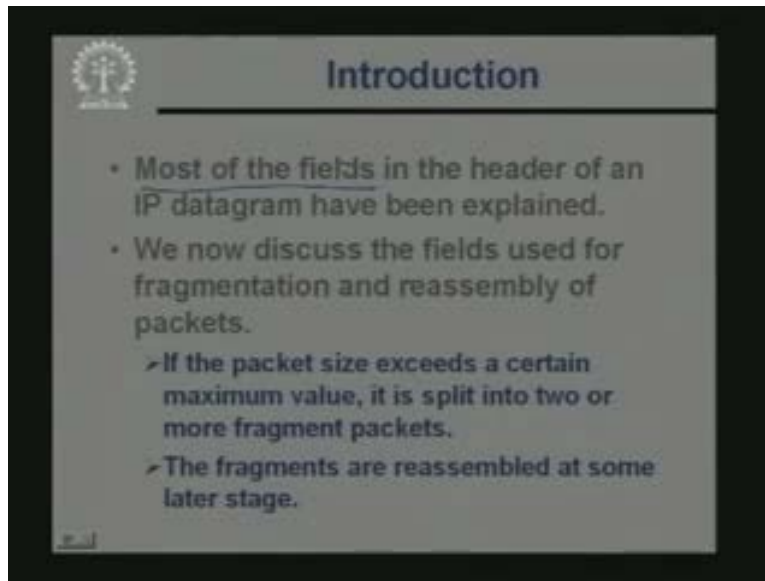


**Internet Technology**  
**Prof. Indranil Sengupta**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**  
**Lecture No #04**  
**TCP/IP – Part-II**

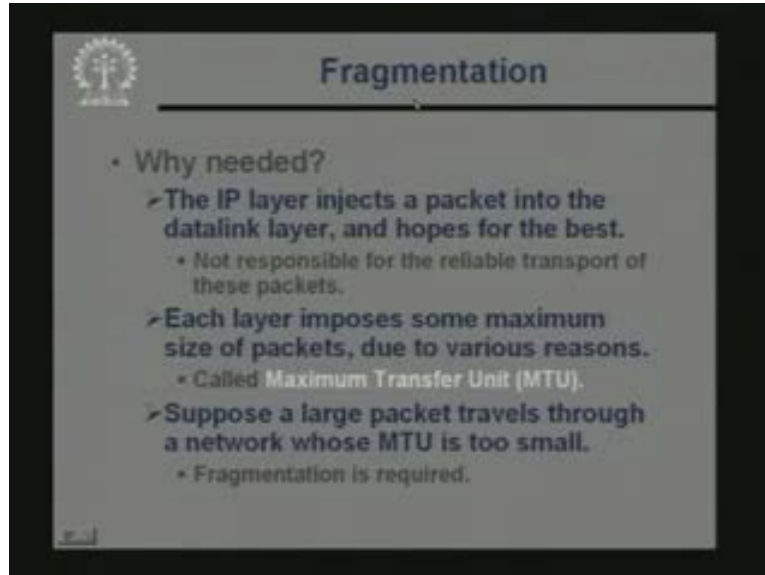
Now if you recall in our last lecture we were talking about the header fields in an IP datagram. Some of the header fields we have discussed. But a few of them we have not looked at as it. So in this lecture to start with we shall first be looking at those particular fields in the IP header that are responsible for fragmentation and reassembly of the packets.

(Refer Slide Time: 01:11)



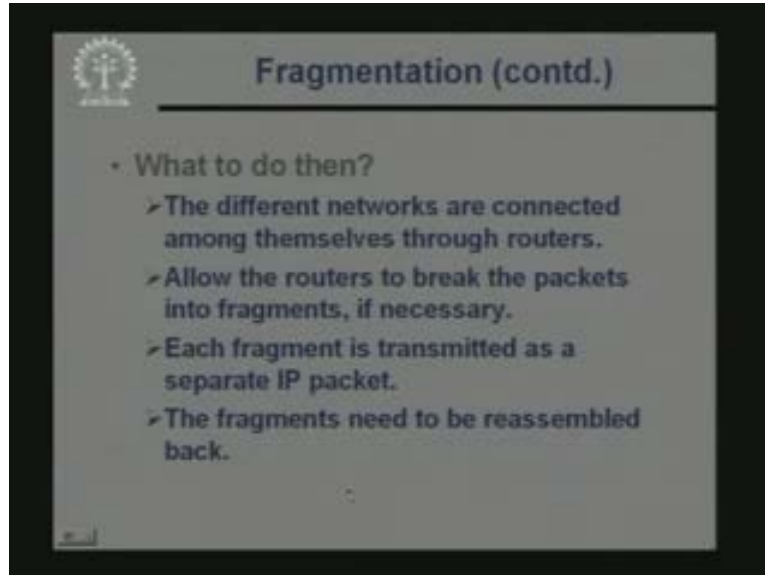
So just I had mentioned that we have already discussed most of the fields in the IP datagram headers. So today to start with we shall be discussing those fields which are responsible for fragmentation and reassembly of packets. Now the reasons why fragmentation or reassembly of packets is required are as follows. Suppose a packet has to flow through particular network. Now if the maximum transfer unit of that network is not large enough to carry the packet as it is then the packet has to be broken up into smaller pieces called fragments and the fragments can be carried through the network on its way to the final destination. So a packet may be split into two or more fragments. Now since we are breaking a packet into smaller pieces sometime or somewhere later we must reassemble the fragments back to form the original packet. So this is the basic concept behind fragmentation and reassembly of packets as they flow through the network.

(Refer Slide Time: 02:41)



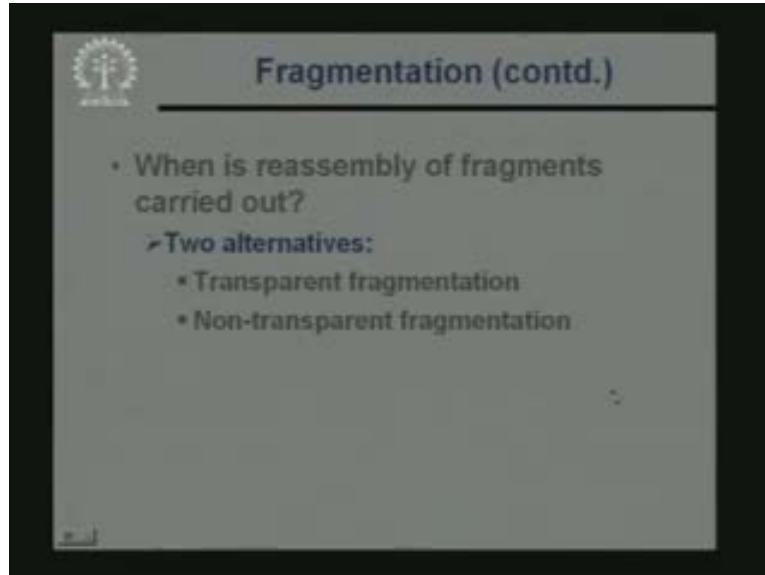
Now fragmentation, why is it required in IP? Let us try to answer this. See we have mentioned that the IP layer is a simple datagram transport service. It does not look for any reliability. It simply injects the packet into its lower layer which is the data link layer and it hopes that the datalink layer would be carrying the packet without any error to the next destination. So the IP layer is certainly not responsible for the reliable transport of the packets. This is important and moreover each layer will impose some maximum size of the packets that can flow through. For example if you are underlying network is Ethernet, Ethernet has a maximum packet size about 1600 bytes. So a packet cannot be more than that value if it has to be transported over an Ethernet network. So every network has such a maximum limit to the size of the packet it can carry or transport and this maximum value is called maximum transfer unit or MTU. So MTU is a characteristic of a network and the unit can vary from one network to the other. Now if a large packet travels through a network whose MTU is too small, then we would be requiring fragmentation.

(Refer Slide Time: 04:21)



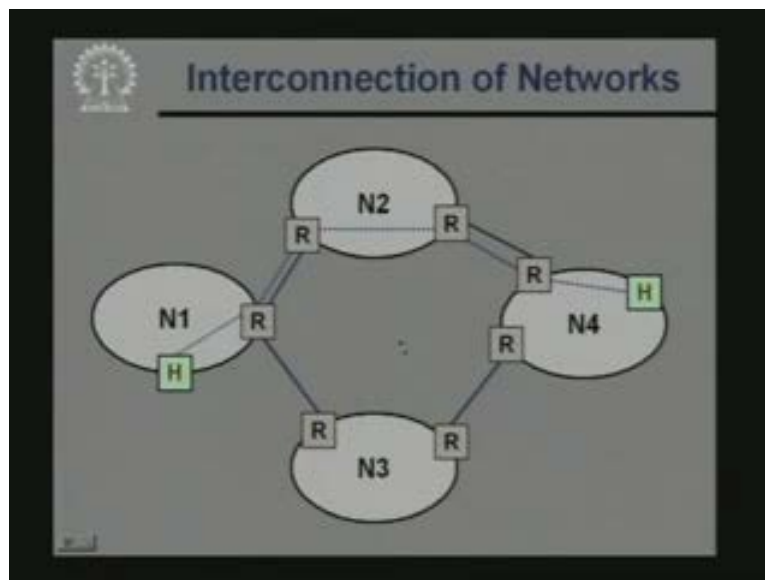
So this is why fragmentation is required. Well now assuming fragmentation is required. Let us see what is actually done in a network. Now you know that the different networks, if there are number of networks that can be connected among themselves through network devices called routers. Now when a packet enters a network through a router the router will have knowledge of the MTU of the network which the packet is trying to enter. So it will be the responsibility of the router to fragment the packet into smaller pieces. So the router will break the packets into fragments. If it cannot, transport it as it is. Now each fragment will be treated as an independent IP packet, it will be transported as a separate IP packet. But however as I had mentioned this fragmented packets need to be reassembled sometime or somewhere in the network. Now the way the packets are reassembled, that distinguishes two different kinds of fragmentation reassembly mechanism in networks that we shall have a look at.

(Refer Slide Time: 05:48)



So with respect to the time, reassembly of fragments is carried out, we can have two different alternatives; transparent fragmentation and non-transparent fragmentation. Now let us see what these two really mean.

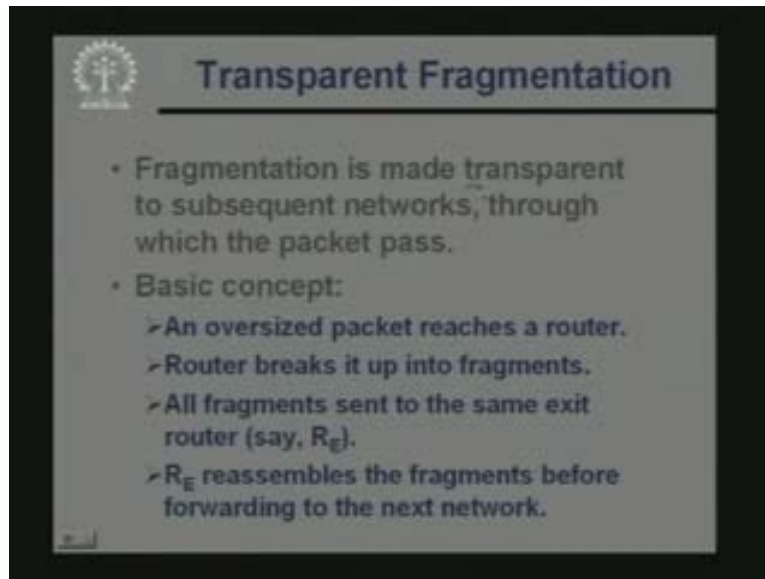
(Refer Slide Time: 06:04)



First we look at a model of an interconnection network. Well the model we look at it is there are several networks N1, N2, N3 and N4. Each of these networks can comprise of several computers. These networks have some routers, these are routers, these are all routers suppose a host here in network N1 wants to communicate with host out here in network N4. So obviously there are several paths or alternatives. Well say a packet can

follow this path there can be other paths also. So this will be our model of network where to networks are connected to each other through routers and each network will be having one or more routers. So a packet enters a network through a router. A packet exits a network again through a router. So routers are the entry and exit points of a network this is our model and this is a realistic model this is what this actually what happens in practice. Well first let us look at the mechanism of transparent fragmentation as the name implies there is something transparent about this mechanism. Let us see what this is.

