

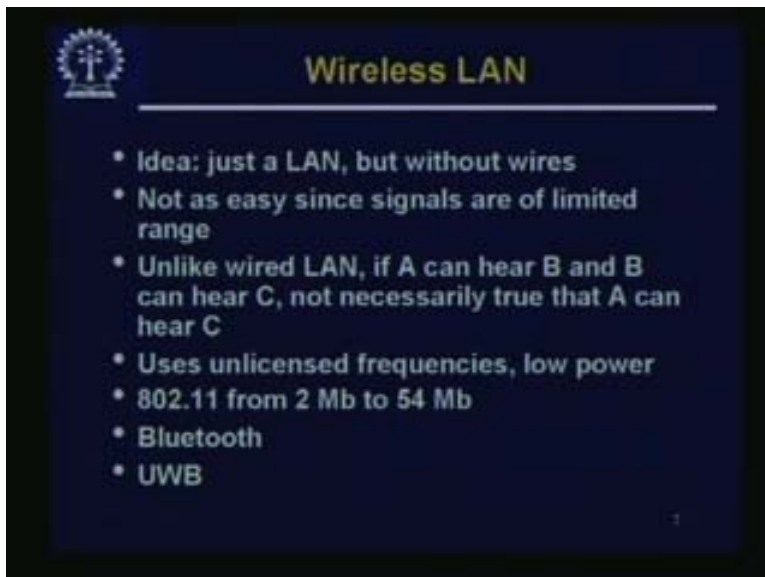
Computer networks
Prof: Sujoy Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture - 23
Wireless Network

Good day. In the last lecture we had discussed about the cellular network and that end of wireless networking; today we will talk more specifically about data networking and wireless LAN, and may be wireless MAN and things like that. Actually there has been an explosive interest in wireless technology in just the last few years, and a number of different systems have come up.

(Refer Slide Time: 01:29)

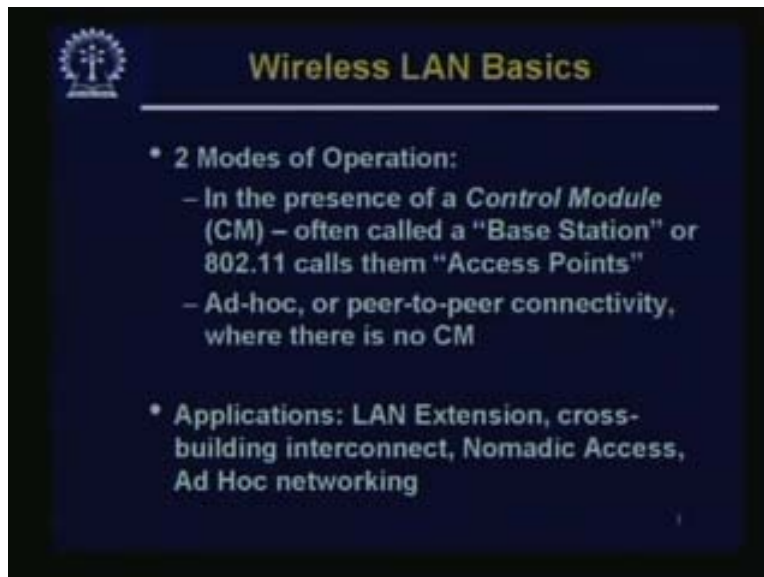


(Refer Slide Time: 01:29)



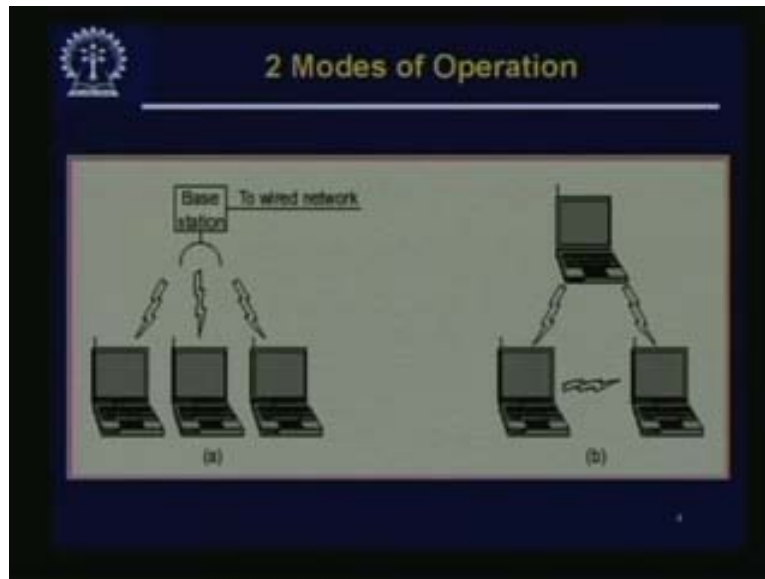
It is not known at this moment what will finally stabilize, but the number of systems have come up and some of them are on drawing board, some of them are on actual deployment. So we will talk about just a few of them, the more important ones today. Today we will talk about wireless networks, and specifically if I may say, wireless LAN. A LAN means a local area network that works without wires, which means you do not have to wire up the whole place; you do not have to have a wire coming into your system; you can walk into a room with a laptop and you are already on the network. But this has some peculiar problems; we will discuss them. This is not as easy since signals are of limited range. Unlike wired LAN, if A can hear B and B can hear C, it is not necessarily true that A can hear C. So this is a problem which we have to handle; secondly in many of the cases, these wireless LANs use unlicensed frequencies and low power. Low power is important because you want to have a small-sized cell so that in another part of the building there may be another cell just giving services to another group of users. As we know that this way, by doing space division multiplexing, we can increase the number of users who are on the network. One of the most important LAN standards today, wireless LAN standard, is 802.11 and there are various versions of 802.11. The speed varies from 2 mbps to 54 mbps. We will also talk a little bit about Bluetooth, which is a personal area network. We will talk a little bit about wireless MAN, which is 802.16 and just mention of few other emerging technologies.

(Refer Slide Time: 03:07)



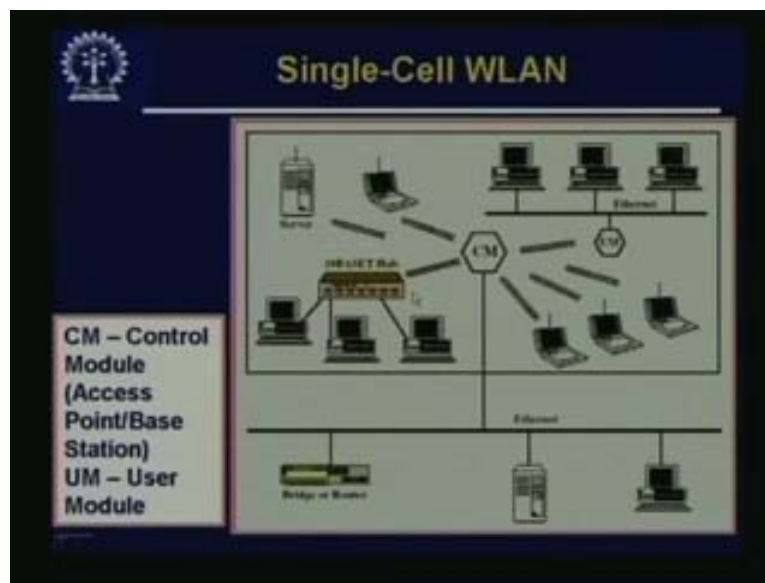
There are two modes of operation in a LAN – in the presence of a control module or a CM often called a base station; just as we have a base station in case of a mobile, similarly here we can have a base station which, in 802.11 parlance, is called an access point or AP. So we can have a base station access point or AP; so we can have a base station or a control module and a number of users. That is one mode of operation. The other mode of operation is a rather ad hoc network; that means, we just have some peers. There is a peer to peer connectivity and there is no central module. So applications could be LAN extensions, cross building interconnect, or nomadic access; that means somebody just moves in and gets immediate access to ad hoc networking.

(Refer Slide Time: 04:30)



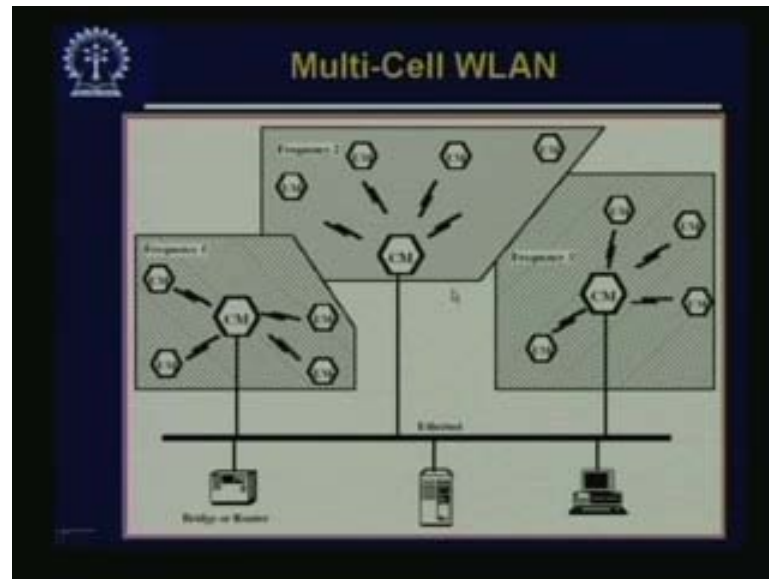
These are the two modes of operation – in one we have a base station, which is controlling them. This is slightly easier to handle than complete peer to peer ad hoc network.

(Refer Slide Time: 04:43)



What happens is this control module or this access point in the case of 802.11 could be connected to a wired network so that all those stations, which are connected to the control module via wireless link, get connected to the entire network so they may connect straightaway to individual PCs or they may connect to some network hub or switch. They may connect to a server and a number of LANs. So this is the picture of a single cell, wireless LAN single cell – WLAN – and we can have multiple cells of WLAN.

(Refer Slide Time: 05:25)



In each of the cells we will have a control module, which will serve some of the user modules. You may note that there may be a region where it is possible to connect to either of the CMs. Also that is something the user module will have to handle.

(Refer Slide Time: 05:51)



Now we will look at WLAN requirement. This is some kind of a wish list actually – what all we would want from wireless LAN. Good use of bandwidth is we want – high throughput – everybody uses a number of nodes; it should be large, may be in the hundreds. A good connection to LAN backbone is required because nowadays just a local network by itself is of limited utility since everybody is getting use to be connected to the entire network meaning the internet even all the time.

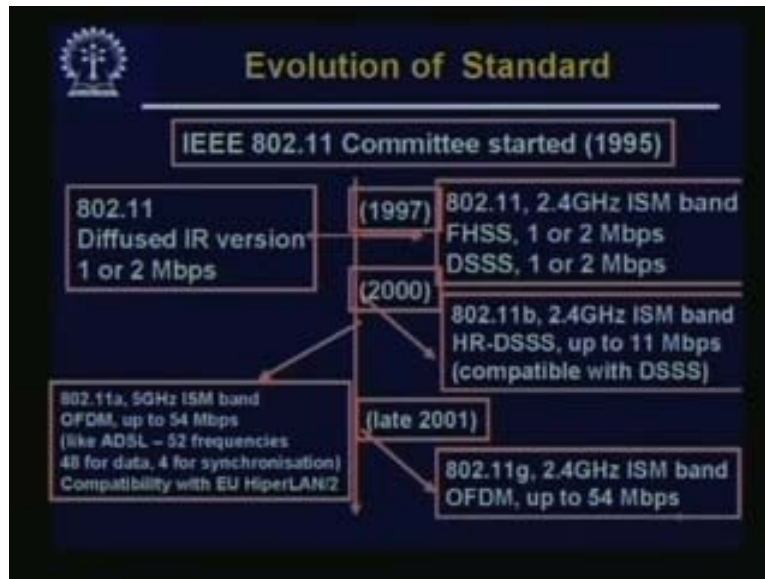
so the backbone connectivity is also important; good service coverage; ok I mean wherever I am I would like to be connected so this to be a good service coverage or range; minimal battery power consumption this an important issue in any kind of mobile system because if the battery consumption becomes high, either you have to carry heavier batteries or you have to charge them often so that is not good so we want minimal battery power consumption; transmission security and robustness – this may be an issue in many cases – because you know so in a wireless system the medium is of course open to everybody alright including snoopers if any so but you would like your communication to remain somewhat private or protected and in some cases that may even become crucial so we want security and robustness ok and some collocated network operation.

(Refer Slide Time: 07:35)



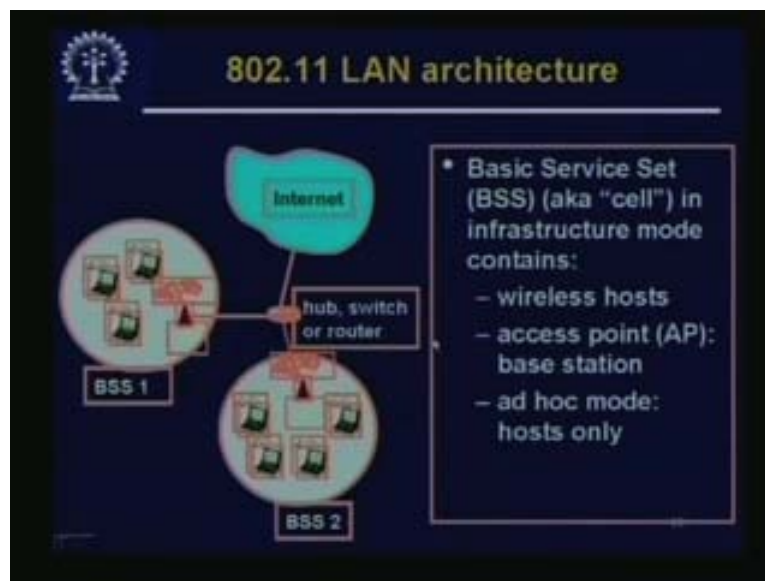
License free operation: this is another important issue. For example, the ISM band consists of industrial, scientific and medical bands of frequencies which are free; there is no license on it. That means operation with the unlicensed band is important because then whoever can develop a good system can go ahead and compete in it, and that way the world technology improves fast. Then people also get cheaper and better quality service. That is why ISM band is generally preferred; but it is not that in a wireless network, we always stick to ISM band. Cell hand-off and network roaming: this is another thing we would like to have. This is some kind of a wish list; that is, not all of them are achieved 100% today, but these are the kinds of things we would like to have, like cell hand-off and network roaming. Just as in voice network we can roam from one cell to another and our call remains online, similarly in network connection, we would like them to remain online when we move from one cell to another. So we require dynamic management, adaptive MAC address management, dynamic and automated addition, deletion, relocation of end systems without disruption. And then we require a choice of physical solutions; for example infrared spread spectrum, narrow band microwave, etc.

