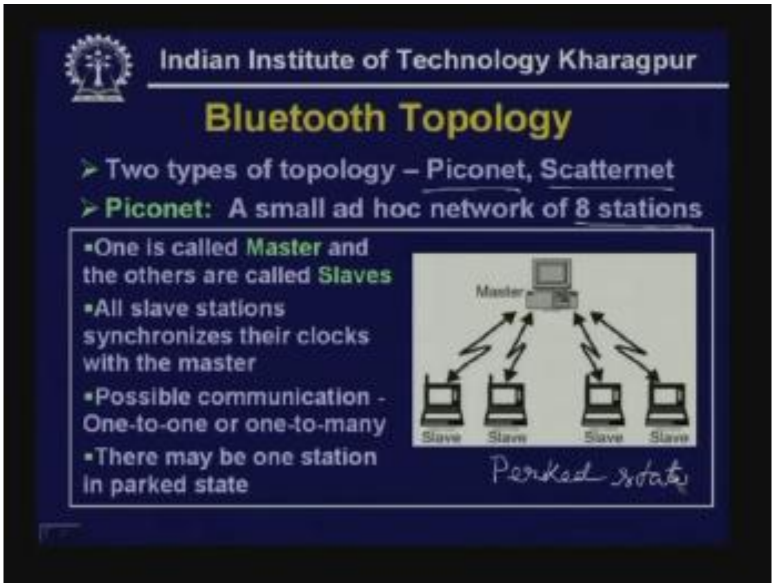
Indian Institute of Technology Kharagpur

Bluetooth

- Wireless Technology developed for Personal Area Network (PAN)
- Designed to connect Computers, Cameras, Printers, etc
- It is an ad hoc type network operable over a small area such as a room
- Based on IEEE 802.15 standard

Here is the Bluetooth topology, it supports two types of topology. First one is Piconet, second one is Scatternet. Piconet is a very small ADHOC network with only eight stations. As you can see it has got a master and others are slaves. So you can have one master and seven slaves. Of course apart from seven slaves one slave can be kept as standby or it can be kept as parked state.

(Refer Slide Time: 38:05)



Indian Institute of Technology Kharagpur

Bluetooth Topology

- Two types of topology – Piconet, Scatternet
- Piconet: A small ad hoc network of 8 stations

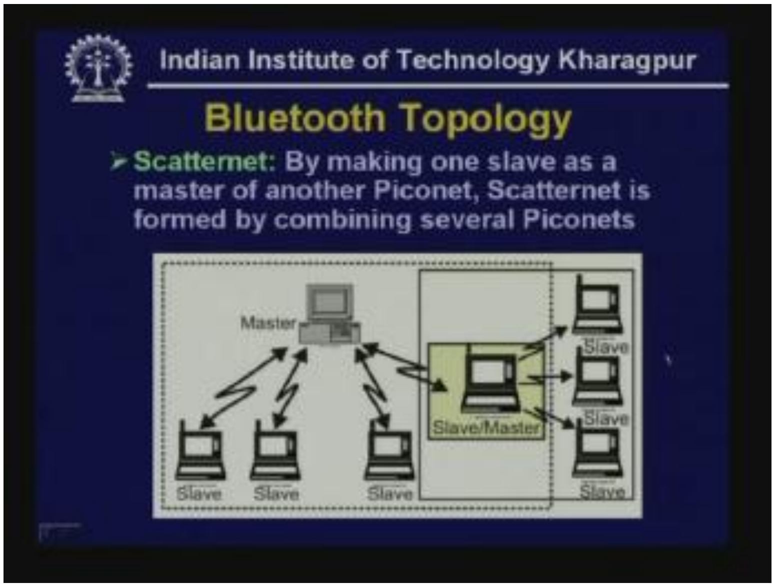
•One is called Master and the others are called Slaves
•All slave stations synchronizes their clocks with the master
•Possible communication - One-to-one or one-to-many
•There may be one station in parked state

Parked state

However, if this particular slave wants to join then one of the active slave has to be taken out. All slave stations synchronize their clock with the master. That means all the communication is performed through the master and possible communication can be one to one or one to many so there are two possibilities and there may be one station in a parked state as I mentioned. That can join only when one of the active slaves is taken out.

The second technology that is being used is Scatternet. As you can say it makes one slave as a master of another Piconet. Here as you can see this is one Piconet (Refer Slide Time: 38:58) and this is the master and this is one of the slaves and this slave is now made master of another Piconet so here you have got eight stations out of which this is one slave and this slave now becomes a master of another Piconet. So in this way you can have Scatternet and number of such mobile stations can be more than 8.

(Refer Slide Time: 39:18)



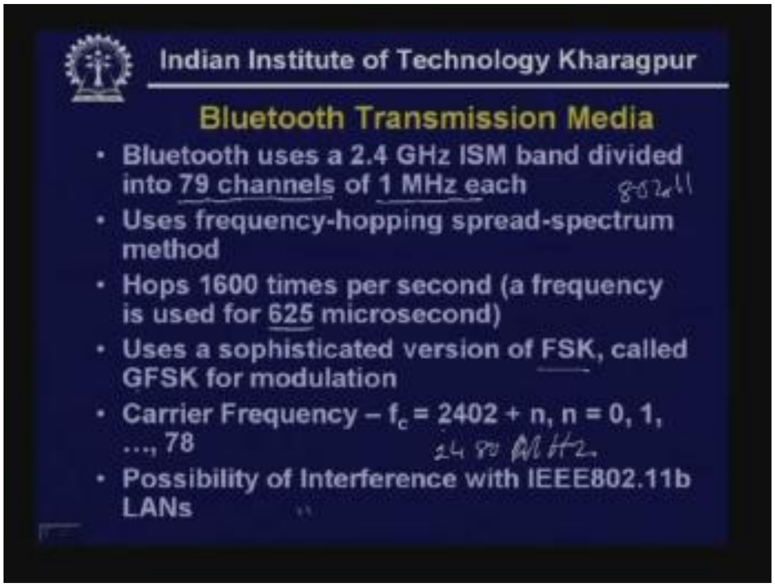
Indian Institute of Technology Kharagpur

Bluetooth Topology

- **Scatternet:** By making one slave as a master of another Piconet, Scatternet is formed by combining several Piconets

So Scatternet is formed by combining several Piconets as it is shown in this diagram. Now let us look at the transmission media.

