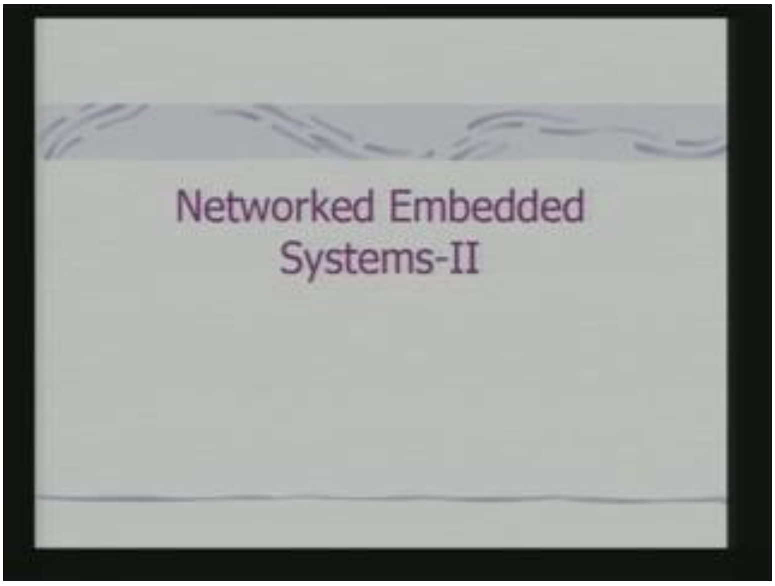
Embedded Systems
Dr. Santanu Chaudhury
Department of Electrical Engineering
Indian Institute of Technology, Delhi

Lecture – 25
Networked Embedded Systems – II

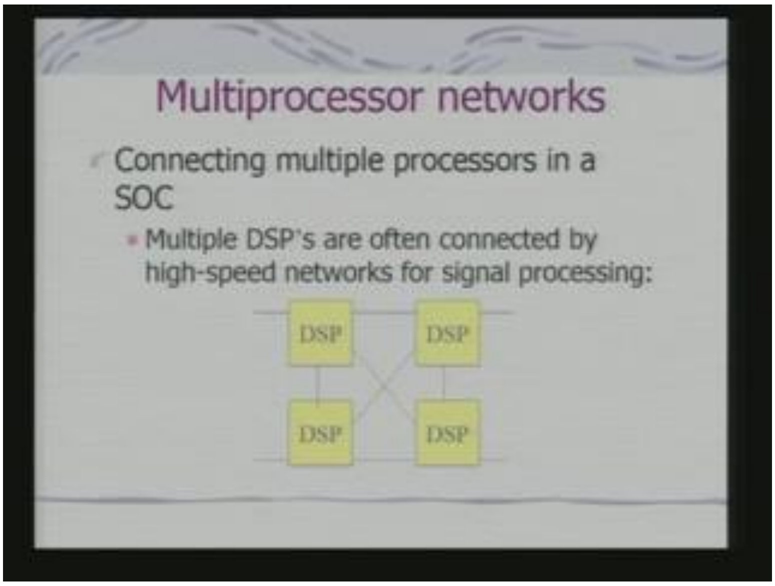
In the last class, we had started looking at network embedded systems. And we have studied a special purpose protocol CAN protocol for connecting embedded micro controllers in an application specific fashion. Today, we shall look at other protocols we shall used with the embedded systems.

(Refer Slide Time: 01:38)



Networked Embedded Systems-II

(Refer Slide Time: 01:41)

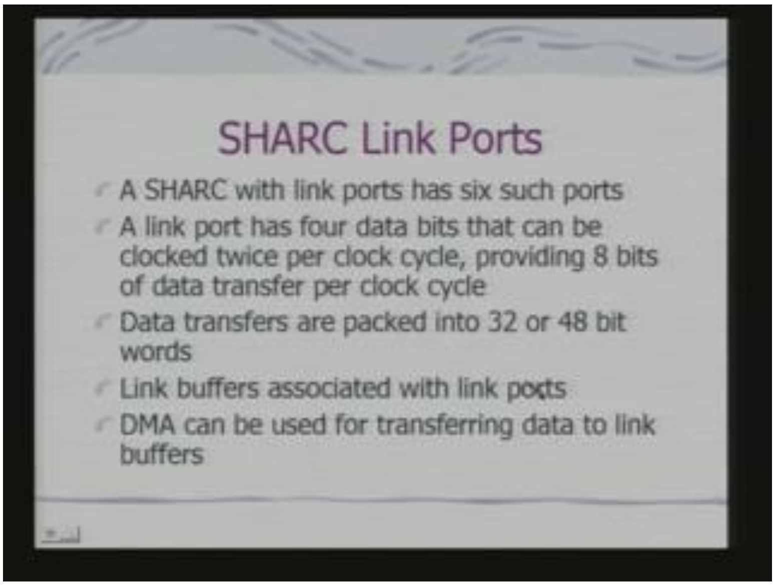


Multiprocessor networks

- Connecting multiple processors in a SOC
  - Multiple DSP's are often connected by high-speed networks for signal processing:

Typically you may use are decide to use multiple processors for an applications where the computation load is high even on associates you have seen that we integrate multiple processing elements. To offer inter connectivity's to this processing elements in as you see in many cases are network is built connecting them an example is multiple DSP's which are connected by a high speed network for doing signal processing applications. So, here what we have shown is direct connectivity in fact, there are 4 DSP's and one DSP is connected to if you see three others. So, they can carry out if required parallel communication with 3 other DSP's typically such a facilities provided on one DSP processor that we had studied earlier that is SHARC.

(Refer Slide Time: 02:51)

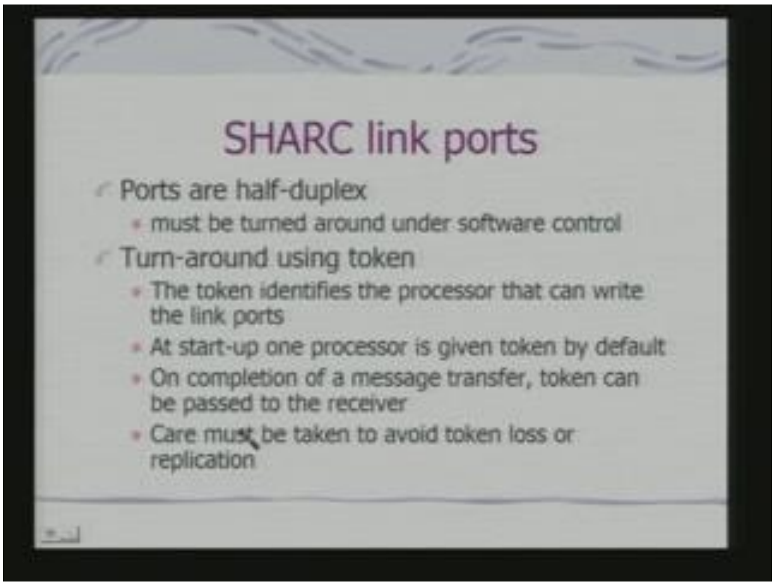


SHARC Link Ports

- A SHARC with link ports has six such ports
- A link port has four data bits that can be clocked twice per clock cycle, providing 8 bits of data transfer per clock cycle
- Data transfers are packed into 32 or 48 bit words
- Link buffers associated with link ports
- DMA can be used for transferring data to link buffers

SHARC has link ports it is not that all SHARC processors will have link ports particular variants to have link ports and if they have link ports they can have a even six such ports. A link port has 4 data bits that can be clocked twice per cycle. So, effectively what we are providing is 8 bits of data transfer per clock cycle. And this data transfers are packed in to 32 or 48 bit words each link port is associated with link buffers. This link buffers contain the data which is to be transmitted and you can use DMA to transfer the data to and from the link buffers.

(Refer Slide Time: 03:52)



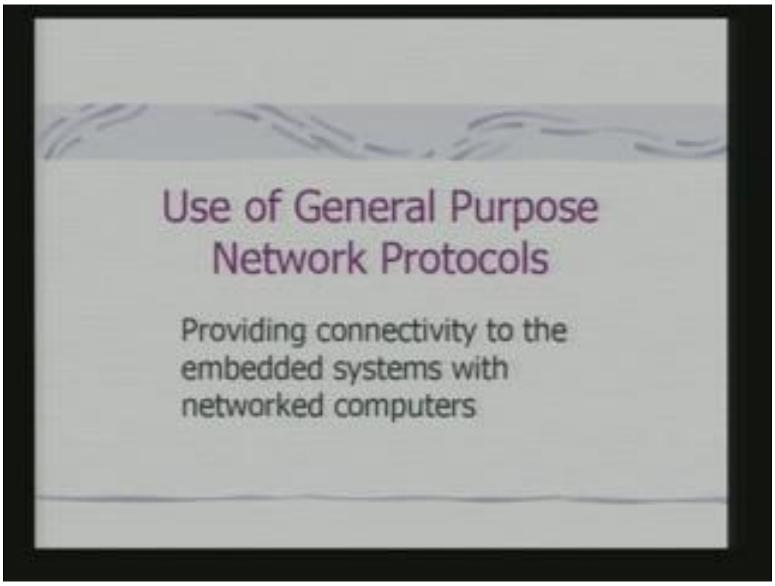
SHARC link ports

- Ports are half-duplex
  - must be turned around under software control
- Turn-around using token
  - The token identifies the processor that can write the link ports
  - At start-up one processor is given token by default
  - On completion of a message transfer, token can be passed to the receiver
  - Care must be taken to avoid token loss or replication

This link buffers a typically half to play in fact for SHARC this link ports are half to play so; that means, one of the processors can transmit along a link port. And the other processor is expect to received data on the corresponding link port both of them can not transmit simultaneously. So, we need to turn this ports around; that means, modalities of operation of this ports have to be changed and these change has to be done under software control. Typically a protocol can be used which is a token based protocol. So, the token identifies the processor that can write the link ports and the token is stored in a particular memory location local to that of the processor. And in fact, this processor are also not sharing any memory among themselves. That start up one processor is given token by default. An completion of a message transfer which may involved a sequence of 8 bytes token can be pass to the receiver when the token receives by the receiver then receiver will change mode and become a transmitter.

So, that is how the turnaround can be done using the token; obviously, under such situation the care must be taken to avoid loss of token or even replication of token. In fact, the token ring network is another network although which is not used in the context of the kind of multiprocessor connection. But token ring network is also similar in concept in which a token is pastor out a system or a processing element which has got the token that is gets a slot for transmission. So, conceptually here if you find if you understand this token is establishing a basic protocol for transmission and reception. In fact, what we have discussed? This is a specific to a set of processors and in fact when we are integrating multiple processing elements on to a cheap. This kind of networks a set up with the network specific protocol design for implementation on the corresponding associate. In many cases you may also find cross bar cross bar switches implemented in the silicon to facilitate communication between processing elements. Next we shall look at general purpose network protocol.

(Refer Slide Time: 06:47)

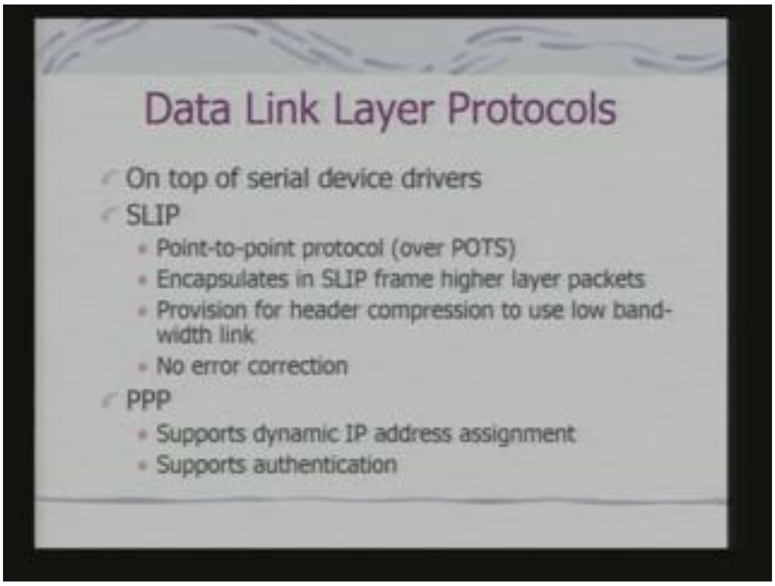


Use of General Purpose Network Protocols

Providing connectivity to the embedded systems with networked computers

What is meant by general purpose network protocols? This is the term which we used for indicating the network protocols is used for connecting the computers. General purpose computers whole across and why would we like these protocol to implemented in the embedded systems? Definitely for providing connectivity to a embedded systems with network computers and these connectivity may be within a local area network may be over a wide area network.

