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

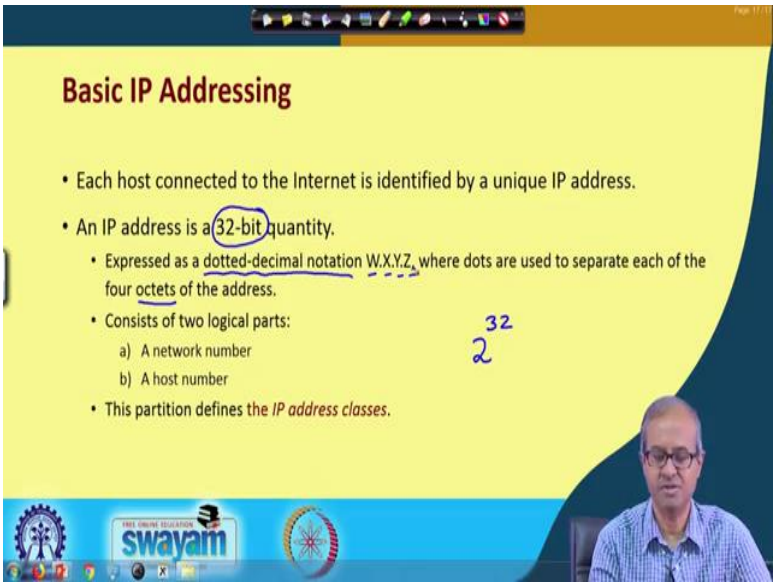
Lecture - 07
IP Addressing and Routing (Part II)

So, let us continue with our discussion on IP Addressing and Routing. If you recall, in our last lecture, we talked about how packet fragmentation and reassembly happens in IP.

(Refer Slide Time: 00:32)

Now, in this lecture, in the part II of it, here we shall be talking about some aspects of IP addressing and the concept of IP address classes. Let us see.

(Refer Slide Time: 00:42)



Well, when you talk about IP addressing we need to understand what is the basic role of IP. IP is a protocol of the TCP/IP family that works at the network layer level, and IP ensures some kind of uniqueness of each node or computers that are connected to the Internet.

At the level of IP, we assign some kind of address to every computer or host and that address is supposed to be unique, because it is very clear, if it is not unique, if you are sending a packet to some other computer, and if there are multiple computers with the same IP address, there will be confusion, the routers will not know where to forward and therefore, this uniqueness in address is very important ok.

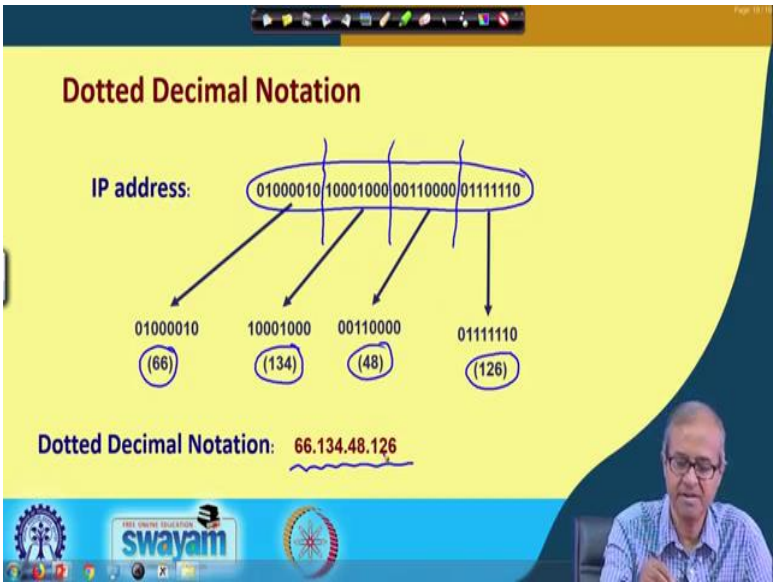
So, each host connected to the internet, it is very important that it has to be identified by unique IP address. And the way IP address is defined, it is a 32-bit quantity. So, you can clearly see, you can have 2^{32}, so many different unique addresses which is about 4 billion. You can have 4 billion such IP addresses that are unique right.

Now, here I will take an example, this 32-bit number or this address, this is a little difficult to remember 0 1 0 1 1 0 1 1, 32 binary digits. So, to make it little concise, there is something called a dotted decimal notation where you divide the 32-bits into 4 bytes which are called octets; and each of this 8 bit quantities, we express in decimal. And you write them as the decimal numbers, W X Y Z separated by dots. This is called the so called dotted decimal notation.