(Refer Slide Time: 09:16)



As I said there are a number of standards that came up; here I am just showing some standards in the 802.11 family. Then there is an 802.15 family; 802.16; and so on. This is just one of them. 802.11 originally was a 2.4 GHz ISM band and used FHSS, which is frequency hopping spread spectrum, with 1–2 mbps speed or direct sequence spread spectrum, DSSS had 1 or 2 mbps, and then slowly it graduated and then it fell over to three standards: 802.11b, which is the most earliest and the most common one; it was followed by 802.11a; and 802.11g. These two are in the 2.4 GHz ISM band, whereas this one is in the 5 GHz ISM band.

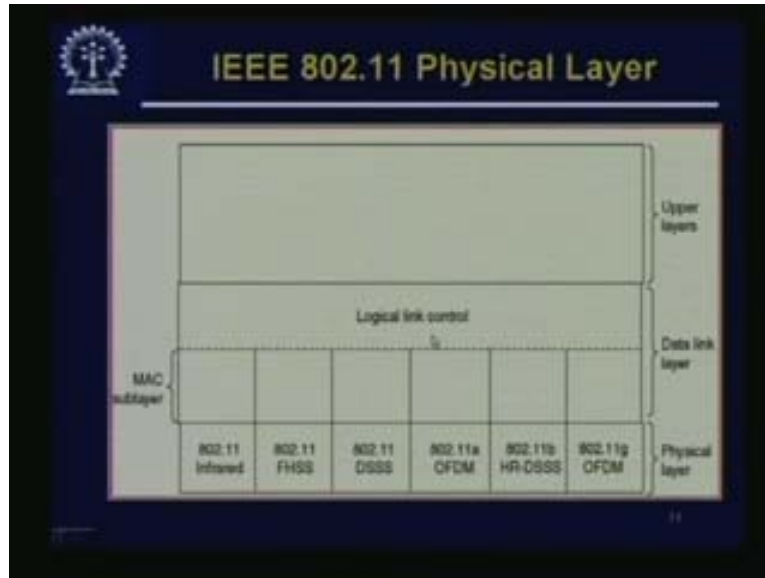
(Refer Slide Time: 10:23)



We will not go in to the details of all these and what exactly are their differences, etc. Today what we are trying to do is that we are just trying to get a general idea, because there are too many standards.

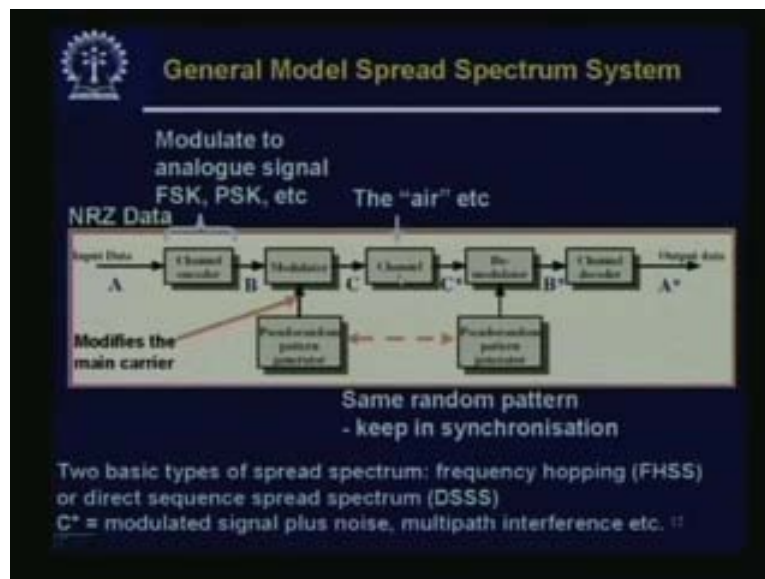
802.11 LAN architecture: by now we know that we will have an access point, which is connected to a hub or a switch or a router. This is in one cell; this is another cell. So cells may be called a basic service set, also known as cell. In infrastructural mode, it contains wireless hosts – so these are the wireless hosts. It contains an access point. In an ad hoc mode, there will not be any access station, so they will all be connecting to each other in a peer-to-peer mode.

(Refer Slide Time: 11:15)



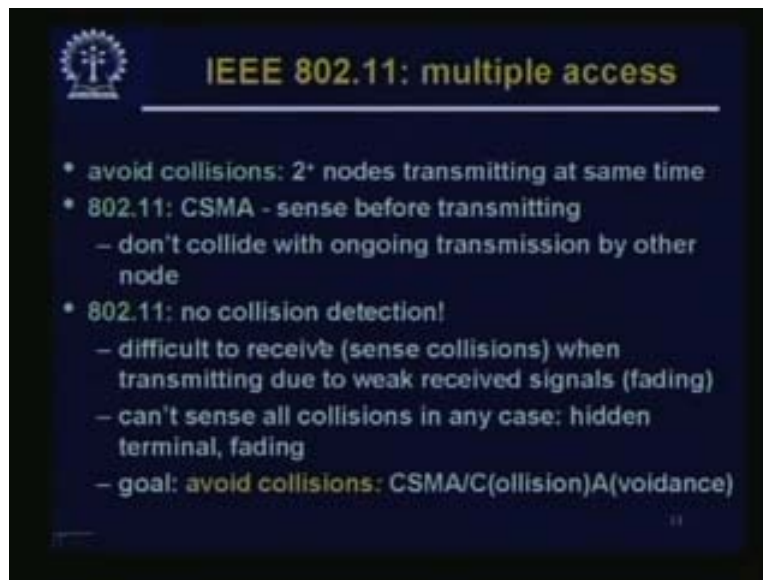
And in the physical layer in 802.11 family itself you see that there are so many techniques that are used – FHSS, which is frequency hopping spread spectrum; direct sequence spread spectrum; orthogonal frequency division multiplexing (OFDM); HRDSSS is another one; OFDM and so on. Above this we have the data link layer, that is, the LLC and the MAC sub-layer, and above that we have the upper layers.

(Refer Slide Time: 11:47)



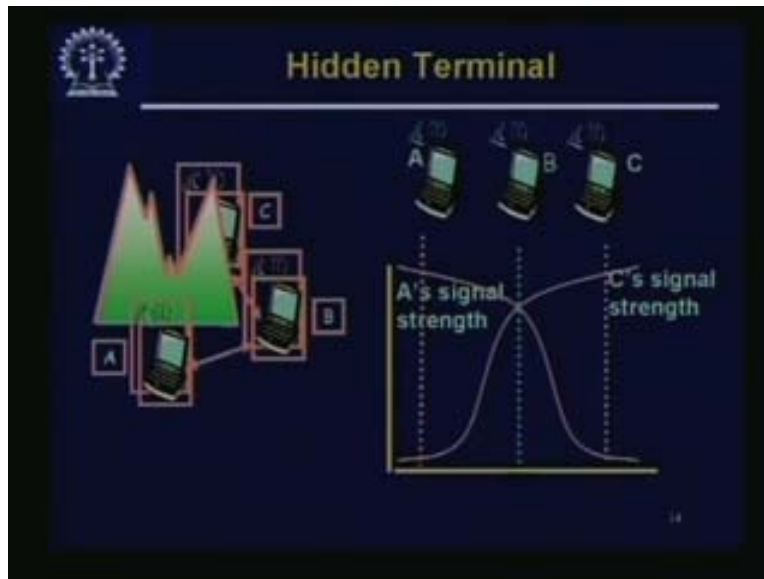
So we do not have the time to go into the details of the physical layer technologies, like, how exactly the multiplexing and multiple access is done, but this is just a very broad and high level view of the system. We have the input data, which is encoded. So that is a channel encoder; it uses either FSK, that is, frequency shift keying, or phase shift keying, FSK or PSK. There are other variations of this. We will just get a feel of this. This feeds into a modulator and then there is a pseudo random pattern generator on the receiver side. This is on the sender side, similarly there is a pseudo random pattern generator on the receiver side and these two are synchronized. So this modifies the main carrier and it then goes into the air or whatever the medium; then it arises at the other end, plus some noise is also added to it, where it is demodulated and it is decoded and then we get the output data.

(Refer Slide Time: 13:00)



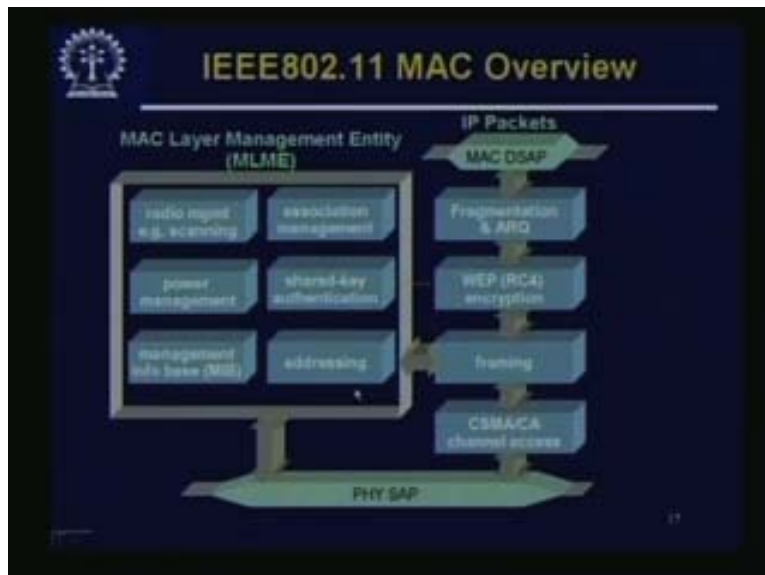
Now how do we – glossing over the physical layer – how do we handle the multiple access of an 802.11? It avoids collisions; that means, we know that when two or more nodes are transmitting at the same time, their signals will collide, and we will have a collision. So 802.11 tries to avoid collision. It does CSMA – if you remember CSMA is carrier sense multiple access. So it does some carrier sensing; it senses the channel before transmitting. Of course it does not collide with the ongoing transmissions by other node, but it does not do any collision detection. And the reason it does not do any collision detection is that if it has to do collision detection, first of all what would happen is that not all traffic is apparent to all the nodes in the network. Due to various reasons it could happen. So that is one reason that even if there is a collision and if you are doing collision detection, you may not be able to detect it at all so that is why the stress here is not to do collision detection like you do in a wired LAN like Ethernet, but to avoid the collision. alright so it is difficult to receive sense collision when transmitting due to weak received signal and fading etc and it cannot sense all collisions in any case – hidden terminal fading so goal is to avoid collisions so this is called CSMA CA. instead of CSMA CD we have CSMA CA that is CSMA with collision avoidance.

(Refer Slide Time: 15:00)



So this is a diagram which shows you this problem about hidden terminal. For example, we have A, B and C. Now B can listen to C; A can listen to B, that means, A B can communicate with each other; B C can communicate with each other; but between A and C there is some kind of an obstacle. So A and C cannot communicate with each other. Even if there is no obstacle like this, the situation could be something like this. Suppose this is A; this is B; and this is C. Now at the point B, A and B have fairly high signal, whereas at C, A signal strength is very low; similarly at A, C signal strength is very low. Some of the terminals may be hidden from some other terminals. This is a problem; that is why our MAC protocol is designed to handle situations like these.

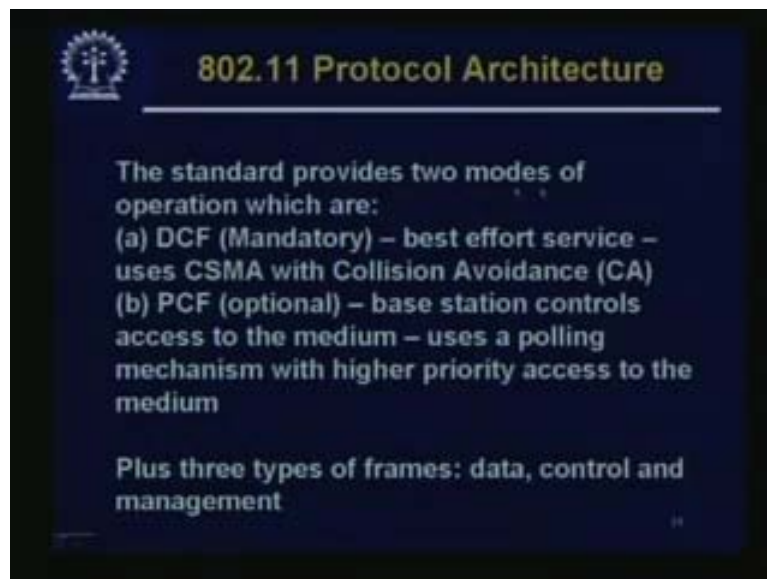
(Refer Slide Time: 16:00)



This is a MAC overview; we have a number of boxes here. I will not go in to all the details like radio management; power management; management information base; this is for network management; there is an addressing; there is a security part, like shared key and association management; similarly there is a fragmentation of large frames and so on. We will not look into all this; we will just mention that for addressing we use the similar 48-bit MAC address, which is Ethernet compliant. You remember that the Ethernet address or the hardware address or the MAC address that we talked about when we discussed Ethernet, is a 6-byte or 48-bit address and 48 is of course a very large address space; that means 2^{48} is 256 trillion, which is a very large number. So there is no shortage of addresses.