(Refer Slide Time: 07:30)



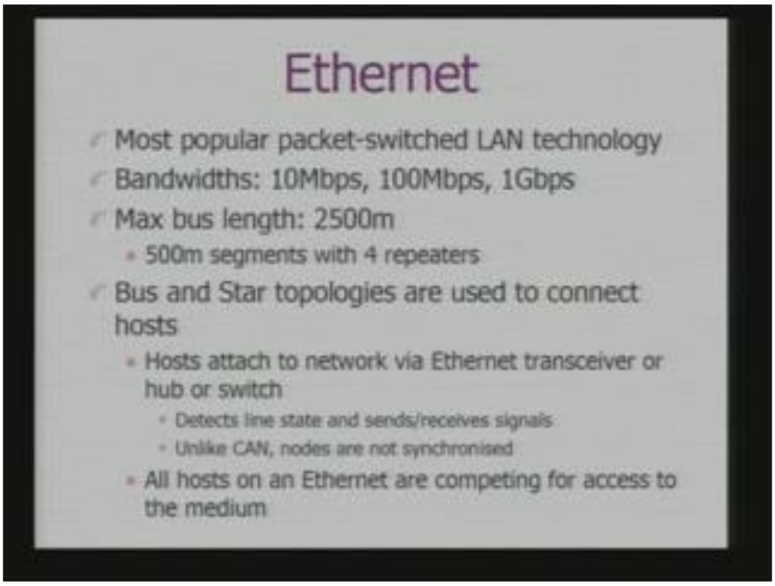
Data Link Layer Protocols

- On top of serial device drivers
- SLIP
  - Point-to-point protocol (over POTS)
  - Encapsulates in SLIP frame higher layer packets
  - Provision for header compression to use low band-width link
  - No error correction
- PPP
  - Supports dynamic IP address assignment
  - Supports authentication

The common data link layer protocol is which are used for establishing communication over serial links are SLIP and PPP. In fact, SLIP is an example of point to point protocol. So, they are when they are communicated communicating if two systems are communicating over a standard telephonic communication line. SLIP can be used for connecting one computer to another computer via mode in event and typically for embedded systems. You will expect that if it is provided with the serial port or an USB port this SLIP bills on the protocol for this kind of connectivity over any kind of serial port that is provided in the embedded appliances. What are the features of the SLIP? It is; obviously, point to point and it encapsulates data in SLIP frame for higher layer processing in fact this is a data link layer.

So, there will be data framing. So, that data framing format is define by the SLIP interestingly this supports provision for header compression, because what is the expected when you are communicating with the serial point to point link the available bandwidth will be small. So, you should have support for compression of the header of the packets, but, the SLIP. The basic disadvantage of the SLIP is it does not support any kind of error correction if you remember with the CAN the, I said there are error correction and that becomes also part of your data link layer functionality. If you look at the other protocol PPP; this supports dynamic ip address assignment; this dynamic ip address assignment cannot be done through SLIP protocols and it also supports authentication. So, that, a minimum security feature end to end security feature can be implemented.

(Refer Slide Time: 9:45)



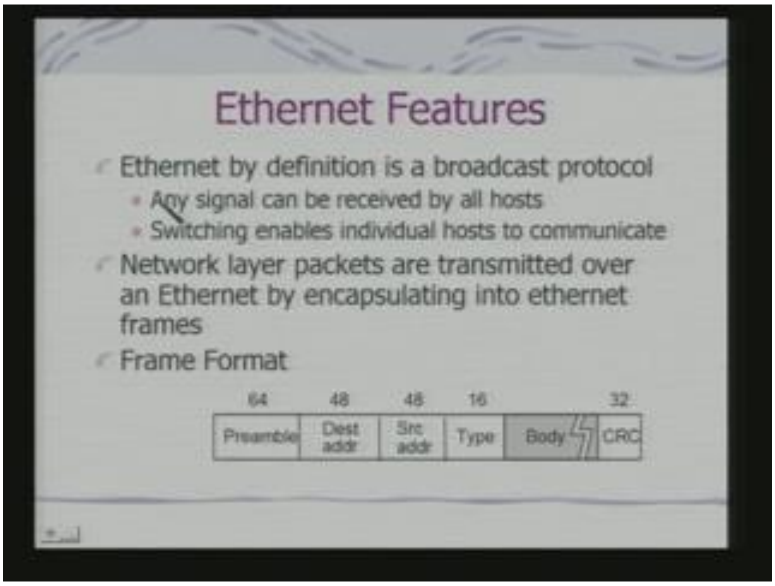
Ethernet

- Most popular packet-switched LAN technology
- Bandwidths: 10Mbps, 100Mbps, 1Gbps
- Max bus length: 2500m
  - 500m segments with 4 repeaters
- Bus and Star topologies are used to connect hosts
  - Hosts attach to network via Ethernet transceiver or hub or switch
    - Detects line state and sends/receives signals
    - Unlike CAN, nodes are not synchronised
  - All hosts on an Ethernet are competing for access to the medium

If you look a the packet switched network in general Ethernet is the most popular packet switched LAN technology it works in typically bandwidths of 10 Mbps 100 Mbps. And even today you got giga bit Ethernet and it can have maximum bus length of about 2500 meters. Typically the whole calculation can be that the segments individually can be a five hundred meters with repeaters built in to that. Commonly bus and star topology are used to connect hosts. Hosts attach to network via what we called Ethernet transceiver or hub or switch. Therefore, all the hosts which are connected via bus can be are fully listen to this going on in the bus. So, a host can detect line state that is the state of the common line connecting the hosts and accordingly decides to send are received signals.

But what is fundamentally different from CAN is that notes are not synchronized with respect to the universal clock in the sense. If you remember in the CAN all the nodes which are intending to transmit a frame will start transmission at the same time. And so, using the principle of dominant beat we can resolve conflict on the basis of the priority value of the identifier here. Ethernet at any point of time any node may decide to transmit beats. This is the basic difference of Ethernet with respect to your CAN or even other buses like your eye to see and therefore, all host are a Ethernet with competing for accessing the media. So, this is a basic conflict scenario which needs to be take care of.

(Refer Slide Time: 12:06)



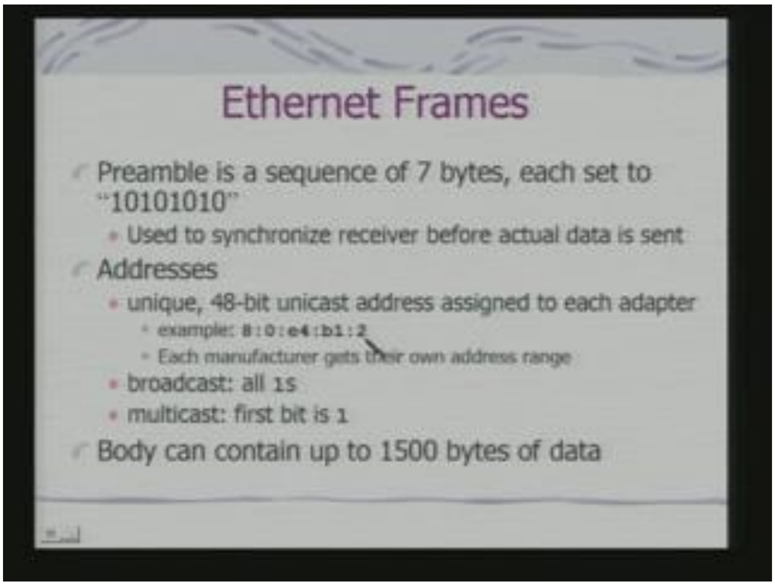
Ethernet Features

- Ethernet by definition is a broadcast protocol
  - Any signal can be received by all hosts
  - Switching enables individual hosts to communicate
- Network layer packets are transmitted over an Ethernet by encapsulating into ethernet frames
- Frame Format

64	48	48	16		32
Preamble	Dest addr	Src addr	Type	Body	CRC

So, as we have already stated that this host are all connected to the common link by definition by a broad cast protocol. Any signal can be received by all hosts and switching enables individual hosts to communicate. Now, network layer packets are transmitted over an Ethernet by encapsulating in to what is called Ethernet frames. And Ethernet frame format is something like this if you look at this packet of the Ethernet frame format you will find that here you have got the destination address you have got a source address. So, by using the destination address processing element, but, a computer would know whether the packet is intended for it or not.

(Refer Slide Time: 12:59)

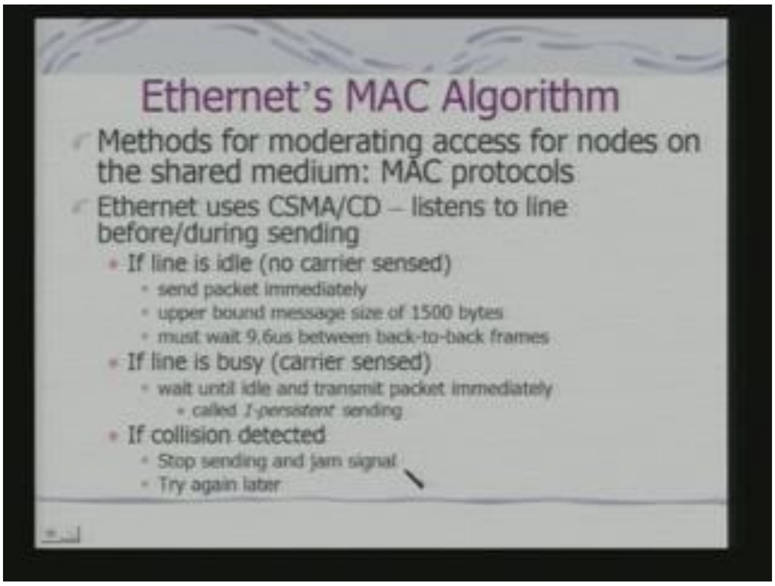


Ethernet Frames

- Preamble is a sequence of 7 bytes, each set to "10101010"
  - Used to synchronize receiver before actual data is sent
- Addresses
  - unique, 48-bit unicast address assigned to each adapter
    - example: `8:0:e4:b1:2`
    - Each manufacturer gets their own address range
  - broadcast: all 1s
  - multicast: first bit is 1
- Body can contain up to 1500 bytes of data

So, in a frame in typically also has a preamble which is of seven bytes and it is used to synchronize receiver before actual data is sent; that means, receiver on receiving this information. So, all of this elements which are connected to the Ethernet can be can ready itself for receiving the data the address is the typical 48 bit unicast address. So, this is an example and each manufacturer can associate its own address. Now, if it is to be broadcasted then you use special address for multicasting also you need to use special address. So, once this address is changed then the hosts listing to the data would understand whether it is intended for multiple receivers are intended for a unique receiver and what you can contain up to 1500 bytes of data.

(Refer Slide Time: 14:05)

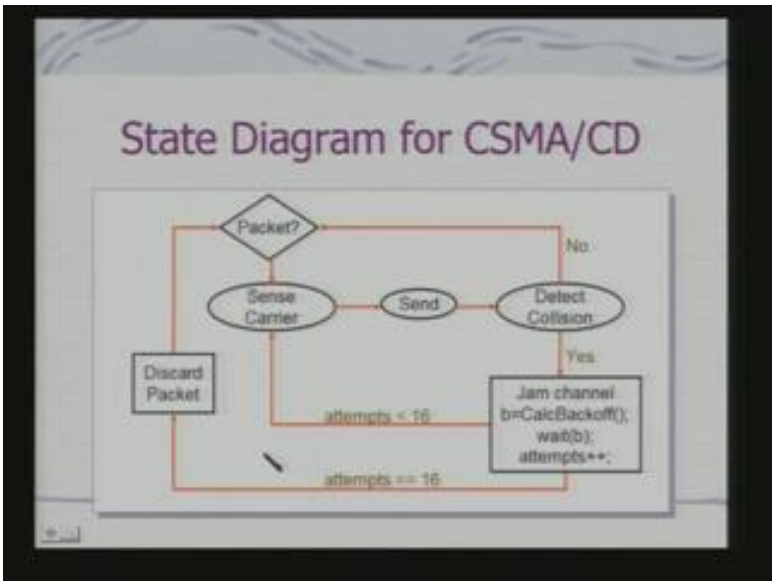


Ethernet's MAC Algorithm

- Methods for moderating access for nodes on the shared medium: MAC protocols
- Ethernet uses CSMA/CD – listens to line before/during sending
  - If line is idle (no carrier sensed)
    - send packet immediately
    - upper bound message size of 1500 bytes
    - must wait 9.6us between back-to-back frames
  - If line is busy (carrier sensed)
    - wait until idle and transmit packet immediately
      - called *1-persistent* sending
  - If collision detected
    - Stop sending and jam signal
    - Try again later

Now, Ethernets MAC algorithm is the most interesting feature of Ethernet, because you need a mechanism as part of this protocol and mechanism for moderating access for nodes on the sheared medium. And that basically defines the MAC protocol media access protocol. Ethernet uses CSMA CD now; obviously, these protocol different from your CAN protocol because it actually resolves the conflicts on the basis of priorities. So, that part is not straight away coming in here. So, what is the basic protocol if line is idle; that means, no carrier is technically sensed send packet. Immediately the upper bound of the message size 1500 bytes and must wait 9.6 micro second between back to back frames, because that gives a basic time interval. If the line is busy wait until idle and transmit packet immediately and these phenomena is called one persistent sending. If collision is detected stop sending jam the signal and try again later. So, when there is a collision detect what you do? You withdraw and then try later on. So, that is why we say that this is collision detect protocol.