Now, we shall see that this 32-bit network address that we are talking about, there are two parts in this address. The first part identifies a network, there are many networks in the world; Internet is essentially a network of networks. So, the first part will identify which network I am talking about. And the second part identifies a host.

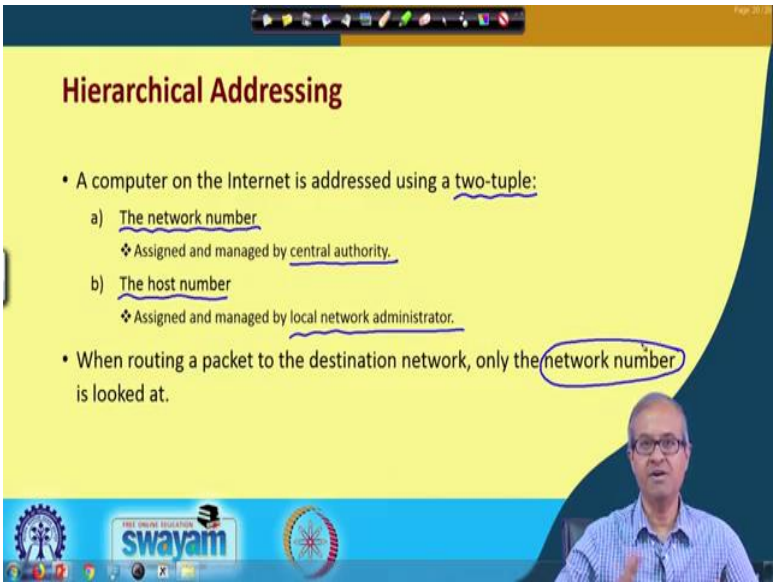
This is somewhat similar to the way we specify the address of our house, we specify our country, we specify a city, we specify a street, then we specify a house number. Similarly, here we specify a network, and within the network which computer a host, which host ok. So, depending on the way this partitioning is carried out, we can define these IP address classes, this we shall see.

(Refer Slide Time: 03:58)



Now, the dotted decimal notation, let us taken an example here. Suppose, here we have 32-bit IP address, you see there are 32-bits, this we have divided up into 4 8-bit chunks, octets; and each of these 4-bits chunks, we are expressing in equivalent decimal ok. And this 32-bit number, we are expressing in a concise form like this 66.134.48.126. This is so called dotted decimal notation which is much easier to write, express and also remember ok. This is the basic idea.

(Refer Slide Time: 04:49)



Now, this hierarchical addressing, I have already talked about that the way we address a computers in two parts, address of the network and address of the host. So, here I am just repeating it again. So, every host or computer that is connected to the Internet is identified by two things, a two tuple, first one I mentioned already the network number.

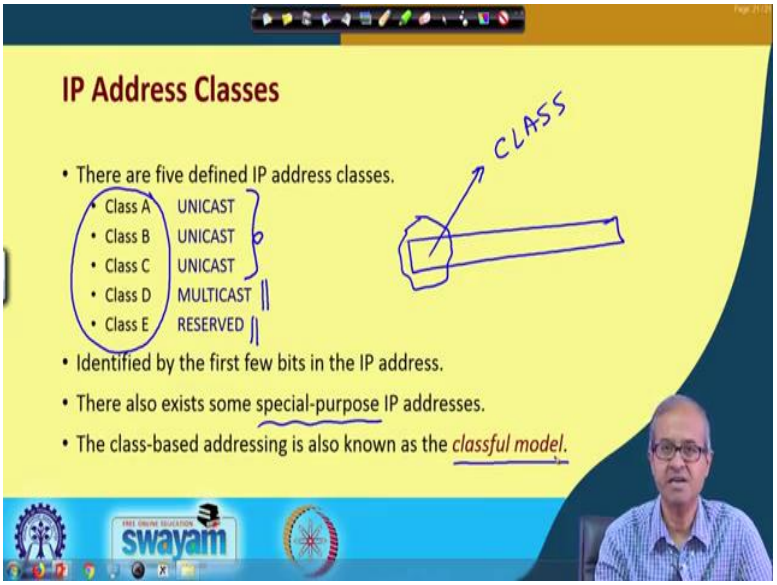
Now, network number has to be unique, all the networks in the world must be assigned a unique number, each of them must be unique. So, this has to be done by some central authority. So, there has to be some central authority which manages this network numbers. And whenever you require to set up a new network, they will give you a unique number, this is the idea.