(Refer Slide Time: 39:40)



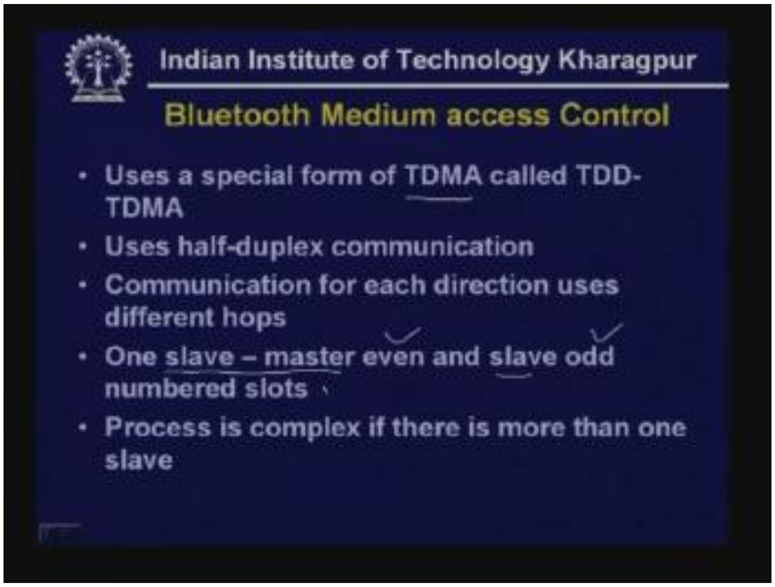
Indian Institute of Technology Kharagpur

Bluetooth Transmission Media

- Bluetooth uses a 2.4 GHz ISM band divided into 79 channels of 1 MHz each 802.11
- Uses frequency-hopping spread-spectrum method
- Hops 1600 times per second (a frequency is used for 625 microsecond)
- Uses a sophisticated version of FSK, called GFSK for modulation
- Carrier Frequency – $f_c = 2402 + n$, n = 0, 1, …, 78 2480 MHz
- Possibility of Interference with IEEE802.11b LANs

The transmission media is same as that being used here, 2.4 GHz ISM band that means it uses the same frequency band that is used in IEEE 802.11 so it uses the same band so there is a possibility of interference. Hence, if you are using Bluetooth and IEEE 802.11 network in the same region there is possibility of interference because of the use of same frequency bands and as you see here also it uses 79 channels each of 1 MHz and it uses Frequency Hoping Spread Spectrum method in case of 802.11 and it hops 1600 times per second so a frequency is used for 625 microseconds only. It uses a sophisticated version of frequency shift key called GFSK for modulation. So the carrier frequencies can be starting with 24002 MHz or 2.402 MHz to, as you can say add 1, add 2 and so on so 2.402 plus 78 means it can go up to 2.80 MHz.

(Refer Slide Time: 42:15)



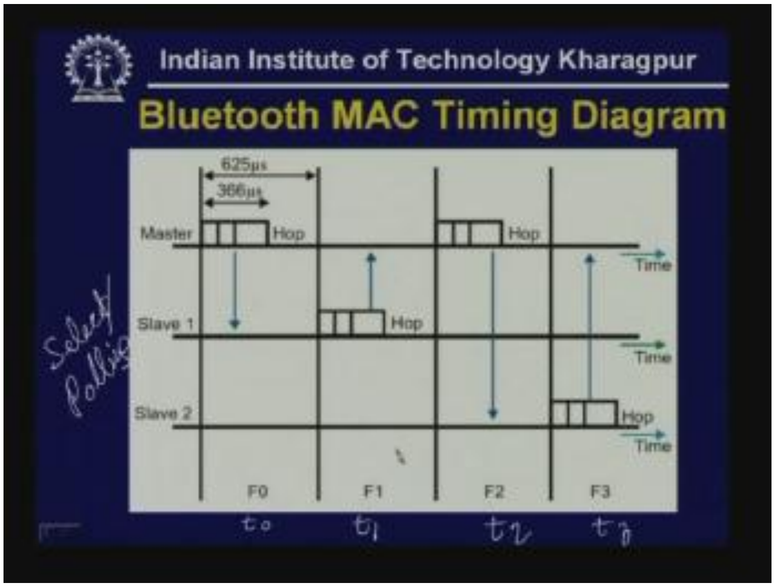
Indian Institute of Technology Kharagpur

Bluetooth Medium access Control

- Uses a special form of TDMA called TDD-TDMA
- Uses half-duplex communication
- Communication for each direction uses different hops
- One slave – master even and slave odd numbered slots
- Process is complex if there is more than one slave

There is a possibility of interference with IEEE 802.11b because they use the same transmission media. so far as the medium access control is concerned it uses a special form of TDMA called TDD TMDA this is essentially some kind of duplex medium half duplex communication as we shall see it performs some kind of half-duplex communication using this TDD TDMA approach and communication for each direction uses different hops different frequencies so the possible alternatives are one slave one master. Therefore, whenever there is one slave one master communication then master uses even slots and slave uses odd numbered slots. This process is more complex when there is more than one slave. Let us see how it is actually being done.