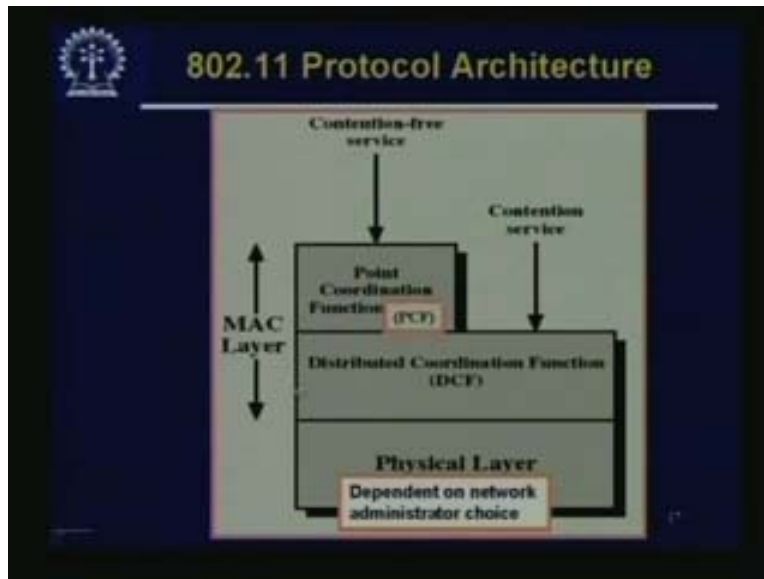
So a bunch of addresses may be given to these. The same kind of 48-bit addresses are used for this also. Making it Ethernet compliant has its advantage because Ethernet is just another ubiquitous kind of network. Another point is that we have an acknowledgement request kind of a system, where some frames and some fragments, etc. are acknowledged. So if the acknowledgement does not come we have retransmission. We also have some error correction; and radio link security; data authentication; data encryption; simple scrambling; or peer-to-peer, etc. We will not be discussing these as do not have the time. In the radio link, there is a question of quality of service. There is this CSMA CA – we will look into this channel access mechanism in some more detail. Dedicated real time support systems are also there; they are with PCF. So there are actually two mechanisms, which may be simultaneously present in the same system – DCF and PCF – we will be talking about these. The standard provides two modes of Operation: DCF, which is mandatory.

(Refer Slide Time: 18:36)



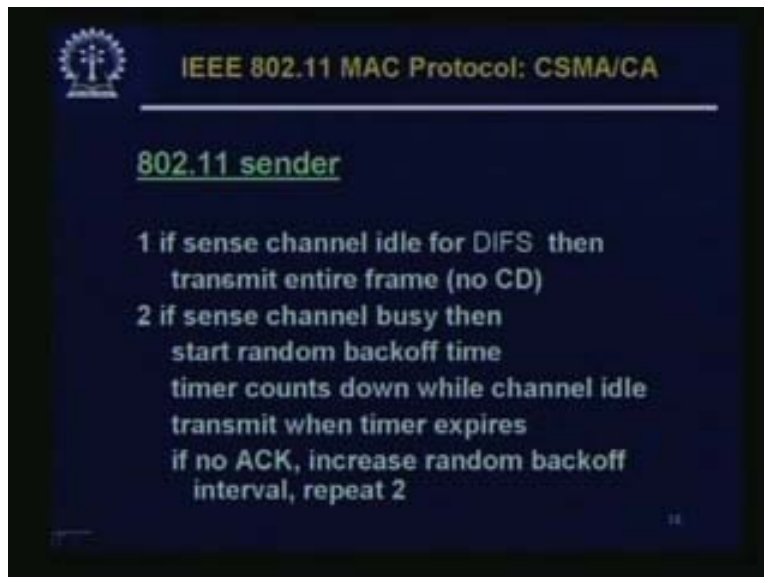
That means every 802.11 system has to be following DCF at least. So it is a best effort service that uses CSMA CA; that is, CSMA with collision avoidance. And there is another mode, which may optional, which is PCF. This is a base station. This is a distributed control function and this is a point control function. This base station controls access to the medium and uses a polling mechanism with higher priority access to the medium. So actually, if PCF is there, what PCF can do is that actually PCF can take precision. So for DCF, it can give some guaranteed kind of service or quality of service to some users. There are three different types of frames: data frames, control frames, and management frames.

(Refer Slide Time: 19:35)



So one is the point coordination function which is PCF the other is the distributed coordination function which is the DCF. ok so and how I mean which one you are using may be you are not using PCF at all so that would be a network administrator's choice. So the if you are using PCF that would give you some contention free service whereas if you are using DCF you are using a service where there may be contention. Of course you can use PCF and DCF at the same time. Alright so how does the protocol work? From the sender's side it senses if the channel is idle for DIFS.

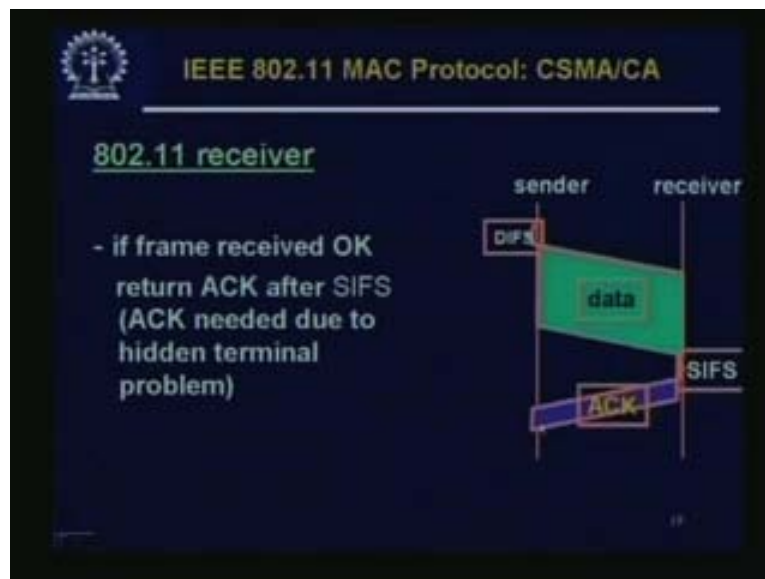
(Refer Slide Time: 20:11)



DIFS is the period of time which can be configured; it then transmits the entire frame. So it just cannot send some thing as soon as the channel is idle; it has to wait for at least DIFS amount of time. And it does not do any collision detection.

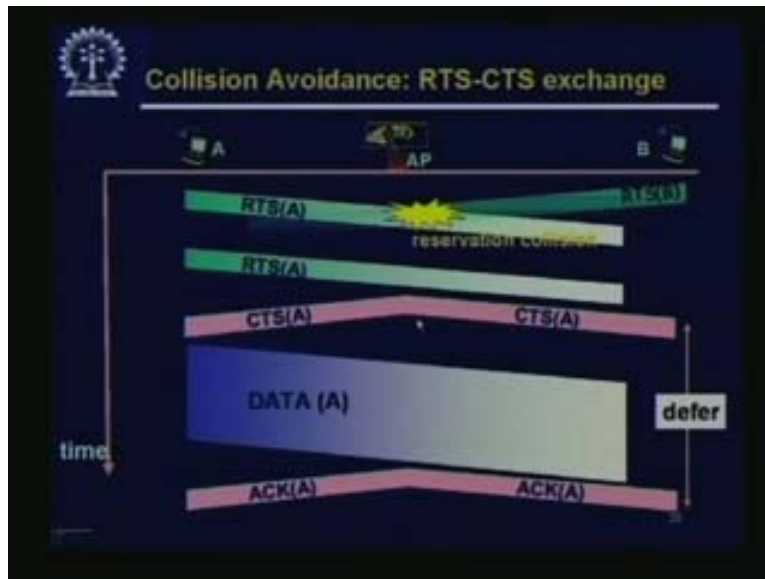
How does it know that there will not be any collision? Just because you have waited for DIFS amount of time does not mean that there will not be any collision; there may still be collision because somebody else may also be listening to the channel waiting for DIFS amount of time and start transmitting, and you are not doing any collision detection. The point is that you will not get an acknowledgement. Unlike the Ethernet system, where there is no acknowledgement, this is an acknowledgement based system. So you will get an acknowledgement; if you get the acknowledgement you know that there is a collision and if you do not get an acknowledgement you know that there is a problem, so you retransmit. If, on the other hand, you sense the channel to be busy, then you start some random back-off time, similar to Ethernet where you do binary exponential back-off, etc. We start random back-off time. The timer counts down while the channel is idle, transmits when timer expires. If there is no acknowledgement, we increase random back-off interval and repeat step 2. This is the way system works: if there is no acknowledgement, it means that it has not succeeded. So you increase the back-off time and repeat. Another reason why collision detection is not done in wireless network is that for many of the radio systems, it is difficult to do transmission and reception at the same time. So collision detection means you keep on doing collision detection while you are transmitting. You just keep on listening whether it is going through or there is some garbled message in the medium. But that is difficult to do in many systems; so that is another reason why CD is not done. In the receiver it is simple; if it gets the frame then it returns the acknowledgement.

(Refer Slide Time: 22:51)



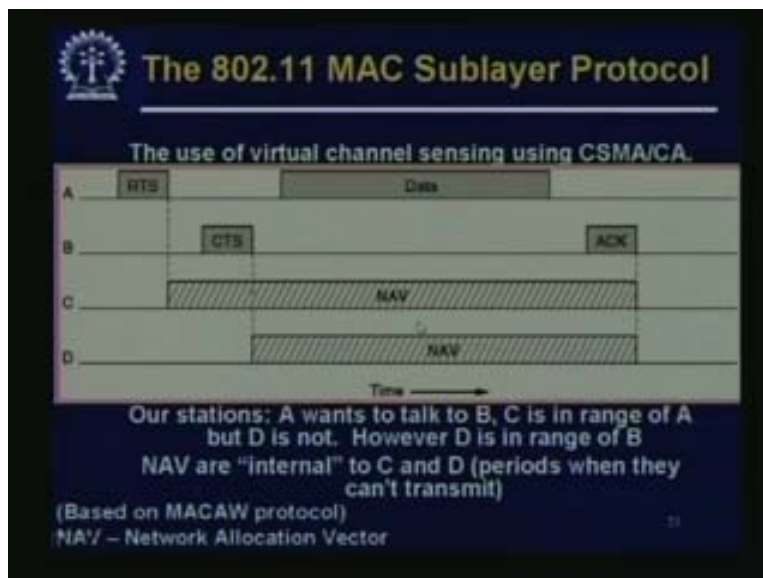
SIFS is another time interval, which is defined. So after some time, it will send the acknowledgement. Acknowledgement is needed for the hidden terminal problem. So there is the sender; there is the receiver; and suppose after DIFS amount of time the sender has sent some data, the receiver has received it. After SIFS amount of time, it sends back the acknowledgement.

(Refer Slide Time: 23:26)



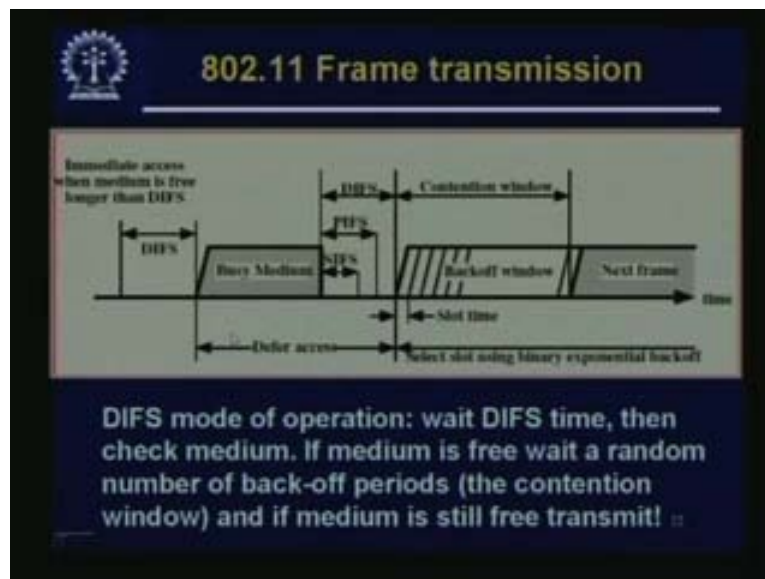
There is another scheme which uses this RTS CTS exchange. Suppose A wants to communicate – this is the AP and this is B – so A wants to communicate and let say B also wants to communicate. So A sends a request for transmission – it is just a reservation request. B also sends the reservation request at the same time, and there is a collision. Since there is a collision, none of them will get it. Actually they will get it by some signal from AP as we will see. After some time A may be sending the request again and maybe it is has gone through; so once it goes through AP will issue a CTS that now CTS A can be sent. And please note that CTS A not only reaches a it also reaches B. And since now B knows that it has been reserved by A, B will back off or defer for a considerable period of time. B will defer for quite a bit of time and A will send its data, then A will get its acknowledgement. This is an RTS CTS based scheme.

