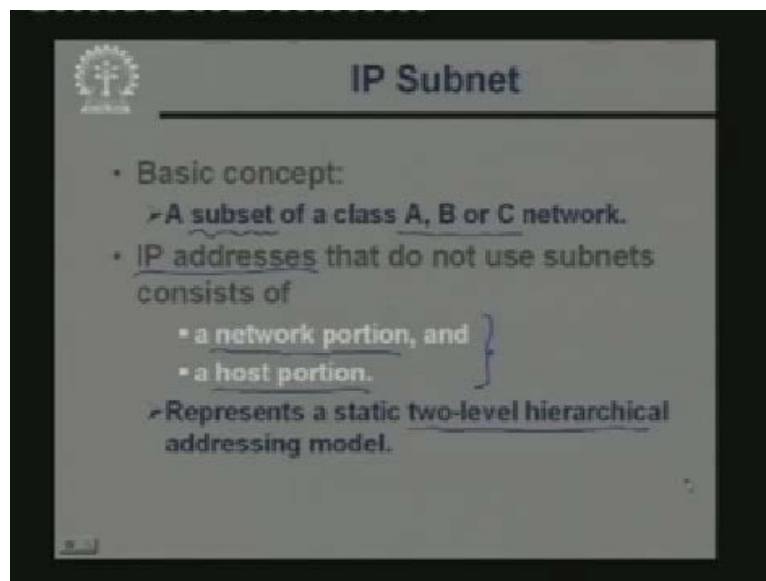


**Internet Technology**  
**Prof. Indranil Sengupta**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**  
**Lecture No #06**  
**IP Subnetting and Addressing**

(Not audible: (00:46)) Now, we shall be starting our discussion on IP addressing and routing. Now if you recall what we have discussed in our last few lectures, we had looked at the TCP IP protocol suite. We had looked at the basic functionalities of the IP TCP and the UDP protocols specifically. We had mentioned that the IP protocol is responsible for the delivery of packets from a source to a destination through a number of intermediate nodes which are typically routers. So we shall today look at some more details about how this addressing at the level of IP is achieved. So IP subnetting and addressing is the topic of our discussion today. So we start with something called IP subnetting. Well we talked about IP addresses in our classes; we talked about the different address classes in IP A B C which are usually used for point to point, communication over IP. But we shall today first look at a concept which is known as subnetting and we shall see how this use of subnets or subnetting can allow us to have more efficient management of the available IP address space.

(Refer Slide Time: 02:17)



So IP subnet, the basic concept is that well you are already familiar with the IP classes A, B and C network. So a subnet you can very roughly define as a subset of one of the address classes either class A, class B or class C network. So if you a standard IP network and if you somehow make some subsets of the network, for example I split one larger network into 4 smaller subnetworks, then each of the subnetworks are called subnets. So this is the basic concept of subnet. Now conventionally when you use IP addresses without any subnets then the addresses consists of two components, as you know the first component identifies the network and the second component identifies the host. And this obviously represents a two-level hierarchy. So two-level hierarchical addressing model is used in the conventional IP addressing.

(Refer Slide Time: 03:30)

**IP Subnet (contd.)**

- IP subnets introduces a third level of hierarchy.
  - a network portion ✓
  - a subnet portion ✓
  - a host portion ✓
- Allow more efficient (and structured) utilization of the addresses. ✓
- Uses network masks.
  - Natural / Default network masks. ✓
  - Custom / Subnet network masks. ✓

The diagram illustrates the three levels of hierarchy: a large box labeled 'Net' (Network portion), a smaller box labeled 'Host' (Host portion) nested within the 'Net' box, and a third, shaded box nested within the 'Host' box, representing the 'subnet portion'.

But when you are talking about subnets what we are actually doing is that we are introducing another level in the hierarchy. We have the network portion; we have the host portion as it is. But there is a third portion that comes in this is called the subnet portion. Now the concept is that in conventional IP addresses there are two portions one portion identifies the network, the other portion identifies the host. Now, in subnets the basic concept is that the number of bits which are available for addressing the host. This is further subdivided into two parts. So one of these parts we call as the subnet portion and the remaining smaller part is now used to address the host. So these three levels of hierarchy net subnet and host this is characteristic of the IP subnetting process and we shall see that using subnets we can have more efficient utilization of the address spaces.

Now in order to have IP subnet we use something called address masks. This address mask is basically a bit pattern a pattern of zeros and ones which will tell us in an IP address which portion of the address actually represents the network and which portion of the address actually represents the host. Now there are two kinds of network mask you can have. You can see these one is the natural or the default network mask which are representative of the conventional class A, B, C networks. But the other one is this is this can be defined as per the user requirements. This is custom or subnet network mask. These two kinds of mask we can define and we shall now see what these two kinds of masks are really.

(Refer Slide Time: 05:42)

The slide, titled "Natural Masks", features a logo in the top left corner. It contains the following text:

- Network mask **255.0.0.0** is applied to a class A network **10.0.0.0**.
- In binary, the mask is a series of contiguous 1's followed by a series of contiguous 0's.

Below the text, the binary representation of the mask is shown: **11111111 00000000 00000000 00000000**. A blue oval highlights the first eight bits (11111111), with an arrow pointing to the label "Network portion". Another blue oval highlights the remaining 24 bits (00000000 00000000 00000000), with an arrow pointing to the label "Host portion".

We'll first talk about natural mask. Let us take a specific example. Take a class A network say 10.0.0.0, this is the address of a class A network. For this class A network we define a mask as 255.0.0.0. Now this mask if you represent in binary it represents a bit pattern like this. This 255 means a sequence of eight 1s followed by 24, 0s. Now in a mask which is actually a bit pattern, the pattern of the mask is like this that at the beginning you have a sequence of ones, at the end you will have a sequence of zeros. So these zeros and ones cannot be interspersed arbitrarily. The bit pattern will start with a sequence of ones. It will end with a sequence of zeros. Now at the beginning the block of ones will indicate that how many bits of the address actually represents the network number or the network. So in this mask the first eight bits are one this represents that whenever we have an address like this. The first eight bits of this represents the network. This is the network portion and the remaining is the host portion. So a class A network will have a mask of 255.0.0.0 because in a class A network the first eight bits represent the network portion well excluding the special bit at the beginning of course. So this pattern is called the natural mask for class A.

(Refer Slide Time: 07:34)

**Natural Masks (contd.)**

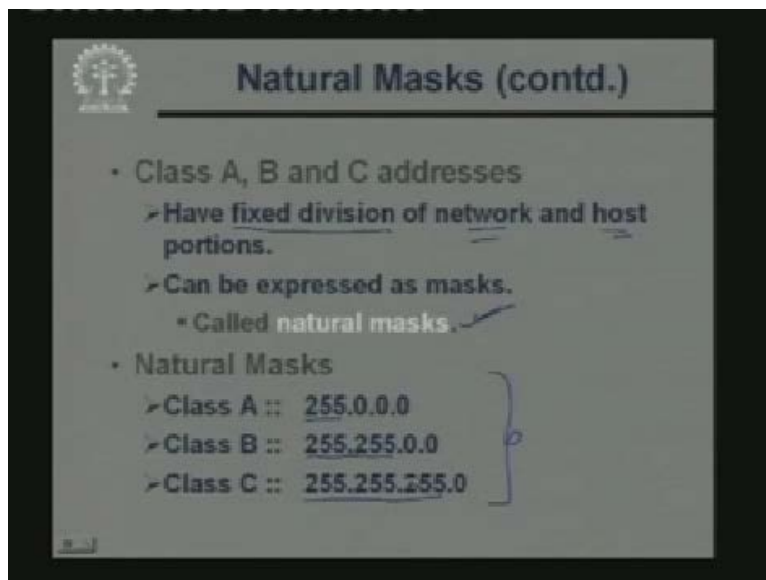
- Provide a mechanism to split the IP address 10.0.0.20 into
  - a network portion of 10, and
  - a host portion of 20.

	Decimal	Binary
IP address:	10.0.0.20	00001010 00000000 00000000 00010100
Mask:	255.0.0.0	11111111 00000000 00000000 00000000
		<u>Network</u> <u>Host</u>

10.0.0.0

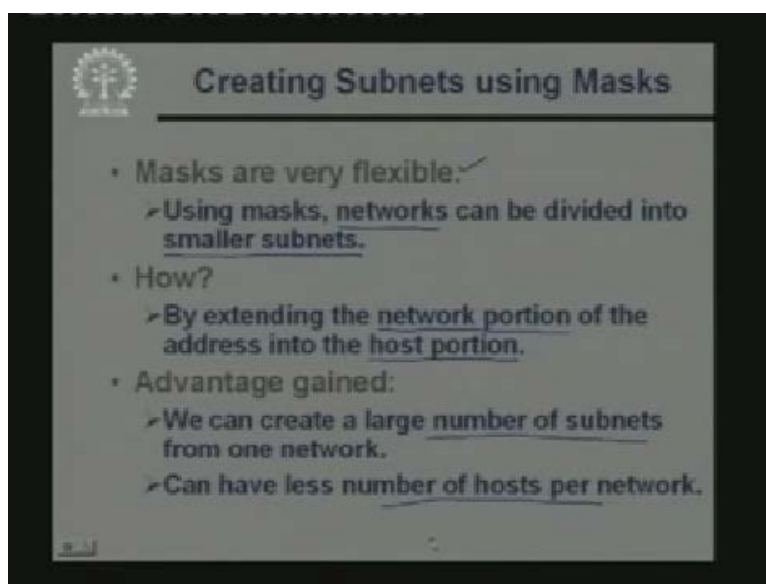
So let us take an example. Suppose you have an IP address of a host as 10.0.0.20, this represents a class A addressing scheme. Now with respect to class A addressing you know this means you have a network portion of 10 remaining 24 bits are host portion of 20. Now in terms of the bit patterns the IP address can be represented like this. 10.0.0.20 but for class A told you the mask will be 255.0.0.0, this represents 8 ones at the beginning followed by 24, zeros. Now actually what will be done by the intermediate internet nodes are the routers is that this IP address and the mask will be bitwise ANDED together. So if you do a bitwise AND since the last 24 bits of the mask are zeros, so the last 24 bits of the result will also be zero. It is only the first eight bits which will come out and will get a result as 10.0.0.0, this will be the result after ANDING and this will indicate the network number. So given any IP address and the corresponding subnet mask any intermediate node can find out the corresponding network address by doing a bitwise ANDING. Because knowing the network address is important because the IP layer software which is running on that node will be responsible for taking a decision where to forward the packet next in order to reach the destination. So knowing the destination network number is important.

