

Data Communication
Prof. A. Pal
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 34
TCP/ IP - I

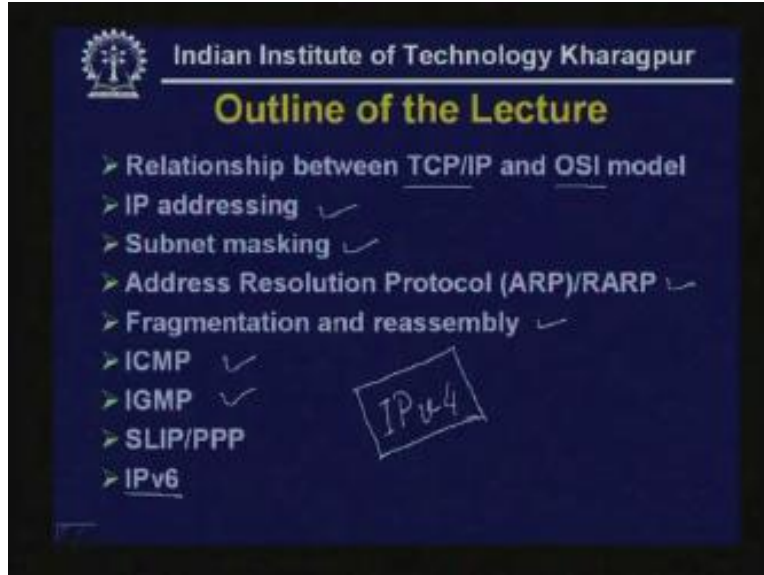
Hello and welcome to today's lecture on TCP/IP.

(Refer Slide Time: 01:00)



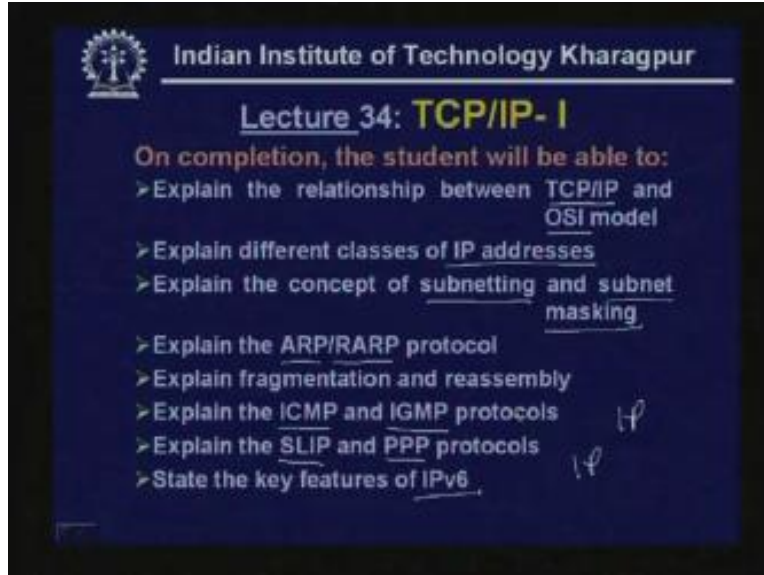
We shall continue our discussion on internet and internetworking. Here is the outline of today's talk.

(Refer Slide Time: 02: 38)



First we shall discuss about the relationship between TCP/IP and the popular OSI model, then we shall discuss about various issues related to internetworking. For example, particularly IP addressing then in that context subnet masking and also the address resolution protocol ARP and RARP and then we shall consider fragmentation and reassembly in IP. Also, there are several companion protocols like ICMP and IGMP which are related to internetworking and used along with the internet protocol IP protocol which we shall discuss about. Then we shall discuss about two protocols SLIP and PPP which are used by home users for connecting their computers to the internet service provider using IP. And although at present IPv6 is commonly used but it has got a number of limitations which can be overcome by the use of IPv6 but it is yet to become popular. In this lecture I shall just give an overview of IPv6.

(Refer Slide Time: 03:50)



Indian Institute of Technology Kharagpur

Lecture 34: TCP/IP- I


On completion, the student will be able to:

- Explain the relationship between TCP/IP and OSI model
- Explain different classes of IP addresses
- Explain the concept of subnetting and subnet masking
- Explain the ARP/RARP protocol
- Explain fragmentation and reassembly
- Explain the ICMP and IGMP protocols
- Explain the SLIP and PPP protocols
- State the key features of IPv6

And on completion the students will be able to explain the relationship between TCP/IP and the OSI model, they will be able to explain the different classes of IP addresses and they will be able to explain the concept of subnetting and subnet masking and they will be able to explain Address Resolution Protocol and Reverse Address Resolution Protocol ARP and RARP. They will be able to explain fragmentation and reassembly that is necessary while doing internetworking and they will be able to explain ICMP and IGMP protocols and how they are used in congestion with IP protocol.

Then they will be able to explain the SLIP and PPP protocols and they will be able to explain how they are used for internet access by using IP. They will also be able to state the key features of IPv6. **As I mentioned in the last lecture** you will require a combination of hardware and software for internetworking.

(Refer Slide Time: 04:36)

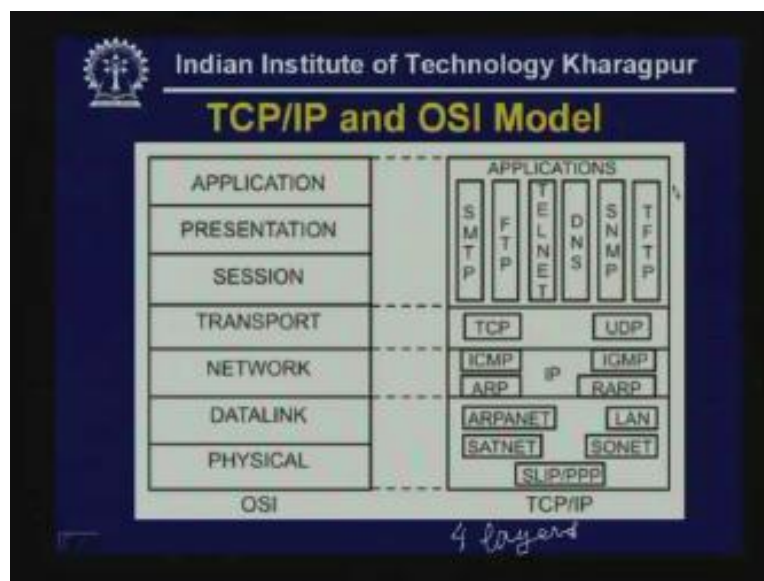
 Indian Institute of Technology Kharagpur

Introduction

- **Hardware:**
 - Repeaters/Hubs:** Physical Relay or Layer-1 Relay
 - Bridge:** Data Link Relay or Layer-2 Relay
 - Router:** Network Relay or Layer-3 Relay
 - Gateway:** Layer-7 Relay – works above network layer, such as application layer
- **Software:**
 - TCP/IP:** Acts as a glue to link different types of LAN and WAN to provide Internet, a single integrated network for seamless communication

And in the last lecture we have discussed about various hardware like; repeaters and hubs, bridge, routers, gateways and so on, these are the different hardware that will require internetworking. In today's lecture we shall discuss about the software particularly one of the two software that is a protocol which is known as TCP/IP. And as I mentioned this acts as glue to link different types of LAN and wan to provide internet, a single integrated network for seamless communication. So TCP/IP is essentially a software, it's a set of protocols. We shall see the relationship between TCP/IP and OSI model.

(Refer Slide Time: 07:14)



Although the TCP/IP was developed much earlier than OSI model always we try to map a particular protocol with the OSI model. Let us see what is the relationship between the TCP/IP and the OSI model.

As you can see the TCP/IP has got only four layers in contrast to several layers of OSI model. For example, for the lowest layer any specific thing can be used here which is a combination of physical and data link layer and one is free to use any type of network like Arpanet, Local Area Network LAN, satellite network, sonnet or they can use simple serial links like SLIP and PPP which provides the physical and the data link layer. So, the physical and data link layer forms one layer in TCP/IP.

Then there is a layer which is corresponding to network layer which is IP Internet Protocol and it has got several other companion protocols like ARP, RARP, ICMP and IGMP **which we shall discuss in this lecture** then there is a protocol TCP or UDP which can be considered as transport layer protocol and finally the session, presentation and application all are not present in the TCP/IP there exists a single application layer which provides a number of protocols for various applications like SMPT for transfer of mail, ftp for transfer of files, telnet for sending mails and SMPT which is used for monitoring network, SNMP Simple Network Management Protocol is used for management purpose and TFTP so these are the various application layer protocols which we shall discuss in the next lecture.

(Refer Slide Time: 08:27)

Indian Institute of Technology Kharagpur

Internetworking Issues

- Addressing
- Fragmentation and Re-assembly
- Routing
- Error detection/Error Control
- Congestion control and QoS
- Security
- Packetizing
- Flow Control
- Naming

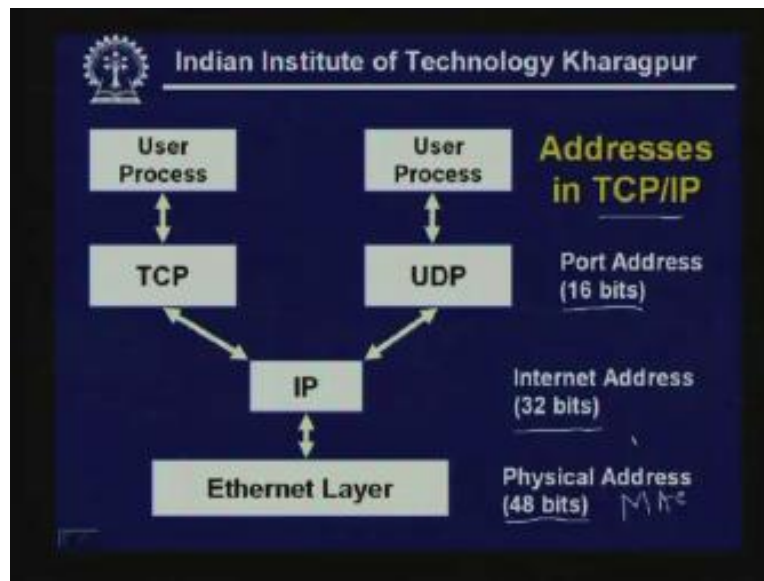
➤ IP provides unreliable, connectionless **best-effort** datagram delivery service