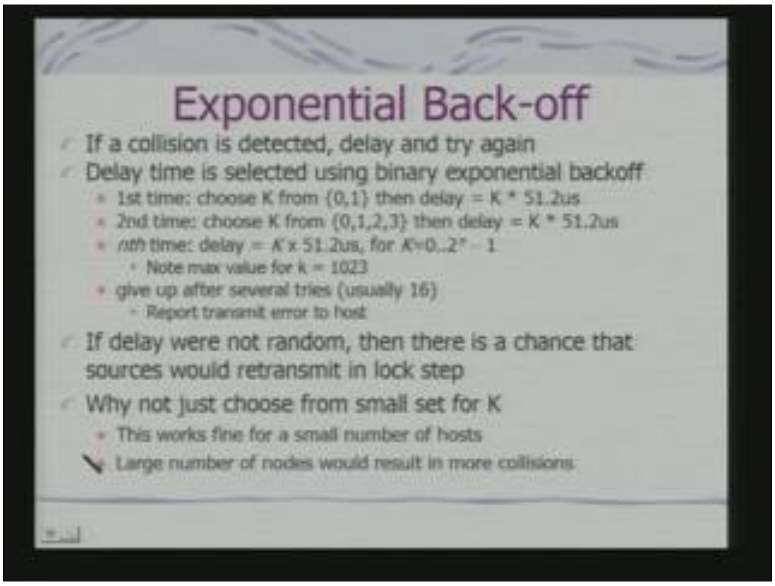
(Refer Slide Time: 15:44)



State Diagram for CSMA/CD

So, let us look at the state diagram of the corresponding protocol machine. So, when we have a packet which is to be transmitted packet is what a frame according to Ethernet format you sends a carrier and you can send, but, you also detect for the collision. So, if you detect the collision what you do? You go back; that means you detect the collision. So, it cannot send the packet and again you go back and retry that is you no collision. So, the next packet can be send without any problem if there is a collision it is detected. Then you jam the channel in the sense that you do not send the packet you calculate the parameter called B we shall see how the parameter can be calculated and you make subsequent attempt after a waiting period. Now, if the attempts what you say is less than 16 they can upper bound in the number of attempts then you go back and try sending the packet again. If it is more than 16 are equal to 16 in this case if you using the number a 16 you basically discard the packet and report an error fine. So, this is the basic state diagram for CSMA CD which is followed by Ethernet.

(Refer Slide Time: 17:19)



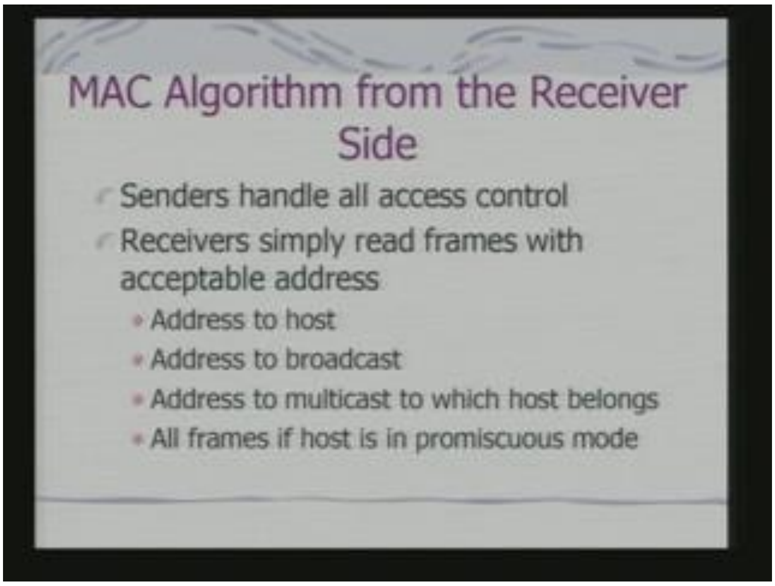
Exponential Back-off

- If a collision is detected, delay and try again
- Delay time is selected using binary exponential backoff
  - 1st time: choose K from {0,1} then delay = K * 51.2us
  - 2nd time: choose K from {0,1,2,3} then delay = K * 51.2us
  - *nth* time: delay = *K* x 51.2us, for *K*=0..2^n - 1
    - Note max value for k = 1023
  - give up after several tries (usually 16)
    - Report transmit error to host
- If delay were not random, then there is a chance that sources would retransmit in lock step
- Why not just choose from small set for K
  - This works fine for a small number of hosts
  - Large number of nodes would result in more collisions

Now, the interesting feature is of how do you back of; that means, when you detect the collision how do you decide what will be the next time instance for the transmission? So, the delay time is chosen in a random fashion in fact, this a choice of K. And on the basis of the choice of K you randomly make a choice of K and that defines the delay this is a exponential back off, because the back off time changes and increases. So, the maximum value of K that can be 1 0 2 3 and you can give a after several choice what we say that I on this case what is important to note this value of K is randomly chosen. So, the delay that is applied is a random delay. So, why delay is random?

Because if there is no random delay then there is chance that sources would retransmit in lock step. That means, they would again land up in to a collision and why not just choose from a small set for K this works fine for a small number of hosts that if the number of hosts increases. Then large number of nodes would result in more collision of the small number of K and that is why used larger number of k. Now, what is important to know as a embedded system designer that because of this random rate parameter getting involved the performance of the Ethernet is not completely predictable. Because if I what to have any real time service the ported on Ethernet I would like to have prêt editable performance. Because of the exponential back off with the random selection of delay the performance of Ethernet is not strictly predictable..

(Refer Slide Time: 19:16)

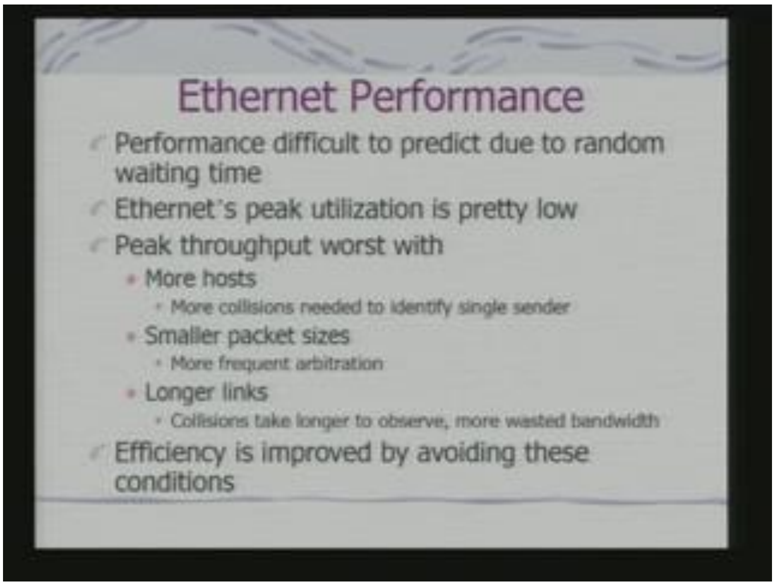


MAC Algorithm from the Receiver Side

- Senders handle all access control
- Receivers simply read frames with acceptable address
  - Address to host
  - Address to broadcast
  - Address to multicast to which host belongs
  - All frames if host is in promiscuous mode

The MAC algorithm from the side of the receiver is very straight forward, because sender handles all access control receivers jobs is simply to read frames with acceptable address. If it address to a particular host if it is a address to a broadcast are address to multicast to which host belongs. Then it will read that frame are if it is a promiscuous mode for some reason or other it will read all the frame. So, this is a very straight forward MAC algorithm for the receiver.

(Refer Slide Time: 19:54)

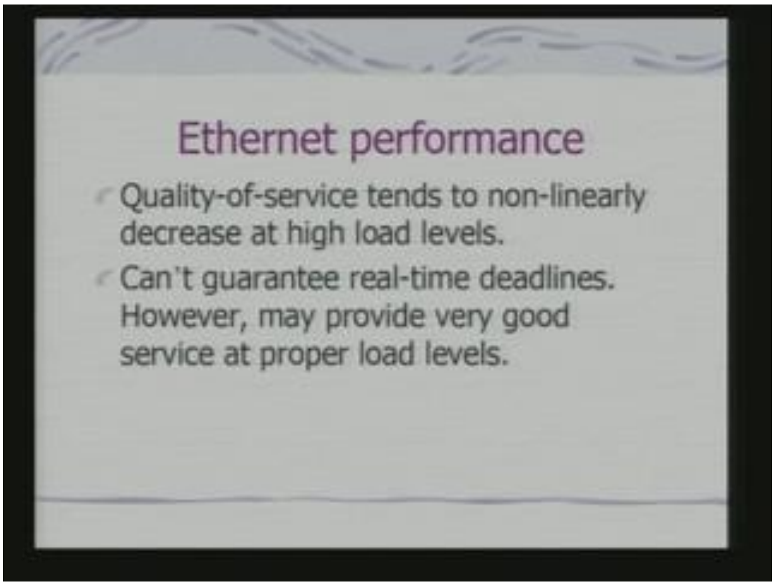


Ethernet Performance

- Performance difficult to predict due to random waiting time
- Ethernet's peak utilization is pretty low
- Peak throughput worst with
  - More hosts
    - More collisions needed to identify single sender
  - Smaller packet sizes
    - More frequent arbitration
  - Longer links
    - Collisions take longer to observe, more wasted bandwidth
- Efficiency is improved by avoiding these conditions

So, if you look at the performance, because the performance is a key issue. If you want to connect multiple embedded system in a Ethernet the problem is as I have already stated performance is difficult to predict due to random waiting time. And that is also one of the reasons why Ethernet peak utilization is pretty low there would be a conflict and there will be a random wait. And they may be time there are no packet transmitted on the link and peak throughput can become worst if you have more hosts. Because there will be more collisions if you have smaller packet sizes then the frequents with which host to try to send packets will be more hence more collisions. Longer links also can source a problem because how is collision detected collision is detected on reading the packet. So, if the delay is long that if the if there the ling the links collisions will take longer to observe. So, there will be a unnecessary wastage of band width. So, efficiency can be improved by avoiding these conditions.

(Refer Slide Time: 21:10)



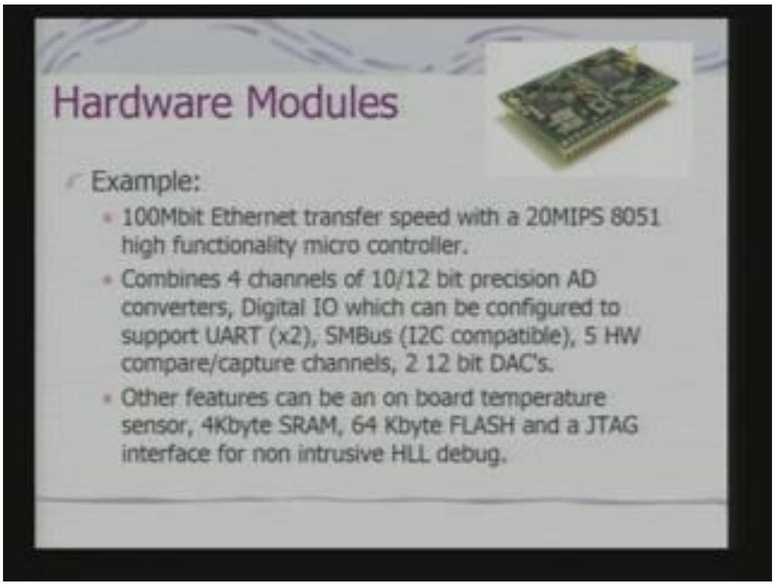
Ethernet performance

- Quality-of-service tends to non-linearly decrease at high load levels.
- Can't guarantee real-time deadlines. However, may provide very good service at proper load levels.

So, if you summarize that we are try to say that quality of service tends to non-linearly decrease at high load levels. That means, the delay the basic quality of service here we are trying to talk about is say the delay in the packet arrivals. In fact, the variation in the delay in the packet arrival and not really bounded and that is the reason why you cannot guarantee real time deadlines. But if your load is less; that means, if the number of nodes connected is less may provide good service. So, in fact, you will also find that video conferencing or teleconferencing equipments coming enabled with Ethernet. So, basically you can use Ethernet for video conferencing applications when the load is less.