(Refer Slide Time: 43: 00)



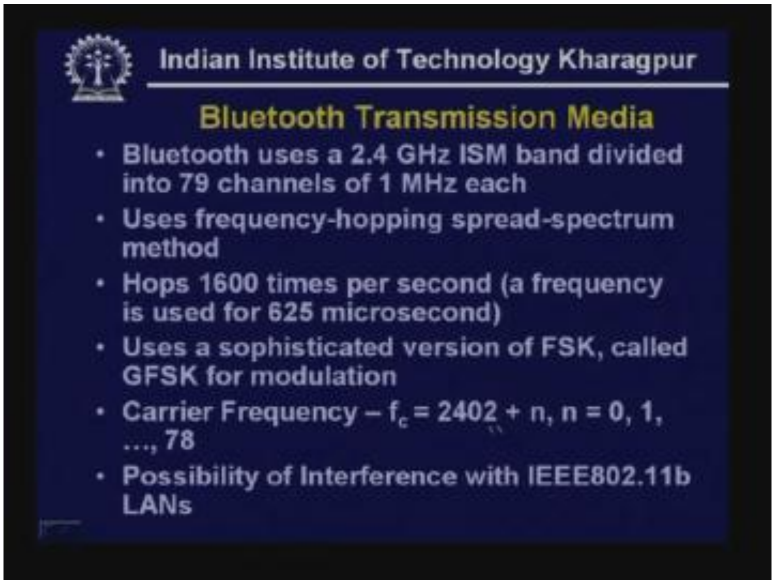
Indian Institute of Technology Kharagpur

Bluetooth MAC Timing Diagram

As you can see here this is the master this is the dwell time, and dwell time is 625 microseconds out of which 366 microseconds is used for sending data and remaining is used for hop control. So it uses a carrier frequency of F0 in the slot t_0 which is the even number of slot. Then the slave sends in slot number t_1 the odd number slot and uses frequency F1. So the frequency hopping is taking place then again master sends in slot t_2 using frequency F2 so in this way alternately it is sent as master slave, master slave so there is some kind of half-duplex communication takes place between the master and slave using frequency hopping.

These are the frequencies that is being used as shown here (Refer Slide Time: 43:31) F0 is 2402 MHz; F1 is 2403 MHz and so on. On the other hand, here as I mentioned this is single slave communication. When you have got multiple slaves the process is little complex.

(Refer Slide Time: 43:40)



Indian Institute of Technology Kharagpur

Bluetooth Transmission Media

- Bluetooth uses a 2.4 GHz ISM band divided into 79 channels of 1 MHz each
- Uses frequency-hopping spread-spectrum method
- Hops 1600 times per second (a frequency is used for 625 microsecond)
- Uses a sophisticated version of FSK, called GFSK for modulation
- Carrier Frequency – $f_c = 2402 + n$, n = 0, 1, …, 78
- Possibility of Interference with IEEE802.11b LANs

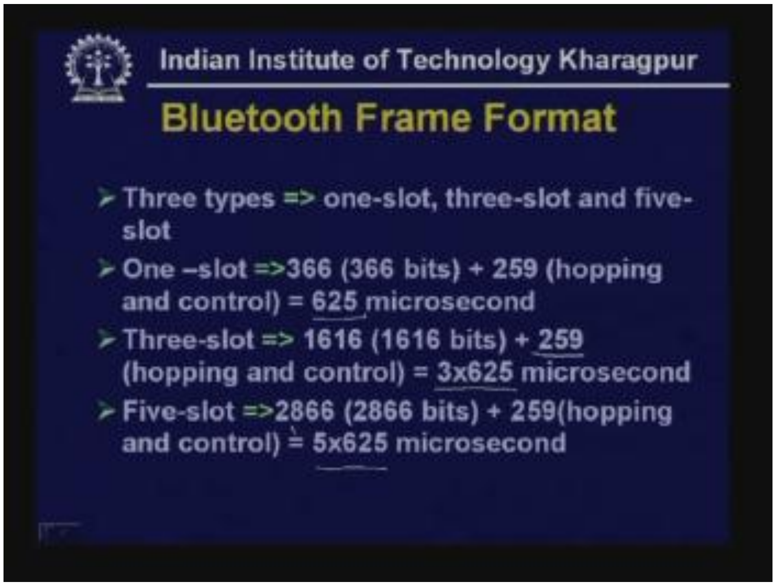
First the master initiates the communication, it sends a frame using frequency F0 in slot t_0. Then essentially it is some kind of select and polling approach. So the station which is being selected or polled responds in the next slot t_1 and uses frequency F1 and it sends the data. In the next sequence again the master sends using slot t_2 even number of slots and uses a frequency F2.

Now it can select another slave then this slave two can respond and sends using frequency F3 in slot t_3. So in this way several slaves can communicate if they are being selected or polled by the master stations. Here also half-duplex communication takes place. However, the even frequencies are being shared by different slaves to send their data one after another.

So far as the Bluetooth Frame Format is concerned there are three types; one-slot, three-slot and five-slot. in case of one-slot it can send 366 bits plus 259 time is used for hopping and control as shown (Refer Slide Time: 45:00) in this case. So this time is used for sending data and this part is used for hopping and control. So, as a consequence the total of 366 bits can be sent in 625 microseconds.

On the other hand, if it is a three-slot frame then as you can see it is divided into two parts, this hopping and control time is fixed, however, during this time after subtracting this much time the total number of bits that can be sent is shown here in three-slot frame. On the other hand, in five-slot frame the total time you get is 5 into 625 microseconds so it is within this time so you can send 2866 bits plus 259 microseconds for hopping and control that is being used.