(Refer Slide Time: 24:49)



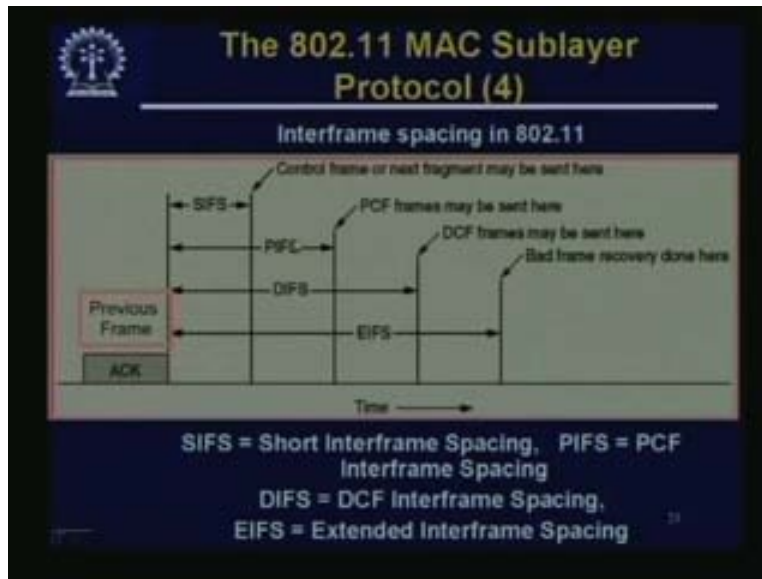
This is another example. A wants to send data; so it sends an RTS and gets a CTS from B. A can now send the data. By the way, this RTS and CTS have been detected by C and D also, so what they do is that now they know that somebody is communicating so this NAV or network allocation vector. It automatically puts itself off. This is a very polite kind of system so it automatically puts itself off till it gets the acknowledgement. A wants to talk to B, C is in range of A, but D is in the range of B. That is why the NAV of C starts here, whereas when B sends a CTS meant for A, then D catches it and starts its own NAV. That means it starts its own blocking time; this is called virtual channel sensing.

(Refer Slide Time: 25:55)



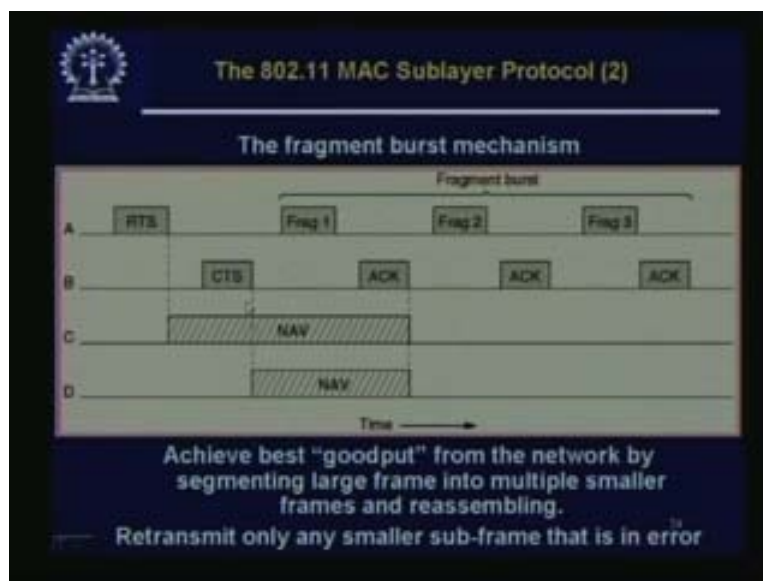
Now just to mention how this point coordination function and distributed coordination function work at the same time – the PCF and DCF – and why we use DIFS and SIFS – these two periods of time. In DIFS there are actually three time intervals, which are configured. This is DIFS; this is PIFS for point control function; and this is SIFS. Please note that when the medium is busy, after that if somebody wants to send, he cannot send immediately. He has to wait for DIFS amount of time. If PCF is also operating at the same time and PCF wants to send something, PCF has to start doing that within this PIFS amount of time. So somebody wanted to send and is waiting for DIFS; when he gets this, when the PCF grabs the channel, then this other node will defer for a longer time and there is an SIFS, after which acknowledgements are sent. And after this DIFS, there is a contention window where there may be a random back-off and the next frame is sent.

(Refer Slide Time: 27:19)



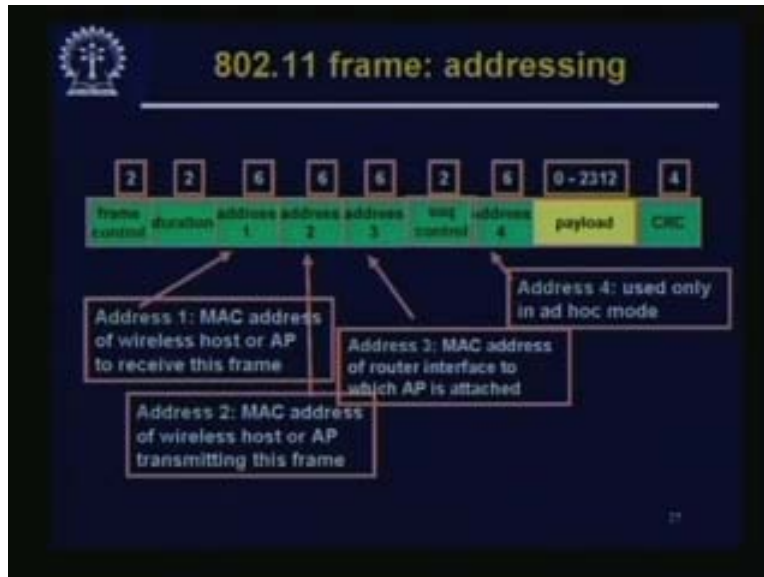
Suppose this was the previous frame. Within SIFS, the acknowledgement and the control frame and next fragment may be sent here; so either acknowledgement or control frame or next fragment is sent here. PCF: frames may be sent here. That means after PIFS amount of time, the PCF or point coordination function will grab the channel. If PCF has not done that, then after DIFS amount of time, it can be distributed – that means anybody can try to send anything. There is another time which is called EIFS, for bad frame recovery. So SIFS is for short inter frame spacing; PIFS is for PCF inter frame spacing; DIFS is for DCF inter frame spacing; and EIFS for extended inter frame spacing. These are the different kinds of spacing. This way this PCF and DCF can work at the same time. Another point is that if you have a very large frame, there may be a problem in the sense that if a large frame becomes garbled, a large frame has a larger window, where it puts off everybody.

(Refer Slide Time: 28:38)



So for better throughput, it may be a good thing to break up a large frame into smaller fragments. After an RTS CTS, it may send as one small fragment; then acknowledgement fragment to an acknowledgement; and so on. The other thing is that a large frame is more likely to beget errors and if you just do the calculation, you will find that if you break it up, there may be orders of magnitude difference between the error probability of a large frame and a small frame. So overall, your throughput may be much better and in an especially noisy situation, your throughput may be much better if you send smaller fragments. For smaller fragments, first of all you can do some error handling locally, and you can handle it – that is one thing. Secondly, for a large frame, the probability of error is much higher.

(Refer Slide Time: 29:46)



We will discuss just a little bit about the 802.11 frame addressing. If you remember, in an Ethernet, we had two addresses: the source address and the destination address. Here, actually very surprisingly, we have four addresses. And just to show you why, address 1 is the MAC address of wireless host or AP to receive this frame. So this is the destination, immediate wireless destination, that is, wherever you want to land up on this wireless link. Address 2 is the MAC address of wireless host or AP transmitting this frame. This is the source address, so to say. Now the point is that, after all, quite often what you want to do is that you are not always interested in the technology used for this wireless transmission. You are trying to connect to a network, which is in the outside world.

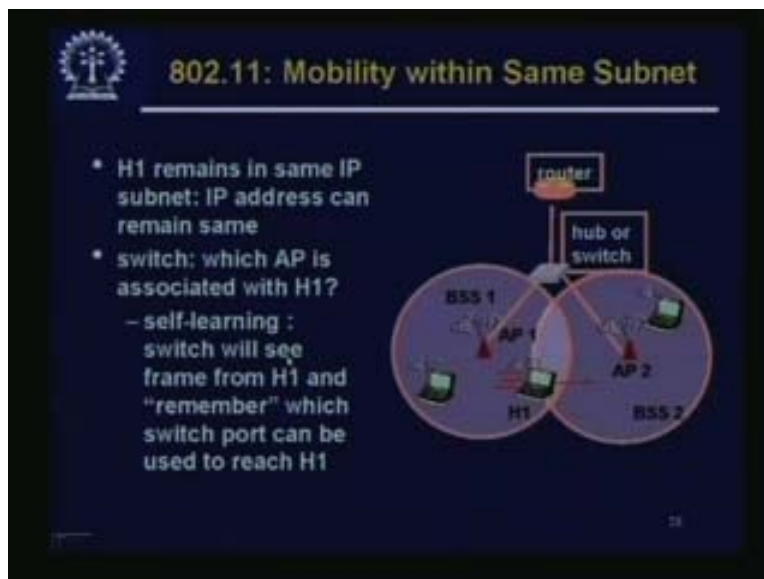
So this is what will happen – this access point will connect to a router, or it may connect to a LAN and that LAN may be connected to a router. So basically what you have to do for going out of this network altogether – that means not only this wireless part of the LAN or the wire part of the LAN – you will have to know the MAC address of that particular port of the router, which you want to reach as a next stop. Then the router will decide to go next so the MAC address of that router must also come from the source itself. So address 3 is for that MAC address of router interface, to which AP is attached and AP may be attached to a LAN and it may have multiple addresses. Address 4 is used only in ad hoc mode; we will not discuss it there. These are the four addresses; yet another thing is the payload. The payload is from 0 to 2 kb. These are all in bytes: all MAC addresses are in 6 bytes; MAC addresses are 18 bytes just for 3 addresses; and for 4 addresses it is 24 bytes.

(Refer Slide Time: 32:10)



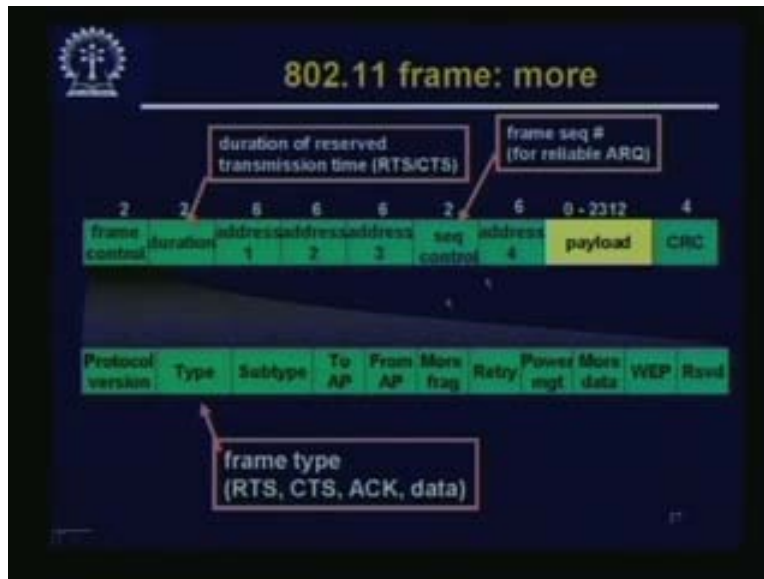
So this is the picture – originally we had a just the routers, MAC address and AP MAC address. These two – destination and source address – when you are sending from a wireless host the AP MAC address, the host MAC address, the router MAC address are address 1, address 2 and address 3.

(Refer Slide Time: 32:36)



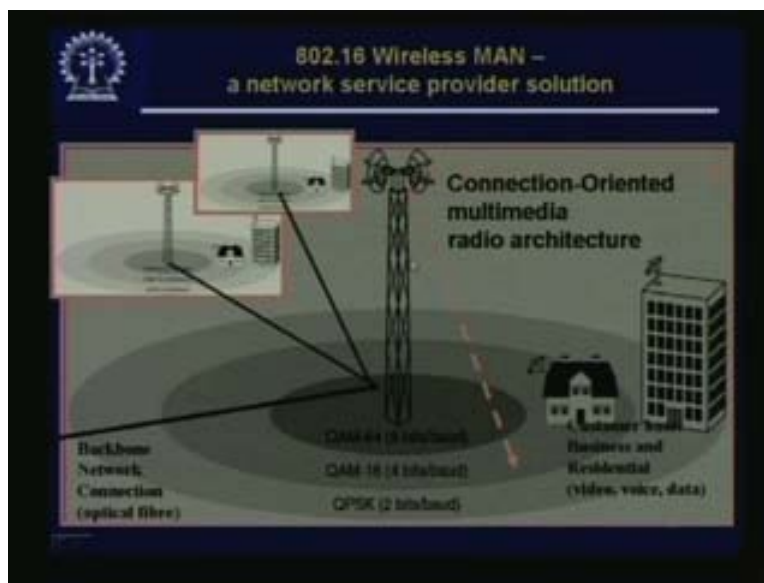
Let us now talk about the other fields – there is a duration of reserved transmission time in the RTS CTS system that we were talking about, and that we showed you. There is a duration of reserved time. Then there is a sequence control – this is the frame sequence number for reliable ARQ. Since you are doing acknowledgement with retransmission request, you require a 6-sum sequence number for that window. We have discussed this and now we have a sequence control number over here. Then of course, there are other fields. It could be frame type; it could be RTS type; CTS type; or the acknowledgement data subtype. We need not go into all of these.

(Refer Slide Time: 33:27)



And then we talk a little bit about the mobility within this, because whenever we are in wireless we want to be mobile. If we are going from one from under one AP to under another AP, that means from one BSS to another BSS there is the basic service set that is from one cell to another, so what the mobile host we will do is that it will sense whoever is stronger and he will connect there so there is some chance of confusion in this. But since he handles it, as he moves he will connect from AP 1 to AP 2. But this is assuming that these two APs are in the same network. If these two APs are in different networks, then the situation is a little more difficult and we cannot handle it at this layer directly.