And if the load increases what will happen? There will be problem in receiving the data and thing you have an unless how the video conferencing appliances is relevant in this context. Because you have to send video as well as audio data packets and I need to have bounded delay for the arrival of packets, because if I have bounded delay then I can allocate fixed buffers. So, that the presentation is not of low quality; that means, if not represent one frame and next frame represent after much delay. So, the continuity is lost your speech is broken in between. So, such kinds of problems will not occur if you know and estimate of the worst case performance of your Ethernet. But that is not always possible and that is a basic bottle net in using Ethernet as a basic network for this kind of application.

(Refer Slide Time: 23:13)



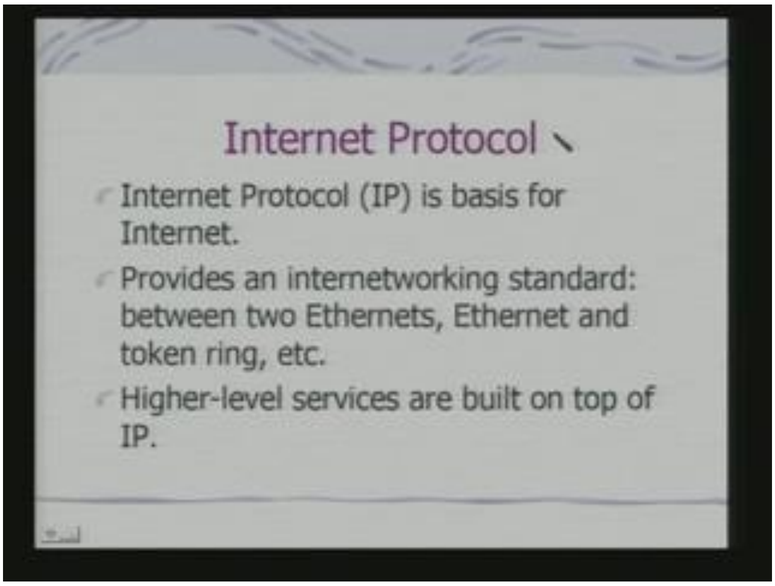
Hardware Modules

- Example:
  - 100Mbit Ethernet transfer speed with a 20MIPS 8051 high functionality micro controller.
  - Combines 4 channels of 10/12 bit precision AD converters, Digital IO which can be configured to support UART (x2), SMBus (I2C compatible), 5 HW compare/capture channels, 2 12 bit DAC's.
  - Other features can be an on board temperature sensor, 4Kbyte SRAM, 64 Kbyte FLASH and a JTAG interface for non intrusive HLL debug.

There are various hardware implementation of Ethernet protocol, because if there is no requirement strictly real time constraints. Then you can use Ethernet for a variety of applications here we are looking at an example hardware. This is an embedded stand alone embedded system why because it has got 100 Mbit Ethernet transfer speed with an 8051 micro controller. That means, this Ethernet protocol is enabled a provided with the hard ware additional hardware as well as with the micro controller. So, along with these you have got 4 channels of AD converter digital IO and you have got I2C compatible bus availability. Then compare and capture channels also it has got one board static RAM one board flash in JTAG interface for high level debug. Now, these kind of products are there today available why they available?

You can add on such a card to your appliance and very easily provide Ethernet connectivity if you see it has got I2C compatibility. So, using the I2C you can connect it your main system and you can have data transfer to this kind of a small food print device n. So, that you can plug through this card your appliance to an Ethernet port and have Ethernet enabled connectivity. Now, in this case the basic protocol here gets implemented on the processor there are also devices in a appliances were you built this stack in the hardware itself. So, the entire stack is built in to hardware may be using in FBGA block which enables more efficient implementation of this protocol. So, at a low cost you get a module with a small food frame which you can add to your appliance.

(Refer Slide Time: 25:30)

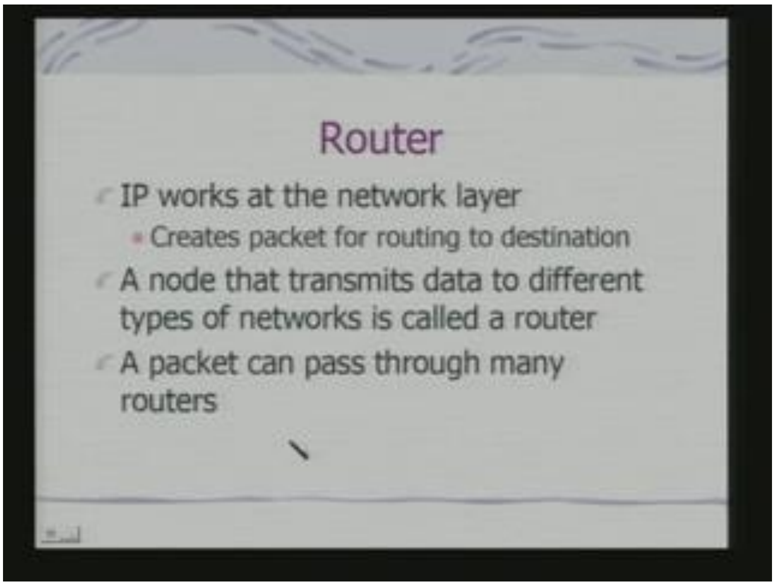


Internet Protocol

- Internet Protocol (IP) is basis for Internet.
- Provides an internetworking standard: between two Ethernets, Ethernet and token ring, etc.
- Higher-level services are built on top of IP.

Next we shall look at internet protocol which is actually the basis for today's internet internet protocol why it is called internet protocol? It provides a internetworking standard that is connectivity between 2 Ethernets, Ethernet and a token ring networks. We have already refer to a token ring network where basically a token past around the processing elements. And when the token is available with the processing element it can transmit data and higher level services are built on top of this internet protocol.

(Refer Slide Time: 26:06)

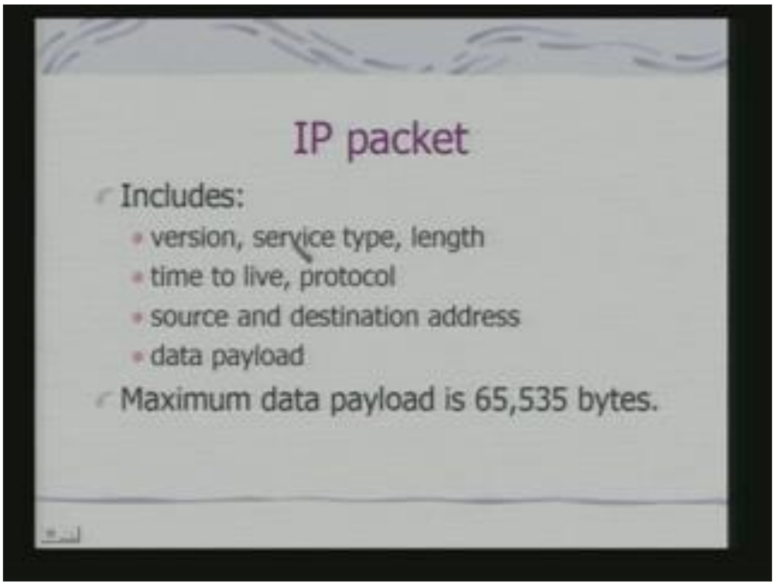


Router

- IP works at the network layer
  - Creates packet for routing to destination
- A node that transmits data to different types of networks is called a router
- A packet can pass through many routers

Now, the internet protocol basically implemented through a router when you are connecting to distinct networks and IP works what we say at the network layer. So, if the network layer the IP protocol creates packets for routing to destination and in fact, a node that transmit data to different types of networks is called a router. So, router may not have top layer protocols implemented its basic job would be to receive packets and rout the packets to the respective networks depending on the destination address. So, a packet on its path can pass through many routers and in fact there may be packets are generating from one destination. But two consecutive packets may be put on to two different route by the router itself and that is the basic reason why we called this a packet switching networks. Packets are switch from one path to another path and you can also realize that if these kind of packets switching takes place at a particular node. This node needs to handle pretty high computation load, because if you are looking at one giga bit Ethernet then switching at the has to meet that speed of the back board.

(Refer Slide Time: 27:44)

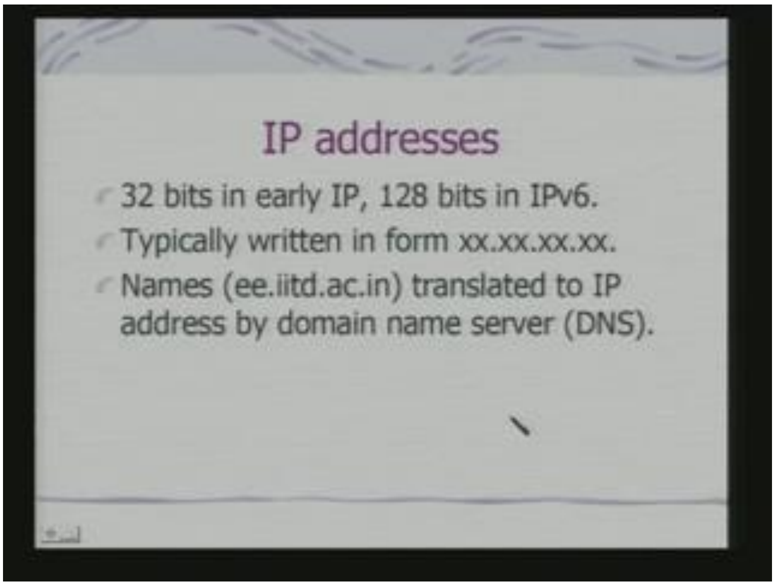


IP packet

- Includes:
  - version, service type, length
  - time to live, protocol
  - source and destination address
  - data payload
- Maximum data payload is 65,535 bytes.

IP packets are have got information's like versions service type length source and destination address as well as data payload and data payload can be maximum of 65535 bytes.

(Refer Slide Time: 27:58)

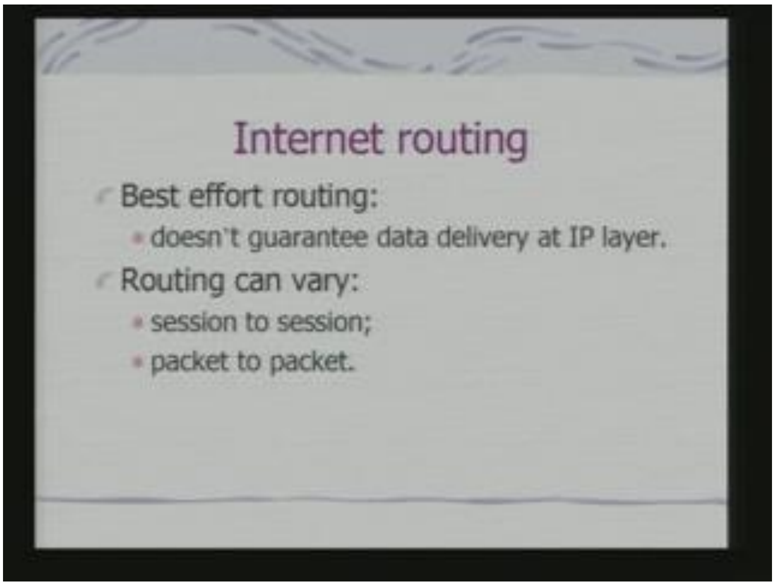


IP addresses

- 32 bits in early IP, 128 bits in IPv6.
- Typically written in form xx.xx.xx.xx.
- Names (ee.iitd.ac.in) translated to IP address by domain name server (DNS).

The addresses are very well known it was 32 bits in early IP and 128 bits in IP version 6. And typically written in a written in this form there can be the number of digits depending on the address that are getting allocated. And you have got the domain name server which transforms this kind of symbolic addresses to actual IP addresses. Please note that this IP addresses are different from that of your Ethernet addresses. So, Ethernet addresses are provided at the manufacturer's level this IP addresses are provided the network administrators.

(Refer Slide Time: 28:42)

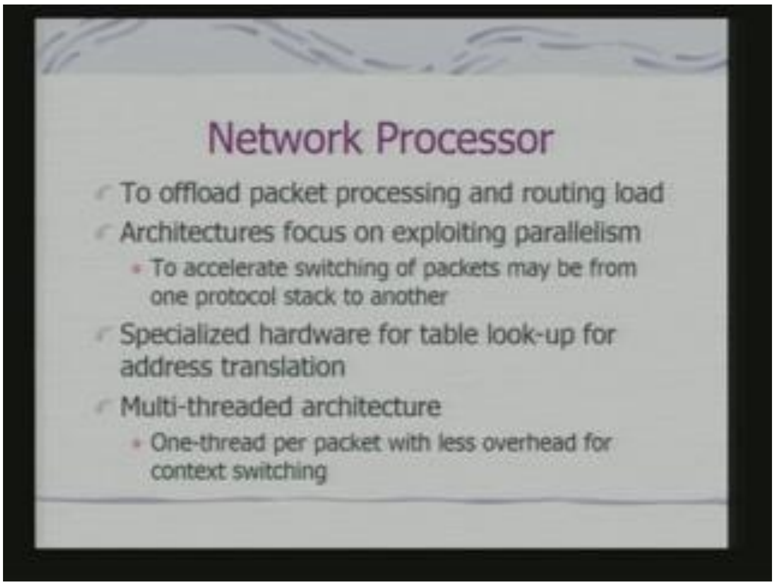


Internet routing

- Best effort routing:
  - doesn't guarantee data delivery at IP layer.
- Routing can vary:
  - session to session;
  - packet to packet.