➤ TCP provides reliable, efficient and cost-effective end-to-end delivery of data

Then as I mentioned there are a number of internetworking issues like addressing, packetizing, fragmentation and reassembly, routing, flow control, error detection and error control, congestion and quality control, security and naming and particularly all these functionalities are provided by two protocols one is IP another is TCP/IP and that's why they are paired together to form TCP/IP and particularly IP provides a unreliable connectionless best effort datagram delivery service. So, if you want reliability and then

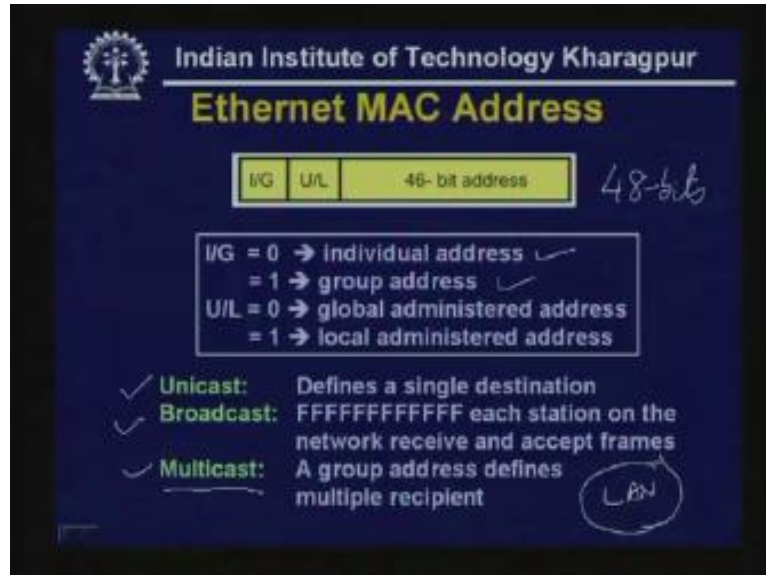
you have to use TCP and TCP provides reliable, efficient and cost effective end-to-end delivery of data so these two together gives you host to host communication in a reliable manner. And particularly the IP will provide these functionalities like addressing, packetizing, fragmentation and reassembly and routing. So these are the functionalities which will be provided by IP protocol which we shall discuss in this lecture.

(Refer Slide Time: 09:43)



First let us focus on addressing. In TCP/IP you will encounter three different types of addresses. As you know if you want to send a letter you have to write the address of the destination and then put the letter in the letter box. Similarly, if you want to send any information you have to know the address of the destination where you want to deliver. In TCP/IP you will encounter three different types of addresses. We have already seen the physical layer address which is also known as MAC address medium access control address, for example, for Ethernet it is of 48-bits and then IP provides you internet address or IP address in short which is 32-bits, on the other hand, the TCP will require some addressing that is 16-bit address and it is known as port address. So you will encounter three different types of addresses in TCP/IP. we have already discussed about the physical address or MAC address.

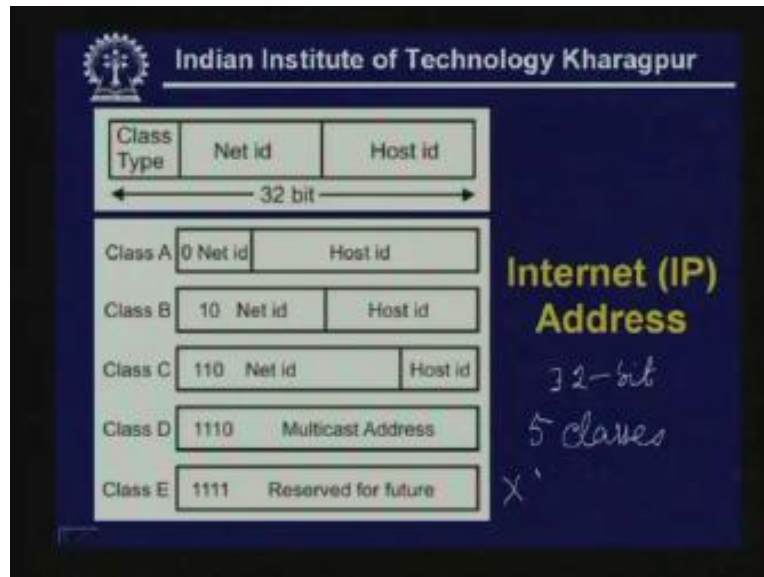
(Refer Slide Time: 11:06)



For example, the physical address comprises of 48-bits and here is the format of that. So, apart from 46-bit addresses the first two bits decides whether it is for individual address or it is group address that means you can use for unicast whenever you have to use the individual address and whenever you are sending to a group of people then you have to use the multicast address and there is another bit u or u by l which gives you the global or universal administrated address or it can be a local administered address. So when it is (i) it corresponds to l and when it is 0 it is corresponds to u.

So we see that whenever broadcasting has to be done all the bits have to be one, each station on the network receives and accepts **the frame**. So, with the help of this MAC address you can do unicasting that means one to one, broadcasting one to all or multicasting which is one to a group of people so you can have three types of delivery by using MAC address over a single network or LAN.

(Refer Slide Time: 13:19)



However, we are interested in internetworking and obviously we would like to communicate between a number of LANs or LAN, WAN and so on so in such a case we have to use internet address. An internet address as I mentioned comprises of 32-bit. This 32-bit has got three different fields; first one is known as provides the class type. Actually the addresses are divided in five classes A B C D E which is specified by first few bits.

For example if the first bit is 0 then it's a class A address, if the first bit is 1 and the second bit is 0 then it is class B address, if the first bit and the second bit both are one and the third bit is zero then it is class C address and if the first three bit are one and fourth bit is zero then it is class D address and if all the first four bits are one then it is class E address. So apart from this class the remaining part is divided into two fields; one is known as network ID, another is host ID. And as you can see (Refer Slide Time: 12:21) in different classes particularly A, B and C, the size of net ID and host ID are different.

In case of class A the net ID comprises only seven bits and host ID compresses 24-bits. So here there are 8-bit of net ID including zero the most significant bit and the host ID comprises 24-bits.

On the other hand, class B you have got 1 0 followed by 14 bits of net ID and you have got 16 bit of host ID. On the other hand, in class C the first 3 bits are 1 1 0 and remaining 21 bits are net ID and 8-bits are host ID. And 1 1 0 and remaining bits here you have got (Refer Slide Time: 13:08) multicast address that means remaining 28-bits provides you the multicast address and class C is 1 1 1 1 this is reserved for user and not presently in use.

(Refer Slide Time: 16:15)

Indian Institute of Technology Kharagpur

Dotted Decimal Notation

Dotted Decimal Notation

11000000 00010010 00001011 10001111

192 . 18 . 11 . 143

Binary
4 octets

Range of Host Addresses

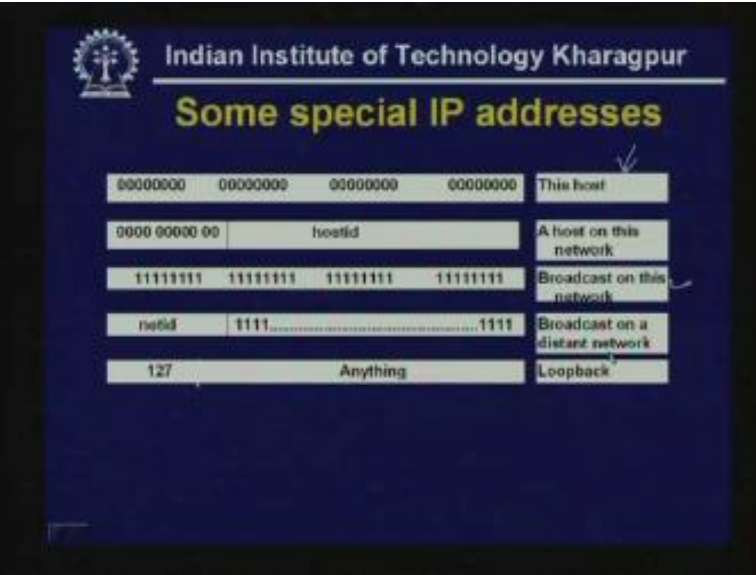
Class	Range
Class A	1.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 233.255.255.255
Class D	244.0.0.0 to 239.255.255.255
Class E	240.0.0.0 to 247.255.255.255

234
0-255
8-bit

There are two ways you can write an IP address. One is in binary form where you have got sequence of ones and zeros. For convenience as you can see it has been divided in four octets each of 8-bits. Then another notation which is commonly used is known as dotted decimal notation. In dotted decimal notation as you can see each octets have 8-bits these 8-bits are represented in decimal form instead of binary. So the range of number that can be in each field is very strong 0 to 255 which can be represented by 8-bit. So by using four octets with the help of their decimals values each separated by dots is known as dotted decimal notation.

By using this dotted decimal notation the range of host addresses for different classes are given here. For example, in case of class 1 it will be found 1.0.0.0 to 127.255.255.255. In case of class B it varies from 128.0.0.0 to 191.255.255.255. So you see whether a address corresponds to class A or class B can be found out by looking at the first field of the dotted decimal notation or first decimal number. If it is in between 128 to 199 it belongs to class B, if it is found within 1 to 127 it is class A and then class C from 192 to 233 then class D is from 234 to 239 then class E is 240 to 247. Hence, this is the range of numbers that is being used. On the other hand, it is from 240 to 247 this is class E of course it is not in use.

