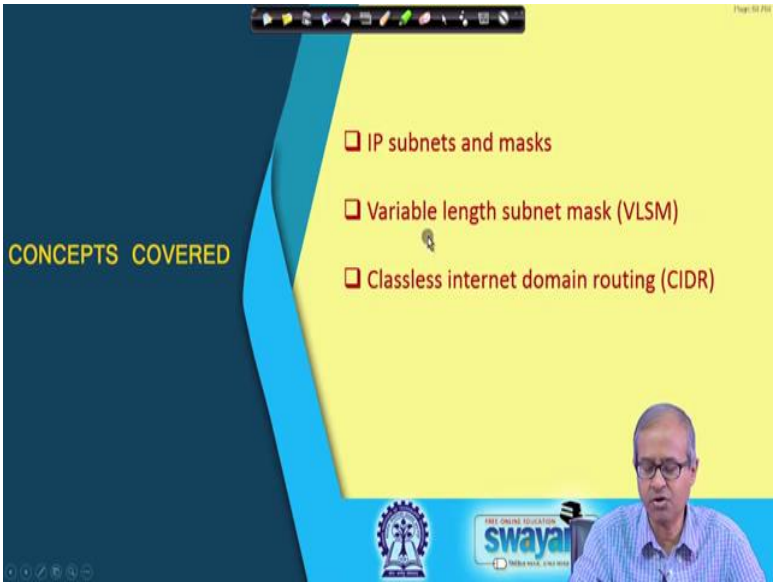
**Ethical Hacking**
**Prof. Indranil Sengupta**
**Department of Computer Science and Engineering**
**Indian Institute of Technology, Kharagpur**

**Lecture - 10**
**IP Subnetting**

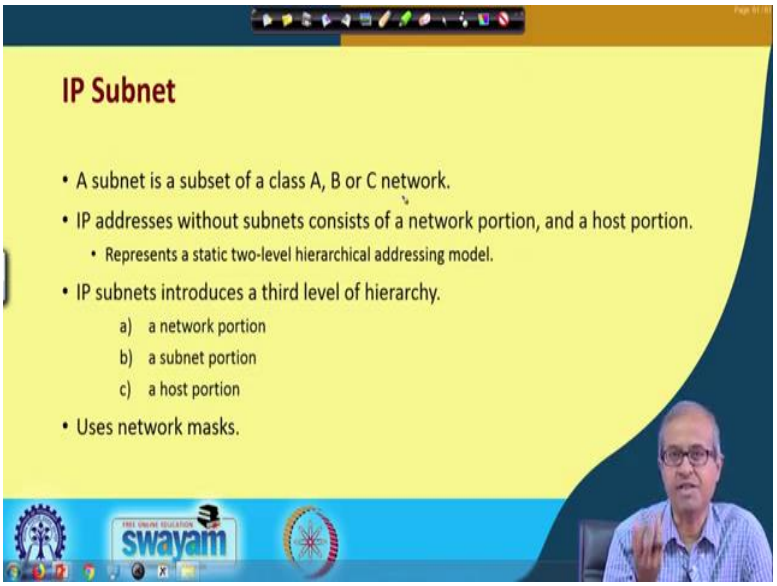
In this lecture, we shall be talking about IP sub networks or subnets. Now, we have already seen, how this IP networks are; class A, class B, class C, we have talked about. Now, when you talk about subnets, the idea is a network, an IP network, it can be class A, B or C. We are further splitting into smaller sub networks; that is the concept of subnets. So, the topic of this lecture is IP Subnetting.

(Refer Slide Time: 00:50)




Now, here we shall be talking about these IP subnets and IP masks, how they are used and we shall be talking about two methods, which can be used for efficient creation of this kind of sub networks. One is called Variable Length Subnet Mask or VLSM; other is Classless Internet Domain Routing or CIDR ok.

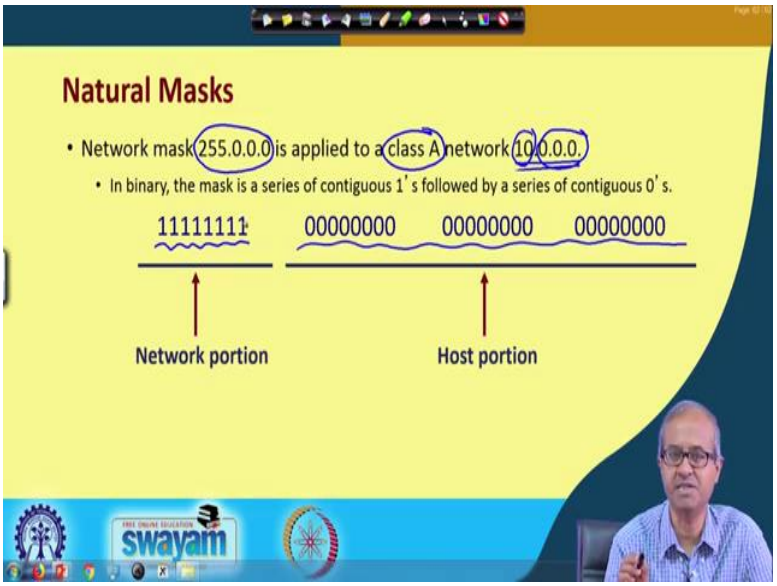
(Refer Slide Time: 01:20)




So, let us first start with IP subnet. Now, earlier we have already talked about the class A, B or C IP networks. Now, there we had seen, that we are using some kind of a two level hierarchical address to identify a particular host on the network. The address consists of a network part and it consists of a host part. The network part is classified as class A, B or C like that.