(Refer Slide Time: 46:20)



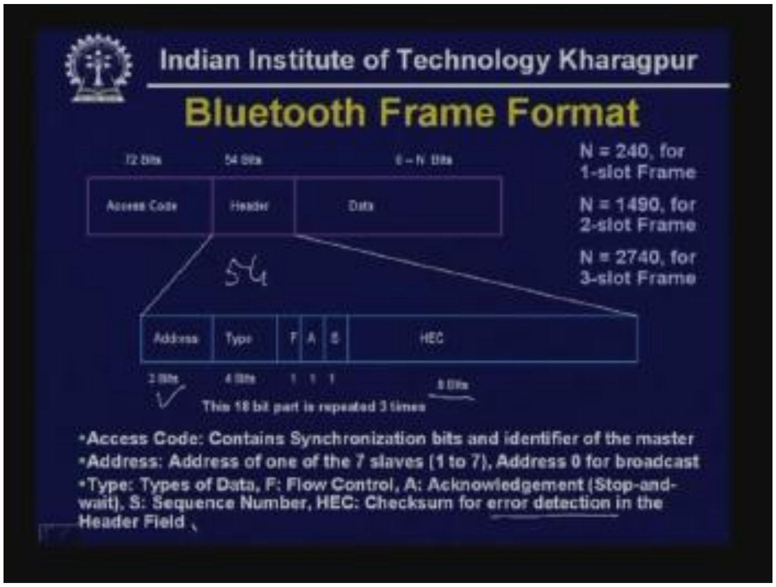
Indian Institute of Technology Kharagpur

Bluetooth Frame Format

- Three types => one-slot, three-slot and five-slot
- One –slot =>366 (366 bits) + 259 (hopping and control) = 625 microsecond
- Three-slot => 1616 (1616 bits) + 259 (hopping and control) = 3x625 microsecond
- Five-slot =>2866 (2866 bits) + 259(hopping and control) = 5x625 microsecond

So you can see the frames can be quite slot comprising one-slot three-slot or five-slot so any one of the frame formats can be used. The detailed frame format is shown here.

(Refer Slide Time: 46:45)



Indian Institute of Technology Kharagpur

Bluetooth Frame Format

72 Bits
54 Bits
0 – N Bits
Access Code
Header
Data
N = 240, for 1-slot Frame
N = 1490, for 2-slot Frame
N = 2740, for 3-slot Frame
54
Address
Type
F
A
S
HEC
3 Bits
4 Bits
1
1
1
8 Bits
This 18 bit part is repeated 3 times

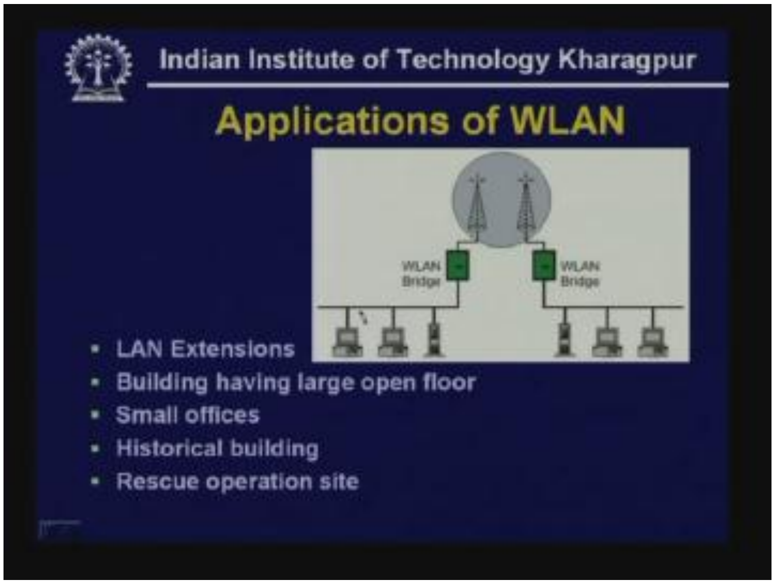
- •Access Code: Contains Synchronization bits and identifier of the master
- •Address: Address of one of the 7 slaves (1 to 7), Address 0 for broadcast
- •Type: Types of Data, F: Flow Control, A: Acknowledgement (Stop-and-wait), S: Sequence Number, HEC: Checksum for error detection in the Header Field

The access code has got 72 bits so it contains synchronization bits, identifier of the master and so on using these 72 bits, then it has got a header of 54 bits so the header is 54 bits and here the eighteen bit is repeated three times so in this 18-bit you have got three bits for address then four bits for type of data that is being sent then as you can see there are three bits; one is flow control, acknowledgment and sequence number. Therefore, here with the help of this approach Bluetooth performs flow control, error control and also acknowledgment by using stop-and-wait control technique and there is a 8-bit checksum that is used for error detection in the header field.

So, as you can see all the features required for reliable communication is provided in this simple frame format. Now comes the data field. In this data field the number of bits can vary from 240 to 2740 so for N is equal to 240 in one-slot frame, N is equal to 1490 for two-slot frame and N is equal to 2740 for three-slot frame so this is the frame format used in Bluetooth.

Now coming to the applications of wireless LAN, wireless LANs can be used in a variety of ways. One is LAN extensions. We have already discussed about wired LANs and different types of wired LANs; the legacy LANs based on IEEE 802 and also the high speed LANs based on FDDI, Fast Ethernet or Gigabit Ethernet. Now they can be extended. For example, here a simple example is shown.