(Refer Slide Time: 17:29)

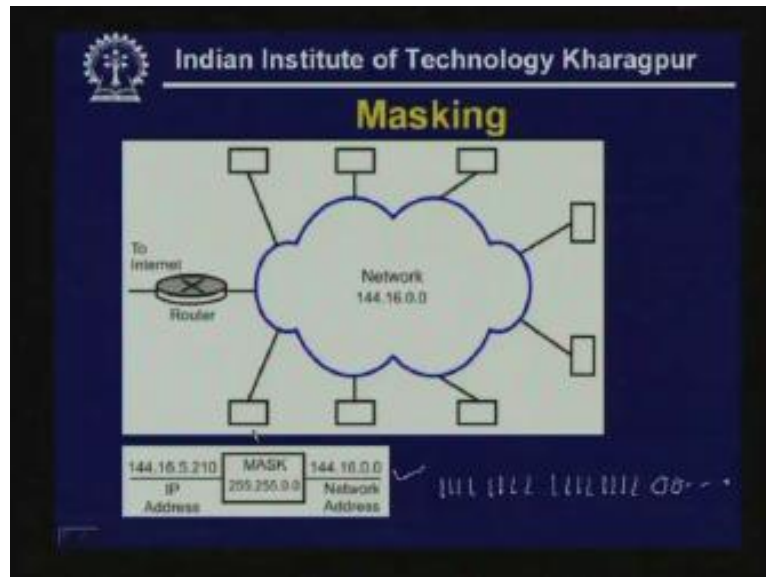


Indian Institute of Technology Kharagpur	
Some special IP addresses	
00000000 00000000 00000000 00000000	This host
0000 00000 00 hostid	A host on this network
11111111 11111111 11111111 11111111	Broadcast on this network
netid 1111...1111	Broadcast on a distant network
127 Anything	Loopback

Now, you may be wondering why 0 is not here in class A. So, for that purpose there are some special IP addresses apart from those general cases. For example, if the address is all 0 it means this host is commonly used at the time of **booting** then if the address is sent to a host on this network but not to a different network then first ten bits can be 0 and the remaining can be the address of the host or host ID. Or if it is a broadcast on this network you are sending to all the computers or systems on the network then it can be all 1.

So you have to exclude all zeros and all ones whenever you count the number of address possible. On the other hand, broadcast on a distant network then you will give the network ID by using ten bits and remaining fields can be all 1. You are trying to broadcast to a distant network and net ID can be ten bits and whenever you want to do loopback and you want to receive on same host then it can be 127 and this field can be anything remaining bits can be **added**. These are some of the special IP addresses.

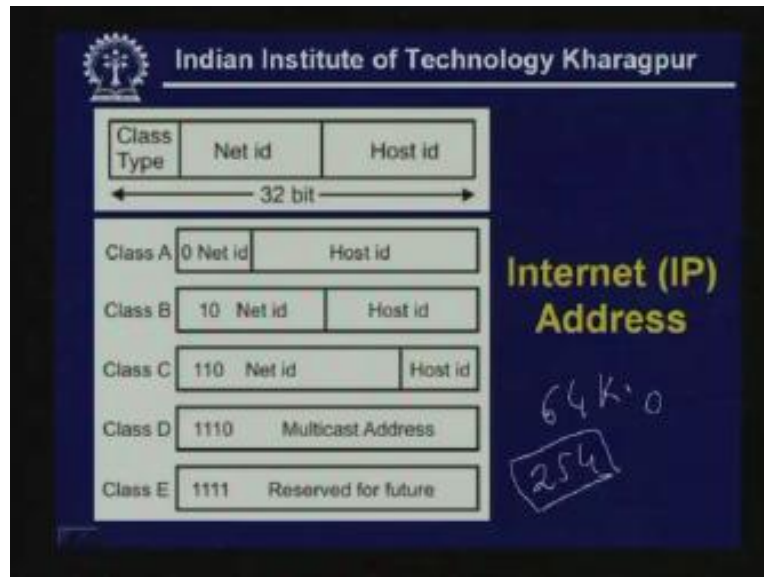
(Refer Slide Time: 19:00)



Now you may be asking whenever an IP address is being used how a particular network receives a particular packet which is made for that network, this is done with the help of a technique known as masking.

As you can see this is the IP address (Refer Slide Time: 17:48) and within this router, the router has to filter up the output packet corresponding to this network so it does not bother about the host ID it only bothers about the net ID. So what is being done is some kind of hand operation is performed with the net ID part that means the mask is 255.255.0.0 that means all bits are 1 so 11111111111111 then remaining bits are 0, this is mask, and this is 144.16.5.210 to filter out the net ID so here is the 144.16.0 then this is being looped into the table of the router and if there is a matching then it receives it otherwise it is not allowed to pass through the router. So, if this matches then it sends it to this network.

(Refer Slide Time: 20:35)



It has been found that this particular technique uses essentially two hierarchical levels of addressing by using net ID and host ID so it uses two levels of hierarchy and unfortunately the number of host and network varies as you choose a particular class.

For example, if class A addressing is used only 8-bit is used for net ID and the remaining is host ID. So, if class A address is taken then if the number of host in a particular network is small then a large number of addresses are wasted. On the other hand, if class B address is taken a good number of addresses is wasted because usually in a single network you don't have 64 k of addresses so with the help of 16 bit you can have 64 k addresses but you may not have 64k addresses. On the other hand, if you take class C address the total number of address available is only 254 excluding that broadcast and all 0 and all 1 so you can have only 256 addresses. So, to begin with if you start with c after sometime it may not be adequate so you have to apply for another address.

(Refer Slide Time: 20:56)

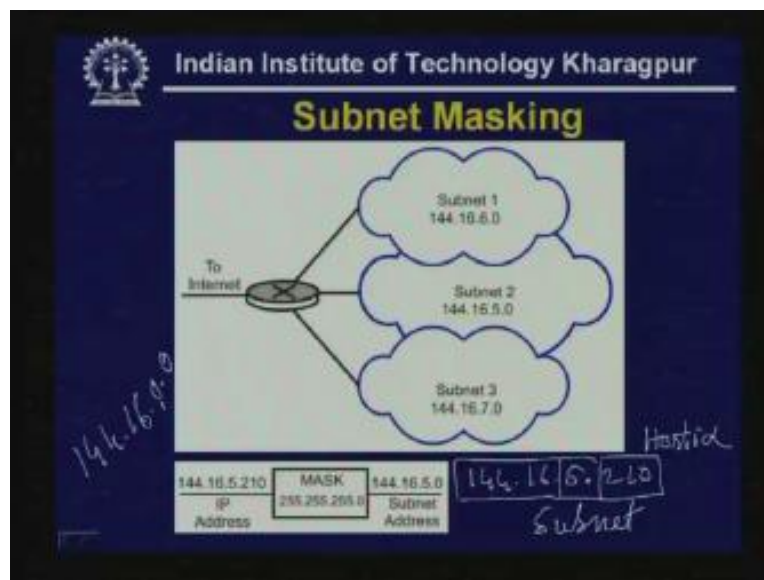
Indian Institute of Technology Kharagpur

Subnetting

- In classical IP addressing the address is divided into two fields: **Netid** and **Hostid**
- This provides IP addresses **two levels** of hierarchy
- Very large number of class A addresses are **wasted**
- Many class B addresses are wasted
- The number of addresses in class C is inadequate in most of the situations
- To overcome this problem, an additional intermediate level of hierarchy in the form of **Subnetting** is used

This problem can be avoided by introducing an intermediate level of hierarchy in the form of subnetting. So what is being done is in subnetting the addresses the addresses divided into three parts; the net ID, subnet ID and the host ID as it is shown here.

(Refer Slide Time: 23:20)

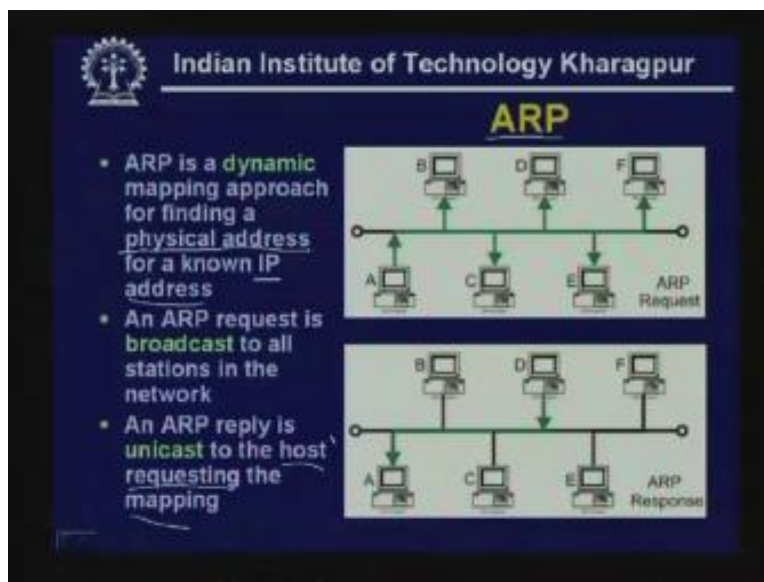


So suppose in this particular address say 144.16.5.210 obviously it is clear that we are using class B addressing so the network address is represented by 144.16 and 0.0 this is the network address. However, within the network 8-bit is used as subnet address and remaining 8-bit is used as the host ID, identification of the host. So by doing this what you can do, to the external world is the same network as you can see here (Refer Slide

Time: 21:52) but locally you can have a number of subnets which can be done by using a special type of masking known as subnet masking. So, instead of sixteen ones you will use twenty four ones in this particular case so that as an address comes by ending with twenty four ones you get an address like 144.16.5.0 and each is sent to different subnets.

As you can see this router can send to all the host corresponding to subnet 144.16.6.0 with the help of subnet mask of 255.255.255.255.0 that means you are using 24 bit ones in the first part. In this way you can do subnet masking and you can have a number of subnets within a single network so to the outside world essentially it is a network of 144.16.0.0 but within the network you can have different subnets. For example, different departments within IIT can have a separate subnet, on the other hand, to the outside of the world it can be a single network having the address 144.16. This is the concept of subnet masking that is being used.