Now, when you are using IP subnets, we are introducing or we are adding a third level in the hierarchy. We are using a network portion and host portion in addition, there is a sub network portion or subnet portion and the subnet portion is specified by using something called network masks. This is what we are doing.

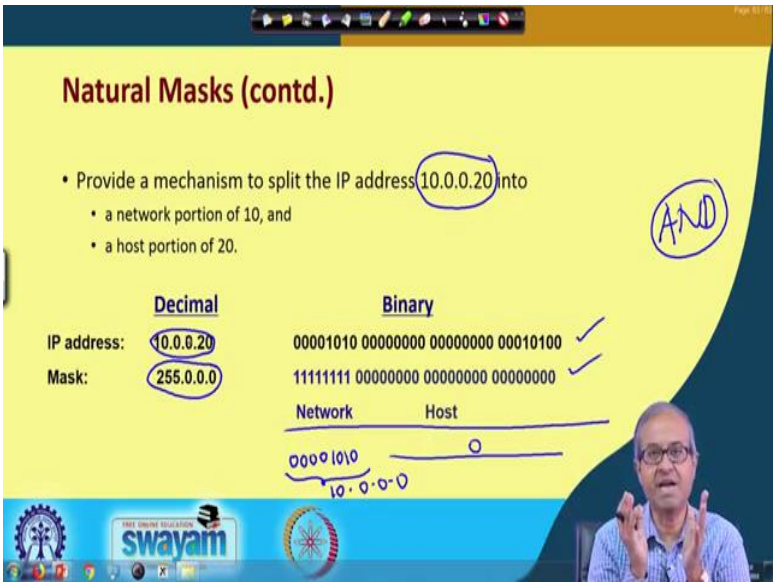
(Refer Slide Time: 02:30)




Now, let us look at the concept of network masks. First, we talk about something called natural masks. Natural mask means class A, B or C, in its purest form. There are no sub networks; that is what is meant by natural mask. Let us see what the natural mask is; when we take the example of a class A network, let us say the network addresses 10.0.0.0, well you see conceptually what it means. The first 8 bits indicates the network number, the remaining 24 bits indicates the host.

What I do, I define something called a mask. Mask is a stream of 0s and 1s, well not arbitrary stream, first few bits will be 1s followed by all 0s. 1s indicate that these are bits corresponding to network; 0s indicate these are bits corresponding to host. So, when I say first 8 bit is network, last 24 bits is host, I write the mask like this, first 8 bits are 1s, remaining 24 bits are 0s. So, when I write this mask again in dotted decimal notation, it becomes 255.0.0.0. So, class A network will be having a natural mask of 255.0.0.0, because the first 8 bits represent network. So, first 8 bits are 1s.

(Refer Slide Time: 04:36)

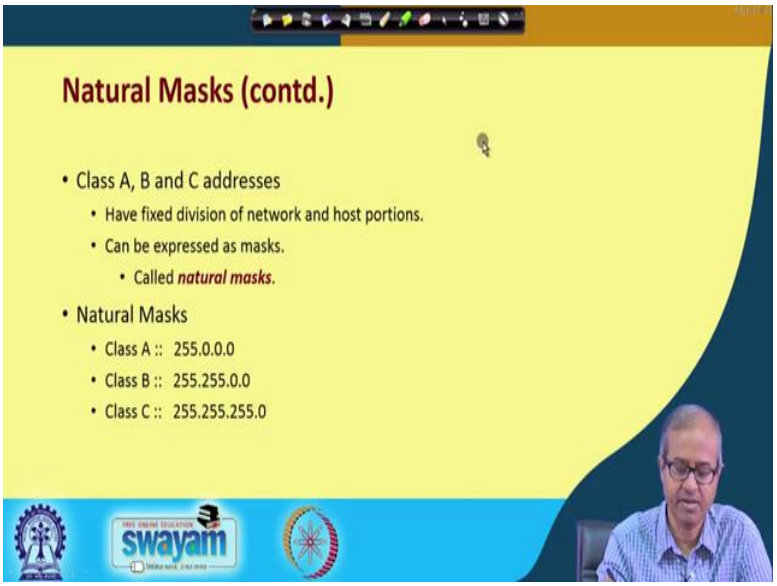



So, let us take a specific example. Suppose, we have a specific IP address of a host on this class A network sorry, it is a 10.0.0.20, this is the IP address. This is my IP address and already we have seen that the natural mask is 255.0.0.0. So, if I write it in binary 10.0.0.20 is this and 255.0.0.0 is this.