(Refer Slide Time: 34:25)

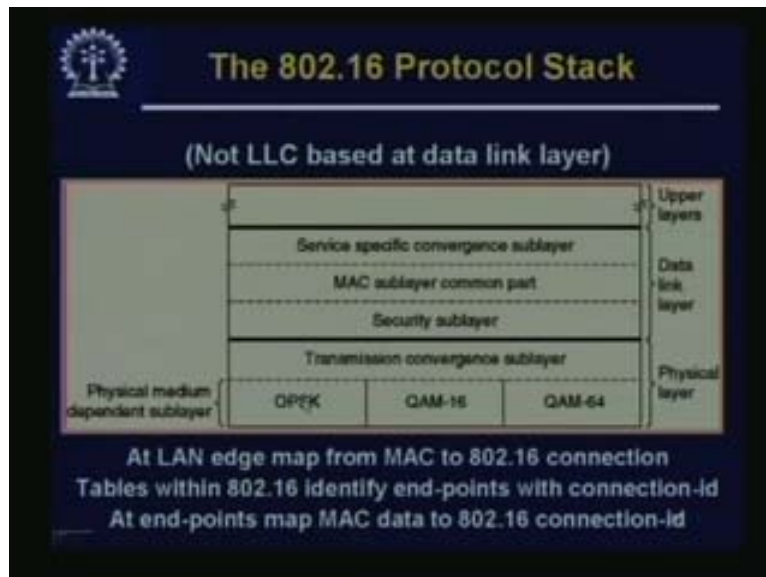


We have quickly covered 802.11, which is the most common kind of wireless LAN that we see today. In many places, we have 802.11; actually in some places they are also called hot spots.

That means this is under some AP, so that if a person is in that hot spot he can connect to the network and there are some campuses, at least some places, where a large number of APs have been deployed so that you are continuously – wherever you are in that whole campus – always in the network. That is one kind of system, that is, 802.11. Next we come to another kind of wireless systems, namely wireless MAN; that means wireless metropolitan area network. What we want to do is that we want to connect an entire metropolis with this; obviously this 802.11 is no longer sufficient. First of all, the power is low. Actually in 802.11, in order to handle more number of users, we keep the power low so that we have smaller sized cells, etc., but in this metropolitan area network there will be many users in the same cell; working in that 2.4 GHz ISM band will not be sufficient any more.

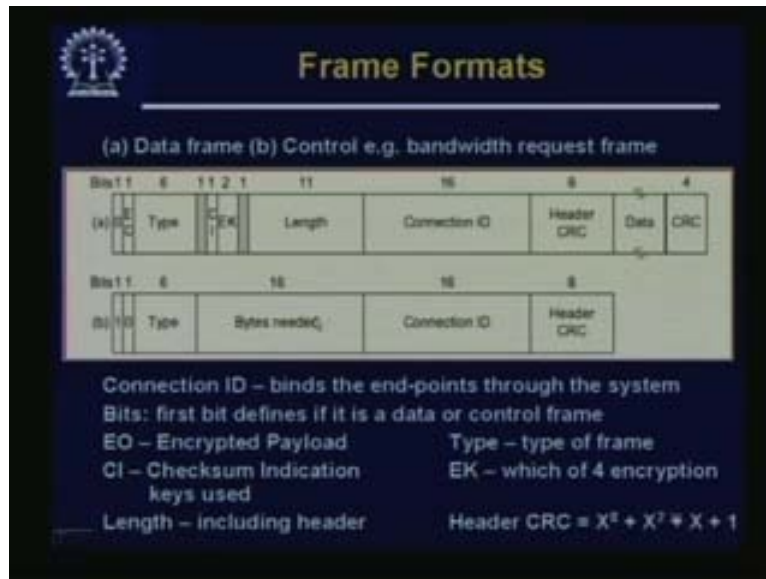
So we have to go for a much wider range of frequencies, and for this, we need to go to a higher frequency in the so-called millimeter wave region. Millimeter wave means when the wavelength is at the millimeter order. There is a standard for this wireless MAN; this is called 802.16. What we might do is that we might have a large tower because these millimeter waves usually travel in straight lines. So what we have to do is that we have to have a line of sight to the base station. We have to have a large tower so that everybody can be on the line of sight, and these different base stations may be connected through a wired network, or this base station would be connected to the general network through may be a fiber optic line or something.

(Refer Slide Time: 37:02)



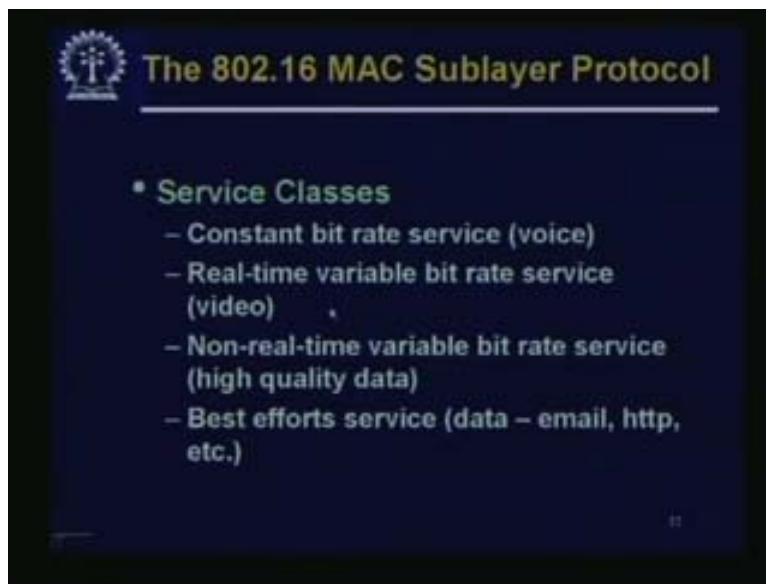
This is the 802.16 protocol stack; this is orthogonal phase shift keying or quadrature amplitude modulation QM 16 or QM 64. We are not going into these or the different kinds of modulation techniques, which are used. There is a transmission convergence sub-layer; that means how to handle it from here – once again we do not bother about this. We will just talk a little bit about the MAC sub-layer common part and the service specific convergence layer. We will just talk a little bit about it. As I said, so many systems are coming up these days that it will not be possible to handle all of them.

(Refer Slide Time: 37:46)



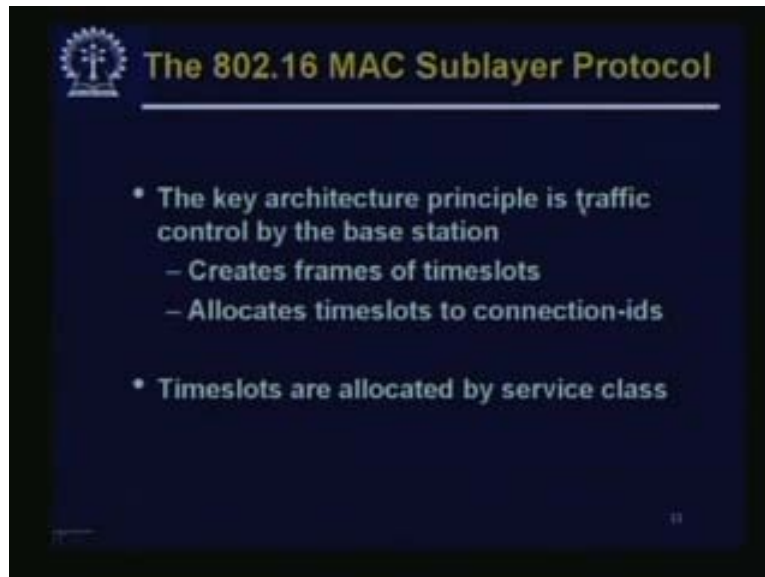
This is just the frame format. There may be a data frame and the control frame. The control frame is the bandwidth request frame. There is a connection ID; this binds the end points to the system. There is a connection ID, through which any particular system would get a chance to communicate. The first bit defines if it is a data or a control frame; if it is a data frame, the first bit is 0, if it is the control frame, the first bit is 1. Then it says whether the payload is encrypted or not; 1 or 0 type is the type of the frame. There are management frames and things like that; so C1 is the check sum. There is a check sum indication key that is used. Once again, we need not go in to all the details but it uses CRC error correction. So header is the header portion; for the header portion there is a CRC and the data connection ID etc. Basically the access to the medium is controlled through this connection ID.

(Refer Slide Time: 39:04)



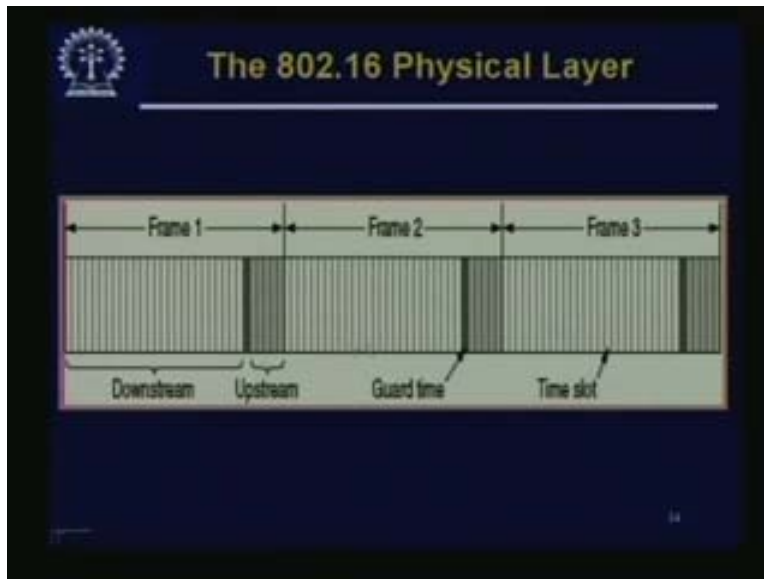
There are different service classes, which are defined in this: one is the constant bit rate service for voice real time; variable bit rate service (this is a VBR); RTVBR or a non-real time variable bit rate service, that means, NRTVBR, for high quality data; and for ordinary data, email, http, etc., this is the best efforts service. There are different service classes in 802.16, and all these are possible because here the MAC is simply controlled by the base station.

(Refer Slide Time: 39:53)



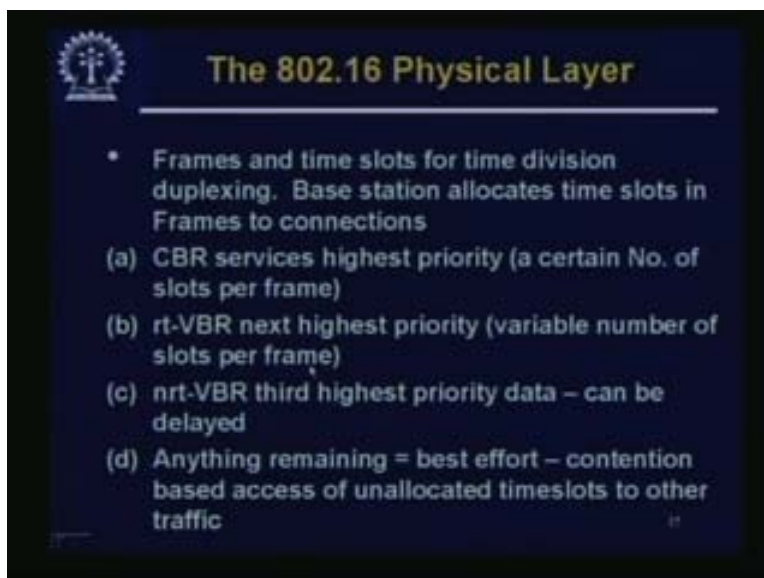
The key architectural principle is traffic control by the base station. The base station controls the traffic totally. It creates frames of time slots and allocates timeslots to connection IDs. So time slots are allocated by service class. This means that if there is a constant bit rate service, what the base station would do is that in every frame it is going to allot one or more slots to this constant bit rate service, so that it gets constant rate updates. So whoever reserves or requests that constant bit rate service, if he is not using it at any particular point of time, then it is going empty. That is why he has to pay higher for this constant bit rate service. Similarly there are variable bit rate services, and finally, with just a slightly higher priority than the non-real time one and just the available bit rate service, whatever else is left may be given to those connection IDs, which are only getting available bit rate service.

(Refer Slide Time: 41:11)



These are just pictures showing frames and each of the frames will have some slot. There are some guard times between the frames. Some of the slots are reserved for upstream traffic, whereas some of the other slots are for the downstream traffic. Quite often, what happens is that in this metropolitan area networks or in many networks, the downstream traffic turns out to be much higher than the upstream traffic. We all know, for example, if you are surfing the net, which is a very popular activity, you just send one request, which is a very small thing, and in response to your http request, a large page with a lot of graphics, etc., may be downloaded. So the downstream traffic turns to be much larger. There is a lot of asymmetry here; that is why there are a few upstream slots and a lot of downstream slots.