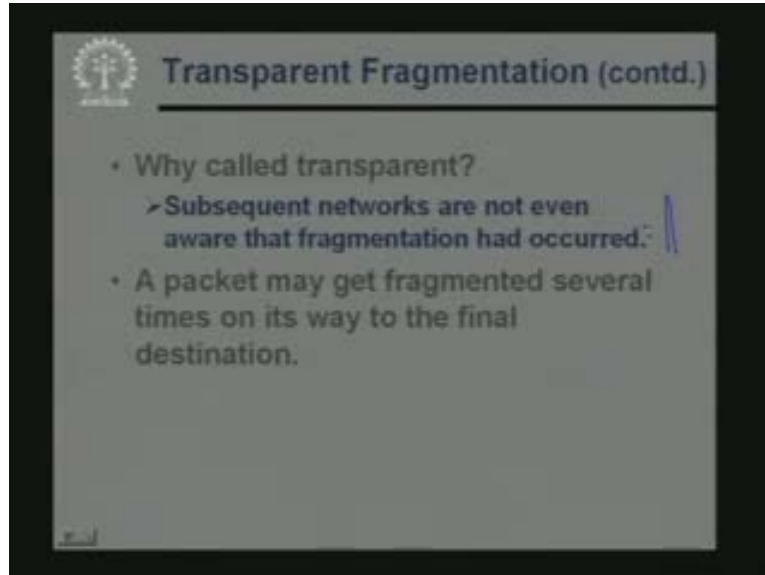
(Refer Slide Time: 07:40)



When you say transparent, what you mean is that fragmentation is made transparent to subsequent networks. This means that even though a network fragments a packet because it is empty too small. The subsequent network will not be aware of the fact that fragmentation is taken place. This means that the network which was responsible for fragmentation is also responsible for reassembling the fragments back. So that when you go to the next network it is the original packet which goes not the fragments. This is what the transparency is all about. So the basic concept as I have mentioned say a large packet reaches a router on its way to entering a network.

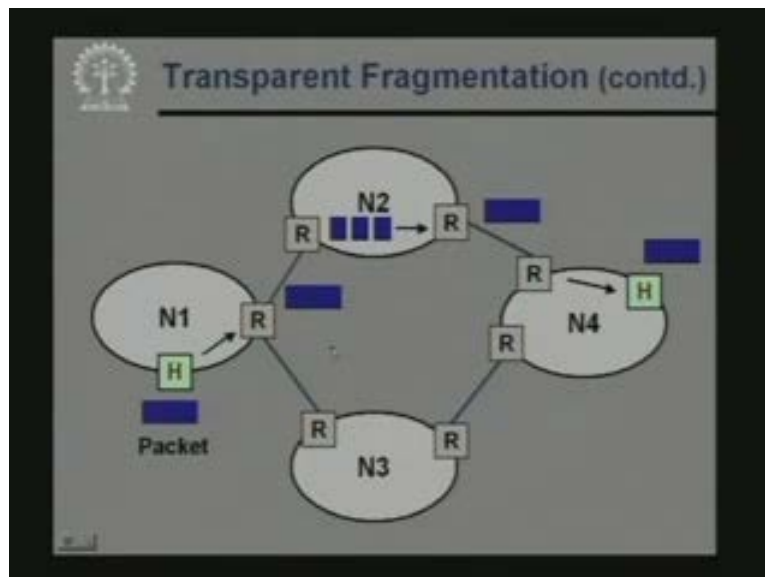
Now if the MTU is small enough, the router will break the packet into fragments and when the router breaks into fragments it also identifies something called an exit router. The particular network can have several routers through which the packet can exit. But in this scheme all the fragments must exit through the same exit router say R E. So it will be the responsibility of the exit router to reassemble the fragments before it is forwarding to the next network. So when the packet goes to the next network it is already reassembled and in and it is in the original form.

(Refer Slide Time: 09:26)



And as I mentioned this scheme is called transparent because the subsequent networks are not aware of the process of fragmentation. And in general packet may get fragmented several times and also reassemble several times on its way to the final destination. Because as it traverses through several networks, each of the network can potentially fragment it and again reassemble it back. So in this way it proceeds.

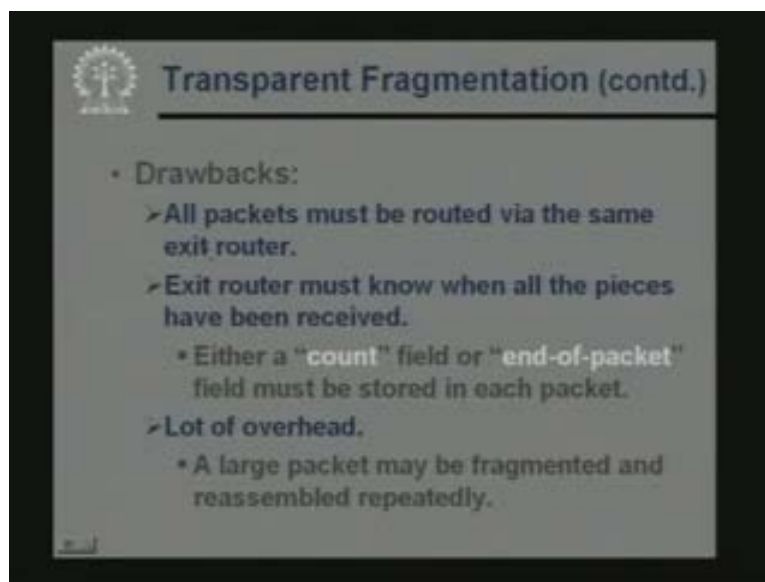
(Refer Slide Time: 09:57)



Diagrammatically this scheme can be explained as follows. Well look at the same network diagram comprising of 4 routers N1, N2. Suppose you have a packet out here. This is a packet which you want to send to a destination host out here. So this packet first

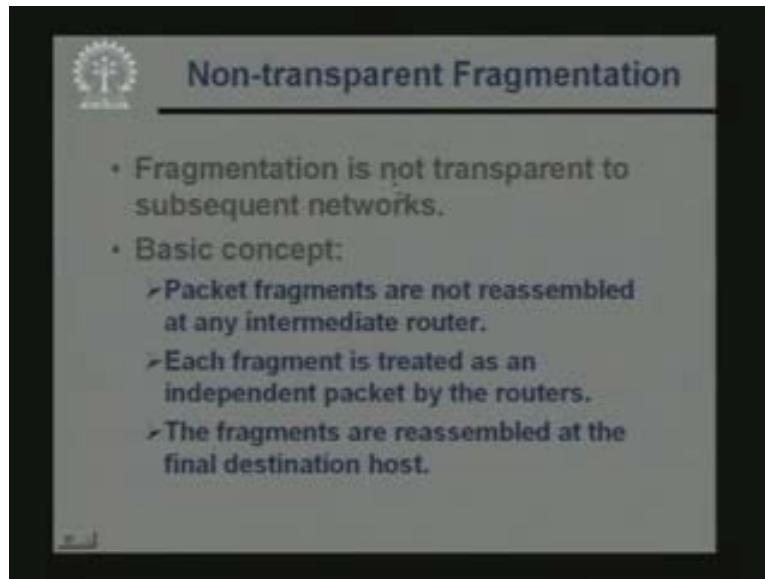
comes out of an exit router. This is the exit router and it enters another network N2. This router at the entry point of N2 finds that the packet is too big. So it fragments the packets into three pieces and it directs all these fragments to an exit router. Now in general this network can have more than two routers. That is there can be another router here also. So when this fragment reaches the exit router it is the responsibility of this exit router to reassemble them and form the original packet. So the network N4 where the packet goes next is not aware of the fact that this fragmentation and this reassembly have taken place in this network N2. So this is the idea behind transparent fragmentation. Now transparent fragmentation has some drawbacks because as a packet flows you are fragmenting and reassembling the packet may be several times. So let us see what the main drawbacks are.

(Refer Slide Time: 11:42)



The first drawback is that with respect to a network all packets must be sent through the same exit router. This means that all though several paths may exist the packets must always follow the same path. These does not well you can say does not make good utilization of the network resources and moreover since it is the responsibility of the exit router to reassemble the fragments. So the exit router must know when all the pieces have been received. So you must have either a count field in the fragment header indicating how many fragments are there or some kind of end of packet field. So that the exit router can know that well I do not have any more fragments I can reassemble them now. Now since a large packet may get fragmented and reassembled several times this method incurs a lot of overhead in general. So this is what transparent fragmentation is all about. Now next let us look at the other alternative the non-transparent fragmentation mechanism.

(Refer Slide Time: 13:03)



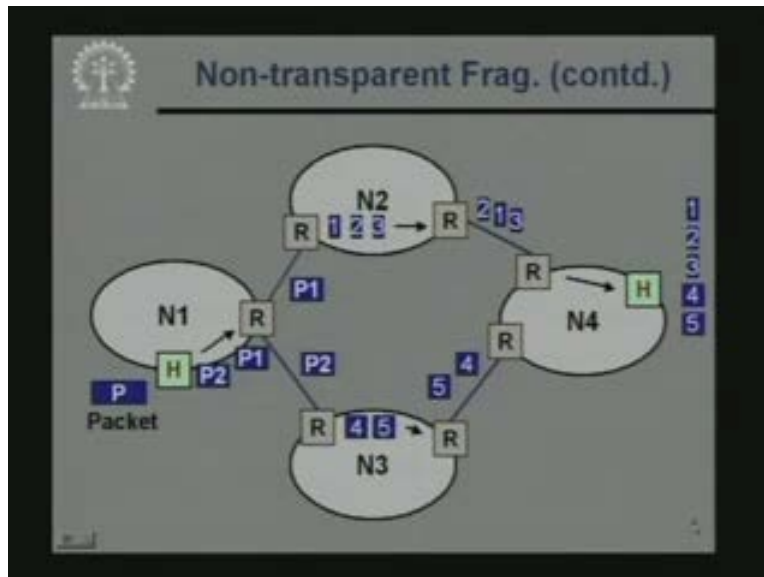
The slide is titled "Non-transparent Fragmentation" and features a logo in the top left corner. It contains the following text:

- Fragmentation is not transparent to subsequent networks.
- Basic concept:
  - Packet fragments are not reassembled at any intermediate router.
  - Each fragment is treated as an independent packet by the routers.
  - The fragments are reassembled at the final destination host.

Non-transparent Fragmentation, the basic idea is that fragmentation is not transparent to subsequent networks. Because subsequent networks will know that fragmentation has taken place. So the fragments are not reassembled immediately by the exit routers in a network right. So the basic the fragments which have been created are not reassembled by any intermediate router. This is an important point and unlike transparent fragmentation each fragment is treated as an independent packet. Well in transparent fragmentation mechanism the fragments were not really treated to be independent because the exit router had to receive all the fragments and put together them into the original packet again. So they were treated as fragments; not as independent packets. But in this method the fragment are all treated as independent packets and where does the reassemble done. The reassembly is carried out at the final destination host. So in this scheme the final destination host must have the capability to reassemble the fragments. This puts some extra burden on the receiving host.



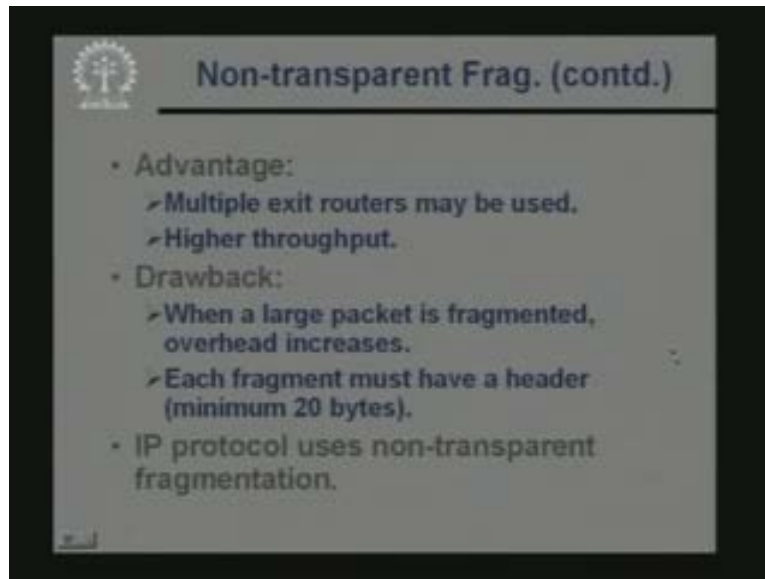
(Refer Slide Time: 14:38)



So illustrate diagrammatically again. Suppose a packet P which is generated by a host out here is getting fragmented in this network itself. So this packet P is getting fragmented into two fragments P1 and P2. Now it is now since P1 and P2 are independent here. It is not necessary they all should be sent to the same next hop network may be P1 goes to the network N2 and P2 goes to network N3 depending upon MTU of N2 and N3. This P1 and P2 packets may get fragmented. Say P1 gets fragmented into three pieces and P2 gets fragmented into two pieces 4 and 5. These fragments are sent may not be through the same path, through several paths several alternative paths to an exit router.

It is not necessary that the packets arrive at the router and the fragments in the same order for example 3 first, then 1, then 2. Here say 4 first, 5 first in order it comes. So it follows different paths and reaches the destination network and finally to the host and it is the responsibility of the host to receive all these 5 fragments and then put them in order. So it is the final destination host which does the reassembly of the packets. Now in this method you can immediately see since the fragments were following several different paths the transport of the fragment is faster. Because you are making much better utilization of the network resources you can follow several different paths to send the packets.