And the second part is the host number within that network ok. This of course, can be managed by the local authority. Suppose, in your organization, you have a unique network number, but inside you have 1000 computers, you can number them 1, 2, 3, 4, 5, 6 up to 1000 that is up to your local administrator to manage that numbering ok. So, the host numbering can be done by the local network administrator.

And now when the routers forward, route the packets, they do not look at the host part, they will only look at the network number part, because the first task of the router will be to send the packet to the correct network. So, only the network number is looked at and once the packet reaches the correct, the correct network, the router of that network will

receive that packet and inside the network it will forward it to the correct host. This is how routing of the packet occurs.

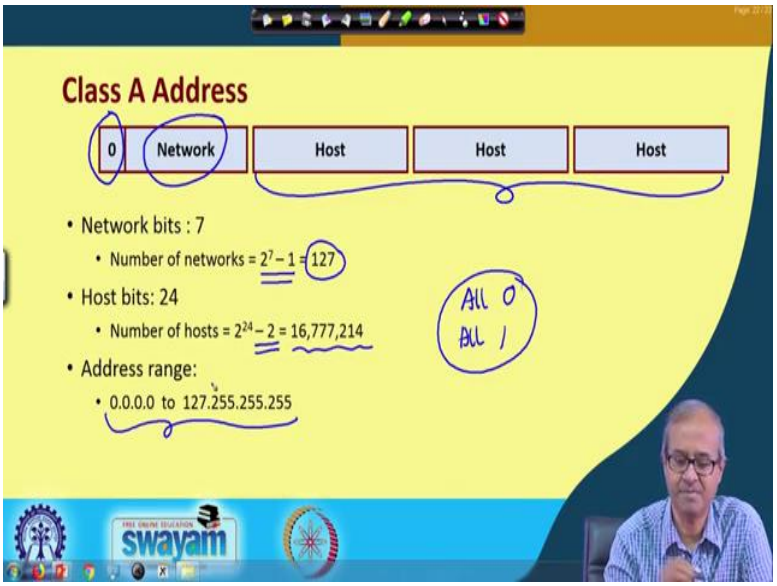
(Refer Slide Time: 07:00)



Now, talking about the IP address classes, there are five defined IP address classes, where class A, B, C are used to assign addresses to individual computers. They are called unicast addresses. unicast means address of a single node. Class D is used for multicast; I want to send a packet to multiple computers at the same time, I can use class D address. And class E is reserved, you can use it for some special purpose if you want.

Now, which class a particular IP address belongs to. Suppose, I give you an IP address like this, 32-bit IP address. Just by looking at the first few bits, you will be able to identify which class the address belongs to ok; we will see how. And we shall also see later there are some special purpose IP addresses which serve some or which have some special meaning ok. And this kind of IP addressing where we define the classes is sometimes also referred to as the classful model of addressing fine.

(Refer Slide Time: 08:29)

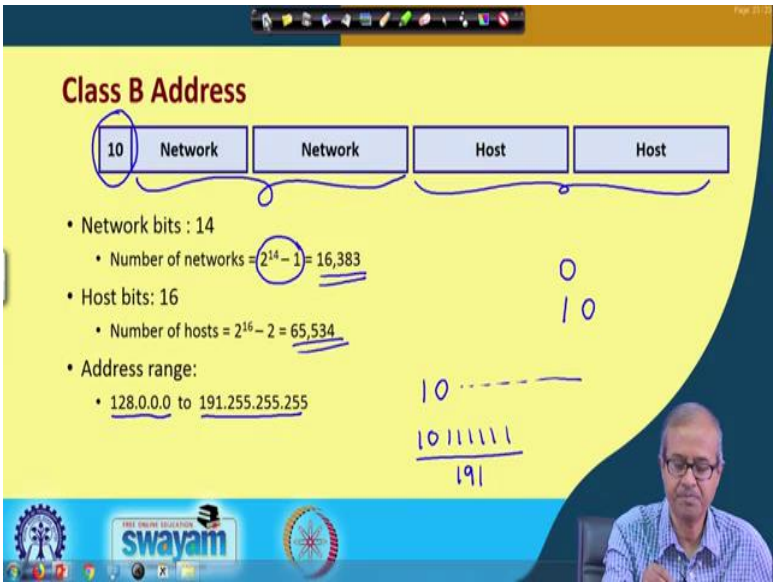


Let us look at the class A address first. In class A address, the way we identify that this is a class A addresses, that it must start with 0, any address that starts with 0 is identified as a class A address. The next 7 bits identify the network, the last 24-bits identify the host within a network, because there are seven network bits that can be 2^7 combinations.