(Refer Slide Time: 25:26)

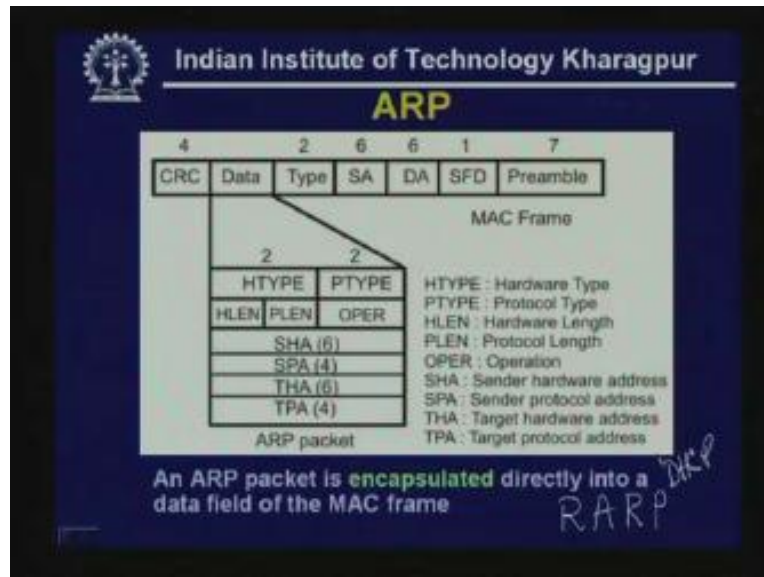


Now comes the question of another protocol known as address resolution protocol. As you know, for delivering a packet to a host or a router within a network in the data link layer it is necessary to know the network MAC address or physical address as we can call it. So, if a particular host or a router does not know the physical address of the destination device then how it will know that is provided with the help of ARP address resolution protocol in a dynamic manner. So it does dynamic mapping approach for finding the physical address for knowing the IP address. That means the IP address of the destination is known but for delivering the packet it is necessary to use the physical address so physical address can be obtained by using this ARP protocol.

This is done in two steps. ARP request is a broadcast so the user sends ARP request so the ARP user sends a broadcast message to all the stations. As you can see suppose A is the host which is looking for the destination physical address so it sends a packet that means ARP sends a packet on this network and it is a broadcast message. So it is received

by all the host in that network then the host which is actually requesting the mapping that means the concerned host which matches with the destination IP address sends the reply, here in this case it is unicast that means one to one so it sends a packet to host A providing the physical address.

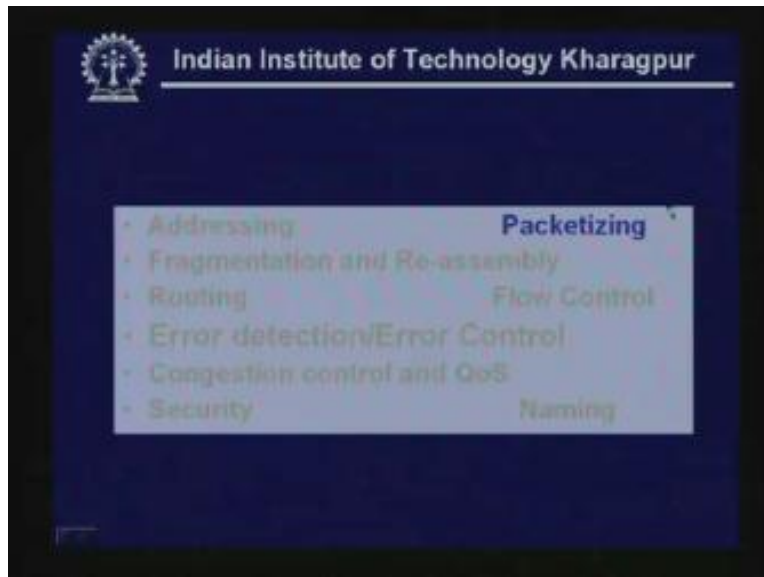
(Refer Slide Time: 27:21)



For that purpose some kind of special type of frame is being used. So this is the ARP packet and ARP packet is encapsulated in a MAC frame. As you can see (Refer Slide Time: 25:37) this is the typical Ethernet frame preamble, then Synchronization Frame Detection SFD, then data, then destination address, source address this are all 48-bit addresses then in this case the type specifies that it is a ARP protocol and here as you can see there is field corresponding to the hardware address that is the physical address as well as the protocol address that is your IP address so six bytes and four bytes and target hardware address and target protocol address.

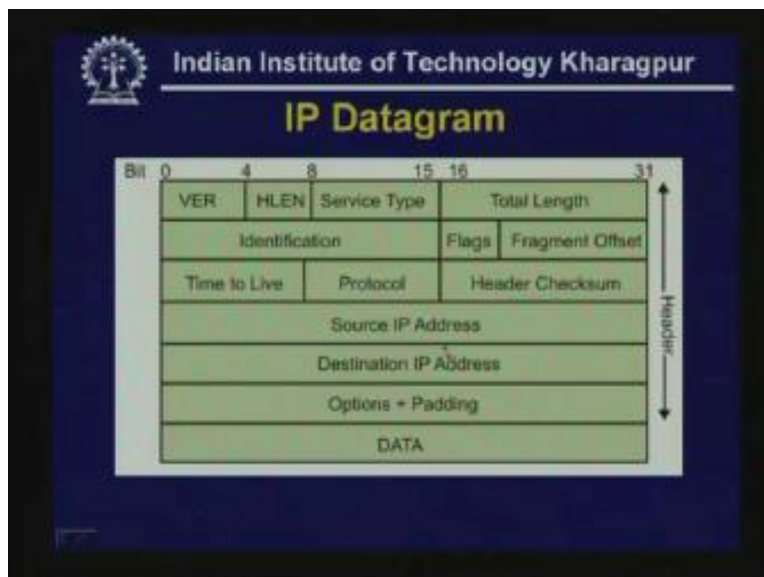
So initially target hardware address is given all 0 and whenever it is returned the proper target address is provided. This is how with the help of ARP a particular station can know about the physical address if a station knows about the IP address. The reverse one operation is being performed by RARP. In case of RARP the physical address is known but IP address is not known. For example, this can happen in a diskless station, at the time of booting it should know the IP address although it knows its physical address. Therefore, to know the IP address it sends a request to the server and server sends a reply with the IP address. But presently RARP is gradually getting obsolete and it is being replaced by another protocol which is known as DHCP, we shall discuss about it later on.

(Refer Slide Time: 27:32)

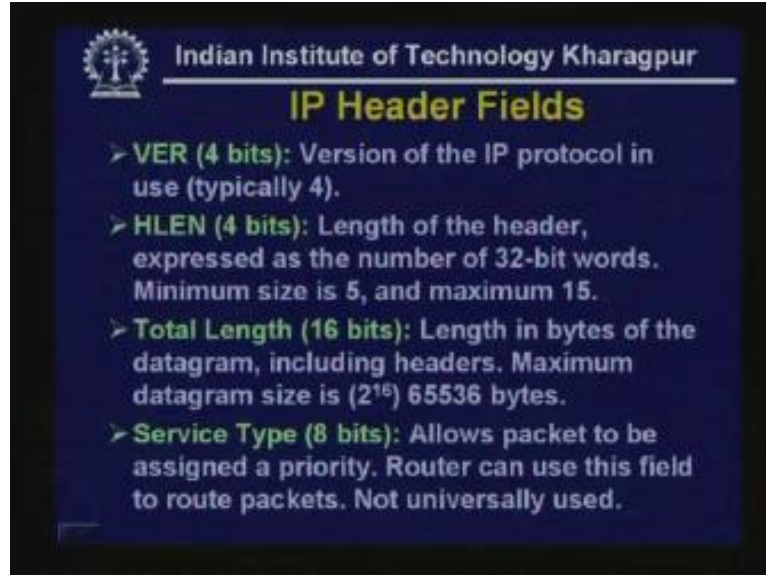


Now let us consider the second issue that is packetizing. Packetizing means the data has to be sent in a format of frame and the packet is used by the internet protocol to frame a datagram **or frame**. So the datagram includes the header comprising a number of fields and apart from data it adds a header. The header has a number of fields as explained here.

(Refer Slide Time: 28:00)




(Refer Slide Time: 29:20)



For example, it has got the version field which is represented by four bits. For example, presently the IP protocol is IPv4 that is being used. Thus, if we use IPv6 then that has to be mentioned in the version field. Then header length 4-bit says about the length of the header expressed as the number of 32-bit words so minimum size is 5 and maximum is 15. So the header length is specified with the help of this field then you have got the total length of the frame length in bytes of the datagram including header, maximum datagram size so you can see the IP frame or datagram can be of 64536 bytes which is of the maximum size of the datagram. The service type field actually allows packets to be assigned a priority so router can use this field to route packets but however it is not universally used.

(Refer Slide Time: 30:08)


 Indian Institute of Technology Kharagpur

IP Header Fields

- **Time to Live (8 bits):** Prevents a packet from traveling forever in a loop. Senders sets a value, that is decremented at each hop. If it reaches zero, packet is discarded.
- **Protocol:** Defines the higher level protocol that uses the service of the IP layer
- **Source IP address (32 bits):** Internet address of the sender.
- **Destination IP address (32 bits):** Internet address of the destination.
- **Identification, Flags, Fragment Offset:** Used for handling fragmentation.

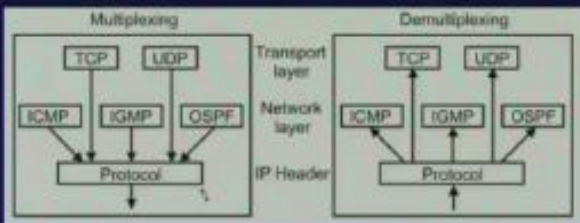
Then there are other fields such as time to live. It prevents a packet from traveling forever in a loop, the senders sets a value that is decremented at each hop. If it reaches zero, packet is discarded. We have already discussed about flooding and flooding can be restricted by controlling the number of hops. Hence, this field can be used for that purpose. Then the protocol field is there which defines the higher level protocol that uses the services of the IP layer. So the packets will be coming from different higher level protocols so it has to do some kind of multiplexing with the help of this protocol field as shown here.