(Refer Slide Time: 16:30)

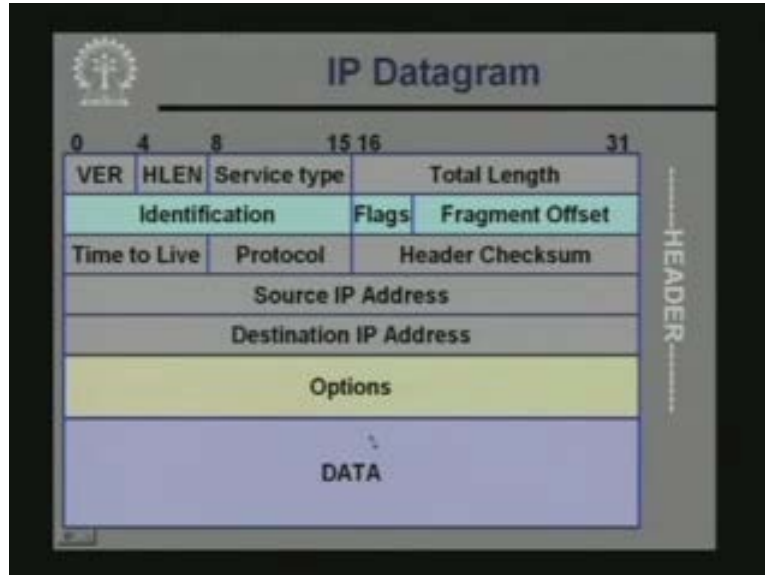


The slide is titled "Non-transparent Frag. (contd.)" and features a list of points. In the top left corner, there is a small circular logo with a gear and a cross. The text is as follows:

- Advantage:
  - Multiple exit routers may be used.
  - Higher throughput.
- Drawback:
  - When a large packet is fragmented, overhead increases.
  - Each fragment must have a header (minimum 20 bytes).
- IP protocol uses non-transparent fragmentation.

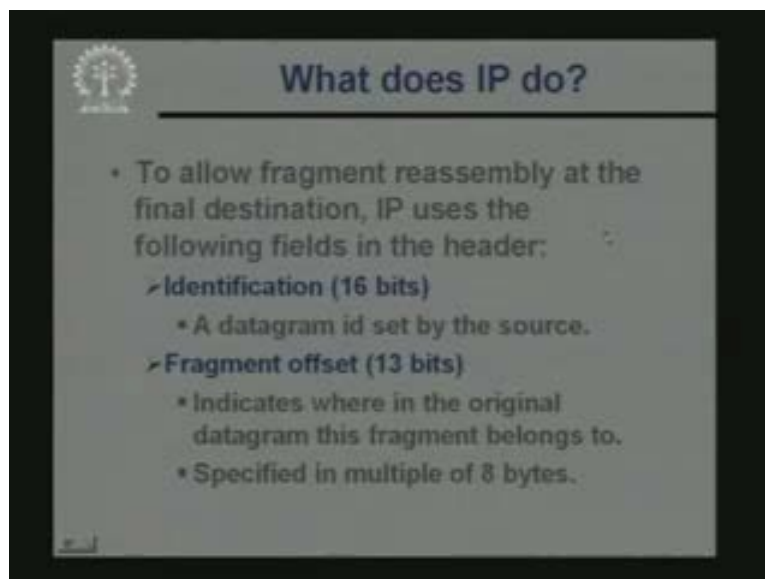
Now some of the advantages in this scheme is that, here as I just mentioned multiple exit routers you can use which means higher throughput because if you had used the same exit router then the total speed would be limited by the capability of that exit router. But now since you can sent out the packet through several routers the process can be faster drawback is that when a large packet is fragmented overhead increases. Because each of these fragments will be carried as a separate entity right up to the final destination and you recall that each fragment is an IP packet and its own right and must carry minimum of 20 Bytes of header. So for this reason overhead in terms of the header bytes is more point to note is that the IP protocol uses non transport fragmentation. So routers can fragment but reassembly is done only at the final destination host.

(Refer Slide Time: 17:45)



So let us again look at the header structure of an IP datagram. Well we have explained most of the fields in the IP header. There are three fields which are responsible for handling fragmentation and reassembly. These are identification flags and fragment offset. Now let us see what these three fields really mean.

(Refer Slide Time: 18:18)

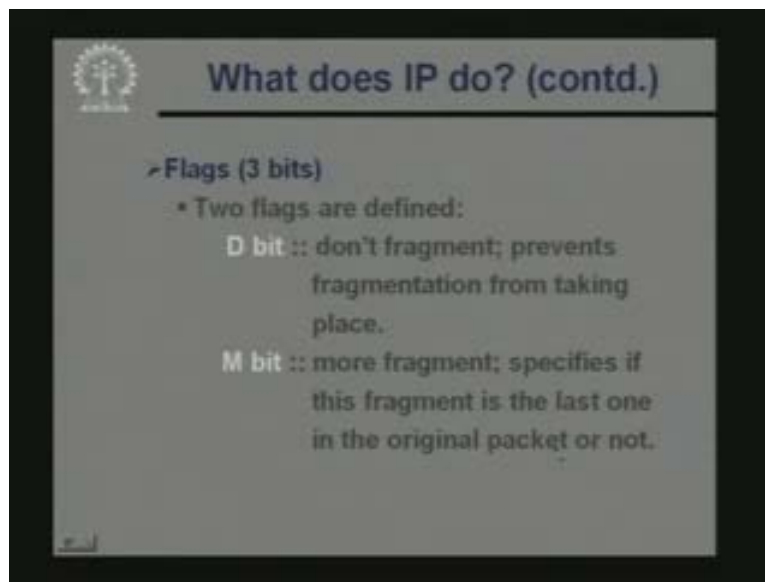


So IP layer since it uses non transparent fragmentation reassembly has to be carried out at the final destination. Now in order that the final destination can successfully carry out the reassembly each fragment must carry relevant information. Now the relevant information is as follows. First is an identification number which is 16 bits, it is basically some kind

of identifier. A datagram id which is set by a source. Suppose a packet has a datagram id of say 10. Now when that packet gets fragmented into three fragments each of the fragments will also carry the same id 10, 10 and 10. So that the receiver can identify well all this fragments of the same id so they belong to the same master packet. This is the purpose of the identification field then there is a fragment offset field which is 13 bits.

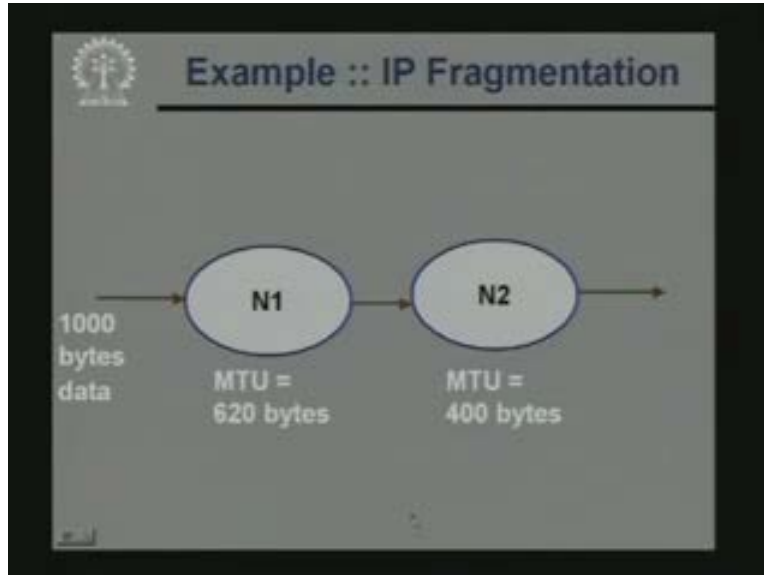
This actually indicates suppose I had a big packet from this from this packet a smaller fragment was created say like this. From this portion of the original packet the fragment was created. Now the point to notice that the receiver must know that with respect to the original packet exactly where the present fragments belongs to this field indicates where in the original datagram this this packet of fragment will fit in. Since this is a 13 bit field and a datagram size is 16 bits, if you recall, so this offset is specified in multiple of 8 bytes. So whatever value is specified there it is multiplied by 8 and that is treated as the beginning address in the original packet. Now since it is specified as a multiple of 8 a fragment size can be only in multiples of 8. This is something you must remember.

(Refer Slide Time: 20:41)



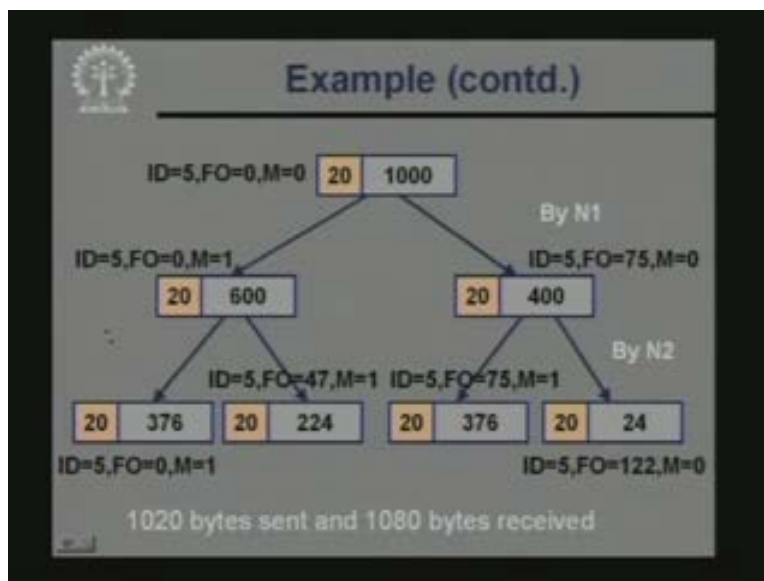
And there are some flag bits also. All though the flag is a 3 bit field, but out of those 3 bits, 2 of them are defined. One is a D bit which is called do not fragment bit. So if a packet carries the D bit equal to 1, the intermediate routers will not fragment the packets. Say if the destination host is not capable of doing the reassembly then the source will set the D flag to 1. So that no one will fragment the packet if the packet size is small enough, it can be transported otherwise the packet will be dropped somewhere down the line if it is large enough. Now M bit is a field which is called more fragments. Now if it if M equals to 1, it specifies that there are more fragments in this packet. If M equal to 0 it says that this fragment is the last one in the original packet. So just by looking at the M bit the receiver can know whether the present packet is the last one in the original packet or there are more following it.

(Refer Slide Time: 22:03)



Now we take an example to illustrate how fragmentation is carried out by IP layer. Let us take a scenario like this where a packet has to flow through two networks N1 and N2 in sequence. Suppose we are trying to send a 1000 byte data through these two networks, N1 has a MTU of 620 bytes including header, this N2 has an MTU of 400 bytes. So N1 can carry IP packet of size 620 maximum N2 can carry 400 maximum. Now let us see that how the original packet gets fragmented.

(Refer Slide Time: 22:50)



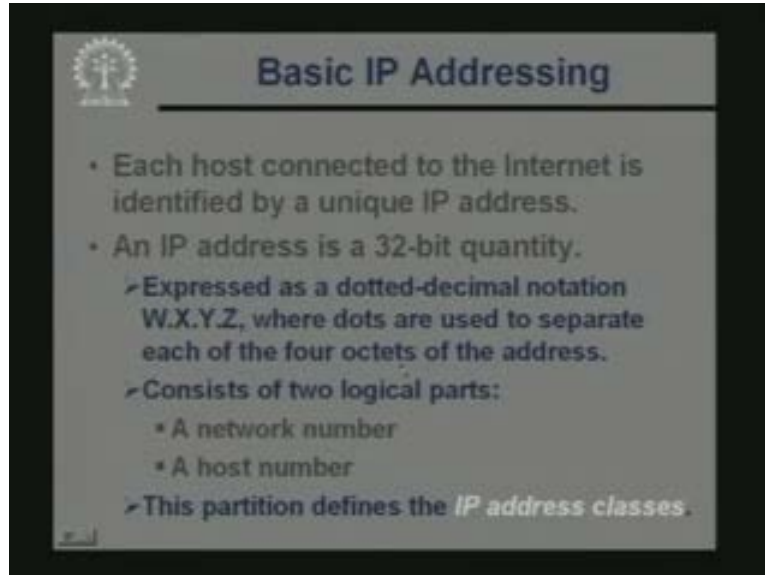
Well lets look at this diagram this is the initial scenario the initial packet had 1000 bytes of data and IP will put in 20 bytes of header. So it is a 1020 bytes packet originally. In the

original packet say the identifier id the datagram ID was set as 5. Since this is an unfragmented packet the fragment offset field is 0 and since there are no more packets following and the more bit is also 0. Now the first network you look back at the first network which had an MTU of 620 bytes. So the first network will be dividing this packet into two parts. One will be 600 plus 20, 620 other will be 400 plus 20, 420. So you see that this one packet gets broken into 2 packets. In the first one this ID is still 5 fragment offset is 0 because this is the first part of the fragment and more bit is 1 because there are more fragments following. For the second one ID is 5 fragment offset is 75 because the second packet is located at a relative location of 600 and since it is a multiple of 8  $600 \div 8 = 75$ .