(Refer Slide Time: 09:30)



So continuing with natural masks. For class A B C. As you know you have fixed division of the bit patterns representing the network and host, these are called network masks and the network or the natural the natural or the default masks for class A B or C networks are like this. For class A network the first 8 bits represent a network for B the first 16 bits and for C the first 24 bits. So if you look at a mask value like this you know that you are using the default class A, B or C addressing schemes without really having a subnet. A subnet means you are dividing a say for example class A network into smaller subnetworks. But if we have a mask value which goes like this we are not really trying to carry out that kind of a division.

(Refer Slide Time: 10:32)



So now let us see how you can use masks to create subnet. That is the more important or you can say more widely used you can say application of masks; creating subnets out of an IP address. Out of an IP address or out of an IP network. So the first thing is that as I had said using masks is very flexible. Why? Because as per our requirements we can divide a larger network into smaller subnetworks. Well if we can divide a larger network into smaller subnetworks we can possibly make much better utilization of the available address for example. If our institution contains 4 departments, each with certain requirements then we can get one address class and we can divide up into 4 groups. So as to cater to the 4 departments, this is one possibility. Now subnets the basic concept is that what we do here is that we extend the network portion of the address into the host portion.

Well what we mean by saying this is that, for example, in a class A network the first 8 bits represent the network. So what we can say that well not the first 8 bit, let the first twelve bits represent the network and the rest represent the host. So we are taking out 4 bits from the host area and we are appending to the network part. So the 8 bits of the natural mask of class A network gets 4 additional bits from the host portion. We get a 12 bit network part out of that network part 8 bits will be the network and 4 bits will be the sub network. So this is the basic idea. Now the advantage gained is obvious as I just mentioned, we can create a number of subnets which are smaller. It can have a smaller number of networks and which can much better match our requirements our requirement may be like that only we want smaller sub networks.

(Refer Slide Time: 12:52)

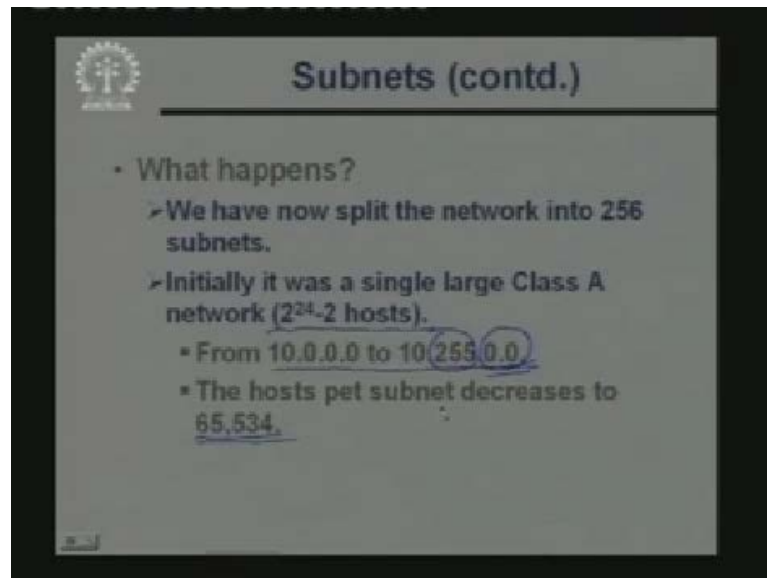
**Example: Subnets**

- Network mask 255.255.0.0 is applied to a class A network 10.0.0.0.
- This divides the IP address 10.5.0.20 into
  - a network portion of 10,
  - a subnet portion of 5, and
  - a host portion of 20.
- The 255.255.0.0 mask borrows a portion of the host space, and applies it to network space.

So let us take an example here. Suppose we have a class A network 10.0.0.0, well for a class A network as we have seen the natural mask would have been 255.0.0.0. But here we are using a mask of 255.255.0.0. What does that mean? We are this mask corresponds to 16 leading ones. 16 leading ones means in the class A network 10.0.0.0, the first 8 bits represent 10. But the next 8 bits also you are borrowing from the host address space. Those next 8 bits you will be representing the sub network or the subnet. So if you take a specific IP address for example 10.5.0.20, this address represents three different things depending on the mask.

The first byte will indicate the network portion, the second byte will indicate the subnet portion and the last 16 bits will indicate the host portion. Now the network mask can be used to identify this because just by looking at this address the first bit will tell you that this is a class A network. So class A network means the first 8 bits will represent the network. Looking at the network mask you see that well you have another 8 bits in the network part. So the next 8 bit will obviously correspond to the sub network and the remaining part will be the host.

(Refer Slide Time: 14:34)



The slide is titled "Subnets (contd.)" and contains the following text:

- What happens?
  - We have now split the network into 256 subnets.
  - Initially it was a single large Class A network ( $2^{24}-2$  hosts).
    - From 10.0.0.0 to 10.255.0.0
    - The hosts per subnet decreases to 65,534.

So using the subnets what we have actually done? That we had a very big class A network. But by borrowing those 8 bits, in the second byte of the address we have a effectively split the total class A network into 256 smaller sub networks. Depending on what bit combination we have in the second byte the corresponding sub network will be identified. The first byte will be identifying a class A network. The next byte will be identifying one sub network inside that particular class A network and the remaining 16 bits will identify a host inside this selected sub network. This is how the hierarchical addressing will be carried out.

So initially we had a large class A network with of the order of 2 to the power 24 hosts, 16 million address range was from 10.0.0.0 up to 10.255.0.0. Well but now what we are having using mask of 255 out here we are only restricting ourselves to the last 16 bits. So we are basically having the subnet addresses from 10.0.0.0 up to 10.255.0.0, these are the sub network addresses. Now inside the sub network the last 16 bits will indicate the host number. So it will be 2 to the power 16 minus 2 or 65534. So now we can have potentially 256 sub networks each having well approximately 65000 hosts instead of one single big network with 16 million hosts. So this, the advantage we are gaining we can have much better management of a large network.

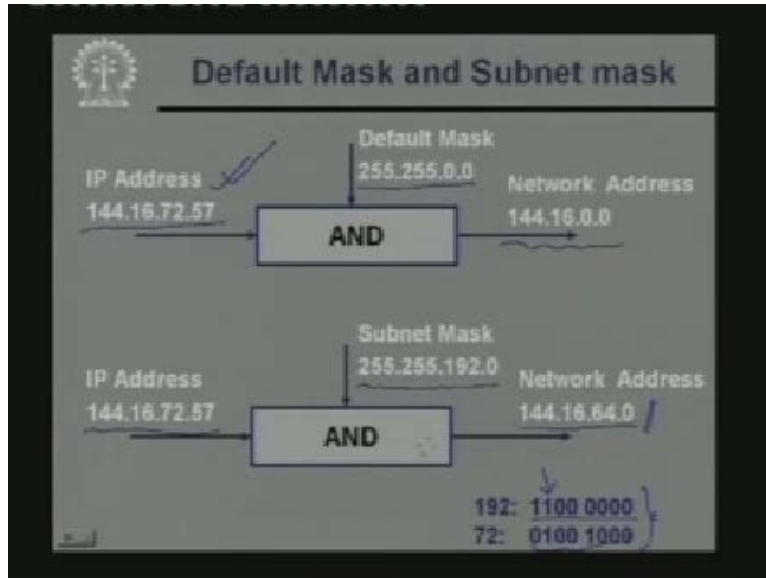
(Refer Slide Time: 16:35)

Decimal	Binary
IP address: <u>10.5.0.20</u>	00001010 00000101 00000000 00010100
Mask: <u>255.255.0.0</u>	11111111 11111111 00000000 00000000
	<u>Network</u> <u>Subnet</u> <u>Host</u>

Now just to look at an example again that same example IP address 10.5.0.20 and this is the mask 255.255.0.0, so if you expand 10.5.0.20 in binary and write also the mask in binary. So as I told you, the first 8 bits will indicate the network. The next 8 bits will indicate the subnet and the last 16 bits will indicate the host. So just by using the mask you can extract the corresponding bits and you can find out that which a network portion is and which is a subnet portion. The first few bits of the address will identify the address class. Accordingly it will give the network portion looking at the subnet mask. Looking at how many additional bits are gone there you can also extract the subnet of the address and the remaining will be host.

(Refer Slide Time: 17:30)

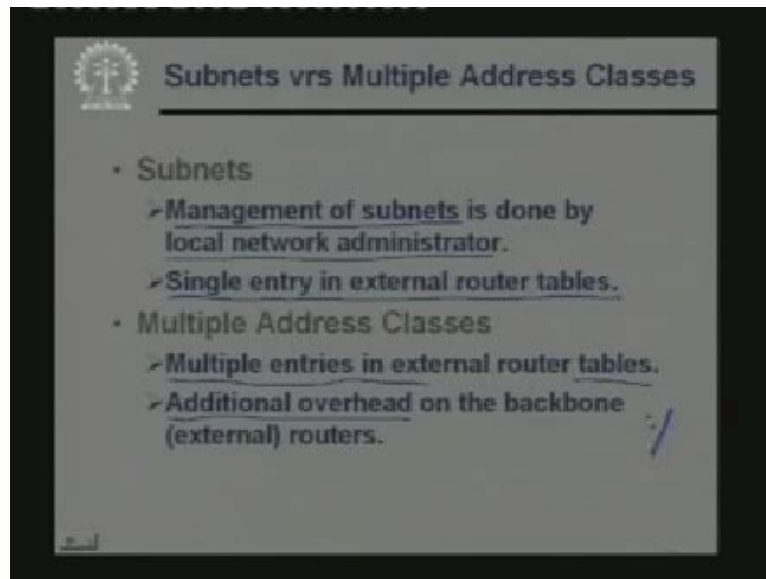




Just to give you an idea well whether you are using default mask or subnet mask whatever the way a router extracts the network address is the same. For example, if you take default mask say you are considering a class B IP address 144.16.72.57, this is a default mask. So the for class B the default mask will be 255.255.0.0, so to get the network address the router will be doing a simple bit by bit ANDING of your IP address with the default mask. So you will be getting 144.16.0.0 as the network address and router can consult its own table to find out where the forward the packet. Next to send the packet to this particular destination network. Now if you are using subnets then you have another scenario. Suppose you have an address like this same address. But now the subnet address is something else subnet mask is 255.255.192.0, 192.0 means 192.0 in binary means 1 1 followed by all 0. So the first two bits of the host you are borrowing.