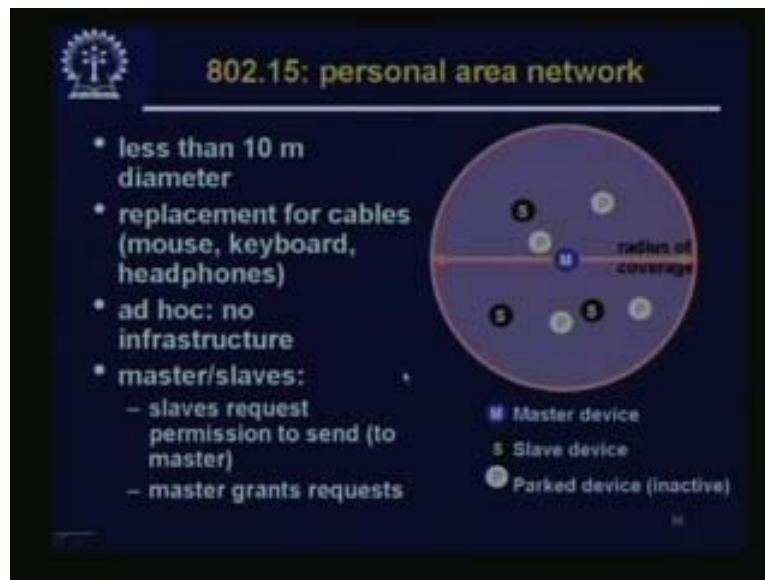
(Refer Slide Time: 42:08)



So frames and time slots are for time division multiplexing or duplexing. Actually it is for time division duplexing, because both upstream and downstream traffics are given some slots.

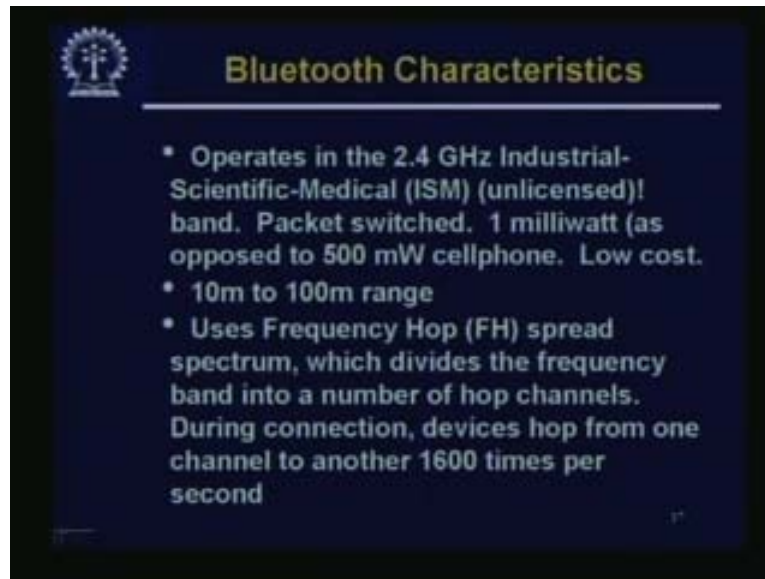
Duplexing means it is going in both directions. Base station allocates time slots in frames to connections. There are some connection IDs, and to a particular connection ID, the base station may allocate time slots. CBR as I said, constant bit rate services, are of the highest priority. RTVBR, that is, real time variable bit rate has the next highest priority; NRTVBR has the third highest priority. This can be delayed and anything remaining is the best efforts contention based access of unallocated timeslots to other kinds of traffic. This is how it is done.

(Refer Slide Time: 42:56)



Next we move on to another end of the spectrum. First we talked about wireless LANs; that means 802.11, and as I mentioned, it has a lot of variations like 802.11 a, b, g, etc. So 802.11 is the LAN side. Then we talked about MAN, metropolitan area network, and now we are going to the other end of the scale, which means very small networks, let us say, personal area networks. That means a small area is covered under a network – between whatever I have in this pocket and this pocket, and my in my hand. We will talk about one thing, which is quite popular, namely Bluetooth, which is 802.15. So 802.15 is for the personal area network group; 802.11 is for local area network; .16 is for metropolitan area network; and .15 is for personal area network. This is less than 10 m in diameter; so you see this is very small. It has a replacement for cables, mouse, keyboard, headphones, etc. So whatever I am using may be replaced by wireless links – that was the idea. This is ad hoc; that means there no infrastructure is necessary. This works with the idea of master and slaves; that means slaves request permission to send to master, and master grants the request. So in any such cell or radius of coverage, there will be a master and then there will be some slaves. M is the master device, S is the slave devices, and P is the parked devices. That means these are inactive at the moment, so they are called parked devices in Bluetooth.

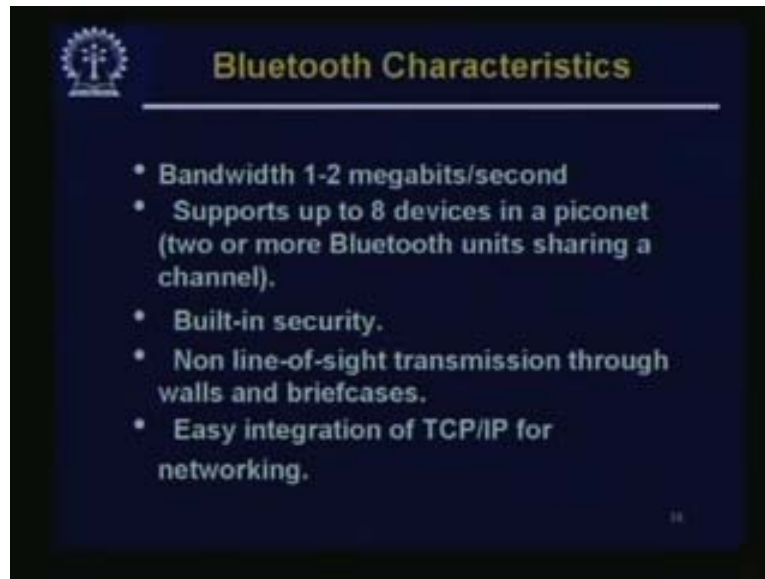
(Refer Slide Time: 44:57)



So Bluetooth and 802.15 are almost the same. There are some small differences, but this not very important. It operates in the 2.4 GHz industrial scientific, that is, ISM band, and is unlicensed, packet switched, and 1 mill watt. This is a very important issue – that this uses a very small amount of power as opposed to, let's say, 500 mill watts for a cell phone. This is low cost; that means up to 10 m to 100 m range and uses frequency hop spread spectrum; so FHSS is used. We will see what kind of an FHSS, which divides a frequency band into a number of hop channels, is used. During connection, devices hop from one channel to another 1600 times per second; so you see it is hopping the frequencies very fast.

So that is one good thing because if some part of the frequency band has noise, it has got better noise immunity because it is hopping such a large number of times. There are a large number of channels – why a large number of channels? We are talking about a personal area network; but nowadays I may be using so many different gadgets, etc., when I am using my PC, I may be having a cell phone; I may be having a laptop; I may also have a desktop in front of me. Each of them will have a mouse and all these peripherals – let's say it has a monitor and all these peripherals may be connected in some way through wireless. So there may be so many things; altogether about 79 channels are possible in Bluetooth and so they go on hopping in the frequency.

(Refer Slide Time: 46:53)

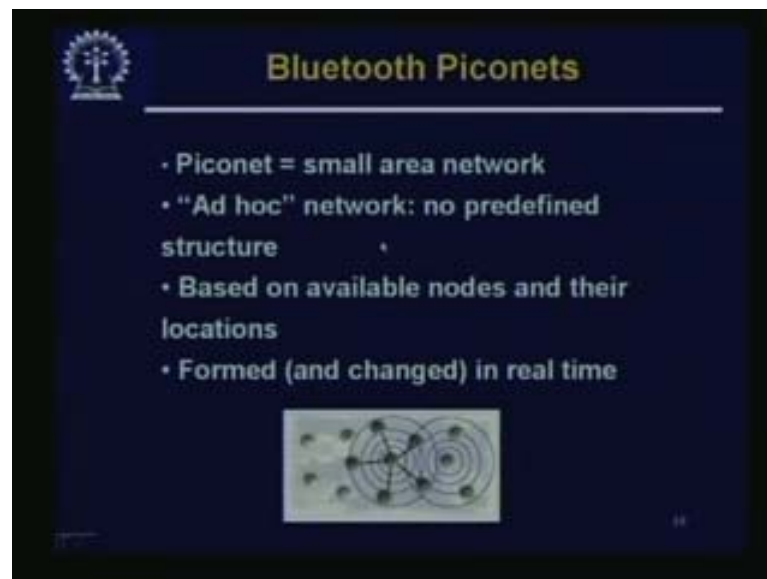


Bluetooth Characteristics

- Bandwidth 1-2 megabits/second
- Supports up to 8 devices in a piconet (two or more Bluetooth units sharing a channel).
- Built-in security.
- Non line-of-sight transmission through walls and briefcases.
- Easy integration of TCP/IP for networking.


Bandwidth is 1–2 mbps; we are not looking for a very large bandwidth over here, but this is just more for control and function rather than downloading files. It supports up to eight devices in a piconet. What is a piconet? Two or more Bluetooth units sharing a channel is called a piconet. It has some built-in security line of sight transmission through walls and briefcases because of the frequency band which it uses. It uses integration of TCP/IP for networking.

(Refer Slide Time: 47:30)



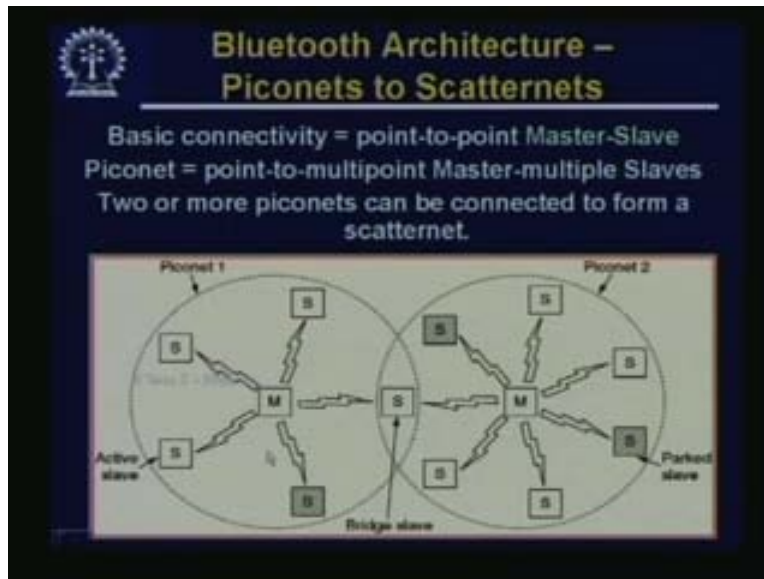
Bluetooth Piconets

- Piconet = small area network
- "Ad hoc" network: no predefined structure
- Based on available nodes and their locations
- Formed (and changed) in real time



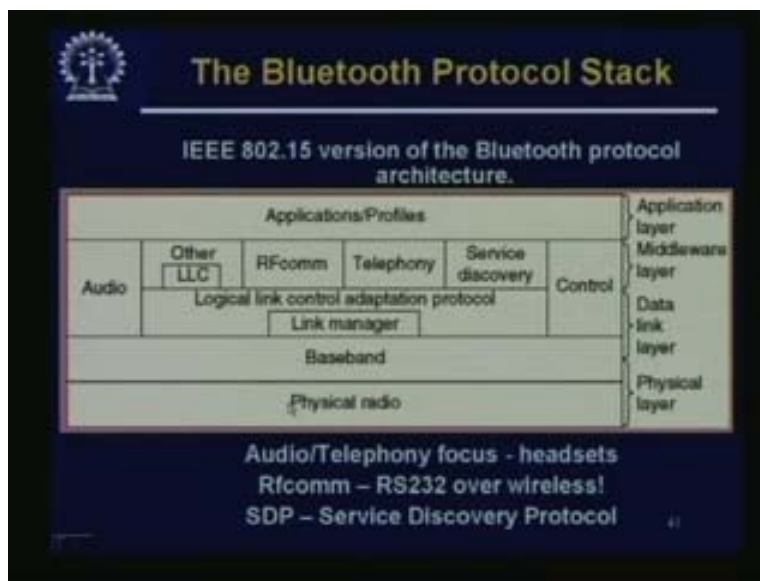
So piconet is a small area network. It is ad hoc, which means that a network with no predefined structure. There is no predefined structure; it is based on available nodes and their locations; it is formed and changed in real time. As you can see, these networks are being formed and being changed in real time; so they may be changing all the time.

(Refer Slide Time: 47:56)



The basic connectivity is point-to-point; that means from the master to the slave. Piconet is point-to-multipoint master multiple slaves; two or more piconets can be connected to form a scatternet. By the way, how does a piconet start? Anybody can start it and claim himself to be a master, and the other devices, which are coming in later, will become the slaves. So anybody can start and become a master. This is one piconet; this is another piconet; and they may be connected. The two piconets may be connected to a scatternet. If you want to have a scatternet, then we have to have a bridge from this piconet to this other piconet. So we have a bridge slave.

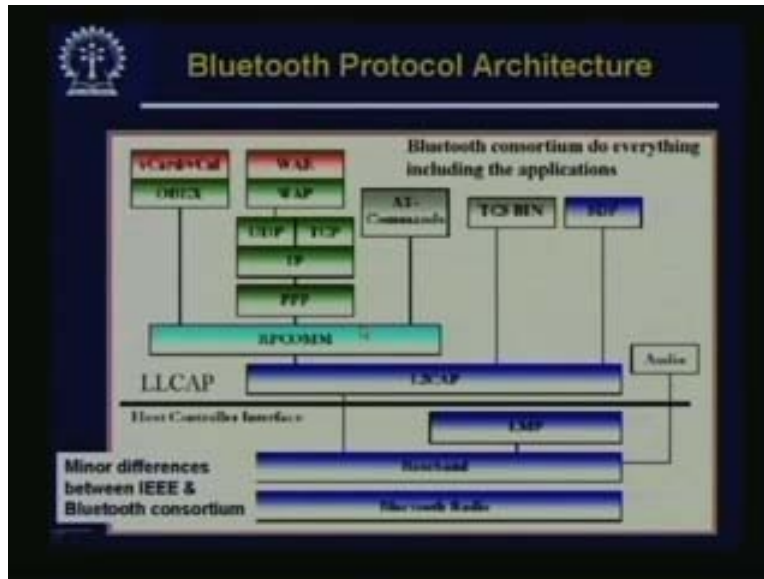
(Refer Slide Time: 48:39)



So 802.15 version of the Bluetooth protocol architecture – these two are slightly different, but we will not bother about it. We have the application profiles; then we have the physical radio base band and the link manager.