Now, this mask actually tells you, how many bits of the address we need to consider to know the network number, means if I do a bit by bit AND operation, bit by bit ANDing, first 8 bits are one in the mask, if you do AND so the first 8 bits will be 0 0 0 0 1 0 1 0 which is 10 in decimal, but remaining all bits are 0s, if you do an AND everything will be 0.

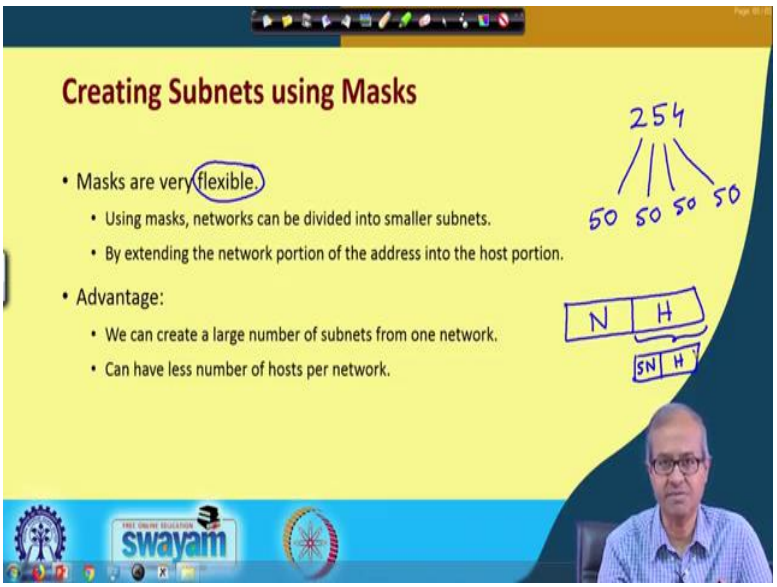
So, in dotted decimal notation, it will 10.0.0.0, which will indicate the network number. So, from the mask if you do a bit by bit AND, you are masking the host part, making it all 0 and you are extracting the network number, that is the main purpose of the mask.

(Refer Slide Time: 06:25)




So, natural mask for class A we have already seen, in a very similar way for class B, the natural mask will be first 16 bits, a network, 255, 255 then 0, 0, for class C first 24 bits indicate network 255, 255, 255 and then host, last 8 bits. So, these are the natural masks. So, natural mask has fixed division, but when we use so called subnets, we can have arbitrary masks, not necessarily this kind of subnet masks.

(Refer Slide Time: 07:08)

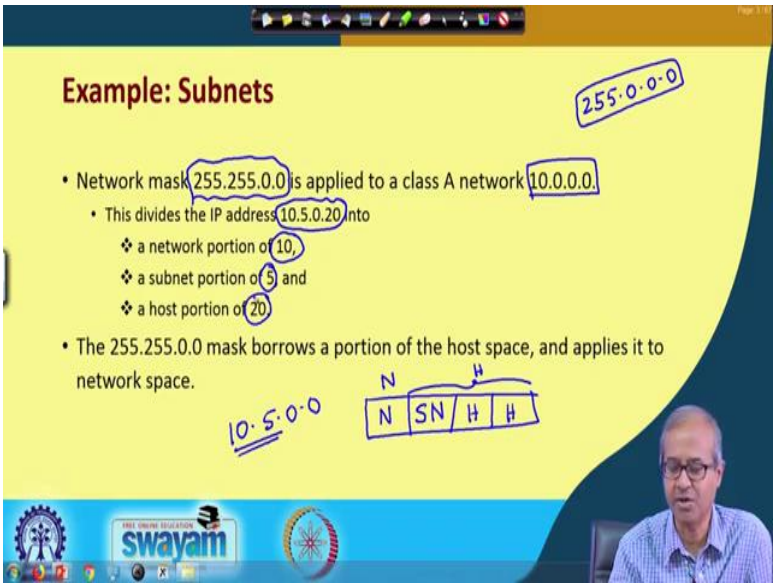



So, here as I have said when you are using subnetworks, here again, we are using masks and these masks are very flexible. Like for example, in a class C network, I can have 254

hosts in a network, if I want I can divide it into four parts; wherein each part I can have let us say 50 computers each, 50, 50, 50, 50, this will be subnetworking. Well, we shall see how we can do this.

Basically, what we will do in the IP address, as we know there are two parts; one is the network part, other is the host part. What we are doing, we are taking the host part. Now, in the host part we are again doing some kind of a partitioning, subnetwork and host. Some of the bits of this host part we are using to identify the subnetwork number and the remaining bits to indicate a host within the identified subnetwork right.