Now, when the routing takes place what we say this is a best effort routing. So, there is no guarantee for data delivery at IP layer. So, even when the routing is talking place and router is routing the packets it will try to match the availability of the bandwidth, but, and it is a best effort. So, there is no guarantee there is no guarantee that packets will be delivered with regard to a deadline. So, routing can vary from session to session and even packet to packet and if you are really looking at multimedia data transfers over such a network where the deadlines becomes important you got to have additional protocol layers implemented on top of them to have efficient routing. Now, how does this routers have implemented?

(Refer Slide Time: 29:40)



Network Processor

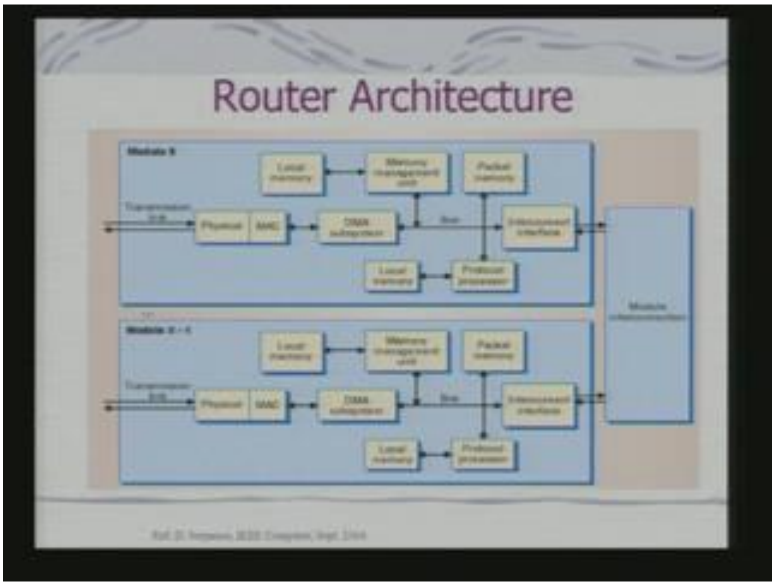
- To offload packet processing and routing load
- Architectures focus on exploiting parallelism
  - To accelerate switching of packets may be from one protocol stack to another
- Specialized hardware for table look-up for address translation
- Multi-threaded architecture
  - One-thread per packet with less overhead for context switching

In fact, routers are again examples of embedded systems, because routers do have processing elements, but, they are not really general purpose computers the basic jobs is to receive packets and rout packets. So, you have got network processors which had been used for implantation of this kind of router. So, basic job of a network processor to offload packet processing and routing load and in fact you may also find that for a general purpose application are general purpose computer may have a network processor card which is functioning as a router. So, your main processor may be offloaded of this tasks that is also is possible also you can have stand alone routers as well. So, the architecture of this type of processor which are targeted for use in routers. The basic focus is to exploit parallelism to accelerate switching of packets may be from one protocols stack to another.

We have considered an example I have routing of packets from a one it Ethernet to the another Ethernet. This is one Ethernet network to another Ethernet network, but, it can be from one Ethernet network to a token ring network. Then it has to be a protocol translation, because protocol of Ethernet is different from that of the token ring say your packet headers have to be strip the packet has to be reframed. So, that it can be put on to another network. So, that job is to be a handle by the network processor. So, what you find is that there are basic objective is exploit parallelism to take care of this thing. One very important part of routing is table look up for address translation because on the basis of the address you need to know where the packet is to send next. So, address look up are even the routing table look up if you already maintaining the routers in many cases maintain the routing table maintenance of router table requires facilities for very first table look up. So, if such a facilities implemented in hardware it becomes easier and more efficient.

So, you have got specialized hardware for table look up also this architecture are multi threaded architecture what did, what is meant by multi threaded architecture? It means that in hardware itself there is a support for individual threads. So, you can associate a thread with each packet and the whole system itself behaves that is the your processor behaves in such a way that it is handling a thread independent of other thread. So, if you remember when thread is implemented through os operating systems keep track of the thread keep track of the PC. But here when we have the hardware support the hardware itself provides the book keeping task meets the book keeping requirements for managing multiple threads. And if you can have one thread per packet with less overhead for contact switching you have actually doing what meeting the requirement of switching packet and putting it to a another network depending on the requirement.

(Refer Slide Time: 33:24)

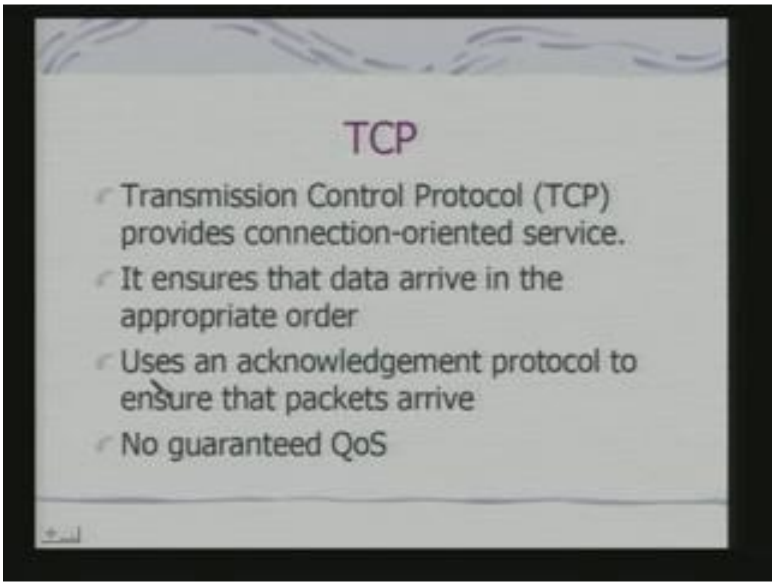


Router Architecture

So, the router look something like this, what you have shown here is a router consisting of multiple modules not just a single modules. But multiple modules and these 2 blocks are taking care of a physical layer requirements as well as MAC protocol which were already discussed, because router come at the network layer level. So, you have got your local memory and this is DMA subsistence. So, the DMA subsistence will do the transfer from to a packet memory to the MAC on the bus. And here the protocol processor did not be involved over the actual data transfer what does the protocol processor would do?

Protocol processor can do protocol translation I have already told you it can also do what actual finding of the route for the packet and this modules are connected via interconnection block. So, what you find you first, that each module now can operate independently and that gives you the maximal parallelism for the packet processor. So, this two architectures are identically depending on what is the speed on which we like to work. They can be multiple such modules being make use of and infact all this routers are nothing, but, examples of your embedded systems. TCP is an transmission control protocol which is provides connection oriented services that is from source to destination.

(Refer Slide Time: 35:04)

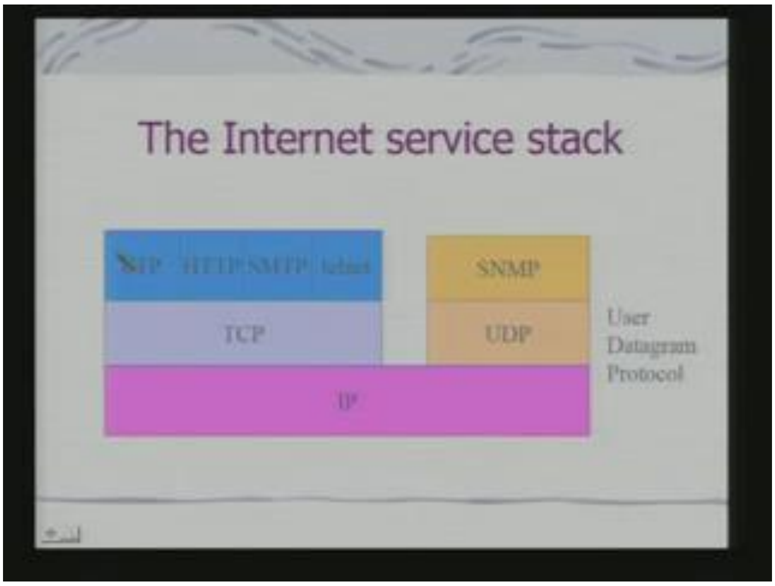


TCP

- Transmission Control Protocol (TCP) provides connection-oriented service.
- It ensures that data arrive in the appropriate order
- Uses an acknowledgement protocol to ensure that packets arrive
- No guaranteed QoS

The complete connection is provided by the TCP layer if you remember what the IP doing getting a packet routing it in different way, but, where is the origin of the packet packets origin is at an application. Now, with respect to the application the transport control protocol TCP maintains the connectivity with that of the destination application. In fact, there would be a other layers where from where the packet would generate and other features would be managed with respect to the packet. But connection oriented a management is primarily done by the TCP protocol. So, the first job is to make sure that the data arrive in a appropriate order, because this packets are put in to different routes packets can arriving different order. They have to be assemble in correct order that is top of the city it is also uses an acknowledgement protocol to ensure that the packets arrive. But; however, there is no guarantee quality of service guarantee quality of service is again very simple quality of service is that you are looking for may be a bound in the delay for the packets arriving and in fact one parameter which we refer to as getter that is the variation in the deal. So, even if you have the variation in the delay bounded then also there is a QoS guaranteed. The TCP really does not guarantee quality of service on top of TCP basically applications are built. So, here the basic model is you can have the file transfer protocol.

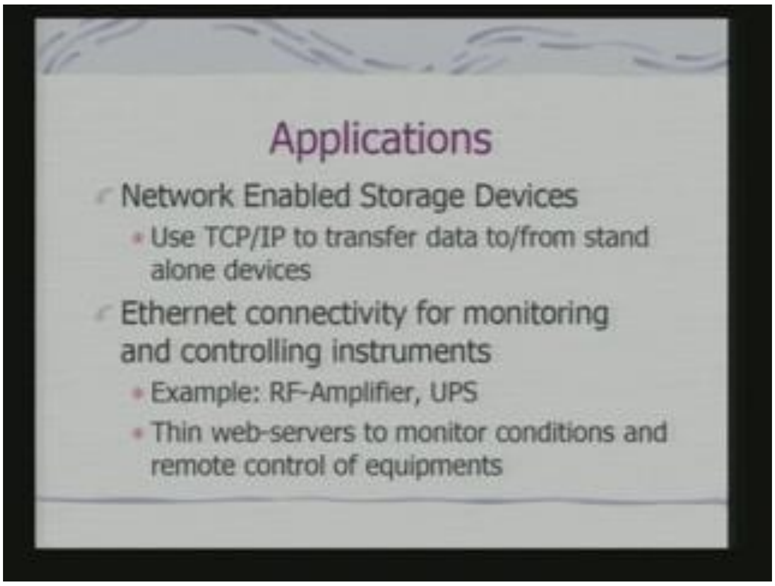
(Refer Slide Time: 36:51)



The Internet service stack

This is your each http protocol hyper text transfer; this is your basically mail protocol; this is a telnet remote login protocol; this is for UDP user data gram protocol and this is simple network management protocol. So, this is the various protocols stop level protocols which sit on top of IP and TCP and IP and UDP. In fact, today you will find the many of your embedded system really have support for your HTTP protocol implementation so that you can access those devices over HTTP link from any computer. So, what is the advantage of that? Advantage is you if you have the web browser you can access a monitor a remote device.

