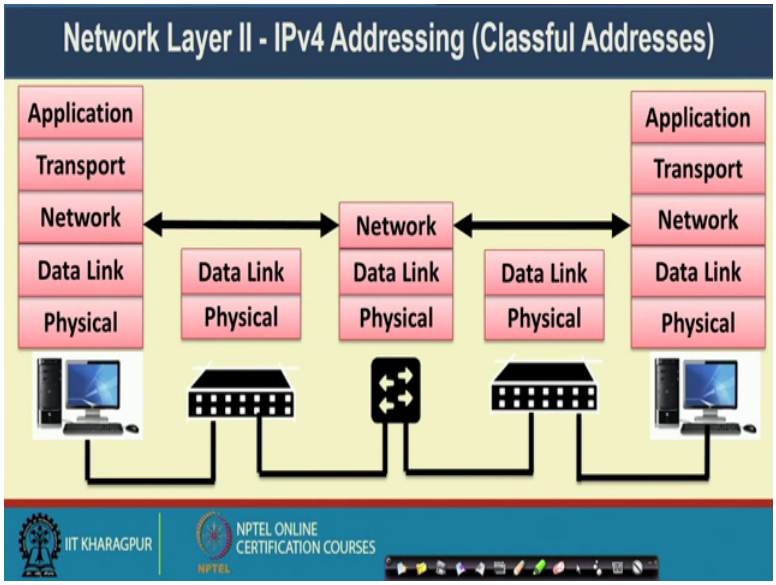
Computer Networks And Internet Protocol
Prof. Sandip Chakraborty
Department of Computer Science And engineering
Indian Institute of Technology, Kharagpur

Lecture – 27
IP Addressing (IPv4) I – Classful Addressing

(Refer Slide Time: 00:34)

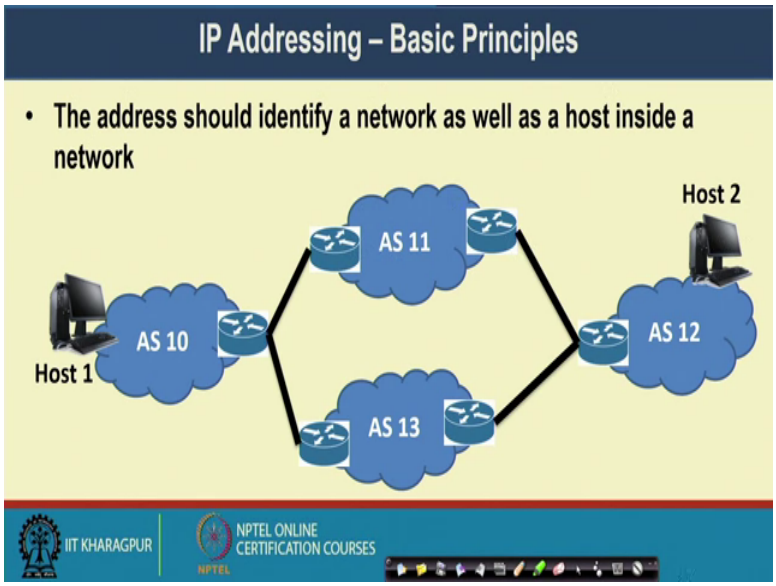


Welcome back to the course on Computer Network and the Internet Protocols. So, in the last class, we have looked into the basic internet architecture or in the terms of autonomous system and internet service providers. And we are discussing about the requirement for network addressing.

So, in this particular lecture, we will look into that how will you uniquely identify a particular host inside the network using this concept of IP addresses. So, here we look into the IP version 4 or IPv4 as we call it in short. So, this internet protocol or the IP traditionally or the initial version of IP was IP version 4, and now it is also most of the time we use IPv4.

And from IPv4, there was another version of IP which people have explored, which is not generally used, but in many of the cases or in many of the countries that particular version of IPs are also being used, so that is being called as IP version 6 or IPv6 in short. So, we will first look into IPv4 in details, and then we will go to go to the details of IP version 6 or IPv6.

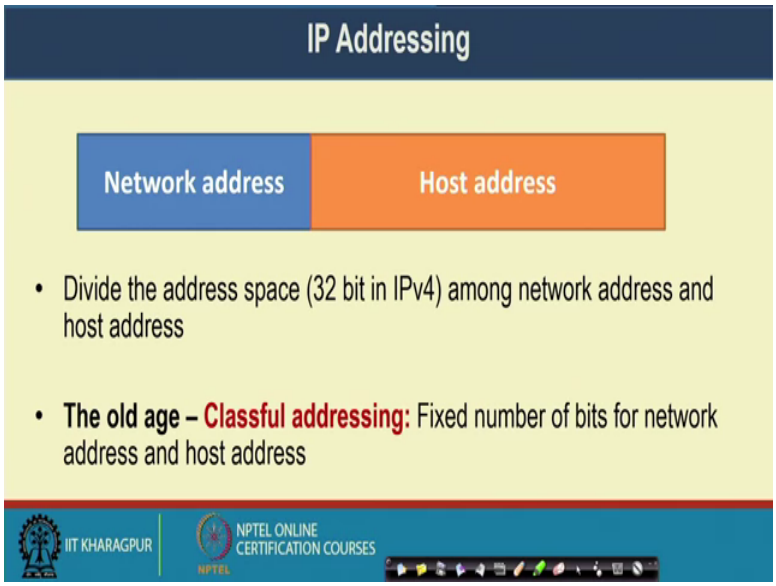
(Refer Slide Time: 01:36)



So, in IPv4, so let us look into that how a particular address is being done. So, as you are mentioning that the requirement for IP addressing is that the address should identify a network as well as an unique host inside that particular network. So, it need to identify the network as well as the host inside the network uniquely. So, you have a component for the network address, and you should have a component to uniquely identify a host inside the network, so the way we do the postal address.