So if you again do a bit by bit ANDING, so the first 2 bytes 144.16 will come in. But for the last 192 and 72. So here the bit patterns are shown. So if you do a bit by bit ANDING only this particular bit will remain. The others will all become 0, this means 64. So the network address will be 144.16.64.0. So in this way the router can do a bit by bit ANDING of the IP address with the mask whatever is specified to find out the ultimate network or sub network address. So this one thing maybe coming to mind is that well we are doing this ANDING. But who specifies the sub network. The IP address is coming through a router, but who tells the router that this is the particular sub subnet mask you have to use. Well this point we shall be taking up later will show or will see with an example that in a router there is some information about the subnet masks to be used corresponding to the destination addresses of the packets which are coming. There are some rules which are set in the router using the rules you can automatically select the subnet mask to be used.

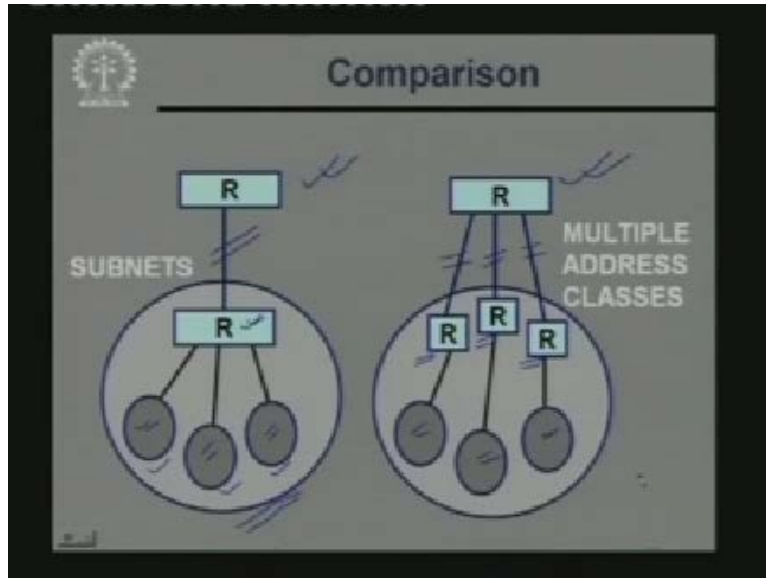
(Refer Slide Time: 20:07)



Now let us address another problem. Well we can use subnets to divide a large network into smaller sub networks. Now if we do that, as you can understand that the management of the subnets will be done by the local network administrator. Because to the external world there is still a single network subnetting is done inside my organization. In order to suit my need but to the outside world our organization still represents a single network, say class B or class C whatever. So if you are using subnets it means you need a single entry in the external router tables well external routers means the routers which are residing outside my organization through which the packets are coming to me. So the other alternative that we can have is multiple address classes. Now instead subnets what you can have suppose you have 4 departments.

Now you can have 4 different Class C addresses and give one to each of the departments. Now there of course it can solve the purpose, but one problem is that now your organization is not in no longer identified by a single network. There are 4 independent networks inside your organization. So with respect to the external router, router will have to keep track of these four different networks. So there will be some additional overheads in the routers with regards to multiple entries in the tables. This is something you have to remember, you can use multiple address classes. But you are not doing justice to the external routers you asking them to work a little more to store more information in the tables. Obviously their operation will become slower.

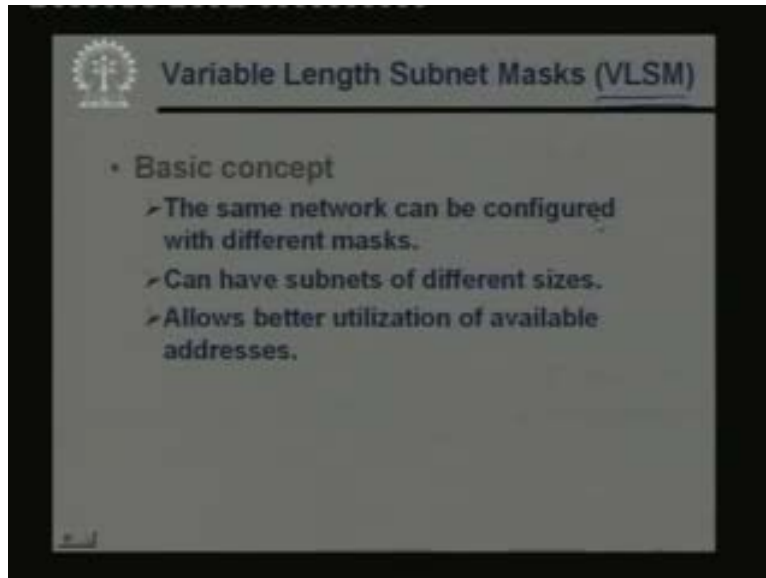
(Refer Slide Time: 22:20)



So pictorially, if you are using subnets then the external router, this is your organization, this circular block is your organization, and there are three departments say. So the external router will be forwarding all packets to your internal organization router it will be identified by a single network and your internal router will be doing subnetting. It will be forwarding the packets to one of the three departments say. But if you are using multiple address classes, this means that inside your organization, there will be three different routers corresponding to the three networks and from the outside world there will be three different links. So obviously the overhead in this external router will be more because it has to keep or maintain more information about the addresses of the networks inside the organization.

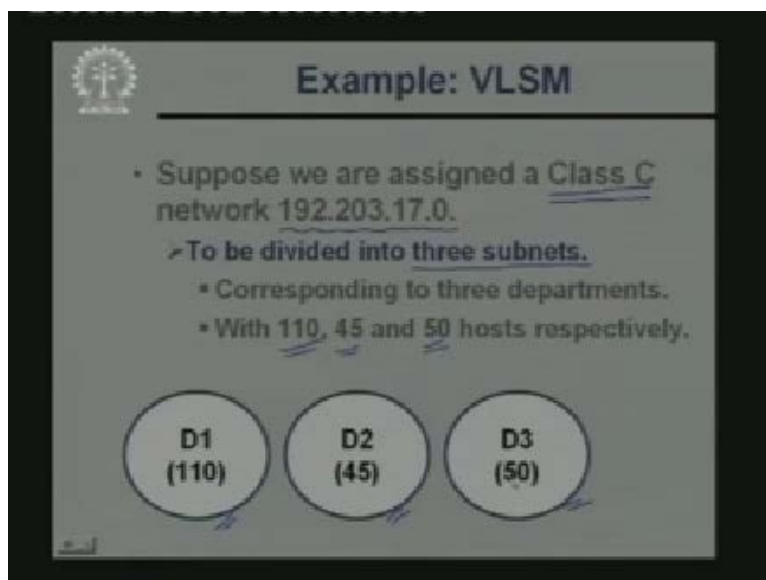
So now let us look at another scheme which has been proposed in order to increase or improve the usability of this concept sub subnets. Well subnets uses masks and once we apply a mask to a network it gets divided into several sub networks. Now the classical mask is fixed for a particular network well what I mean by this statement is that suppose I am using subnet I can apply only one mask to a particular network. For example I use a mask to divide a network into 256 sub networks. But I do not have the flexibility of applying several different masks to the same network in order to further and further split the network into smaller pieces.

(Refer Slide Time: 24:24)



Now this new concept Variable Length Subnet Mask or VLSM addresses precisely this issue. The say is that the same network can be configured with different mask. Unlike the conventional subnetting where only a single mask can be used in a network, by doing this you can subnets of different sizes. This is again unlike the classical subnetting where all the subnets are of the same size. But here we can have one subnet of size 128 another of size 64 another of size 32 and so on. So this obviously this will allow better utilization of the addresses because again coming back to that example of your organization. So all the departments in your organization may not be having a similar requirement. Some maybe requiring more addresses some maybe requiring less. So you can use this concept of VLSM to partition the address in a much more flexible and better way.

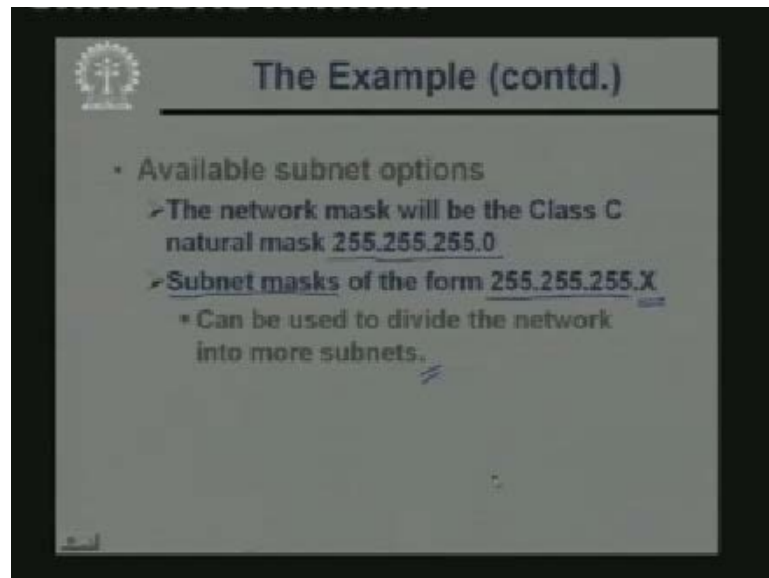
(Refer Slide Time: 25:24)



Let us illustrate the concept of VLSM with the help of an example. Suppose we have an organization and we have been assigned a class C address say 192.203.17.0, this is the class C address we have. Now in a class C address we can potentially have up to 254 hosts. But say