(Refer Slide Time: 30:53)

 Indian Institute of Technology Kharagpur

Multiplexing and Demultiplexing

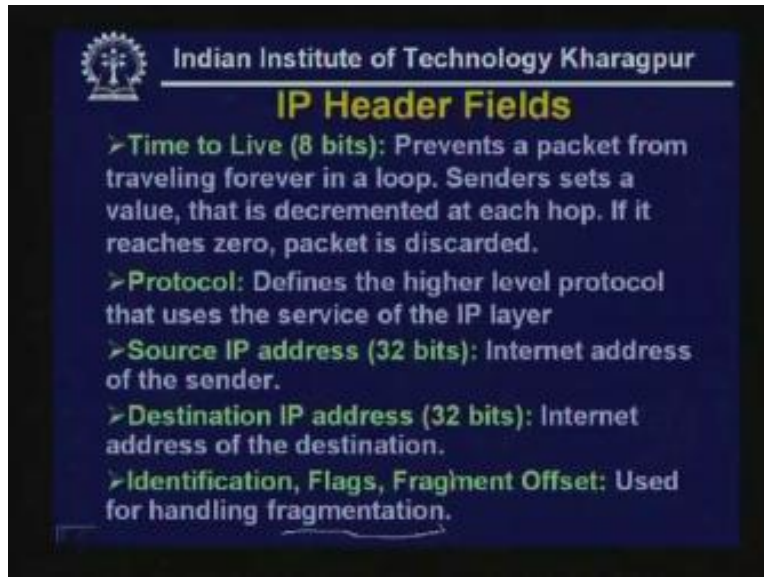
- IP datagram can encapsulate data from several higher level protocols
- **Protocol field** specifies the final destination protocol to which IP datagram to be delivered



The diagram illustrates the process of multiplexing and demultiplexing in the IP layer. It is divided into two main sections: Multiplexing and Demultiplexing. In the Multiplexing section, data from various higher-level protocols (TCP, UDP, ICMP, IGMP, OSPF) is sent to a 'Protocol' box, which then encapsulates it into an 'IP Header'. In the Demultiplexing section, the 'IP Header' is processed by the 'Protocol' box, which then sends the data back to the respective higher-level protocols (TCP, UDP, ICMP, IGMP, OSPF). The layers involved are the Transport layer (TCP, UDP) and the Network layer (ICMP, IGMP, OSPF).

The protocol field allows some kind of multiplexing. The packets are coming from a number of upper layers like ICMP TCP IGMP UDP OSPF so these are the different higher level protocols and it receives a packet and sends it to the next lower level. Obviously whenever it reaches the destination you have to do the demultiplexing. By looking at the protocol field it again delivers it to the proper protocol like ICMP or TDP TCP or IGMP or UDP or OSPF. So, for the purpose of the multiplexing and demultiplexing this protocol field is necessary.

(Refer Slide Time: 31:10)



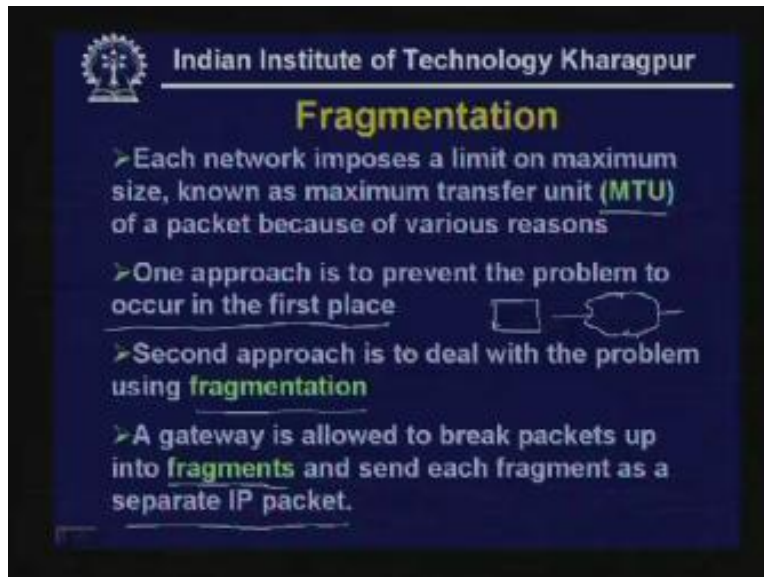
Then the source IP address is necessary which is 32-bits the destination IP address and this identification, flags and fragment fields are used for the purpose of fragmentation.

(Refer Slide Time: 31:17)



Let us consider the fragmentation and reassembly and see how it is being performed in the IP layer.

(Refer Slide Time: 33:25)



Why fragmentation is necessary?

As you know each network imposes a limit on maximum size known as maximum transfer unit or MTU of a packet because of various reasons. There may be various reasons for restricting the size of a packet. As you know, if packet size is very large then the probability of error in the packet increases. So, to reduce the probability of error of a packet the size is restricted or different standard uses or different size of packets or

frames. As you have seen IP allows 64 kilobytes. On the other hand, Ethernet uses 1500 bytes, so in this way different standards use different packets.

When you do internetworking the packets are originating from different networks and they have to pass through different types of network. Suppose a network receives a packet which is bigger than it can handle then how this problem can be tackled. There are two ways of handling it. One approach is to prevent the problem to occur in the first place that means the source takes care of them. The source is requested to send packets of minimum size so that maximum size is allowed by any network in that path from source to destination. This is one approach which you may call prevention.

The second approach to deal with this problem is to use fragmentation. What can be done, this gateway is allowed to break packets up into fragments and send each fragment as a separate IP packet. This is the second approach which is commonly used in most of the cases to have more flexibility.

(Refer Slide Time: 38:59)

Indian Institute of Technology Kharagpur

Reassembly

➤ Fields related to fragmentation in IP

- **Identification:** 16-bit field identifies a datagram originating from the source host.
- **Flags:** There are 3 bits, the first bit is reserved, the second bit is do not fragment bit, and the last bit is more fragment bit.
- **Fragmentation offset:** This 13-bit field shows the relative position of the segment with respect to the complete datagram measured in units of 8 bytes.

4800

Diagram illustrating fragmentation of a datagram (4800 bytes) into four fragments:

- Fragment 1: Offset = 0
- Fragment 2: Offset = 5
- Fragment 3: Offset = 200
- Fragment 4: Offset = 400

However, fragmentation is very easy, breaking anything is very easy but putting them together is very very difficult, **even a child knows about it.** So similar situation arises in reassembly, fragmentation can be done but reassembly is a more difficult problem. Let us see how it can be done.

Reassembly is performed in IP with the help of three fields; identification, flags and fragmentation. In general how reassembly can be done? Reassembly can be performed by using two different approaches. First one is known as transparent fragmentation. In this case the gateway router which receives the packet breaks it up as it passes through the network with the maximum size then as it reaches the exit gate way or exit router it is reassembled. So it comes out of the network as it was received. So within the network it is fragmented but as it comes out it comes as the original packet, it is reassembled by the

exit router. In this case the problem is each and every packet has to be routed through the same exit gateway. Therefore, as it passes through different networks it is transparent to the source as well as the destination. The destination receives a reassembled packet as it has been sent by the source. This is known as transparent fragmentation as it is done by the ATM network. Of course in ATM network instead of fragmentation they use the different term known as segmentation so the transparent fragmentation is being done.

On the other hand, in case of internet protocol or IP non transparent fragmentation is done. Here as the packet passes through different networks it is broken down or fragmented depending on the maximum size that is allowed within the network. For example, here the gateway where the packet has entered has fragmented the original frame into a number of frames and the exit router does not do anything so it can be exceeded to different paths. The sender sends one packet and through this network when it comes out three packets are going towards the destination and as it enters another network it is further fragmented so each packet is fragmented into two so six IP packets are generated by the network two. Hence, it is the responsibility of the router to the destination node to do the reassembly that's why it is called non transparent fragmentation which is done by the IP protocol using three fields; identification, flags and fragmentation offset field.

(Refer Slide Time: 37:20)

The slide is titled "Reassembly" and is from the Indian Institute of Technology Kharagpur. It lists fields related to fragmentation in IP:

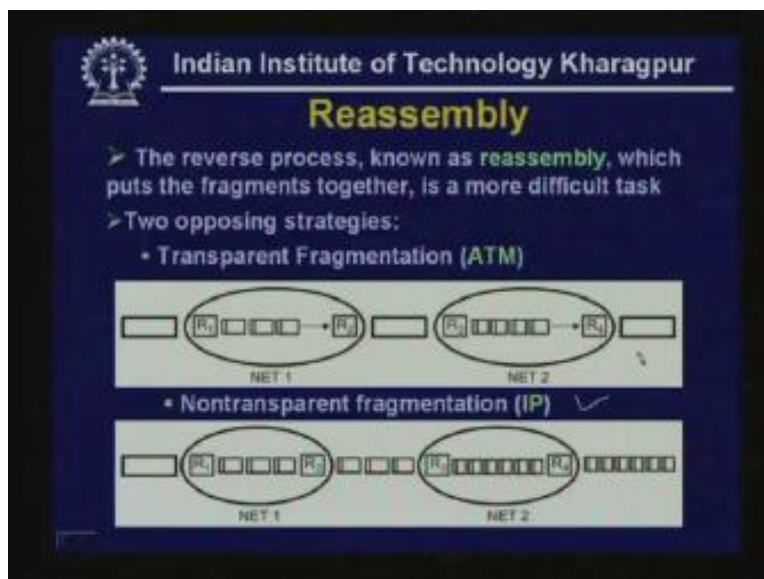
- **Identification:** 16-bit field Identifies a datagram originating from the source host.
- **Flags:** There are 3 bits, the first bit is reserved, the second bit is **do not fragment** bit, and the last bit is **more fragment** bit.
- **Fragmentation offset:** This 13-bit field shows the relative position of the segment with respect to the complete datagram measured in units of 8 bytes.

A diagram illustrates the fragmentation of a datagram. A horizontal bar represents the datagram with segments labeled H (header) and data. The segments are numbered 1000, 3200, and 4800. The diagram shows the datagram being fragmented into four segments, each with an offset value: OFFSET = 0, OFFSET = 0, OFFSET = 200, and OFFSET = 400.