And so, in case of a postal addressing, we use this name of the locations like this India inside that West Bengal, inside that Kharagpur or in the district term say west Midnapore, from there it is a Kharagpur, then from Kharagpur to IIT Kharagpur and then finally, Sandip Chakraborty. So, that way this entire hierarchical way is helped to uniquely identify a person in a postal mail. Similarly, this hierarchical way will help into uniquely identify a host in a network. So, let us look into that how this basic hierarchic of addressing is being done in IPv4.

(Refer Slide Time: 02:53)

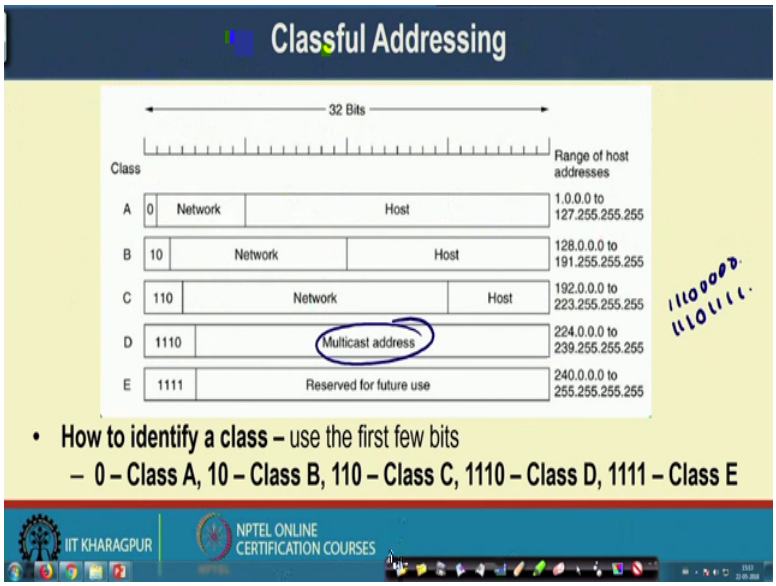


So, the whole idea is to break, this entire address space into two groups, one group is for the network address part, and the second group is for the host address part. So, in IPv4, we used 32 bits for identifying a address of a host. So, this 32 bit address is divided into the network address part and the host address part.

Now, the old idea was divide that how will you divide this entire 32 bit into the network address and the host address. So, the old idea was to use something called a classful addressing, where you have fixed number of bits for this network address component, and the remaining bits was for the host address component. So, you have a fixed division between the network and the host. And accordingly, the entire address space is divided into multiple classes, so that particular concept we used to call as classful addressing.

So, although nowadays we do not use this classful addressing concept, but this idea of classful addressing is useful for you to understand that what we are actually using nowadays. So, this entire philosophy of IP address is come from this classful addressing concepts. So, let us look into this classful addressing concept in little details.

(Refer Slide Time: 04:18)



So, in class full addressing, this is the broad concept that I have the 32 bit address, this entire 32 bit address space, I will divide it into the network address and the host address. And we have five different classes from class A, class B, class C, class D, and class E, so this five different classes of addresses.

Now, the first question comes that whenever you are dividing this entire address space into five different classes class A, class B, class C, class D, and class E, then how will you uniquely identify this individual classes. So, for that, what we do in classful addressing, in classful addressing, we use the first few bits.

So, if your first bit is 0, then it is a class A address. If the first two bits are 1 and 0, then it is class B address. If the first three bits are 1 1 0, it is a class C address. If they are 1 1 1 0, it is a class D address. And if it is 1 1 1 1, then it is a class E address. Now, interestingly here you can see that none of these words or none of these identifier for a class is a proper prefix of another. So, whenever you are trying to scan these 32 bits of bit stream, if you find out that the first bit is 0 that means, it is a class A address.

If the first bit is 1, then you look into the second bit. If the second bit is 0, then it is class B IP address. If the second bit is 1, then you look into the third bit. If the third bit is 0, then it is class C IP address. If the third bit is 1, then you look into the fourth bit. If the fourth bit is 0, then it is class D IP address. If the fourth bit is 1, then it is class E IP address, so that way just by standing the bits so, doing a bit shift operation, and then

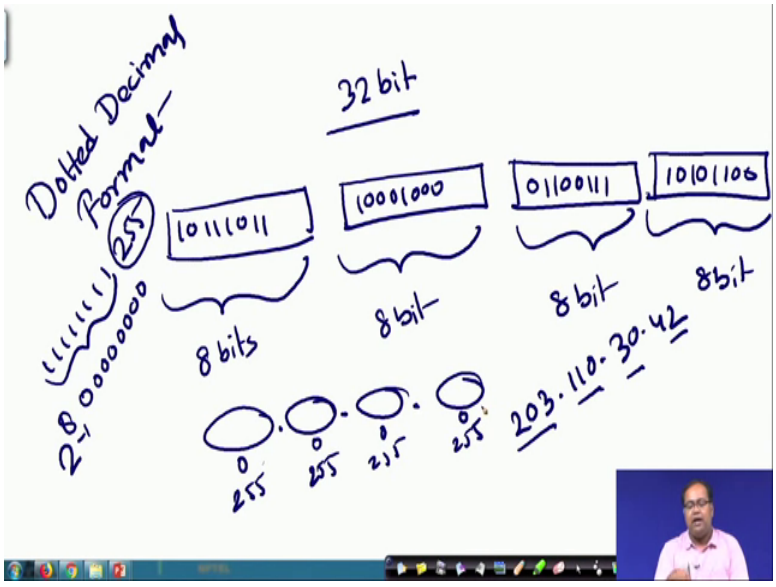
doing a logical (Refer Time: 06:13) you will be able to find out that what is the corresponding class of IP address that you are being used.