(Refer Slide Time: 48:55)



Indian Institute of Technology Kharagpur

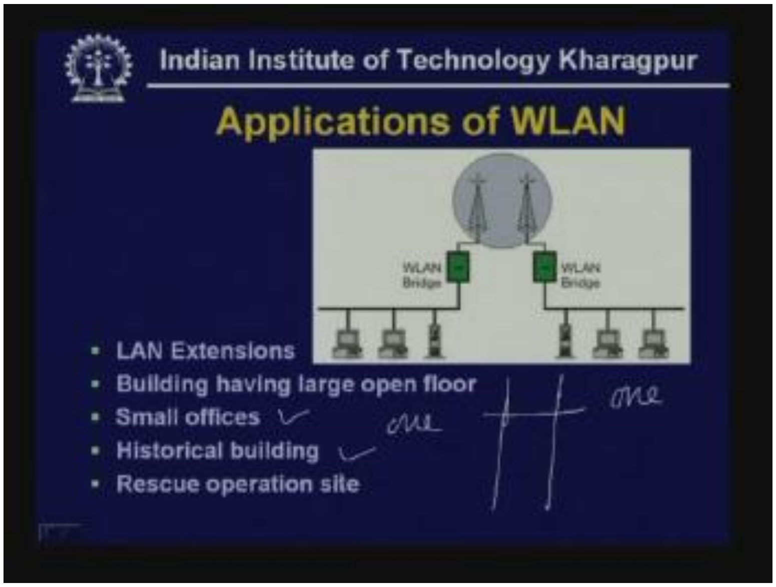
Applications of WLAN

- LAN Extensions
- Building having large open floor
- Small offices
- Historical building
- Rescue operation site

Here, for example, this is one wired LAN, this is another wired LAN so two wired LANs and this is in one building and this is another building so these two are located in two separate buildings and in between you have got some kind of a road. Obviously it is very difficult to dig through the road and setup wire connection. Instead of that one can setup two wireless LAN regions on the roof top and the two LANs can be linked with the help of this wireless LAN. So in this way the communication between two LANs can be established with the help of wireless LAN regions. So you can see here we have used for the extension of wired LANs.

Now, wireless LAN can be used in buildings having large open floor. Suppose in an auditorium which has a large open floor it is not possible to setup wired LANs, interconnections so one access point can be setup with it can be put somewhere then all the mobile stations can communicate and particularly in auditoriums and other places these wireless LANs can be used very easily. Then in small offices, when you have got a very small office then it is not really necessary to have 5028 wired LAN, you can have one small access point and then several desktops or even laptops having wireless LAN interface can be interfaced and in that way it is very flexible to have a small office using wireless LAN.

(Refer Slide Time: 50:49)



Indian Institute of Technology Kharagpur

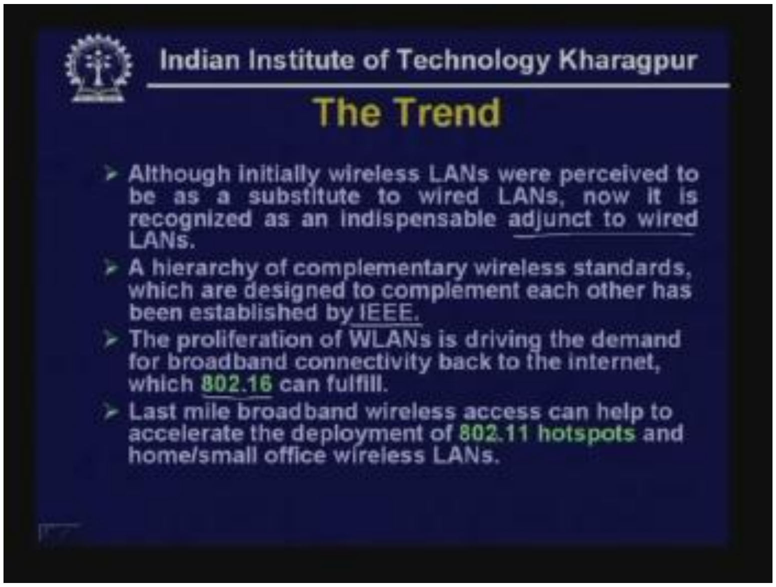
Applications of WLAN

- LAN Extensions
- Building having large open floor
- Small offices ✓
- Historical building ✓
- Rescue operation site

Another important application of wireless LAN is in historical buildings. You have got some historical buildings which cannot be tempered, you cannot really deploy wired LAN, by putting a wire you cannot really dig, you cannot make a hole in the wall, you cannot do anything of that kind in such a situation like museum and other historical buildings you can setup wireless LAN very easily and perform communication.

Since the deployment type of wireless LAN is very small it can be used in rescue operation site. Suppose there is flood, earthquake and some kind of a disaster then in such a situation you can very quickly setup a wireless LAN and establish communication with one another. These are the possible applications of wireless LAN. Obviously I have given a very small number of applications. The application domain is increasing with time and it is possibly limited only by imagination. Now, here is the trend of wireless LAN.