So  $600 \div 8$  this gives you this figure 75 and since there are no more packets following more bit is 0. Now these fragments reach the second network N2. So for N2 again the MTU is 400 bytes. This packet gets fragmented, but here you look this 600 byte, does not get fragmented into  $380 + 20 = 400$ . But 380 is not divisible by 8. I told you that a fragment will always be divisible by 8 the data. So you use the nearest number which is divisible by 8 that is 376. So the other packet will take the rest 224. So for the first one ID is 5 FO 0 M equal to 1. This is the first portion for the second one ID is again five FO will be 47 because  $376 \div 8 = 47$  and M equal to one there are more. Similarly this will get fragmented in a similar way. So here FO will be 75. This will carry this 75 and for the next one FO will be  $75 + 376 \div 8$ , this will become 122 and for the last one the more fragment bit will be 0. There are no more fragments, so the final destination will be receiving these 4 fragments and using this ID FO and M information.

It can put together back in order, but one you thing you just look here that originally packet was size 1020. But at the receiving end there are 4 packets which mean 8 bytes of header. So we have received 1000 and 80 bytes. So there are 60 bytes of overhead in this fragmentation process. So IP uses fragmentation fine, but these includes additional overheads in terms of the additional header bytes or header information it carries. So this finishes our discussion on IP fragmentation. Now let us look at how IP addressing is carried out. Because you recall we had mentioned one of the main purposes of the IP protocol is to allow a packet to move from one you can say node to the other those are actually routers. These nodes are actually routers in terms of a real network for one node to the other on its way to the final destination network. So in order to that each of these intermediate nodes must have some idea regarding the address of the destination. Just by looking at the address it should be able to tell that well this is a better path to follow not the other path. So we will later how these routing decisions are taken in general. But first we look at the problem of basic IP addressing.

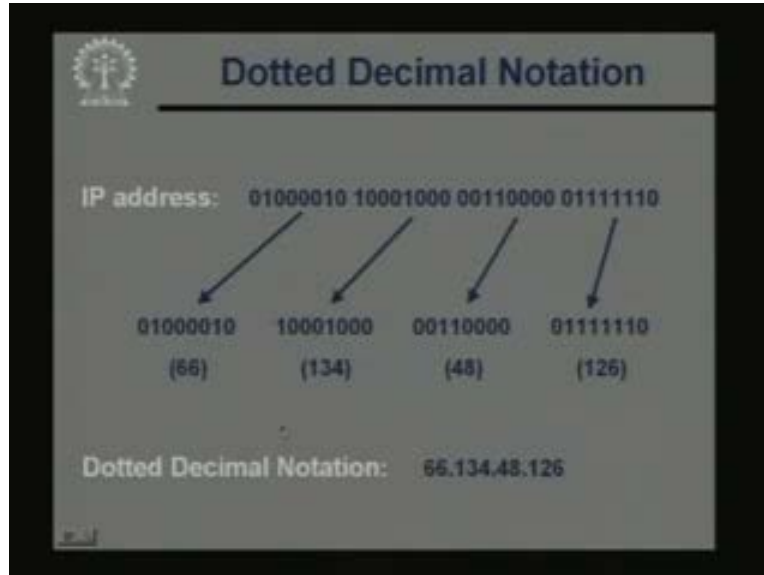
(Refer Slide Time: 27:41)



But first we look at the problem of basic IP addressing. Well one thing we had seen earlier that the source and destination address in the IP protocol is a 32 bit quantity that is the IP address. Now in the internet scenario, now if you want one host to communicate with other they must all have unique IP address. Because when you are sending a packet with a destination IP address, you must be sure that there is only one computer in this world who has this particular address. If there are more then there will be confusion and the packet may be delivered in the wrong place. So we have the concept of IP address which is supposed unique with respect to each host. This is a 32 bit quantity and representing a 32 bit quantity has a streams of 0 and 1s is inconvenient. So it is typically expressed as a so called dotted decimal notation. Dotted decimal notation means there are 4 decimal numbers W. X. Y. Z separated by dots and W. X. Y. Z represent the decimal equivalence of each of the 4 octets or the 8 bit chunks in the address.

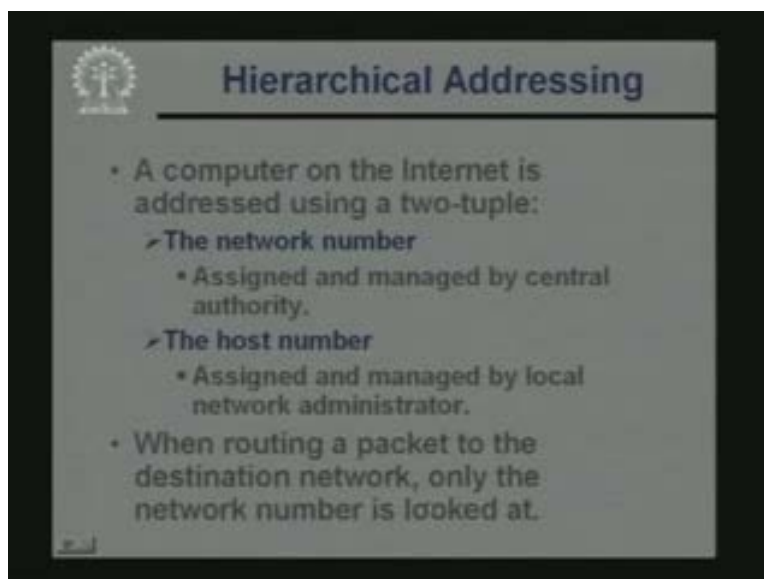
Well we have an example I will show you now this IP address logically contains two parts. Well one part identifies the network. Suppose your computer is located inside your organization network. So the first part of your compute address will identify the address of your network. So using that information the packet must reach your network. So there is one part in the address which identifies the network where the destination host belongs. But the other part indicates the host number which means ones the packet reaches the destination host. Then after that you use this host number to identify the computer where this packet has to be delivered or has to go. Now this division of IP address into two logical parts network number and host number. This can be done in a very simple systematic way, we shall see very shortly. There are something called IP address classes which are defined. We can use this IP address classes for this kind of logical division.

(Refer Slide Time: 30:37)



Well first let us look at the dotted decimal notation with respect with the example. Suppose I have an IP address, this is a 32 bit quantity like this. This 32 bit address I am dividing out into four 8 bit chunks. These are the 4 octets and each of the 4 chunks I am converting into decimal. This is 66, this is 134, this is 48 and this is 126. So after you convert each of these into decimal I simply write down the decimal numbers separated by dots and this is the so called dotted decimal notation. So we typically express the IP address of the machine in this form 4 numbers separated by dots this so called dotted decimal notation.

(Refer Slide Time: 31:44)



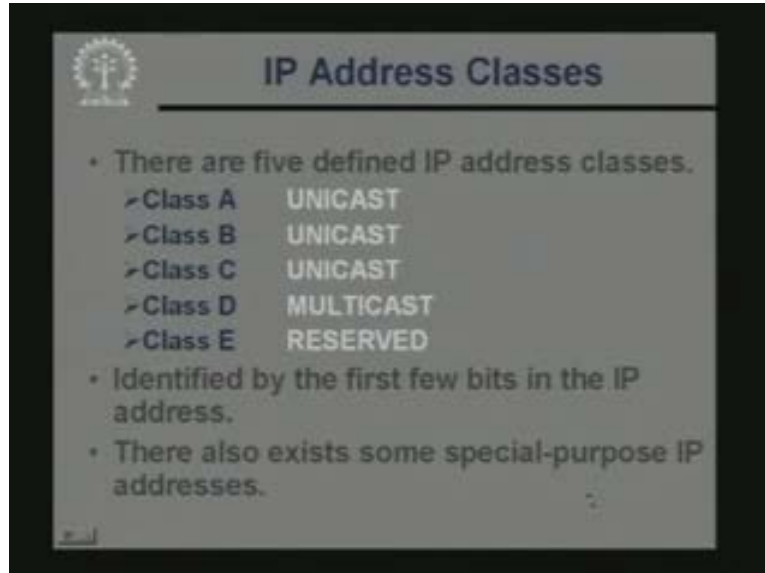


So talking we just mentioned that when we want to address the computer which is connected to the internet we actually specify two things the network number and the host number this actually represents a hierarchy in terms of the addressing. Now whenever you want to mention the network number well as I had mentioned the network number is something unique to your network. So whenever a node or a router sees that the network number of the destination address is something say x. So it knows where the network x is located and it tries to throw or forward the packet direction. So somehow the network addresses must be ensured to be unique across the world. So for this purpose there has to be some kind central authority that grants and manages these network numbers.

So if your organization has a network address no other computer network in the world must have or can have the same address, this must be ensured. So the network numbers the assignment and management is done by some central authority. So just whenever when you want to set up your own network, you can apply to the central authority. They will be granting you a new network number new unused network number you can use it for your network. The next part of the address the host number of course this is a local issue. Once the packet enters your network the way you number or address a host it is up to you. So these are assigned and managed by the local network administrator. So there is one part of the address which is managed globally.

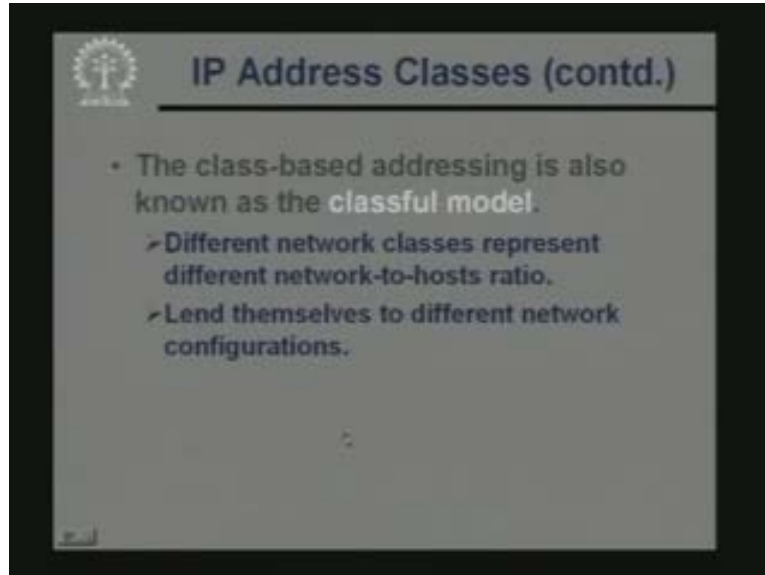
There is another part of the address which is managed locally but when you talk about routing a packet actually we talk about leading a packet to the correct destination network. So in order that the packet reaches the correct destination network we need not look at the whole of the address. We need to look at only the network portion of the address. The host portion of the address will be required only after the packet has reached or arrived at the destination network. So this is one thing which should be kept in mind this is very important that it is only the network portion of the address which is responsible or is used for the purpose of routing the packets. So this is what is mentioned out here.

(Refer Slide Time: 34.56)



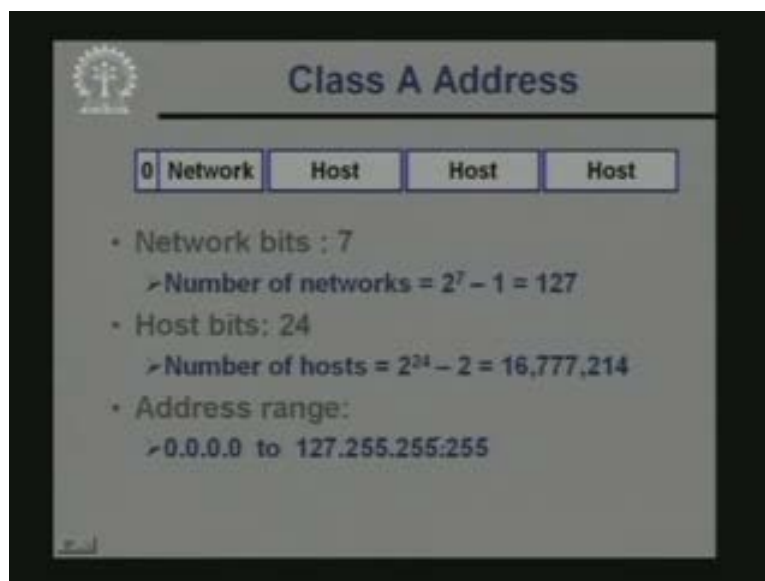
Now, in terms of the IP addresses. IP address are divided into several classes as you can here A B C D E. So out of them you can leave out E. E is really not used, this is a reserved category. Well if you want to do some experimentation on IP addresses you can use this class E the first three classes A, B and C. These are so called unicast address unicast means that using these addresses you are identifying one particular network on the internet. The addresses uniquely specify one computer. In contrast class D is a multicast address. MULTICAST means you want to send a packet to a group of computers. Say all computers which are belonging to a LAN you want to send them all at the same time. So this is something called multicasting. The address will be such that it will be broadcast or multicast to all the computers within a particular group. Now which class the IP address belongs to this is identified by the first few bits in the IP address. Now in addition to these classes we shall see that there also exists some special purpose IP addresses. Now let us see this in some detail.