Now, for this five different classes of address, you have this kind of network address and the host address division part. But, even before going to that in IP based protocol, we have a concept of multicast. So, what is this, is multicast that some time it is required to send a packet not to a single destination, rather a group of destinations. So, you have a group of machines, which are being identified by a single address. And whenever you are trying to send a packet, the packet will be deliver to all the machines in that group.

So, it is similar to like a broadcast mail or sometime we call it as a multicast mail. So, in case of a multicast mail, say if you want to send it to all the B.Tech students or the CSE department, so your address would be to all B.Tech students, department of CSE, IIT Kharagpur, Kharagpur 721302, West Bengal, India.

If you are sending a letter by this address that means, a copy of that letter will be sent to all the B.Tech students, which are there in; who are there in the Computer Science Department of IIT Kharagpur, so that is the concept of multicast. And IP also uses this concept of multicast, and keep provisioning for using multicast IP addresses. So, this class D addresses are multicast addresses. And with this initial bits that the initial bits as 1 1 1 0. So, this multicast addresses start from 224 dot 0 dot 0 dot 0 to 239 dot 255 dot 255 dot 255.

(Refer Slide Time: 08:13)



So, just for this notation briefly, if you are not familiar with this particular notation, so what we do that this entire 32 bit IP address, this 32 bit IP address we divide into 8 bit chunks. So, if we divide into 8 bit chunks, we will have four different chunks of 8 bits. So, this is the first chunk, this is the it is a second 8 bit chunk, this is the third 8 bit chunk, and this is the fourth 8 bit chunk. So, every individual chunk is a 8 bit chunk. So, you have some 8 bit say 1 0 1 1 1 0 1 1, 1 0 0 0 1 0 0 0, 0 1 0 0 1 1 1, 1 0 1 0 1 1 0 0 something like this.

Now, in that the representation of the IP address, we write it in the dotted decimal format. What is this dotted decimal format, the dotted decimal format is that for this 8 bits, we represent this 8 bit binary in a 8 bit integer. So, we represent it in a 8 bit integer, and then put a dot, then again represent this as 8 bit integer, so this 8 bit integer, again a dot, the third 8 bit integer a dot and a final 8 bit integer. So that way an IP address looks like something like 203 dot 110 dot 30 dot 42. So, each of these are 8 bit integers.

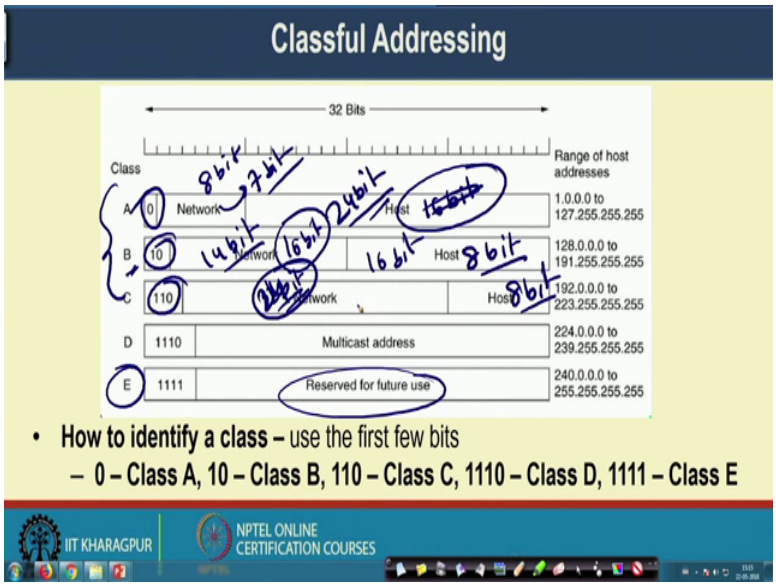
Now, if it is a 8 bit integer that means, a maximum you can have up to 2 to the power 8, so you can go up to that, so 2 to the power 8. So, if you if you start with all 1s, then that is the maximum. And the minimum is so, 1 2 3 4, 1 2 3 4, you can go from all 1's to all 0's.

So, if you have all 1's that means, it is it comes to be 255 2 to the power 8 minus 1, so it comes to be 255. So, these individual dotted decimals, they go from 0 to 255. So, the every individual chunk can go from 0 to 255, so that is the way we represent the entire IP address in the dotted decimal format.

Now, in this dotted decimal format, the multicast IP addresses they range from 224 dot 0 dot 0 dot 0 to 239 dot 255 dot 255 dot 255. So, 224 corresponds to these four g 1 1 1 0 followed by again four 0's. And 239 corresponds to 1 1 1 0, so that means, it is from 1 1 1 0 0 0 0 0 that would be the first chunk dot the remaining things, then 1 1 1 0 1 1 1 1, so that corresponds to 239. So, it moves from 224 to 239 that is the multicast use.

This class E IP addresses, they are reserved for future use, they are not normally used. So, it is from 240 dot 0 dot 0 dot 0 to 255 dot 255 dot 255 dot 255. So, they are reserved for future use. The other three classes of IP addresses class A, class B, and class C, they are divided into the network address and the host address part.