(Refer Slide Time: 08:36)

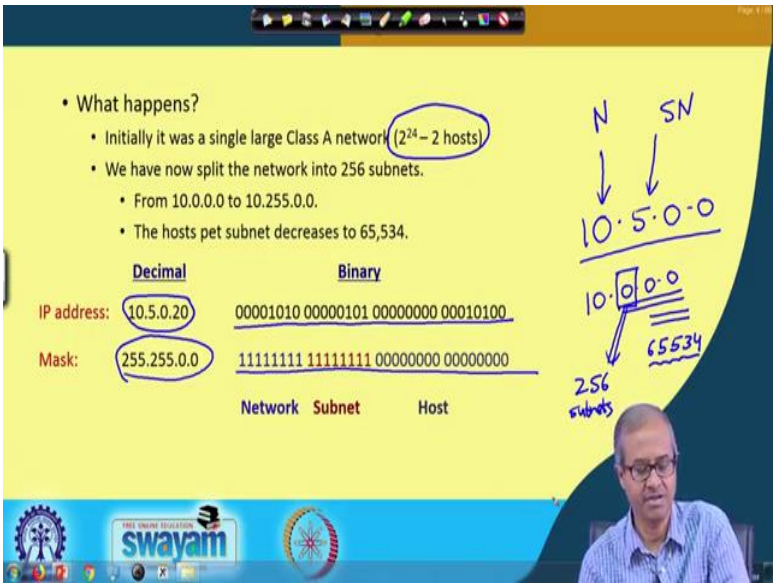



So, let us take an example of; so, let us take class A network 10.0.0.0, for which you recall the natural mask was 255.0.0.0. This was the natural mask, but now we are using a mask of 255.255.0.0. What does that mean? In this network there were 4 parts, in this address there were four parts; first was the network, the remaining three was the host. Now, when I say 255.255.0.0, essentially I am saying my first 16 bits are my network, 255.255, but already the first 255 is network, because it starts with 10.

So, the next 255 also I am borrowing as the network, this will be my sub network. So, as if this will be my network, subnetwork, host, host. So, if I now have an address like this; for example, 10.5.0.20 then, if we apply the natural mask of class A 255.0.0.0, you will get the network part 10 0 0 0. Now, if we apply this subnet of mass 255.255.0.0, you will

be getting 10.5.0.0. 10 is already there, so the subnet of number will be 5 and whatever remains last part, last 16 bits is 20. This is how sub networking works.

(Refer Slide Time: 10:45)

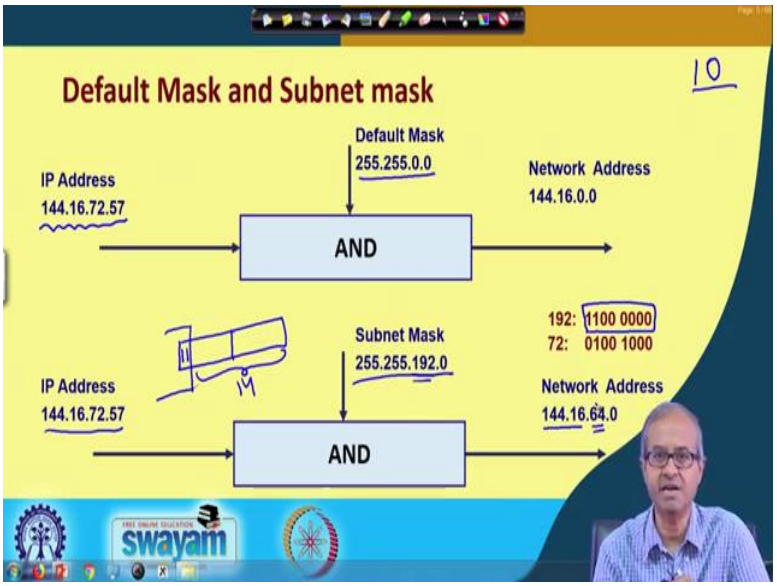



So, here I am just illustrating this. This is the IP address I was talking about, in binary I am writing like this 10 5 0 20, mask is this. So, if I do a bit by bit AND, again I mean I will get 10.5.0.0. So, this will give you my sub network number. Now, already because this is a class A network, I know that this is my network number.

So, whatever remains that will be my sub network, this 5. So, essentially what we have done in a class A network. Let us say 10.0.0.0, there were 24 bits for the host. So, you had a maximum of $2^{24} - 2$ hosts possible, but now we are using this second byte to identify a sub network.

So, you are left with only the last 16 bits. In the last 16 bits how many hosts can be there 65534, $2^{16} - 2$ and, because this can have 256 combinations, you can have up to 256 subnets and each of the subnets will be having up to 65534 hosts. This is how sub networking works.

(Refer Slide Time: 12:44)