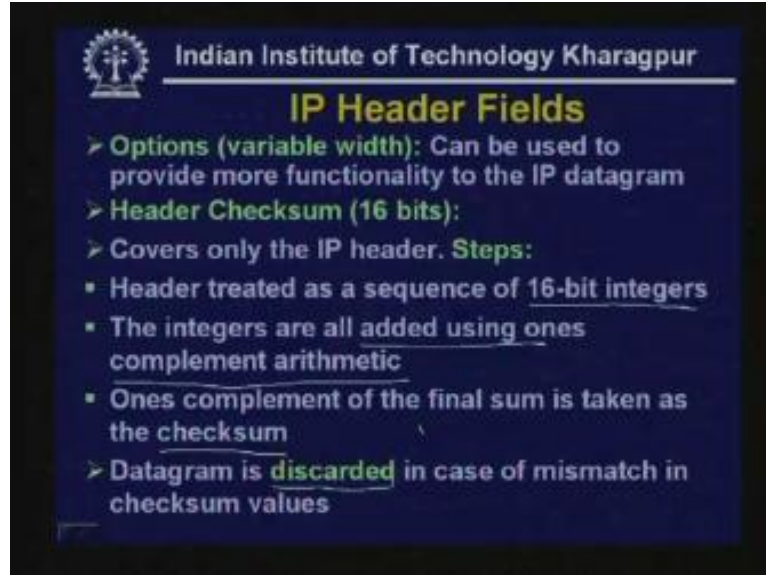
Identification part is a sixteen bit field that identifies a datagram originating from the source host. So this identification part remains unaltered as it is fragmented. There are three flag bits, the first flag bit is not used, the second bit is the do not fragment field bit and the last field it is more fragment field. That means whether it has to be fragmented or more fragmented has to be specified here. That means with the help of these two bits one can specify whether fragmentation has to be done or not to be done.

Then the fragmentation offset is specified with different fields with the relation to the original data. Here it is explained with the help of a packet which is of 4800 bytes which is divided into three fragments. as you can see each will have a header and it is divided into three fragments (Refer Slide Time: 37:58) so here it is divided into 0 to 1599 then 1600 to 3199 and 3199 to 4799 so these are the three packets. now as you have seen the maximum size is 64 kilo bytes which cannot be represented by thirteen bits that's why it is expressed in terms of eight bytes so this 1600 is divided by 8 to get an offset of 200 and 200 is return in that offset field. Similarly, here it is 3200 which is the offset from the with respect to the beginning which is divided by 8 to get 400 and 400 is returned of course in binary in thirteen bits in that fragmentation offset field. This is how it is fragmented and these fragmented packets as it reaches the destination the destination known will be able to do the reassembly by using this information so it uses the non transparent fragmentation techniques as I have explained here.

(Refer Slide Time: 39:13)



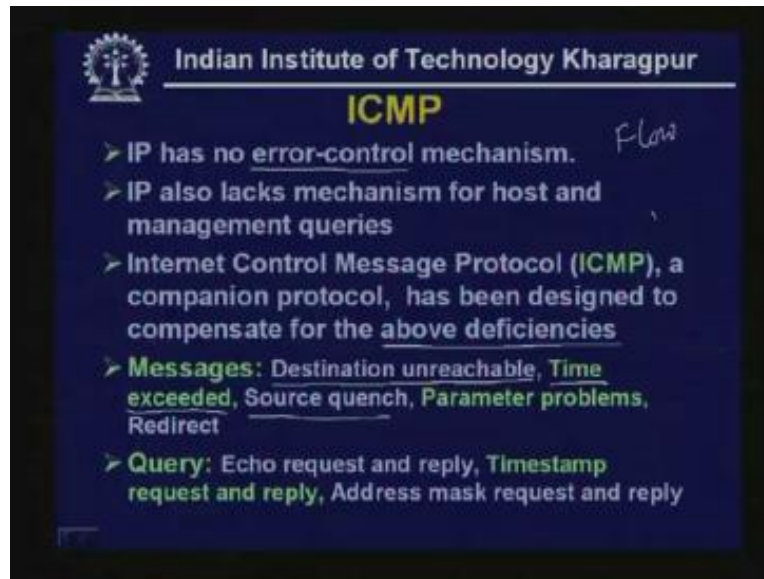
(Refer Slide Time: 39:51)



There is other options field, this can be used to provide more functionality to the IP datagram and there is a checksum field which is of sixteen bits. Checksum is done only for the header part so header is treated as sixteen bit integers, the integers are all added using ones complement arithmetic, then the ones complement of the final sum is taken as the checksum and if the checksum does not match then the frame is discarded.

Now let us discuss about ICMP a companion protocol used along with IP protocol. We have seen that IP is a best effort unreliable protocol. So if an error occurs, if a frame gets corrupted or if it is not delivered then the source will not know about it. Since IP has no error control mechanism there is no flow control mechanism. ICMP stands for Internet Control Message Protocol which has been designed to compensate for these deficiencies. that means it is an unreliable one but the source should know what is happening what is happening to a particular packet that is being provided with the help of this ICMP and ICMP can send a number of messages or it can do the query.

(Refer Slide Time: 41:59)



It can send different types of messages for example destination unreachable. a packet is sent and the router is not able to deliver the packet. so in such a case although the packet is not delivered a ICMP packet is generated informing the source that the packet that was sent is has not reached the destination or time exceeded. so a packet is discarded as the time is exceeded. In such a case also an ICMP frame is sent to the source to inform that a packet has been discarded because it was out of time.

Source quench: As you know the IP protocol does not provide flow control or congestion control, it is not supported by IP. In such a case source quench somehow provides the functionality of flow or congestion control. Thus, whenever a particular packet is discarded because of congestion then a source quench packet is sent to the source informing that the packet has been discarded and moreover congestion still exists in the network.

Parameter problem: Whenever the frame reaches with incorrect field in such a case parameter problem arises which is also informed to the source.

(Refer Slide Time: 44:17)

Indian Institute of Technology Kharagpur

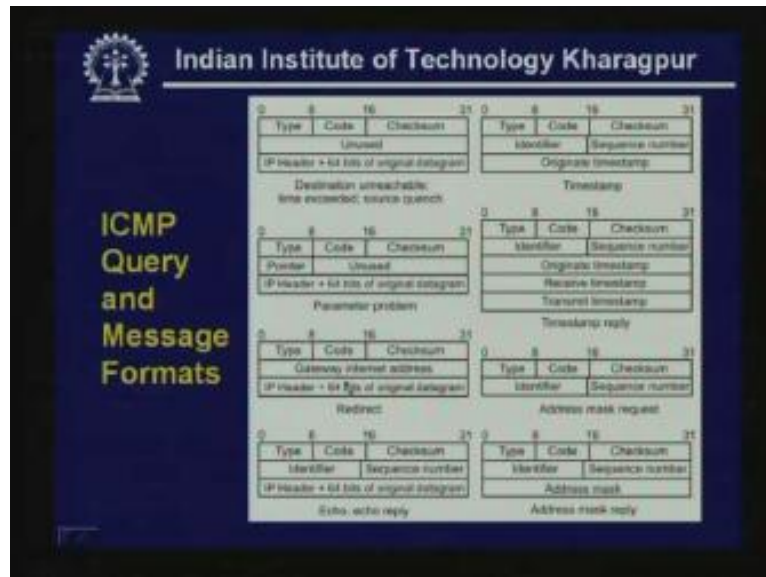
ICMP

- IP has no error-control mechanism. *Flow*
- IP also lacks mechanism for host and management queries *IP*
- Internet Control Message Protocol (ICMP), a companion protocol, has been designed to compensate for the above deficiencies
- **Messages:** Destination unreachable, Time exceeded, Source quench, Parameter problems, Redirect *live Flow / Congestion*
- **Query:** Echo request and reply, Timestamp request and reply, Address mask request and reply *Delay*

Redirect message: this is necessary. Whenever a router receives a packet it is not made for that particular router. So it redirects it towards the proper destination at the same time it informs the source about the redirection. These are the various messages that is being supported by ICMP.

Also, different kinds of queries can be performed. For example, in the case of echo request and reply, a station can send a request to another destination station to know whether the station is live, whether it is working or not working. Similarly, in the case of time stamp request and reply a source can send a frame to the destination and destination will also use the time stamp and reply. So, by this the round-trip delay can be estimated or this can be also used to synchronize two clocks the source clock and the destination clock. So, for synchronization of two clocks or measurement of delay this can be used.

(Refer Slide Time: 44:36)



Then we have the address mask request. A particular station may not know about the subnet mask so that can be queried and it can get the reply. For that purpose there are a number of message formats which are shown here. For example, destination unreachable, time exceeded, source quench, time stamp request, time stamp reply and so on.

(Refer Slide Time: 44:42)



(Refer Slide Time: 46:06)

Indian Institute of Technology Kharagpur

Routing Protocols

- Routing types: **unicasting** and **multicasting**
- Unicasting is a **one-to-one** communication
- Protocol types: **Interior** and **exterior**
- Interior: Intra-AS (Autonomous System)
 - **Routing Information Protocol (RIP)** ✓
 - Based on distance vector routing
 - **Open Shortest Path First (OSPF)** ✓
 - Based on Link state routing
- Exterior: Inter-AS
 - **Border Gateway Protocol (BGP)**
 - Based on path vector routing

Handwritten diagram: Two circles labeled 'AS' connected by a line, with an arrow pointing from one to the other.

Then comes the question of routing. As you know there are three different types of routing namely unicast, multicasting and broadcasting. Unicast is a one to one communication and there are two different types of protocol; one is known as interior and the other one is known as exterior protocol. As you know the network is divided into a number of autonomous systems. So the communication within the autonomous systems can be performed with the help of two protocols known as Routing Information Protocol RIP and Open Shortest Path First protocol OSPF. Routing Information Protocol is based on distance vector routing and Open Shortest Path First protocol is based on link state routing which you have **already discussed in detail while discussing routing techniques.**

Whenever the routing has to be done outside the autonomous systems say inter autonomous system routing has to be done for that purpose you require a different type of protocol for example Border Gateway Protocol or BGP which is based on path vector routing which is provided to do this routing. So these are the different protocols used in IP.

(Refer Slide Time: 47:32)



Indian Institute of Technology Kharagpur


Multicasting and IGMP

- Multicasting is used to send a message to a select **group of users** (one-to-many)
- IP supports multicasting using **class D** address having more than 250 million addresses
- The Internet Group Message protocol (**IGMP**) has been designed to help a **multicast router** to identify hosts in a LAN environment
- IGMP uses three types messages: **query message, membership report** and **leave report**

However, it has to also support multicasting. As we know that class D is having more than 250 million addresses for the purpose of multicasting. So multicasting is used to send message to a group of users which is supported by IP so you have to use some suitable protocol for that purpose. However, to keep track of different groups a special protocol is used which is known as IGMP or Internet Group Message protocol. **Don't get confused with the routing protocol.** IGMP is not a multicasting routing protocol but it helps multicast routing. It has been designed to help multicast router to identify hosts in a LAN environment.