Well, out of them there is one special, all 0 is not used it, taking away the all zero combination there can be 127 possibilities, there can be 127 class A networks. And inside each such network there are 24-bits in the host part, 2^{24} combinations are possible, out of that two of the combinations are used for some special purpose, we will see later the all 0 and all 1 combinations.

So, if you take away these two, this become $2^{24} - 2$ which is of the order of 16 million. So, this is used for very large networks up to 16 million computers in a single network right. And if you look at the address range, the first bit is 0, and you can have all 0. So, 0.0.0.0 and 0 followed by all 1, it comes to 127.255.255.255. This is in dotted decimal notation. So, just by looking at the address, you can know that if it is in this range, this will be a class A address ok.

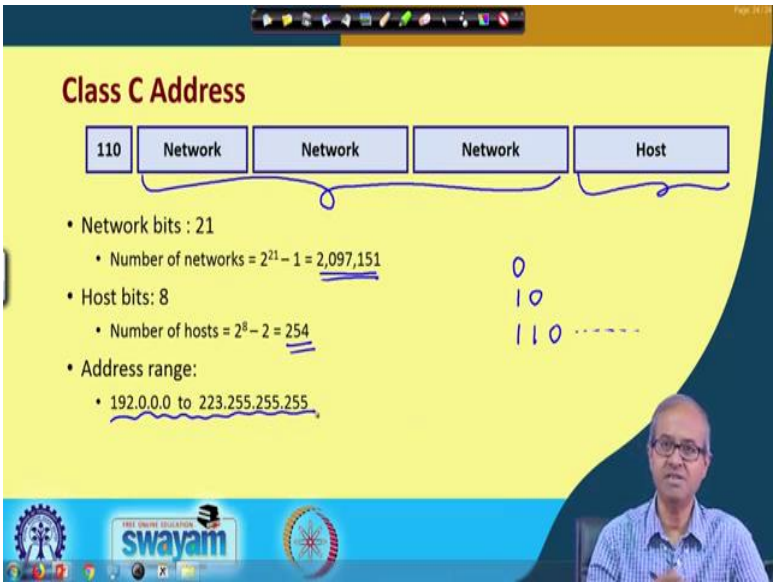
(Refer Slide Time: 10:29)



Now, let us look at class B; class B is uniquely identified again by the first few bits, by the first 2 bits. Anything starts with 0 means class A; anything that starts with 1 0 means class B ok. Now, here we have 14-bits for your network, 2-bits are left a side and 16-bits for the host. So, you can have again similarly $2^{14} - 1$ which is about 16000 networks. And each network and have $2^{16} - 2$, about 65,000 computers. This is how class B networks are.

And if you again try to look at 1 0, starting with 1 0 and remaining all others can be all 0 to all 1s. So, the range will be 128, see 1 0 and all 0, the first byte will be 128, all are 0.0.0.0 up to 191, 1 0 followed by 6, this is 191, 191.255.255.255. This is the range of class B addresses.

(Refer Slide Time: 11:53)

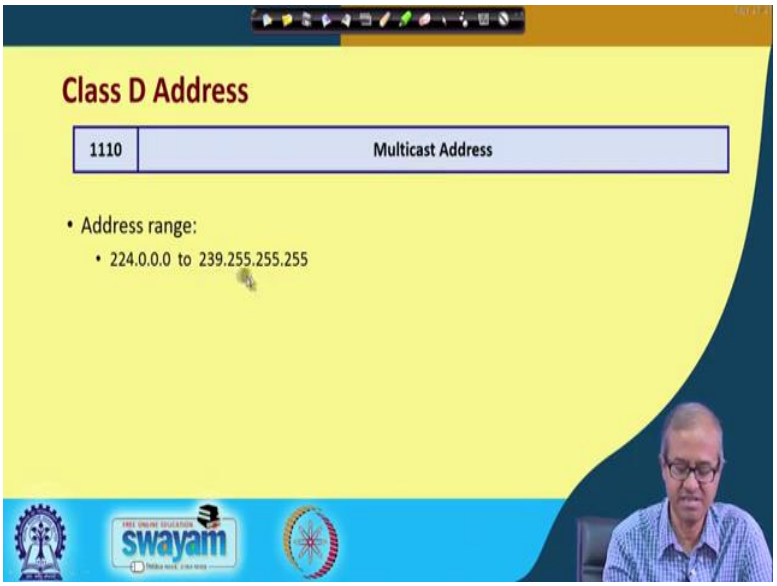


Similarly, let us look at class C. Well, for class C, again anything starting with 0 is class A; starting with 1 0 is class B; starting with 11 0 is class C. So, you see there is some kind of uniqueness, just by looking at the first few bits, you will be able to identify which address class it is ok.