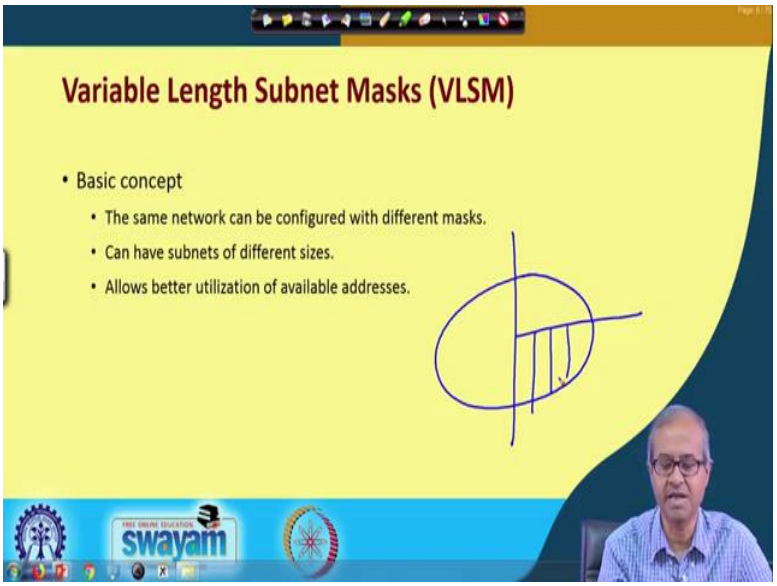



Now, here pictorially whatever we have said bit by bit ANDing, I am showing for default mask and also subnet mask. Let us take an example here of a class B address. This is a class B IP address starting with 144; you can check 144 starts with 10, which is class B. So, for IP for class B address the default mask is 255.255.0.0. So, if you do a bit by bit AND, you will be left with 144.16.0.0 which is your network address, but if you are using subnet masking, the same IP address, see 192 means what?

192 means this pattern, first two bits are 0, which means in a class B the last 16 bits indicated host, but in this subnet I am also using 2 more bits, these 2 bits I am taking out. So, I am left with 14 bits for the host. So, if I have one address like this and if I have a subnet mask like this, means if I do a bit by bit AND again, you can say this 144.16 will remain and 192 and 72 if you take a bit by bit AND, these bits were all become 0, only this one will remain 0 1 0 0 0 which is 64.

This will be the network address ok, network id including the sub network. So, 144.16 is the class B network and 64 is the sub network number within that class B network. This is how you can extract the sub network number from a network.

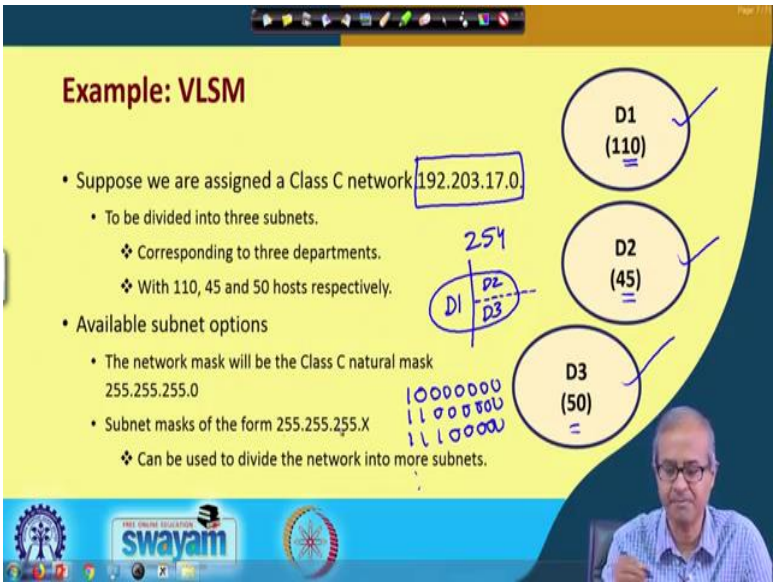
(Refer Slide Time: 15:01)




Now, we have something called variable length subnet mask. The idea is that the same network depending on a scenario, you can configure with different masks. Like earlier, what I said if I use the example, I had said just the previous example; I am splitting a particular network into certain number of subnets.

A number of hosts per subnet is fixed, but for variable length subnet mask I am saying, I can use variable like let us say I have a big network, I first divide it up into equal and one part I make half, this part I do not make half and one part I make 4, like this unequal pieces, I can make. This is the concept of variable length subnet mask, let us see how it works and obviously, this will allow better utilization of available address space.

(Refer Slide Time: 16:10)

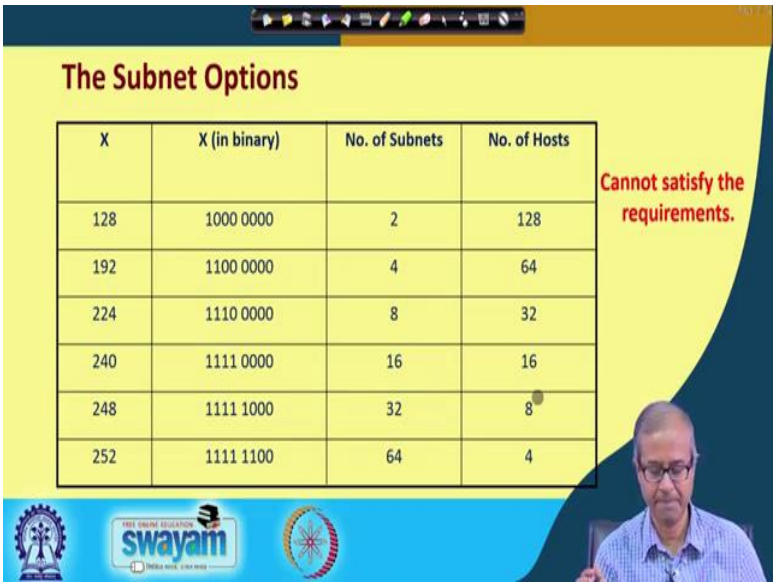



Well here, I am taking a very specific example suppose, I have a class C network 192.203.17, 24 bits are network and 0 last is the host part ok. Let us say in an organization there are three departments; D1, D2, D3, I am trying to make three different sub networks and the number of computers are 110, 45 and 50. Now, in a class C network, you can have 254 hosts total. So, you have let us say a total class C network, I am having 254. Now, if we divide it into half, it will be approximately 127 something.