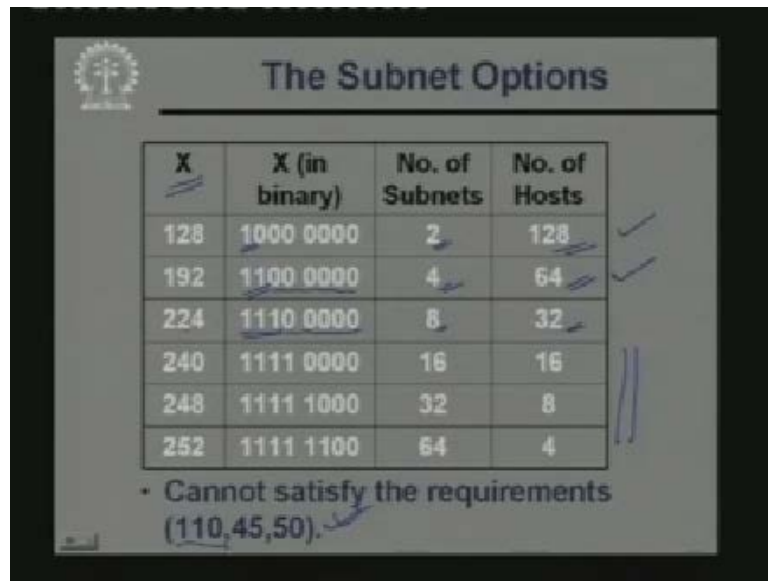
in our organization there are three departments and the requirements corresponding to the three departments are as follows. We want to divide them in to three subnets and the number computers in these three departments are 110, 45 and 50. So as this picture shows there are three departments D1, D2, D3 with requirements which are varying. Now let us explore that whether using simple subnetting can we provide a solution or if not what should be done? So this is the problem we want to solve there are three departments with 110, with 45 and with 50 hosts in them.

(Refer Slide Time: 26:44)



Now let us first look at the conventional subnet option. Now for class C address you know that the natural mask will be 255.255.255.0, now if we are trying to subnet a class C network. So those subnet masks will be of the form the first three will be 255, last byte will be something X. So we are actually borrowing some bits from the host part that X will tell you how bits you are borrowing. So using some non zero value of X with leading ones you can divide the network into subnets. Now let us see that how the different values of X will affect the number of subnets and their sizes.

(Refer Slide Time: 27:33)



X	X (in binary)	No. of Subnets	No. of Hosts
128	1000 0000	2	128
192	1100 0000	4	64
224	1110 0000	8	32
240	1111 0000	16	16
248	1111 1000	32	8
252	1111 1100	64	4

• Cannot satisfy the requirements (110,45,50).

Well, let us look at this table. The first column shows the value of X. The second column shows that number in binary this is decimal this is binary and the third column shows that how many subnets you are breaking into and the fourth column that how many hosts you can have in each subnet. So if X is 128 which means only one leading bit is 1. This means that you are dividing the available 256 space bit space, 256 space into 2 subnets 128 bits. (28:11) So number of subnets is 2 we have 128 bit. If you use two leading ones which means 192 we have 4 subnets and 6 bits for the host we have 6 available bits. This means 64, if you have three leading ones 224, it means we have 8 subnets and we have 5 bits for the host means 32 and so on.

You can divide into subnet in this way. But if you again think of our requirement which we had we wanted to divide the network into 3 chunks 110, 45, 50. None of these values of X will be satisfying our requirements because the first row will not solve because it is dividing into 2 subnets but we need three. The second row will not solve because it is dividing into more than 3. But the sizes of the networks are not sufficient to cater to all of them one of them requires 110. So this conventional subnet will not work. Because conventional subnet whatever value of X you define that will fix the number of subnets you are having and the sizes of the each subnet. Because size of each subnet are constrained to be the same. So now let us see what can be done in this particular scenario.

(Refer Slide Time: 29:36)

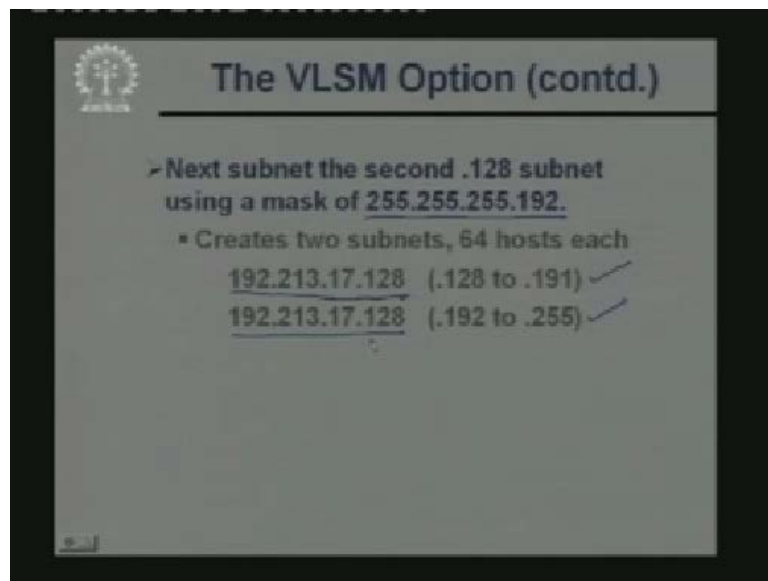
**The VLSM Option**

- Basic concept:
  - First use the mask **255.255.255.128** to divide the network address into two subnets with 128 hosts each.
    - 192.203.17.0 (.0 to .127)
    - 192.203.17.0 (.128 to .255)

256  
110 128 128  
45 64 24 50

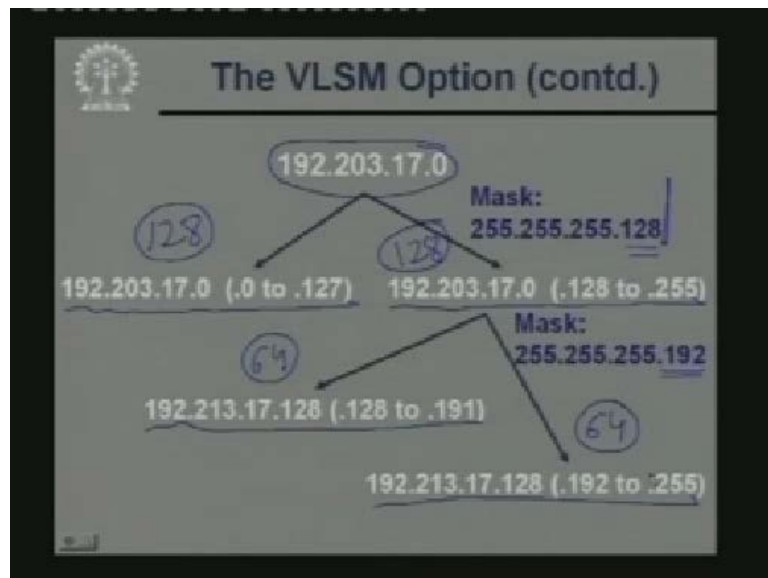
So now we exercise the variable length subnet mask or VLSM option. VLSM option you can think of as some kind of hierarchical subnetting. Instead of doing a subnetting at one level we are doing it in a hierarchical way. Let us see how we are doing it. At the beginning we are dividing the class C networks into two parts 128 each, for that purpose we use the subnet mask 255.255.255.128, this 128 has a single leading one. It will be dividing the class C network 192.203.17 which we had into two sub networks this and this, the first sub network will be having the host addresses ranging from 0 to 127 and the next one from 128 to 255. This is what we do at the first level. Server process effectively we had well we are ignoring that two. Let us call it 256. We had 256 addresses at the first we divide them into 128 each. Now the idea is that one of these 128 is sufficient to cater to our requirement for the first department which was 110. So now what we are trying to do we will further divide this second 128 into 64 and 64. Now if we are able to do this then we can cater to the needs of the other two departments as well 45 and 50. This is the basic concept we are trying to follow. So this is the first level of subnetting we have done to divide into 128 and 128 at the next level the second network.

(Refer Slide Time: 31:32)



We again subdivide, now the second network will be having an address .128 because all addresses will be having that bit 1. Now we use another subnet mask .192 where the next bit is also 1. So now this second sub network of size 128 gets divided up into 64 and 64. The first of which will be having addresses from 120 to 191 and the last 192 to 255. So now let us see diagrammatically how this we have achieved?

(Refer Slide Time: 32:10)

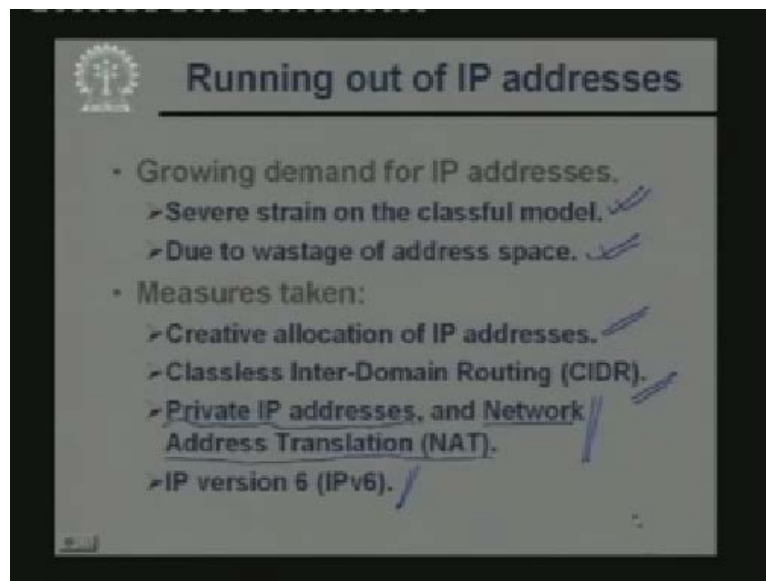


Now this diagram shows the subnetting of the original class C address network. This was the class C which you had originally first we use the mask of this .128 to split up into two networks of 128 each this had a size of 128. This also had a size 128, these were the addresses this is the IP address and this is the address range. This was the address out here.