(Refer Slide Time: 36:30)



Now this class based addressing this class A B C D E as I had mentioned. Here in these addressing schemes there is a fixed and well defined partition of an address with respect to the network part and host part. Network address part and the host address part, this partition is fixed and this mode of addressing a computer based on address classes is also called the so called classful model. Depending upon the network classes as we will see the network to host ratios of the network can vary. Depending on which class we use you can have different network configurations. These we will see very shortly how this is done.

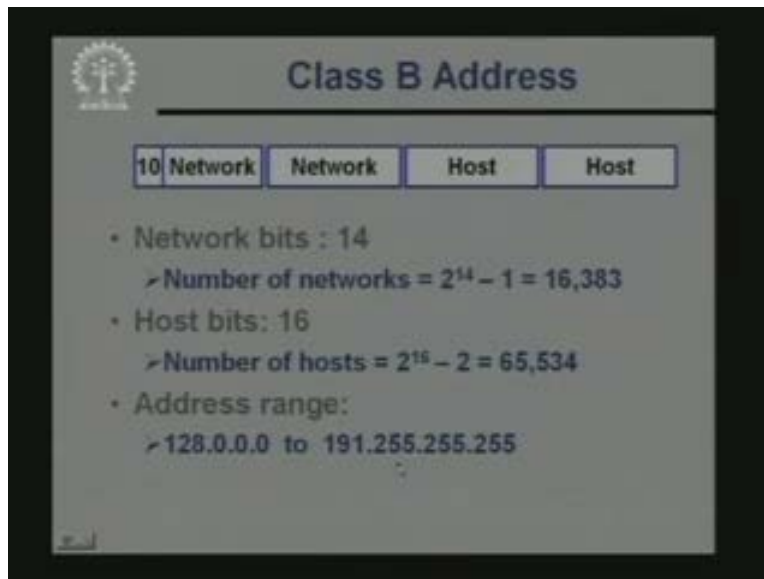
(Refer Slide Time: 37:21)



First let us see the basic characteristic of the different address classes first the class A. Class A represents those networks which are very large in size particularly the very big internet service providers. They would like to have a class A kind of address. Let us see what class A address says. In a class A address first thing is that these are the 4 octets; 1, 2, 3 and 4. A class A address begins with a number 0, the 7 bits out here represents the network. So other number of network bits is 7 and host is 24. 24 bits represents the host. In 7 bits although the total number of combination is 2 to the power 7 or 128 we shall see that out of the one particular combination is left aside for some other purpose.

So actually the total number of such network addresses you can have in class A will be a one less it is 127. Similarly for the hosts each of these class and networks can have of the order of 2 to the 24 hosts. Out of them we will see again that the all 0 and the all one combinations are used for some other purpose. So actually you have two addresses less it comes to a figure like this 16 above 16 million. So number of hosts in a class and network can be large as 16 million based on this address assignment in the dotted decimal notation a class A address can range from 0, 0, 0, 0 up to 127, 255, 255, 255. That means all zeros up to all ones. This is the range, so if you see an IP address within this range you can immediately identify that is a class A address.

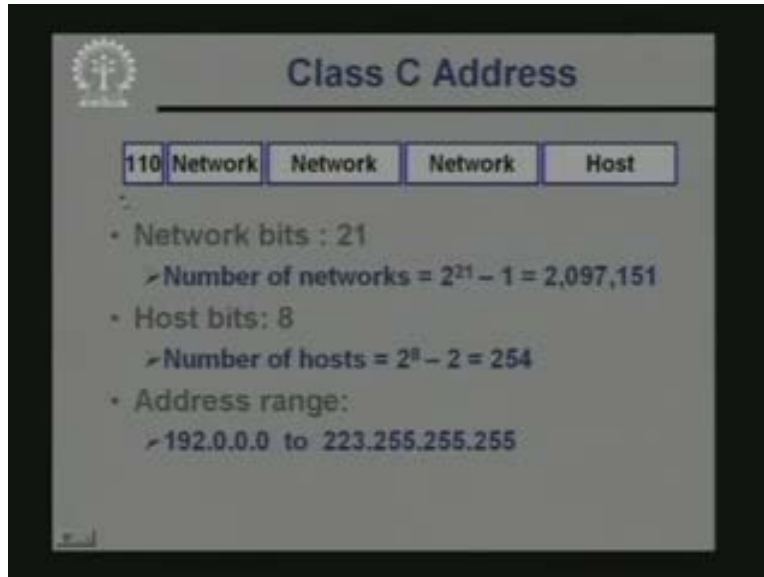
(Refer Slide Time: 39:25)



Now class B belongs represents the network which are medium in size; smaller than class A, but larger than class C we will see later. In class B the division between network and host is like this this. Address starts with 1 0, so just by looking at the first few bits you can identify class A and class B. The next 14 bits represent the network and the last 16 bits represent the host. So total number of networks will be 2 to the power 4 again 1 less than that 16383 and total number of hosts will be last 16 bits 2 to the power 16 take out the all zero and all one combination it is 65534. And if you just put all zeros and all ones and convert it to dotted decimal notation you will see that the range of address is that comes here is 128 000 up to 191, 255, 255, 255. This is the range of addresses in class B

networks. Now class C network represents the ones which are smallest in size for most purposes class C networks are sufficient for our purpose. There the number of computers is host in a network can be up to 254. Now let us see the break up.

(Refer Slide Time: 40:55)

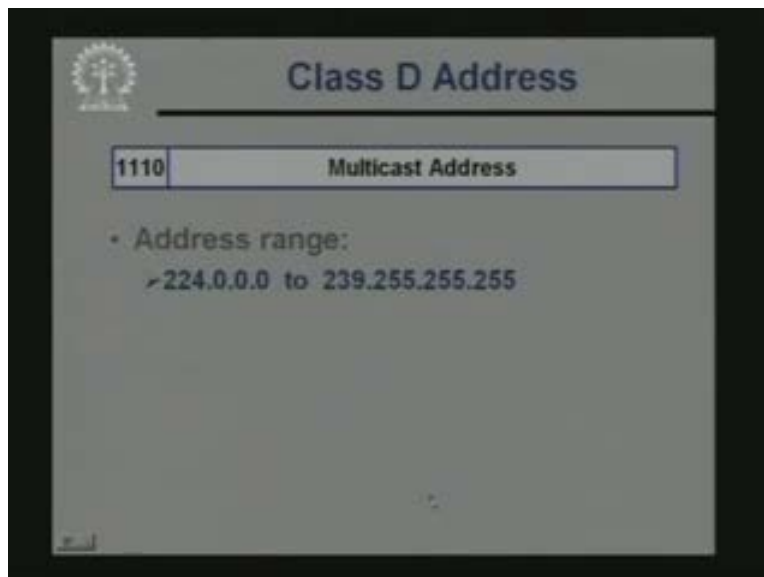


The slide, titled "Class C Address", features a logo in the top left corner. It displays a bit breakdown of a Class C address: "110" followed by three boxes labeled "Network" and one box labeled "Host". Below this, it lists the following details:

- Network bits : 21
  - Number of networks =  $2^{21} - 1 = 2,097,151$
- Host bits: 8
  - Number of hosts =  $2^8 - 2 = 254$
- Address range:
  - 192.0.0.0 to 223.255.255.255

Here the address starts with 110 in order to distinguish it from class A or class B. Next 20 bits represent the network; last 8 bit represents the host. So you can have very large number of class C networks of the order of 2 million. But the number of hosts in each network is only 254 addresses in the range 192.0.0.0 up to 223.255.255.255, they belong to the class C address category.

(Refer Slide Time: 41:36)

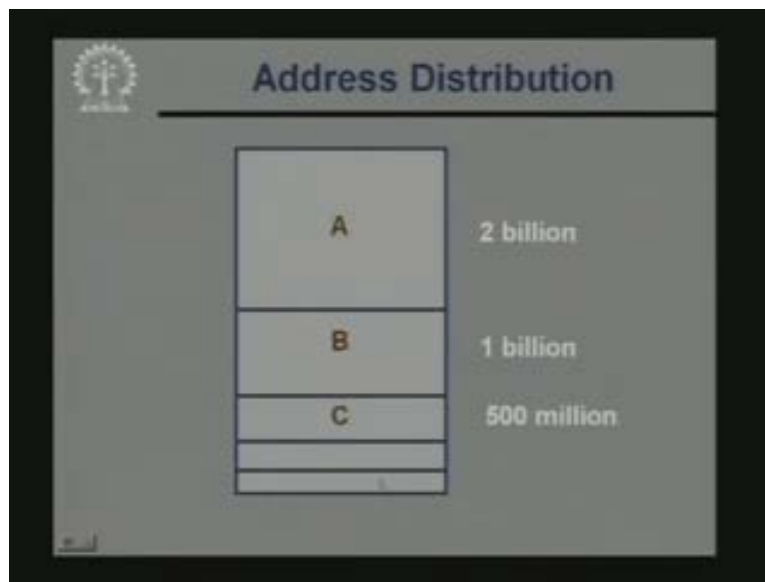


The slide, titled "Class D Address", features a logo in the top left corner. It displays a bit breakdown of a Class D address: "1110" followed by a box labeled "Multicast Address". Below this, it lists the following details:

- Address range:
  - 224.0.0.0 to 239.255.255.255

Now lastly is class D address. Well I am not going the detail of this now. The class address is will start with 1110 and after that whatever you specify here this will identify the address of a group. This is sometimes called a multicast address so depending upon what is the group address I am giving. The packet will be broadcast to all members of that group. This is the idea, so address range is this. Now you see just by looking at IP address you can identify which address category the address belongs to. Given an IP address, you look at only the first few bits of the address the rule is very simple. If the first bit is 0, if it is zero then you can it is class A. If it is 10 then you can say it is class B and if it is 110 then you can say it is class C. There is no ambiguity; just the first few bits uniquely identify the address classes. Depending on the bits the routers or the intermediate nodes can easily identify the address classes and accordingly perform or take the routing decisions. Now in terms of the number of addresses in the whole 2 to the power 32 bit address space of an IP address. Let see how much this classes A, B or C consume. See in class A the first bit starts with 0. So we are taking away half of the total addresses.

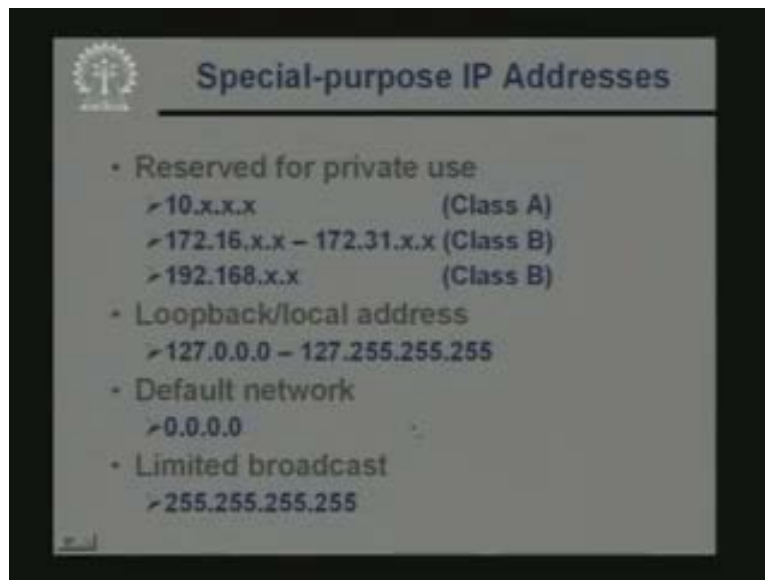
(Refer Slide Time: 43:47)



So among the total 2 to the power 32 or approximately 4 billion addresses, the first two billion addresses are taken up by class A. The next one billion addresses is taken up by class B the next 500 million addresses is taken up by class C and the last 500 million are shared by class D and E. So this gives you an idea about well how these addresses are distributed. Now in this context let me tell you one thing that when this addressing scheme and this internet came up. Then people use to apply for these addresses and this address categories or classes were allotted to them. Now realistically speaking a class A network can have up to 16 million hosts. But realistically speaking very you just think of the practical scenario.