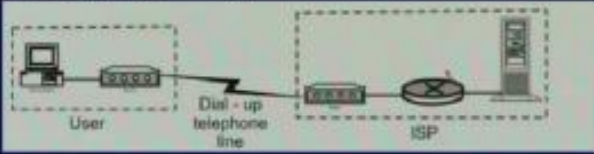
IGMP uses three types of messages like query message, membership report and leave report and it operates in a somewhat similar manner as ICMP. We have already discussed how ICMP works. So in a somewhat similar manner IGMP works and does the function of multicasting.

(Refer Slide Time: 49:55)

 Indian Institute of Technology Kharagpur

(Serial Line IP) SLIP

- Stations send raw IP packets over serial line with a special flag byte (0xC0) for framing
- No error detection and correction supported
- IP addresses should be known in advance
- Supports only IP
- No standard
- No authentication



We have discussed about different types of LANs, WANs which are used in the internetworking. Now as I said suppose a home user wants to use TCP/IP how can he do it? By using serial link it can be done and that can be done by using serial line IP or slip. So in this case stations send raw IP packets over serial line with special flag byte (0xC0) and if it appears in the IP frame then you have to use suitable techniques so that this is not repeated in the IP frame.

However, it has got a number of limitations. It does not use error detection and correction. So error detection correction is not supported by slip protocol. IP addresses should be known in advance. That means source and destination addresses should be known and it supports only IP protocol and other protocols which are used in internetworking is not supported and also it does not use any authentication.

Moreover, there is no standard for slip, different manufacturers have developed different versions of slip which are not compatible to each other. These are the limitations, and how it is used is shown here. Suppose this is the home user which uses a dial up telephone line or it can use this line as well (Refer Slide Time: 49:23) to get internet service from internet service provider. Thus it can use slip protocols and with the help of modems it can set up a serial link then it can use the slip protocol to communicate between the host and the router in the internet service provider premises to communicate to send IP frames between these two edges.

(Refer Slide Time: 50:50)

Indian Institute of Technology Kharagpur

PPP

- Point to Point Protocol (PPP)
- Developed to overcome the limitations of the SLIP protocol
- PPP performs **error detection**, supports **multiple protocols**, allows **IP addresses to be negotiated** at connection time, permits **authentication**
- PPP uses HDLC framing

1 Flag	1 Address	1 Control	1/2 Protocol	Variable Information	2/4 FCS	Flag
01111110	11111111	00000011		Information		01111110

Therefore, to overcome the limitations of slip a protocol has been introduced known as PPP Point to Point Protocol and it performs error detection, it supports multiple protocols, it allows IP addresses to be negotiated that means the IP addresses need not be known before hand it permits authentication so it makes it reliable compared to slip. This PPP protocol uses HDLC framing. As we have seen in the previous case, it does bit stuffing. Whenever this is not been done 0x appears in the IP packet similarly here also bit stuffing can be done whenever flag bit appears in the data field.

(Refer Slide Time: 51:58)

Indian Institute of Technology Kharagpur

PPP

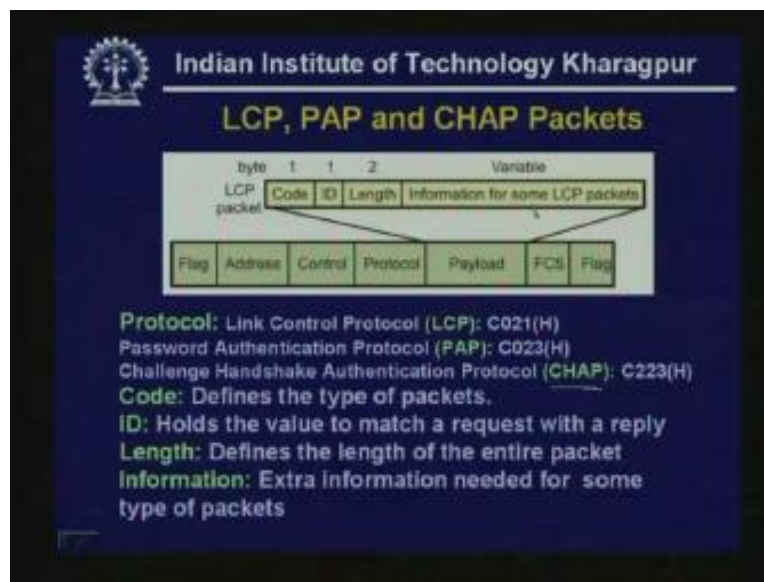
- A **Link Control Protocol (LCP)** is used for **bringing up, testing, negotiating options and bringing down**
- A **Network Control Protocol (NCP)** is used to **configure in the network layer**

```
graph TD; Idle -- "Carrier detected" --> Establish; Establish -- "Failed" --> Failed; Establish -- "Success" --> Authenticate; Authenticate -- "Success" --> Communicate; Authenticate -- "Failed" --> Failed; Communicate -- "done" --> Terminate; Communicate -- "NCP configuration" --> Communicate; Terminate -- "Drop carrier" --> Idle; Failed --> Idle;
```

This is the flow diagram for PPP protocol. Apart from using this HDLC framing it sets up the link with the help of Link Control Protocol LCP so it uses for bringing up testing and negotiating options and also for bringing down.

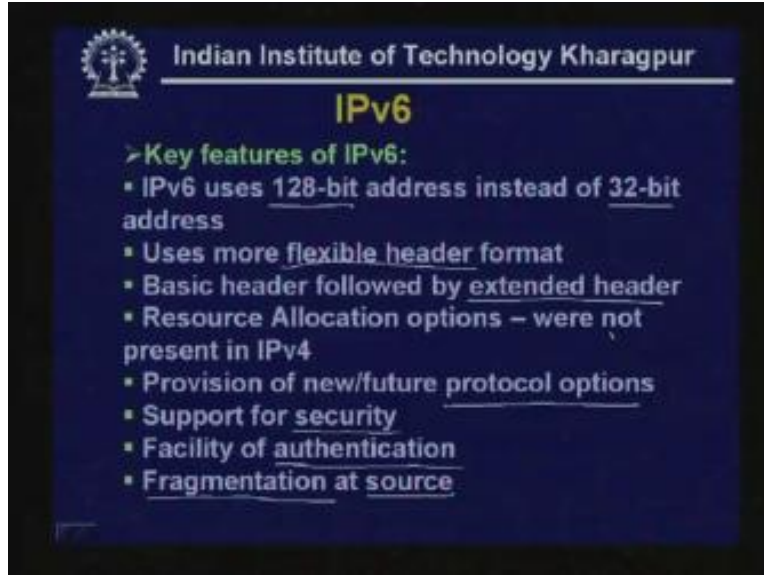
As you can see in the initial case it can be in the idle state, and when the link is established it goes to established state and when the carrier is detected **if it feels** it comes back to idle then it does the authentication **and by if it feels** it goes to the terminate state and if the authentication is successful it goes to the communication protocol by using the network control protocol which is used to perform the configuration purpose and to perform communication between the two devices.

(Refer Slide Time: 52:57)



For that purpose different packets like the LCP, PAP and CHAP packets are encapsulated in that HDLC frame. For example, this protocol field specifies what type of packet it is such as LCP or PAP or CHAP. LCP stands for Link Control Protocol, PAP stands for Password Authentication Protocol and CHAP stands for Challenge Handshake Authentication Protocol. The payload has got different codes or different functions and ID holds for the value of match with request and reply and extra information needed for some type of packets. This is how different packets can be put in the payload of the HDLC frame.

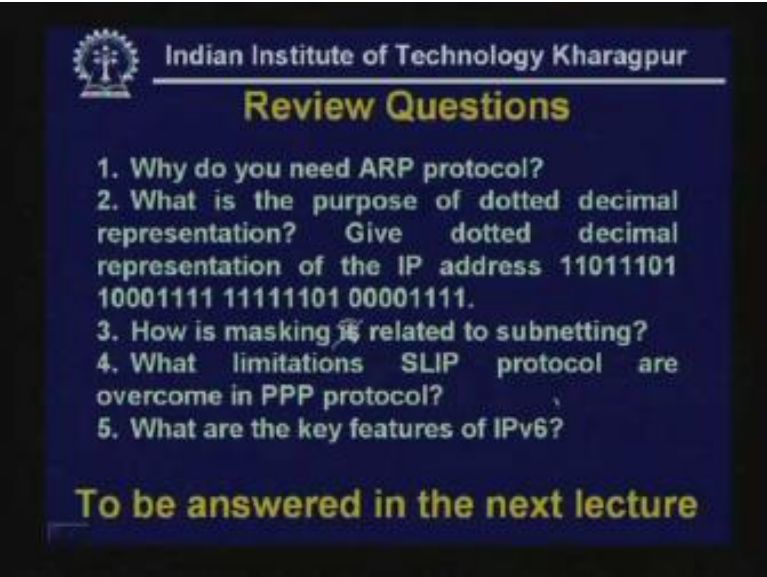
(Refer Slide Time: 54:07)



I think our discussion will not be complete if I don't mention about IPv6. We have seen that IPv4 which is now very popular has got a number of limitations which is being overcome in IPv6 and these are the key features of IPv6.

It uses 128-bit address instead of 32-bit address so 30-bit address is gradually becoming sufficient and it uses more flexible header format compared to IPv4 and basic header followed by extended header. It is used in two levels. It performs resource allocation options which were not provided in IPv4, there is provision for new or future protocol options and it supports for security. There is facility for authentication and in this case the fragmentation is done at source instead of performing that and non transparent fragmentation. So these are the key features of IPv6. Now it is time to give you the review questions.