Now the second subnet we again applied another mask. This time with 192 in the last byte which will allow this network to be divided up into further two sub networks. Like this which will be having a maximum capacity of 64 each. In fact this kind of partitioning is very well solving our problem which we had at hand to cater to the need of the three departments whose sizes of the capacities were 110, 45 and 50. So this VLSM is an option which is available to you. But before using VLSM. You should be careful about one thing. You should be sure about the fact that the routers which you are using they are compatible with the VLSM protocol. Now VLSM is supported by most of the modern router protocol. But some of the older protocols do not support VLSM. So this is something you must remember.

(Refer Slide Time: 34:04)



Running out of IP addresses, now let us talk about a very general and global problem. Talking in a very general way. As I had mentioned that when the internet first evolved this IP addressing scheme was there the address class A, B, C, were formulated. Now at that time when an organization applied for an address class it was given immediately. So if I need one 1000 addresses. I could apply for a class B network and get the entire class B network although the class B network had a capacity of 65000 possibly I am using only 1000 or 2000 of those. So a very large chunk of the available addresses were wasted. So what has happened in the process is that most of the IP addresses have become full or occupied. So other than some of the class C address most of the class B and class A networks are now not available. So now IP address is becoming a very important and rare commodity now a days. Now people are thinking more and more how to better utilize this IP addresses.

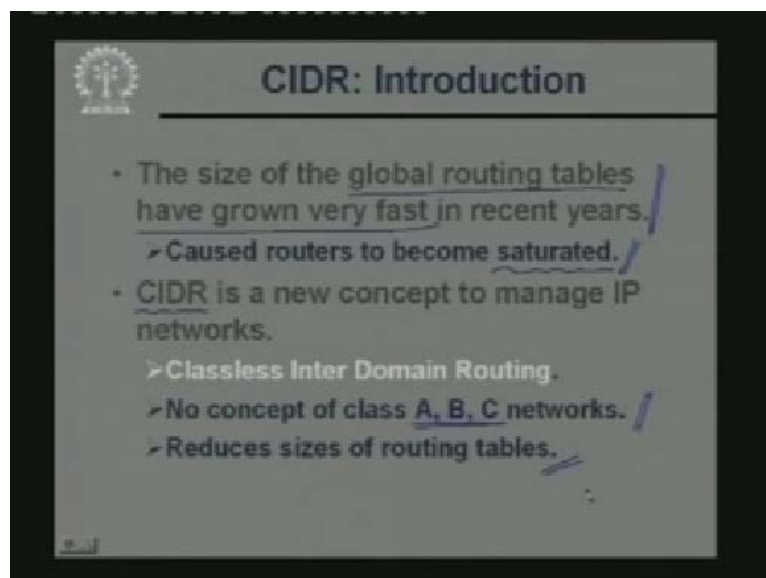
So that the way internet is expanding and exploding in size the phase can be maintained, there should not be any constraint on that. So as I had mentioned that the growing demand for IP addresses has put severe strain on the conventional model that the classful model class A B C. Huge wastage of address space due to unplanned growth. Subsequently some measures were taken the first measure. Of course it is some kind of a geographical planning Creative allocation of IP addresses. So now instead of directly allocating address classes to the customers. Now what people are saying that, well it is better to allocate the address classes to the internet service providers. The internet service providers will be doing subnetting

themselves and the customers will be getting one subnet possibly out of that ISPs total address space. So in that way the ISP can make much better utilization of the available address which they have moreover geographically the addresses that are allocated in the different areas of the globe that can also be fixed and distributed.

So that by looking at the address you can have some rough idea from where or which part of the globe the address is coming. But this has obvious limitation because for most of it the growth of the internet was not planned. So one possible alternative which we would be looking at now is something called Classless Inter-Domain Routing CIDR. Well here we are using IP address again but we are not using the concept of IP address classes A, B, C anymore we are forgetting the concept of classes. We will see this and we shall see two other things later. One is that well I just mentioned in our last lecture that we have several private IP address classes like the class A network starting with 10., that represents a private class A network. So what they say is that you use internally private IP addresses and use a device called a network address translator or a network address transmission mechanism at the gateway of your network.

So we will see later that how this scheme works and how this means this can solve. You can say requirement of say large number of addresses for an organization say even if the organization has say for example 2000 users. You can do with two or three addresses only. Internally you can use private addresses they will be a network address transmitter which will be doing some kind of translation automatically. And dynamically and other alternative this also we will discuss is IP version 6 well currently we have the IP version 4, which is dealing with 32 bit IP addresses. But subsequently in the new proposal the version 6, the number of bits and the in the IP address has been extended to 128 and 128 is a pretty large number. So that is another alternative. First let us look at the basic concept behind classless internet routing protocol CIDR, Classless Inter-Domain Routing.

(Refer Slide Time: 38:56)



Now CIDR basically addresses the problem that we have mentioned. This is a related problem, that is size of the global routing tables have grown very fast. And the external or the

back bone routers the size of the tables has become very large and they have tended to become saturated and have become slow. CIDR is a new concept which have evolved and most of the new routers and protocols today it supports CIDR. This is a concept to manage IP network. So essentially the concept of class A, B, C network is now gone, we are not explicitly categorizing the network classes and this also reduces the sizes of the tables in the routers.

(Refer Slide Time: 39:52)

**Basic Idea Behind CIDR**

- An IP address is represented by a prefix, which is the IP address of the network.
- It is followed by a slash, followed by a number M.
  - M: number of leftmost contiguous bits to be used for the network mask.
  - Example: 144.16.192.57 / 18

111-1100-0

Now what is the basic idea? Now in the so called classful model the IP address was preceded by some special bits and those special few bits identify the address class. And once you have the address class the division of your network and the host part was predefined. But in the classless model the concept is this well you have no such special bits at the beginning of the address. You have a full 32 bit address. But in addition to that 32 bit you have another number and that number will tell you that how many bits of that thirty two bit address is your network address. So now you can have potentially a 17 bit network address or 20 network address. Any arbitrary value. It is not only constrained to 8, 16 or 24 as in case of class A B C. So by that second number you can specify exactly how many bits you require.

So IP address is represent by a prefix which is the IP address. In this example, this is the prefix followed by a slash and then a number M. In this example this eighteen is the number M. This M indicates the number of leftmost contiguous bits to be used for the network mask. Essentially this number identifies this mask, this number of 18 means there will be 18 ones at the beginning followed by 14 zeros. This will be the nature of your mask. So now instead of explicitly storing the mask you store only that number 18 or whatever. This is basic idea behind CIDR.

(Refer Slide Time: 41:50)

**CIDR: An Important Rule**

- The number of addresses in each block must be a power of 2.
- The beginning address in each block must be divisible by the number of addresses in the block.

➤ A block that contains 16 addresses cannot have beginning address as 144.16.223.36

➤ But the address 144.16.192.64 is possible.

Now in CIDR there are some rules to be followed. The first is that since you are dividing the address into two parts by defining that number M. So clearly the number of addresses in each block has to be a power of 2. Because ultimately some fixed number of bits are available for the host if k number of bits are available then  $2^k$  the power k hosts will be that that will power of 2. Now another thing the beginning address in each such block well in this case the subnets are called blocks. That must be divisible by the number of addresses in the block well what I mean to say is that suppose I have a block that contains 16 addresses which means that the last 4 bits in the address are for the host and the remaining 28 bits are the network.

So 16 addresses per block. So each block will be having a starting address and an ending address. Now this says if you have a block with 16 addresses, then you cannot have the beginning address of the block as like this. Because this address is not fully divisible by 16; you have 36 at the last byte. But address like this where you have 64, this is divisible by 16. This can be starting address, so if someone asks you that, what that, if is this is a possible starting address of a block with size 16 you can just check whether that address, that starting address is divisible or not. If it is divisible you can say that well it is possible otherwise not.

(Refer Slide Time: 43:45)

**Example: CIDR**

- An organization is allotted a block with beginning address:  
144.16.192.24 / 29  
What is the range of the block?

Start addr: 10010000 00011000 11000000 00011000  
End addr: 10010000 00011000 11000000 00011111

There are 8 addresses in the block:  
144.16.192.24 to 144.16.192.31

Just an example, suppose an organization has been allotted a block like this. This is the address and 29 is the number of bits in the network. So 144.16.192.24 if you write down in binary it looks like this. The last three digits are 0 because 29 bits are for the network, 3 bits for the host an end address will be first bits will be the same the last bit will be all ones. So there will be 8 addresses in the block and if you compute them to decimal there will start from a value like this. It will go up to a value like this. So 144.16.192.24 up to 144.16.192.31, this range you can have for this particular block.

(Refer Slide Time: 44:55)

**Recent Trend**

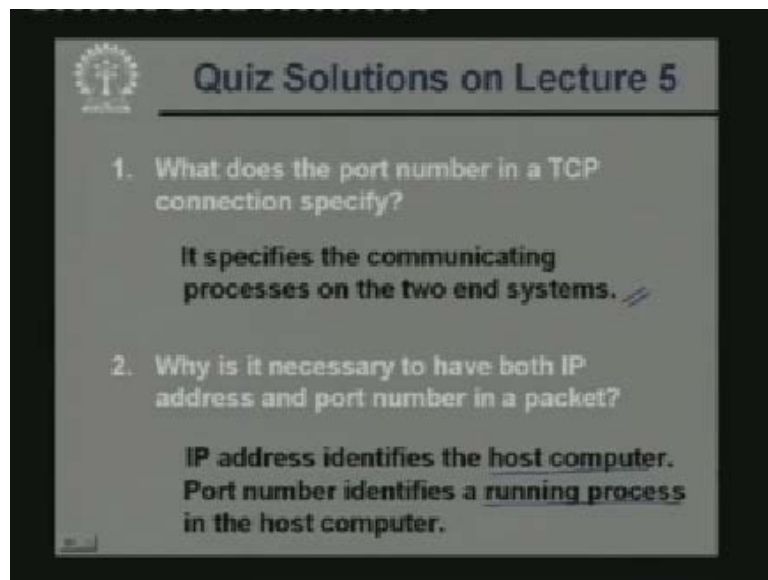
- Move on to CIDR addressing.
  - Existing classful networks can also be represented using this notation.
    - Class A: W.X.Y.Z / 8
    - Class B: W.X.Y.Z / 16
    - Class C: W.X.Y.Z / 24
- Recent routers support CIDR.