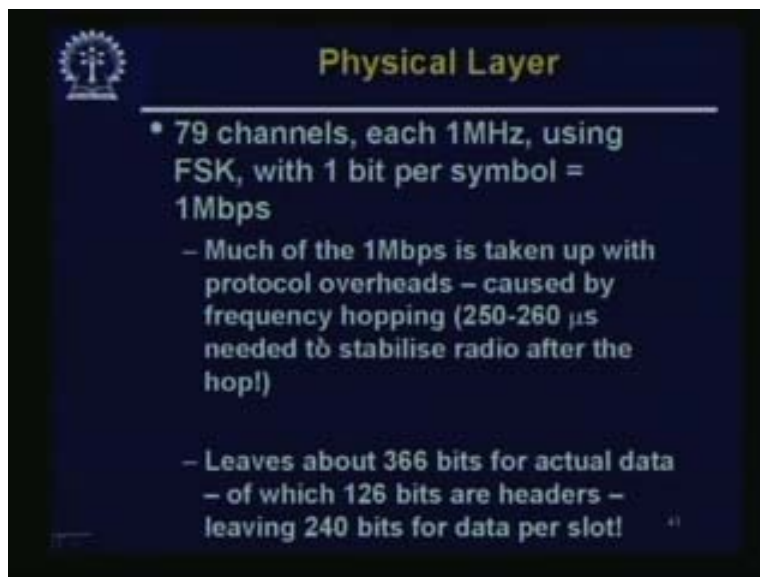
Link manager means the radio link manager, and then there is a middle layer, which is the service discovery, telephony, RF communication, and so on. Once again, we do not have the time to go into the details of this. The idea is that you can switch from one kind of service to another kind of service, depending on the context and situation.

(Refer Slide Time: 49:27)



This is a more detailed picture of the different kinds of protocol. Let us skip this also.

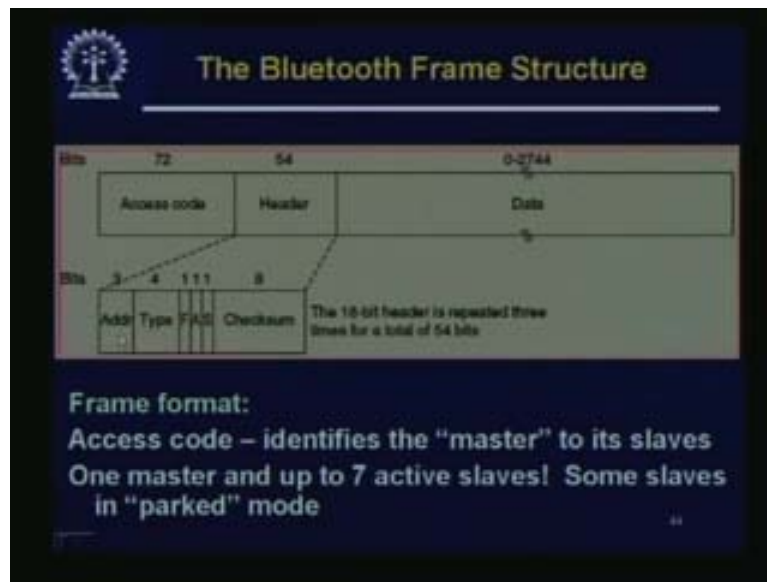
(Refer Slide Time: 49:39)



In the physical layer, it has 79 channels, each 1 MHz, using frequency shift keying with 1 bit per symbol. So it comes out to about 1 mbps per channel. Of course, this is 1 mbps. The individual devices finally do not get a 1 mbps throughput for the payload part, because the efficiency is quite low. Much of the 1 mbps is taken up with protocol overheads caused by the frequency hopping.

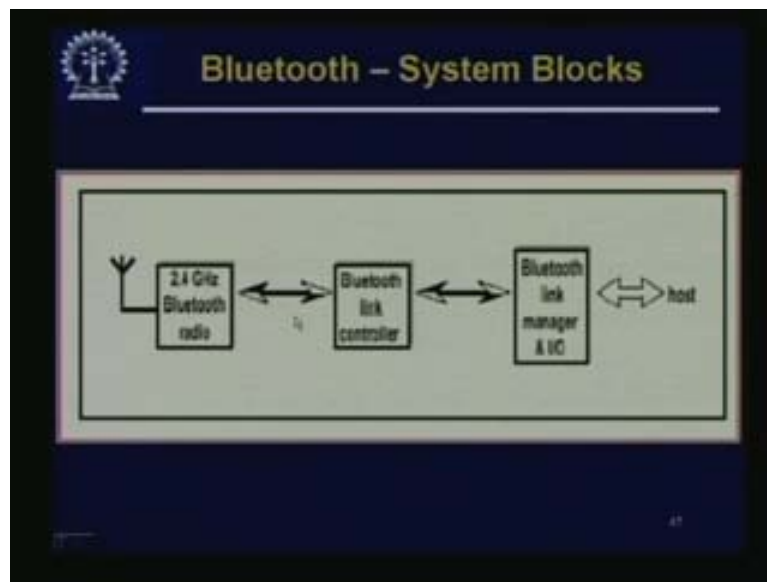
So this takes about 250 to 260 micro seconds needed to stabilize the radio after the hop. So this leaves about 366 bits for actual data, of which 126 bits are headers, leaving only 240 bits for data per slot. So what was supposed to be 1000 bits has become 240 bits. But for small devices, which are getting locally connected to each other, even 240 bits per second kind of speed may be more than enough. But so many different channels are possible; 79 channels are possible. This is just a little bit about the Bluetooth frame structure; we have the access code, and then the header, and then the data.

(Refer Slide Time: 50:49)



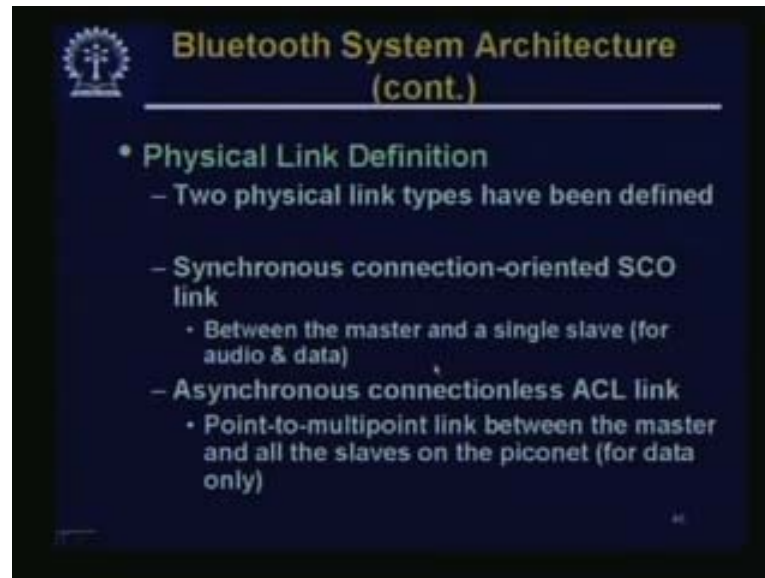
And the header will contain the address type, etc., and some flags and some checksum; also it is an 18-bit header. It is repeated three times for a total of 54 bits. The access code identifies the master to its slaves; one master and upto seven active slaves. Some slaves are in parked mode.

(Refer Slide Time: 51:17)



So these are the system blocks: we have a Bluetooth radio; a Bluetooth link controller; and a Bluetooth link manager.

(Refer Slide Time: 51:29)



So two physical link types have been defined: one is synchronous connection oriented link – between the master and a single slave for audio and data – and the asynchronous connectionless ACL link, point-to-multipoint between the master and all those slaves on the piconet for data only. This is for data and this is used for others. If some voice channel is there, you can get a synchronous connection oriented link there so that you get acceptable quality of service.

(Refer Slide Time: 52:08)



Multiple access scheme is based on FH CDMA, that is, frequency hopping CDMA. High speed of hops and code division multiple access offers the best properties for ad hoc radio systems. As I said, 79 hop carriers have been defined at a 1 MHz spacing.

(Refer Slide Time: 52:26)

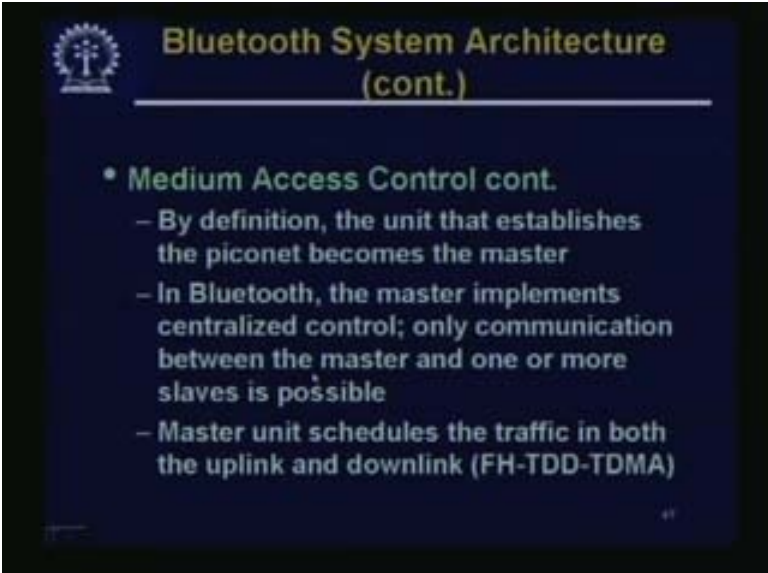


Bluetooth System Architecture (cont.)

- **Medium Access Control**
 - Bluetooth has been designed to allow a large number of independent channels, each channel serving only a limited number of participants
 - Theoretically, the spectrum with 79 carriers can support 79Mb/s
 - Different channels have different masters and therefore also different hopping sequences and phases

The Bluetooth has been designed to allow a large number of independent channels, each channel having only a limited number of participants. Theoretically, the spectrum with 79 carriers can support 79 mbps, but as we have seen, the efficiency may be something of the order of 25%. So it will be much less than that. Different channels have different masters and therefore, they also have different hopping sequences and phases.

(Refer Slide Time: 52:59)

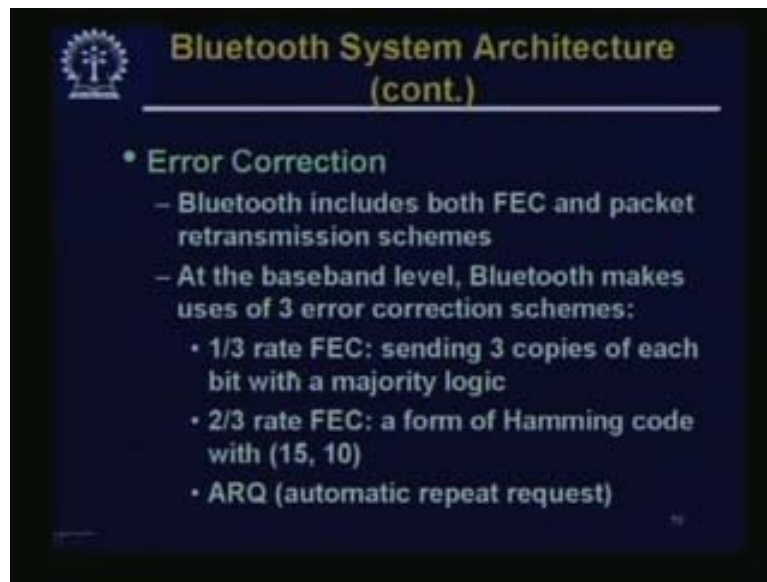


Bluetooth System Architecture (cont.)

- **Medium Access Control cont.**
 - By definition, the unit that establishes the piconet becomes the master
 - In Bluetooth, the master implements centralized control; only communication between the master and one or more slaves is possible
 - Master unit schedules the traffic in both the uplink and downlink (FH-TDD-TDMA)

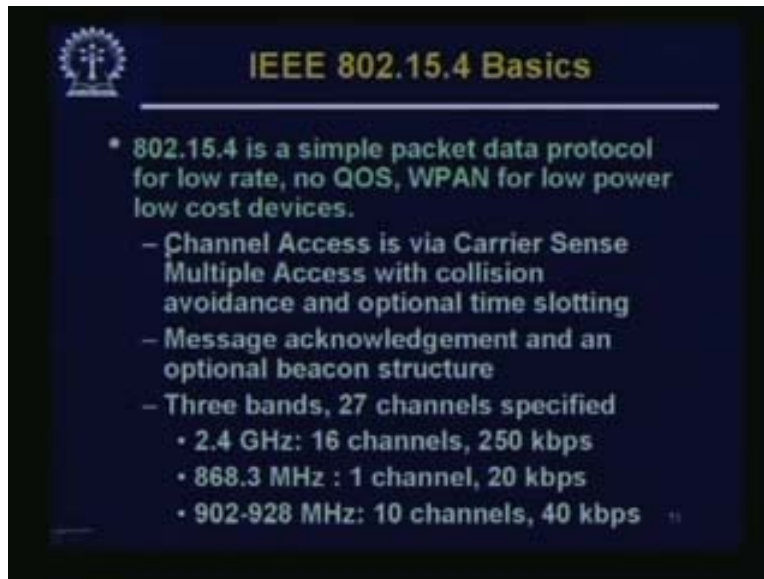
By definition, the unit that establishes the piconet becomes the master. As I said, anybody can start a piconet and become his master. In Bluetooth, the master implements centralized control; once again we do not try to do any distributed control. It is a small system so we do a centralized control by the master. Communication is possible only between the master and one or more slaves, which means that the slaves do not communicate with each other directly. It has to go through by the master. The master unit schedules the traffic in both the uplink and the downlink.