Suppose an ISP internet service provider has obtained a class A address. But it is very unlikely that the number of you can subscribers or customers are in the range of 16 million. It is typically much less than that. This means that a very large number of these address are actually wasted. Someone has grabbed an address class is not allowing else to use them and he is wasting a very large chunk of this address. In fact this phenomenon occurs acquires the entire spectrum classes A B C may be all of them. As a result we were facing with a situation today that we are running out of IP address. We do not have much spare IP addresses or available IP networks which are available for fresh deployment. These are problem will have to address.

(Refer Slide Time: 45:48)



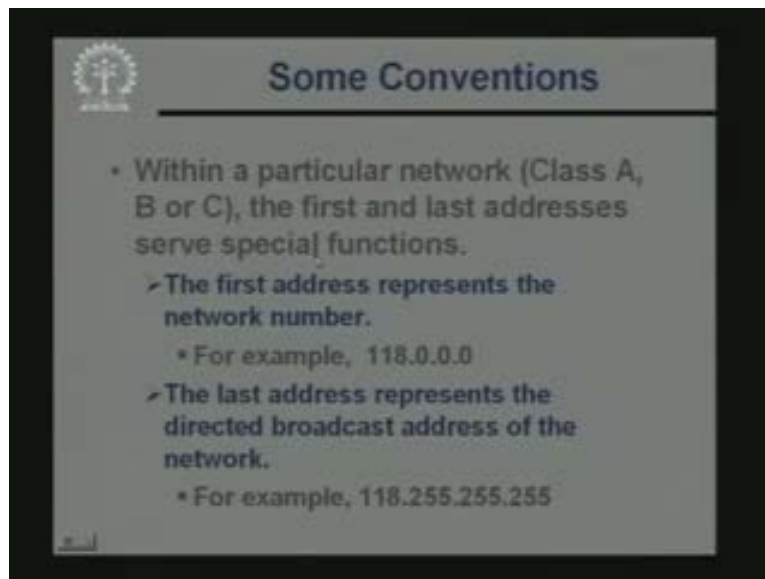
Now, talking about some of this special purpose IP addresses, some of the addresses are used for private networks. A class A address that starts from 10 in the first octet, 10 dot something this is a private class A network. Similarly a class B network that starts with 172.16 up to 172.31, these 16 class B networks are also private and 192.168, this is also class B network this is also private. See these private addresses are meant to be used only inside a private network. This means suppose my computer has a private network I cannot communicate with another computer on the internet directly. Because the routers on the way will not recognize my address as a valid one.

Private addresses are not meant for global routing. But your question you may ask a question but today most of us are getting connected to the internet. So what is the usefulness of these kinds of private addresses? Well there is usefulness number one thing is that as I had just mentioned that IP address has become a very scarce rare commodity today. You cannot get as many IP addresses you need in today's scenarios. So you may be given only a few IP addresses by your service providers. What you can do then is internally you use all private IP addresses. But at the gateway you use some kind of a proxy server or a network address translator. We shall be discussing these issues later

which will be automatically translating your private address into one of the valid address before the request is sent out in the internet.

In this way you can manage with a few IP addresses. But internally you can have a large number of computers. You can have those private IP addresses given or assigned to them. There are some addresses these are called loop back addresses, these are actually not for the purpose of communicating between two machines loop back addresses are meant. Suppose you have a computer, you have two processes running on the computer suppose the processes want to communicate among themselves. Then use a loop back address which means that the packet will not go out of this computer. It will remain within this computer and not necessary block the network outside. Default network, is a default network typically the same network where you belong to and all ones 255.255.255.255; this is a limited broadcast address which typically represents broadcast to all machines on the LAN where you are in.

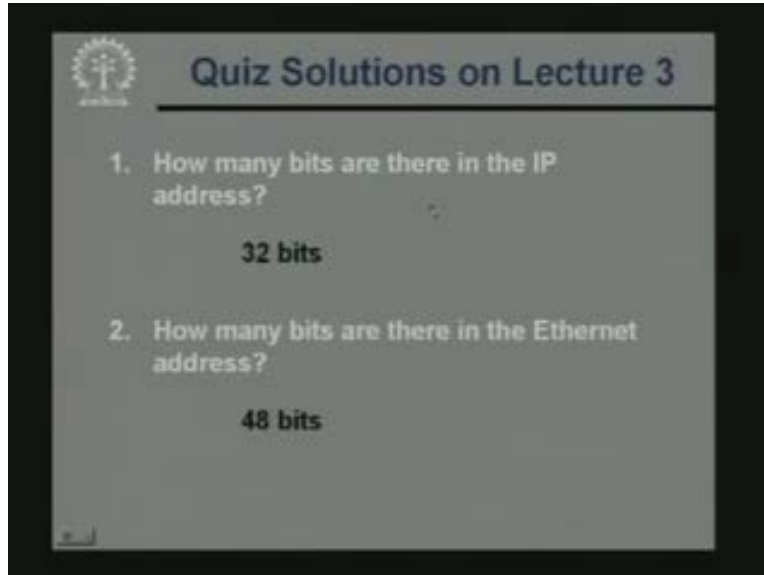
(Refer Slide Time: 49:20)



And some conventions you also follow that within a particular network the first and last addresses are special functions. The first address for example 118.0.0.0 is the first address this represents the network number. So this cannot be used as the host number and the last address which ends with 255. This represents a directed broadcast address to this network 118.0.0.0. So if you have an address like this, this will go to all computers which are located in this network 118.0.0.0. So for this purpose the number of hosts is actually too less than the total possible of addresses; this I have mentioned. So with this we come to the end of today's lecture. Now let us very quickly go through the solutions of the questions which we have posed in our lecture. Then we shall represent some quiz questions for today's lecture as well. So solutions to quiz questions on lecture 3.



(Refer Slide Time: 50:37)

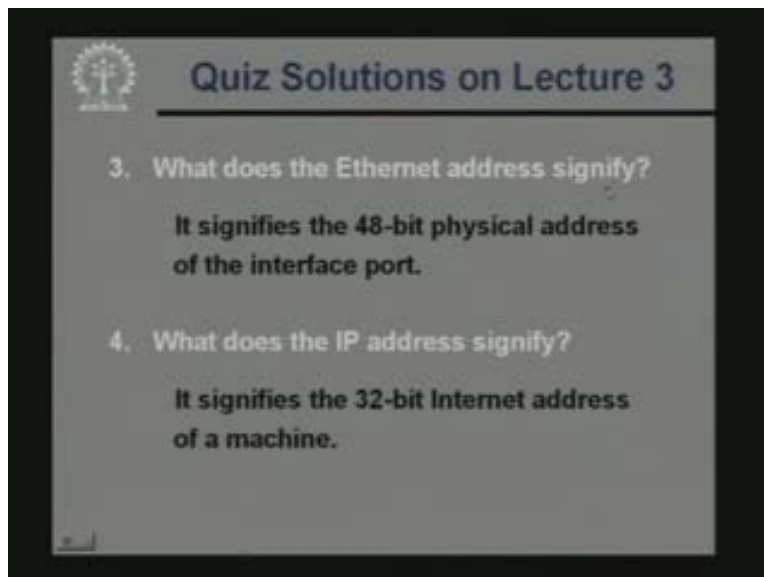


The first question says how many bits are there in the IP address. Well IP address is a 32 bit quantity; obviously the answer will be 32.

How many bits are there in the Ethernet address?

This answer is also fairly straight forward Ethernet address is a 48 bit quantity so the answer is 48.

(Refer Slide Time: 50:59)

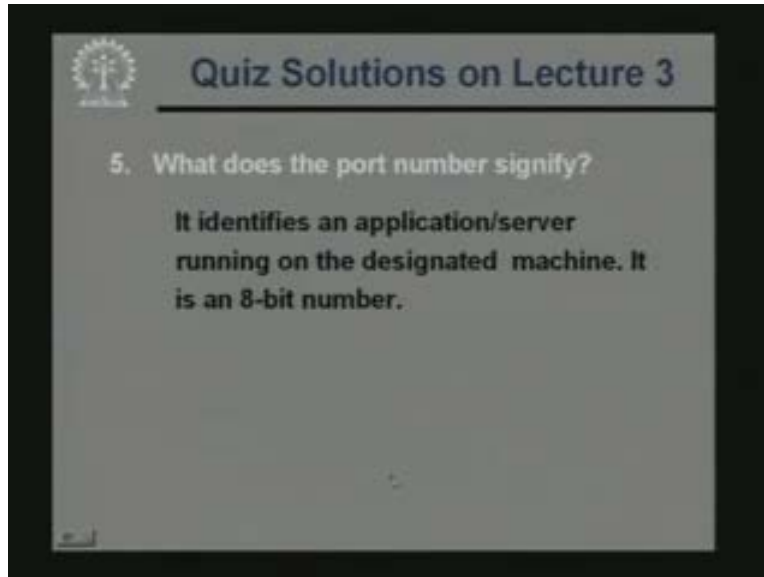


What does the Ethernet address signify well I have mentioned that Ethernet address is representative of the network interface card? So whenever you give the 48 bit Ethernet address, it actually identifies the physical address of your interface port which is your

network interface card. So Ethernet address identifies a particular network interface card which sits on a particular computer. So this is the answer, it signifies the 48 bit physical address of the interface port.

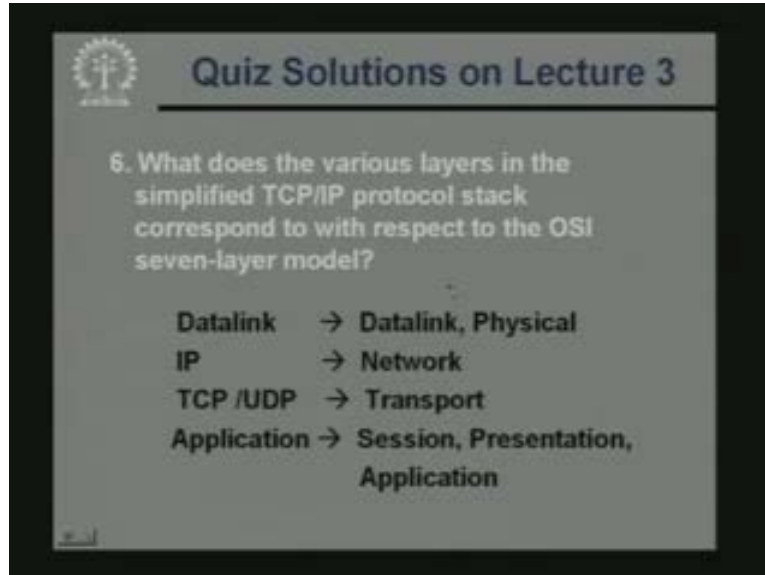
What does the IP address signify? Well IP address signifies the 32 bit internet address of a machine. So I mentioned that a computer can have several addresses Ethernet address at the level of the physical and data link layer. It can have an IP address at the level of the network layer. So the network layer protocol only looks at the IP address portion.

(Refer Slide Time: 51:57)



What does the port number signify? Well this was also discussed in the previous lecture. So a port number is an entity which works at the transport layer level. So at this layer level two application programs on two machines they are communicating among themselves and port number will specify the two programs on the two machines which are talking among themselves. So it identifies an application or a server program running on the designated machines on the two sides it is an 8 bit quantity.

(Refer Slide Time: 52:35)



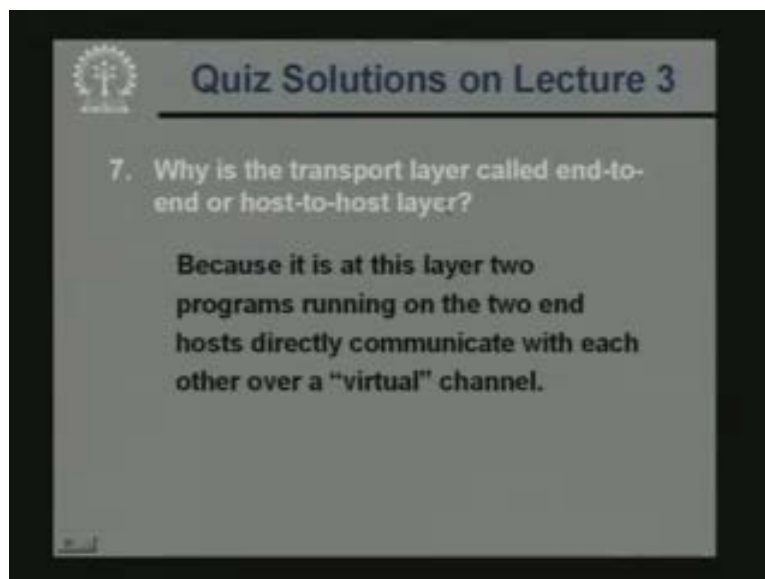
The slide features a logo in the top left corner and the title "Quiz Solutions on Lecture 3" in the top right. The main content is a question and its corresponding answers.