Now, in class C, you see there are 21-bits you are using for networks and only 8-bits for the host, that means, networks where relatively fewer number of computers are there for such things, for such cases class C is most suitable. With 21-bits you can have about 2 million networks, and with 8 bits in the host, you can have 254 computers, hosts per network.

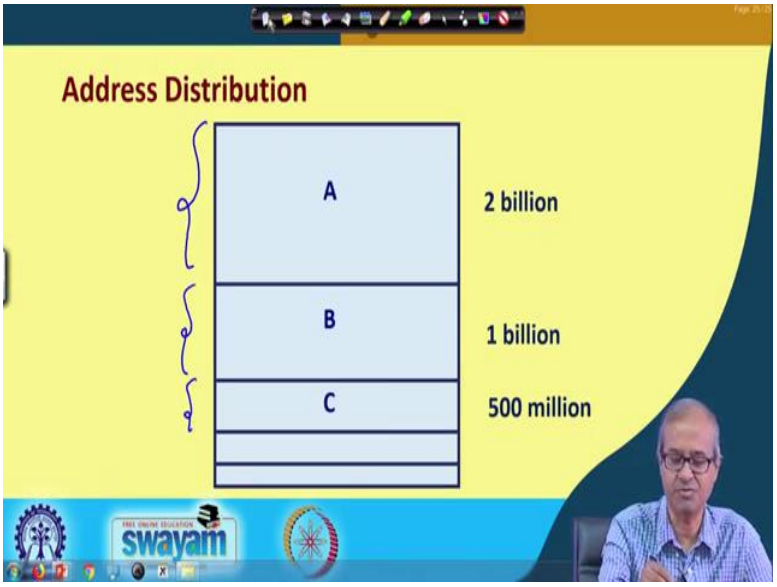
And again if you just expand 1 1 0 followed by all 0 to all 1, you can find this is the range of the IP addresses. So, just if you are given an IP address, just if you remember this numbers, by looking at the IP address, you will be able to know which address class this IP address belongs to.

(Refer Slide Time: 13:13)



Now, class D address starts with similarly 1 1 1 0, this is a multicast address as I said. So, if, so the network if you are sending a packet using this multicast address starting with 1 1 1 0, then the packet will be delivered to all the computers in that network, the idea is something like that. I am not going into detail. The address range similarly is like this.

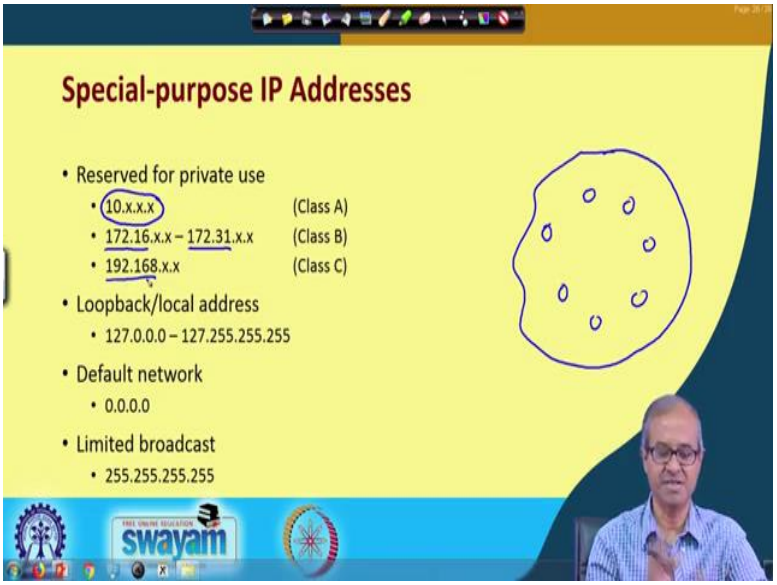
(Refer Slide Time: 13:40)



Now, address distribution is like this, you see class A networks are few in number, but in each network the number of computers can be huge. So, in terms of the total number of address, this class A occupies the maximum, followed by class B and finally, followed by

class C ok. This is the address distribution if you are interested to know, this is how it works.