Now as I had said the recent trend most of the routers, they support this CIDR. In the recent trend is to use or to move on to CIDR addressing completely. Well if you talk about compatibilities some of the networks maybe already class full. So you cannot make all of them classless just overnight. So the thing is that even the exiting classful networks can be

represented by CIDR notation, class A network can be represented by an address like this. Some IP address slash 8 means first 8 bits are the network class B address slash 16 and class C address slash 24. Now as I had told that the recent routers, they support CIDR.

Now in today's lecture we have seen an idea that how this IP address subnetting can be used for better management of networks and we have seen that just extending the concept of subnetting, we can have VLSM and we can go one step further in having CIDR which offers you complete flexibility. Now in our next class we shall be looking at some issues regarding IP routing. Now the subnetting is fine, but how the subnets are used by the routers actually while routing the packets. What kind of information the routers maintain their tables, these we shall be seeing in our next lecture. So we come to the end of this lecture. We now have a look at the solutions to the problems that were posed in our last class. Solutions to quiz questions from lecture 5.

(Refer Slide Time: 46:38)



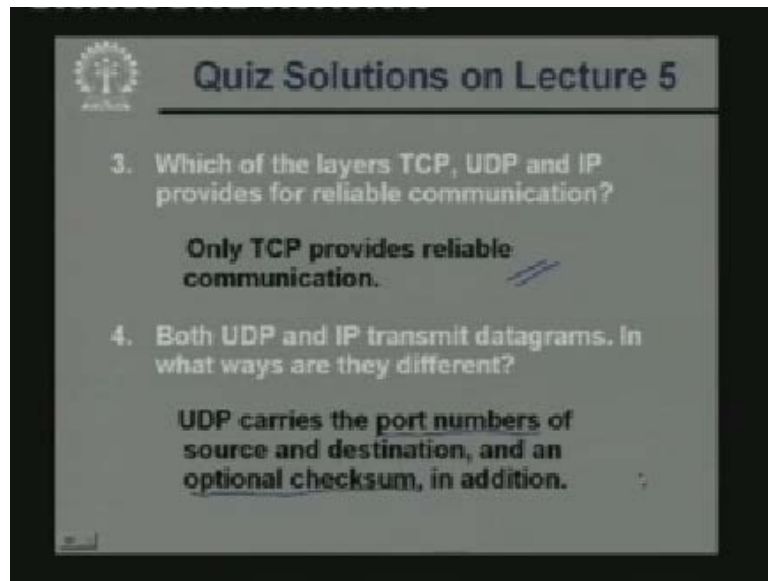
The first question was what does the port number in a TCP connection specify?

Now here we have mentioned that the port number in a TCP or for that matter even in UDP connection any transfer level protocol they identify the two applications on the two end hosts who are communicating among themselves. So this port number is a way of identifying the two communicating end parties. It specifies the communicating processes on the two end systems.

Why is it necessary to have both IP address and port number in a packet?

Well this question I have addressed repeatedly that IP address identifies the host and port number identifies the application or the process running on that host. So it is again hierarchical addressing. First you have to identify the host computer, then you to identify a process running on that host computer.

(Refer Slide Time: 47:46)



The slide is titled "Quiz Solutions on Lecture 5" and features a logo in the top left corner. It contains two quiz questions and their solutions. Question 3 asks which layer (TCP, UDP, or IP) provides reliable communication, with the answer being "Only TCP provides reliable communication." Question 4 asks how UDP and IP differ, with the answer being "UDP carries the port numbers of source and destination, and an optional checksum, in addition."

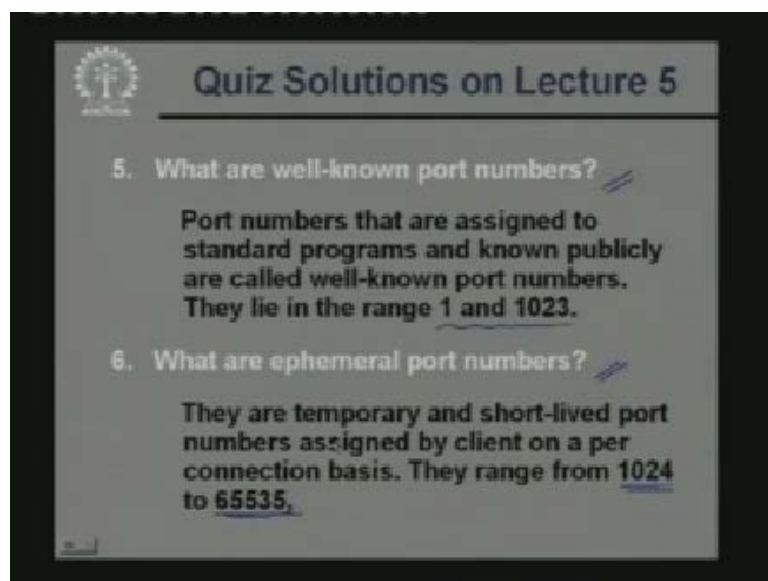
Which of the TCP, UDP and IP provides reliable communication?

Well here I told you IP is a datagram service by very definition, it is unreliable. And UDP and IP are not much different UDP simply adds a few extra information to an IP packet and sends it. So UDP is also unreliable but TCP put some extra effort with respect to putting the sequence number acknowledgements window. All these things in order to achieve reliability over an unreliable IP network. So if a part of the message is lost it explicitly requests for retransmission in that way provides reliability, so only TCP is reliable.

Both UDP and IP transmit datagrams how they are different?

Now this I told you just now that UDP contains some extra fields in addition to IP they are the port numbers of the source and the destination and an optional checksum value. These are the two things which are stored.

(Refer Slide Time: 48:57)



The slide is titled "Quiz Solutions on Lecture 5" and features a logo in the top left corner. It contains two quiz questions and their solutions. Question 5 asks for well-known port numbers, with the answer being "Port numbers that are assigned to standard programs and known publicly are called well-known port numbers. They lie in the range 1 and 1023." Question 6 asks for ephemeral port numbers, with the answer being "They are temporary and short-lived port numbers assigned by client on a per connection basis. They range from 1024 to 65535."

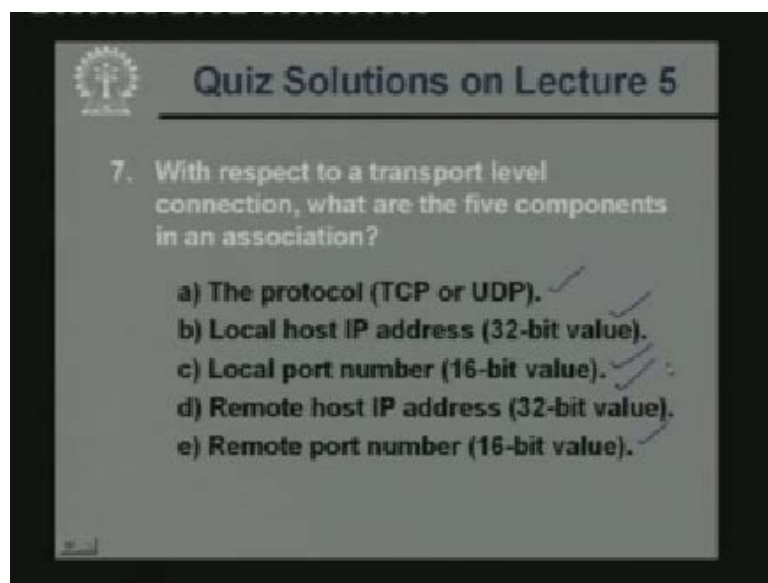
What are well-known port numbers?

Well I told you in a client-server scenario, when a client is connecting to a server, there are some well-known or well defined programs which everyone uses and the port numbers for them are publicly known. These are well known port numbers and usually the well-known port numbers range from 1 up to 1023.

What are ephemeral port numbers?

Well ephemeral port numbers are temporary port numbers which are used by clients. Now a client when it requests, some kind service to the server the server after processing request has to send back a response. So the server must also know what is the port number of the client? That certainly not a well-known port number. So the client has to put a temporary port number every time it sends out a request. That is called ephemeral port numbers. They can range for 1024 up to maximum of 65535.

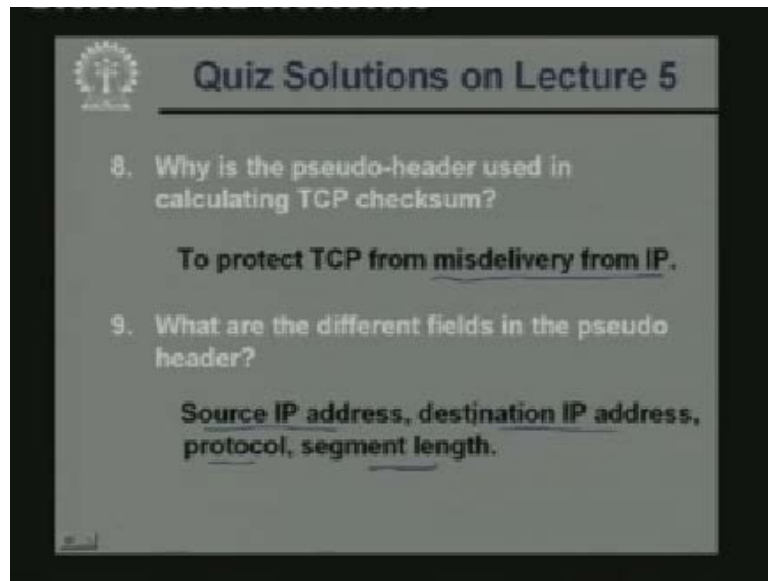
(Refer Slide Time: 49:59)



With respect to a transport level connection, what are the five components in an association? This we have mentioned we need to have the protocol local IP, address local port number, remote IP address and remote port number, these are the five things.