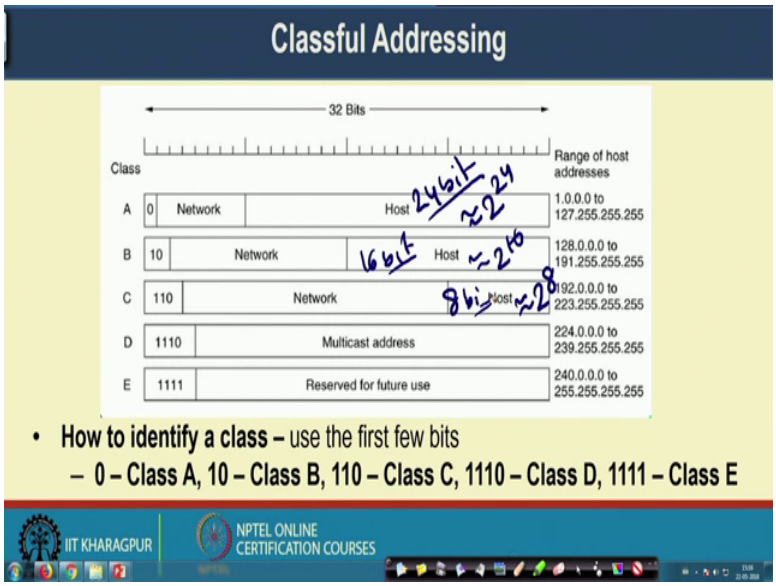
(Refer Slide Time: 12:06)



Now in case of class A IP address, we have 24 bit in case of class A in case of class A, it was 24 bit host address. And 8 bit of network address out of which 1 0 was reserved for denoting class A, so you have a total of 7 bit. In case of class B IP address, you have 16 bit of host address, and then 16 bit for the network address. So, out of this 16 bit, two bits are reserved for denoting it as a class B, so you can have a total of 14 bit.

In case of class C IP address, you have 8 bit of host address. So, whenever you have a 8 bit of host address in the network address part, you can have 32 bit. Out of this 32 bit sorry you have 24 bit. Out of this 24 bit, you have 3 bits results. So, whenever you have 3-bits result, the remaining bits you can use for the network IP part.

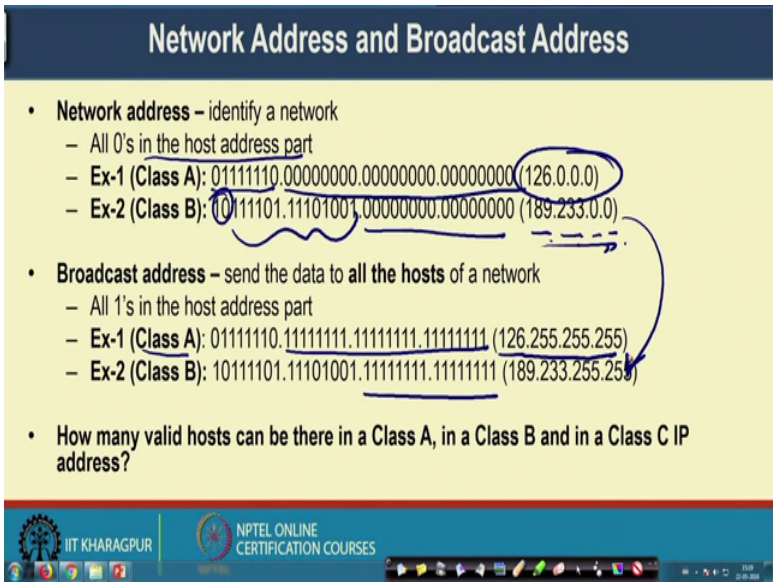
(Refer Slide Time: 13:22)



Now, in this case, you can see that class A, it supports maximum number of hosts, so class A supports maximum number of host. So, the supported host can be as high as so, if we are using 24 bit host address for class A. So, the supported number of host can be as high as 2 to the power 24. Obviously, it is not exactly equal to 2 to the power 24, we will later on look into that there are certain reserved IP addresses.

So, it is slightly less than 2 to the power 24, but close to 2 to the power 24. So, in case of class A you can support close to 2 to the power 24 number of host. In case of class B, you can support close to 2 to the power 16 number of host because you have a 16 bit of host address. In case of class C, you can support around 2 to the power 8 number of host close to the power 8 number of host because you have a 8 bit of host address, well.

(Refer Slide Time: 14:12)



So, the question is that this network address, it is used to identify a network. And this host address part it is used to uniquely identify a host inside a network. Now, we have in every individual class of IP addresses, we have two special address; one address we call as the network address, and the second address we call it as a broadcast address.

So, the network address is the part when where we have all 0's in the host address part. So, it is used to uniquely identify a network. So, a class A network is identified as all the 0's in the host part. So, in case of class A, you will have 24 number of 0's in the host part; and you will this 8 bits at the network part with this initial reserved 0.

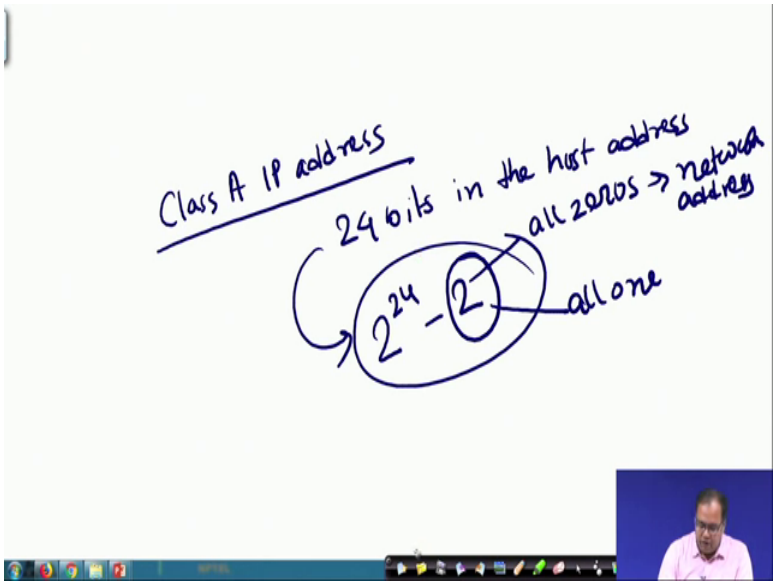
So, this entire thing which is in dotted decimal format 126 dot 0 dot 0 dot 0 that uniquely identify a class A network. Similarly, a class B network, you have all these host address part the 16 bits they are equal to 0. So, they 0's and the initial two bits are 1 0, then the remaining part your network address part. So, in the dotted decimal format it is 189 dot 233 dot 0 dot 0 that denotes class B network address.