**6. What does the various layers in the simplified TCP/IP protocol stack correspond to with respect to the OSI seven-layer model?**

**Datalink → Datalink, Physical**  
**IP → Network**  
**TCP /UDP → Transport**  
**Application → Session, Presentation, Application**

What does the various layers in the simplified TCP IP protocol stack correspond to with respect to the OSI seven layer models? This also I discussed in the TCP IP suite. Whatever we refer to as the data link model actually is a combination of datalink and the physical layer model in the OSI. The IP layer is the network layer equivalent in OSI, TCP or UDP are the transport layer protocols and whatever we say the application layer. They may be combinations of session presentation and application. So this is how correspondence between TCP IP 4 layer protocol suites and the OSI 7 layer protocol suite corresponds to.

(Refer Slide Time: 53:24)



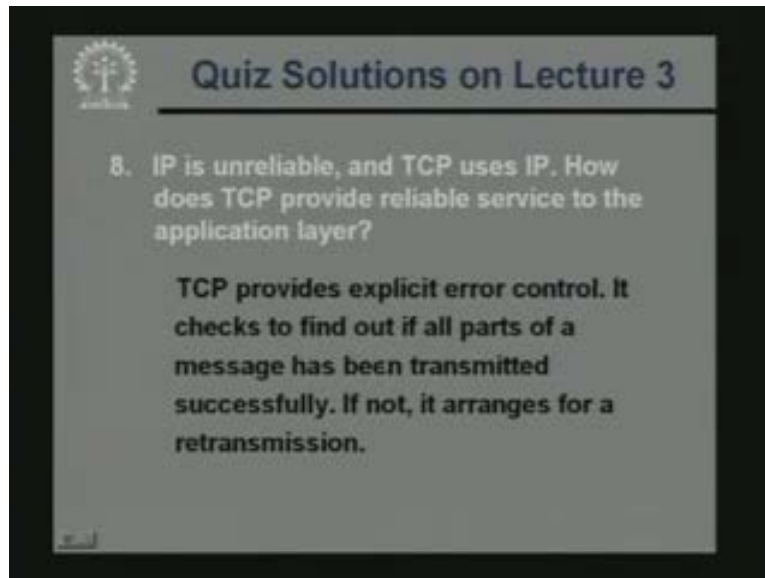
The slide features a logo in the top left corner and the title "Quiz Solutions on Lecture 3" in the top right. The main content is a question and its answer.

**7. Why is the transport layer called end-to-end or host-to-host layer?**

**Because it is at this layer two programs running on the two end hosts directly communicate with each other over a "virtual" channel.**

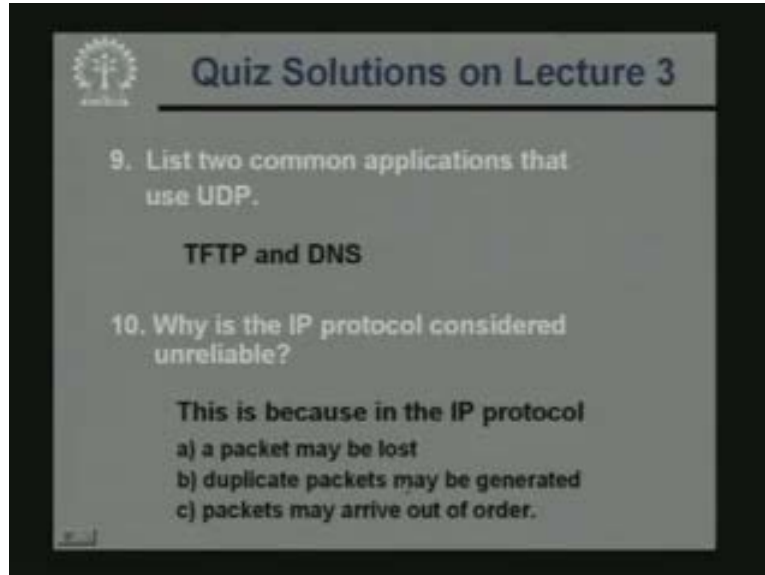
Why is the transport layer called end to end or host to host layer? This is so called because it is at the transport layer where the two programs running on the two ends directly communicate with respect to over a virtual channel. So it is at this layer, the two entities in the two sides treat the intermediate network as a true black box. That is why this is called an end to end or a host to host layer.

(Refer Slide Time: 53:52)



Well IP is unreliable and TCP uses IP. IP how does TCP provide reliable service to the application layer? Well it is true that IP is unreliable datagram is delivery is not guaranteed. But TCP explicitly provides error control. It explicitly keeps track of which portions of an original message have been correctly received and which portion have not been received. If a part has not been received and explicit request is sent back to send back that junk. In this way TCP provides reliability in terms of transmission this is what is mentioned here.

(Refer Slide Time: 54.41)



The slide is titled "Quiz Solutions on Lecture 3" and features a logo in the top left corner. It contains two quiz questions and their solutions. Question 9 asks for two common applications that use UDP, with the answer being TFTP and DNS. Question 10 asks why the IP protocol is considered unreliable, with the answer being that it does not check for errors, leading to packet loss, duplicates, and out-of-order delivery.

**Quiz Solutions on Lecture 3**

9. List two common applications that use UDP.

**TFTP and DNS**

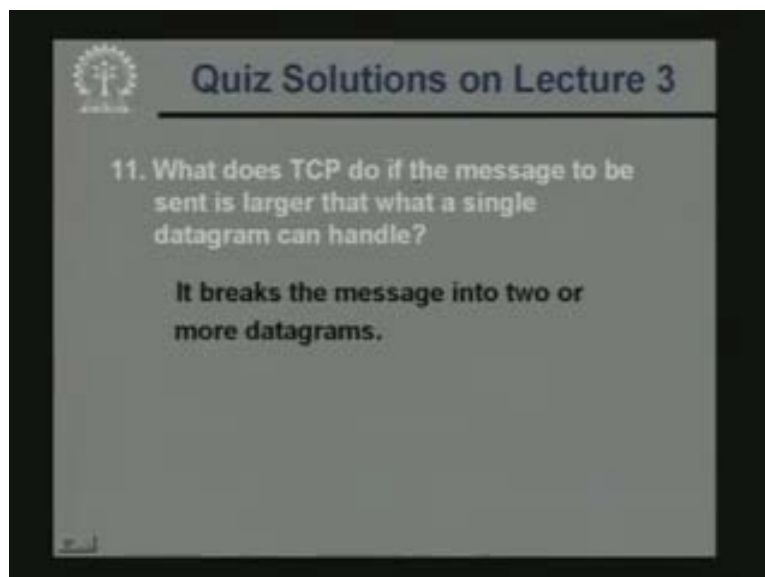
10. Why is the IP protocol considered unreliable?

**This is because in the IP protocol**

- a) a packet may be lost
- b) duplicate packets may be generated
- c) packets may arrive out of order.

List 2 common application that uses UDP. Well trivial FTP and the domain name system DNS. These are 2 protocols which use UDP rather than TCP at the transport layer level. Next question why is the IP protocol considered unreliable? Because IP protocol does not check for any error, a packet may be lost duplicate packets may be get generated due to time out and retransmission and packets may also arrive out of order because packets can follow different paths.

(Refer Slide Time: 55:17)



The slide is titled "Quiz Solutions on Lecture 3" and features a logo in the top left corner. It contains one quiz question and its solution. Question 11 asks what TCP does if the message to be sent is larger than what a single datagram can handle, with the answer being that it breaks the message into two or more datagrams.

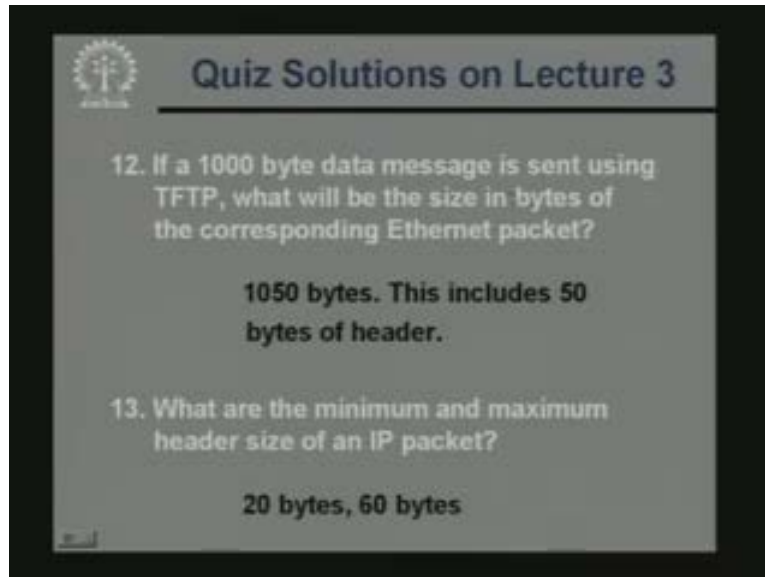
**Quiz Solutions on Lecture 3**

11. What does TCP do if the message to be sent is larger than what a single datagram can handle?

**It breaks the message into two or more datagrams.**

What does TCP do at the message to be sent in the larger than what a single datagram can handle? Obvious the TCP layer will be breaking up the message into smaller packets and sending them to the IP layer for transport. It will be breaking the message into smaller packets or datagrams

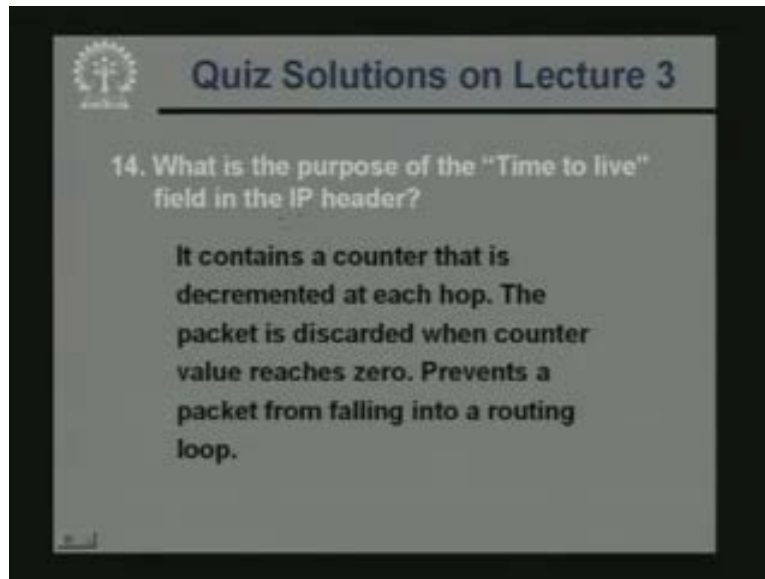
(Refer Slide Time: 55:37)



Well if a 1000 byte data message is sent using TFTP. What will be size in bytes of the corresponding Ethernet packet? Well here if you just remember the example we have discussed in our pervious lecture we had seen that in the TFTP protocol. A total of 50 bytes of header is getting added up to the Ethernet layer level because before the packet can actually delivered. So if the data message is 1000 bytes, the total bytes that are actually transferred 1000 and 50.

What are the minimum and maximum header sizes of an IP packet? Minimum depends on the essential fields. It is twenty bytes you know maximum depends on the size of the header length field. It can be maximum 15, it represent the number of 32 bit chunks in the header. So 15 means 15 into 4 it would become 60. So the range is 20 bytes minimum, 60 bytes maximum.

(Refer Slide Time: 56:41)



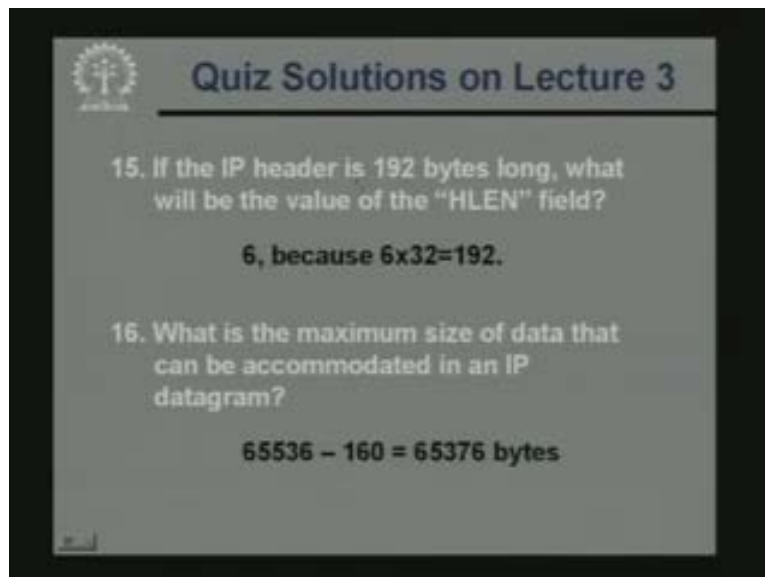
The slide features a logo in the top left corner and the title "Quiz Solutions on Lecture 3" in the top right. The main content is a quiz question and its solution.