(Refer Slide Time: 50:16)



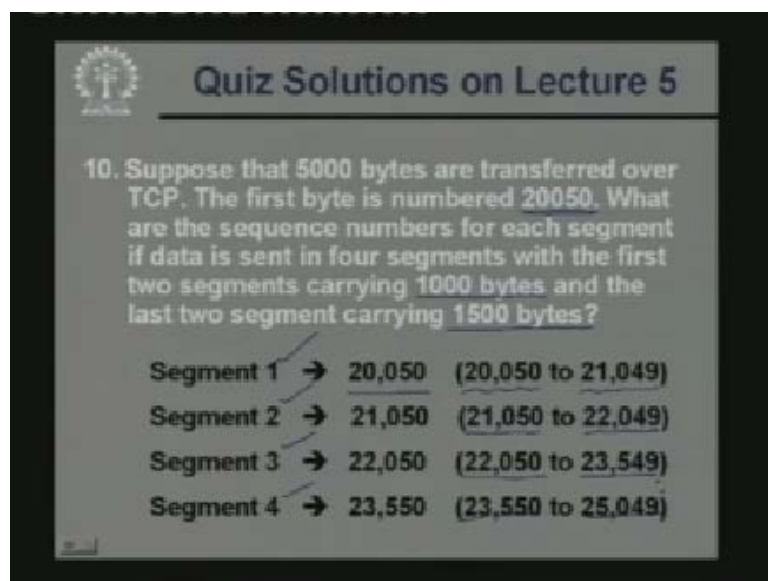
Why is the pseudo-header used in calculating TCP checksum?

Well we had mentioned that while computing checksum in a TCP packet in addition to the TCP headers some of the headers are borrowed from IP. This is done primarily to prevent misdelivery from IP well even if by mistake the IP layer sends the packet to the wrong host. There upon computing the checksum the error will be found put and packet may be discarded.

What are the different fields in the pseudo header?

Pseudo header contains source IP address, destination IP address, which protocol you are using and the length of the segment. These are borrowed from the IP protocol.

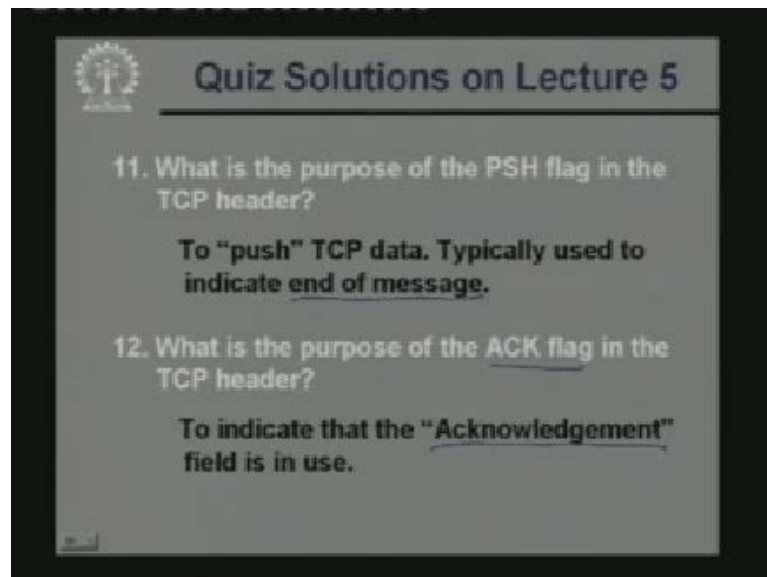
(Refer Slide Time: 51:02)



This is a question on TCP. It is said there are 5000 bytes which are transfer over TCP. The first byte number is 20050, 20050. What are the sequence numbers for each segment where

the first two segments carry 1000 bytes each and the last two segments 1500 bytes each? Where it is easy to find out, for the first segment the starting byte number is 20050 and the number of bytes is 1000. So it will be starting with 20050 up to 21049, the second segment is also 1000 bytes in size. So it will start with 21050 up to 22049 segment 3 is 1500 bytes start with this end with this 1500. Fourth one is also 1500 start with this end with this. So just by looking at the size of the segment you can compute the end addresses.

(Refer Slide Time: 52:14)



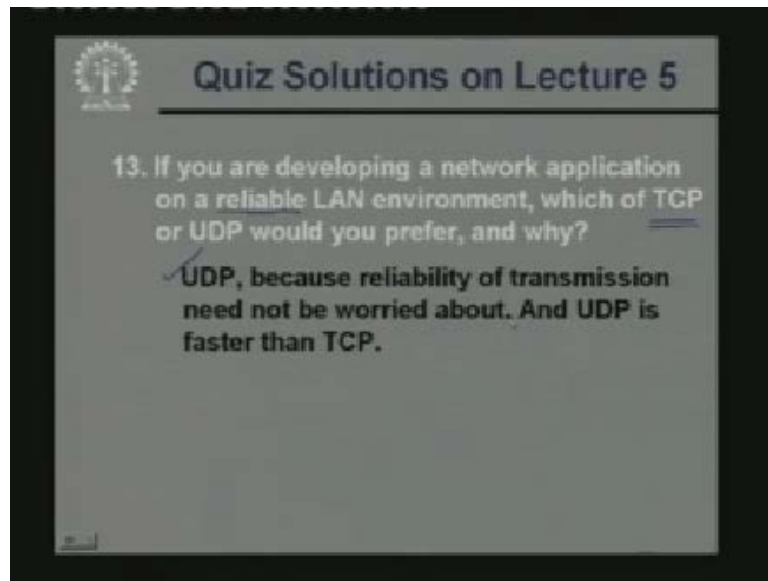
What is the purpose of the push flag in the TCP header?

Well push flag is used to push TCP data but this is conventional use to indicate the end of the message indicate that there are no more segments following corresponding to a given message. This is the last segment of a message.

What is the purpose of the ACK flag?

This is an Acknowledgment field this is used to acknowledge the correct receipt of a segment by the receiver to the sender. This goes from the receiver back to the sender, so the sender can know that whether the segment was sent and received correctly or not.

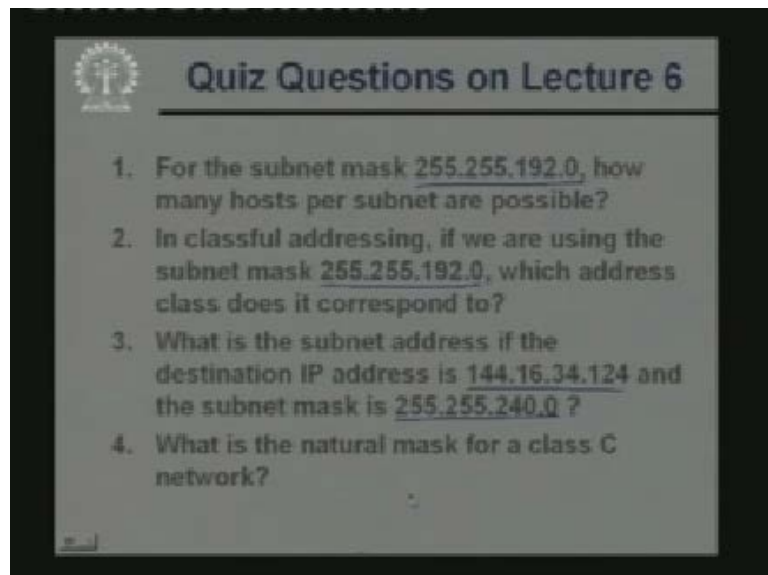
(Refer Slide Time: 52:52)



Well if you are developing a network application on a reliable LAN environment which of TCP or UDP you would prefer?

Well if the network is reliable then we do not need the additional features that TCP provides. We would possibly prefer UDP because UDP has much less overhead both in terms of header size and also in terms of the speed of delivery of the packets. So possibly the packets would move much faster in UDP as compared to TCP. So now let us look at the questions from today's lecture from lecture number 6.

(Refer Slide Time: 53:33)



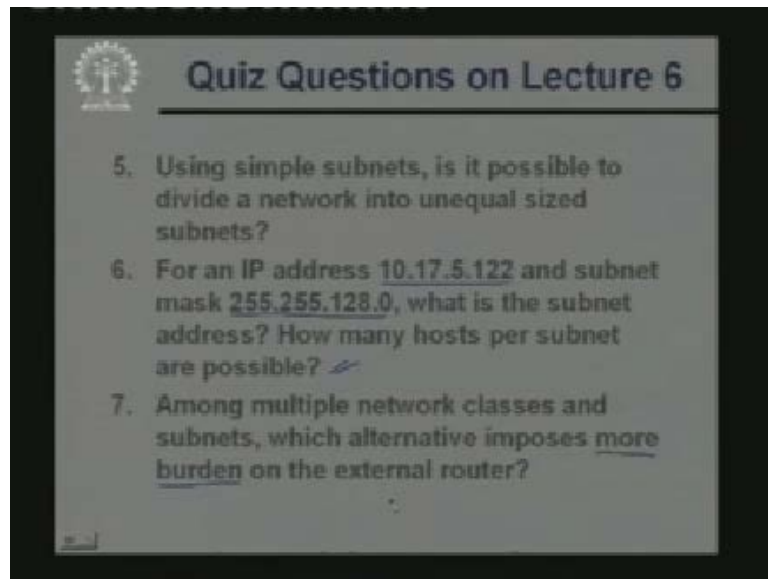
For the subnet mask, this how many hosts per subnet are possible?

In classful addressing if we use the subnet mask this which address class does it corresponds to well just by looking at the subnet you can find out.

What is the subnet ad if the destination IP address is this and subnet mask is this?

What is the natural mask for a class C network?

(Refer Slide Time: 54:08)

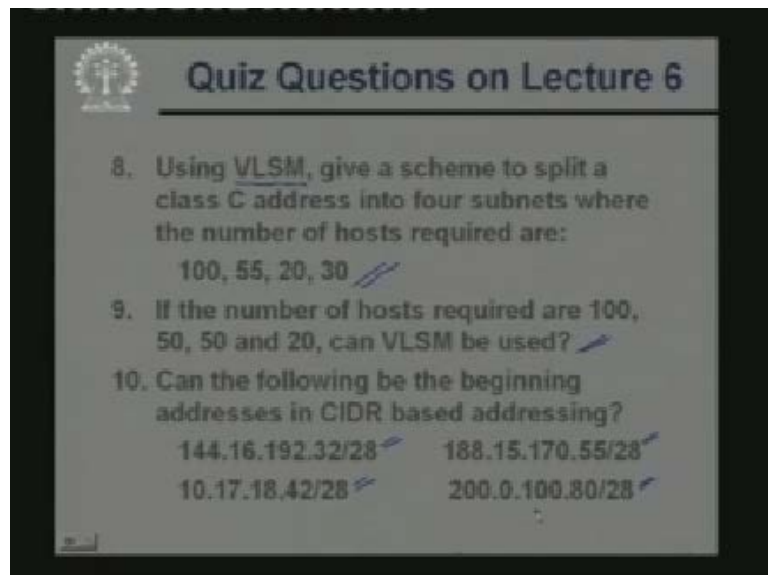


Using simple subnets, is it possible to divide a network into unequal sized subnets?