Similarly, we have a broadcast address. So, a broadcast address means if you send the packet, send the IP datagram with that particular address as the destination address. So, with this broadcast address at the destination address, that means, all the host in that network will get that packet, so that is why we call it as a broadcast address.

So, in case of broadcast address, the broadcast addresses are denoted as all 1's in the host address part. So, in case of broadcast address, you have all the 1's in the host address part. So, in case of a class A broadcast address, you have so you it corresponds to this 126 dot 0 dot 0 this dot 126 dot 0 dot 0 dot 0 this network address, you have these all the 1's in the host address part that means, 126 dot 255 dot 255 dot 255 as the broadcast address.

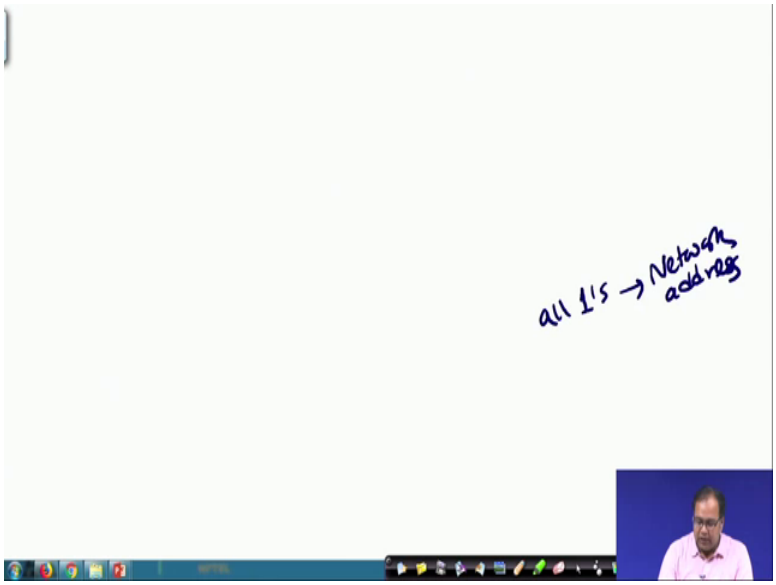
Similarly, for the class B network, 189 dot 233 dot 0 dot 0 if you put all 1's at the host address part that means, it corresponds to the broadcast address for this network. So, the broadcast address for 189 dot 233 dot 0 dot 0 is 189 dot 233 dot 255 dot 255, so that way for every individual network address you should not put all the 0's in the host address part or all the 1's in the host address part. So, these two are being omitted, because these two are being omitted. So, this all 0's and all 1's are not used as a host address. So, if you just take a class A IP address, and if I ask you that how many number of valid host can be there in case of a class A IP address. So, we can compute it like this way.

(Refer Slide Time: 17:41)



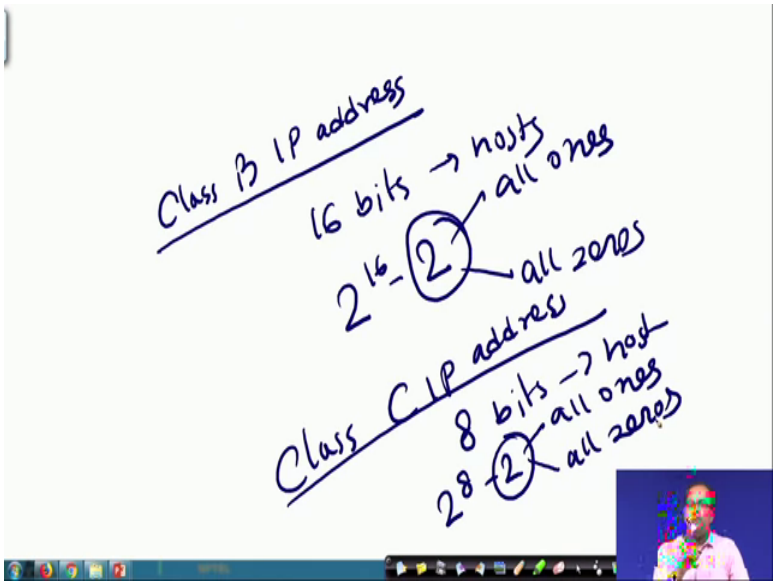
Say for a class A IP address. I have 24 bits in the host address part. Whenever you have 24 bits in the host address, that means, your number of valid host for a class A IP address is 2 to the power 24 minus 2. So, these 2's are we are omitting all 0's and all 1's in the host address part. So, all 0's which is to denote the network address.

(Refer Slide Time: 18:35)



And all 1's which is to denote all 1's to denote the network address. So, these two are omitted. Now, in case of so that was for a class A IP address. So, in case of a class A IP address we are omitting all 0's and all 1's. So, we have a 2 to the power 24 minus 2 number of valid hosts in a class A IP address.