14. What is the purpose of the "Time to live" field in the IP header?

**It contains a counter that is decremented at each hop. The packet is discarded when counter value reaches zero. Prevents a packet from falling into a routing loop.**

What is the purpose of the time to live? This I have mentioned time to live field is actually a counter which gets decremented as the packet flows from one node to the next. Now if the count value reaches 0, the packet is discarded. This field is prevent a datagram from falling into a loop.

(Refer Slide Time: 57:03)



The slide features a logo in the top left corner and the title "Quiz Solutions on Lecture 3" in the top right. The main content is two quiz questions and their solutions.

15. If the IP header is 192 bytes long, what will be the value of the "HLEN" field?

**6, because  $6 \times 32 = 192$ .**

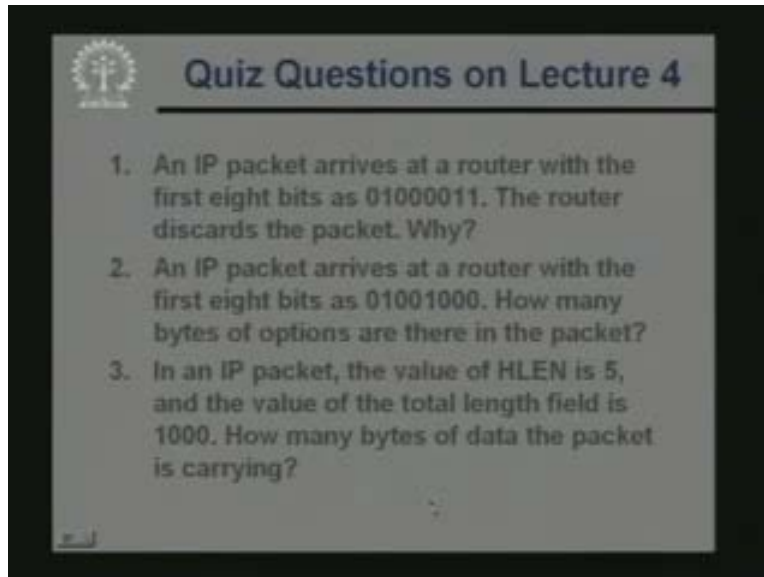
16. What is the maximum size of data that can be accommodated in an IP datagram?

**$65536 - 160 = 65376$  bytes**

If the IP header is 192 bytes long, what will be the value of HLEN field? Well this 192 means actually 6 into 32. So HLEN is 6.

What is a maximum size of data that can be accommodated in IP datagram? See IP datagram total size is 64K 65536 after the minimum 20 bytes is header 160 bits. So the total data bits you can have maximum is 65376 bytes. So now lets us very quickly look at today's questions.

(Refer Slide Time: 57:43)

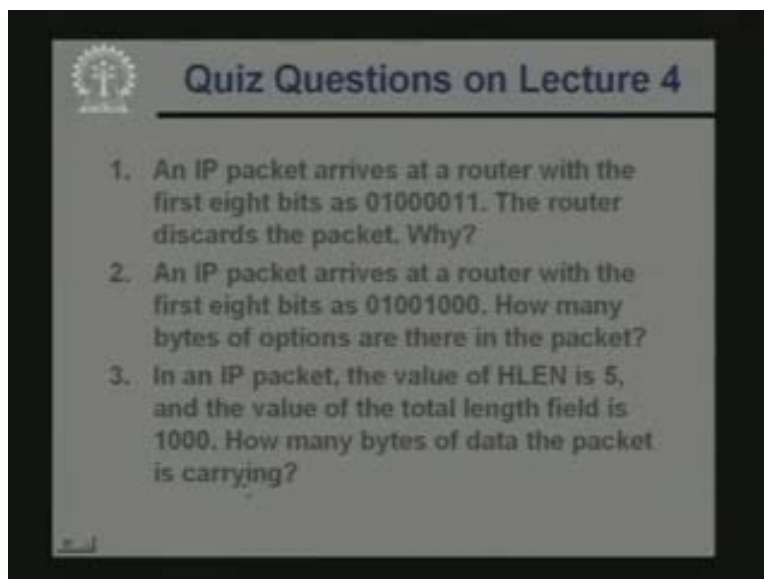


The slide is titled "Quiz Questions on Lecture 4" and features a logo in the top left corner. It contains three numbered questions:

1. An IP packet arrives at a router with the first eight bits as 01000011. The router discards the packet. Why?
2. An IP packet arrives at a router with the first eight bits as 01001000. How many bytes of options are there in the packet?
3. In an IP packet, the value of HLEN is 5, and the value of the total length field is 1000. How many bytes of data the packet is carrying?

An IP packet arrives at a router with first 8 bits as this. The router discards the packet why an IP packet arrives with the first 8 bits as this combination. How many bytes of options field are there in the packet? In an IP packet the value of the header length is 5 and total length is 1000. How many bytes of data are there in the packet?

(Refer Slide Time: 58:06)



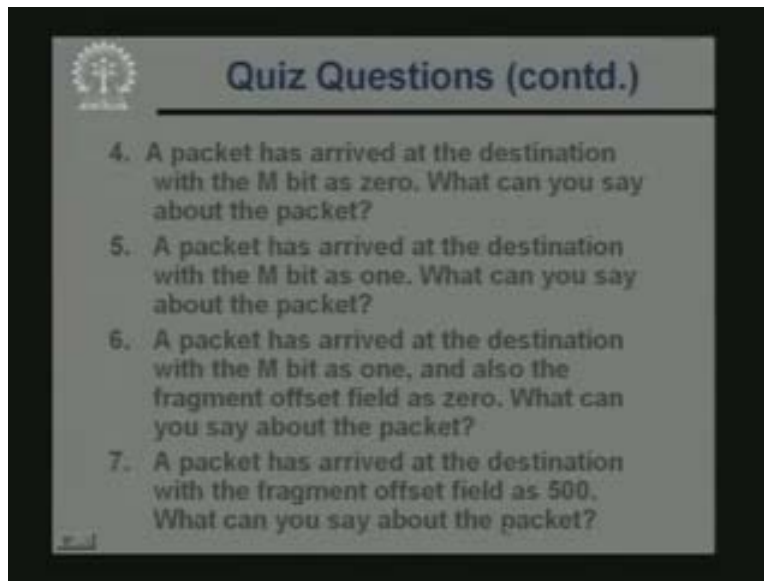
The slide is titled "Quiz Questions on Lecture 4" and features a logo in the top left corner. It contains three numbered questions:

1. An IP packet arrives at a router with the first eight bits as 01000011. The router discards the packet. Why?
2. An IP packet arrives at a router with the first eight bits as 01001000. How many bytes of options are there in the packet?
3. In an IP packet, the value of HLEN is 5, and the value of the total length field is 1000. How many bytes of data the packet is carrying?



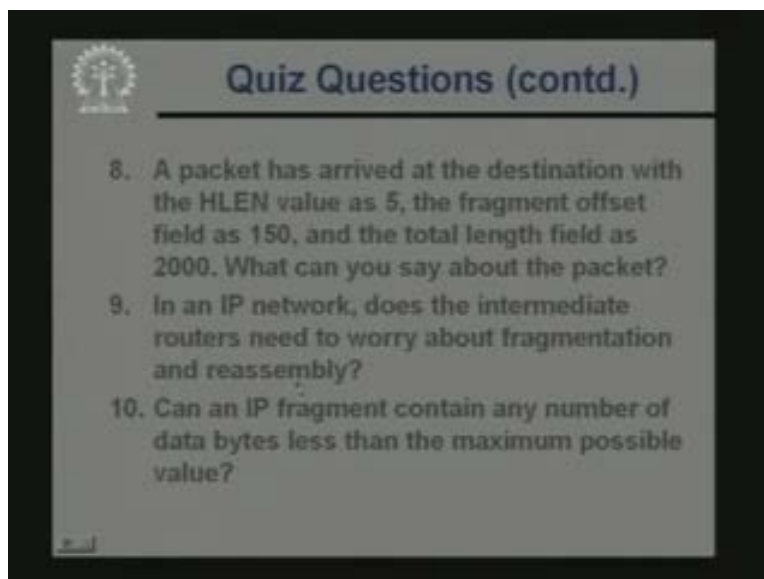
A packet arrives with the M bit as 0. What can you say about the packet? A packet arrives with M bit as 1. What can you say about the packet? A packet arrives with the M bit on one and the fragment offset is 0. What can say about the packet? A packet arrives with the fragment offset as 500. What can you say about the packet?

(Refer Slide Time: 58:30)



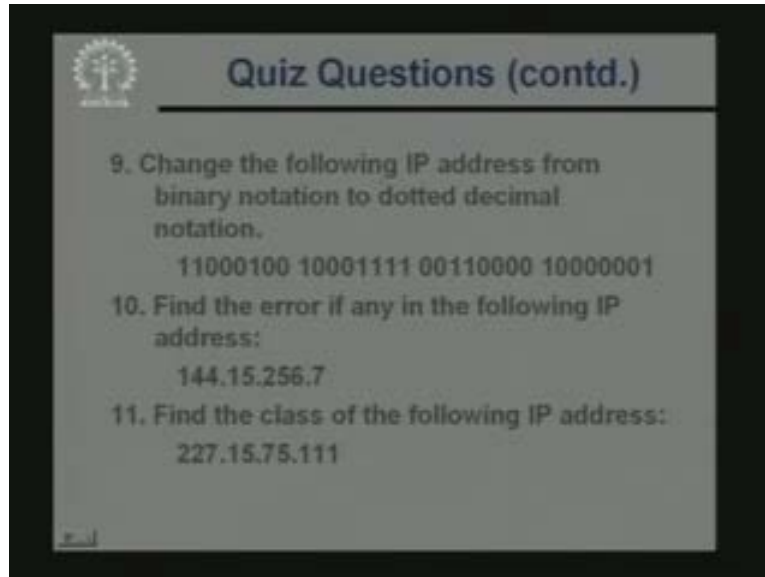
A packet arrives with header length 5, fragment offset 150 and the total length 2000. What can you say about the packet? In an IP network does the intermediate routers need to worry about fragmentation and reassembly.

(Refer Slide Time: 58:41)



Can an IP fragment contain any number of data bytes less than the maximum possible value?

(Refer Slide Time: 58:50)



A slide titled "Quiz Questions (contd.)" with a logo in the top left corner. It contains three questions:

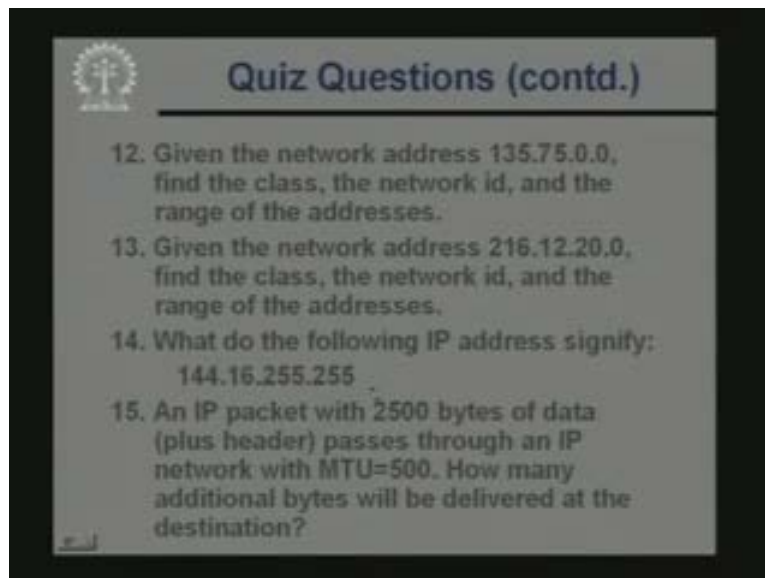
9. Change the following IP address from binary notation to dotted decimal notation.  
11000100 10001111 00110000 10000001

10. Find the error if any in the following IP address:  
144.15.256.7

11. Find the class of the following IP address:  
227.15.75.111

Change the following IP address from binary notation to the dotted decimal notation, very simple. Find the error if any in the following IP address is in the dotted decimal notation. Find the class of the following IP address, this is the IP address.

(Refer Slide Time: 59:06)



A slide titled "Quiz Questions (contd.)" with a logo in the top left corner. It contains three questions:

12. Given the network address 135.75.0.0, find the class, the network id, and the range of the addresses.

13. Given the network address 216.12.20.0, find the class, the network id, and the range of the addresses.

14. What do the following IP address signify:  
144.16.255.255

15. An IP packet with 2500 bytes of data (plus header) passes through an IP network with MTU=500. How many additional bytes will be delivered at the destination?

Given the network address these find the class network id and the range of addresses. Similarly for another address, for this address find the class network id and the range. What do the following IP addresses signify? 144.16.255.255 and IP packet with 2500 bytes of data plus header passes through a network with and MTU 500 bytes. How many additional bytes will be delivered? So with this we will come to the end of today's lecture. See you next time.