(Refer Slide Time: 37:41)



Applications

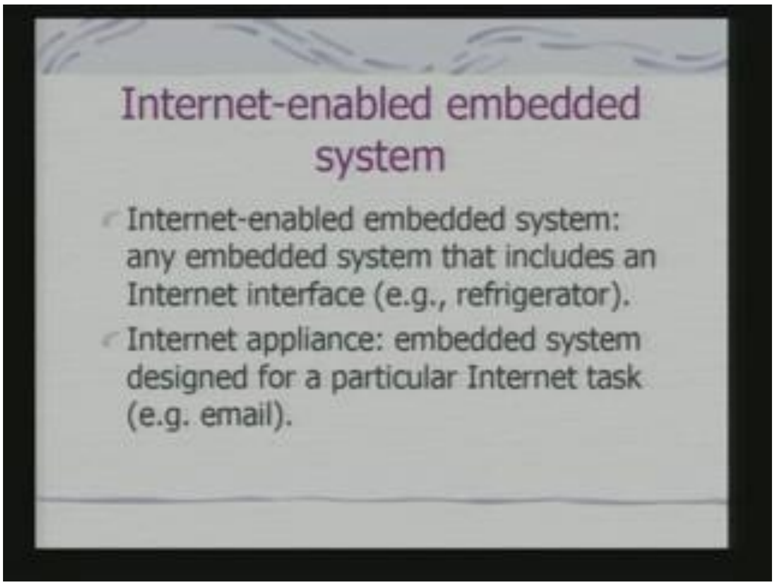
- Network Enabled Storage Devices
  - Use TCP/IP to transfer data to/from stand alone devices
- Ethernet connectivity for monitoring and controlling instruments
  - Example: RF-Amplifier, UPS
  - Thin web-servers to monitor conditions and remote control of equipments

So, let us see some example. So, you can have network enables storage devices we have typically found that have got a hard disk or a magnetic tape which is typically associated with the computer it need not be. So, I can have a hard disk with a embedded system attached to it making it a network enabled storage system. So, the data storage takes place over a network. So, you can have say for example, in your home are network enabled data store using which you can store may be a TV program which you are receiving in a digital format may also store your telephone directory from your PDA using a network. So, then if this storage devices becomes stand alone devices if they become TCP IP enabled. So, use TCP IP to transfer data to and from stand alone devices. So, these protocol gets implemented I have already showed module for a implementation of Ethernet on that similar module you can have the complete TCP IP implementation.

And you attach that your hard disk hardware you get a effectively and network storage system. Then you can provide Ethernet connectivity as well as TCP IP connectivity for monitoring and controlling instruments I can have a radio frequency amplifier which they use for a broad cast rather applications. Now, you want to monitor it condition that you want to set parameters to the RF amplifier. How to do that? You can have a digital interface if you have a digital interface then using the digital interface you can do a remote connection. And through the remote connection you can provide this features and other example is an UPS if you want to monitor battery life of an UPS remotely. So, what you provide? You provide a TCP IP as well as Ethernet enabling features in fact, if you remember we had send an example of a vending machine which is Ethernet enabled.

So, that the complete a stock monitoring can be done from a remote location in fact on this devices if they really implementing TCP IP on top of this TCP IP you may find thin web servers very basic web servers implemented and why web servers? Because if I am using a web browser any computer which has got a basically a web browser are you can use that web browser to connect to this devices. So, if you have a web server running at the device then I can connect to those device s using my browser monitor it conditions set their parameters. So, I get a complete facility for remote monitoring and remote controlling of any equipment in fact that is the major application of Ethernet and TCP IP for in the embedded domain. So, we get with this we call internet enabled embedded system.

(Refer Slide Time: 41:08)

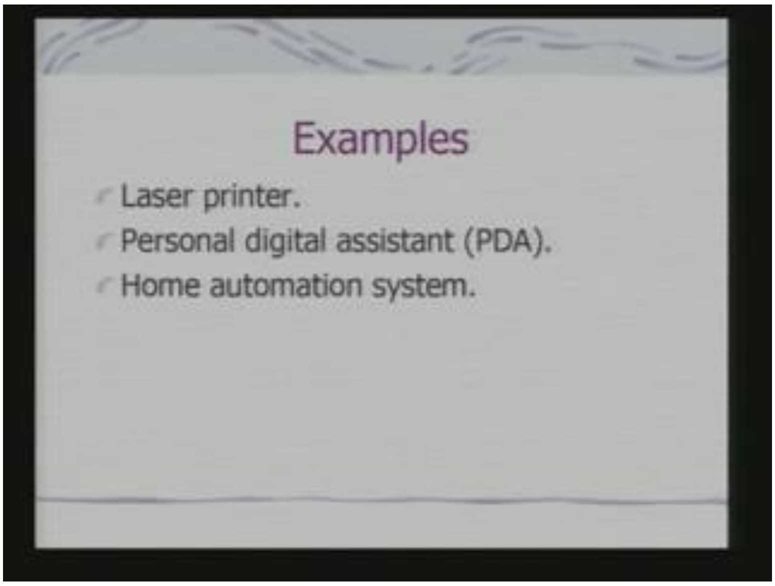


Internet-enabled embedded system

- Internet-enabled embedded system: any embedded system that includes an Internet interface (e.g., refrigerator).
- Internet appliance: embedded system designed for a particular Internet task (e.g. email).

This class of devices also known as internet enabled embedded systems and any embedded system that are includes in the internet interface you have a refrigerator and on the refrigerator you can set the temperature over the internet. So, you get need to have an our home server a theme home server you can have internet appliances which can be a email device. In fact, a there are email devices we just stand alone email devices and in fact there are devices which has got pane interface. So, stand alone email device the pane interface instead of typing in you can actually write letters and send it why mean. So, that becomes what effectively implementation of on top of TCP IP your mail server. There are other examples like laser printer, personal digital assistant, home automation system refrigerator.

(Refer Slide Time: 42:06)

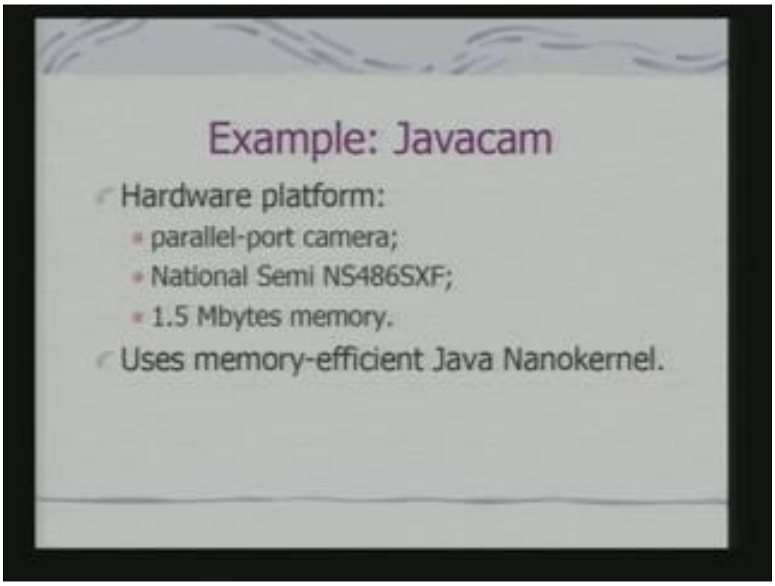


Examples

- Laser printer.
- Personal digital assistant (PDA).
- Home automation system.

An example of that so, you can have geezer connected why internet you can have your micro connected why internet and you can control everything before when you reach home you can set the temperature on the geezer why you trying. So, that the basic model that being talked about in this context let us take an example a java came that is the remote visualization in fact today.

(Refer Slide Time: 42:31)

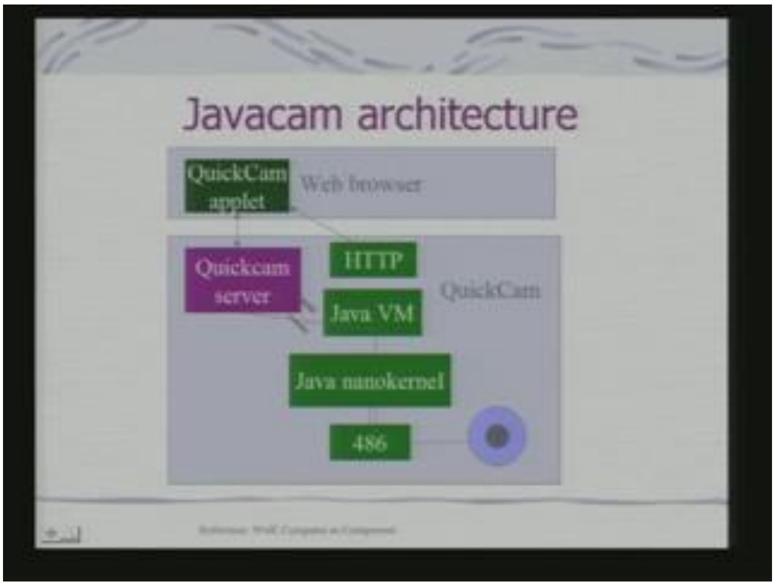


Example: Javacam

- Hardware platform:
  - parallel-port camera;
  - National Semi NS486SXF;
  - 1.5 Mbytes memory.
- Uses memory-efficient Java Nanokernel.

You can get more sophisticated system you get cameras which you control it can do a pan tilled control you can have over the internet. This is a very simple straight forward implementation around a processor which is more like a 486 like a classical 486 processor which can support about 1.5 mega bytes of memory. And it has got a parallel port interface and what it uses? Uses a memory efficient you say Java nanokernel which is something like your java KVN, Java virtual machine which your intent for your small handle devices.

(Refer Slide Time: 43:16)



Javacam architecture

QuickCam applet

Web browser

Quickcam server

HTTP

Java VM

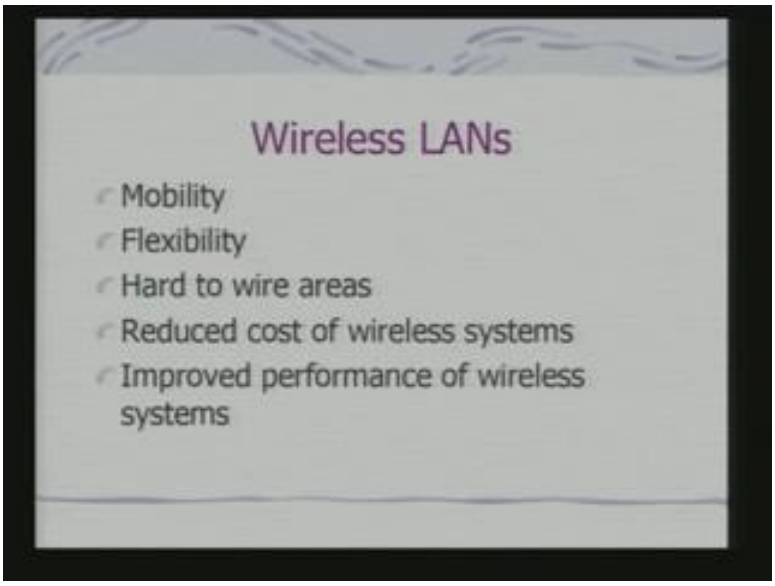
QuickCam

Java nanokernel

486

So, effectively what you have this is your camera and you implement a server a quickcam server, quickcam server on top of your java virtual machine and at the web browser you can have a applet. So, you download that applet applet establishes connection the quickcam server and you basically get the images downloaded. And see what is happening from stand alone camera please keep in mind that this is not an web cam in classical sense where you connect the web cam to a PC this a standalone java camera. So, effectively the HTTP server is implemented on top of this simple 486. So, you put it anywhere you do not need a computer just plug it on to a TCP IP socket and you can do a communication and a pictures when if you have the wireless Ethernet. Then this can be an wireless camera in fact, commercially such wireless cameras right you can do pan till control are available to them.

(Refer Slide Time: 44:21)

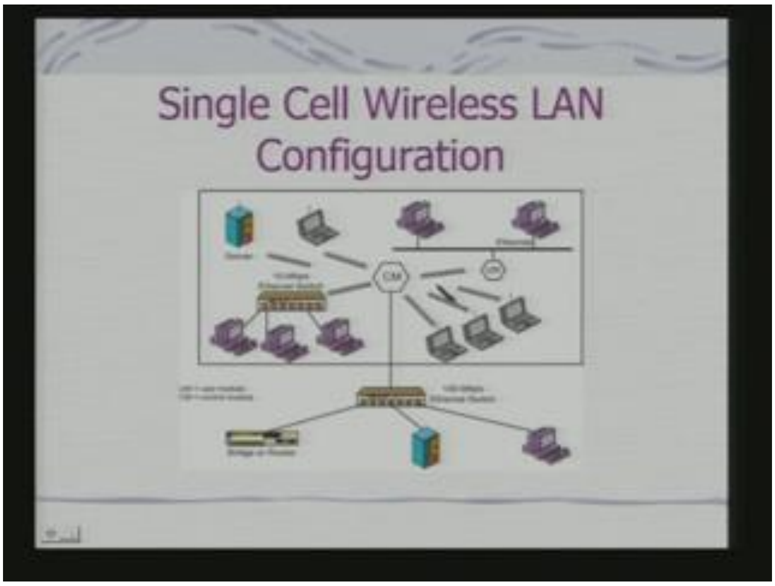


Wireless LANs

- Mobility
- Flexibility
- Hard to wire areas
- Reduced cost of wireless systems
- Improved performance of wireless systems

So, this texts towards called wireless lines. So, wireless lines are; obviously, enabled your mobility flexibility and this is expect to be used where the wiring is difficult to be done.