(Refer Slide Time: 19:09)



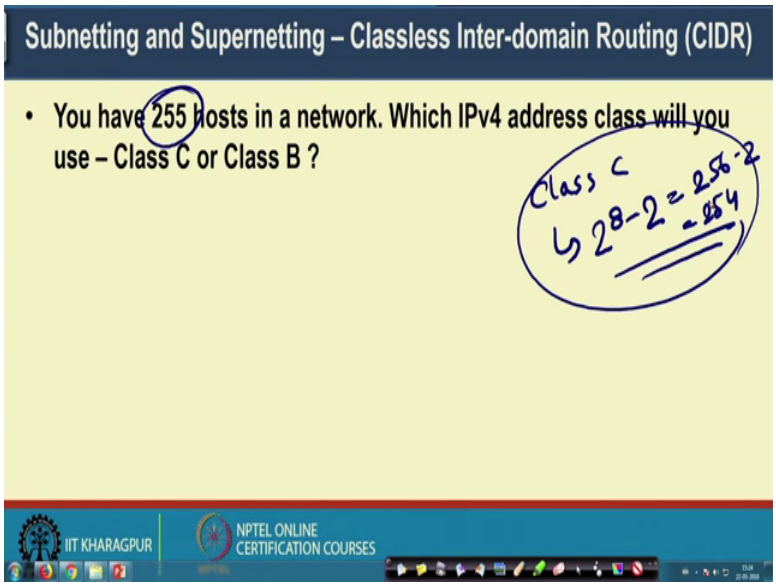
Similarly, if you go for class B IP address, in a class B IP address, you have 16 bits for the hosts, so; that means the number of valid hosts are 2 to the power 16 minus 2. Again

for these two we are omitting all 1's which is the broadcast address; and all 0's which is the network address.

For a class C IP address, you have 8 bits in host. So, because you have 8 bits in host, so the number of valid address is 2 to the power 8 minus 2. So, these 2 is again omitting all 1's and all 0's. So, every time for a particular network address, we should not use all 0's at the host address part or all 1's at the host address part, because these two denotes the special addresses of the network address and the broadcast address.

So, if all 1's at the host address part is a broadcast address, where the packet is being forwarded to all the host in that network. And in a in case of a all 0's that is a special address which is used to denote that particular network. So, the utility of this network address we look into that when we discuss about this routing procedure.

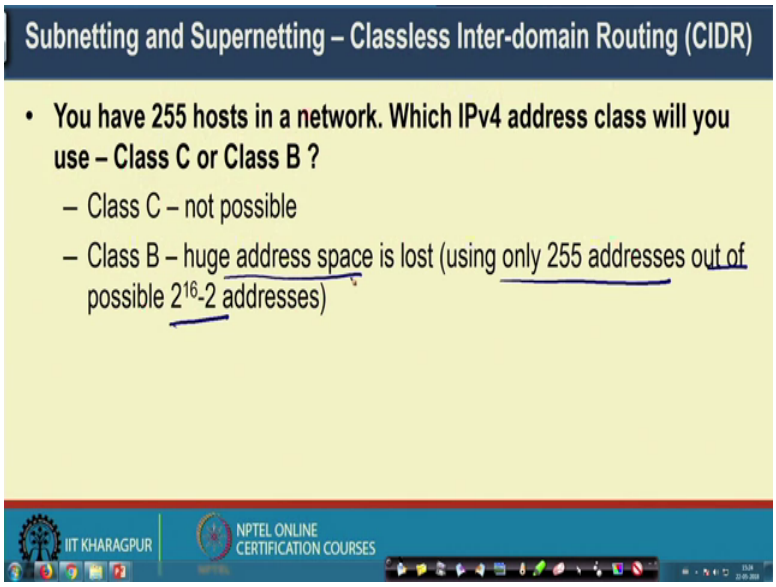
(Refer Slide Time: 20:52)



Now, one interesting question say you have to 255 number of host in the network. Now, the question comes that which IPv4 address class you should use. So, whether you should use a class C IP address or you should use a class B IP address. Now, if you look into a class C IP address in case of a class C IP address, you have 8 bits in the host pace. So, for a class C IP address, your number of valid host is 2 to the power 8 minus 2 which is equal to 256 minus 2 that is equal to 254. So, you have 254 number of valid hosts.

So, whenever you have 254 number of valid host in case of a class C IP address, and you want to support 255 number of host, obviously, we will not be able to support that with a class C IP address, so that class C IP address is not possible in this case.

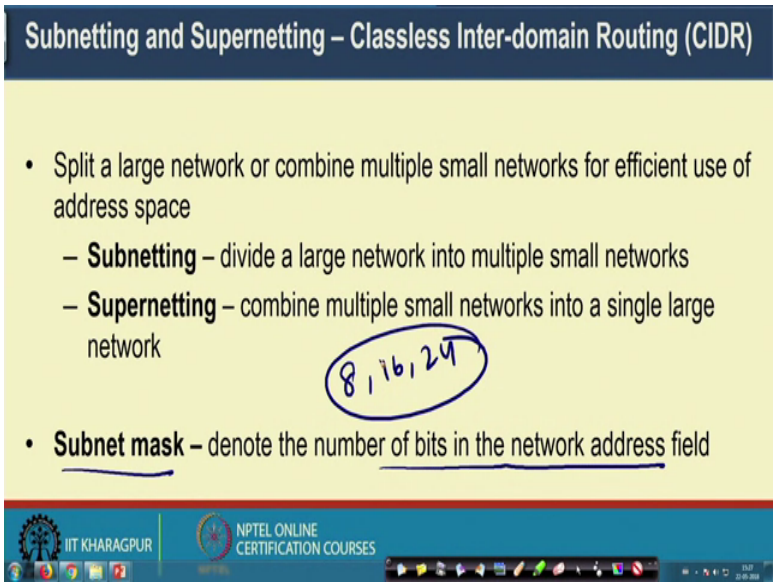
(Refer Slide Time: 21:52)



But, if you use a class B IP address, in case of a class B IP B IP address, you can support 2 the power minus 16 number of different host, but here you are just using 255 addresses. So, you are using only 255 address, in 255 different addresses out of possible 2 the power 16 minus 2 addresses, so that is you are losing or you are wasting a huge address space. So, that was the major problem with the classful IP address that was initially designed as a part of IPv4 addressing mechanism.