Now, in this you can accommodate D1, because it is 127, D1 requires 110, but in the other part you again have 127, but you need D2 and D3. So, you can make the other part into half and this is enough for 45 and 50, you can put D2 in one and you can put D3 in the other. So, the idea is something like this.

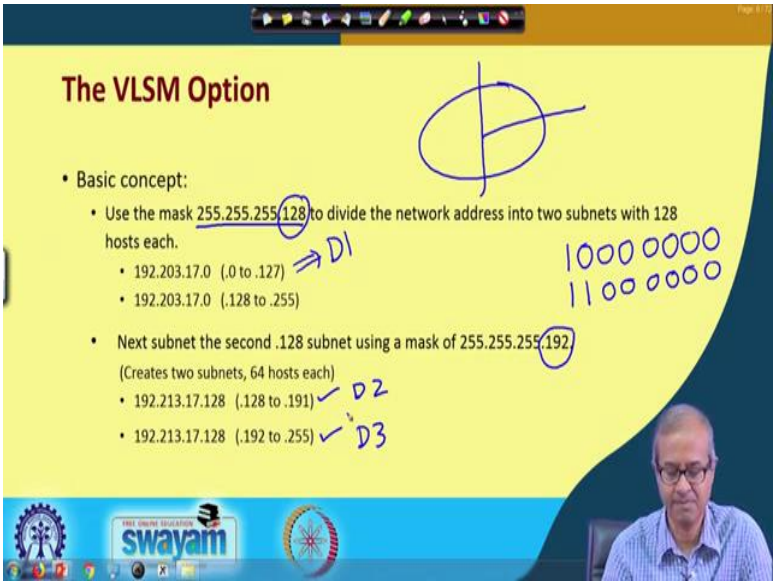
So, there are two subnet options we will see, the first one; let us say that the, if you can do without VLSM, by using normal subnet masks can we do? Let us say we have a class C address just using some subnet mask with class C, 255.255.255. some value of X. X can be either 1 followed by 7 0s or it can be 1 1, it can be so many things, 1 1 1, so many options. So, let us explore whether any of these can satisfy our requirement.

(Refer Slide Time: 18:29)




So, I have shown a table for various values of X, if X is 128 means 1 followed by 0s, number of subnet is 2 with 128, 128 each approximately, if I make it 1 1, which is in decimal 192 sorry. So, it will be divided into four subnets with 6 bits, 64 each. So, department one cannot be accommodated. So, if you make it more, it will become even smaller. So, none of these can accommodate D1, D2, D3 altogether. So, we cannot use normal subnets in this particular example right.

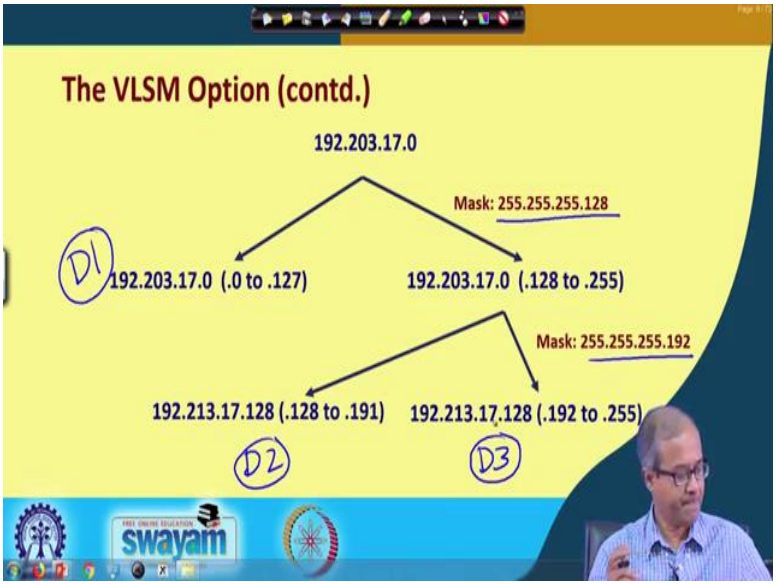
(Refer Slide Time: 19:14)



So, let us look at the VLSM option. Now, VLSM; what do you do? First, we use this mask to divide the whole network into half, two subnets with 128 host each. First one, we will be having address with host number 0 to 127, second one we will having host number 128 to 255. Then first one, I assign to D1, the larger one, second one so I again divided into half by using another subnet, you see this, this 128 means what? This 128 means 1 followed by eight 0s, 7.