(Refer Slide Time: 53:20)



Indian Institute of Technology Kharagpur

The Trend

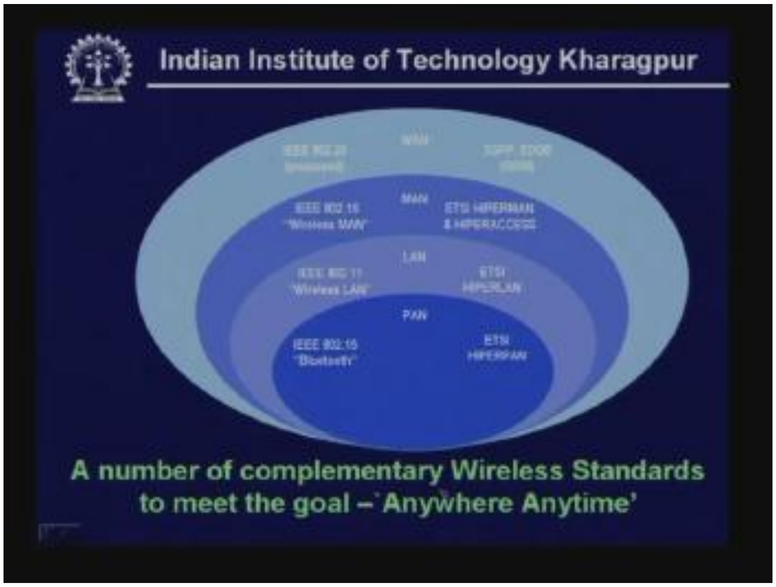
- Although initially wireless LANs were perceived to be as a substitute to wired LANs, now it is recognized as an indispensable adjunct to wired LANs.
- A hierarchy of complementary wireless standards, which are designed to complement each other has been established by IEEE.
- The proliferation of WLANs is driving the demand for broadband connectivity back to the internet, which 802.16 can fulfill.
- Last mile broadband wireless access can help to accelerate the deployment of 802.11 hotspots and home/small office wireless LANs.

Although initially wireless LANs were perceived to be a substitute of wired LANs now it is recognized as an indispensable adjunct to wired LANs. That means when the wireless LAN was announced people thought that wireless LANs will gradually replace the wired LANs but this has not happened because of the limitations particularly lower data rate and other limitations. But now what is being considered is, wireless LAN is being considered as an adjunct to wired LANs so both of them will coexist and both of them will interoperate so in this way they will work with each other.

And a hierarchy of complementary wireless standards which are designed to complement each other has been established by IEEE. So a hierarchy of various wireless standards have been developed which will help in the proliferation of wireless LANs so the proliferation of wireless LANs is driving the demand for broadband connectivity back to the internet so this is essentially a wireless metropolitan area network standard and this can fulfill this limitation and last mile broadband wireless access can help to accelerate the deployment of 802.11 hotspots and home and small office wireless LANs.

Nowadays in many public places like airports, hospitals and so on these kinds of hotpots are being deployed where wireless LAN access points are available with which the mobile users can communicate. and as I mentioned the hierarchy of standards for private area network, local area network, metropolitan area network and wide area network IEEE has a series of standards like IEEE Bluetooth which is 802.15, then 802.11 LAN, 802.16 metropolitan area network then IEEE 802.20 that is being proposed for wide area network.

(Refer Slide Time: 54:25)

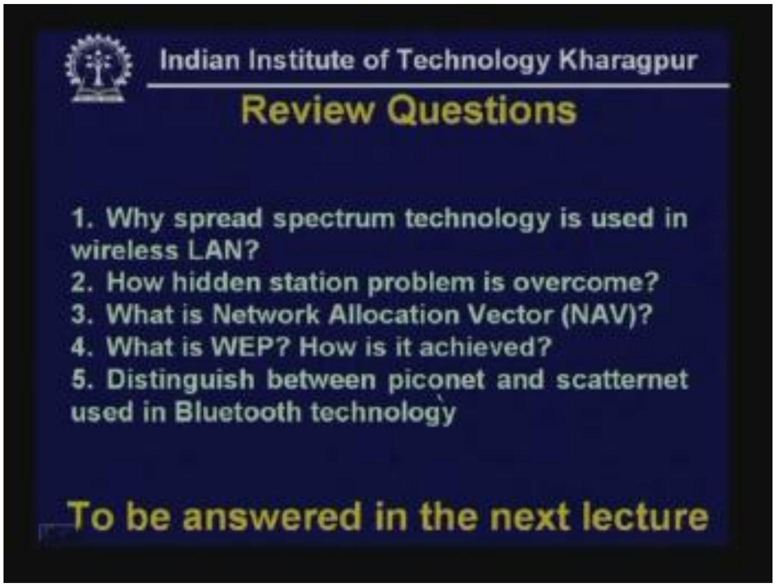


Indian Institute of Technology Kharagpur

A number of complementary Wireless Standards to meet the goal – 'Anywhere Anytime'

So a number of complementary wireless standards are being developed to meet the goal anywhere any time, you will be able to communicate from anywhere at any point in time. Now this is time for giving you review questions.

(Refer Slide Time: 55:05)



Indian Institute of Technology Kharagpur

Review Questions

1. Why spread spectrum technology is used in wireless LAN?
2. How hidden station problem is overcome?
3. What is Network Allocation Vector (NAV)?
4. What is WEP? How is it achieved?
5. Distinguish between piconet and scatternet used in Bluetooth technology