So, that is why from this classful addressing we are moving towards a direction which we call as the classless addressing or it is recently called as classless inter domain routing or CIDR. Now, the idea of CIDR is that you can split a large network into multiple small networks or you can combine multiple small networks together to have a larger network. So, that you can provide a handful of IP addresses to the hosts inside that network.

(Refer Slide Time: 23:09)



So, for that we have these two different concepts sub netting and super netting. So, the idea of sub netting is to divide a large network into multiple small networks and a idea of super netting is to combine multiple small networks into a single large network. So, this concept of sub netting and super knitting together they form this concept of classless inter domain routing or the CIDR.

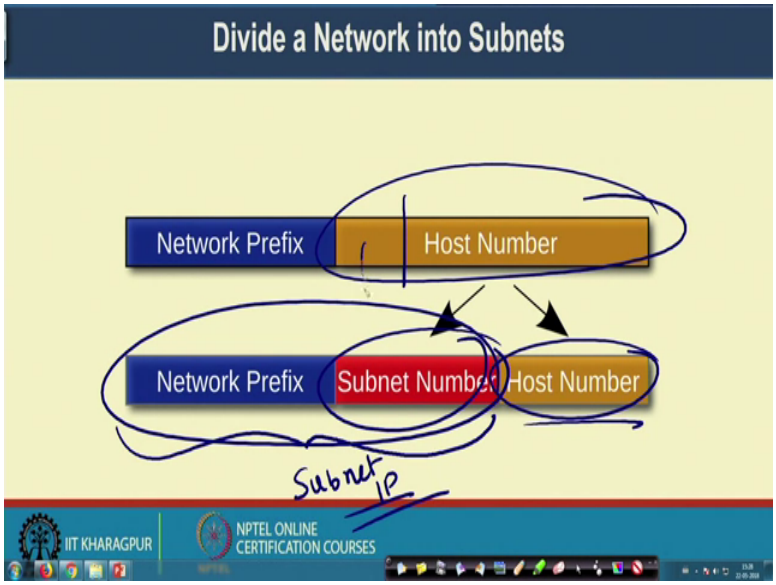
So, the CIDR is the concept used for the routing mechanism by utilizing this classless addressing scheme that we will look later on. But the idea here is that rather than binding the class boundary at 8 bit, 16 bit or 24 bit, can I use something in middle. So, can I combine multiple smaller subnets together to form a larger subnet, which we call as super netting or can I break a large subnet into multiple small subnet and then allocate IP addresses or 1 class of IP address to individual subnets so that is the concept of sub netting.

So, this concept of sub netting and supernetting leads to another thing like now we do not have a fixed class boundary. Whenever do you do not have a fixed class boundary, you need to have another information to determine that what is your class boundary. So, to determine the class boundary we used the concept called the subnet mask. So, this subnet mask it denote the number of bits in the network address field.

So, right now you are not going to use this 8, 16 or 24 bit fixed numbers in subnet mask rather the things are variable, because the things are variable your subnet mask actually

determining that how many numbers are there in your address space which is determining a subnet or the corresponding network IP address.

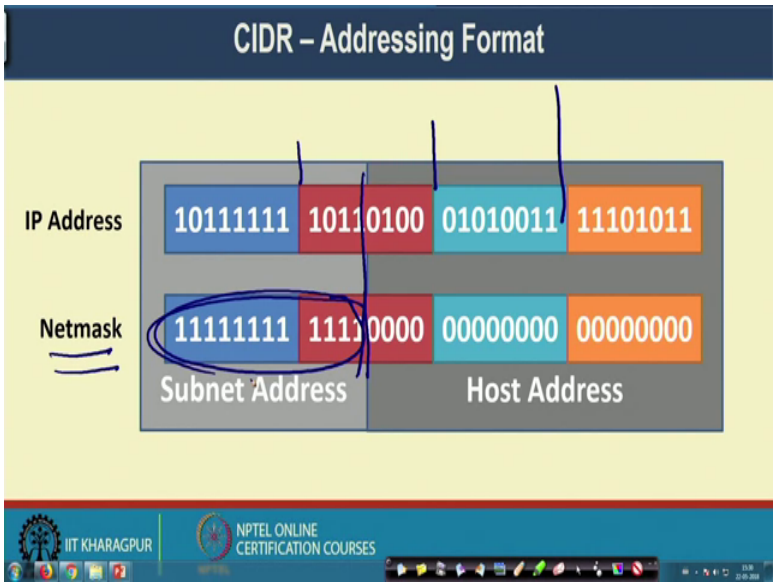
(Refer Slide Time: 24:59)



So, let us look into the entire thing. So, in case of your classful IP addresses, you had the network prefix along with the host number. So, this entire host number space is now divided into subnet number and the host number. So, this original network prefix from classful addressing and a subnet number that together gives you the subnet IP. So, this subnet IP is the IP of the network on which your machine belongs to.

So, now we are not using this fixed networks rather we are saying that a network consist of multiple subnets in a hierarchical fashion. So, the subnets are being combined together form a network and that network work as a subnet in the next layer, so that way it is multiple subnets are there, they are again getting combined and forming another set up another network, and that hierarchical fashion is going on. And this entire network prefix and the subnet number that forms this entire team forms your subnet IP and then you have the host number field. So, we are taking certain bits from the host numbers to denote the subnet number.