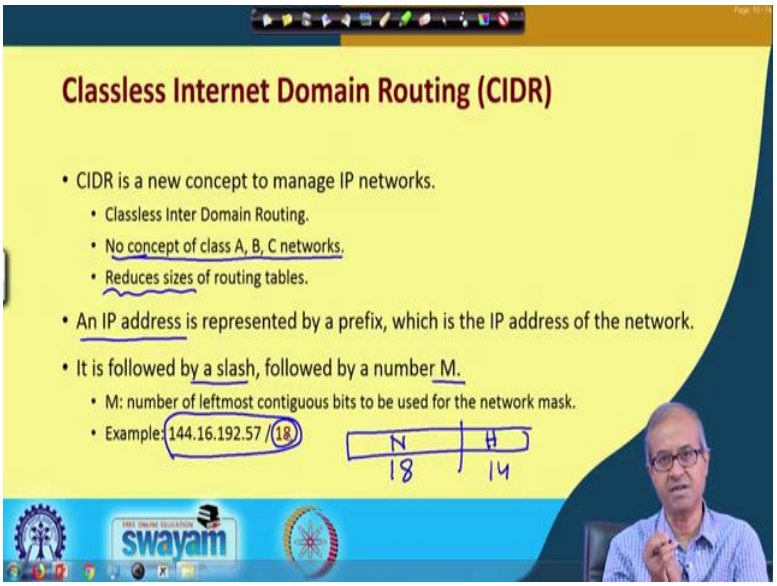
All 0s and 192 means what? 192 means 2 1s followed by six 0s. So, I again divide the second part into half by using a mask with dot 192. So, this 128 to 255 was there now, it will be divided into 128 to 191, 192 to 255. This I assigned to D2, this I assigned to D3, this is how I do using VLSM.

(Refer Slide Time: 20:39)




So, let me show it diagrammatically, this was my original class C, first I use a mask of this, I divided into two parts, this one part I assigned to department D1, D1 is done, the next part, where the host address is 128 to 255, I use the second mask. This again is divided into two parts, this I assigned to D2, this I assigned to D3. So, the idea is that if your router inside your organization supports VLSM, you can have this kind of multiple masks along with this IP address, for this IP network, you are using to provide this kind of partitioning whatever you require right. This is an added advantage here.

(Refer Slide Time: 21:38)

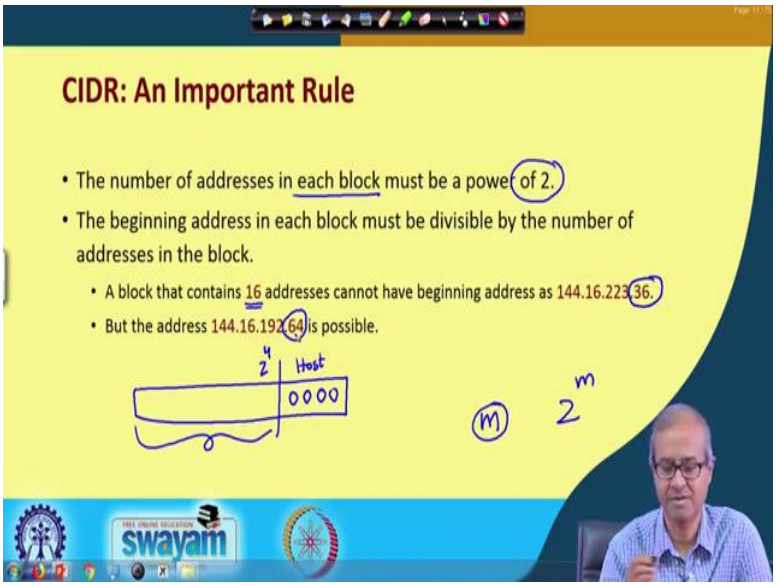



Now, there is another type of addressing, you can, you can use instead of class A, B, C or VLSM is an extension of that basically, you take one address class on that, you use variable size masks, but now, we are using another philosophy which we are saying classless. We are not talking about address classes at all.

Classless here, we have no concept of class A, B or C and this gives certain advantages, like the routing tables in the routers, they get reduced in sizes, because we do not have to store the whole masks like that. Now, the way we specify CIDR addresses is like this, we specify an IP address followed by a slash, followed by a number M. Let us take an example. So, I specify this 144.16.192.57/18, what does this 18 indicate?

18 indicates that I have this 32 bit IP address, whatever is given. The first 18 bits, this will be my network and the remaining 14 bits will be my hosts. Now, this number can be anything, this can be 18, it can be 17, 15, 14, 11. I am not restricting myself to only class A B or C ok. This number M slash something this I can use anything in a flexible way, depending on the size of my organization, size of my network. I can do any arbitrary partitioning, this is the advantage of CIDR.