(Refer Slide Time: 54:41)



Indian Institute of Technology Kharagpur

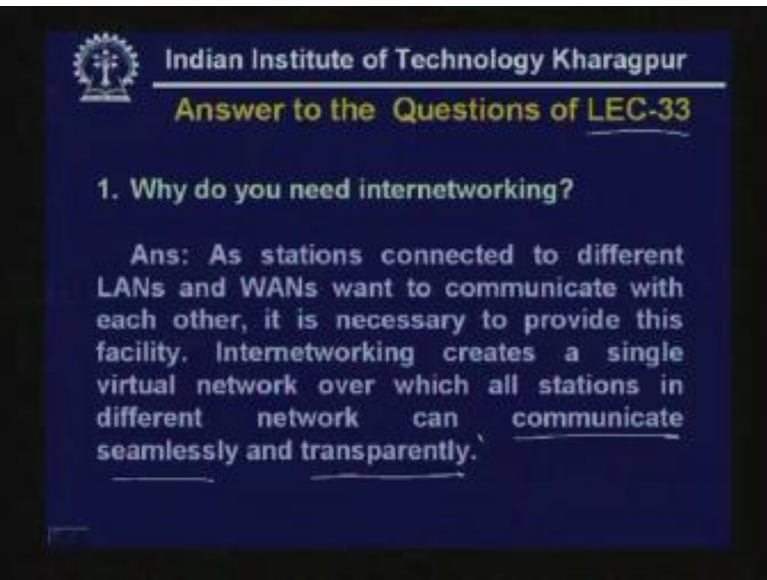
Review Questions

1. Why do you need ARP protocol?
2. What is the purpose of dotted decimal representation? Give dotted decimal representation of the IP address 11011101 10001111 11111101 00001111.
3. How is masking related to subnetting?
4. What limitations SLIP protocol are overcome in PPP protocol?
5. What are the key features of IPv6?

To be answered in the next lecture

- 1) Why do you need ARP protocol?
- 2) What is the purpose of dotted decimal representation? Give dotted decimal representation of the IP address given here.
- 3) How is masking related to subnetting?
- 4) What limitations SLIP protocol are overcome in PPP protocol?
- 5) What are the key features of IPv6?

(Refer Slide Time: 55:10)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-33

1. Why do you need internetworking?

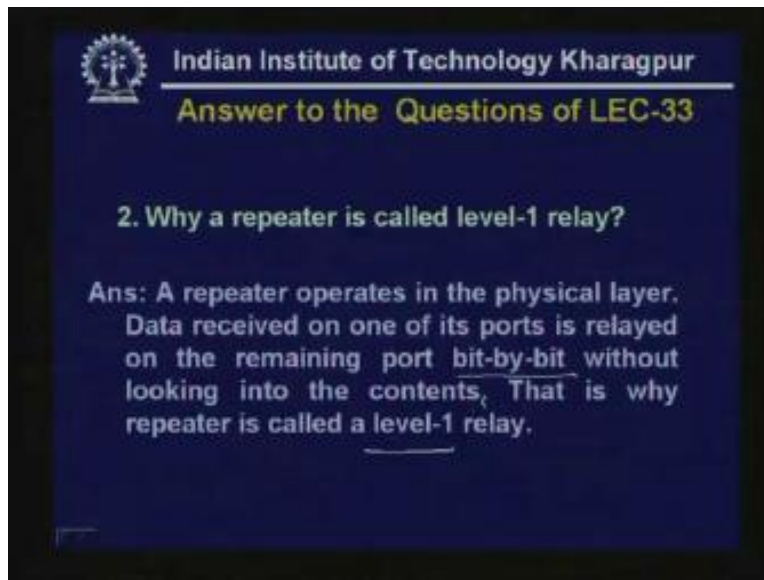
Ans: As stations connected to different LANs and WANs want to communicate with each other, it is necessary to provide this facility. Internetworking creates a single virtual network over which all stations in different network can communicate seamlessly and transparently.

Now it is time to give you the answer to the questions of lecture – 33.

1) Why do you need internetworking?

As stations connected to different LANs and WANs want to communicate with each other it is necessary to provide this facility internetworking creates a single virtual network over which all stations in different network can communicate seamlessly and transparently so that is the purpose of internetworking.

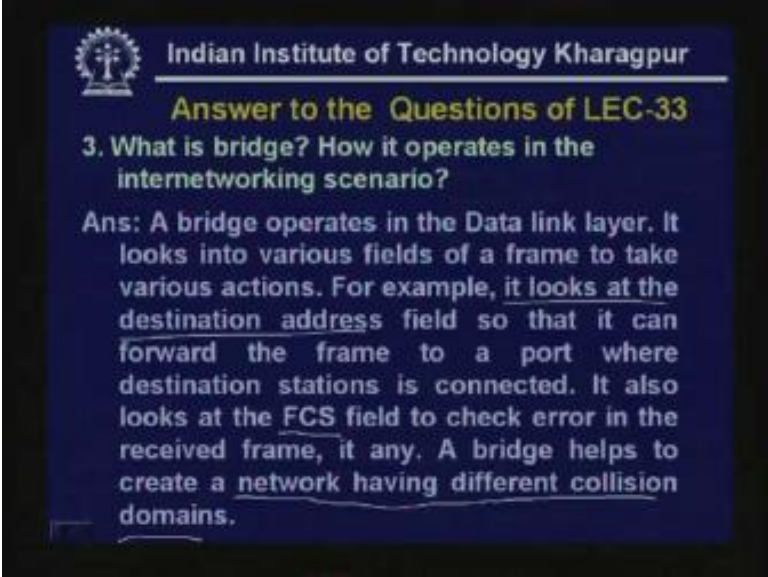
(Refer Slide Time: 55:30)



2) Why a repeater is called level - 1 relay?

A repeater operates in the physical layer data received on one of its ports is relayed to the remaining port bit by bit without looking at the contents that is why a repeater is called a level - 1 relay.

(Refer Slide Time: 56:02)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-33

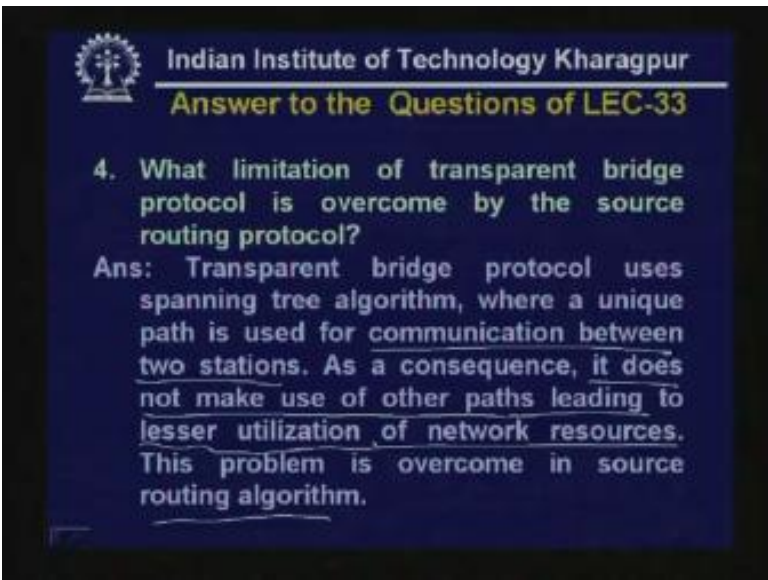
3. What is bridge? How it operates in the internetworking scenario?

Ans: A bridge operates in the Data link layer. It looks into various fields of a frame to take various actions. For example, it looks at the destination address field so that it can forward the frame to a port where destination stations is connected. It also looks at the FCS field to check error in the received frame, if any. A bridge helps to create a network having different collision domains.

3) What is a bridge? How it operates in the internetworking scenario?

A bridge operates in the data link layer it looks into various fields of a frame to take various actions for example it looks at the destination address field so that it can forward the frame to the port where destination stations is connected it also looks at the frame check sequence field to check error in the received frame if any a bridge helps to create a network having different collision domains as you have discussed in detail.

(Refer Slide Time: 56:28)



Indian Institute of Technology Kharagpur

Answer to the Questions of LEC-33

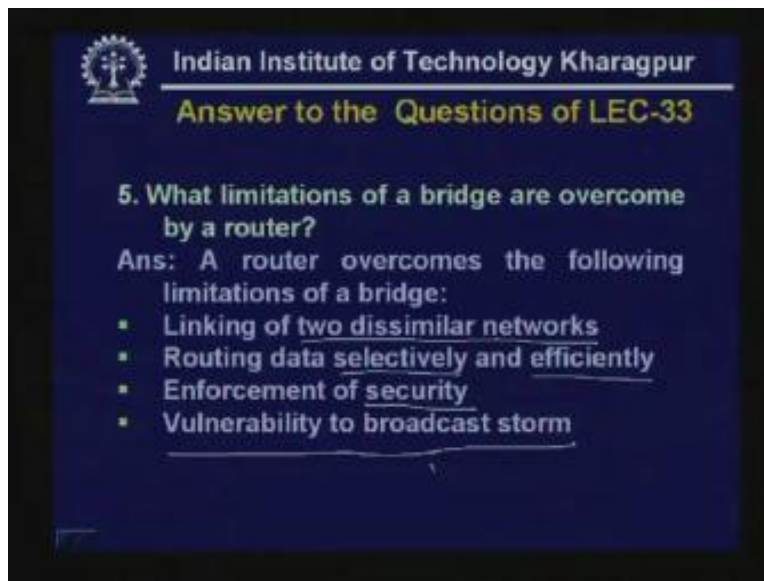
4. What limitation of transparent bridge protocol is overcome by the source routing protocol?

Ans: Transparent bridge protocol uses spanning tree algorithm, where a unique path is used for communication between two stations. As a consequence, it does not make use of other paths leading to lesser utilization of network resources. This problem is overcome in source routing algorithm.

4) What limitation of transparent bridge protocol is overcome by the source routing protocol?

Transparent bridge protocol uses spanning tree algorithm where a unique path is used to communication between two stations as a consequence it does not make use of the other path leading to lesser utilization of the network resources this problem is overcome in source routing algorithm.

(Refer Slide Time: 56:52)



5) What limitations of a bridge are overcome by a router?

A router overcomes the following limitations of a bridge linking of two dissimilar networks routing data selectively and efficiently enforcement of security vulnerability to broadcast storm so this are the advantages of router over bridge so with this we come to the end of today's lecture so there will be another lecture on TCP/IP where I shall mainly focus on TCP, thank you.