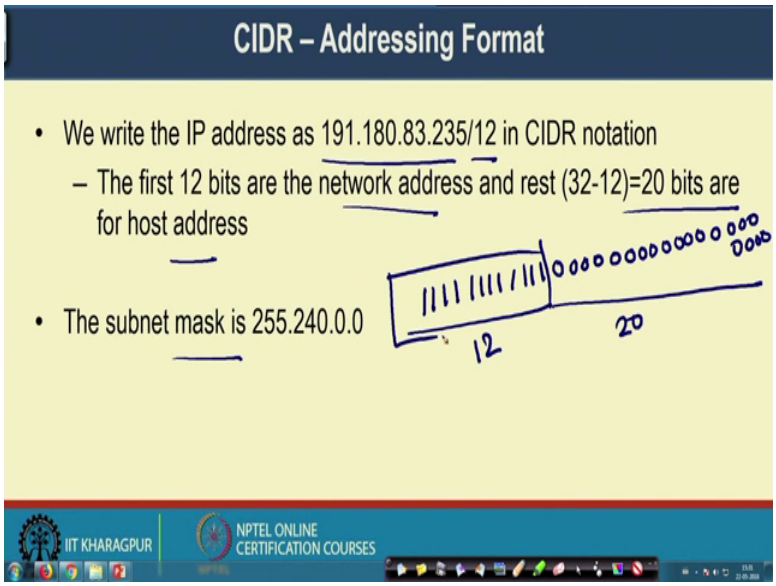
(Refer Slide Time: 26:16)



So, here is one example. So, in case of your IP address say these are this is your IP address, in this four 8 bit chunks. And as I mentioned that you require this netmask or subnet mask to determine that how many number of bits are there to denote your network IP or the subnet IP.

Now, we use the term network and the subnet interchangeably. So, you have this subnet addressing part. So, this subnet mask determines that well, the subnet mask is again a 32 bit binary, where there are few consecutive 1's and then few consecutive 0's. So, these few consecutive 1's determines that well up to this part is your subnet address. So, if you think about a class A IP address, in case of class A IP address, this was your network address; in case of plus B this was your network address boundary; in case class C, this was your network address boundary. Now, we are not using those fixed boundary rather a variable boundary in that variable boundary this subnet mask the where we have all 1's. So, this all 1's denote that this many number of bits are your subnet IP belongs to that determines your subnet IP.

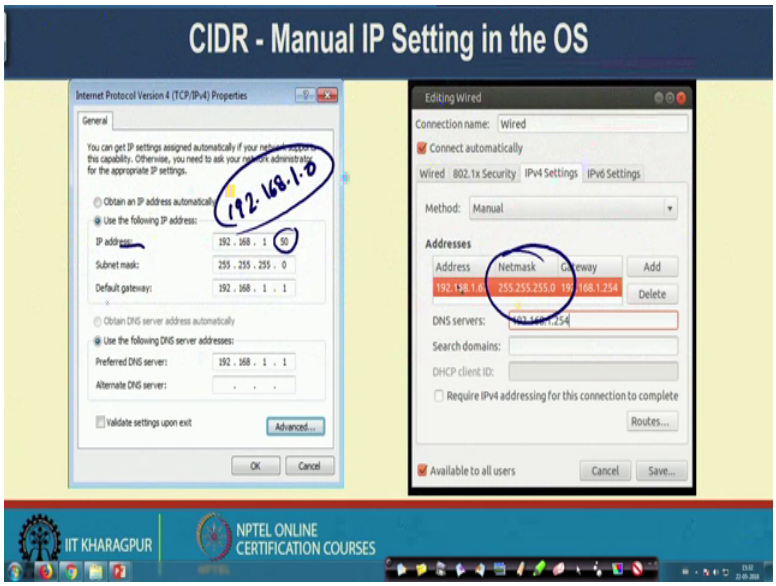
(Refer Slide Time: 27:54)



So, in CIDR addressing format, we write the IP address in this format. So, we have the IP address in the dotted decimal format followed by slash some number. So, this number determines that how many bits in the subnet mask are 1, so that means, if I my address is 191 dot 180 dot 235 dot slash 12; that means, the first 12 bits are the network address and the remaining 20 bits are the host address.

So, the first 12 bits of network address means my subnet mask would be the first 12 bit will be 1; and the remaining bits will be another 8 bits remaining bits will be 0. So, I will have 12 number of bits first 12 number of bits as 1's in the subnet mask; and remaining 20 number of bits are 0's. So, this determined that well the first 12 bits denotes my subnet IP.

(Refer Slide Time: 29:07)



So, in case of CIDR if you have done this manual IP, manual IP setting in different operating systems, so you have to provide the IP address and the corresponding subnet mask. And you will see that here the subnet mask is 255 dot 255 dot 255 dot 0 that means, that 24 bits the first 24 bits are the subnet IP; and the remaining 8 bits are used to denote the host address.

So, in this particular IP address, from this particular IP address, you can determine that because this first 24 bits are my network IP so the network IPs 192 dot 168 dot 1 dot 0 under this network it is number 50 host is identified by this IP address so that is the beauty of the subnet mask. Similarly, whenever you are setting up the things in Linux you can also set it with this net mask field. So, this word subnet mask and netmask are used interchangeably. In Windows, we use the term subnet mask; and in Linux we use the term net mask.

So, that is the broad idea about the way you give allocate IP addresses to different machines. In the next class, we look into 1 specific example of this CIDR with subnetting and supernetting that given a IP address pole, how can you divide that IP address pole into multiple subnet and then allocate IP addresses to different host inside that subnet, that is that we will discuss in the next class.

So, thank you all for attending this class today.