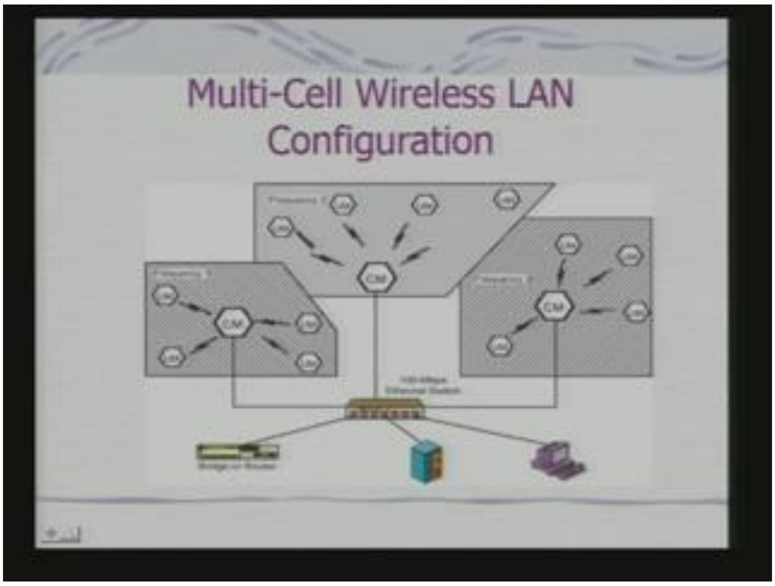
(Refer Slide Time: 44:37)



Single Cell Wireless LAN Configuration

And the basic configuration you look at is a we see as a single cell wireless lines. So, the basic idea is that you have the Ethernet; you have the Ethernet connectivity this is your basic backbone and this is your Ethernet switch and you can have all this systems connected via wireless link. So, you have got a cell, a single cell and this single cell wireless link which is connected to your 100 Mbps Ethernet switch and other devices are connecting to this single cell .This can be from a switch or from any of this stand alone systems.

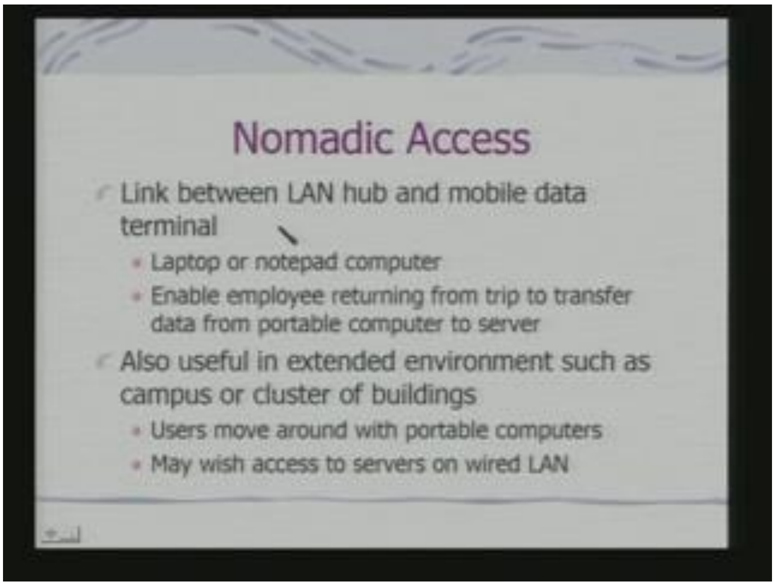
(Refer Slide Time: 45:22)



Multi-Cell Wireless LAN Configuration

They can be also multi cell configurations. So, here you have got multiple cells and you have got systems connected via this multiple cells. And each of the cells communicate using may be its own frequency and then each of this cells connected to the backbone Ethernet switch. And so, that provides connectivity of these devices to your basic network. This is a basic conceptual model of the wireless LAN.

(Refer Slide Time: 45:51)

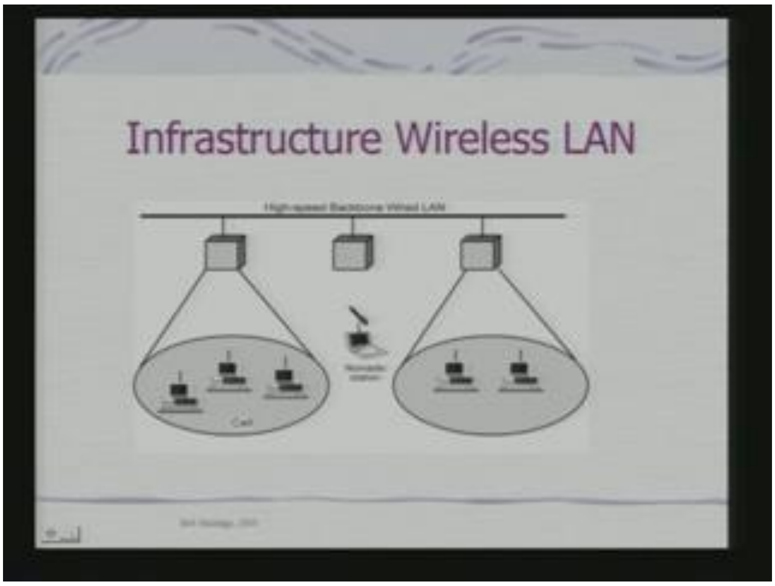


Nomadic Access

- Link between LAN hub and mobile data terminal
  - Laptop or notepad computer
  - Enable employee returning from trip to transfer data from portable computer to server
- Also useful in extended environment such as campus or cluster of buildings
  - Users move around with portable computers
  - May wish access to servers on wired LAN

This wireless LAN provides what we called nomadic access link between LAN hub and mobile data terminals you can move around with your laptop or notepad. Also useful in extended environment such as campus or cluster of buildings users move around with portable computers and may wish access to servers on wired LAN. In fact, we have such networks in this institute itself also today you will find the ear puts and other becoming this kind of wireless LANs enables. So, you get nomadic access using your laptops or even your pampers.

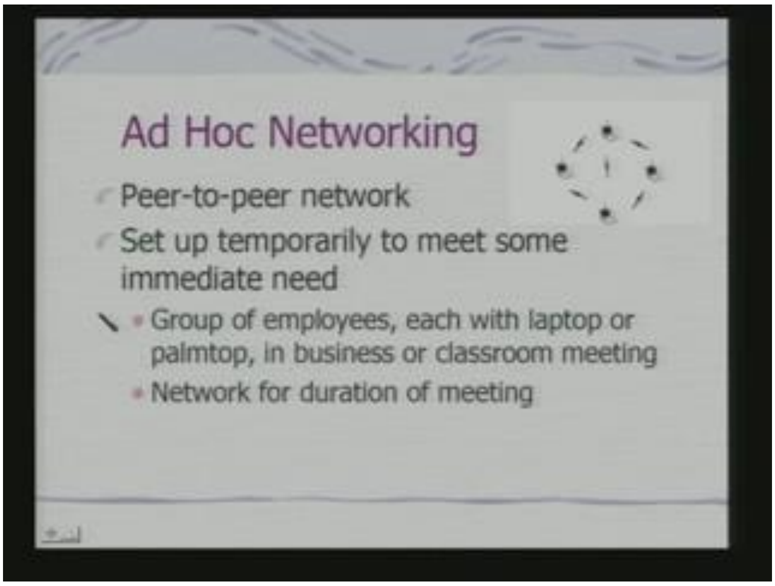
(Refer Slide Time: 46:30)



Infrastructure Wireless LAN

So, basic infrastructure wireless LAN is conceptually this you got a high speed backbone wired line. And these are the cells and you have got the basic nomadic stations you can move from one cell to another cell. And when you are at any of the cells you can access all the servers which are at the connected to the infrastructure backbone.

(Refer Slide Time: 46:48)

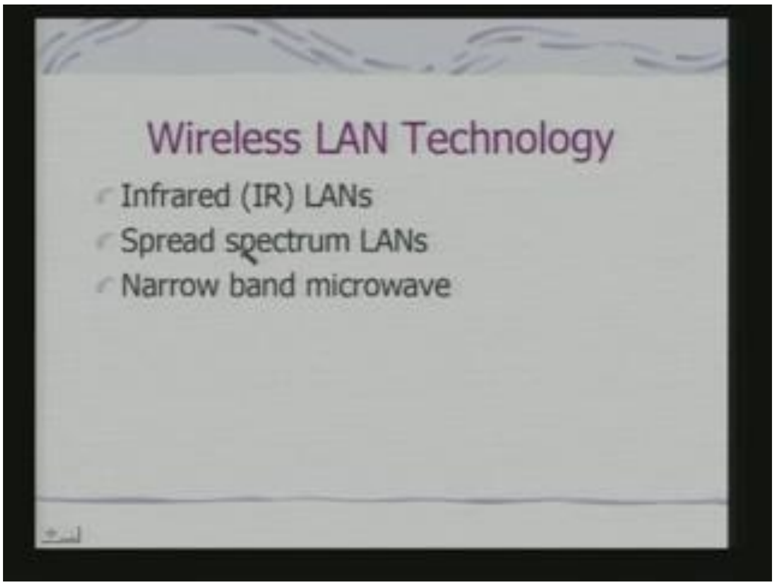


Ad Hoc Networking

- Peer-to-peer network
- Set up temporarily to meet some immediate need
  - Group of employees, each with laptop or palmtop, in business or classroom meeting
  - Network for duration of meeting

The other aspect of this is AD HOC networking. So, in this case you do not talk about a backbone you are basically trying to set up the network among this individual stations themselves. So, it is a peer to peer network set up temporarily to meet some immediate need it can be a group of employees it can be a network for duration of a period. So, if you look at that wireless LAN that for provides a what provides for connectivity where wiring is difficult provides for connectivity in an nomadic fashion. That you can move around also provides a facility for AD HOC networking that is a set of station suddenly coming together and setting up the network on being discovered by each other. The basic technology of infrared LANs spread spectrum LANs and narrow band microwave LAN.

(Refer Slide Time: 47:41)

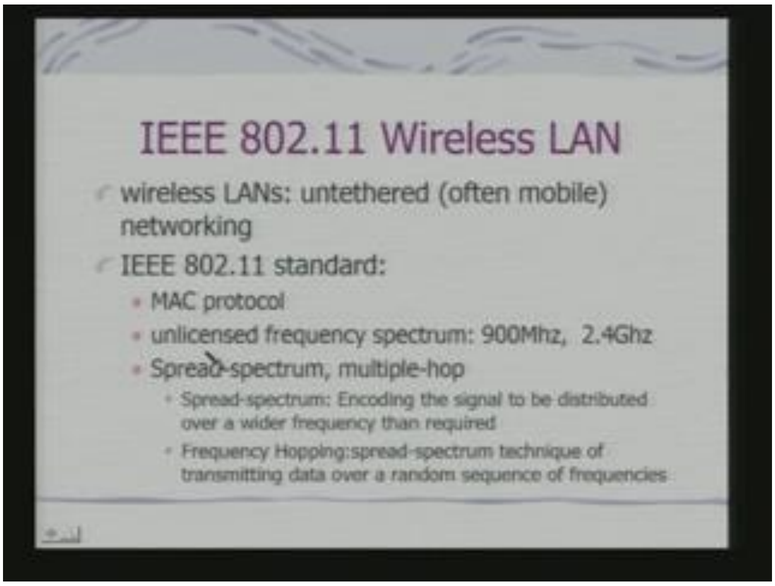


Wireless LAN Technology

- Infrared (IR) LANs
- Spread spectrum LANs
- Narrow band microwave

So, maturity of infrared LANs very simple infrared LAN we have already look that IR DA protocol can be used for their purpose and maturity of the LAN. We shall look at and we have today as spread spectrum LANs narrow band microwave are also used for this purpose.

(Refer Slide Time: 48:01)



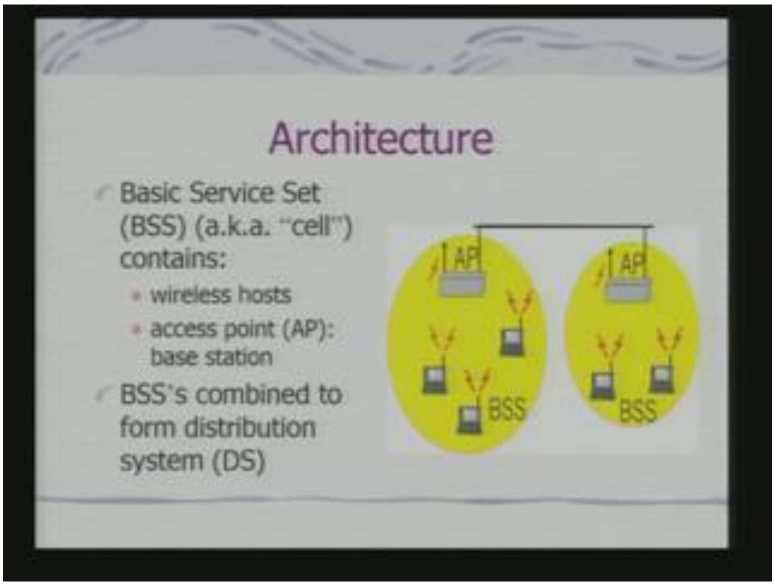
IEEE 802.11 Wireless LAN

- wireless LANs: untethered (often mobile) networking
- IEEE 802.11 standard:
  - MAC protocol
  - unlicensed frequency spectrum: 900Mhz, 2.4Ghz
  - Spread-spectrum, multiple-hop
    - Spread-spectrum: Encoding the signal to be distributed over a wider frequency than required
    - Frequency Hopping:spread-spectrum technique of transmitting data over a random sequence of frequencies

The most well known LAN technology is 802.11 in fact, whatever applications we have talked about using Ethernet today, they are getting transported on 802.11. You would like to control a device as an amplifier or an UPS ideally you like it to be on a wireless LAN. So, you are not consuming a Ethernet port you can place it anywhere in the lab and you can connect to it in a remote fashion. So, 80211 basically provides a MAC protocol and it is uses unlicensed frequency spectrum 900 mega hertz, 2.4 gigahertz, because these frequencies when you are used you do not need to take licenses. Because other frequencies are preserved and reserve for various applications like TV transmissions defense communications so on and so for these uses spread spectrum.