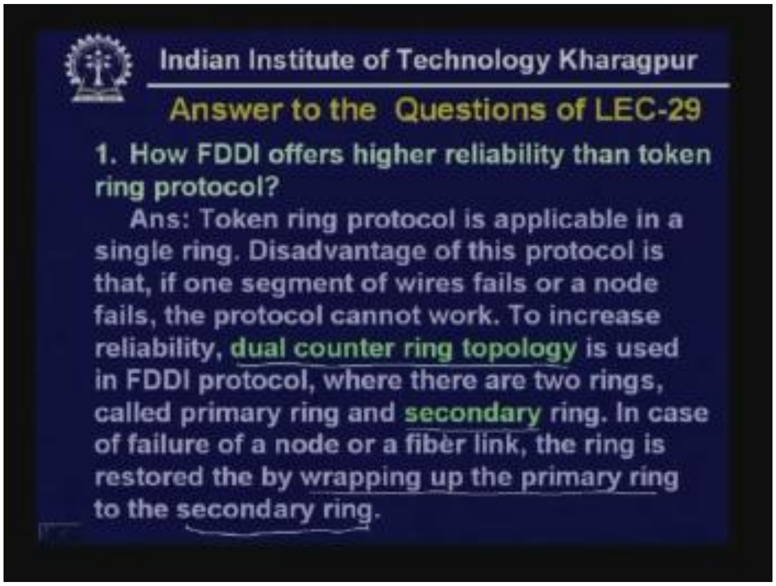
To be answered in the next lecture

1) Why spread spectrum technology is used in wireless LAN
2) How hidden station problem is overcome?
3) What is network allocation vector?
4) What is WEP Wired Equivalent Privacy and how is it achieved?

5) Distinguish between Piconet and Scatternet used in Bluetooth technology.

So these are the five questions and here are the answers to the five questions given in the last lecture.

(Refer Slide Time: 55:50)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-29

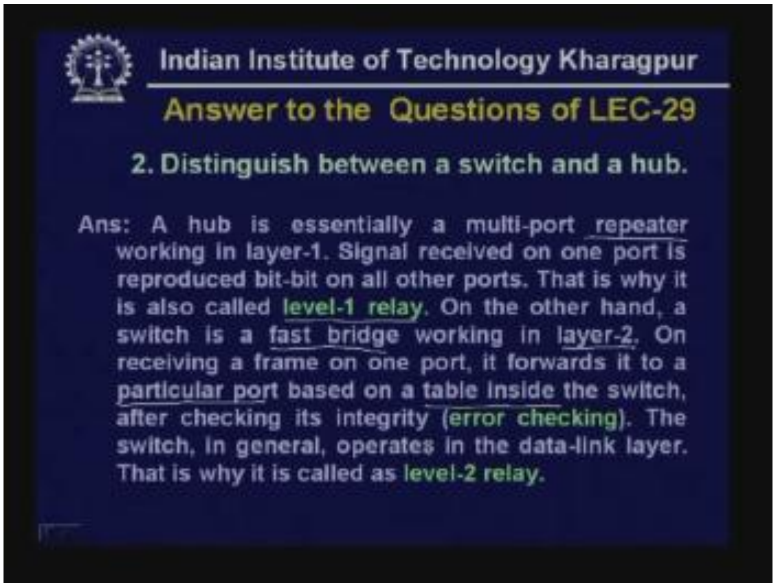
1. How FDDI offers higher reliability than token ring protocol?

Ans: Token ring protocol is applicable in a single ring. Disadvantage of this protocol is that, if one segment of wires fails or a node fails, the protocol cannot work. To increase reliability, dual counter ring topology is used in FDDI protocol, where there are two rings, called primary ring and secondary ring. In case of failure of a node or a fiber link, the ring is restored the by wrapping up the primary ring to the secondary ring.

1) How FDDI offers higher reliability than token ring protocol?

As I mentioned this dual counter ring topology that is being provided gives you high reliability and if a particular link is disconnected or a station gets disconnected then a secondary ring is used to reconfigure the topology and with the help of that communication is done by wrapping up the primary ring with the secondary ring. This is how high reliability is achieved.

(Refer Slide Time: 56:25)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-29

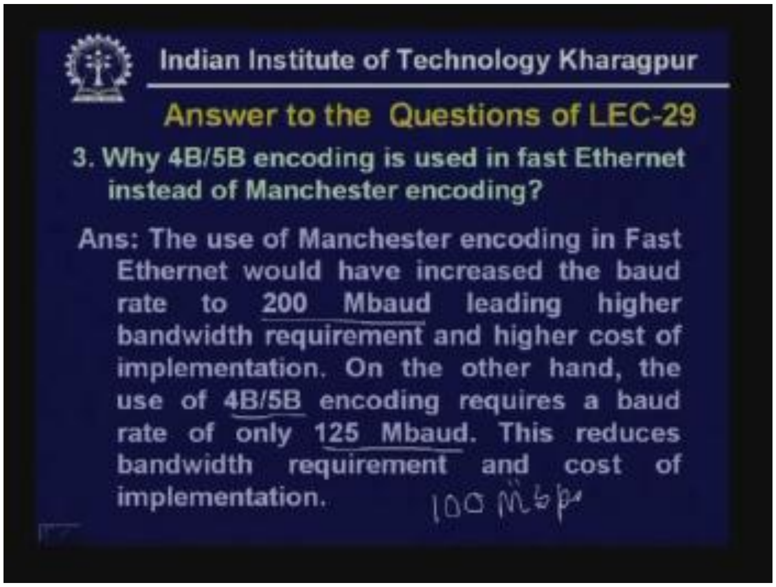
2. Distinguish between a switch and a hub.

Ans: A hub is essentially a multi-port repeater working in layer-1. Signal received on one port is reproduced bit-bit on all other ports. That is why it is also called level-1 relay. On the other hand, a switch is a fast bridge working in layer-2. On receiving a frame on one port, it forwards it to a particular port based on a table inside the switch, after checking its integrity (error checking). The switch, in general, operates in the data-link layer. That is why it is called as level-2 relay.

2) Distinguish between a switch and a hub.

A hub is essentially a multi-port repeater and it works as a level one relay. On the other hand, a switch is a fast bridge working in layer two. So, on receiving a frame on one port it forwards it to a particular port contrary to the hub which sends to all other ports. Here it is sent to a particular port based on a table inside the switch after checking the integrity. The switch in general operates in the data link layer or layer to layer as I mentioned.