(Refer Slide Time: 23:45)

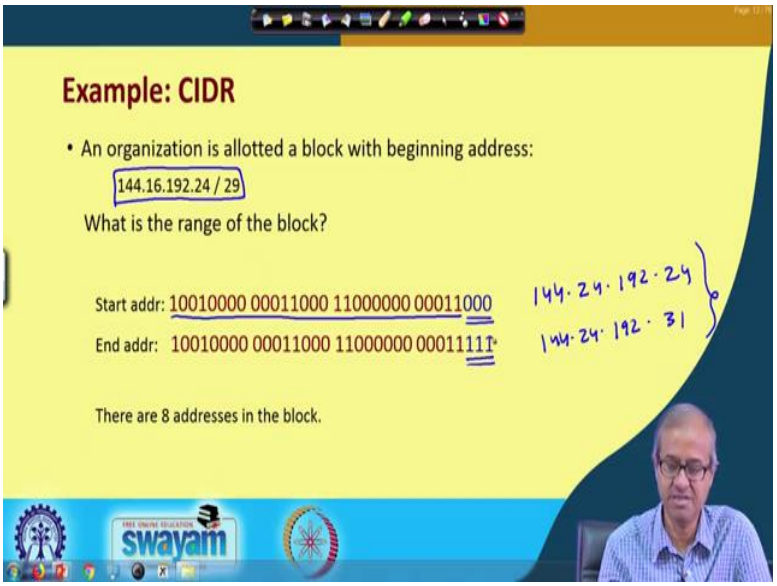



Now, there are some constraints or rules that need to be followed here. First rule is that in CIDR number of addresses in each block you are defining must be a power of 2, because you are using certain number of bits for address network, certain number of bits for host. Suppose, you are using M bits for the host, so number of host will; obviously, be $2^M$. So, it is some power of 2. Now, the beginning address in each block must be divisible by the number of addresses in this block. See the idea is like this.

Let us take an example; suppose, the first few bits are the address, let us say last 4 bits are my host. So, there can be 16 hosts, 4 bits, what it says; the beginning address in each block must be divisible by the 16. See any address where the last 4 bits are 0, this will obviously be divisible by 16, because you look at the weight $2^0$, $2^1, 2^2, 2^3$ here, the next bit position the weight is $2^4$, 16.

So, it is clearly divisible by 4, because this is all 0. So, a block that contains 16 addresses can never have the starting address as this, because this is not divisible by 16, but you can have 64, because 64 is divisible by 16. So, just by looking at the address, you can say that it is correct or not, whether this can be the starting address in a CIDR block or not ok, fine.

(Refer Slide Time: 25:44)

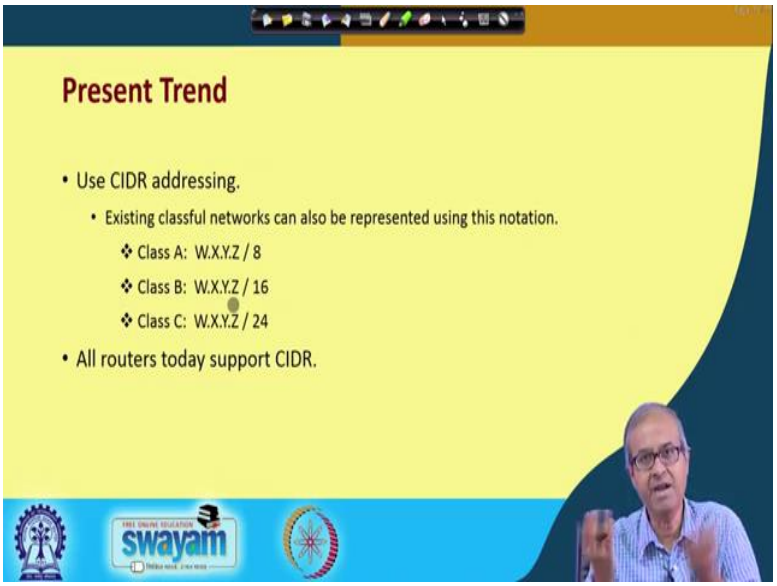



So, let us take a very specific example; suppose, an organization is assigned a CIDR network like this. Nowadays, you see when you ask for an address, you will not be given an IP address class A, B or C, you will be given a CIDR address like this 144.16.192.40/29. Now, let us try to understand, what is the meaning of this?

144.16.192.24 is this and 29 means; first 29 bits are the address, last 3 bit are the host. So, last 3 bit can go from 0 0 0 up to 1 1 1. So, this starting address will be this, the ending address will be this. So, starting address will be what; you can just compute decimal whatever, let us try to compute 128, 60, 144.24.192.24 like this.

So, the last address will be something 144.24.192.31. These are the range of addresses. There are 8 addresses in the block right. So, if you are given a CIDR address, you can calculate the start address, end address and number of addresses in the block.

(Refer Slide Time: 27:22)




And in fact today, almost all routers the way the routing tables are configured, they use this CIDR convention for addressing, class A, B, C is no longer used, because it is very wasteful of IP address. See your organization may be having only 10, 20, 30 computers, but you are taking a class C address; let us say and you are blocking all 255 addresses ok. So, it is not very efficient in terms of utilization.

So, CIDR is very convenient, but the equivalent class A, class B, class C, if you have some network, class A you can represent like this slash 8, class B. You can represent as slash 16 and class C as slash 24. So, CIDR is a generalization of the so called class full addressing ok. You can use the class A, B, C and more than that, this is the idea and all routers today, support CIDR. So, with this we come to the end of this lecture, where we have looked at the various aspects of this IP addressing, IP subnetting and various ways of creating subnets using VLSM and CIDR.

Thank you.