What is spread spectrum? The signal, the base band signal is distributed over a wider frequency than that is required or in fact typically for all this use multi hob spread spectrum; that means, we use multiple frequency slots. So, you have got a random sequence of frequency and the data is spread over this frequencies and number of frequencies and how they will be distributed that is also a random. Because that minimizes the problem of interference because this a to be used in a kind of a variety of scenario. So, there can be source of problems and noise. So, you would like to make it interference resistance that is why the spread spectrum frequency hopping is used as a physical layer specification for these kind of networks.

(Refer Slide Time: 49:55)

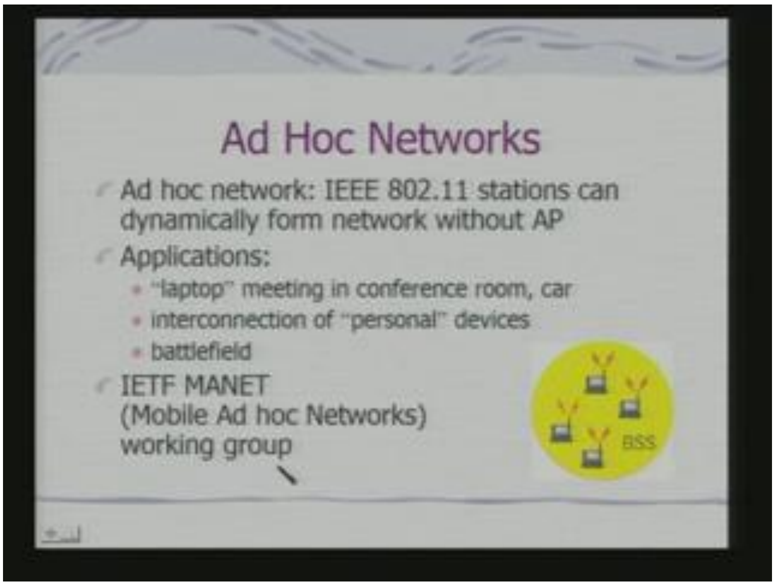


Architecture

- Basic Service Set (BSS) (a.k.a. "cell") contains:
  - wireless hosts
  - access point (AP): base station
- BSS's combined to form distribution system (DS)

So, the basic architecture is what you have a basic service set or a cell which contains wireless hosts and access points this access points can be connected to a wide line. So, basically the base model we have already shown you and BSS's combine to form what is called a distribution system.

(Refer Slide Time: 50:19)



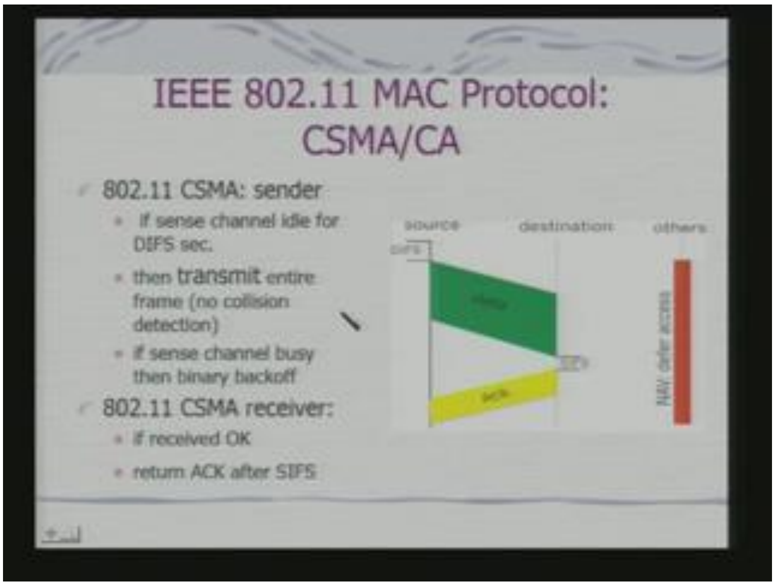
Ad Hoc Networks

- Ad hoc network: IEEE 802.11 stations can dynamically form network without AP
- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield
- IETF MANET (Mobile Ad hoc Networks) working group

.

When you have an Ad hoc network stations can then what is happening you are really not having an access point access point is more of a infrastructure network which is providing you nomadic access. So, dynamically form a network without an access point in fact, there are this IETF MANET mobile Ad hoc networks and there are this protocols which is built on top of this 802.11 to enable this kind of Ad hoc network setup.

(Refer Slide Time: 50:53)



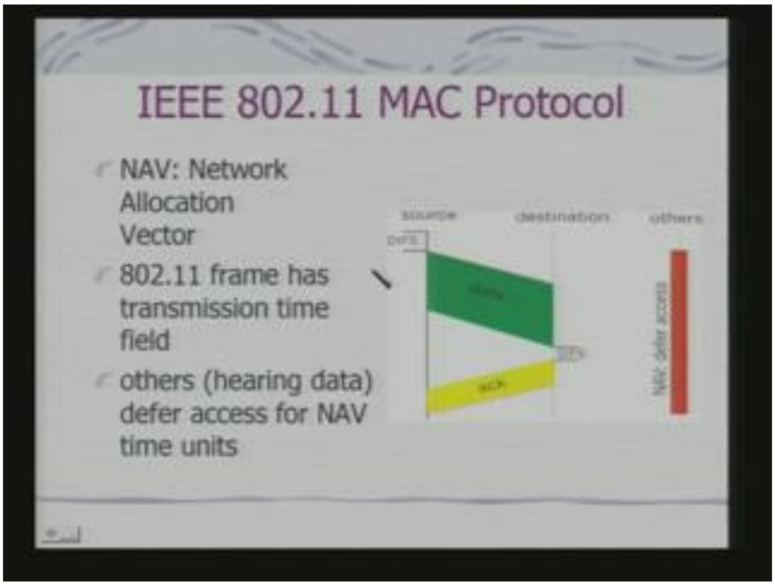
IEEE 802.11 MAC Protocol: CSMA/CA

- 802.11 CSMA: sender
  - if sense channel idle for DIFS sec.
  - then transmit entire frame (no collision detection)
  - if sense channel busy then binary backoff
- 802.11 CSMA receiver:
  - if received OK
  - return ACK after SIFS

source
destination
others
DIFS
data
SIFS
ACK
NAV: defer access

So, what is the basic MAC protocol it is CSMA CA that is a collision avoidance and not collision detection. This is basic difference if you see there are looking at variety of the MAC protocols than Ethernet now 802.11. Now, what does it do if sense channel idle some DIFS second there is some bound DIFS second then transmit entire frame, because you have collision. If the channel is sense to be busy then you do a binary back off and receiver what it does you received and return knowledge of the a certain time period which is SIFS. So, this is the very basic description of the MAC protocol not going in to the details this is the very basic description of the MAC protocol. So, effectively what we are doing is that the source after the DIFS it senses the channel if its finds a channel to be idle for about DIFS second it sends the data. Now, destination waits for SIFS second and there is no data then it sends the acknowledgement the other differ access using what is called NAV. What is your NAV?

(Refer Slide Time: 52:20)



IEEE 802.11 MAC Protocol

- NAV: Network Allocation Vector
- 802.11 frame has transmission time field
- others (hearing data) defer access for NAV time units

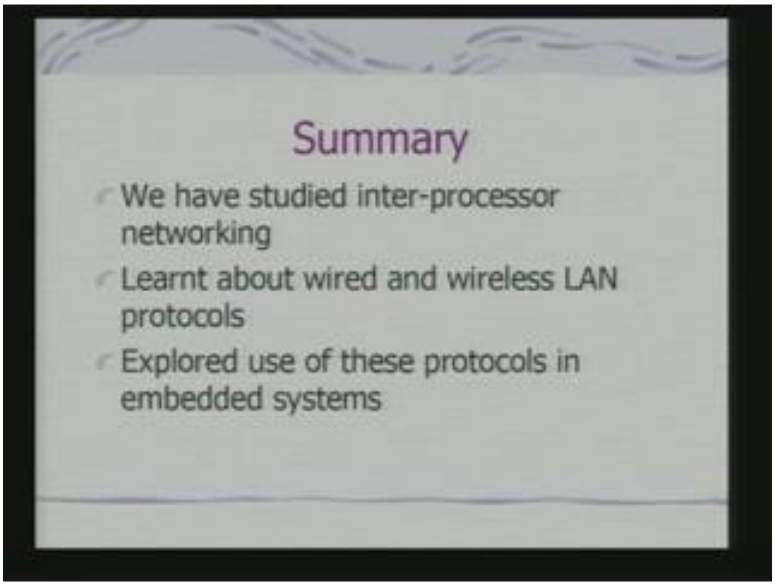
NAV is called network allocation network. So, 802.11 has transmission time field. So, there is a specific transmission time field and other what we do on hearing the data defer access for NAV time units the defer access for NAV time units. So, when there is collision if you look in to it what we are doing what we are telling as that it is not the collision detect it just sends as when there are activity on the network or not. If there is no data being transmitter and if that observation is made for a fixed time period which is your DIFS? Then only the transmitter starts sending the data. And then what it happens the receiver sends back acknowledgement after a certain time period.

Now, others what will others do others will defer that is one hearing the data differs access for a certain NAV time units. This NAV time units is called network allocation network . So, this network allocation network allocation vector is associate with the nodes and they provide for this deferring time period. So, it is not like a exponential back off. So, the back off is with regard to a NAV that is the defer time period which is specified through NAV allocation vector and 802.11 has got transmission time field. So, transmission time field also tells you that the time required when for a such a transmission is taking place. So, effectively here there is no collision detection what you have got is the collision avoidance why, because you have the collision detection. If you look in to it one very interesting feature you should know is that collision detection means you are actually using energy to transmit and then detecting the collision.

So, when it is a wireless link you would like to preserve energy. So, why would you like to transmit the data and detect the collision? So, this is the very basic motivation you can realize why this protocol should be around collision avoidance. And in fact, today you will find this kind of I already gave a example that what if you 802.11.So, on top of 802.11 you can have if I see there is an infrastructure network to an access point you can have what you can have the entire protocol built. So, your 802.11 is available on a device. So, effectively the device now becomes part of your LAN and it can be moved around if it is a basically if it is a nomadic access particularly important for your appliances.

Because really you may not like appliances to set up Ad hoc network what do you like for a appliances just like a testing equipment or a instrument or even a device like camera to be taken all around. And still have network access and preciously the basic motivation of enabling this wireless network on variety of devices and embedded devices. So, basically they implement these 802.11 Mac protocol and they implement the spread spectrum communication to meet the requirements of physical layer specification on top of that higher layers can be also implemented. And provided for so example of a camera would be what you have got even http server implemented on such a camera and that camera has got of the lower level your wireless link. So, that brings as the ends of today’s lecture.

(Refer Slide Time: 57:05)



Summary

- We have studied inter-processor networking
- Learnt about wired and wireless LAN protocols
- Explored use of these protocols in embedded systems

So, what you have studied? Today, we have studied inter processing networking. Learnt about wired and wireless LAN protocols and explored use of these protocols in variety of embedded systems if you have any questions? See the question is 802.11 doing guarantee there is a collision is not. So, there would be; obviously, collision, because there are multiple elements or multiple stations which may like to transmit that the same time. But what is important is in terms of protocol each station senses the carrier and if it is find that noting it getting transmitted then only it starts transmission. So, it is a collision avoidance. So, if it find see the basic difference is what in an normal Ethernet you actually detect a collision; that means, you sends the carrier can you send the data packet detect the there is a collision. So, the packet is what is being send and hence you should back off. So, you should jam in this case what is happening that way it is detecting there is some activity on the channel. So, it basically has to defer its activity how long it would defer that depends on NAV location. So, that is why it is a collision avoidance.