(Refer Slide Time: 57:05)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-29

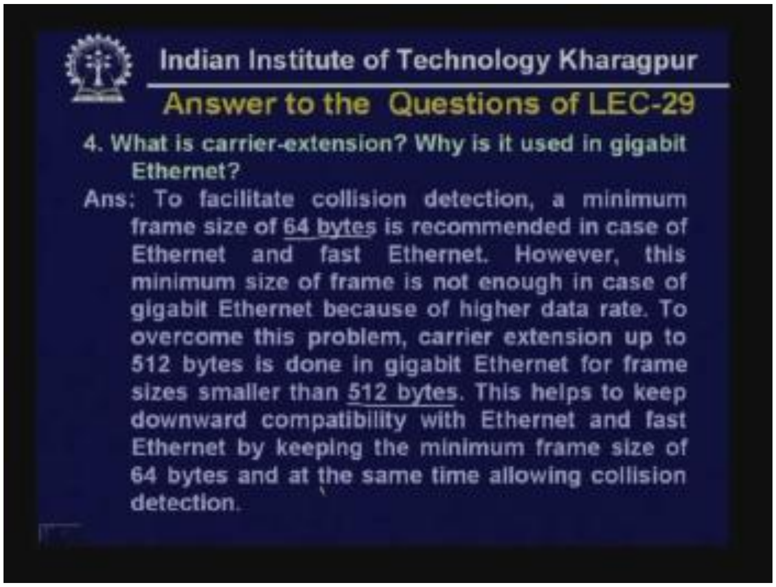
3. Why 4B/5B encoding is used in fast Ethernet instead of Manchester encoding?

Ans: The use of Manchester encoding in Fast Ethernet would have increased the baud rate to 200 Mbaud leading higher bandwidth requirement and higher cost of implementation. On the other hand, the use of 4B/5B encoding requires a baud rate of only 125 Mbaud. This reduces bandwidth requirement and cost of implementation.

100 Mbps

3) Why 4B/5B encoding is used in Fast Ethernet instead of Manchester encoding?
This is used to reduce the baud rate. Essentially if Manchester encoding was used then it will require 200 mega baud but by using four B by five B it is possible to use only 125 mega baud and to achieve the data rate of 100 Mbps. This reduces the cost of implementation.

(Refer Slide Time: 57:34)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-29

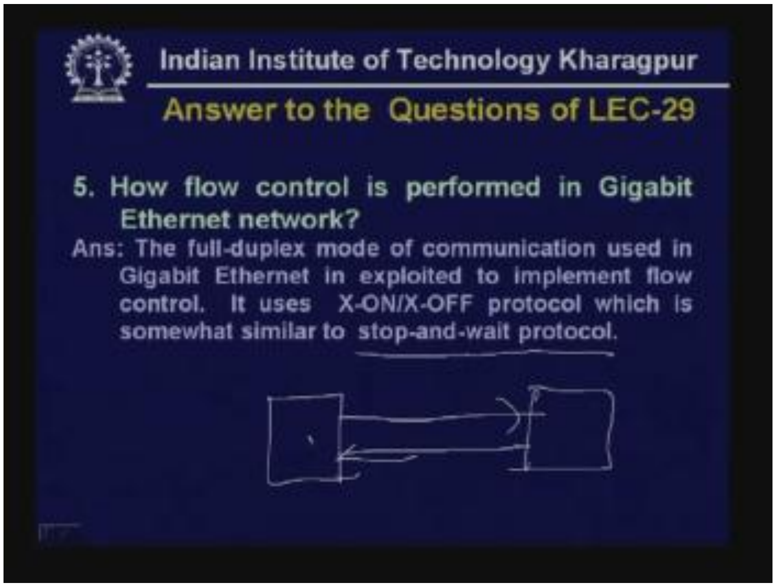
4. What is carrier-extension? Why is it used in gigabit Ethernet?

Ans: To facilitate collision detection, a minimum frame size of 64 bytes is recommended in case of Ethernet and fast Ethernet. However, this minimum size of frame is not enough in case of gigabit Ethernet because of higher data rate. To overcome this problem, carrier extension up to 512 bytes is done in gigabit Ethernet for frame sizes smaller than 512 bytes. This helps to keep downward compatibility with Ethernet and fast Ethernet by keeping the minimum frame size of 64 bytes and at the same time allowing collision detection.

4) What is carrier extension? Why is it used in Gigabit Ethernet?

For detection of collision a minimum size of frame is required. However, as the speed is increased the size has to be increased. But instead of increasing the frame size carrier extension is being performed up to 512 bytes so that the collision can be detected in Gigabit Ethernet so essentially carrier extension is being done for collision detection.

(Refer Slide Time: 58:08)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-29

5. How flow control is performed in Gigabit Ethernet network?

Ans: The full-duplex mode of communication used in Gigabit Ethernet in exploited to implement flow control. It uses X-ON/X-OFF protocol which is somewhat similar to stop-and-wait protocol.

5) How flow control is performed in Gigabit Ethernet network?

The full-duplex mode of communication is exploited in Gigabit Ethernet network to implement X-ON X-OFF protocol which is somewhat similar to stop-and-wait protocols. So you have got two stations and you have got full-duplex communication. So, if one station is sending at a fast rate using the other link the receiver can request to send at a lower rate or stop sending until it is ready. So this Gigabit Ethernet uses this X-ON protocol.

With this we conclude our lecture on LAN technology. We discussed three different types of LANs; legacy LANs, first LANs, high speed LANs and finally in this lecture we have considered wireless LANs. And in the next lecture in the next two lectures we shall consider other uses of medium access control techniques, thank you.