(Refer Slide Time: 14:15)



Now, I mentioned that there are some special purpose IP addresses also which are used, which are reserved for some special purposes. First there are something called private IP addresses. Suppose, I have an organization; I want to use some computers inside my organization to communicate among themselves. I did not want or I did not need to have unique IP addresses which are not used anywhere in the world, because I am using only within my organization and boundary inside.

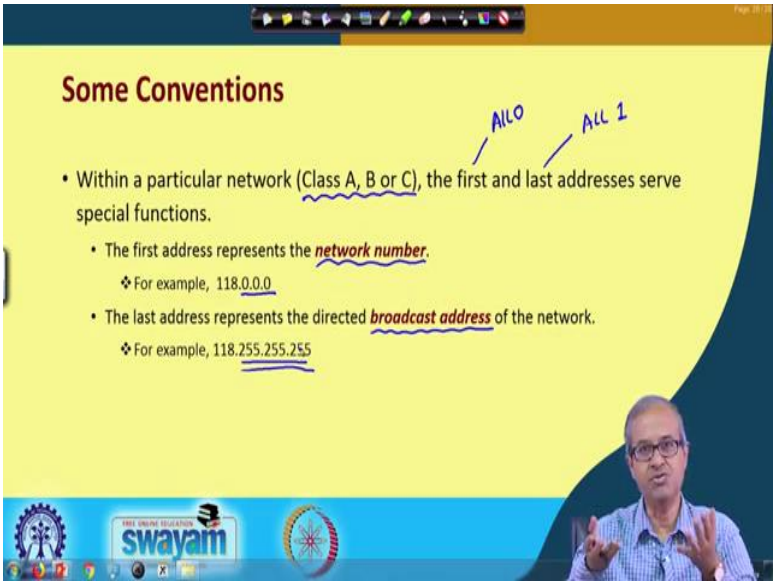
So, I can use something called private IP addresses which can be used by others also that is not supposed to be used, used publicly with other networks, only inside your network you can use this private addresses. Like for class A, this is identified as a private address, any address that started 10., 10. something that is a private class A IP address. Class B there are actually 16, 172.16 to 172.31, there are 16 such private class B networks which are identified as private. Similarly, for class C, this 192.168, this is a private class C network.

So, there are many cases while you use private addresses inside your organization, but when you are going out of the organization, you have use some kind of a network address translator or some kind of an address translation mechanism to get a unique address or a proxy server, you can access the outside world, this is how you work ok, all right.

Now, there is something loopback or local address, any address that starts with 127 that is assumed to be a local address, local address means, it never goes out of the network, it will remain inside, that is referred to as a local address ok. Suppose, even from your computer if you try to send a packet to 127. something, it will come back to your own computer, it will not go to anywhere else, that is referred to as a loopback, the local address.

Default network, any network address is 0.0.0.0, that is your default network. The current network is usually the default network, you can specify which is the default ok. And similarly if we use an address all 1s, all 255, it means limited broadcast, means broadcast within your present network. So, if you want to send a packet to all computers within your network, you can use this limited broadcast address ok. This is how the IP routers handle the packets by looking at the address where to forward, it will take a decision like that.

(Refer Slide Time: 17:40)



Now, some convention; now, I told you that for the host part there are two addresses which has special purpose the all 0 and all 1. The convention that is followed this as follows. For all of class A, B or C networks, the first and last addresses, first means as I had said the all 0 address, all 0 and the last address means all 1, they serve special purpose. The all 0 address specifies the network number like 118 is the address of the network. If you write 0.0.0 in the host part, this will identify the network 118.0.0.0 that is identified, this identifies the network. And if you write all one like this, this refers to the broadcast address of the network.

See, if you write an address as 118.255.255.255, the packet will be sent to the 118 network and it will broadcast to all the computers inside that network . So, these two all 0 and all 1 are used for special purposes. All 0 indicates the network which is particularly used inside the routers to maintain the routing table that we shall see later and all 1 is used for broadcast ok.

So, with this we come to the end of this lecture. Now, here we have seen some issues regarding IP addressing, in particular we looked at the IP address classes and so on. Now, in the next lectures, we shall be looking into some more detail on the TCP and UDP protocols, because these are the two very important protocols in the TCP/IP protocol suite that runs on top of the IP layer. They have different you can say functionalities, features and we shall be looking into some more details on that in our next lectures.

Thank you.