(Refer Slide Time: 53:39)



There are various types of error corrections, which are possible. This includes both FEC and packet retransmission schemes at the base band level. Bluetooth makes use of three types of error correction schemes: one-third rate FEC, sending three copies of each bit with majority logic; two-third rate FEC, a form of some kind of hamming code; or automatic repeat request or ARQ. So this is the error correction scheme that is used.

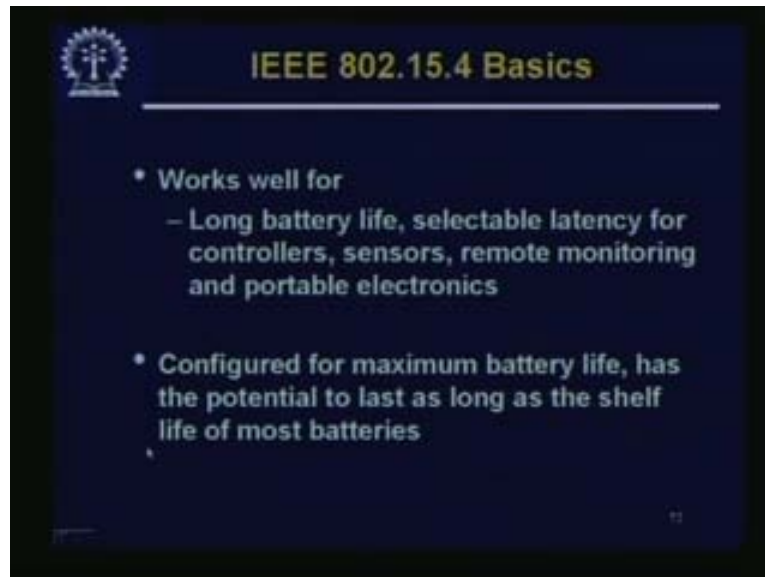
(Refer Slide Time: 54:10)



Just now we have talked about three different ends of the spectrum. I will just mention one or two more, just to show that there are all kinds of other possibilities. For example, after this Bluetooth became somewhat popular, there was a group who wondered why not makes the radius of operation of this even smaller. But here the main emphasis would be on long battery life, so that you put a small battery in a small device and it will just work till the battery's shelf life is over. It will have a very low power. We have the 802.15.4. Similarly, there is an 802.15.2 and 802.15.3.

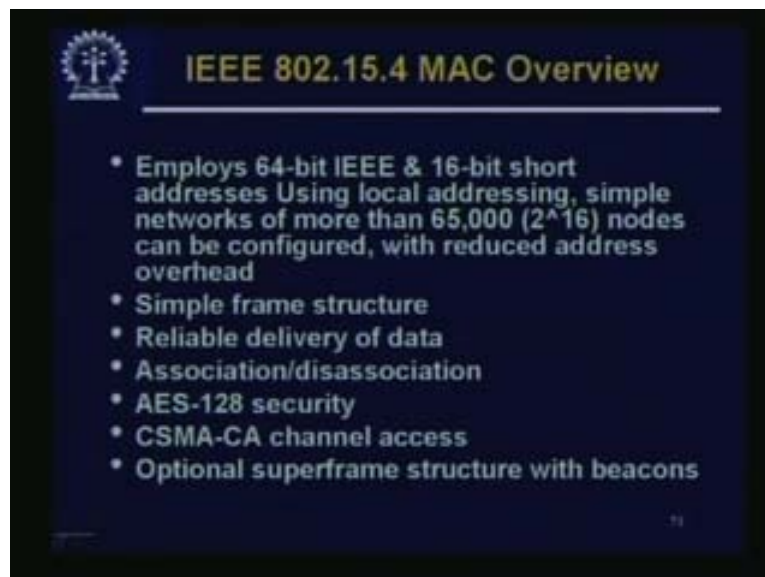
We are not covering any of them; this is just to give you a feeling of the kinds of things, which are going on. 802.15.4 is a simple packet data protocol for low rate; it has no quality of service; has wireless personal area network; is a low power, low cost, device. So low power and low cost are the most important things. Naturally you will get low rate also, but for many applications, this may be quite fine. The channel access is via carrier sense multiple access with collision avoidance, and optional time slotting. It has message acknowledgement and an optional beacon structure – beacon means the signal, which may be sent centrally to synchronize other systems. So three bands and 27 channels are specified: 2.4 GHz and 16 channels; 868.3 MHz and so on.

(Refer Slide Time: 55:56)



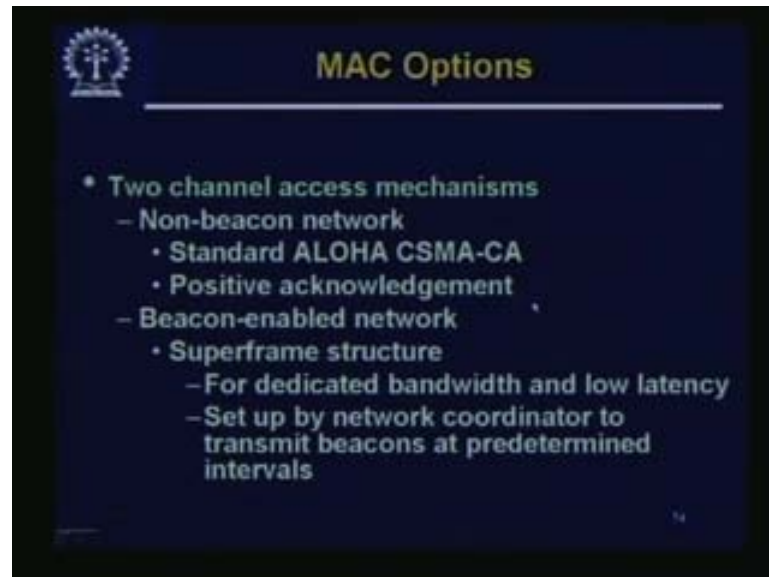
It works well for long battery life; it has selectable latency for controllers, sensors, remote monitoring, and portable electronics. For example, a sensor just stays there; it is supposed to do its work, which is sensing, and may be send little bits of data from time to time. So it has a low rate, no quality of service guaranty, etc. is required, but low power and low cost are very important. That is the focus of this particular group. It is configured for maximum battery life; has the potential to last as long as the shelf life of most batteries.

(Refer Slide Time: 56:40)



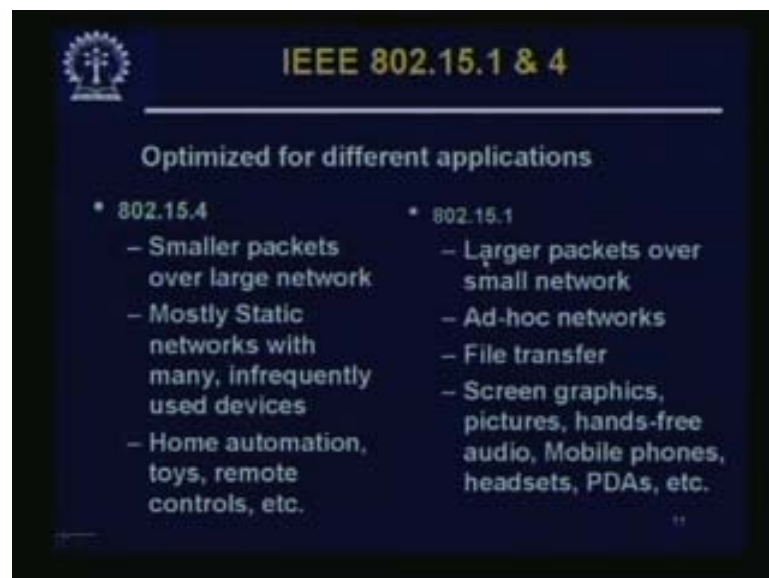
So MAC uses 64-bit IEEE or 16-bit short addresses, using local addressing. That means, if it is just locally, you can have your own 16-bit or you can use the full 64-bit IEEE address; it has a simple frame structure, reliable delivery of data, etc.

(Refer Slide Time: 57:01)



So as I said, there are two channel access mechanisms: one is the non-beacon type, where it uses a standard ALOHA with CSMA CA, that is collision avoidance, and positive acknowledgement; or we can have a beacon enabled network, where it is synchronized. It has a super frame structure for dedicated bandwidth and low latency setup by network coordinator to transmit beacons at predetermined intervals.

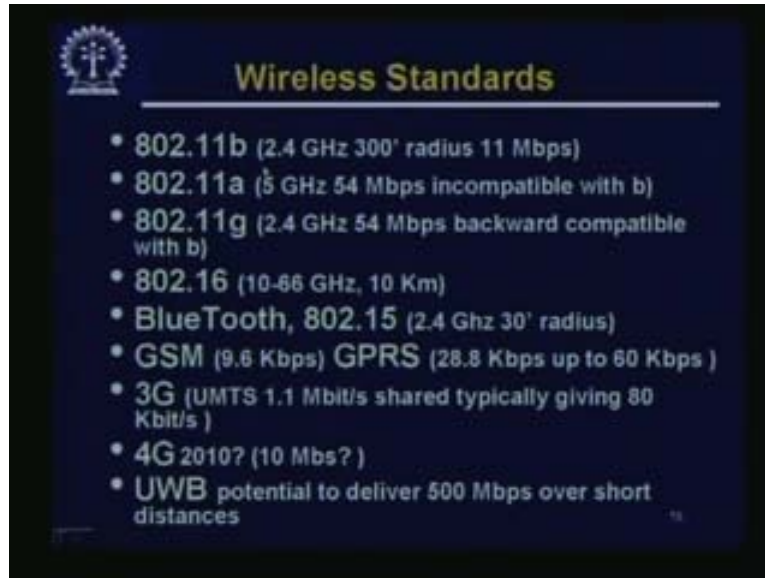
(Refer Slide Time: 57:30)



Let us now compare quickly between 802.15.4, which is the low rate and low power one, and 15.1, which is the standard Bluetooth: it transmits smaller packets over large network and larger packets over small network. They are mostly static networks with many infrequently used devices. This is an ad hoc network, which is more dynamic. You can do things like file transfer here, which you do not look forward to doing here. This may be used for home automation, toys, remote control sensing, etc.

This may be used for screen graphics, pictures, hands-free, etc. So this is a somewhat different niche of application, which is the two groups, but both use wireless with different emphases.

(Refer Slide Time: 58:15)

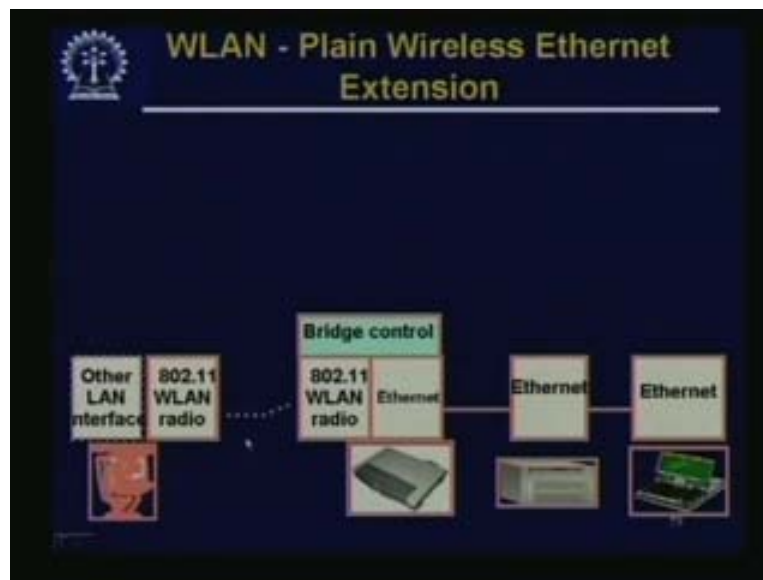


The slide, titled "Wireless Standards", lists the following:

- 802.11b (2.4 GHz 300' radius 11 Mbps)
- 802.11a (5 GHz 54 Mbps incompatible with b)
- 802.11g (2.4 GHz 54 Mbps backward compatible with b)
- 802.16 (10-66 GHz, 10 Km)
- BlueTooth, 802.15 (2.4 Ghz 30' radius)
- GSM (9.6 Kbps) GPRS (28.8 Kbps up to 60 Kbps)
- 3G (UMTS 1.1 Mbit/s shared typically giving 80 Kbit/s)
- 4G 2010? (10 Mbs?)
- UWB potential to deliver 500 Mbps over short distances

As I said, there are many standards – I just listed some of them. There are many more, which I have not put over here: 802.11 b, which gives 11 mbps; a, which gives 54 mbps; g, which gives 54 mbps, but this is backward compatible with b, because b was the one which was most widely deployed in the beginning. 802.16 is for a MAN; Bluetooth has about 30-foot radius; we have talked about GSM GPRS when we talked about cell phones; it is going to 3G. People also talk about of 4G, but nobody knows when even 3G will actually get widely deployed. We have just seen UWB, and there are so many others.

(Refer Slide Time: 58:59)



The one last point is that if you have a wireless LAN, you would want to have a bridge for connecting the TCP/IP stack, etc. We will talk about TCP/IP later on. To transmit from one to another, we require a bridge in-between. This WLAN may be a plain wireless LAN extension and the application will sit on top of this. We require a seamless support for this bridge; that is very important. There are a large number of such protocols, because there is a lot of interest over there. Some of these protocols, etc., will tie up some of them and naturally become very widely used and this is one of the most important areas of networking today. Thank you.