For an IP address this and subnet masks this what is the subnet address? How many hosts per subnet are possible?

7. Among multiple network classes and subnets which alternative imposes more burden on the external router? This I have discussed.

(Refer Slide Time: 54:39)

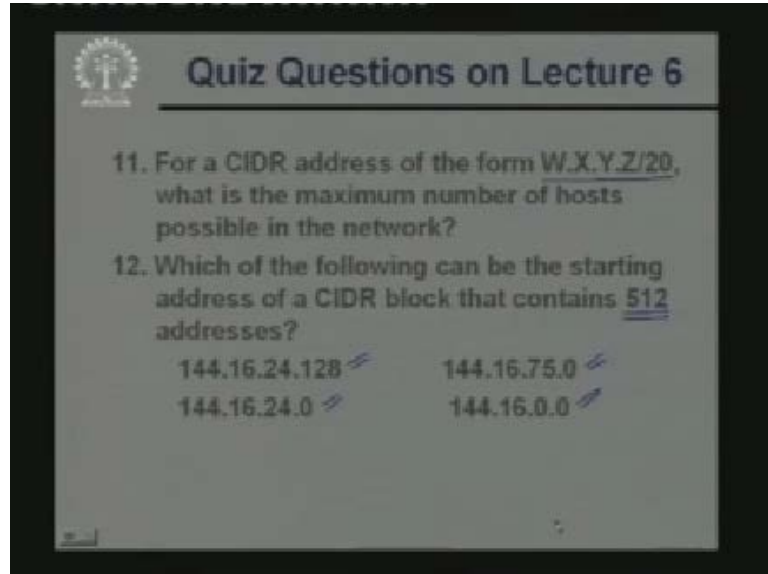


Using VLSM give a scheme to split a class C address into 4 subnets where the number of hosts required are like this 100,55,20 and 30.

So here you can follow this scheme which I have discussed in the class one example I have worked you can follow similar scheme.

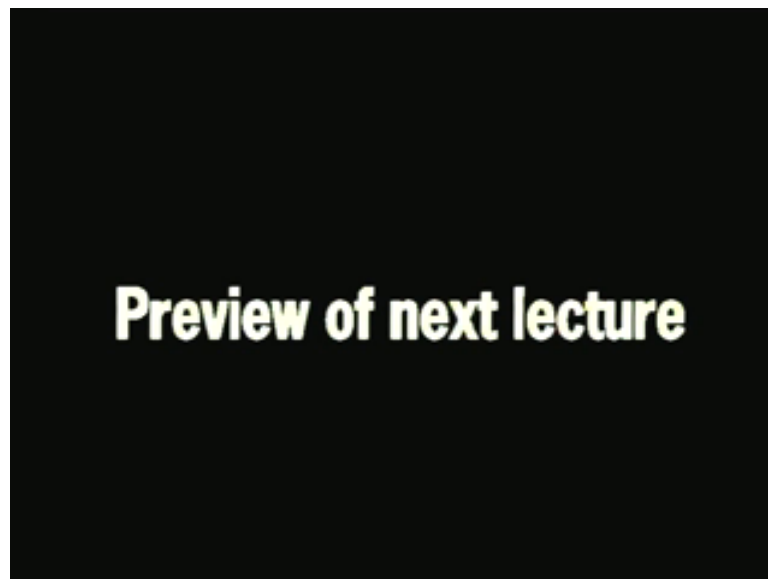
Now the same question If the number of hosts required are 100, 50, 50 and 20 can VLSM be used. Can the following be the beginning addresses in CIDR based addressing? There are 4 addresses which are given you will have to tell whether they are starting addresses are not.

(Refer Slide Time: 55:50)



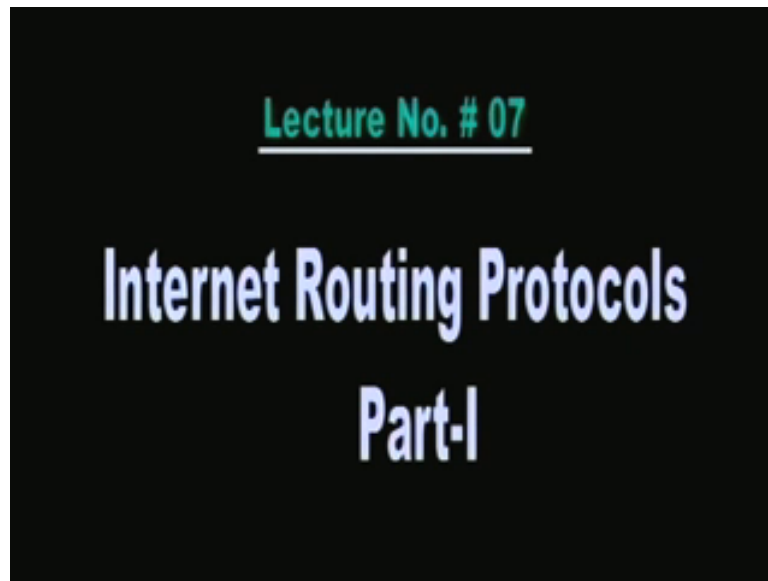
For a CIDR address of the form something slash 20, what is the maximum number of hosts that can be that are possible in the network? Which of the following can be the starting address of a CIDR block that contains 512 addresses? Here again we have 4 IP addresses. Now you will have tell that which of these can be starting addresses of the CIDR block. So with this we come to the end of today's presentation. Thank you.

(Refer Slide Time: 56:01)



Preview of next Lecture.

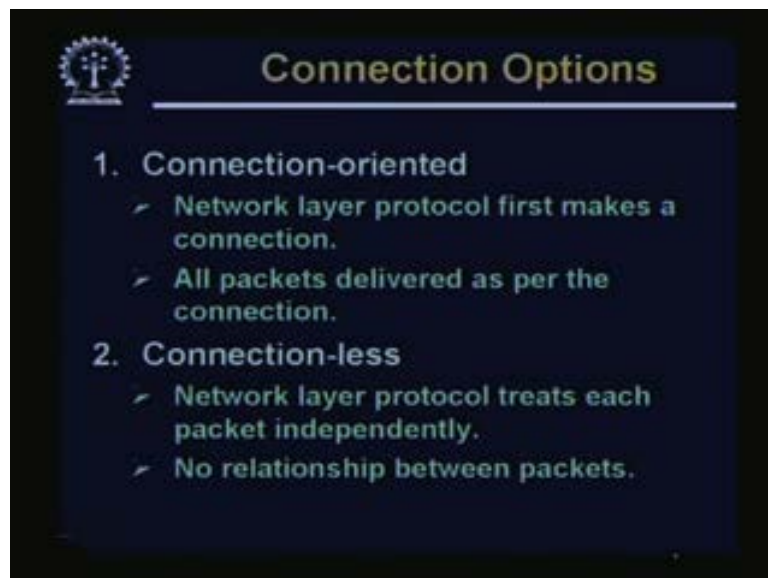
(Refer Slide Time: 56:02)



Internet Routing Protocols Part-1.

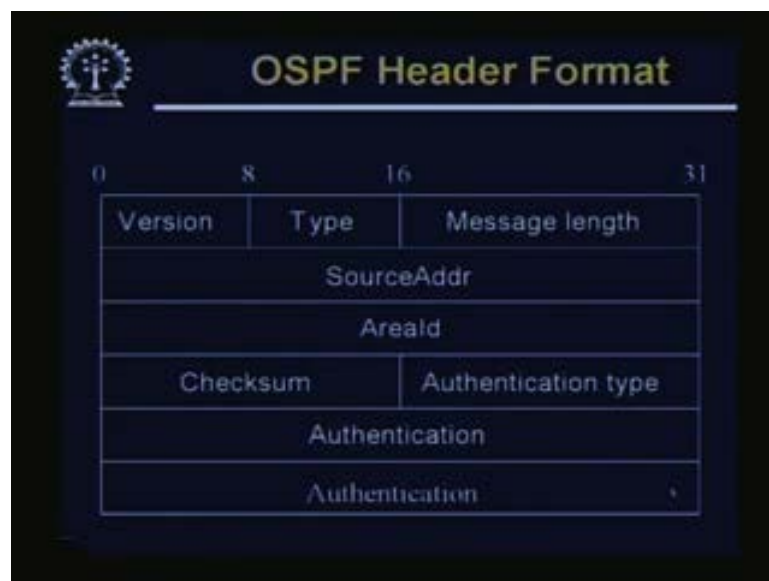
And today we shall start our discussion on Internet Routing Protocols. Now here we shall be talking about some of the ways in which routing of the data packet actually takes place in the internet scenario. You may recall that in the last few classes we have already discussed a few things related to IP addressing and some routing, characteristics of the IP addresses. In particular we had talked about the IP address masks, we had talked about the classless internet routing, and means, we had also talked about the variable length subnet masks. No using these technologies we can make more efficient utilization of an available address block. Depending on the requirements of an organization, we can suitable partition the addresses and make suitable subnets designed as per the needs. Now today we shall primarily start our discussion actual routing protocol which people use in the internet scenario.

(Refer Slide Time: 57:23)



Now to start with the talk about of the starting connection options, now we broadly speaking from the two computers of the internet trying to send and receive packets between themselves, we can either have connected oriented approach or we can have connectionless approach. Now in the connection-oriented approach, this is essentially what we know as the virtual circuit mode of data transfer. Here any first step before any data transfer can take place is to have a connection established between the two parties. And the establishment of the connection is the responsibility of the network layer. And once the connection has been established, all the packets would be delivered along the path that has been established as part of the connection and all the packets will be following the same path. This is one characteristic of the one connection oriented approach.

(Refer Slide Time: 58:38)



Now in OSPF there are number of fields in the header. And we are not going to details of this, version of OSPF, which type of OSPF packet you are sending, message length, source address, this is the area which is the autonomous system basically, checksum and some authentication related fields.